it management

Der Motor für Innovation
Mai/Juni 2025

INKLUSIVE 48 SEITEN
it security

DIGITALER ARBEITSPLATZ

Vom Wildwuchs zur Effizienz

Boris Ovcak, Campana & Schott

THOUGHT LEADERSHIP

AB SEITE 14
Aagon

AB SEITE 18
DriveLock

KI-CODE OHNE HALLUZINATIONEN

Mehr Zuverlässigkeit in der Softwareentwicklung

API-PLATTFORMEN

Rückgrat oder Innovationsbremse?

www.it-daily.net


e3mag.com
DEUTSCH
Information und Bildungsarbeit von und für die SAP®-Community
The global independent platform for the SAP® community
ENGLISCH
SPANISCH
La plataforma global e independiente para la comunidad SAP®
SAP® ist eine eingetragene Marke der SAP SE in Deutschland und in anderen Ländern weltweit.

EINE SYMBIOSE MIT ZUKUNFT

LIEBE LESERINNEN UND LESER,

haben Sie sich schon einmal gefragt, wofür eigentlich der ganze erzeugte Strom aus Windkraftanlagen genutzt wird? Und wussten Sie, dass diese Anlagen teilweise soviel Strom produzieren, dass er zeitweise gar nicht ins öffentliche Netz eingespeist werden kann?

Wenn ich aus meinem Fenster schaue, sehe ich 14 Windräder rund um meinen Wohnort verteilt. Tagsüber spaziere ich manchmal sehr nah an ihnen vorbei und ärgere mich, dass die so hässlich in der Landschaft stehen, nachts ärgere ich mich gelegentlich über das Brummen der Rotorblätter, aber meistens übersehe ich sie einfach.

Umso begeisterter war ich, als ich für diese Ausgabe einen Artikel erhalten habe, in dem es um eine weitere sinnvolle Nutzung von Windkraftanlagen geht: die Einbindung eines Rechenzentrums direkt in den Fuß eines Turbinenturms. Quasi zwei Fliegen mit einer Klappe schlagen: Zum einen wird die Energie direkt da genutzt, wo sie produziert wird, ohne Übertragungsverluste, und zum anderen werden dringend benötigte Rechenzentren in bestehende „Gebäude" integriert. Finde ich eine super Sache und sollte ruhig häufiger realisiert werden. Denn der Bedarf an Rechenzentren wächst nachweislich.

Für das Datenmanagement eröffnen sich dadurch ebenfalls neue Perspektiven. Diese dezentralen Knoten eignen sich ideal für Edge-Computing-Anwendungen oder regionales Backup. Gerade in Zeiten von KI eine clevere Idee!

Denken Sie mal darüber nach!

Herzlichst,

Carina Mitzschke | Redakteurin it management & it security

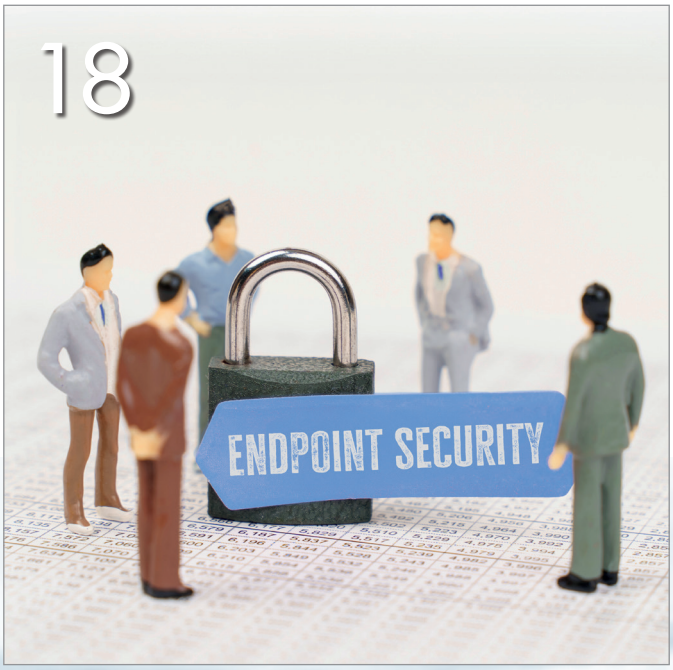
INHALT

COVERSTORY

THOUGHT LEADERSHIP

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

IT MANAGEMENT



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**

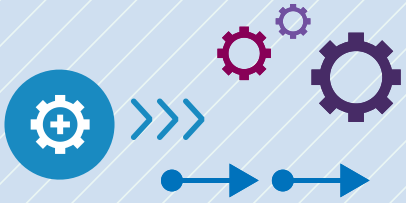
FÜNF MYTHEN ÜBER MANAGED SERVICES

... UND WARUM DIESE LÄNGST ÜBERHOLT SIND

Das Outsourcing von IT-Dienstleistungen hat sich zu verschiedensten Kooperationsformen von Managed Services weiterentwickelt, die aus der modernen IT-Landschaft nicht mehr wegzudenken sind. Doch nach wie vor halten sich hartnäckige Mythen über angebliche Gefahren und Risiken, die damit verbunden sein sollen. Einer kritischen Prüfung halten sie jedoch nicht stand:

#1 Latente Abhängigkeiten:

Seit den ersten Outsourcing-Konzepten sorgt der Begriff des „Vendor-Lock-in" für Schweißperlen auf der Stirn von IT-Verantwortlichen. Er beschreibt die Abhängigkeit von einem externen Dienstleister, aus der es kein oder nur ein sehr teures Entrinnen gibt. In modernen Managed-Services-Verträgen sind Exit-Szenarien eindeutig geregelt, beispielsweise in Bezug auf die Datenportabilität. Zudem sind sie so flexibel ausgelegt, dass notwendige Anpassungen an veränderte Aufgabenprofile schnell und gemeinsam umgesetzt werden können.



#2 Kontroll- und Steuerungsverlust:

Durch eine planvolle Aufgabenverteilung, bei der kritische IT-Bereiche sowie die Steuerung und Koordinierung der Provider im Unternehmen verbleiben, wird der Angst vor dem Verlust der Kontroll- und Steuerungsfähigkeit der Boden entzogen. Auch hier ist die Art der Vertragsgestaltung entscheidend. Die in den Verträgen festgehaltenen Service Level Agreements (SLAs) legen Art und Umfang der IT-Leistungen detailliert fest, klar geregelte Eskalationsmechanismen beschreiben den Umgang mit Abweichungen.

#3 Verlust von internem Know-how:

Die wahrscheinlich am wenigsten begründete Furcht ist die vor dem Abfluss der internen IT-Expertise. Tatsächlich ist das Gegenteil der Fall. MSP sind eben kein Ersatz für die IT-Abteilung, sondern deren verlängerter Arm. Dafür bringen sie externe Expertise ein, die das interne Know-how des Unternehmens bei richtigem Set-up nicht ersetzt, sondern es um Expertenwissen und Best Practices ergänzt. Dies sorgt für einen fruchtbaren Austausch durch regelmäßige Reviews, Workshops und transparente Kommunikationskanäle, erweitert das Wissensspektrum der IT-Abteilung und entlastet sie zudem von vielen operativen Aufgaben.

#4 Verlust an Flexibilität und Agilität:

Moderne SLA-Modelle sind von vorneherein auf hohe Anpassungsfähigkeit ausgelegt. So ist es möglich, rasch auf veränderte Bedingungen zu reagieren oder neue Ideen schnell umzusetzen. Zudem kommen Innovationsinitiativen häufig von den MSP selbst. Ihre Qualität resultiert nicht zuletzt daraus, immer an der Spitze der technologischen Entwicklung zu stehen – sie müssen also per se selbst auf Flexibilität und Agilität ausgerichtet sein.

#5 Überholte Sicherheitsbedenken:

Je enger die Kooperation zwischen Unternehmen und externen Dienstleistern, desto wichtiger ist der Aspekt der Vertraulichkeit und der Sicherheitsmechanismen hinsichtlich des Schutzes sensibler Daten und Informationen. Bei der Skepsis gegenüber MSP wird häufig übersehen, dass der Datenschutz in deren ureigenstem Interesse liegt. Sie investieren mindestens ebenso massiv in modernste Sicherheitsinfrastrukturen und Sicherheitsteams wie die Unternehmen selbst. Viele MSP haben aus diesem Kompetenzfeld sogar ein eigenes Geschäftsmodell gemacht und bieten überlegene Sicherheitslösungen nach strengsten Compliance-Standards.

www.cgi.com

Cybersicherheitstrends 2025

SICHERHEITSEXPERTEN WARNEN VOR KI-VERSTÄRKTER RANSOMWARE

Der Ivanti-Report „Stand der Cybersicherheit 2025" identifiziert nach Befragung von 2.400 Experten Ransomware als Hauptbedrohung. Über ein Drittel der Sicherheitsexperten (global 38%, Deutschland 37%) sieht KI als verstärkenden Faktor für Ransomware-Angriffe.

Angesichts der Bedrohungslage halten sich lediglich 29 Prozent (in Deutschland sogar nur 24 Prozent) der Sicherheitsexperten für optimal auf Ransomware-Angriffe vorbereitet – ein alarmierendes Defizit, das die Dringlichkeit robusterer Schutzmaßnahmen verdeutlicht. Moderne Cybersicherheit erfordert einen flexiblen, durchdachten Ansatz, der nicht nur absolute Sicherheit anstrebt, sondern auch das Gleichgewicht zwischen Geschäftsrisiken und Chancen berücksichtigt. Exposure Management bietet eine effektivere Lösung für das Management und die Minderung von Risiken in diesem komplexen Umfeld.

Die Untersuchung von Ivanti zeigt, dass das Konzept des Exposure Managements weitgehend bekannt ist: So gibt knapp die Hälfte (49% global, 51% in Deutschland) der Sicherheitsexperten an, dass die Geschäftsführung ein hohes Verständnis für das Thema besitzt. Gleichzeitig setzen nur wenige der befragten Unternehmen diesen Ansatz aktiv um. Aktuell planen gerade einmal 18 Prozent (D) ihre Investitionen in Exposure Management im Jahr 2025 zu erhöhen.

www.ivanti.com

40 %

der befragten Sicherheitsexperten bewerten Ransomwareangriffe als hohe Bedrohung für ihr Unternehmen

MEHR WERT
Stand der Cybersicherheit 2025

Vishing-Angriffe explodieren

BEDROHUNG FÜR DIE KOMMUNIKATIONSSICHERHEIT?

Das ATO (Advanced Threat Operations)-Team von Ontinue hat seinen Halbjahresbericht vorgelegt, in dem es die aktuellen Trends und Entwicklungen im Cybersecurity-Bereich analysiert. Wie zu erwarten war, sind Ransomware-Attacken nach wie vor eines der beliebtesten Mittel von Hacker-Kollektiven und Cyberkriminellen. Ein beunruhigender Trend ist, dass die Hacker-Gruppen immer weniger auf reine Programmierkenntnisse setzen, sondern neuerdings vermehrt auf allgemeine IT-Skills. Potenzielle Hacker werden zunehmend nach ihren Fähigkeiten im Hinblick auf das Navigieren in Unternehmensnetzwerken, die Bewertung und Deaktivierung von Backups sowie das Hacken von Datenbanken und virtualisierten Umgebungen rekrutiert.

Insgesamt sind Ransomware-Attacken im letzten Halbjahr um 132 Prozent gestiegen, allerdings sind die Lösegeldzahlungen im Jahr 2024 um 35 Prozent gefallen. Während 2023 noch 1,25 Milliarden US-Dollar in die Taschen von Cyberkriminellen flossen, um verschlüsselte Daten wieder freizukaufen, waren es im vergangenen Jahr nur noch rund 814 Millionen US-Dollar. Der Grund dafür liegt in besseren Backup-Strategien und Incident-Response-Plänen, allerdings auch in neuen Regularien, die Zahlungen zunehmend verbieten. Das alles führt zu einem Umdenken bei Hacker-Gruppen, die ihre Taktik nun anpassen: Anstatt die Daten lediglich zu verschlüsseln, stehlen sie diese und drohen, sie öffentlich zu machen, um Unternehmen zur Zahlung zu zwingen.

Vishing auf dem Vormarsch

Der aktuelle Threat Intelligence Report enthüllt eine zunehmende Raffinesse beim Voice Phishing. Das sogenannte Vishing hat durch die immer leistungsfähigeren GenAI-Modelle, die Stimmen täuschend echt klonen können, ein neues Bedrohungslevel erreicht. Hacker verwenden die KI-Modelle, um realistische, aber eben gefälschte Deepfakes von Stimmen vertrauenswürdiger Personen zu erstellen. Damit ausgestattet, rufen sie ausgewählte Opfer an, fragen nach Anmeldedaten und bringen sie dazu, betrügerische Transaktionen zu genehmigen.

Allein im ersten Quartal 2024 verzeichnete das ATO-Team von Ontinue einen Anstieg der Vorfälle, die im Zusammenhang mit Vishing stehen, um gigantische 1.633 Prozent im Vergleich zum vorherigen Quartal. Viele dieser Angriffe leiteten die Opfer auf gefälschte Microsoft-Support-Seiten, die häufig auf .shop-Domains gehostet wurden. Dort wurden die Benutzer aufgefordert, betrügerische Support-Nummern anzurufen.

Die aktuellen Vishing-Kampagnen verdeutlichen, wie Social Engineering in Kombination mit KI-basierten Deepfakes zu einer immer effektiveren Methode für Cyberkriminelle wird, um an sensible Daten zu kommen oder Zugang zu geschützten Systemen zu erhalten.

www.ontinue.com

WELCHE ANGRIFFSMETHODEN WERDEN VORRANGIG GENUTZT?

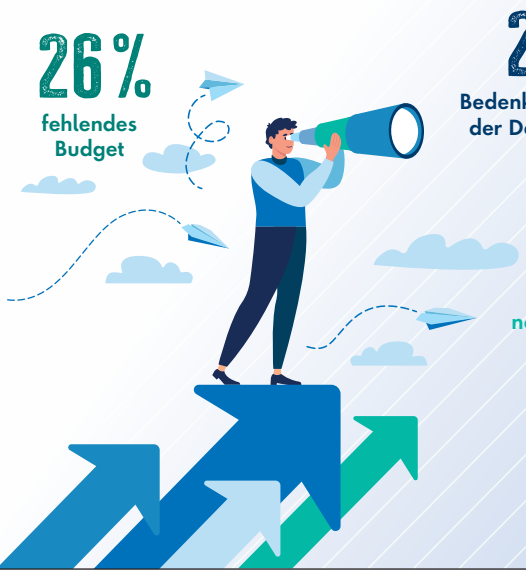
	E-MAIL-BOMBING	MALVERTISING
AKTION	Massive Spam-E-Mail-Flutung	Umleitung auf gefälschte Webseiten
ZIEL	Postfächer unbrauchbar machen	Gerätekompromitiertheit suggerieren
FOLGE	Nutzer werden frustriert	Verunsicherung der Nutzer
METHODE	- sich als Helpdesk ausgeben - Fernzugriff anbieten - Nutzer unter Druck setzen	- Gefälschte Support-Nummern anzeigen - Fernzugriffs-App installieren lassen - Maschinenkontrolle erlangen

VORTEIL KI-AGENTEN?

VIELFÄLTIGE HERAUSFORDERUNGEN FÜR UNTERNEHMEN

Eine Umfrage von SnapLogic zeigt, dass deutsche IT-Führungskräfte KI-Agenten eine Einsparung von 18 Arbeitsstunden pro Woche zutrauen. 47 Prozent vertrauen darauf, dass sie ebenso effizient wie Menschen arbeiten, 37 Prozent halten sie für effektiver. 84 Prozent der Befragten erwarten innerhalb der nächsten 12 bis 18 Monate spürbare Geschäftsergebnisse durch den Einsatz von KI-Agenten. Bereits 51 Prozent setzen diese Technologien ein, im Durchschnitt 26 Agenten pro Unternehmen. Bis Ende 2025 wird erwartet, dass deutsche Unternehmen im Schnitt 23 KI-Agenten nutzen.

VOR WELCHEN HERAUSFORDERUNGEN STEHEN UNTERNEHMEN?



26 % fehlendes Budget

28 % Bedenken hinsichtlich der Datensicherheit

29 % Sorge vor Datenschutzrisiken

24 % es fehlt an notwendigen Schnittstellen und Systemen

19 % mangelndes Grundvaerständnis für die Technologie

Datenschutz und Sicherheitsbedenken

Unternehmen stehen bei Einführung von KI-Agenten vor vielfältigen Herausforderungen. Auf die Frage, was sie davon abhält, KI-Agenten zu implementieren oder deren Einsatz auszuweiten, nennen gerade kleinere Unternehmen fehlendes Budget (26 %). Unabhängig von der Unternehmensgröße werden vor allem technische, kulturelle und sicherheitsbezogene Aspekte genannt: Knapp ein Drittel der Befragten hat Sorge vor Datenschutzrisiken (29 %), weitere 28 Prozent äußern allgemeine Bedenken hinsichtlich der Datensicherheit. Auch aufseiten der Mitarbeitenden gibt es Hindernisse: 24 Prozent der Unternehmen fehlt es an Mitarbeitenden mit den erforderlichen Fähigkeiten, und 19 Prozent berichten von einem mangelnden grundlegenden Verständnis für die Technologie. Zudem ist für viele Unternehmen die technische Infrastruktur weiterhin ein Problem: 24 Prozent geben an, dass es an den notwendigen Schnittstellen und Systemen fehlt.

www.snaplogic.com/de/

Vom Wildwuchs zur Effizienz

SO SCHAFFEN UNTERNEHMEN EINEN ERFOLGREICHEN DIGITALEN ARBEITSPLATZ

Die digitale Transformation bietet Organisationen enorme Potenziale zur Optimierung ihrer Arbeitsweise. Doch gerade wegen der Vielzahl an Tools und Technologien sehen sich viele Unternehmen mit einer fragmentierten IT-Infrastruktur konfrontiert. Unterschiedliche Systeme, Endgeräte sowie Kommunikations- und Kollaborations-Tools existieren nebeneinander, ohne miteinander zu kommunizieren. Das führt zu ineffizienten Prozessen und ungenutzten Möglichkeiten. Der digitale Arbeitsplatz kann sein volles Potenzial erst entfalten, wenn Unternehmen eine vereinheitlichte Infrastruktur schaffen, die technologische Effizienz steigert und eine nahtlose Zusammenarbeit zwischen den Mitarbeitenden ermöglicht.

Boris Ovcak, Partner und Practice Division Head of Transformation of Work bei Campana & Schott, erläutert, warum die Harmonisierung nicht nur für den Erfolg des digitalen Arbeitsplatzes, sondern auch für die effektive Nutzung von Künstlicher Intelligenz entscheidend ist.

it management: *Herr Ovcak, wo stehen Unternehmen aktuell in Bezug auf den digitalen Arbeitsplatz und welche Herausforderungen gibt es?*

Boris Ovcak: Der digitale Arbeitsplatz ist in vielen Unternehmen mittlerweile Realität – doch die tatsächliche Umsetzung entspricht oft nicht den Erwartungen. Das zeigt auch unsere Social Collaboration Studie 2025, die wir gemeinsam mit der TU Darmstadt durchgeführt haben: Während zwei Drittel der Unternehmen in der DACH-Region angeben, einen digitalen Arbeitsplatz implementiert zu haben oder aktiv daran zu arbeiten, gibt es nach wie vor Herausforderungen. Besonders die Fragmentierung bleibt ein wesentliches Hindernis. Im Laufe der Jahre hat sich ein Flickenteppich aus Tools und Systemen gebildet, die oft nicht miteinander harmonieren. Dieser Wildwuchs verursacht nicht nur unnötig hohe Lizenzierungs- und Wartungsausgaben, sondern beeinträchtigt auch die Effizienz der Mitarbeitenden.

> ES GEHT DARUM, EINE INFRASTRUKTUR ZU SCHAFFEN, IN DER SYSTEME UND TOOLS NAHTLOS MITEINANDER KOMMUNIZIEREN. DAS REDUZIERT KOMPLEXITÄT UND STEIGERT PRODUKTIVITÄT.
>
> **Boris Ovcak, Partner und Practice Division Head of Transformation of Work, Campana & Schott, www.campana-schott.com**

it management: *Wie lässt sich diese Vereinheitlichung umsetzen? Müssen Unternehmen dazu ihre komplette IT-Infrastruktur umstellen?*

Boris Ovcak: Es geht nicht darum, alles von einem einzigen Anbieter zu beziehen, sondern eine Infrastruktur zu schaffen, die zusammenarbeitet. Vereinheitlichung bedeutet, Systeme und Tools so zu konsolidieren, dass sie miteinander nahtlos kommunizieren können. Die Plattformen müssen offen und flexibel sein, um

mit Drittanbieterlösungen zu interagieren und eine reibungslose Zusammenarbeit zu ermöglichen. Dadurch können Unternehmen ihre digitale Infrastruktur optimieren, ohne sich auf einen einzigen Anbieter festzulegen. Ich fasse das gerne unter dem Begriff „InfraPlay" zusammen, der die notwendige Infrastruktur für digitale Kollaboration beschreibt.

it management: *Welche Vorteile bringt diese Vereinheitlichung für die Mitarbeitenden in ihrer täglichen Arbeit?*

Boris Ovcak: Die Mitarbeitenden nutzen eine Plattform, die alle Funktionen vereint – von Kommunikation über Dokumentenmanagement bis hin zu Meetings. So wird die Komplexität reduziert und die Produktivität gesteigert, da weniger Zeit für den Wechsel zwischen Systemen verloren geht. Der Zugriff auf Informationen wird nahtlos: Mitarbeitende müssen nicht mehr herausfinden, aus welchem System die Daten stammen, weil alles integriert ist. Und ein weiterer wichtiger Aspekt ist die Integration von KI, die dann erst effizient möglich wird.

it management: *Sie sprechen es an: KI wird immer wichtiger in der digitalen Transformation von Unternehmen. Welche Rolle spielt eine harmonisierte IT-Infrastruktur hier?*

Boris Ovcak: In unserer Studie gaben 41 Prozent der Unternehmen in der DACH-Region an, KI-Technologie bereits zu nutzen – um genauer zu sein: Generative KI-Tools wie ChatGPT, Copilot oder Gemini. Um ihr volles Potenzial auszuschöpfen, benötigt KI jedoch eine konsolidierte Datenbasis. Wenn Unternehmensdaten über verschiedene Systeme verstreut und nicht erreichbar sind, schränkt das den Nutzen von KI stark ein. Harmonisierung sorgt dafür, dass alle relevanten Daten problemlos für KI-Anwendungen zugänglich sind. Für Mitarbeitende bedeutet dies, dass die KI ihnen die Informationen in Echtzeit liefern kann, die sie gerade benötigen.

Ein zweiter Aspekt bezüglich Harmonisierung und KI ist das User Interface: Insbesondere Organisationen, die frühzeitig mit der Bereitstellung eigener GPTs begonnen haben, stehen heute vor der Herausforderung, ihren Mitarbeitenden ein zentrales User Interface für ihre KI-Anwendungen zu bieten – so dass nicht je Anwendungsfall erst die richtige Anwendung beziehungsweise der entsprechende GPT geöffnet werden muss.

it management: *Wie lässt sich IT-Sicherheit gewährleisten, wenn eine konsolidierte Infrastruktur sämtliche Systeme und Daten miteinander verknüpft?*

Boris Ovcak: Die zentrale Speicherung und Verknüpfung von Daten stellt hohe Anforderungen an die IT-Sicherheit. Eine konsolidierte Infrastruktur ermöglicht es, Sicherheitsmaßnahmen effizient und gezielt umzusetzen. Moderne IT-Sicherheit verfolgt einen ganzheitlichen Ansatz: Sicherheitsrichtlinien werden zentral implementiert und Zugriffsrechte präzise gesteuert. So können Unternehmen sicherstellen, dass nur autorisierte Mitarbeitende auf sensible Daten zugreifen können.

it management: *Während Büroangestellte oft Zugang zu den neuesten digitalen Tools haben, bleiben Frontline Worker, also Mitarbeitende ohne festen Arbeitsplatz, häufig außen vor. Stellt das langfristig ein Problem dar?*

Boris Ovcak: Etwa 80 Prozent der weltweiten Belegschaft arbeiten ohne festen Arbeitsplatz. Diese Gruppe wird bei der Digitalisierung häufig übersehen und hat oft keinen Zugang zu den gleichen digitalen Tools wie der klassische Information Worker. Das schränkt ihre Produktivität und die Integration ins Unternehmen ein – viele relevante Unternehmensinformationen erreichen diese Personen schlichtweg nicht.

Unternehmen müssen Lösungen entwickeln, die ihnen denselben Zugang zu digitalen Tools wie ihren Kolleginnen und Kollegen im Büro ermöglichen. Mobile Mitarbeiter-Apps und cloudbasierte Kommunikationsplattformen sind hier gute Möglichkeiten, die Integration voranzutreiben. Wenn Frontline Worker dieselben Tools nutzen können, steigert dies ihre Effizienz, Motivation und Bindung ans Unternehmen – auch das hat die Social Collaboration Umfrage gezeigt.

it management: *Welche Stolperfallen sehen Sie bei der Einführung digitaler Arbeitsplätze oder Erweiterungen dieser, beispielsweise mit GenAI?*

Boris Ovcak: Die Einbindung der Mitarbeitenden ist entscheidend. Technologie allein kann eine Transformation nicht erfolgreich machen – es braucht die Akzeptanz und aktive Beteiligung der Menschen, die mit ihr arbeiten. In unserer täglichen Arbeit mit Kunden sehen wir, dass der wahre Erfolg eines digitalen Arbeitsplatzes nicht nur in der Technologie liegt, sondern auch in der Bereitschaft der Mitarbeitenden, diese Veränderungen mitzutragen. Es geht darum, eine Kultur zu schaffen, die den digitalen Wandel aktiv unterstützt. Wenn Menschen und Technologie harmonieren, entfaltet sich das volle Potenzial der digitalen Transformation, und Unternehmen sichern sich nachhaltigen Erfolg.

it management: *Herr Ovcak, vielen Dank für dieses Gespräch.*

VORGEHENSMUSTER FÜR SOFTWAREARCHITEKTUR

KOMBINIERBARE PRAKTIKEN IN ZEITEN VON AGILE UND LEAN

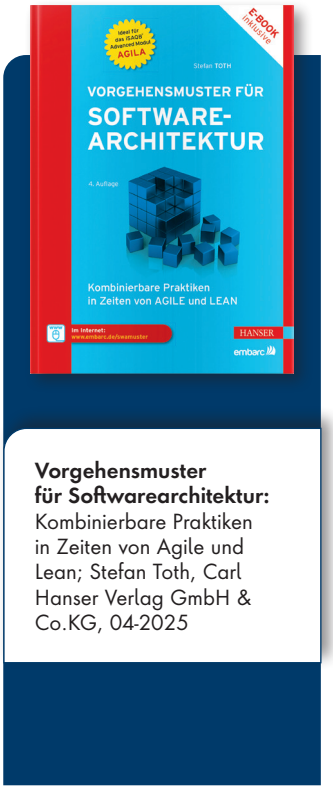
Egal ob „Agile", „Lean", „Cloud" oder „Flow" – moderne Vorhaben in der Softwareentwicklung arbeiten dynamisch, hoch flexibel und ergebnisorientiert. Auch Softwarearchitektur kann zielorientiert und pragmatisch entstehen, durch Entwicklungsteams gemeinsam getrieben sein oder „Just-in-time" festgelegt werden. Einen Konflikt zwischen Dynamik und Architektur gibt es nicht. Alles, was es braucht, sind zeitgemäße Praktiken und das richtige Mindset.

Dieses Buch beinhaltet kein weiteres Vorgehensmodell für die Softwareentwicklung. Stattdessen werden leichtgewichtige Bausteine guter Architekturarbeit vorgestellt, die problemorientiert eingesetzt werden können, um das eigene Vorhaben zu verbessern.

Das ermöglicht ein schrittweises Lernen und Adaptieren neuer Praktiken, ohne große Einstiegshürde. In der bewährten Struktur von Mustern wird ein übliches Problem aus dem Alltag von Entwicklungsvorhaben geschildert und mit einer methodischen Lösung versehen. Die Lösungen referenzieren aufeinander, sind kombinierbar und ergeben insgesamt das Bild einer neuen Architekturdisziplin.

Aus dem Inhalt:

- Risikogetriebene Softwarearchitektur
- Die Rolle Architecture Owner
- Architekturarbeit in Backlogs
- Architekturvision
- Walking Skeleton
- Architekturprinzipien
- Der Pfad des geringsten Widerstands
- 2-Speed-Architecture
- Architektur-Radar
- NFR-Tests und Chaos Engineering
- Architektur-Communities
- Architektur-Kata



Vorgehensmuster für Softwarearchitektur: Kombinierbare Praktiken in Zeiten von Agile und Lean; Stefan Toth, Carl Hanser Verlag GmbH & Co.KG, 04-2025

ENDPOINT-STRATEGIEN

Die moderne IT-Landschaft stellt Unternehmen vor ein Dilemma: Steigende Compliance-Anforderungen, wachsende Angriffsflächen und komplexe IT-Infrastrukturen treffen auf begrenzte Ressourcen.

Die Vielfalt an Sicherheitslösungen und neuen Angriffsvektoren erfordern moderne, integrierte Strategien. Gleichzeitig setzt sich der Trend zur hybriden IT-Landschaft durch – Unternehmen wollen nicht zwischen Cloud und On-Premises wählen, sondern flexibel beide Ansätze kombinieren.

Eine zentrale Rolle spielt dabei auch Unified Endpoint Security: Sie ermöglicht nicht nur eine ganzheitliche Absicherung und Verwaltung aller Endgeräte, unabhängig vom Standort , sondern auch Effizienzgewinne durch vereinheitlichte Richtlinien und automatisierte Reaktionsprozesse.

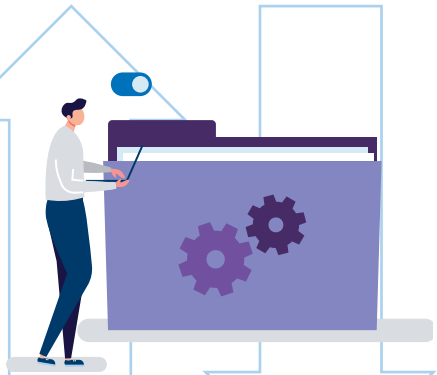
Hybrides UEM

DIE ZUKUNFT DER ENDGERÄTEVERWALTUNG

Unternehmen stehen heute vor der Herausforderung, eine Vielzahl von Endgeräten zu verwalten – vom klassischen Desktop-PC bis hin zu mobilen iOS- und Android-Geräten. Gleichzeitig steigen die Anforderungen an IT-Sicherheit und Compliance, während IT-Abteilungen mit begrenzten Ressourcen arbeiten müssen. Eine Lösung dafür sollen hybride UEM-Plattformen bieten, die klassisches Client Management mit cloud-basierten UEM-Funktionen verbinden. Über das Konzept sprach it management mit Sebastian Weber, Chief Evangelist beim UEM-Spezialisten Aagon.

it management: *Herr Weber, Client Management ist heute sowohl on-premises als auch aus der Cloud möglich. Worin besteht der Unterschied?*

Sebastian Weber: Für die übergreifende Verwaltung von IT-Infrastrukturen hat sich mittlerweile eher der Begriff Unified Endpoint Management herausgebildet. Früher hieß es jedoch „Client Management". Das war in der Regel eine On-Premises-Software für strukturiertes, zentralisiertes und automatisiertes Administrieren sowie Dokumentieren von Endgeräten (PC, Server, mobile Endgeräte) mit einem Windows- oder Linux-Betriebssystem. Heute stehen wir vor einer ungleich heterogeneren IT-Infrastruktur, zu der selbst verständlich auch iOS- und Android-Geräte gehören. Verwaltet werden diese bislang oft mit cloud-basierten UEM-Systemen, von denen Intune das bekannteste und gebräuchlichste ist. Kein Wunder, ist es doch im oft gewählten Enterprise-Lizenzvertrag Microsoft 365 E3 enthalten.



it management: *Als Hersteller eines verbreiteten UEM-Systems plädieren Sie für einen hybriden Ansatz, das heißt die Kombination aus Cloud und on-premises. Weshalb?*

Sebastian Weber: Ganz einfach: Die Cloud bietet Skalierbarkeit und Mobilität, während Inhouse-Systeme ihre Stärken bei der Sicherheit und Kontrolle ausspielen. Dies lösen wir durch eine Kombi-

nation, konkret die Integration von Intune in unser UEM. So können Unternehmen selbst entscheiden, welche Komponenten sie in der Cloud betreiben und welche lokal verbleiben.

it management: *Wo liegen die Mängel eines rein cloud-betriebenen UEMs, in diesem Fall von Intune?*

Sebastian Weber: Zunächst einmal bietet das Microsoft-Tool mit grundlegenden Funktionen wie dem Verteilen von Exe- und MSI-Dateien oder dem Sperren von Geräten eine solide Basis für die Verwaltung mobiler Endgeräte, aber eben nur für diese. Für die Verwaltung von Servern sind wiederum Zusatzlösungen erforderlich. Funktionale Einschränkungen finden sich außerdem bei der Administration von SNMP-Geräten und bezüglich einer detaillierten Inventarisierung. Admins erhalten insgesamt nur eine Teilansicht ihrer IT-Infrastruktur und übersehen Risiken daher leichter.

Die Bordmittel eines Client-Betriebssystems spricht ein Cloud-UEM oft nur rudimentär an. Es dockt üblicherweise an die Mobile-Schnittstelle des Devices an, die gegenüber einem nativen Agenten deutlich weniger Funktionalität aufweist. Einem Gerät (oder einer Gruppe von Geräten) wird ein Software-Update zugewiesen, der Cloud-Anbieter entscheidet aber eigenmächtig, wann er Sicherheitslücken schließt oder den neuesten Patch einspielt. Es gibt kaum Spielraum, selbst einzugreifen und etwa Ports zu sperren.

it management: *Welche Vorteile bietet demgegenüber eine On-premises-Lösung?*

Sebastian Weber: Grundsätzlich ist sie auf eigenen Servern installiert (auch in der Private Cloud eines Hyperscalers möglich), verfügt über eigene Agenten und bietet größere Vielfalt durch manuelle Clients, Agents oder ein zusätzliches Gateway. Sie beinhaltet Funktionen wie Remote Control, Lizenzmanagement, Asset Management oder Windows Update

EINE HYBRIDE LÖSUNG STELLT SICHER, DASS ALLE ENDPUNKTE JEDERZEIT DEN AKTUELLEN SICHERHEITSRICHTLINIEN ENTSPRECHEN.

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

Management für Clients und Server und Microsoft365, an die bei Intune gar nicht zu denken ist.

Sogar Microsoft-Lösungen wie Defender und BitLocker lassen sich direkt über sie steuern, auch ohne Cloud-Anbindung. Weil sich die Daten in der eigenen Umgebung befinden, sind sie sehr gut geschützt, und das Unternehmen ist unabhängig vom Internet und dem Status des Servers in der Cloud. Weitere Vorteile eines lokalen Systems: Sicherheitsbereiche lassen sich gut voneinander abgrenzen und individuelle Lösungen mit No-Code/Low-Code einrichten.

Auf der anderen Seite fallen Kosten für Hardware und Lizenzen an. Deren Hochskalierung kann ebenfalls schnell viel Geld und Zeitaufwand verschlingen. Und ihr Hauptnachteil: Mobile Geräte sind nicht oder nur schlecht anbindbar.

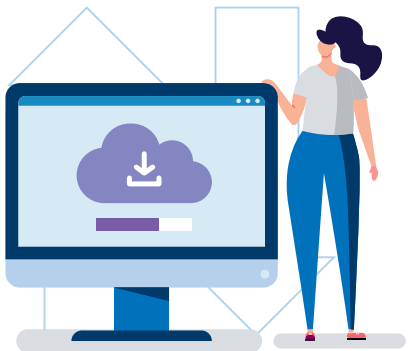
it management: *Ein hybrides UEM verbindet nun beide Ansätze?*

Sebastian Weber: So ist es. Unsere ACMP Suite erweitert die Verwaltung überwiegend mobiler Endgeräte auf die gesamte IT-Infrastruktur, einschließlich Clients, Server und weiterer IT-Komponenten. Geräte- und Benutzer-Gruppen aus Intune werden in die UEM-Lösung überführt, sind darin sichtbar und lassen sich detailliert managen – in ACMP, über Intune. Außerdem werden sämtliche Arten von Apps verteilt, an Android-, iOS- und Windows-Geräte.

it management: *Wie profitieren IT-Abteilungen konkret von der Zusammenführung?*

Sebastian Weber: Sie müssen nicht mehr zwischen mehreren Systemen wechseln, sondern arbeiten mit einer übersichtlichen, zentralen Plattform, auf der sie sowohl klassische als auch mobile Endgeräte einheitlich verwalten können. So behalten sie beispielsweise Update-Zeitpunkte im Blick und können Patch Management präziser steuern – etwas, das Intune nur eingeschränkt bietet. Auch Compliance-Anforderungen aus NIS2, ISO 27001 oder KRITIS lassen sich besser umsetzen. Unternehmen, die eine einheitliche IT-Security- und Compliance-Plattform benötigen, können mit einem hybriden Ansatz ihre Sicherheits- und Risikomanagementprozesse strukturiert verwalten.

Ein weiterer Vorteil ist die tiefere Integration bestehender IT-Prozesse. Während Intune sich primär auf die Geräteverwaltung konzentriert, ermöglicht ACMP eine umfassendere IT-Automatisierung. Beispielsweise können Skripte zur Fehlerbe-



hebung oder Software-Rollouts zentral gesteuert werden, ohne dass Administratoren manuell eingreifen müssen. In unserem UEM-System lassen sich auch mehrere Intune-Portale zusammenfassen – das kann selbst Microsoft nicht. Laut Gartner verfügen wir damit über einen absoluten USP.

it management: *Trotz alledem: Intune ist kostenlos und kann schon einiges, für Ihr UEM hingegen fallen Lizenzgebühren an. Schwierig gegenüber dem Management zu verargumentieren, oder?*

Sebastian Weber: Nur auf den ersten Blick. Eine Geschäftsleitung, die nur überflüssige Zusatzkosten sieht, berücksichtigt dabei nicht die langfristigen Folgen. In Wirklichkeit ist es so, dass die kurzfristige Einsparung von Lizenzkosten zu höheren versteckten Kosten durch manuellen Mehraufwand, Fehleranfälligkeit und mögliche Sicherheitsrisiken führt.

it management: *Welche Sicherheitsvorteile bietet ein hybrides UEM?*

Sebastian Weber: Sicherheit ist einer der Hauptgründe, warum Unternehmen nicht ausschließlich auf cloud-basierte Lösungen setzen. Intune allein bietet keine tiefgreifenden Audit- und Sicherheitsfunktionen. ACMP hingegen ermöglicht eine umfassende IT-Sicherheit, indem es Schwachstellenmanagement, Third-Party-Patch-Management und Windows-Update-Management integriert. So werden nicht nur Clients, sondern auch Microsoft 365-Produkte zentral gepatcht. Zudem haben Unternehmen die Möglichkeit, sensible Daten in ihrer eigenen Infrastruktur zu halten und unabhängig von der Internetverbindung zu bleiben.

Gerade in regulierten Branchen, wie dem Finanz- oder Gesundheitssektor, ist diese Kontrolle entscheidend. Unternehmen, die den Vorgaben von DORA oder der KRITIS-Verordnung unterliegen, benötigen lückenlose Nachverfolgbarkeit und Dokumentation ihrer Sicherheitsmaßnahmen. Eine hybride Lösung stellt sicher, dass alle Endpunkte jederzeit den aktuellen Sicherheitsrichtlinien entsprechen.

it management: *Wie sieht es mit der Skalierbarkeit aus?*

Sebastian Weber: Klein anzufangen und die Infrastruktur je nach Bedarf zu erweitern ist ein entscheidender Faktor. Startet ein Unternehmen mit einer Cloud-Infrastruktur, kann es schrittweise On-Premises-Kapazitäten hinzufügen, um mehr Kontrolle und Funktionalität zu erhalten. Die ACMP Suite kann demnächst auch direkt in Microsoft Azure betrieben werden, wodurch Unternehmen noch flexibler entscheiden können, wie sie ihre Infrastruktur gestalten. Das heißt, selbst Unternehmen, die primär auf Cloud-Lösungen setzen, können weiterhin von den erweiterten On-Premises-Funktionen profitieren.

it management: *Wo liegen die Herausforderungen des Ansatzes?*

Sebastian Weber: Eine hybride Infrastruktur erfordert eine gut durchdachte Integration der beiden Systeme. Deshalb war es uns wichtig, eine einheitliche Benutzeroberfläche zu schaffen, die sowohl Intune- als auch On-Premises-Geräte abbildet. So vermeiden wir Fragmentierung und sorgen für eine zentrale Steuerung. Ein weiterer Aspekt ist die Schulung der IT-Teams: Wer bisher nur mit einer reinen Cloud- oder On-Premises-Lösung gearbeitet hat, muss sich mit den neuen Möglichkeiten vertraut machen. Je intuitiver die UEM-Konsole also zu bedienen ist, desto besser. Zusätzlich spielt die Performance eine wichtige Rolle. Gerade in großen Netzwerken mit tausenden Endgeräten ist es wichtig, dass Abfragen und Steuerungsprozesse effizient ablaufen.

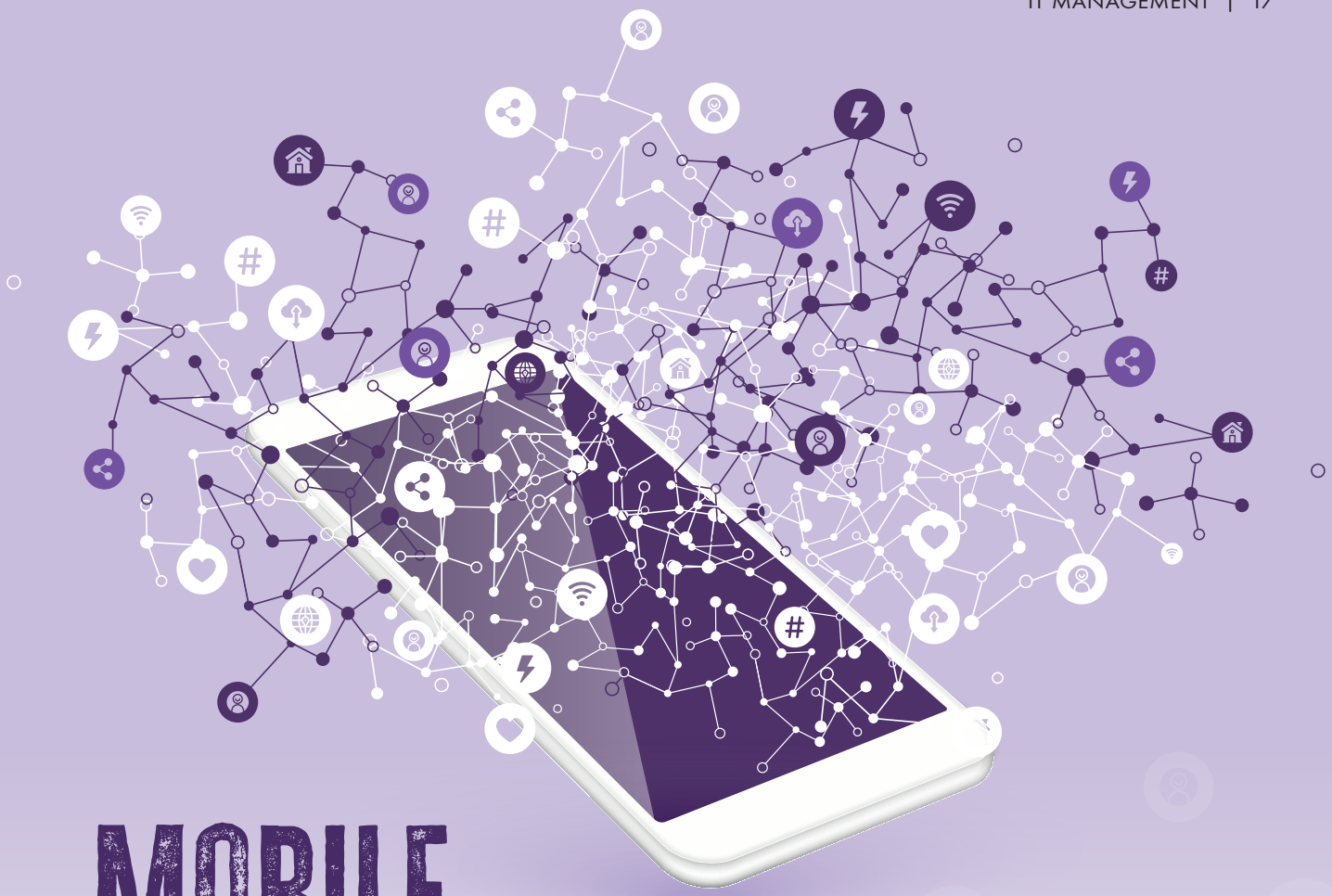
it management: *Welche Rolle spielen Managed Service Provider (MSP) in Ihrer Strategie?*

Sebastian Weber: MSPs profitieren besonders von unserer Lösung, da sie mehrere Intune-Portale in einer Plattform zusammenführen können. Dadurch lassen sich Kundensysteme effizient verwalten, ohne sich durch verschiedene Oberflächen klicken zu müssen. Ein hybrider UEM-Ansatz macht es für MSPs einfacher, ihren Kunden eine nahtlose und sichere Verwaltung aller Endpunkte zu bieten. Unerlässlich ist in diesem Zusammenhang eine feingranulare Mandantenverwaltung. Dadurch können MSPs verschiedene Kundenumgebungen getrennt administrieren, ohne dass sich Daten oder Steuerungsprozesse vermischen.

it management: *Zum Abschluss: Wie sehen Sie die Zukunft des UEM?*

Sebastian Weber: Die Zukunft ist hybrid. Unternehmen wollen nicht zwischen Cloud und On-Premises entscheiden müssen, sondern beides kombinieren, um das Beste aus beiden Welten zu nutzen. Mit unserer ACMP Suite bieten wir genau diese Flexibilität und Sicherheit. Wir arbeiten kontinuierlich an neuen Funktionen, um unsere Lösung weiterzuentwickeln und den steigenden Anforderungen der IT-Welt gerecht zu werden. Gerade mit Blick auf zunehmende Cyberbedrohungen wird eine umfassende und zentralisierte Endgeräteverwaltung immer wichtiger.

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



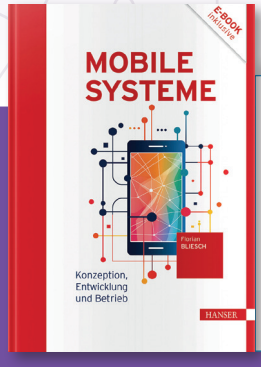
MOBILE SYSTEME

KONZEPTION, ENTWICKLUNG UND BETRIEB

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

AUS DEM INHALT

- Mobile Systeme: Komponenten und Basistechnologien
- Mobile Geräte: Klassen, Technik und Infrastruktur
- Mobile Entwicklungsframeworks: Nativ, Cross-Plattform, Hybrid
- Mobile User Experience (UX)
- Mobile Application Life Cycle Management (ALM), Mobile Application Management (MAM)
- Mobile Security: Risiken und Prävention
- Mobile KI
- Mobile Business: Geschäftsmodelle und globaler Markt
- Mobile XR und Mobile Metaverse
- Green IT und Green Coding
- Technikfolgenabschätzung und soziokulturelle Implikationen



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

Endpoint Security im Wandel

VON INSELLÖSUNGEN HIN ZUR INTEGRIERTEN PLATTFORM

AVP, DLP und EDR
Firewall, IAM und MFA
EPP, ATP – das kennt man ja …

Wer hier jetzt automatisch „MfG" von den Fanta Vier im Kopf hat, kennt sich offensichtlich sowohl mit gängigen Endpoint Security Kürzeln wie auch mit deutschem Hip-Hop der ersten Stunde gut aus.

Die Vielzahl an Abkürzungen unterstreicht, was auch die vergangene it-sa 2024 mit einem Ausstellerrekord, Besucherwachstum und brummenden Messehallen gezeigt hat: Die Security-Branche wächst und am Markt präsentiert sich eine inzwischen fast unüberschaubare Menge von Anbietern und Lösungen. Die Branche wird diversifizierter und spezialisierter.

Das ist in Anbetracht der ebenso wachsenden Vielfalt an Sicherheitsrisiken und Angriffsflächen gut, ist aber für Unternehmen und Sicherheitsverantwortliche auch eine Herausforderung: Denn Security-Teams setzen heute diverse Sicherheitslösungen ein. All diese Lösungen müssen evaluiert, implementiert, verwaltet und überwacht werden – das bedeutet mehr Management, mehr Prozesse, mehr Monitoring. Der Einsatz isolierter Systeme ist aber nicht nur kostenintensiv und erhöht den Management-Aufwand. Schlimmstenfalls führen isolierte Lösungen auch dazu, dass die Transparenz über Sicherheitsrisiken fehlt und damit zusätzliche potenzielle Schwachstellen entstehen.

Die aktuelle Studie „IT-Sicherheit heute und morgen" des Analystenhauses techconsult im Auftrag von DriveLock zeigt, dass isolierte Sicherheitssysteme nicht mehr den Anforderungen einer modernen IT-Infrastruktur gerecht werden. Etwa jede zweite bis dritte Sicherheitslösung läuft als eigenständiges System ohne Verbindung zu anderen Sicherheitskomponenten.

Dabei führt bereits jeder zusätzliche Zugangspunkt, sei es durch mobile oder IoT-Geräte oder andere vernetzte Systeme zu mehr Komplexität der IT-Infrastruktur und sorgt für zusätzliche potenzielle Schwachstellen. Security-Lösungen sollten dieser Komplexität begegnen und IT-Security-Teams ruhigen Schlaf bescheren, statt ihre Arbeitslast weiter zu erhöhen.

Eine Lösung für dieses Problem wachsender Lösungsvielfalt ist der Ansatz der Unified Endpoint Security, der im Folgenden näher erläutert wird.

Unified Endpoint Security – Konzept und strategische Notwendigkeit

Unified Endpoint Security (UES) ist kein ganz neues, aber ein noch immer nicht ausreichend populäres Konzept in der Endpoint-Sicherheit.

MEHR WERT
IT-Sicherheit heute und morgen

Und weil Sie sich gut mit Abkürzungen und Endpoint Security auskennen, fragen Sie sich wahrscheinlich jetzt:

„Ich kenne UEM (Unified Endpoint Management); was ist denn der Unterschied zwischen UEM und UES?"

Keine Sorge, wir klären das auf.

UEM und UES haben vieles gemeinsam, doch der entscheidende Unterschied liegt in den letzten zwei Wörtern der Abkürzungen – Management versus Security. UEM kümmert sich um die zentrale Verwaltung aller Endpunkte Ihrer Organisation. UES bringt das Ganze auf die nächste Ebene und betrachtet darüber hinaus auch Angriffsprävention, -erkennung und -behebung auf Endgeräten.

UEM bringt sowohl während des Provisionings als auch im laufenden Betrieb eine Standardisierung und Homogenisierung in das Operating System- und Software-Management auf allen Arten von Endpoints. Es deckt Patching, Richtlinienverwaltung und Device Management ab. UES legt hier noch eine Schippe drauf: Es sorgt für die Härtung der Endpoints und bringt hierfür eine ganze Reihe von Sicherheitsfunktionen mit; von Schwachstellenmanagement, Antimalware, Device und Applikationskontrolle hin zur Anomalie-Erkennung und mehr.

UES steht für eine zentralisierte Verwaltung aller Sicherheitswerkzeuge, die miteinander integriert sind und auf einer einzigen Plattform laufen. UES bietet einen umfassenden Ansatz, um Angriffe schnell zu erkennen, zu kontrollieren und zu beheben und vereint hierfür die Komponenten von UEM, EPP (Endpoint Protection Plattformen), EDR (Endpoint Detection and Response) und MTD (Mobile Threat Defense) auf einer zentralen Plattform mit einem einheitlichen Administrations-Dashboard.

UNIFIED ENDPOINT MANAGEMENT (UEM):

Verwaltung und Kontrolle aller Endgeräte, von Desktops bis zu mobilen Geräten, in einer einheitlichen Plattform.
Endpoint Protection Platform (EPP) und Endpoint Detection and Response (EDR:
Schutz vor und Erkennung von und Reagieren auf Bedrohungen wie Malware, Ransomware und Exploits.
Mobile Threat Defense (MTD):
Schutz mobiler Geräte vor Phishing, unsicheren Apps und Netzwerken

Diese Integration vereinfacht die oftmals komplizierten Prozesse für Sicherheitsteams signifikant und steigert deren Produktivität und Effizienz erheblich.

Der Ansatz fördert eine Zusammenarbeit zwischen IT-Operations- und Endpoint-Security-Teams, die häufig mit unterschiedlichen Tools und Kompetenzen arbeiten.

Die Integration von Menschen, Prozessen und Tools ermöglicht:

- Zentrale Informationsquellen: Einheitliche Übersicht über Endpointe, Risiken und Compliance.
- Erweiterte Workflows: Verknüpfung von Sicherheitsreaktionen (z. B. virtuelle Patches) mit umfassenden Maßnahmen wie der vollständigen Patching-Routine für Endgeräte.

Zusammenfassend bietet UES eine durchgängige Absicherung des gesamten Lebenszyklus von Endgeräten – von der Bereitstellung über die Verwaltung bis hin zum täglichen Betrieb.

Die Notwendigkeit für integrierte Konzepte und Lösungen unterstreichen die Ergebnisse der Studie „IT-Sicherheit heute und morgen": 90 Prozent der befragten Unternehmen nehmen eine eskalierende Bedrohungslage wahr. 71 Prozent der befragten IT-Sicherheitsverantwortlichen beobachten einen deutlichen Anstieg von Phishing-Attacken. Gleichzeitig stagniert das Sicherheitsbewusstsein ihrer Mitarbeitenden.

Die Studie identifiziert weiterhin drei zentrale Problembereiche, denen Unternehmen in der IT-Sicherheit begegnen müssen: Ressourcen- und Personalengpässe, Komplexität und Integration sowie Transparenz und Verwaltung. Die Überlastung von IT-Teams und hohe Betriebskosten zählen zu den größten Hür-

MIT IHRER MODULAREN STRUKTUR UND DER MÖGLICHKEIT ZUR INTEGRATION IN BESTEHENDE SYSTEME STELLT DIE HYPERSECURE PLATFORM EINE FLEXIBLE UND ZUKUNFTSSICHERE LÖSUNG DAR.

Andreas Fuchs, Director Product Management, DriveLock SE, www.drivelock.com

den. Integrationsprobleme und die Vielzahl an unterschiedlichen Lösungen erschweren es Unternehmen, ihre Sicherheitsarchitektur effizient zu betreiben. Zudem führt die fragmentierte IT-Infrastruktur zu operativen Ineffizienzen und Sicherheitslücken.

Diese Problembereiche erfordern eine umfassende Strategie, die die Sicherheitsarchitektur von Unternehmen proaktiv stärkt. Die Studie zeigt zudem weiter, dass 75 Prozent der IT-Sicherheitsverantwortlichen integrierte Plattformlösungen in diesem Zusammenhang positiv oder als zukunftsweisend bewerten.

Eine zentrale Sicherheitsplattform kann diesen Herausforderungen entgegenwirken, indem sie Verwaltungsprozesse vereinfacht, automatisiert und standardisiert. Durch eine einheitliche Benutzeroberfläche und integrierte Tools werden redundante Aufgaben reduziert und Arbeitsabläufe optimiert. IT-Teams gewinnen dadurch wertvolle Zeit für strategische Sicherheitsprojekte und die Gesamtkosten sinken durch den Wegfall von Insellösungen.

DriveLocks Hypersecure Platform und europäische Security-Allianz

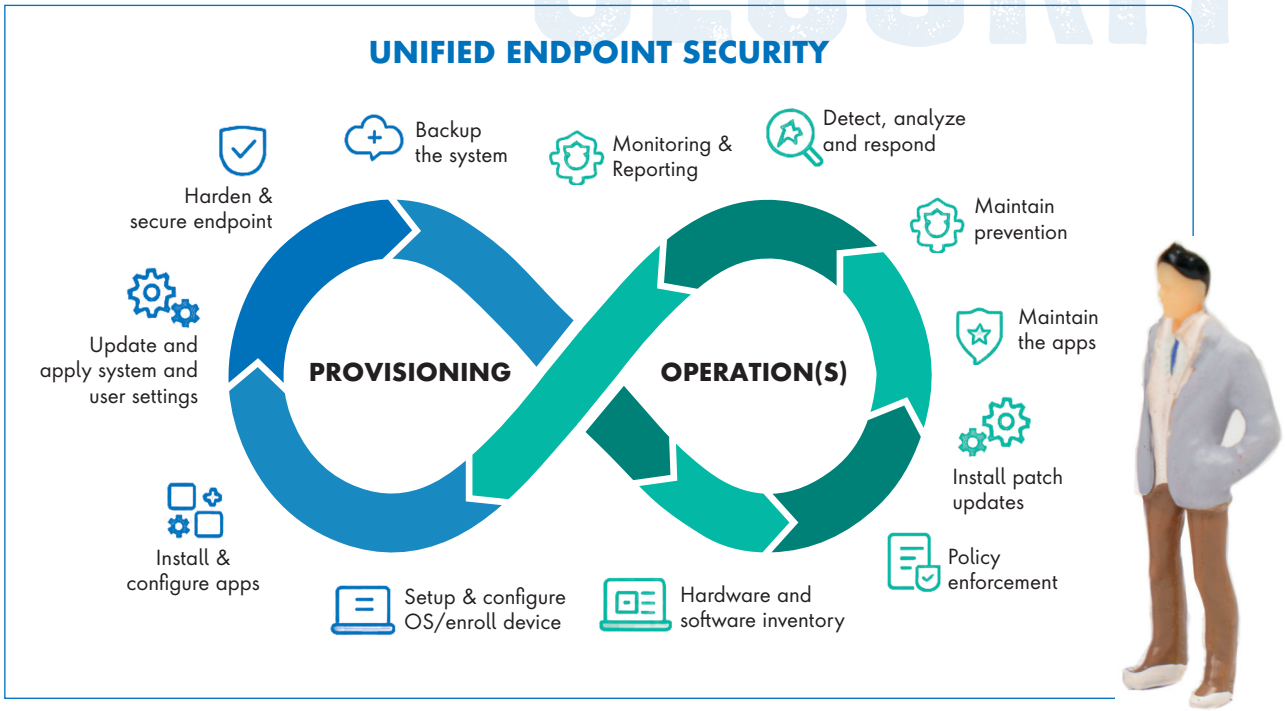
Hier kommt die HYPERSECURE Platform von DriveLock ins Spiel: Sie vereint bereits ein umfangreiches Portfolio an eigenen Sicherheitstools und erweitert dieses strategisch mit Lösungen von Drittanbietern. Jüngstes Beispiel für die Erweiterung der Plattform ist die Akquisition von idgard durch DriveLock. idgard ist führend im Bereich des sicheren cloud-basierten Datenaustauschs.

Mit ihrer modularen Struktur und der Möglichkeit zur Integration in bestehende Systeme stellt die HYPERSECURE Platform eine flexible und zukunftssichere Lösung dar. Eine Schlüsselkomponente ist die Zusammenarbeit innerhalb einer europäischen Security-Allianz, die zum Ziel hat, Security-Kompetenz in Deutschland und Europa zu bündeln und die Souveränität von Unternehmen wie Organisationen zu stärken.

Fazit

Die zunehmende Vielfalt von Sicherheitslösungen und wachsende Angriffsflächen stellen Security-Teams vor erhebliche Herausforderungen im Bereich der IT-Sicherheit. Neue Angriffsvektoren erfordern innovative und umfassende Sicherheitsstrategien. Der Ansatz der Unified Endpoint Security bietet eine effektive Lösung. Durch die Implementierung einer integrierten Security-Plattform können Unternehmen nicht nur die Effizienz ihrer Sicherheitsmaßnahmen steigern, sondern auch eine höhere Transparenz und Kontrolle erzielen.

Andreas Fuchs



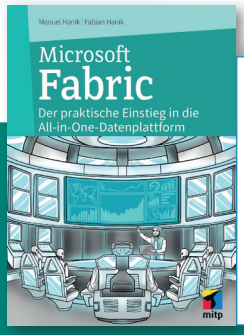
MICROSOFT FABRIC

DER PRAKTISCHE EINSTIEG IN DIE ALL-IN-ONE-DATENPLATTFORM

Mit diesem Buch erhalten Sie eine praxisorientierte Einführung in die einzelnen Komponenten der All-in-One-Datenplattform Microsoft Fabric. Es eignet sich sowohl für Einsteiger als auch für Expertinnen und Experten im Datenbereich. Ein grundlegendes Verständnis von Daten sowie erste Erfahrungen mit Python und SQL sind an einigen Stellen von Vorteil.

Praktische Einführung anhand eines durchgehenden Beispielprojekts
Anhand eines fiktiven Beispiels wird ein komplettes End-to-End-Datenprojekt in Microsoft Fabric umgesetzt, wobei alle relevanten Schritte – von der Datenanbindung über Datentransformationen bis hin zum finalen Dashboard – detailliert erläutert werden. Sie haben die Möglichkeit, alle Schritte selbst umzusetzen und das komplette Beispielprojekt praktisch nachzuvollziehen.

Mit anschaulichen Visualisierungen
Alle Komponenten von Microsoft Fabric werden anhand einer Reise durch eine fiktive Datenfabrik veranschaulicht und mit zahlreichen Illustrationen visualisiert. Auf diese Weise werden sowohl grundlegende Konzepte als auch Best Practices für die Umsetzung von Datenprojekten mit Microsoft Fabric leicht verständlich erläutert.



Microsoft Fabric:
Der praktische Einstieg in die All-In-One-Datenplattform;
Manuel Hanik, Fabian Hanik;
mitp Verlags GmbH & Co.KG; 04-2025

GRENZENLOSE MÖGLICHKEITEN

MICROSOFT 365 COPILOT UND MASSGESCHNEIDERTE KI-ASSISTENTEN IM VERGLEICH

Generative KI verändert die Arbeitswelt. Immer öfter werden damit Texte für E-Mails, Präsentationen oder Ergebnisprotokolle erstellt, Programmcodes, Bilder und Videos generiert oder Analysen durchgeführt. Der Wertschöpfungsbeitrag der neuen Technologie hat sich innerhalb kürzester Zeit vervielfacht. Die Akzeptanz ist hoch, auch weil generative KI bisher zeitraubende Routinearbeiten innerhalb von Sekunden erledigt.

Bleibt die Frage, ob sich das Potenzial bereits mit KI-Lösungen von der Stange im gewünschten Umfang heben lässt oder der Nutzen für Ihr Unternehmen mit einem maßgeschneiderten Tool um ein Vielfaches höher wäre?

Was Sie tun können, wenn die Dateninfrastruktur Ihres Unternehmens weit über die M365-Welt hinausgeht und Sie die Power der generativen KI dennoch voll ausschöpfen möchten? Lassen Sie sich einen Custom Copilot entwickeln.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 17 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/download

Mobile-IT-as-a-Service

SIEMENS MOBILITY OPTIMIERT PROZESSE MIT MASSGESCHNEIDERTER LÖSUNG VON PANASONIC TOUGHBOOK

MEHR WERT

TOUGHBOOK
Mobile-IT-as-a-Service

Siemens Mobility UK&I revolutioniert seine mobile IT-Infrastruktur durch den Einsatz des Mobile-IT-as-a-Service (MaaS) von Panasonic TOUGHBOOK. In ihrem neuen Montage- und Servicezentrum für Züge in Großbritannien nutzen die Servicetechniker robuste TOUGHBOOK Geräte für die Verwaltung von Komponenten, Zustandsbewertungen, Inspektionen und Wartungsarbeiten.

Das innovative Abo-Modell von Panasonic bietet Unternehmen eine umfassende IT-Lösung für die Ausrüstung von Mitarbeitern im stetigen mobilen Einsatz - ohne Vorabkosten und mit flexiblen monatlichen Gebühren.

Es umfasst nicht nur die Bereitstellung ausfallsicherer und langlebiger Hardware, sondern auch essenzielle Software und umfangreiche Support-Dienste. Dies ermöglicht es Unternehmen, ihre mobilen Mitarbeiter stets mit den neuesten Technologien auszustatten und ihre Produktivität zu maximieren.

Ein besonderer Vorteil von TOUGHBOOK MaaS ist die Anpassungsfähigkeit an spezifische Kundenanforderungen. Unternehmen können ihre Lösungen schnell an veränderte Bedingungen anpassen und am Ende der Vertragslaufzeit nahtlos auf neue Geräte und Services umsteigen.

Zudem unterstützt das Modell die Kreislaufwirtschaft durch die Aufarbeitung und Wiederverwendung von End-of-Life-Geräten.

Siemens Mobility UK&I setzt TOUGHBOOK Geräte für eine Vielzahl von Aufgaben ein, darunter die Verwaltung von Komponenten, Zustandsbewertungen, digitale Zwillingsinspektionen, Wartungsarbeiten, Arbeitsanweisungen, Mitarbeiterkommunikation und die Einhaltung von Gesundheits- und Sicherheitsvorschriften.

Mit dem TOUGHBOOK MaaS von Panasonic setzt Siemens auf eine zukunftssichere, effiziente und nachhaltige IT-Lösung, die den Anforderungen moderner, mobiler Arbeitsumgebungen gerecht wird.

www.toughbook.de

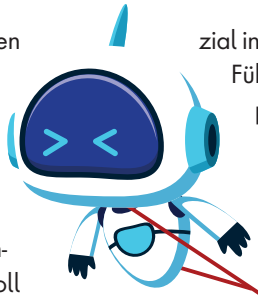
Panasonic CONNECT
TOUGHBOOK

KI BRAUCHT FÜHRUNG

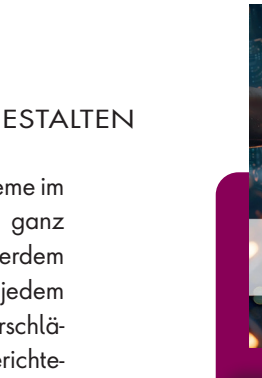
KI-TRANSFORMATION IM UNTERNEHMEN ERFOLGREICH GESTALTEN

Dieses Buch gibt Ihnen das nötige Wissen an die Hand, um die Auswirkungen und daraus entstehenden Chancen der Künstlichen Intelligenz in der Arbeitswelt zu verstehen. Es zeigt, wie Sie KI erfolgreich in Ihrem Unternehmen einführen und die Zusammenarbeit von Mensch und Maschine sinnvoll gestalten. Sie lernen, wie Sie KI zu Ihrem Vorteil und ohne Berührungsängste nutzen können.

Führung neu denken
Erfahren Sie, wie sich Führungsansätze im Zeitalter der KI verändern und welche bewährten Konzepte Sie auch für die KI-Transformation anwenden können. Ein innovatives Kapitel demonstriert das Potenzial intelligenter Systeme im Führungsalltag ganz praxisnah. Außerdem finden Sie zu jedem Thema Vorschläge für zielgerichtete Prompts zum praktischen Einsatz.



Unternehmen zukunftsfähig gestalten
Entdecken Sie Modelle und Strategien, mit denen Sie Ihr Unternehmen ganzheitlich für die KI-Zukunft aufstellen. Ein Ausblick auf kommende Entwicklungen hilft Ihnen, bereits heute die Weichen für morgen zu stellen.



KI braucht Führung:
KI-Transformation im Unternehmen erfolgreich gestalten; Jan Ahrend; mitp Verlags GmbH & Co.KG; 02-2025

UCC am Puls der Zeit

NEUPRÄGUNG DER KOMMUNIKATIONSLANDSCHAFTEN

IN DER HYBRIDEN ARBEITSWELT VON HEUTE SIND UNTERNEHMEN MEHR DENN JE AUF ZEITGEMÄSSE UND FLEXIBLE UCC-PLATTFORMEN ANGEWIESEN.

Florian Buzin, CEO, STARFACE GmbH, www.starface.com

Anrufe, Sprachnachrichten, Chats, Mails, Video-Meetings – Mitarbeiter tauschen sich in der heutigen Arbeitswelt auf multiplen Kanälen mit Kollegen und Kunden aus. Moderne UCC-Plattformen bieten dabei viele Ansatzpunkte, Arbeitsprozesse zu optimieren und die hohen Anforderungen an zeitgemäße Kommunikation besser zu erfüllen.

Telefonie trifft KI

Eine Schlüsselrolle kommt dabei auch im UCC-Umfeld der Künstlichen Intelligenz zu: Das größte Potenzial der KI liegt dabei aktuell in Funktionen wie Speech-to-Text (STT), Text-to-Speech (TTS) und KI-gestütztem Chat, über die sich intelligente IVR-Systeme (Interactive Voice Response) oder Support-Chats für eine bessere Kundenbetreuung einrichten lassen. Um dieses Potenzial zu erschließen, erweitern Hersteller wie STARFACE ihre Systeme aktuell daher um OpenAI-Schnittstellen oder integrieren KI-Funktionen in Form dedizierter Add-on-Module.

Mehr Flexibilität durch neue Schnittstellen

Um neue Technologien wie KI, aber auch Drittanbieteranwendungen wie Microsoft Teams oder Lösungen wie DATEV passgenau integrieren zu können, müssen moderne UCC-Plattformen grundsätzlich offen konzipiert sein. Diese hohe Flexibilität ist aber nur mit einer kontinuierlich optimierten API-Infrastruktur möglich. Daher wurde beispielsweise STARFACE 9 im aktuellen Release nicht nur um die angesprochene OpenAI-, sondern auch eine dedizierte CSTA-Schnittstelle und eine neue Multiline-TAPI für 3rd-Party-UCC-Lösungen erweitert. Dies macht es internen Teams aber auch externen Entwicklungspartnern leicht, neue Module und Add-Ons zu entwickeln und für die Community bereitzustellen.

Schlüsselaspekt Usability

Neue Funktionen und Add-Ons nützen allerdings wenig, wenn umständliche Bedienpfade und verschachtelte Dashboards die Mitarbeiter im Arbeitsalltag frustrieren. Gerade im UCC-Bereich, wo die Zahl der Kanäle und Kontakte stetig steigt, erwarten die Anwender heute ein hohes Maß an Usability und Übersichtlichkeit. Seit Jahren werden übersichtliche, auf Anwenderanforderungen zugeschnittene UCC-Clients angeboten, die sich über flexible Workspaces präzise in die individuelle Arbeitsumgebung einfügen. Komfortfunktionen, wie farbcodierte Präsenzinformationen, komfortable Videotelefonie und nahtlose Mobilintegration machen es den Mitarbeitern dabei leicht, miteinander und mit den Kunden in Verbindung zu bleiben.

Mehr Sicherheit und Cyberhygiene

In Zeiten zunehmender Cyberattacken erfordert auch die Telefonie zuverlässige Sicherheitsmechanismen. Neben einer robusten Cyberhygiene – etwa mit Blick auf starke Passwörter für mobile und drahtgebundene Endgeräte – gilt es dabei vor allem, die privilegierten Admin- und Service-Accounts auf der UCC-Anlage zuverlässig zu schützen. Ein separater Admin-Login ist eine wichtige erste Barriere gegen Eindringlinge. Diese lässt sich zusätzlich verstärken, wenn die Anmeldung über OAuth erfolgt und idealerweise starke Multifaktor-Authentifizierung (MFA) über externe Identity-Management-Systeme wie Microsoft Entra ID oder Google Identity ermöglicht.

Fazit

In der hybriden Arbeitswelt von heute sind Unternehmen mehr denn je auf zeitgemäße und flexible UCC-Plattformen angewiesen. Telefonie ist dabei aber nicht gleich Telefonie: Innovative KI-, Usability- und Security-Funktionalitäten bieten Unternehmen viele spannende Ansatzpunkte, um ihre Kommunikation effizienter, performanter und sicherer zu machen – und so die Weichen für eine enge und erfolgreiche Kundenkommunikation zu stellen.

Florian Buzin

IP-Tischtelefone

IM GESCHÄFTLICHEN UMFELD NACH WIE VOR UNVERZICHTBAR

Apps für die Kommunikation mögen auf den ersten Blick ideal erscheinen, doch bieten IP-Telefone Vorteile, die weit über die reine Macht der Gewohnheit hinausgehen. Es geht um fundamentale Aspekte wie Audio-Qualität, Zuverlässigkeit, Benutzerfreundlichkeit und Sicherheit.

Schnurgebundene wie schnurlose IP-Telefone der neuesten Generation nutzen (HD) Sprach-Codecs, Echo-Unterdrückung und adaptive Jitter-Puffer zur Unterdrückung von Hintergrundgeräuschen oder Erkennung von Sprechpausen, um kristallklare Gespräche zu vermitteln. Im Gegensatz dazu ist die Audio-Qualität von Smartphone- oder Laptop-Apps stark von den eigenen Komponenten, der Stabilität des WLANs im Unternehmen oder der Mobilfunkverbindung abhängig. Dabei werden Gesprächsabbrüche, Verzögerungen oder eine insgesamt schlechte Qualität der Sprachübertragung oft als Zeichen mangelnder Professionalität ausgelegt.

Multifunktionale Begleiter

Während IP-Telefone speziell für die Unternehmenskommunikation entwickelt wurden und deshalb eine maximale Serviceverfügbarkeit gewährleisten müssen, sind Apps meistens für den Einsatz auf Consumer-Geräten konzipiert und dadurch anfällig für Software-Fehler, Kompatibilitätsprobleme oder unzureichende Akkulaufzeiten. Ein plötzlicher Geräteausfall aufgrund eines leeren Akkus oder ein unerwarteter App-Absturz kann den Verlauf eines wichtigen Geschäftsgesprächs empfindlich stören.

Hinzu kommt die „Benutzerfreundlichkeit": Moderne IP-Telefone unterstützen die nahtlose Integration mit CRM-, ERP- und anderen Lösungen, darunter KI-Systemen, die Gesprochenes in Texte umwandeln und dafür kristallklare Aufzeichnungen benötigen. Diese Integration rationalisiert Kommunikationsprozesse durch Funktionen wie Click to Dial und Pop-up-Fenster mit Kundeninformationen während eines Anrufs oder die automatische Anrufprotokollierung. Die zusätzliche Integration der IP-Endgeräte mit weiteren Kommunikationstools wie Videokonferenzen, Instant Messaging und kollaborativen Anwendungen oder gar mit Gebäudeautomationssystemen macht sie zudem zu multifunktionalen Begleitern im Geschäftsalltag.

Schutz der Datenintegrität

Ein oft unterschätzter Aspekt ist die Sicherheit. IP-Telefone bieten verschlüsselte Verbindungen und fortschrittliche Sicherheitsmechanismen zum Schutz der Datenintegrität und zur Abwehr unbefugten Zugriffs. Apps hingegen, insbesondere bei Nutzung über öffentliche WLAN-Netze, können aufgrund von Schwachstellen im Betriebssystem des verwendeten Geräts anfälliger für das Abhören oder den Missbrauch von Daten sein. Ob im Homeoffice oder im Büro: Ein IP-Telefon hilft ebenfalls dabei, eine klare Trennung zwischen Beruflichem und Privatem zu schaffen.

Zu guter Letzt gelten IP-Endgeräte in bestimmten Branchen als unabdingbar. Sie funktionieren verlässlich in herausfordernden Umgebungen wie Industriehallen oder Reinräumen und bieten spezialisierte Funktionen wie Notruftasten oder eine Man-down-Funktion. In der Logistik ermöglichen Schnurlosmodelle eine reibungslose Kommunikation in großen Lagerhallen, und in Krankenhäusern stellen sie für spezielle Anforderungen wie Patientenrufsysteme, Lokalisierung von Gerätschaften oder stille Alarmierung eine zuverlässige Lösung dar.

Es ist also nicht verwunderlich, dass die Nachfrage nach IP-Telefonen mit erweiterten Integrationsfunktionen weiter ansteigt. Die neueste Studie von Market Insight zollt dem weltweiten IP-Telefonmarkt eine jährliche Wachstumsrate von 13,50 Prozent bis 2029. Snom entwickelt seine Geräte kontinuierlich weiter, mit dem Ziel, auch in Zukunft eine zentrale Rolle in der Unternehmenskommunikation zu spielen.

www.snom.com/de

Grüne IT-Energie im Windrad

WESTFALENWIND IT UND RITTAL REVOLUTIONIEREN NACHHALTIGE RECHENZENTREN

Windkraftanlagen produzieren so viel Strom, dass er zeitweise gar nicht ins öffentliche Netz eingespeist werden kann. Rechenzentren wiederum benötigen so viel davon, dass sie Netzbetreiber vor große Herausforderungen stellen. Bei WestfalenWIND IT hat man eins und eins zusammengezählt – und Rittal mit an Bord geholt.

Die Idee ist einfach: Der Strom wird dort genutzt, wo er ohnehin klimaneutral produziert wird – direkt im Windrad. Was vor mehr als zehn Jahren als Experimentalprojekt begann, ist unter der Marke windCORES längst in industriellem Maßstab skalierbar.

Die erfolgreiche Realisierung des Projekts ist dabei keinesfalls vom Himmel gefallen. Zwar klingt es einfach, ein Windrad als bestehende Infrastruktur zu nutzen und Racks einzubauen. Es gibt aber limitierende Faktoren. So muss neben der Statik, der Sicherheit und der Brandlast auch die begrenzte Fläche einkalkuliert werden. Gemeinsam mit Rittal entwickelte WestfalenWIND IT ein Drei-Ebenen-Modell, das es ermöglicht, ein mehrgeschossiges Rechenzentrum in den Fuß eines Turbinenturms zu bauen. Damit wird die Wirtschaftlichkeit pro Windenergieanlage erheblich erhöht. Auch die Bestückung der Racks bietet Spielraum.

„Wie bei einem Buddelschiff"

Die Umsetzung in die Praxis gelang nach intensiver Vorplanung: „Das war schon eine Herausforderung wie bei einem Buddelschiff, denn die ganze Technik muss durch einen kleinen Eingang passen", berichtet Dr. Fiete Dubberke, Co-Founder von windCORES.

Michael Nicolai, Leiter Rittal IT Vertrieb in Deutschland, ergänzt: „Für uns ist der energieeffiziente Betrieb von Rechenzentren schon lange ein Kernthema. Da lag eine Zusammenarbeit mit einem Produzenten von günstigem und nachhaltigem Strom auf der Hand. Es ist eine klassische Win-win-Situation, die sich im gemeinsamen Gestaltungswillen äußert: Wir suchen keine Probleme, wir lösen sie."

Die Lebensadern von Rechenzentren sind ihre Stromversorgung und Netzwerkanbindung. Erstere liegt bei windCORES buchstäblich nahe: Der Strom kommt direkt aus dem Generator der Windkraftanlage, zumindest während 90 Prozent des Jahres. In der übrigen Zeit muss Strom aus dem öffentlichen Netz bezogen werden. WestfalenWIND IT arbeitet mit zwei verschiedenen Netzbetreibern zusammen, um jederzeit eine qualitativ hochwertige Stromversorgung gewährleisten zu können. Bei vielen Anwendungen lassen sich große Rechenlasten auch zeitlich steuern und in Phasen mit viel Wind legen. So könnte das Rechenzentrum fast vollständig mit regenerativer Energie betrieben werden. Auch bei der Netzwerkanbindung wird mit doppeltem Boden gearbeitet. Zwei Backbone-Anbindungen sorgen für redundante Datenautobahnen zum Internetknoten DE-CIX nach Frankfurt. „Unsere Infrastruktur ist sehr latenzarm und bandbreitenperformant aufgestellt", versichert Fiete Dubberke.

Steile Lernkurve

Neben der technischen Umsetzung galt es zunächst, weitere Herausforderungen zu meistern: Es dauerte eine Weile, bis alle Genehmigungen für die erste windCORES-Anlage im Kreis Paderborn vorlagen. Mittlerweile ist windCORES II im nordrhein-westfälischen Lichtenau in Betrieb genommen worden. Dort werden künftig sowohl HPC für KI als auch Simulationen für autonomes Fahren ausgeführt. Während die Infrastruktur, wie Si-

WINDCORES: VOM PILOTPROJEKT ZUM REALEN INDUSTRIE-STANDARD

Das Pilotprojekt gewann 2019 bereits den Deutschen Rechenzentrumspreis. Jetzt wurde daraus ein skalierbares Industrieprojekt mit Rittal IT-Infrastruktur. Ein großer Automobilhersteller verlegt umfassende Anwendungen in ein windCORES-Rechenzentrum mit 50 Racks. Dort werden künftig High-Performance-Computing für KI und GenAI sowie Simulationen für autonomes Fahren klimaneutral ausgeführt. Die Umsetzung erfolgt im Colocation-Modell mit einem IT-Dienstleister. Rittal liefert für WestfalenWIND IT die Komplette Infrastruktur, darunter drei Sicherheitsräume, IT-Racks, Klimatisierung, unabhängige Stromversorgung (USV) und Monitoring.

cherheitsräume, IT-Racks oder die Klimatisierung, von Rittal zur Verfügung gestellt wird, agiert WestfalenWIND IT als nachhaltiger IaaS-Anbieter inklusive kompletter Cloud-Lösungen.

Apropos Infrastruktur: Sie ist ein wichtiges Kriterium bei allen Wirtschaftlichkeitsberechnungen. Dass der Bedarf an Rechenkapazität seit Jahren stark wächst und dieser Trend aufgrund neuer Technologien weiter anhalten wird, ist sicher. Die Realität hinkt diesen Ansprüchen aber manchmal hinterher: Bis ein herkömmliches Rechenzentrum gebaut ist, können mitunter Jahre vergehen – von der zusätzlichen Flächenversiegelung ganz zu schweigen. Windkrafttürme stehen bereits. „Es sind zwar kleinere Einheiten, die aktuell bis zu 1 MW an IT-Leistung bereitstellen können. Aber die Infrastruktur ist da und fast sofort verfügbar. Sie bietet einen echten Mehrwert für den RZ-Markt", betont Fiete Dubberke.

Eine vierstellige Anzahl der Türme eignet sich in Deutschland für die RZ-Aufrüstung, und klar, sie sind ein Blickfang. Aber das Konzept, umweltfreundlichen Strom möglichst in der Nähe des Erzeugers zu nutzen, lässt sich mit ein wenig Flexibilität auch auf andere Weise realisieren. Das funktioniert, weil WestfalenWIND IT früh und massiv in die komplette Kette der Stromerzeugung und -weiterleitung investiert hat. So hält der Geschäftsführer auch Containerlösungen an einem Windrad oder einem der unternehmenseigenen Umspannwerke für potenziell geeignet, falls der Turm selbst keine Option ist. Allein im Kreis Paderborn stehen dafür Werke in einer Größenordnung von rund 450 Megawatt zur Verfügung. Bei der Sicherheit müssen hier wie dort keine Abstriche gemacht werden. Alle benötigten Vorkehrungen und Maßnahmen werden genauso wie in jedem anderen Rechenzentrum nachgewiesen. Zusätzlich wird eine TIER-3-Zertifizierung angestrebt.

Seeing is Believing

Ziel der WestfalenWIND IT ist es nun zum einen, neue Kunden für die innovativen Rechenzentren zu gewinnen. „Auf dem Papier mögen manche noch Zweifel haben. Aber wer eine Anlage einmal an Ort und Stelle gesehen hat, ist in der Regel schnell überzeugt", weiß Fiete Dubberke zu berichten. Zum anderen soll das Konzept weiterentwickelt werden. Waren die bisherigen Arbeiten weitgehend eigenkapitalfinanziert, läuft seit 2023 ein dreijähriges Forschungsprojekt, das der Bund mit insgesamt rund 2,5 Millionen Euro fördert. In diesem Rahmen will ein Konsortium die Infrastruktur und Betriebsführung eines HPC-Clusters innerhalb mehrerer Windenergieanlagen entwickeln.

Im aktuellen Marktumfeld stehen die Ampeln für windCORES mittlerweile auf Grün. Die intelligente Nutzung vorhandener Infrastruktur mit klimaneutral erzeugter Energie bietet eine marktfähige und skalierbare Alternative. „Für neue Technik braucht es immer den richtigen Zeitpunkt", ist Michael Nicolai überzeugt, „und der ist jetzt."

David Schahinian | www.rittal.de

Nachhaltiges Edge Computing

SO ERGRÜNT DER NETZWERKRAND

Die Datenmengen in Unternehmen wachsen exponentiell und ihre IT-Infrastruktur wird immer verteilter und disaggregierter. Unternehmen betreiben zunehmend Edge Computing, sprich: Sie verarbeiten immer mehr Daten nahe an dem Ort, an dem sie entstehen, und nicht in einem zentralen Rechenzentrum oder einer Cloud. Dafür gibt es eine ganze Reihe an Gründen: Am Standort der Datenerhebung ist das Internet nicht zuverlässig verfügbar, die Bandbreite reicht nicht aus, die Kosten für die Datenübertragung wären zu hoch, die Latenzen zu groß, oder die Daten sind so sensibel, dass sie das Unternehmen besser nicht verlassen.

Gleichzeitig rückt das Thema Nachhaltigkeit auf der Agenda von Unternehmen immer weiter nach oben. Sie wird zunehmend als entscheidender Faktor für langfristigen Erfolg, nachhaltiges Wachstum und gesellschaftliche Verantwortung anerkannt. Deshalb haben sich viele Unternehmen inzwischen eigene Nachhaltigkeitsziele gesetzt. Da die Dimension ihrer Edge-Infrastrukturen wächst, beziehen sie auch diese zunehmend in ihre Nachhaltigkeitsbetrachtungen mit ein.

Das beginnt bereits bei der grundsätzlichen Entscheidung, ob Daten am Netzwerkrand oder zentral verarbeitet werden sollen. Das Edge kann dabei mit einigen Vorteilen punkten, hat gegenüber Rechenzentrum und Cloud aber auch einige gravierende Nachteile. Die Verarbeitung der Daten vor Ort reduziert den Energieaufwand für den Transfer von Daten über weite Strecken zu den Rechenzentren und in die Clouds. Zentrale Infrastrukturen ermöglichen dagegen aber naturgemäß eine insgesamt effizientere Nutzung von Ressourcen und Energie als dezentrale Infrastrukturen. Da zentrale Infrastrukturen von viel mehr Nutzern verwendet werden erzielen sie Effizienzgewinne, die kleine Edge-Installationen meist nicht erreichen können.

Das Edge ist in vielen Fällen alternativlos

So oder so gibt es zahlreiche Anwendungen, bei denen das Rechenzentrum oder die Cloud von Haus aus keine akzeptable Alternative darstellen. Dazu zählen:

- Anwendungen, die niedrige Latenzen oder hohe Bandbreiten erfordern wie beispielsweise Hochfrequenz-Handelssysteme im Finanzwesen oder Computer-Vision-Systeme in einer Fertigungsstraße;

EDGE COMPUTING WÄCHST LÄNGST AUS SEINEM ANFANGSSTADIUM HINAUS UND WIRD INZWISCHEN VON ZAHLREICHEN BRANCHEN GENUTZT.

Chris Kramar, Director und General Manager OEM Solutions DACH, Dell Technologies, www.dell.com

- Unternehmenskritische Legacy-Systeme wie etwa SCADA. Sie vertragen oft keinerlei Ausfälle, laufen häufig in lokalen Air-Gapped-Netzwerken oder nutzen nicht standardisierte Protokolle, die eine lokale Datenverarbeitung zwingend erforderlich machen;

- Anwendungen, die strengen gesetzlichen Anforderungen an Datenschutz und Datensicherheit unterliegen.

Mehrere Möglichkeiten für ein nachhaltigeres Edge

Solche Anwendungen werden bislang oft in nicht klimatisierten Räumen betrieben, beispielsweise in einem Hinterzimmer im Einzelhandel oder in einer Fabrikhalle. Nachhaltig ist das natürlich nicht. Unternehmen können aber andere Wege gehen, um den Betrieb solcher Anwendungen am Netzwerkrand umweltfreundlicher zu gestalten. Folgende Möglichkeiten stehen ihnen zu Verfügung:

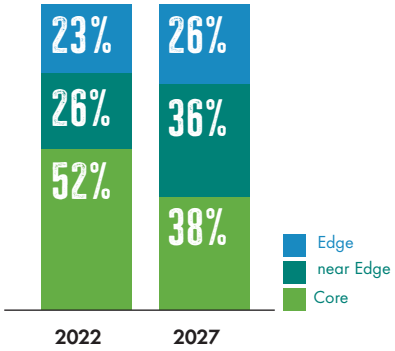
- Beim Aufbau neuer oder bei der Erneuerung bestehender Edge-Infrastrukturen können Unternehmen moderne Rechnungszentrums-Technologien nutzen. Dazu zählen etwa neue Energiekonzepte wie der Einsatz von Gasgenera-

toren, freie Luftkühlung oder die Nutzung der Abwärme zur Beheizung von Gebäuden oder zur Erzeugung von Warmwasser auf dem Firmengelände. Moderne Server ermöglichen weitere Optimierungen bei der Energieeffizienz. Sie bringen neuere Chips mit, die bei gleichem Energieverbrauch mehr Leistung erbringen, nutzen neue Materialien für eine bessere Kühlung und verwenden Kühltechnologien wie Flüssigkeits- oder Tauchkühlung.

> Für Unternehmen mit umfangreicher oder stark verteilter Edge-Verarbeitung kann Edge as a Service (EaaS) eine nachhaltige Alternative sein. Cloud-, Colocation- und Rechenzentrums-Anbieter bauen zunehmend kleine, verteilte Rechenzentren an strategischen Standorten auf, etwa in städtischen Ballungsgebieten oder in Industrieparks, um die Latenz für Unternehmen in der Region zu minimieren. Diese Mini-Rechenzentren bieten ähnliche Effizienzvorteile wie große Rechenzentren oder Clouds.

> Eine spezielle Variante von Edge as a Service ist Multi-Access Edge Computing (MEC). Beim Aufbau ihrer 5G-Infrastruktur richten Telekommunikations-Betreiber auch eigene Edge-Computing-Standorte für die Verarbeitung ihrer 5G-Workloads ein. Diese Standorte nutzen sie nicht nur für sich selbst, sondern bieten sie auch Unternehmen an. Diese können für ihre Anwendungen Rechenressourcen mieten, die sich in Mobilfunk-Basisstationen oder in unmittelbarer Nähe davon befinden. Dabei profitieren Unternehmen nicht nur von den Energieeffizienz-Gewinnen durch die geteilten Ressourcen, sondern auch von den hohen Geschwindigkeiten und der flächendeckenden Abdeckung der 5G-Netze.

IMMER MEHR DATEN WERDEN AM EDGE VERARBEITET



Im Jahr 2027 werden bereits % aller Daten am Edge oder in der Nähe davon verarbeitet werden

(Quelle: 451 Research, Edge Workload Total Adressable Market (TAM), 2023).

Unternehmensweite Nachhaltigkeit fördern

Zur Betrachtung von Edge Computing unter dem Gesichtspunkt der Nachhaltigkeit zählt aber nicht nur seine möglichst umweltgerechte Gestaltung, sondern auch sein gezielter Einsatz. IoT-Daten, die am Netzwerkrand gewonnen und verarbeitet werden, können nämlich einen wichtigen Beitrag dazu leisten, unternehmensweit nachhaltiger zu wirtschaften. Fertigungsstraßen beispielsweise können damit energieeffizienter arbeiten; und intelligente Gebäude können mit Daten, die sie vor Ort analysieren, den Energieverbrauch optimieren, indem sie etwa in ungenutzten Räumen automatisch Klimaanlagen und Licht ausschalten oder die Heizung in Abhängigkeit vom Wetter regulieren.

Edge Computing wächst längst aus seinem Anfangsstadium hinaus und wird inzwischen von zahlreichen Branchen genutzt. Das allgemeine Verständnis für seine Auswirkungen auf die Nachhaltigkeit entwickelt sich gerade erst. Der Aufbau einer grüneren Edge-Infrastruktur – sei es on-Premises oder mithilfe der wachsenden Schar von EaaS-Anbietern – ist ein entscheidender Schritt nach vorn. Darüber hinaus kann das Edge gezielt dafür eingesetzt werden, zentrale Geschäftsprozesse im Sinne der Nachhaltigkeit umzugestalten und zu optimieren.

Chris Kramar

Alternative zu Großrechenzentren

MODULRECHENZENTREN: FLEXIBEL, EFFIZIENT UND ZUKUNFTSSICHER

Modulrechenzentren bieten eine effiziente Lösung für veränderte Anforderungen an die IT: Sie können genau dort platziert werden, wo schnelle, flexible und hochverfügbare Rechenleistung benötigt wird.

Besonders in datenintensiven oder latenzkritischen Anwendungsfeldern wie Künstlicher Intelligenz (KI), dem Internet der Dinge (IoT) oder der Industrie 4.0 spielen modulare Rechenzentren ihre Stärken aus. Ihr größter Vorteil liegt in ihrer Nähe zu den Daten: Durch die dezentrale Verarbeitung lassen sich Datentransfers minimieren, so dass Unternehmen ohne Verzögerung auf Daten zugreifen können. Dies ist essenziell für die Verarbeitung großer Datenbestände in KI-Anwendungen – das Large Language Model (LLM) kommt zu den Daten.

Nachhaltigkeit und Kostenersparnis

Dank ihrer Mobilität lassen sich diese Rechenzentren zudem schnell an dem gewünschten Standort aufbauen. Und sie punkten, wenn es um die Energieeffizienz geht. Niedrige PUE-Werten sorgen dafür, dass Betriebskosten sinken und der ökologische Fußabdruck minimiert werden kann. Obwohl kompakt, erfüllen modulare Rechenzentren höchste Sicherheitsanforderungen und sind nach EN50600 zertifizierbar. Ein weiterer Vorteil liegt in ihrer Wartungsfreundlichkeit. Ein Paradebeispiel für die zunehmende Bedeutung modularer Rechenzentren ist die Übernahme der innovIT AG durch den IT-Dienstleister und Rechenzentrumsbetreiber noris network. Damit lassen sich nicht nur innovative KI-Rechenzentren anbieten, sondern auch Managed Services wie Private-Cloud-Systeme on Premises bereitstellen.

> OBWOHL KOMPAKT, ERFÜLLEN MODULARE RECHENZENTREN HÖCHSTE SICHERHEITSANFORDERUNGEN UND SIND NACH EN50600 ZERTIFIZIERBAR.
>
> **Florian Sippel, COO, noris network AG.**
> **www.noris.de**

Florian Sippel

ROBOTIK-ADOPTION IN DER INDUSTRIE

BEGEISTERUNG UND BEDENKEN

TOP-ROLLEN FÜR ROBOTIK IN DEUTSCHEN UNTERNEHMEN

Eine Erhebung unter 1.000 Führungskräften liefert neue Erkenntnisse zum Robotereinsatz. 71 Prozent der Befragten nutzen bereits Robotik oder planen deren Implementierung. 77 Prozent der Teilnehmer sowohl in Deutschland als auch international erwarten, dass Robotik zentrale Branchenaufgaben übernehmen wird. Allerdings äußern etwa 30 Prozent der deutschen Befragten Vorbehalte gegenüber der direkten Zusammenarbeit mit Robotern.

Global fördern besonders Sicherheitsfortschritte und Risikominimierung sowie nachgewiesene Leistungsfähigkeit das Vertrauen in diese Technologien. Deutsche Entscheidungsträger beschäftigen sich verstärkt mit dem wirtschaftlichen Nutzen und der Transformationsumsetzung.

Fast ein Drittel der weltweit Befragten (32 Prozent) hält den eigenen Arbeitsplatz noch nicht für bereit, Roboter einzusetzen. Das könnte für Arbeitgeber zur Herausforderung werden – sowohl bei der Nutzung der Technologie als auch bei der Sicherheit der Mitarbeiter. Zudem sorgen sich 58 Prozent über mögliche Sicherheitsrisiken, und 29 Prozent berichten, dass in ihrer Organisation bereits gefährliche Situationen mit Robotern aufgetreten sind.

www.qnx.com

Software-WORM-Archiv

MAXIMALE UNABHÄNGIGKEIT VON TECHNOLOGIEZYKLEN

Die revisionssichere Archivierung von Daten war schon immer ein wichtiges Thema – nun gewinnt sie zunehmend an Bedeutung. Vorschriften zur sicheren Aufbewahrung von Daten, wie sie Behörden oder Regelwerke zur Aufbewahrung spezieller digitaler Daten im medizinischen Umfeld fordern, sind vielfältig. Verstärkt wird der Aufwand an Archivierung durch die fortschreitende Digitalisierung.

Die Herausforderung liegt in den mittlerweile sehr kurzen Innovationszyklen der Informationstechnologie, denn sie trifft auf gesetzliche Aufbewahrungsfristen von bis zu 30 Jahren. Folglich sind die Aufbewahrungspflichten meist deutlich länger als der Technologie-Lifecycle von Speichermedien. Da die Archivdaten jedoch jederzeit zur Verfügung stehen müssen, sind Unternehmen entweder dazu gezwungen, alte Technologien über Jahrzehnte am Leben zu erhalten oder die Archive häufig und kostenintensiv auf neuere Technologien zu migrieren. Eine dritte Möglichkeit ist es, sich von den Neuerungen der Hardware zu befreien und die Archive einmalig in eine Lösung zu überführen, die aufgrund ihrer Technologie von den Zyklen nicht betroffen ist. Eine hardware-unabhängige WORM (Write Once Read Many)-Archivsoftware, wie FileLock von GRAU DATA – einem seit Jahren auf Archivierung spezialisierten Softwarehersteller - kann die Lösung für die langfristige und revisionssichere Aufbewahrung von Daten sein. Bei dieser Lösungsvariante werden die Daten im WORM-Format auf nahezu jeder Art von Speichermedium geschrieben und Administratoren können ihre Hardware-Plattformen unabhängig ändern und modernisieren. Und damit Unternehmen sicher sein können, dass sie auch langfristig auf die passende Technologie setzen, liegt für FileLock ein Rechtsgutachten von KPMG vor, das diese Archiv-lösung nach den gesetzlichen Vorschriften absichert.

EINE LANGFRISTIGE UND REVISIONSSICHERE ARCHIVIERUNG VON DATEN SOLLTE UNABHÄNIG VON DEN INNOVATIONSZYKLEN SEIN.

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

WORM gestern, heute und morgen aktuell

In einem WORM können die Daten nach der Speicherung zwar gelesen, jedoch nicht mehr verändert oder überschrieben werden. Im Gegensatz zu hardware-basierten WORM-Lösungen ist FileLock ein Software-WORM, das eine Unabhängigkeit von Hardware und Speichermedien garantiert. Das Software-WORM wird auf einer lokalen Festplatte oder im unternehmensweiten Speichernetzwerk eingerichtet und etabliert eine dedizierte Softwareschicht, in die nicht eingegriffen werden kann. Zugelassen sind lediglich Schreibvorgänge für neue Dateien und das Lesen existierender Daten. Der Betrieb des Software-WORM erfolgt auf einer separaten und besonders geschützten Festplattenpartition. Eine zusätzliche Verschlüsselung der Daten sorgt für Sicherheit gegen Manipulation der Daten von außen.

Mit maximaler Unabhängig in die Zukunft

Die Datenarchivierung sollte möglichst wenig zusätzlichen Administrationsaufwand und Kosten erfordern. Ein hoher Automatisierungslevel und eine Unabhängigkeit von den Technologiezyklen der Hardware sorgen für eine deutliche Entlastung über viele Jahre hinweg. Gleichzeitig gilt es, die allgemeinen und branchenspezifischen Vorschriften der Revisionssicherheit einzuhalten, was mit geprüften und zertifizierten Lösungen zu bewerkstelligen ist. Die Lösung liegt in einer plattformunabhängigen und schlanken WORM-Software-Lösung wie FileLock, die trotz stetigem Datenzuwachs und IT-Modernisierungen langfristig für Revisionssicherheit sorgt.

Kai Hambrecht

GRAU DATA
Your data \ Your control _

API-Plattformen

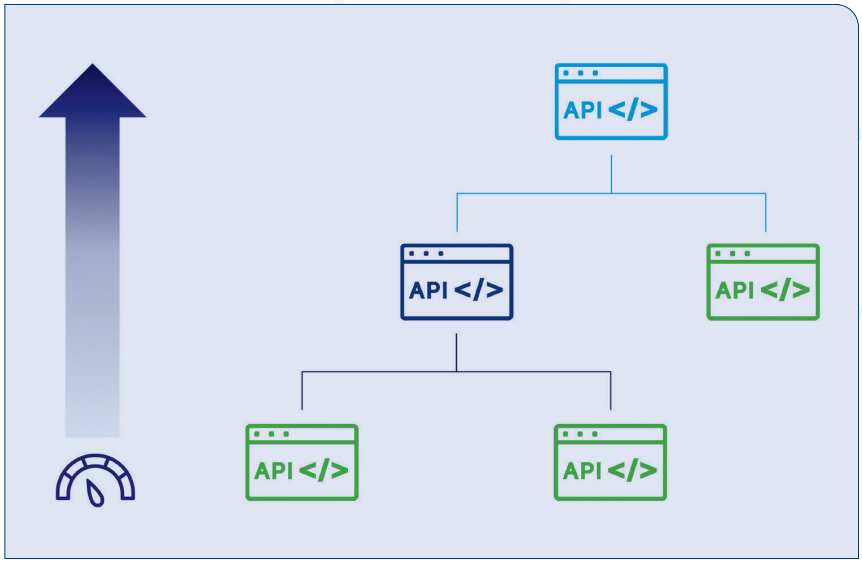
RÜCKGRAT DER DIGITALISIERUNG ODER INNOVATIONSBREMSE?

APIs sind das Bindeglied der modernen IT-Welt. Sie verbinden Daten, Systeme und Technologien miteinander, ermöglichen neue Geschäftsmodelle und beschleunigen den Fortschritt in nahezu allen Branchen. Ohne sie wäre der Zugriff auf die wertvolle Ressource „Daten" stark eingeschränkt – und damit die Entwicklung neuer digitaler Lösungen, von kontaktlosem Bezahlen bis hin zur Automatisierung unternehmensinterner Prozesse. Eine unstrukturierte API-Landschaft kann jedoch genau das Gegenteil bewirken: Komplexität wächst, Wartungskosten steigen, Innovationen werden gebremst.

Zwischen Antrieb und Risiko

Eine gut durchdachte Schnittstellenarchitektur kann die digitale Transformation erheblich beschleunigen. Dies gelingt, wenn Unternehmen grundlegende Funktionen nicht immer wieder von Grund auf entwickeln, sondern auf bestehenden Lösungen aufbauen und dadurch Zeit und Ressourcen sparen. Als Indikator und KPI für den Erfolg dient die Wiederverwendungsrate einer API. Denn auch wenn APIs häufig für einen konkreten Anwendungsfall entwickelt werden, sollten sie immer so gestaltet sein, dass sie auch für andere Projekte genutzt werden können. Ein Beispiel aus dem Finanzwesen verdeutlicht dies: Eine API kann den Kontostand eines Kunden ändern, eine andere ihn in Echtzeit abrufen. Durch ihre Kombination entsteht eine Überweisungs-API, die zunächst die Deckung prüft und die Transaktion nur bei ausreichendem Guthaben freigibt. Diese Überweisungs-API lässt sich dann flexibel über verschiedene Kanäle nutzen – im Online-Banking, in mobilen Apps oder als Service für FinTechs.

Während früher vorwiegend monolithische Anwendungen dominierten, schaffen APIs heute also wesentlich mehr Flexibilität. Dadurch entstehen jedoch auch neue Herausforderungen: Die IT besteht jetzt aus unzähligen APIs, die miteinander kommunizieren. Diese einzelnen Systeme müssen verwaltet werden, und auch die Verbindungen zwischen ihnen müssen stabil und sicher bleiben.



Die Wiederverwendung von APIs beschleunigt Delivery und Innovation.
(Quelle: Stefan Mesquita, Deutsche Bank API Banking)

Die unterschätzten Risiken einer unkontrollierten API-Landschaft:

- **Technische Schulden:** Ohne eine klare Strategie entstehen inkonsistente, redundante oder veraltete APIs, die schwer zu warten und zu nutzen sind. Dies führt zu höheren Wartungskosten und erschwert auch die Einführung neuer Technologien.

- **Sicherheitsrisiken:** APIs sind ein beliebtes Ziel für Cyberangriffe. Eine robuste Sicherheitsarchitektur ist daher unerlässlich, um Sicherheitslücken zu vermeiden.

- **Mangelnde Standards:** Fehlende Vorgaben für die Entwicklung und Verwaltung von APIs führen zu Inkonsistenzen und ineffizienter Nutzung sowie zu einer verstärkten Individualisierung einzelner APIs, was die Wartung, Skalierbarkeit und Anpassbarkeit erheblich erschwert.

- **Undurchsichtige Landschaft:** Je mehr APIs ohne zentrale Steuerung und Dokumentation entstehen, desto unübersichtlicher wird die Gesamtlandschaft. Dies führt zu einem Verlust an Transparenz und Kontrolle.

Struktur & Stabilität statt Komplexität

Um das Potenzial von APIs voll auszuschöpfen, bedarf es einer durchdachten Steuerungsebene, wie zum Beispiel einer API-Management-Plattform. Diese hilft dabei, Zugang, Sicherheit und Performance zentral zu koordinieren. Doch was

macht eine API-Plattform darüber hinaus erfolgreich?

5 zentrale Bausteine einer erfolgreichen API-Plattform:

#1 API-Governance für Skalierbarkeit:
Einheitliche Standards wie Namenskonventionen, Versionierung und Sicherheitsprotokolle sorgen für eine konsistente und leicht verwaltbare API-Landschaft.

#2 Developer-Portal für Transparenz & Effizienz:
Die Bereitstellung einer zentralisierten API-Dokumentation und Ressourcen wie Code-Snippets erleichtern die Integration und minimieren Fehler.

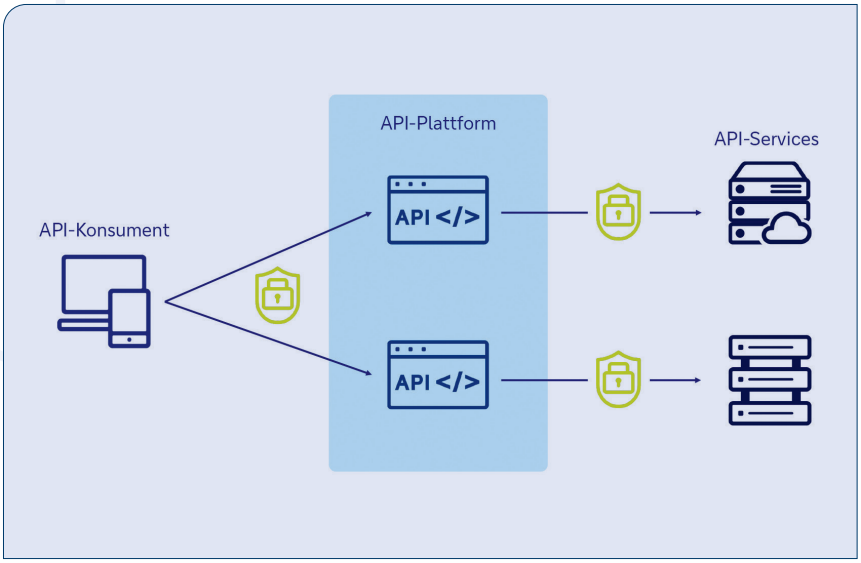
#3 Monitoring & Observability zur Problemfrüherkennung:
Die Überwachung der API-Performance verhindert Ausfälle und sichert Stabilität.

#4 Strukturiertes API-Lifecycle-Management:
Die kontinuierliche Optimierung neuer APIs und eine strukturierte Abschaltung veralteter APIs sorgt für Übersichtlichkeit und Effizienz.

#5 Cross-funktionale Zusammenarbeit:
Eine gemeinsame API-Strategie stellt sicher, dass alle Teams auf die gleichen Ziele hinarbeiten.

Agilität & Wachstum durch APIs
APIs sind mehr als Schnittstellen – sie bilden die Basis agiler, skalierbarer Systeme und eröffnen neue Möglichkeiten. Sie erleichtern die Bereitstellung von Diensten über verschiedene Plattformen, ermöglichen die gezielte Anpassung an Kundenbedürfnisse und fördern innovative Geschäftsmodelle. Eine durchdachte API-Strategie verschafft deshalb technologischen Vorsprung und entscheidende Wettbewerbsvorteile.

Um mit dem Unternehmenswachstum Schritt zu halten, ist eine flexible, skalierbare API-Governance nötig. Klare Stan-



API-Plattform: Entkopplungsschicht für schnellere und flexiblere Integration.
(Quelle: Stefan Mesquita, Deutsche Bank API Banking)

dards verbessern die Zusammenarbeit zwischen Teams, beschleunigen die Entwicklung und vereinfachen das Onboarding neuer Entwickler. So können Unternehmen schneller auf Marktveränderungen reagieren und ihre Innovationskraft steigern. Die Monetarisierung von APIs erschließt ihnen zudem neue Umsatzpotenziale und Kunden, beispielsweise indem sie ihre Schnittstellen Drittanbietern wie etwa Vergleichsportalen zur Verfügung stellen.

Ein zentraler Erfolgsfaktor ist der API-First-Ansatz, der eine frühzeitige OpenAPI Specification (OAS) voraussetzt. Eine präzise Spezifikation ermöglicht es Entwicklungsteams, parallel zu arbeiten und Implementierungen nahtlos zu integrieren. Dadurch können Produkte schneller auf den Markt gebracht werden. Mock APIs und Contract Testing stellen sicher, dass APIs frühzeitig getestet und iterativ optimiert werden können – das minimiert Verzögerungen und fördert eine schlanke Entwicklung. Darüber hinaus sorgen Microservices für maximale Flexibilität. Die Entkopplung einzelner Komponenten ermöglicht unabhängige Updates, optimierte Skalierung und reibungslose Weiterentwicklung ohne Beeinträchtigung des Gesamtsystems. In Kombination mit API-Governance und API-First-Prinzipien entsteht eine leistungsfähige Architektur, mit der Unternehmen effizient auf neue Anforderungen reagieren können.

> API-PLATTFORMEN ERMÖGLICHEN ES UNTERNEHMEN, SICH SCHNELL AN MARKTVERÄNDERUNGEN ANZUPASSEN UND INNOVATIONEN VORANZUTREIBEN – WENN SIE RICHTIG GEMANAGT WERDEN.
>
> **Stefan Mesquita, Chief Product Owner API Banking, Deutsche Bank, https://developer.db.com/**

Fazit

APIs bilden das Rückgrat der Digitalisierung – ohne eine klare Strategie führen sie jedoch zu technischen Schulden und bremsen die Innovationkraft. Die Entwicklung einer API-zentrierten Architektur erfordert ein grundlegendes Umdenken auf technischer sowie organisatorischer Ebene. Bereits in der Planungsphase müssen Sicherheitsaspekte, Designprinzipien und Skalierbarkeitsfragen berücksichtigt werden, um APIs langfristig als wertschöpfende Assets zu etablieren. Unternehmen sollten APIs deshalb nicht nur als technisches Werkzeug, sondern als strategische Instrumente für ihre Geschäftsentwicklung begreifen. Eine maßgeschneiderte API-Strategie muss dabei Sicherheit und Offenheit in Einklang bringen, um Innovationen zu fördern, ohne Kontrolle und Compliance aus den Augen zu verlieren. Werden APIs richtig eingesetzt, entfalten sie ihr volles Potenzial als Katalysatoren für digitale Transformation und Wachstum.

Stefan Mesquita

Mobiles Zahlen mit der Smartwatch

Nahtlose Integration von Bankgeschäften für sichere Smartwatch-Zahlungen

Vergleichsportale

Bündelung von Echtzeitdaten für nahtlose Vergleiche und Vertragsabschlüsse

Sofortzahlungen

Sichere Zahlungsabwicklung in Echtzeit über APIs

Anwendungsbeispiele:
Wie APIs neue Geschäftsmöglichkeiten schaffen.

(Quelle: Stefan Mesquita, Deutsche Bank API Banking)

HÖCHSTE ZEIT FÜR WINDOWS 11

WARUM SIE NICHT LÄNGER WARTEN UND IHRE ARBEITSPLÄTZE AUF WINDOWS 11 UMSTELLEN SOLLTEN

Eine Dekade lang war Windows 10 das weltweit führende Betriebssystem. Laut Statista lag der globale Marktanteil im Januar 2023 bei rekordverdächtigen 78 Prozent. Die Zukunft gehört dem System dennoch nicht. Es wird von Microsoft turnusmäßig durch Windows 11 ersetzt. Wir erklären, was das bedeutet und wie Sie Ihr Unternehmen richtig vorbereiten.

Stichtag für den Windows 10 „End of Support" ist der 14. Oktober 2025. Von diesem Tag an wird Microsoft für das etablierte Betriebssystem keine kostenlosen Softwareupdates und Sicherheitsfixes mehr bereitstellen. Offiziell eingestellt wird auch der technische Support.

Die PCs funktionieren danach zwar weiterhin, werden aber nicht mehr aktualisiert. Im Klartext heißt dies: Unternehmen, die betagte Windows 10 PCs bis zum Stichtag nicht ausgetauscht oder auf Windows 11 upgegradet haben, gehen hohe Risiken ein.

Wir erklären, was das bedeutet und wie Sie Ihr Unternehmen richtig vorbereiten.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 17 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/download

Datenaustausch ohne Grenzen

INNOVATIONSSTRATEGIEN FÜR VERNETZTE UNTERNEHMEN

Unternehmen haben das ökonomische Potenzial von Daten entdeckt. Doch am Austausch von Daten untereinander hakt es noch. Was viele Unternehmen abhält, sind ihre offene Fragen zur Implementierung, Kompatibilität und zum Datenschutz. Wie können diese Einstiegshürden aus dem Weg geräumt werden?

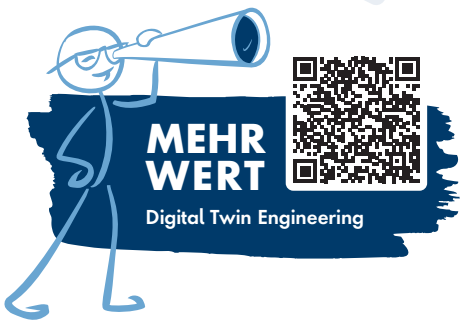
Der Austausch von Daten bietet einen effektiven Hebel für wirtschaftliches Wachstum, so viel steht fest. Doch die Anzahl der Firmen, die dieses Potenzial nutzen, hält sich weiterhin in Grenzen. Während der Anteil an Unternehmen, die Daten anderer einholen, inzwischen auf über ein Drittel gestiegen ist, stagniert der Anteil, der eigene Daten an andere herausgibt auf einem deutlich niedrigeren Niveau. Das zeigt eine Bitkom-Umfrage aus dem vergangenen Jahr. Für den Wirtschaftsstandort Deutschland ist es wichtig, die dafür verantwortlichen Hürden abzubauen.

JETZT LIEGT ES AN UNTERNEHMEN, DAS ENORME WIRTSCHAFTLICHE POTENZIAL VON DIGITALEN DATENRÄUMEN ZU NUTZEN.

Frank Schnicke, Leiter der Abteilung „Digital Twin Engineering", Fraunhofer-Institut für Experimentelles Software Engineering IESE, www.iese.fraunhofer.de

Digitale Datenräume als Basis für einen effizienten Datenaustausch

Möglich wird der effiziente und sichere Datenaustausch über digitale Datenräume. Hier entsteht zurzeit ein vielschichtiger Markt. Pilotprojekte sind beispielsweise Catena-X für die Automobilindustrie sowie weitere Datenräume, die aus der Initiative Manufacturing-X von Wirtschaft, Politik und Wissenschaft hervorgegangen sind. Zusätzlich haben wir vom Fraunhofer-Institut für Experimentelles Software Engineering IESE gemeinsam mit Partnern den AAS Dataspace for Everybody als einfach nutzbare Datenraum-Plattform entwickelt. Mit dieser können Firmen digitale Datenräume besonders niedrigschwellig testen und in Anwendung bringen.



Verwaltungsschalen ermöglichen interne und externe Kompatibilität

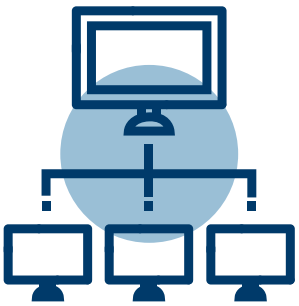
Die Nutzung von Datenräumen setzt voraus, dass eigene Daten digital erfasst werden. Doch Digitalisierung ist kein Selbstzweck. Daher empfehle ich Unternehmen immer, schnelle Mehrwerte zu identifizieren, die gleichzeitig auf strategische Ziele einzahlen: Dort, wo Betriebe am meisten Zeit und Geld verlieren, sollten sie mit der Digitalisierung anfangen. Früher sind dabei oft Silos entstanden, die sich später nur aufwändig integrieren ließen. Deshalb ist es wichtig, Daten gleich so anzulegen, dass sie mit anderen Elementen zusammen funktionieren. Dazu eignen sich Digitale Zwillinge auf Basis von Verwaltungsschalen.

Ein Digitaler Zwilling ist eine virtuelle Repräsentation von realen Assets und Prozessen. Unternehmen, die Digitale Zwillinge ihrer physischen Assets haben, können damit Analysen und Simulationen durchführen, Optimierungen finden oder sogar ihre Produktion steuern. Die Daten in Verwaltungsschalen liegen in standardisierten Formaten vor. Damit sind sie mit weiteren Digitalisierungsprojekten kompatibel, ebenso wie mit zukünftig beschafften IT- und OT-Systemen. Die Interoperabilität ist also sichergestellt.

Mit niedrigschwelligem Einstieg schnell in die Anwendung kommen

Beim AAS Dataspace for Everybody lassen sich Verwaltungsschalen mithilfe der Werkzeuge der Open Source Software Eclipse BaSyx schnell und unkompliziert erstellen. Nutzen Betriebe solche vorkonfigurierten Softwarewerkzeuge profitieren sie von einer erheblichen Kosten- und Zeitersparnis. Das kann die Digitalisierung in Industrieunternehmen um ein Vielfaches beschleunigen und ebnet noch mal deutlich mehr Unternehmen als bislang den Zugang zu Digitalen Zwillingen.

Sind die notwendigen Daten im Unternehmen erst einmal erfasst, ermöglicht es der AAS Dataspace for Everybody, ihren Austausch mit anderen Firmen zunächst in einer Prototypumgebung zu testen. Onboarding und Bedienung sind hierbei gezielt einfach gehalten, sodass

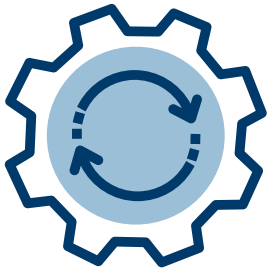


Betriebe schnell in die Anwendung kommen. Nachdem der Datentausch erprobt wurde, kann die Migration zum Produktivbetrieb mit Service Level Agreements von Partnern des Fraunhofer IESE nahtlos erfolgen.

Die Vorteile des Datenaustausches nutzen

Generell gilt: Wer eigene Daten vorliegen hat, kann und sollte mit diesen auch in den Austausch gehen. Vielen Unternehmen ist bereits klar, dass sie mit zusätzlichen externen Daten genauere Berechnungen und Optimierungen vornehmen können. Doch oft wird unterschätzt, was das Herausgeben von Daten erwirken kann. Es kann einerseits Bedingung für den Erhalt von Daten in einem fairen Austausch, aber auch ein aktiver Wettbewerbsvorteil zur Kundengewinnung sein. Darüber hinaus ist es möglich, eigene Daten zu verkaufen und damit eine neue Umsatzsparte zu generieren.

Deutlich wird der Vorteil an einem simplen Beispiel: Digitalisiert ein Unternehmen seine Produktion, kann ein Kunde den Bestellstatus einsehen oder auf den Digitalen Produktpass zugreifen. So profitieren beide Seiten: Das produzierende Unternehmen bietet einen automatisierten und damit günstigen Service. Der Kunde wiederum spart sich Arbeitszeit durch manuelle Nachfragen. Die Produktionsdaten sind darüber hinaus natürlich für mehr als den Bestellstatus nützlich. Auch eine Steuerung der Produktion lässt sich perspektivisch darauf aufbauen.



Daten kontrolliert und sicher mit anderen teilen

Eine weitere Anwendungsmöglichkeit von Datenräumen bietet sich insbesondere bei digitalen Geschäftsmodellen. Kaufen Unternehmen ein digitales Produkt, wie beispielsweise ein Simulationsmodell, können sie dieses mehrwertschaffende Asset über den Datenraum sofort nutzen. Möchten sie das Modell zu einem späteren Zeitpunkt um eine Komponente erweitern, kann diese über den Datenraum unmittelbar und passgenau bereitgestellt werden. So können digitale Assets modular aufgebaut werden und sind dabei einfach zu integrieren.

SO FUNKTIONIERT DER DATENAUSTAUSCH

Daten, die vom Realen Asset A stammen, können über den Datenaustausch im AAS Dataspace beispielsweise dazu genutzt werden, das Reale Asset B zu ooptimieren.

Beim AAS Dataspace for Everybody können Unternehmen darüber hinaus auch entscheiden, wo die Daten gehostet werden – im Datenraum oder in der eigenen IT. Bei letzterem verbleiben sämtliche sensiblen Informationen auf unternehmenseigenen Servern. Damit schaffen wir das größte Hindernis für Unternehmen aus dem Weg: ihre Sorge über eine nicht kontrollierbare Verwendung der Daten. So ist auch in der eingangs zitierten Bitkom-Umfrage der Datenschutz tatsächlich der meistgenannte Grund, warum ein Datenaustausch zurzeit noch nicht stattfindet.

AAS DATASPACE FOR EVERYBODY

- Niedrigschwellig nutzbare Plattform für digitale Datenräume
- Auf Basis von Verwaltungsschalen (AAS – Asset Administration Shells)
- Eingebettete Middleware Eclipse BaSyx ermöglicht, Digitale Zwillinge unkompliziert zu erstellen
- Hosting der Daten erfolgt im Datenraum oder der unternehmenseigenen IT
- Unternehmen können den Datenaustausch in Prototypumgebung testen
- Einsatz im Produktivbetrieb mit Service Level Agreements möglich

Mit Datenräumen wie dem AAS Dataspace for Everybody ist das Einhalten des Datenschutzes aber ganz klar möglich.

Die technischen Hürden sind mit den geschilderten Entwicklungen entscheidend niedriger geworden. Ebenso besteht ein politisches Interesse daran, die rechtlichen Rahmenbedingungen für die Nutzung von Datenräumen einheitlich zu klären. Jetzt liegt es an Unternehmen, das enorme wirtschaftliche Potenzial von digitalen Datenräumen zu nutzen. Mit ihnen können Geschäftsprozesse effizienter gestaltet, die Interoperabilität verbessert und neue Geschäftsfelder erschlossen werden. Besonders Unternehmen, die frühzeitig auf diese Technologie setzen, können sich damit einen klaren Wettbewerbsvorteil sichern.

Frank Schnicke

E-MAIL MARKETING

KUNDENEINBLICKE BLEIBEN OBERFLÄCHLICH

Der E-Mail geht es so gut wie noch nie: Jedes dritte Unternehmen erhöht seine Versandfrequenz, jedes vierte hat diese seit 2021 verdoppelt. Parallel dazu wird immer mehr in vernetzte Versand- & Datenbanksysteme investiert – E-Mail wird automatisiert, skaliert und integriert. Aber was nützt ein wachstumsstarker Kanal, wenn er in alten Mustern verharrt?

Diese Erkenntnisse liefert die siebte Auflage der Benchmark-Studie, die in Kooperation zwischen absolit Dr. Schwarz Consulting und DDV Deutscher Dialogmarketing Verband e.V. entstanden ist.

www.absolit.de

29 %
der Unternehmen erhöht seine E-Mail-Versandfrequenz

35 %
der Unternehmen kennen ihre Newsletter-Leser kaum

43 %
lassen neue Abonnenten über 30 Tage auf die erste Mail warten

DIE FAKTEN:

NUR 13 %
der Mails erfüllen grundlegende Barrierefreiheits-Standards

7 VON 10
Unternehmen senden bei Inaktivität stur weiter

ENTERPRISE AGILITY

NEUE ÄRA DER UNTERNEHMENSAGILITÄT?

Unternehmensagilität ist keine Methode, sondern eine Kernkompetenz. Sie ist Resilienz in Aktion – die Disziplin, kontinuierlich kleine und große strategische Veränderungen vorzunehmen, um Wachstum, Skalierung und Leistung voranzutreiben. Hochagile Organisationen erreichen ihre Projektziele doppelt so häufig wie weniger agile. Sie kämpfen seltener mit Scope Creep, vermeiden Budgetverluste und scheitern seltener mit Projekten.

Agilität ist damit zu einer unternehmerischen Notwendigkeit geworden. Laut dem „Enterprise Agility"-Report nutzen hochagile Unternehmen zwar oft agile Methoden, aber echte Agilität erfordert eine dynamische Mischung aus Veränderungs- und Projektumsetzungsansätzen.

Unternehmensagilität zu erreichen, ist somit nicht einfach, denn sie erfordert einen tiefgreifenden kulturellen Wandel und konsequente Anstrengungen. Sie hängt von klarer Kommunikation, flexiblen Arbeitsweisen, dem intelligenten Einsatz von Technologie und befähigten Teams ab. .

Agilität auf mehreren Ebenen

Erfolgreiche Agilität geht weit über die Anwendung einzelner Methoden hinaus. Daher darf sie sich nicht rein auf die operative Ebene beschränken. Entscheidend ist ein agiles Mindset, das sich in Führungsverhalten, Unternehmenskultur und strukturellen Rahmenbedingungen manifestiert. Der Report hebt dabei drei Kernbereiche hervor:

#1 **Kulturelle Agilität:** Schaffung eines lernorientierten und psychologisch sicheren Umfeldes

#2 **Agile Governance:** Ermöglichen von schnellen und dezentralen Entscheidungen

#3 **Zukunftsorientierte Kompetenzen:** Aufbau von Skills, die über klassisches Projektmanagement hinausgehen

Agility Reboot in der IT-Branche

Die IT-Branche wird von einer „Fail-Fast"- und „First-Mover"-Mentalität angetrieben. Obwohl sie nach wie vor der agilste Sektor ist, ist sie in den letzten vier Jahren nicht agiler geworden. Dennoch sind mehr als die Hälfte der Unternehmen in diesem Bereich hervorragend, wie die PMI-Untersuchungen zeigen. Und der Anteil derjenigen, die von geringer Agilität berichten, ist seit 2021 um über 26 Prozent zurückgegangen. Widerstandsfähig zu bleiben, ist ein Gebot der Branche.

Agilität bestimmt Projekterfolg

Die Nachfrage nach unternehmerischer Agilität wird in den kommenden Jahren weiter steigen und zu erwartende Disruptionen werden die Art und Weise, wie sich Organisationen anpassen, und das Ausmaß, in dem Agilität ihren Projekterfolg bestimmt, neu gestalten.

Während die KI-Entwicklung in den Unternehmen voranschreitet, wird die Aufrechterhaltung einer Kultur der Unternehmensagilität ihnen helfen, sich auf neue Geschäftsmodelle vorzubereiten. Was auch immer die Zukunft bringt, eines ist sicher: Die Notwendigkeit, die Agilität von Unternehmen auf die nächste Stufe zu heben, wird bestehen bleiben.

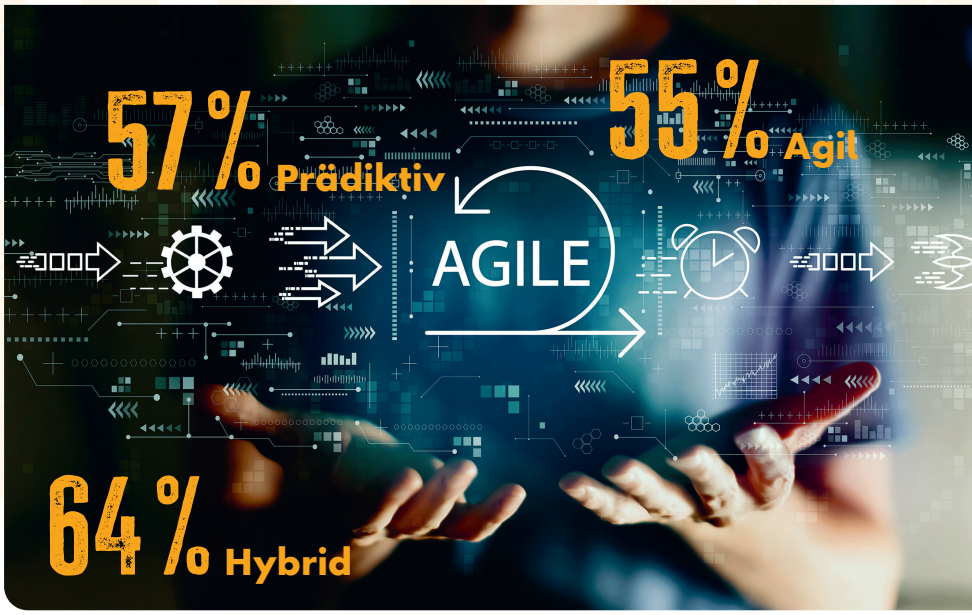
www.pmi.org

MEHR WERT

"Enterprise Agility"-Report

ARBEITSWEISEN

In der gesamten Branche verwenden die Unternehmen immer oder häufig



Datenarchivierung

SO LÄSST SICH DAS WACHSTUM UNSTRUKTURIERTER DATEN BEWÄLTIGEN

Die Geschwindigkeit, mit der unstrukturierte Daten – wie Texte, Videos, Bilder und Social-Media-Posts – erzeugt werden, nimmt kontinuierlich zu. Mittlerweile fallen 80 bis 90 Prozent aller Daten in diese Kategorie. Gleichzeitig ist der Zeitrahmen für die aktive Nutzung von Daten immer kleiner geworden. Dank Edge Computing, IoT-Systemen, maschinengenerierten Daten und nicht zuletzt generativer KI beschränkt sich der Zeitraum für die Datennutzung heute weitgehend auf rund 30 bis 90 Tage. Dann werden die vorhandenen Daten aufgrund der Flut neu hinzukommender Daten entweder weniger nützlich oder sogar überflüssig.

Viele Unternehmen versuchen inzwischen fast vergeblich, mit der rasanten Entwicklung Schritt zu halten. Denn der ständige Zustrom unstrukturierter Daten erfordert praktisch fortlaufende Erweiterungen des Speichersystems – mit den damit verbundenen Kosten. Eine moderne Archivierungsstrategie ist für die Verwaltung von Speicher- und Hybrid-Cloud-Systemen deshalb unabdingbar.

Der Begriff Archivierung wird allerdings häufig falsch verstanden, was zu einiger Verwirrung führen kann. Beispielsweise sind Tiering und Archivierung zwei unterschiedliche Dinge. Einfach erklärt, kann man sich das Thema Archivierung etwa als Umzugsunternehmen vorstellen, das Papierdokumente aus Aktenschränken räumt, in Kartons packt und extern einlagert. Sobald diese Aufgabe erledigt ist, wird das Umzugsteam nicht mehr gebraucht. Sollten die Dokumente in Zukunft aber wieder benötigt werden, dann können diejenigen Personen darauf zugreifen, die die entsprechende Zugangsberechtigung zu den Akten haben.

EINE MODERNE ARCHIVIERUNGSSTRATEGIE MUSS UNTERNEHMEN IN DIE LAGE VERSETZEN, DIESE SPRICHWÖRTLICHE NADEL IM HEUHAUFEN ZU FINDEN.

Sascha Hempe, Regional Sales Manager, DACH & Nordics, Datadobi, https://datadobi.com/

Tiering hingegen entspräche einem spezialisierten Bibliothekar, der ständig vor Ort ist, um jeweils eine Datei in ein besonderes Ablagesystem zu verschieben. Nur der Bibliothekar weiß, wie die einzelnen Dateien wieder zurückgeholt werden können. Das Tiering ist im Grunde eine andere Bezeichnung für hierarchisches Speichermanagement (HSM). Tiering- oder HSM-Lösungen werden schon seit vielen Jahren in unterschiedlichen Formen erprobt, doch sie bringen in der Praxis meist mehr Probleme als wirklichen Nutzen.

NAS-Cloud-Gateways bieten keine echte Archivierung

Cloud-Gateways kommen zunehmend in hybriden Speicherumgebungen zum Einsatz und können eine kostengünstige Lösung für den wachsenden Speicherbedarf sein, denn sie verbinden den lokalen Speicher mit öffentlichen Cloud-Speichern. Mit ihrem globalen Dateisystem bieten NAS-Cloud-Gateways über die Cloud Zugriff auf Dateien, die bisher im lokalen NAS-Speichersystem (Network Attached Storage) aufbewahrt wurden. Die NAS-Gateway-Appliance wird von manchen Nutzern als Archiv-Front-End verstanden. Allerdings handelt es sich auch hierbei nicht um eine echte Archivierung, da die dateibezogenen Metadaten im NAS-Gateway gespeichert sind. Das bedeutet, dass der Zugriff auf die gespeicherten Inhalte im Falle eines Abrufs – ähnlich wie beim Tiering – durch das Gateway geregelt wird.

Sowohl Tiering als auch Gateways stellen Unternehmen damit vor ein großes Problem: Was passiert, wenn die Lösung außer Betrieb geht, veraltet ist oder der Anbieter keinen Support mehr leistet? Wie lassen sich die gespeicherten Daten später wieder abrufen, wenn die Anwendung dafür nicht mehr verfügbar ist? Eine gut durchdachte Archivierungsstrategie löst dieses Dilemma. Den Vorgang der Datenarchivierung und die Plattform, auf der die archivierten Daten gespeichert werden, darf man dabei nicht miteinander verwechseln. Zwar ist die Wahl des richtigen Archivspeichers wichtig, aber bei der Archivierungsstrategie geht es um weit mehr als nur um das Speicherziel.

Denn beim Vorgang der Datenarchivierung müssen geschäftskritische Entscheidungen darüber fallen, was archiviert werden soll und wohin welche Daten anschließend auf Grundlage festgelegter Richtlinien verschoben werden sollen. Bei Bedarf müssen sich plötzlich wieder benötigte Daten zwischen Milliarden anderer Dateien anhand bestimmter Kriterien schnell auffinden lassen, beispielsweise anhand der Zeitspanne seit dem letzten Zugriff, seit der letzten Änderung einer Datei oder auch anhand einer bestimmte Benutzerkennung.

Eine moderne Archivierungsstrategie muss Unternehmen deshalb in die Lage versetzen, diese sprichwörtliche Nadel im Heuhaufen zu finden, sie auf eine ge-

eignete Archivierungsplattform zu verschieben und über eine herstellerunabhängige Option zeitnah abzurufen.

Eine moderne Archivierungsstrategie

Bei der Entwicklung einer Archivierungsstrategie ist es wichtig, abzuwägen, ob ein aktives Archiv, ein Langzeit-Archiv oder eine Kombination aus beiden genutzt werden soll. Ein aktives Archiv ist für Daten geeignet, bei denen eine gewisse Wahrscheinlichkeit besteht, dass sie später wieder abgerufen werden müssen. Ein Langzeit-Archiv wird dagegen für Daten verwendet, bei denen diese Wahrscheinlichkeit eher gering ist, die aber entweder zur Einhaltung gesetzlicher Vorschriften oder aus Governance-Gründen weiterhin aufbewahrt werden. Das Langzeit-Archiv kann zudem als nächster Speicherort für Daten aus dem aktiven Archiv dienen, die einen festgelegten Schwellenwert überschritten haben, der durch die Unternehmensrichtlinien definiert ist.

Der erste, wichtige Schritt bei der Entwicklung einer Archivierungsstrategie besteht darin, Erkenntnisse über das Profil der betreffenden Dateien zu gewinnen. Hilfreich sind dabei die zahlreichen vom Speichersystem zugewiesenen Metadaten, die etwa Aufschluss darüber geben, wann Inhalte erstellt wurden, wann der letzte Zugriff erfolgte, wann Inhalte zuletzt geändert wurden und sogar, ob eine Datei einem aktiven oder inaktiven Benutzer zugeordnet ist (verwaiste Dateien). Mithilfe von Richtlinien können Unternehmen dann festlegen, nach welchen Kriterien Daten auf die Archivierungsplattform verlagert werden sollen.

Ein Beispiel dafür ist, Dateien, die in den letzten drei Jahren nicht abgerufen oder geändert wurden, auf den Archivspeicher zu übertragen. Viele Unternehmen sind sich nicht bewusst, dass im Schnitt über 60 Prozent ihrer gespeicherten Daten in diese Kategorie fallen. Bei Datenmengen im Petabyte-Bereich und Milliarden von gespeicherten Dateien kommt da eine immense Anhäufung von nicht mehr aktiv genutzten Daten zusammen.

Sobald die zu archivierenden Daten identifiziert sind, gilt es, sie so effizient und reibungslos wie möglich auf die neue Archivierungsplattform zu übertragen. Es empfiehlt sich, dazu eine Lösung zu verwenden, die schnell und skalierbar ist und – ganz wichtig – die nicht dauerhaft zu Abruf- und Migrationszwecken betrieben werden muss. Denn in den meisten Fällen ähneln die Archivierungsvorgänge einer Datenmigration. Es handelt sich um eine punktuelle Aktivität, die nur einmalig mit Aufwand verbunden sein sollte – und nicht in einen langwierigen Prozess mit unzumutbaren Folgen ausartet. Unternehmen, die diese Aspekte berücksichtigen, werden das Wachstum unstrukturierter Daten souverän bewältigen.

Sasche Hempe

2025, 2027 oder 2030?

WANN ENDET DIE WARTUNG VON SAP ERP 6 WIRKLICH?

In der SAP-Gemeinde wird in den letzten Jahren kaum ein Thema so intensiv diskutiert wie das Wartungsende von SAP ERP 6. Es kursieren diverse Aussagen und eine Vielfalt an Erklärungen, Tipps und Tricks über mögliche Migrationspfade. Die Frage ist aber, wen betrifft welches Datum und warum?

Es kursieren drei Jahreszahlen – 2025, 2027 und 2030. Und alle drei sind korrekt – allerdings gelten sie für unterschiedliche Packages: Für SAP ERP 6 mit Enhancement Packages 0-5 ist das Ende der Mainstream Maintenance der 31.12.2025. Alle Unternehmen, die danach noch diese Versionen nutzen, haben dann nur noch die Option der „Customer Specific Maintenance", die einen deutlich reduzierten Service umfasst. Im Klartext bedeutet das, dass es keine HR- oder Legal-Changes mehr geben wird und dass die Security-Changes nur noch in begrenztem Umfang zur Verfügung gestellt werden. Kunden mit SAP ERP 6 und Enhancement Packages 0-5 gehen ab dem 31.12.2025 also ein deutlich erhöhtes Risiko ein, dass ihre betriebswirtschaftlichen und rechtlichen Anforderungen nicht mehr unterstützt werden.

Der 31.12.2027 ist das Ende der Mainstream Maintenance für SAP ERP 6 mit Enhancement Packages 6, 7 und 8. Ausschließlich für diese Versionen kann eine Extended Maintenance bei SAP erworben werden. Das ist jedoch nur eine begrenzte Verlängerung, denn auch diese läuft schlussendlich am 31.12.2030 aus.

MIT EINEM ERFAHRENEN PARTNER AN DER SEITE, IST ES FÜR VIELE UNTERNEHMEN NOCH INNERHALB DER GESETZTEN DEADLINES FÜR DIE WARTUNGSFENSTER ZU SCHAFFEN.

Philipp von der Brüggen, CMO, Natuvion GmbH, www.natuvion.com

Etwas mehr Zeit gefällig?

Kunden, die für ihre Migration noch etwas mehr Zeit benötigen, haben grundsätzlich die Möglichkeit, das Wartungsende zwischen drei und fünf Jahre hinauszuzögern. Das ist besonders wichtig für Unternehmen, die den Transformationsprozess noch nicht begonnen haben oder erst in den Anfangsüberlegungen stecken. Eine Transformation von großem Umfang kann bei gutem Verlauf bis zu drei Jahre in Anspruch nehmen – von der Planung bis zum Abschluss.

Um überhaupt ein Hinauszögern des Wartungsendes am 31.12.2025 zu erreichen, müssen SAP ERP 6-Kunden mit Enhancement Packages 0-5 erst auf die Enhancement Packages 6-8 upgraden. Das verschafft diesen Unternehmen einen Zeitgewinn bis 31.12.2027. Sollte dies zeitlich für die Transformation nicht reichen, können sie zusätzlich die Extended Maintenance erwerben. Damit kaufen sie sich Zeit bis zum 31.12.2030.

Soweit zu den Regeln der Upgrades und den theoretisch möglichen Verlängerungen bis zum Wartungsende. Auch wenn es auf den ersten Blick den Anschein macht, dass Unternehmen sich mit diesen Upgrades viel Zeit verschaffen können, machen diese in aller Regel aber wenig Sinn. Denn die Upgrades kosten Zeit, Ressourcen und Geld und sind schlussendlich doch nur eine Übergangslösung – die Migration auf SAP S/4HANA bleibt unausweichlich.

Zeit kaufen macht nur bedingt Sinn

Unternehmen, die die Option der Verlängerung des Wartungsendes mit den Upgrades dennoch in Betracht ziehen, haben sehr unterschiedliche Gründe. Dazu gehört beispielsweise das Betreiben verschiedener Systeme. Unternehmen mit diesen Bedingungen setzten meist Prioritäten und konvertieren erst einmal die wichtigsten Systeme direkt auf SAP S/4HANA und ziehen andere Systeme erst zu einem späteren Zeitpunkt nach. Dafür kann eine Verlängerung tatsächlich Sinn machen.

Ein weiterer Grund ist das Ziel, alles zu konsolidieren und die alten Systeme irgendwann abzuschalten. Beispiele dafür sind Unternehmen, die ein neues System mit neuen Businessprozessen in verschiedenen Regionen einführen wollen. Um das zu erreichen, konsolidieren sie ihre

Systeme erst mal auf dem aktuellsten Stand, um dann den Schritt zu SAP S/4HANA zu gehen. Daran sind meist sehr viele Parteien beteiligt, was das Projekt um zwei bis drei Jahre in die Länge strecken kann.

Unternehmen hingegen, die derartige Besonderheiten nicht haben, sollten sich umgehend auf die Reise machen und möglichst ohne zusätzliche Komplexität und Kosten direkt in die Transformation einsteigen. Vielfach geschieht dies auch bereits. Tendenziell sinkt die Anzahl der Transformationskunden mit den niedrigeren Enhancement Packages (0-5) stark. Das bedeutet, dass viele Unternehmen ihre Transformation bis 31.12.2025 ohne zusätzliche Kosten für das Hinauszögern des Wartungsendes schaffen. Die Zahlen belegen gleichzeitig aber auch, dass es noch einige Unternehmen mit SAP ERP 6 sowie Enhancement Packages 6, 7 und 8 gibt, die die Transformation noch durchlaufen müssen. Für diese Unternehmen wird es langsam eng.

Transformation allein oder mit einem Partner

Die Transformation hin zu SAP S/4HANA ist in den meisten Fällen kein Spaziergang. Und trotz prinzipiell möglicher Wartungsverlängerungen sind die Deadlines bis zum Abschluss der Transformation am 31.12.2025, 31.12.2027 oder 31.12.2030 eng gesteckt. Viele interne IT-Teams sind mit den Details einer Transformation zumindest teilweise überfordert – meist, weil sie nicht die Erfahrung mit großen Transformationsprojekten haben.

Die Transformationsstudie aus 2024 von Natuvion und NTT DATA Business Solutions macht dies besonders deutlich. Knapp 40 Prozent der befragten Unternehmen haben für ihre Transformation ein bis zwei Jahre eingeplant. Nur knapp 19 Prozent planten einen Zeitraum von zwei bis vier Jahren oder länger. 42 Prozent planten mit maximal einem Jahr für die Transformation. Das Resultat: nur 13 Prozent konnten ihre Transformation innerhalb der definierten Zeiträume abschließen und über 46 Prozent überschritten die Zeit um 20 bis 30 Prozent.

Laut Studie gibt es mehrere Gründe, weshalb Unternehmen die eingeplante Zeit massiv überschreiten und damit oft auch den Kostenrahmen der Transformation sprengen. 33,2 Prozent der Befragten bestätigen ein fehlendes oder ungenügendes Transformations-Know-how. Auf dem zweiten Platz unter den Herausforderungen findet sich die detaillierte Schaffung eines Überblicks (Analyse der bestehenden IT-Landschaft und Daten) mit fast 30 Prozent. Die Ergebnisse zeigen zudem, dass die Komplexität des Gesamtprojekts (28,5 Prozent) und der hohe Abstimmungsaufwand (28,3 Prozent) große Herausforderungen bei Transformationsprojekten darstellen. Kein Wunder also, dass über 43 Prozent der befragten Unternehmen ihre Transformationsziele nur teilweise oder nicht erreicht haben.

Der Projektleiter HCM Conversion Christopher Arning bei der Gelsenwasser AG begründet sein erfolgreiches Transformationsprojekt wie folgt: „Ich bin überzeugt, dass ein Schlüssel zum Transformationserfolg der passende Beratungspartner ist. Wir haben einen Partner gefunden, der uns idealerweise ein Gesamtpaket aus strategischer Beratung, fachlicher Expertise und verlässlicher Zusammenarbeit bot."

Die Zeit für die Transformation wird trotz möglicher Wartungsverlängerungen knapp und es gilt, die verbleibende Zeit bestmöglich zu nutzen. Rückschläge während eines Transformationsprojekts oder ein Zeitverzug sind nicht mehr hinnehmbar, was den Druck auf die Transformationsteams nochmals deutlich erhöht. Mit einem erfahrenen Partner an der Seite, der genau weiß, wie große Transformationen geplant und durchgeführt werden, und der über die nötigen Werkzeuge für die Transformation verfügt, ist es für viele Unternehmen noch innerhalb der gesetzten Deadlines für die Wartungsfenster zu schaffen.

Philipp von der Brüggen

Datenfundament für erfolgreiche KI

SO BEWERTEN SIE DIE DATENREIFE FÜR KI-PROJEKTE

Solide Daten sind das A und O beim KI-Einsatz. Eine aktuelle Gartner-Analyse vom 31. Januar 2025, verfasst von den Experten Mark Beyer, Ehtisham Zaidi und Roxane Edjlali, enthält eine umfassende Checkliste zur Bewertung der Eignung von Daten für KI-Projekte. Der Fokus liegt dabei auf kontinuierlicher Überwachung statt einmaliger Datenvorbereitung.

Die Kernaussage der Analyse: KI-Entwickler, Data Scientists und Dateningenieure überschätzen häufig mathematische und statistische Funktionen als Ausgleich für grundlegende Datenprobleme. Dies kann einen selbstverstärkenden Kreislauf des Übervertrauens auslösen, besonders in Situationen, in denen Teams isoliert voneinander arbeiten.

Was bedeutet „KI-bereit" eigentlich?
„KI-taugliche Daten" ist immer ein relativer Begriff. Daten, die für einen KI-Anwendungsfall bereit sind, können für den nächsten völlig ungeeignet sein. Auch Daten, die zu Monatsbeginn KI-bereit waren, müssen kontinuierlich überwacht werden, um sicherzustellen, dass sie weiterhin repräsentativ und nutzbar bleiben.

Der Bericht identifiziert vier Modi der KI-Datenbereitschaft, die vom Umfang der Metadatennutzung abhängen:

#1 **Konzeptnachweis (POC):** Das Risiko wird hauptsächlich durch Fachexperten gesteuert, die lokales Wissen über Datenanforderungen haben

#2 **Multikontext:** Die gleichen Daten werden in verschiedenen Szenarien bewertet, mit Expertenhilfe für A/B-Tests

#3 **Operationalisiert:** Risikomanagement wird von Teams auf Tools verlagert, mit überlappenden Qualifikations- und Kontext-Metadaten

#4 **Produktion:** Automatisierte Prozesse überwachen kontinuierlich Datenänderungen, mit Warnmeldungen bei Abweichungen

Metadaten fallen dabei in zwei entscheidende Kategorien:

#1 **Datenqualifikation:**

- Stellt sicher, dass Daten repräsentativ sind
- Bewertet Datenwerte, Häufigkeit, Verteilung, Integrität und Änderungsmuster
- Erfordert zusätzliche Tools und qualifiziertes Personal für effektive Bewertungen

#2 **Nutzungskontext:**

- Stammt aus nahezu jedem System, jeder Plattform und jedem Prozess
- Umfasst, wie oft und wann Systeme laufen, wer Prozesse initiiert, welche Daten beteiligt sind
- Beinhaltet Komponenten aus Verarbeitungscode-Argumenten („join", „select")

Je stärker diese Metadaten überlappen, desto eher können Risiken von Expertenteams auf Systeme übertragen werden, was mehr Automatisierung ermöglicht.

Checkliste für die KI-taugliche Datenaufbereitung
Der Bericht präsentiert eine umfassende Checkliste, die über 30 Tests umfasst, gruppiert in:

- Traditionelle Ausrichtung (Quantifizierung, Beobachtbarkeitsmetriken)
- Qualifizierte Nutzung (Kontextuelle Qualität, Herkunft, Diversität)
- Zertifiziert für Produktion (Versionierung, Schulung, Einhaltung von Vorschriften)

- Augmentierte Datenbereitschaft (Regressionstests, kontinuierliche Profilierung)

Die Checkliste und Prioritätenmatrix lässt sich am besten in folgendem Kontext verstehen:

- Jede Zeile beschreibt eine spezifische Aufgabe oder einen Prozess, der bei der Nutzung eines Datenbestands für einen KI-Anwendungsfall durchgeführt werden sollte.

- Jede Spalte beschreibt einen der vier KI-fähigen Datenmodi.

- Im Allgemeinen birgt der am weitesten links stehende KI-fähige Datenmodus (KI-Konzeptnachweis) das höchste Risiko für die Organisation. Solche Risiken werden daher am besten von erfahrenen, qualifizierten und validierten Teams oder Experten angegangen, die bei der Datenaufbereitung transparent sind.

- Ebenso geht der rechte Modus (Produktion) davon aus, dass die Datenaufbereitung in hohem Maße automatisiert ist. Dabei ist zu berücksichtigen, dass automatisierte oder erweiterte Datenaufbereitungsschritte sowohl von qualifizierten KI-Experten als auch von Datenverwaltungsexperten validiert werden müssen, die gemeinsam die Effizienz, die Vollständigkeit, die Werkzeuge und die im Betrieb verwendeten Plattformen validieren können.

- Hellblau bedeutet, dass das Risiko weitgehend vom KI-Team übernommen wird. Die KI-Entwickler und Data Scientists müssen in jeder der in jeder Zeile angegebenen Datenaufbereitungsaufgaben über hohe Kenntnisse und Fähigkeiten verfügen.

- Grau oder dunkelblau bedeutet, dass das Risiko weitgehend durch programmatische und sogar automatisierte Bereitstellung der in jeder Zeile angegebenen Datenaufbereitungsfunktion übernommen wird.

BILD 1: CHECKLISTE FÜR KI-DATENBEREITSCHAFT

(Quelle: Gartner, Januar 2025)

	AI-Ready Mode Delivery Approach			
Governance Authority	**Localized**			**Enterprise**
Contextual Responsibility	**Skills Managed Risk**			
AIOps to DataOps Alignment Stage	AI Proof of Concept	Multicontext Valid	Operationalize	Production
AI-Ready Universal Functional Requirements	Metadata accepted	Usage metadata	Alert & modify based	ML-based notification
Traditional Alignment				
Quantification	✔	✔	✔	✔
Observability Metrics	✔	✔	✔	✔
Consistent Content	✔	✔	✔	✔
Verified Source Capture	✔	✔	✔	✔
Qualified Usage („Faimess")				
Contextual Quality	?	✔	✔	✔
Lineage	?	✔	✔	✔
Validated Authority	?	✔	✔	✔
Diversity	?	✔	✔	✔
SLA Performance	?	✔	✔	✔
Variable Access Rights	?	✔	✔	✔
Get multi-content metadata connected (RAG, etc)	?	✔	✔	✔
Semanlic context linked to KG (Tagging, annotation ...)	?	✔	✔	✔
Use-case Commonality	?	✔	✔	✔
Certified for Production (Trust.)				
Versioning	?	?	✔	✔
Training to Production Data Verification	?	?	✔	✔
Risk Compliance	?	?	✔	✔
Regulatory Compliance	?	?	✔	✔
AI Use-case to Technique Alignment	?	?	✔	✔
Ethical Exposure Risk (rephrase AI Governance inputs)	?	?	✔	✔
Data Share Logs	?	?	✔	✔
Observability of content use cases	?	?	✔	✔
Augmentation Enabled Data Readiness				
Regression Testing (Data Engineer Validation, Poisoning	?	?	?	✔
Continous Profilling & Analytics	?	?	?	✔
Change Recognition & Alerting	?	?	?	✔
Explainable Inferred Calculations	?	?	?	✔
Presumed Reuse of Derivations	?	?	?	✔
				System-based Risk

Unstructured (GenAI) Cannot Proceed unless completed ? = Preferred but optional ✔ = Mandatory (staff or automated)

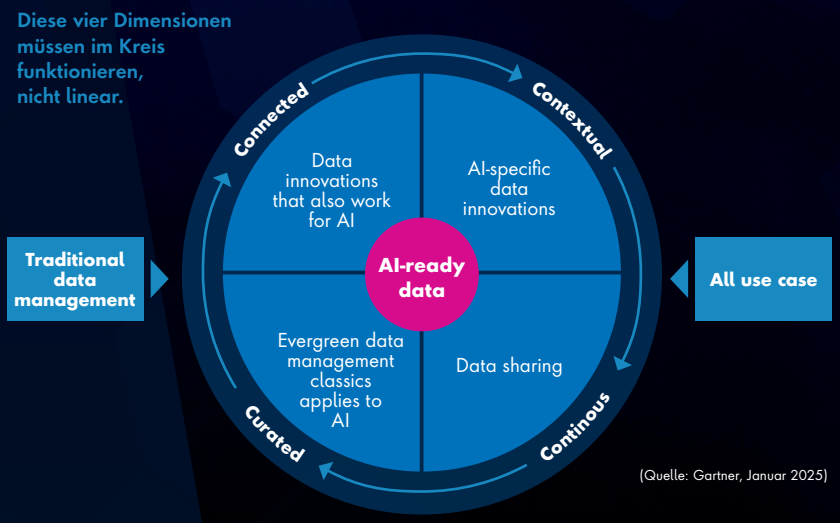
- Ein Häkchen bedeutet, dass die Aktivität in der Zeile obligatorisch ist, um die KI-Fähigkeit für Ihre Datenbestände zu erreichen.

- Ein „?“ bedeutet, dass die Zeile optional ist, die KI-Fähigkeit jedoch verbessert wird, wenn diese Funktion einbezogen wird. Die Aufgaben können von automatisierten Prozessen oder qualifiziertem Personal ausgeführt werden, wobei die Automatisierung eine höhere Konsistenz gewährleistet.

Je mehr Zeilen entweder von qualifizierten Mitarbeitern oder automatisierten Systemen ausgefüllt werden, desto geringer ist das Risiko bei der Verwendung der Daten in bestimmten KI-Modellen.

Wichtig ist, dass die Tiefe (die Anzahl der ausgefüllten Zeilen) entscheidend ist – nicht allein die Automatisierung. Das KI-Implementierungsteam oder der Data Scientist verfügt möglicherweise auch über Fähigkeiten zur Automatisierung ihrer Datenvorbereitung in bestimmten Bereichen (sogar innerhalb ihres Modells). Je tiefer Sie durch die Zeilen in der Liste gehen, desto besser – und die Zeile kann automatisiert oder von qualifizierten Fachleuten verifiziert werden. Wenn zu viele Aufgaben/Zeilen unabhängig von der Automatisierung unvollständig bleiben, liegt die Verantwortung für die Bereitschaft weiterhin beim KI- und Data-Science-Team. Wie jedoch zuvor erwähnt, zeigen KI- und Data-Science-Teams ein übermäßiges Vertrauen in ihren Datenmanagementansatz. Das bedeutet, dass sie für die Entscheidungen und Ergebnisse von KI-Modellen verantwortlich sind, einschließlich wenn sie die Daten modifizieren, ersetzen oder anderweitig falsch vorbereiten.

BILD 2: VON DER DATENVORBEREITUNG ZU KI-TAUGLICHE DATEN.



(Quelle: Gartner, Januar 2025)

KI-Implementierungsteam

KI-Bereitschaft erfordert KI-bereite Daten. Bestehende Datenmanagementpraktiken liefern im Allgemeinen einen fragmentierten Ansatz, wobei die verschiedenen Datenmanagementaufgaben auf sehr unterschiedlichen Ebenen basierend auf Abteilungen, Anwendungen, Entwicklungsteams und mehr erledigt werden. Organisationen können diesem fragmentierten Ansatz entgegenwirken, indem sie sicherstellen, dass ihr KI-Implementierungsteam das Risiko verwaltet und die Verantwortung für die Datenvorbereitung übernimmt. Alternativ sollten Organisationen ihre Anforderungen klar gegenüber Datenmanagementexperten formulieren, die sowohl die Verantwortung als auch die Befugnis für die Bereitstellung der Daten übernehmen werden.

Wenn Führungskräfte KI-Konzeptnachweise für eine schnelle Einführung verfolgen möchten, dann sollten diese Führungskräfte Mitarbeiter einstellen oder schulen, deren kollektive Expertise sowohl Feature Engineering als auch Data Engineering umfasst.

Wenn die Datenmanagementumgebung als weniger ausgereift gilt als der angestrebte Modus, wird auch eine Finanzierung notwendig sein, um die erforderlichen Teams und Plattformen aufzubauen. Ohne die Finanzierung beider Aspekte bleibt das Risiko der Organisation hoch, da sie von Personalmodellen abhängig ist, die erhebliche Neustarts und negative Auswirkungen durch Personalwechsel erfahren können.

Der kontinuierliche Zyklus der KI-Datenbereitschaft

KI-taugliche Daten erfordern einen kontinuierlichen Bewertungszyklus. Traditionelles Datenmanagement bleibt die Grundlage, wird aber durch vier spezifische Dimensionen erweitert:

- **Verbunden:** Dies bezieht sich auf Datenmanagement-Innovationen, die sowohl für traditionelle Datennutzung als auch für KI funktionieren. Gemeint sind Praktiken und Technologien, die die Verbindung zwischen herkömmlichen Datenquellen und KI-Anwendungen herstellen (zum Beispiel moderne Datenintegrationsmethoden, die für beide Nutzungsarten geeignet sind).

- **Kontextuell:** Hierbei handelt es sich um speziell für KI entwickelte Dateninnovationen, die den einzigartigen Anforderungen von KI-Systemen entsprechen. Dies beinhaltet Methoden, die KI-spezifische Datenqualität, Metadaten-Tagging und Kontextanreicherung berücksichtigen, die traditionelle Systeme möglicherweise nicht benötigen.

- **Kontinuierlich:** Dieser Punkt betont die Notwendigkeit des laufenden Datenaustauschs und der Integration. Im Gegensatz zu traditionellen Batch-Prozessen erfordern KI-Systeme oft einen kontinuierlichen Fluss von Daten und Feedback, um relevant zu bleiben und sich an Veränderungen anzupassen.

- **Kuratiert:** Dies bezieht sich auf bewährte Datenmanagementpraktiken, die auch für KI-Anwendungsfälle gelten. Dazu gehören traditionelle Datenqualitäts-, Governance- und Metadatenmanagement-Methoden, die für KI-Zwecke angepasst wurden. Bild 2 positionieren))

Der wichtige Aspekt ist, dass diese vier Dimensionen nicht in einer linearen Abfolge funktionieren, sondern in einem kontinuierlichen Kreislauf. Das bedeutet:

- KI-Systeme benötigen konstante Bewertung und Anpassung der Daten
- Feedback aus einem Bereich informiert die anderen
- Die Datenbereitschaft ist nie „abgeschlossen", sondern ein fortlaufender Prozess
- Änderungen in KI-Modellen können neue Datenanforderungen schaffen, die wiederum den Zyklus neu starten

Im Bericht wird betont, dass dieser zyklische Ansatz entscheidend ist, da KI-Daten sich mit der Zeit entwickeln und verändern, was eine kontinuierliche Überprüfung und Anpassung erfordert.

KONKRETE EMPFEHLUNGEN FÜR DATEN- UND ANALYSEVERANTWORTLICHE

#1 Richten Sie Datenrepräsentativität und Kontext am KI-Nutzungszweck aus:
- Bewerten Sie Variationen im Datenkontext für jeden Anwendungsfall
- Nutzen Sie möglichst viele Metadaten aus bestehenden Systemen

#2 Verbessern Sie die KI-Datenbereitschaft durch erweiterte Metadatennutzung:
- Nutzen Sie Metadaten aus bestehenden Datenprozessen
- Überwachen Sie kontinuierlich Wertedrift, Umstrukturierung und andere Änderungsmuster

#3 Überprüfen Sie die KI-Datenbereitschaft mit der Checkliste:
- Identifizieren Sie, ob wesentliche Governance-Prinzipien validiert wurden
- Bewerten Sie den Abhängigkeitsgrad von Experten gegenüber Tools und Systemen

Fazit

Die Bewertung der KI-Datenbereitschaft erfordert ein Umdenken in Bezug auf Datenqualität und -management. Mit zunehmendem Vertrauen in KI-Systeme fordern Risikomanagement und Führungskräfte umfassendere Überprüfungen und Validierungen, da bisherige Qualitäts-, Governance- und Metadatenpraktiken oft nicht ausreichen.

Durch einen strukturierten Ansatz zur Metadatenerfassung und -analyse können Unternehmen Risiken reduzieren und ihre KI-Investitionen absichern – ein Prozess, der niemals als abgeschlossen betrachtet werden sollte.

Es wird verpflichtende Anforderungen geben. (Die detaillierte Tabelle finden Sie hinter dem QR-Code hintelegt.) Die Verantwortung, die Anforderungen weiter zu vertiefen, kann jedoch entweder von einzelnen KI-Teams oder von den unternehmensweiten Datenmanagement-Teams übernommen werden, die Datenplattformen und -tools nutzen. Die Funktionstiefe kann im Laufe der Zeit erhöht werden, sobald die Mindestanforderungen erfüllt sind.

www.gartner.de

KI-Code ohne Halluzinationen

MEHR ZUVERLÄSSIGKEIT IN DER SOFTWAREENTWICKLUNG

KI-basierte Coding-Assistenten sind in der Lage große Datensätze zu analysieren und Softwareentwicklungsprozesse enorm zu beschleunigen. Allerdings bergen sie auch signifikante Risiken: Sie neigen zu sogenannten „Halluzinationen". Diese können sich als fehlerhafte Funktionsaufrufe, nicht-existierende Bibliotheken oder unlogische Algorithmen manifestieren. Mit den richtigen Strategien lassen sich diese Risiken aber minimieren.

Halluzinationen von vornherein minimieren

Code-Assistenten wie GitHub Copilot oder ChatGPT unterstützen Entwickler weltweit dabei, schneller und effizienter zu programmieren. KI-Halluzinationen stellen dabei aber eine besondere Herausforderung dar.

Während bei Bildgenerierung sechsfingrige Hände oder seltsame Textelemente auf Fotos oft für Belustigung sorgen, können halluzinierte Codezeilen ernsthafte Probleme verursachen – angefangen bei Programmabstürzen bis hin zu Sicherheitslücken. Mit der zunehmenden Integration von KI-Tools in den Entwicklungsalltag wird es für Programmierer daher unerlässlich, wirksame Strategien gegen diese KI-spezifischen Fehler zu entwickeln.

Präzise Prompts

Das altbekannte Informatik-Prinzip „Garbage in, Garbage out" gilt auch für LLMs. Die Qualität des generierten Codes steht in direktem Zusammenhang mit der Qualität der Anfrage. Stellen Sie Fragen daher in einem begrenzten Umfang und überprüfen Sie die Ergebnisse besonders kritisch. Die Nutzungsdaten der KI-Coding-Tools deuten darauf hin, dass die resultierenden Outputs bei solchen Fragen tendenziell akkurater sind.

PRAXISTIPP:

Unterteilen Sie komplexe Aufgaben in kleinere, überschaubare Teilprobleme. Spezifizieren Sie genau, welche Funktionalität, welche Programmiersprache und welche Bibliotheken verwendet werden sollen. Je präziser die Anfrage, desto geringer die Wahrscheinlichkeit von Halluzinationen.

API-Referenzen nutzen

Große Sprachmodelle sind berüchtigt für ihre Referenz-Halluzinationen - etwa wenn sie nicht-existierende Studien zitieren. Moderne KI-Modelle unterstützen inzwischen Zitierfunktionen. Um Halluzinationen zu minimieren, sollten Entwickler diese Features entsprechend nutzen und die KI beispielsweise nach API-Referenzen fragen.

PRAXISTIPP:

Überprüfen Sie stets API-Aufrufe, Bibliotheksimporte und Framework-Funktionen gegen die offizielle Dokumentation. Nutzen Sie die Zitierfunktionen moderner KI-Tools, um Referenzen nachvollziehen zu können.

Wissensgrenzen der KI berücksichtigen

KI-Modelle verfügen über ein „Knowledge-Cutoff-Datum" - Informationen nach diesem Zeitpunkt sind dem System nicht bekannt. Ob ein Tool halluziniert oder verzerrte Ergebnisse liefert, lässt sich unter anderem anhand seiner Wissensgrenzen vorhersagen. Wenn Sie die neuesten Bibliotheken oder Frameworks nutzen möchten, das Tool diese aber nicht kennt, steigt die Wahrscheinlichkeit für fehlerhafte Outputs.

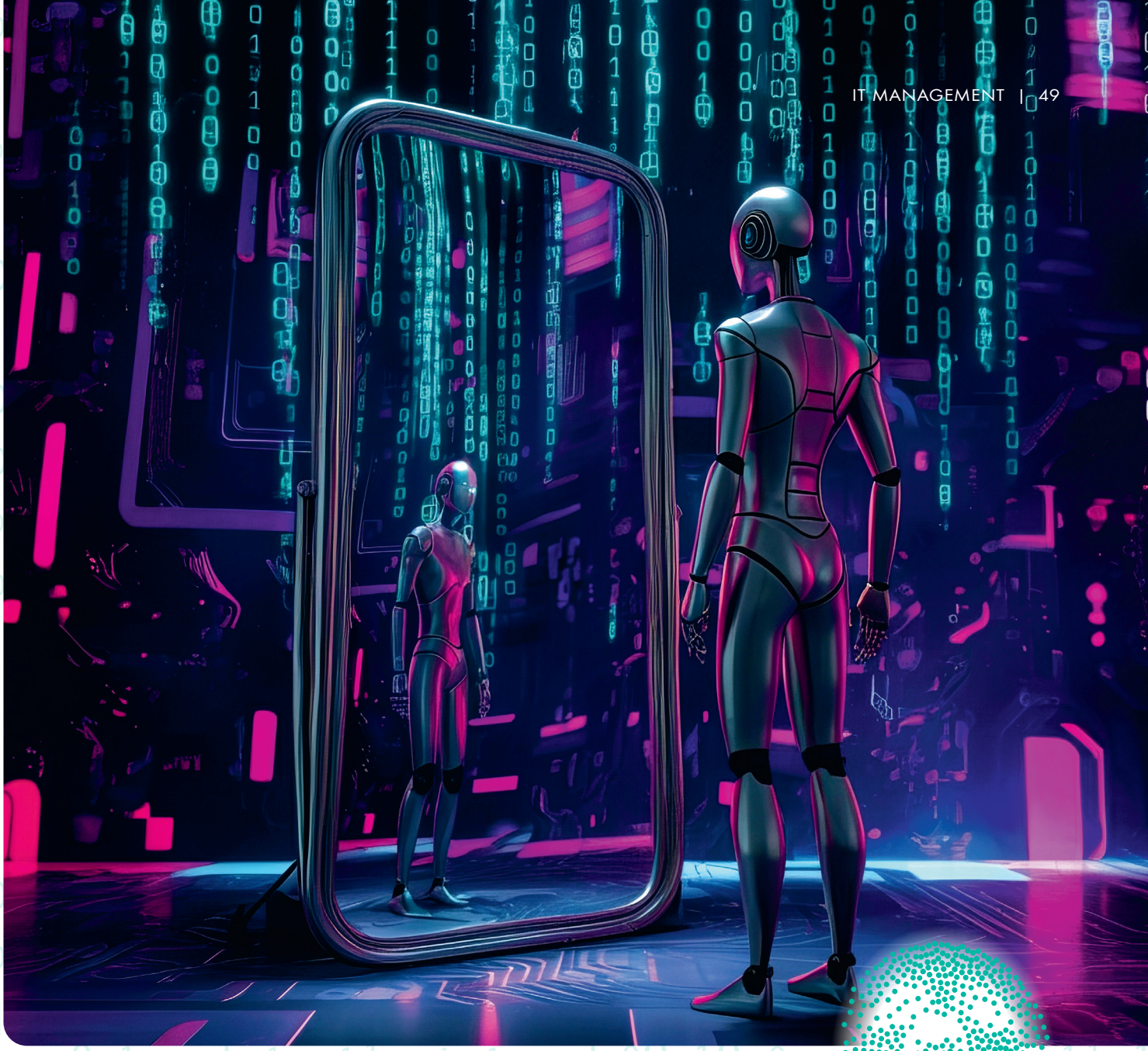
PRAXISTIPP:

Prüfen Sie, ob die verwendeten Bibliotheken und Frameworks vor dem Wissens-Cutoff des KI-Systems veröffentlicht wurden. Bei neueren Technologien ist besondere Vorsicht geboten - hier sollten Sie zusätzliche Überprüfungen einplanen.

Modelle richtig trainieren

Eine erfolgreiche Arbeit mit KI-Coding-Tools hängt maßgeblich vom korrekten Kontext ab. Diese Systeme benötigen klare Anweisungen zu Mustern, Methoden und Programmierstandards, um qualitativ hochwertigen Code zu generieren. Ohne diese Kontextinformationen steigt das Risiko, dass sich problematische Anti-Patterns in den generierten Code einschleichen – subtile Halluzinationen, die erst bei genauerer Betrachtung erkennbar werden.

Besonders effektiv zur Vermeidung dieser Probleme ist das Konzept der Retrieval Augmented Generation (RAG). Diese Technologie stellt eine der wirksamsten Methoden zum „Grounding" von KI-Modellen dar. RAG verbessert die Ausgaben



der Large Language Models erheblich, indem es sie kontinuierlich mit Daten aus verschiedenen Quellen abgleicht:

- Externe Dokumentationen und Best-Practice-Richtlinien
- Interne Codebasen und Unternehmensstandards
- Aktuelle API-Referenzen und Bibliotheksdokumentationen

KI mit KI überprüfen

Ein effektiver Ansatz ist die Nutzung von KI-Systemen zur Überprüfung von KI-generiertem Code. Eine Möglichkeit besteht darin, eine Begleitdokumentation für den Code zu schreiben, damit die KI diesen in einer neuen Instanz evaluieren kann – und ermittelt, ob er den Anforderungen der angepeilten Use Cases entspricht.

PRAXISTIPP:

Lassen Sie von einer KI generierten Code durch eine separate KI-Instanz überprüfen. Bitten Sie das System um eine detaillierte Code-Review mit besonderem Fokus auf potenzielle Fehler, Sicherheitsrisiken und Performance-Probleme.

Menschliche Expertise zur Qualitätssicherung

Trotz aller Fortschritte bleibt menschliche Expertise unersetzlich. KI sollte als Leitfaden dienen – nicht als Quelle der Wahrheit. Entsprechend sollten Sie KI-generierten Code als Vorschlag betrachten und nicht als Ersatz für menschliche Expertise.

Wenn man mit einer Codebasis nicht vertraut ist, kann es schwierig sein, Halluzinationen zu erkennen. Eine tiefe Kenntnis des eigenen Codes ist daher entscheidend, um KI-generierte Fehler zu identifizieren.

PRAXISTIPP:

Behandeln Sie KI-generierten Code wie Code von Junior-Entwicklern: Er muss gründlich reviewt werden. Bleiben Sie mit Ihrer Codebasis vertraut und bilden Sie sich kontinuierlich weiter, um mit neuen Technologien Schritt zu halten.

Umfassende Teststrategie

Etablierte Qualitätssicherungsprozesse sind auch für KI-generierten Code uner-

lässlich. Entwicklungsteams sollten weiterhin Pull Requests und Code Reviews durchführen, so als ob der Code von Menschen geschrieben worden wäre.

Während des gesamten Entwicklungszyklus ist es wichtig, gute Linting-Tools und SAST-Scanner zu nutzen. IDE-Plugins, CI-Integrationen und Pull-Requests sind das absolute Minimum, um zu verhindern, dass Halluzinationen in die Produktion gelangen.

Eine ausgereifte DevOps-Pipeline ist unerlässlich, bei der jede Codezeile einem Unit Test unterzogen wird. Die Pipeline befördert den Code erst dann in die Staging- und Produktionsphase, wenn Tests und Builds bestanden wurden.

PRAXISTIPP:

Implementieren Sie eine umfassende Teststrategie mit:

- Automatisierten Unit-Tests für jede Funktionalität
- Integration-Tests für Komponenteninteraktionen
- Code-Linting und statischer Codeanalyse
- Security-Scans
- Code-Reviews durch erfahrene Entwickler
- Robuster CI/CD-Pipeline

Ein praktischer Ansatz zur Erkennung von Halluzinationen ist die Nutzung des Code-Review-Interfaces, um die Teile der Codebasis zu akzentuieren, die KI-generiert sind. Diese Kennzeichnung erleichtert nicht nur die Identifikation potenzieller Probleme, sondern schafft auch Lernmöglichkeiten für das gesamte Team.

Balance zwischen Effizienz und Sicherheit

KI-Coding-Tools bieten enorme Vorteile hinsichtlich Produktivität und Kreativität. Mit einer durchdachten Strategie zur Vermeidung und Erkennung von Halluzinationen lassen sich diese Vorteile sicher nutzen, ohne Abstriche bei der Codequalität machen zu müssen.

Die Integration von KI in den Entwicklungsprozess erfordert ein ausgewogenes Verhältnis zwischen Automatisierung und Qualitätssicherung. Entwickler, die präzise Prompts formulieren, Quellen kritisch überprüfen, die Aktualität der Wissensbasis berücksichtigen und ihre KI-Modelle mit ausreichend Kontext versorgen, minimieren das Risiko von Halluzinationen erheblich.

Ergänzt durch eine robuste Teststrategie, menschliche Expertise und visuelle Kennzeichnung von KI-Code entstehen so zuverlässige, sichere und wartbare Softwarelösungen, die das Beste aus beiden Welten vereinen: menschliche Kreativität und KI-Effizienz.

Die KI-gestützte Softwareentwicklung steht noch am Anfang ihrer Entwicklung. Mit jedem Update werden die Modelle präziser, die Halluzinationen seltener und die Tools leistungsfähiger. Doch selbst die fortschrittlichsten Systeme benötigen weiterhin menschliche Überwachung und Qualitätssicherung.

Der Schlüssel zum Erfolg

Dieser liegt in einer gesunden Balance: KI als leistungsstarkes Werkzeug betrachten, nicht als Ersatz für fundiertes Entwicklungswissen und bewährte Qualitätssicherungsprozesse. Mit diesem Ansatz wird KI-generierter Code zu einem wertvollen Asset in der modernen Softwareentwicklung – zuverlässig, effizient und frei von Halluzinationen.

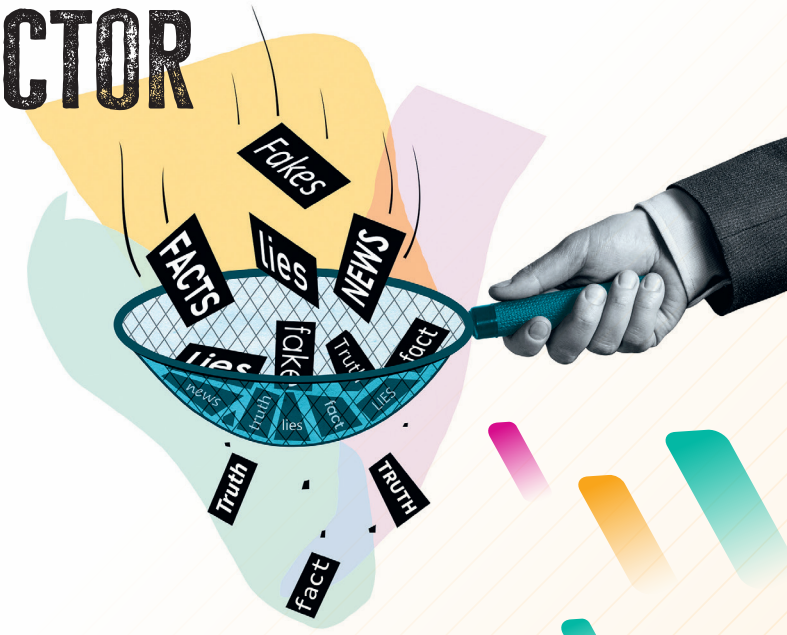
Ulrich Parthier

KI MUSS MAN ALS LEISTUNGSSTARKES WERKZEUG BETRACHTEN, NICHT ALS ERSATZ FÜR FUNDIERTES ENTWICKLUNGSWISSEN UND BEWÄHRTE QUALITÄTSSICHERUNGSPROZESSE.

Ulrich Parthier,
Publisher it management/it security,
www.it-daily.net

DEEPFAKE DETECTOR

ERKENNUNG IN ECHTZEIT



Die Verbreitung von Deepfakes hat exponentiell zugenommen - mit einem Anstieg von 550 Prozent in sozialen Medien zwischen 2019 und 2023. Das Weltwirtschaftsforum stuft diese Entwicklung als wesentliches globales Risiko ein.

Als Antwort darauf präsentierte X-PHY Inc. auf der RSA Conference (RSAC) 2025 seinen neuen „Deepfake Detector". Die Lösung ermöglicht Nutzern die Echtzeit-Verifizierung von Videos, Audios und Bildern mit bis zu 90 Prozent Genauigkeit - direkt auf dem Endgerät und ohne Cloud-Anbindung.

„Der Deepfake Detector stärkt unsere Vision einer ‚Community Root of Trust', in der jede Ebene – von der Hardware über die Daten bis hin zu den Inhalten – als Kontrollpunkt für Authentizität und Sicherheit dient. Durch die Kombination der Deepfake-Erkennung mit unseren bestehenden hardwareintegrierten Schutzmechanismen sorgen wir dafür, dass jedes Endgerät nicht nur Daten schützt, sondern auch aktiv die Vertrauenswürdigkeit der durchlaufenden Informationen erkennt und überprüft", kommentiert Camellia Chan, CEO und Mitbegründerin von X-PHY Inc.

Deepfake-Erkennung auf Abruf

Nach der Aktivierung analysiert der Deepfake Detector mit multimodaler künstlicher Intelligenz (KI) Video-, Bild- und Audiostreams in Echtzeit. Durch die Untersuchung von mikromimischen Gesichtsausdrücken, Stimmprofilen und durch Generative Adversarial Networks (GANs) erzeugten Artefakten erkennt das System Manipulationsversuche sogar über mehrere Videofenster hinweg. Die Erkennung erfolgt vollständig lokal auf dem Gerät. Dadurch bleibt die Privatsphäre der Nutzer geschützt und der Betrieb ist auch ohne Internetverbindung möglich.

Ermöglicht wird dies durch den Einsatz fortschrittlicher zeitlicher und räumlicher KI-Analysen im Deepfake Detector, die auf vortrainierten neuronalen Netzwerken basieren. Diese Modelle sind in der Lage, subtile Unstimmigkeiten in Gesichtsbewegungen, Audiowellenformen sowie Bildartefakten zu erkennen – typische Merkmale von KI-generierten Inhalten.

In Kombination mit X-PHYs patentierten hardwarebasierten Schutzmechanismen entsteht so ein nahtloses Sicherheitsökosystem, das sowohl gespeicherte Daten als auch die Integrität digitaler Kommunikation schützt.

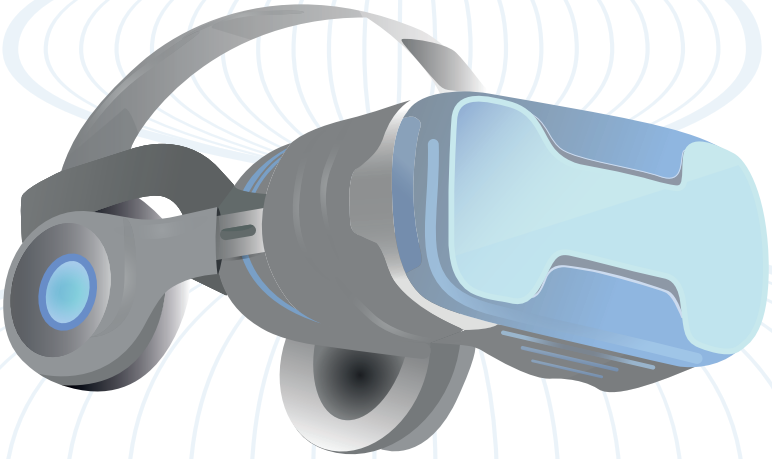
Flexible Bereitstellung, mühelose Integration

Der Deepfake Detector wurde für eine nahtlose Einführung konzipiert und bietet flexible Bereitstellungsoptionen, um unterschiedlichen Anforderungen von Unternehmen gerecht zu werden.

Die Lösung ist anwendungsunabhängig und mit führenden Plattformen wie Teams, Zoom, Webex, Chrome, YouTube und Meta kompatibel. Mit nur einem Klick können Nutzer sie beim Beitritt zu einem Meeting aktivieren – dort läuft sie dann autonom für eine voreingestellte Dauer und kann bei Bedarf erneut gestartet werden.

Basierend auf den Prinzipien des Zero-Trust-Modells fügt die Lösung eine zusätzliche Ebene der Authentifizierung und Verifizierung auf Geräteebene hinzu. Dadurch unterstützt sie Organisationen dabei, ihre Cyber-Resilienz gegenüber KI-gesteuerten Täuschungen zu verbessern und die Abhängigkeit von externen Validierungssystemen zu verringern, die häufig überflüssige operative Komplexität mit sich bringen.

https://x-phy.com



SMARTE BRILLE

WIE WIRD UNSER ALLTAG 2035 AUSSEHEN?

Im Geschichtsunterricht eine Zeitreise ins antike Rom unternehmen, Klavierstunden von einem Meisterpianisten erhalten, während eines einzigen Tages am Strand, in den Bergen und im eigenen Büro arbeiten – all das könnte schon 2035 Realität sein. Möglich machen das Technologien der sogenannten Extended Reality (XR), zu denen zum Beispiel Brillen gehören, die mittels Virtual Reality (VR) oder Augmented Reality (AR) eigenständige virtuelle Welten erlebbar machen oder die Realität um virtuelle Elemente ergänzen. Aber wie realistisch ist eine alltägliche Nutzung dieser Technologien tatsächlich?

Die Antwort findet sich im neuen Leitfaden „Wie wird die XR-Welt im Jahr 2035 aussehen?" des Digitalverbands Bitkom. Die Publikation beschreibt Alltagsszenarien im Jahr 2035, die auf unterschiedliche Weisen XR-Anwendungen einbinden – am Beispiel vier verschiedener fiktiver Personen. Darüber hinaus analysiert der Leitfaden die Entwicklungen, die rund um XR im Bereich der Hardware und der Künstlichen Intelligenz zu erwarten sind, und wie sich Produkte und Marken verändern müssen, um neuen Anforderungen gewachsen zu sein. „Insbesondere Künstliche Intelligenz wird den Mehrwert, den XR-Technologien im Alltag bieten können, nochmal um ein Vielfaches steigern. Wir werden perspektivisch einen persönlichen KI-Assistenten haben, der uns ständig begleitet. Außerdem wird durch KI der Übergang zwischen physischer und virtueller Welt so gestaltet sein, dass er kaum noch wahrnehmbar ist", sagt Dr. Sebastian Klöß, Leiter Märkte und Technologien beim Bitkom. „In wenigen Jahren wird jede und jeder mit nur einer smarten Brille den eigenen Alltag durch virtuelle Elemente vereinfachen oder angenehmer gestalten können."

Derzeit ist die Nutzung von VR-Brillen noch nicht stark verbreitet, das Interesse allerdings groß: Laut einer repräsentativen Bitkom-Studie unter mehr als 1.100 Personen ab 16 Jahren in Deutschland hat im vergangenen Jahr ein Fünftel (22 Prozent) einmal eine entsprechende Brille genutzt, knapp die Hälfte (48 Prozent) würde es allerdings gern in Zukunft tun. Beliebt sind die Brillen bei den Nutzerinnen und Nutzern für Videospiele (95 Prozent), zum Bereisen von Orten (70 Prozent) und um Filme, Serien oder Videos anzusehen (64 Prozent). Beim Shopping (15 Prozent), für Bildungs- und Lernprojekte (11 Prozent) oder für virtuelle Treffen mit anderen (5 Prozent) kommen die Brillen hingegen noch eher selten zum Einsatz. Schon 2024 war sich aber ein Drittel der Deutschen (31 Prozent) einig: VR-Brillen werden künftig Teil der Standardausstattung eines jeden Haushalts sein.

www.bitkom.org

MEHR WERT

Wie wird die XR-Welt im Jahr 2025 aussehen?

SaaS oder On-Premises?

UNTERNEHMEN STEHEN VOR EINER WICHTIGEN IT-ENTSCHEIDUNG

WÄHREND VIELE ITSM-SOFTWAREANBIETER MITTLERWEILE AUSSCHLIESSLICH AUF SAAS SETZEN, BLEIBT TOPDESK EINER DER WENIGEN FÜHRENDEN ANBIETER, DIE BEIDE MODELLE WEITERHIN ANBIETEN.

Sarah-Lee Hofe, Marketing Managerin, TOPdesk Deutschland GmbH, www.topdesk.com

Die Digitalisierung stellt Unternehmen zunehmend vor die Frage, wie sie ihre IT-Infrastruktur optimal gestalten. Dabei geht es oft um die Entscheidung zwischen einer Cloud-basierten Software as a Service (SaaS)-Lösung oder einer lokal betriebenen On-Premises-Variante. Besonders für kleine und mittlere Unternehmen (KMUs) ist diese Entscheidung essenziell. Strenge Datenschutzvorgaben veranlassen viele Organisationen dazu, ihre IT weiterhin selbst zu betreiben. Gleichzeitig wächst der Trend zur Cloud-Nutzung, insbesondere bei Anwendungen, die keine hochsensiblen Personendaten verarbeiten, aber eine hohe Verfügbarkeit erfordern.

SaaS-Trend versus Datenschutz

Immer mehr Unternehmen setzen auf SaaS-Lösungen, da sie eine hohe Verfügbarkeit, automatische Updates und minimalen Wartungsaufwand bieten. ITSM- und ESM-Systeme sind hierfür ein gutes Beispiel: Sie greifen nur auf die für die Servicebereitstellung notwendigen Daten zu und bieten als SaaS-Lösung die Vorteile hoher Skalierbarkeit und effizienter Ressourcennutzung.

Gleichzeitig bleibt der Bedarf an On-Premises-Lösungen bestehen – insbesondere bei Organisationen, die hochsensible personenbezogene Daten verarbeiten. Behörden, Banken und andere sicherheitskritische Institutionen bevorzugen oft die vollständige Kontrolle über ihre IT-Infrastruktur und setzen daher auf lokale Hosting-Optionen.

Wichtige Entscheidungskriterien

- **Kosten:** SaaS reduziert Initialkosten und umfasst Wartung und Updates in der Subscription. On-Premises kann zusätzliche Investitionen für Hardware und IT-Personal erfordern.
- **Implementierungszeit:** SaaS ist sofort einsatzbereit, während On-Premises eine Installation durch das interne IT-Team erfordert.
- **Wartung & Updates:** Bei SaaS übernimmt der Anbieter Wartung und Updates vollständig, während On-Premises-Nutzer diese selbst einplanen müssen.
- **Anpassungsfähigkeit:** On-Premises erlaubt tiefgreifendere Anpassungen, wohingegen SaaS mit einer standardisierten Struktur arbeitet.
- **Sicherheit & Compliance:** Bei SaaS liegt die Verantwortung für die Sicherheit beim Anbieter, On-Premises-Kunden behalten die volle Kontrolle über ihre Daten und Sicherheitsmaßnahmen.

ITSM-Software nur noch als SaaS Variante?

Während viele ITSM-Softwareanbieter mittlerweile ausschließlich auf SaaS setzen, bleibt TOPdesk einer der wenigen führenden Anbieter, die beide Modelle weiterhin anbieten.

Dies ermöglicht Unternehmen, insbesondere in sicherheitssensiblen Branchen wie dem öffentlichen Sektor oder der Finanzwirtschaft, eine passgenaue Lösung für ihre Anforderungen zu wählen. Diese Flexibilität erlaubt Unternehmen, die für sie passende IT-Strategie zu wählen – sei es für eine wartungsarme, skalierbare SaaS-Lösung oder eine datensichere On-Premises-Variante.

Sarah-Lee Hofe

IT Financial Management im Zeitalter der Cloud

HERAUSFORDERUNGEN UND LÖSUNGEN FÜR EINE GANZHEITLICHE KOSTENKONTROLLE

Der Wandel im IT Financial Management (ITFM) wurde maßgeblich durch die voranschreitende Digitalisierung und die zunehmende Nutzung von Cloud-Services geprägt. Was früher durch statische Tools und Prozesse gesteuert wurde, benötigt heute flexible Lösungen, die die dynamische Natur von Cloud-Services widerspiegeln. Dieser Artikel beleuchtet die Herausforderungen, die sich für das ITFM durch den zunehmenden Einsatz von Cloud-Services ergeben, und zeigt, wie ein ganzheitlicher Ansatz helfen kann, den Überblick über alle IT-Kosten zu behalten.

Herausforderungen der Cloud-Ära

In vielen Unternehmen ist ITFM nach wie vor eine statische Disziplin: Budgetplanungen erfolgen jährlich, Controlling und Forecasting monatlich. Dabei kommen häufig traditionelle IT-Controlling-Werkzeuge oder auch Excel zum Einsatz. Solche statischen Tools stoßen jedoch an ihre Grenzen, sobald dynamische Cloud-Services hinzukommen. Cloud-Dienste sind aufgrund ihrer Flexibilität für moderne IT-Landschaften äußerst attraktiv. Sie können nach Bedarf gestartet oder gestoppt werden, was zwar Agilität bringt, gleichzeitig aber auch eine neue Ebene der Kostenplanung und -kontrolle erforderlich macht.

➤ **Schnelle Kostenänderungen und Budgetüberschreitungen:** Ein zentrales Problem der Cloud-Dienste ist ihre Volatilität in Bezug auf Kosten. Werden zusätzliche Ressourcen benötigt, so können diese umgehend gestartet werden, was jedoch auch unvorhergesehene und teilweise erheblich höhere Ausgaben mit sich bringt. In kurzer Zeit können diese Kosten das geplante Budget übersteigen, wodurch die Notwendigkeit entsteht, die Cloud-Kosten in deutlich kürzeren Intervallen zu überwachen und bei Bedarf korrigierende Maßnahmen zu ergreifen.

➤ **Limitierte Cloud-Only-Tools:** Eine erste Abhilfe besteht oft in der Einführung spezieller Cloud-Tools, die ausschließlich die Cloud-Kosten im Blick haben. Der Einsatz solcher Lösungen wird häufig von Cloud Center of Excellence (CCoE)- oder FinOps-Teams initiiert.

Sie erfassen zwar detaillierte Ausgaben der Cloud-Umgebungen, können jedoch keine vollständige Sicht auf die IT-Kosten eines Unternehmens bieten, da sie die Cloud-Kosten isoliert betrachten und keine Verknüpfung mit anderen Kostenkomponenten vornehmen.

➤ **Fehlende Verbindung zwischen Cloud-Assets und Business Services:** Cloud-Tools erkennen die individuelle Nutzung und Kosten der Cloud-Ressourcen, jedoch oft ohne Berücksichtigung der Business-Services, die durch diese Ressourcen unterstützt werden. Dies verhindert eine ganzheitliche Bewertung und eine klare Zuordnung der Cloud-Kosten zu den verschiedenen Business-Services.

➤ **Hybride IT-Umgebungen und Fragmentierung:** Unternehmen setzen vermehrt auf hybride IT-Umgebungen, bei denen neben der Cloud auch On-Premises-Infrastrukturen zum Einsatz kommen. Diese verschiedenen Infrastrukturen sowie zusätzliche Kosten für Personal in Entwicklung, Support und Betrieb werden meist in traditionellen ITFM-Tools verwaltet. Das Resultat ist eine fragmentierte Kostenübersicht, die eine umfassende und exakte Kostenanalyse der Business-Services erschwert.

Konsolidierte Kostenkontrolle

Um den Herausforderungen eines dynamischen und fragmentierten IT-Kostenma-

CLOUD-KOSTEN ISOLIERT ZU BETRACHTEN WIRD DER KOMPLEXITÄT IN HYBRIDEN UMGEBUNGEN NICHT GERECHT. NUR EINE GANZHEITLICHE KOSTENBETRACHTUNG ERMÖGLICHT DIE STEUERUNG AUF BASIS DER WERTSCHÖPFUNG.

Bert Kondruss,
Director Product Management,
USU GmbH, www.usu.com

nagements zu begegnen, wird der Einsatz eines ganzheitlichen ITFM-Tools zunehmend unverzichtbar. Ein solches Tool führt sämtliche Kosten, die mit einem Business-Service verbunden sind – darunter On-Premises- und Cloud-Infrastrukturen sowie Personalkosten – in einer zentralen Datenbank zusammen und bildet sie in einem einheitlichen Kostenmodell ab.

Funktionsweise eines ganzheitlichen ITFM-Tools

Ein ITFM-Tool, das den Anforderungen der Cloud-Ära gerecht wird, übernimmt eine Reihe von Aufgaben, die weit über die bloße Erfassung und Verwaltung einzelner Kostenbestandteile hinausgehen:

#1 **Zentrale Erfassung und Überwachung aller Kosten:** Ein ganzheitliches ITFM-Tool erfasst und überwacht sämtliche Kostenarten (On-Premises, Cloud, Personal) in einem integrierten System. Dies ermöglicht eine umfassende Kostenübersicht über alle Infrastrukturen und Ressourcen hinweg.

#2 **Kostenzuordnung zu Business-Services:** Das Tool übernimmt die Zuordnung der Kosten einzelner Infrastrukturelemente zu den unterstützten Business-Services. Diese Zuweisung erfolgt anhand der in der Configuration Management Database (CMDB) hinterlegten Abhängigkeiten zwischen IT-Assets und Business-Services. Durch diese Zuordnung wird eine Basis für Entscheidungen wie Benchmarking, Make-or-Buy-Analysen und die Berechnung des Business Value eines Service geschaffen.

#3 **Automatisierte Datenerfassung und Cloud-Kostenmanagement:** Die dynamische Natur der Cloud-Dienste erfordert ein automatisiertes Discovery-Verfahren, das die Kosten der genutzten Cloud-Dienste täglich über standardisierte Schnittstellen direkt von den Cloud-Providern einliest. Mithilfe eines standardisierten, hierarchischen Tagging-Schemas werden die Cloud-Ressourcen automatisch mit ihren Abhängigkeiten in der CMDB abgebildet. Anschließend werden die Kosten der einzelnen Cloud-Ressourcen über die Hierarchieebenen hinweg aggregiert, sodass sie sich auf höchster Ebene den jeweiligen Business Services zuordnen lassen.

#4 **Transparenz durch Analyse- und Reporting-Funktionen:** Ein modernes ITFM-Tool bietet umfassende Analyse- und Reporting-Möglichkeiten. Die vollständige Abdeckung aller Kostenarten ermöglicht detaillierte Einblicke in die IT-Ausgaben eines Unternehmens und erlaubt ein Drill-Down bis auf Komponentenebene. Dies schafft Klarheit für diverse Stakeholder – von CxOs über Business-Verantwortliche bis hin zu Operations-Teams, CCoE und FinOps.

Vorteile einer ganzheitlichen ITFM-Lösung

Die Integration aller Kostenarten in einem Tool bringt eine Vielzahl von Vorteilen für das IT Financial Management mit sich:

➤ **Konsolidierte Sicht auf sämtliche IT-Kosten:** Die Einbindung aller Kostenarten in ein zentrales System verhindert die isolierte Betrachtung einzelner Kostenblöcke. Nur eine ganzheitliche Sicht auf alle anfallenden Kosten bietet eine gute Grundlage für Business-Entscheidungen.

➤ **Gemeinsame Datenbasis für alle Stakeholder:** Unterschiedliche Stakeholder – vom CxO über Business- und Operations-Teams bis hin zu FinOps – erhalten relevante Informationen, die auf ihre jeweiligen Bedürfnisse zugeschnitten sind. Dies verbessert die Transparenz und sorgt dafür, dass alle Beteiligten auf einer gemeinsamen Datenbasis arbeiten.

➤ **Vermeidung isolierter Kostenanalysen:** Durch die ganzheitliche Betrachtung lassen sich Kostentreiber besser identifizieren und Optimierungsmaßnahmen gezielt umsetzen. Eine isolierte Betrachtung von Cloud-Kosten, wie sie in traditionellen Cloud-Only-Tools vorliegt, führt hingegen häufig zu Fehleinschätzungen, da die Cloud-Kosten ohne Berücksichtigung der Gesamtkosten bewertet werden.

Fazit

Mit der fortschreitenden Nutzung von Cloud-Diensten in der IT-Landschaft ist ein Umdenken im IT Financial Management unumgänglich. Die dynamische Natur der Cloud erfordert kürzere Überprüfungsintervalle und flexibel skalierbare Lösungen, die alle IT-Kostenarten abbilden. Ein ganzheitliches ITFM-Tool vereint sämtliche Kostenarten und bietet so eine fundierte Basis für Entscheidungen, die das Kostenmanagement der IT-Abteilung nachhaltig verbessern können. Indem die Gesamtkosten eines Business Services zentral erfasst und überwacht werden, erhalten Unternehmen eine präzise und verlässliche Kostenübersicht, die sie in einer zunehmend hybriden und dynamischen IT-Welt unterstützt.

Martin Landis | www.usu.com

E-Rechnung: Pflicht oder Chance?

VON DER GESETZESANFORDERUNG ZUM DIGITALISIERUNGSSCHUB

Komplexe Richtlinien, gesetzliche Vorgaben und ein undurchsichtiger Dschungel an Angeboten haben die Akzeptanz und das Umsetzungstempo der E-Rechnungspflicht zwar etwas gebremst, aber die Einführung der E-Rechnung ist ein zentrales Thema, das aktuell viele Unternehmen und öffentliche Einrichtungen beschäftigt. Das zeigt auch die jüngste Bitkom-Umfrage, denn 88 Prozent der Unternehmen sind trotz E-Rechnungspflicht noch immer nicht vollständig vorbereitet. In vielen Organisationen fehlt es an Know-how und Ressourcen. Organisationen befinden sich in einer Umbruchphase, aber es besteht weiterhin enorm viel Informationsbedarf. Mit den folgenden drei Tipps wird die E-Rechnung in Unternehmen und öffentlichen Einrichtungen nicht mehr als zusätzliche Belastung wahrgenommen, sondern als Katalysator für Digitalisierung und Prozessautomatisierung.

#1 Evaluierung der bestehenden Systeme

Die Integration neuer Lösungen bedeutet immer hohen Aufwand und Kosten, sowohl in technischer als auch organisatorischer Sicht. Die E-Rechnungspflicht betrifft 3,5 Millionen Unternehmen in Deutschland und dies multipliziert mit dem Zeitaufwand für die Implementierung bedeutet schlicht, dass integrierte Lösungen nicht für alle Unternehmen bis zum jeweiligen Stichtag des Gesetzgebers erreicht werden können.

Bestehende Systeme decken oft nur einen Teil der zu digitalisierenden Dokumente ab und sind zudem nicht ausreichend auf die zukünftigen Anforderungen der E-Rechnung vorbereitet. Daher ist eine spezialisierte oder zumindest modulare Lösung wesentlich sinnvoller. Eine Lösung, die flexibel einsetzbar und integrierbar ist und grenzüberschreitende Standards und Formate beherrscht. Das kann unter dem Strich sogar zu einer Reduzierung der Prozesskosten führen.

Unternehmen müssen ihre Systeme also nicht grundlegend ändern, denn es gibt auch Wege, bestehende Systeme ohne langwierige Projekte und hohe Zusatzinvestitionen mit einer flexiblen Lösung zu ergänzen. Wichtig für eine Lösung ist, dass sie den gesamten Prozess der E-Rechnung von der Vorbereitung bis zur Prüfung begleitet, die Dokumentenprozesse automatisiert, die Rechnungen revi-

sionssicher archiviert und an die digitale Steuerdatenübermittlung angebunden ist. Deshalb ist es wichtig, dass die Unternehmen das Angebot auf dem Markt genau prüfen.

#2 Genaue Prüfung der angebotenen Lösungen

Die Unübersichtlichkeit der Angebote auf dem Markt stellt für viele Unternehmen eine große Hürde in der Umsetzung der E-Rechnungspflicht dar. Viele Dienstleister bieten nur Teillösungen an, wie den Versand oder Empfang von E-Rechnungen über unsichere Kanäle. Zudem sind sich Unternehmen oft nicht bewusst, dass in Zukunft weitere Anforderungen hinzukommen werden, wie beispielsweise die Meldung von Umsatzsteuerinformationen an staatliche Plattformen. Dies führt häufig zu Investitionen in Insellösungen oder unzureichende ERP- und DMS-Systeme. Es ist wichtig, einen Dienstleister zu wählen, der das Thema E-Rechnung ganzheitlich und gemeinsam mit den Organisationen angeht und dabei die Prozesse nicht aus den Augen verliert. Ricoh IDX beispielsweise ermöglicht einen flexiblen und effizienten Ansatz, der den Unternehmen Nachrüstungen erspart.

Auch die Sicherheit ist eine große Herausforderung: Über 90 Prozent der Cyber-Angriffe beginnen über das Einfallstor E-Mail, und genau diesen Kanal nutzen viele Unternehmen für den Versand ihrer E-Rechnungen. Eine sichere End-to-End-Lösung bietet umfassenden Schutz und reduziert die Sorge vor einem möglichen Sicherheitsvorfall.

MEHR WERT
Intelligent Data Exchange

UNTERNEHMEN SOLLTEN AUF EINEN TECHNOLOGIEPARTNER SETZEN, DER DAS THEMA E-RECHNUNG GANZHEITLICH UND GEMEINSAM MIT IHNEN ANGEHT UND DABEI DIE PROZESSE NICHT AUS DEN AUGEN VERLIERT.

Ingo Wittrock, Regional Director Marketing Central & Eastern Europe, Ricoh Deutschland, www.ricoh.de

Ein großer Irrglaube vieler Unternehmen ist auch, dass es nur ein ZUGFeRD-Format oder eine E-Rechnung gibt. Ricoh beispielsweise bietet über 400 Datenformate und sichere Übertragungsverfahren an, darunter PEPPOL, EDI, Webservices und API. Insgesamt gibt es rund 20.000 Kombinationsmöglichkeiten, die eine Plattform größtenteils bedienen können muss.

#3 Förderung der Prozessautomatisierung

Die E-Rechnung ist ein sehr wichtiger Baustein der Digitalisierung – nicht nur für Unternehmen, sondern gerade auch im Bereich der öffentlichen Verwaltung. Diese sind bereits seit Jahren verpflichtet, nur noch elektronische Rechnungen zu akzeptieren. Nun steigt der Druck indirekt dadurch, dass bis spätestens 2028 fast alle Rechnungen digital sein müssen. Der Nutzen der E-Rechnung steht außer Frage – Sicherheit, Prozessoptimierung, Nachvollziehbarkeit sind ein großes Plus und Anreiz für weitere Digitalisierungsprojekte.

Eine zertifizierte Lösung wie zum Beispiel Ricoh IDX läuft automatisiert im Hintergrund und hilft, Geschäftsprozesse effizienter zu gestalten. Prozesse, wie beispielsweise das manuelle Einpflegen von Rechnungsdaten in Portale, gehören damit der Vergangenheit an. Denn Unternehmen benötigen eine Systematik, die alle Standards erfüllt und gleichzeitig den Aufwand in jeder Hinsicht so gering wie möglich hält. Mit der Implementierung einer sicheren Dokumentendrehscheibe wird nicht nur der Rechnungsaustausch vereinfacht: Mit einem in die Lösung integrierten hybriden Postausgang kann beispielsweise jeder Sachbearbeiter seine Post per Knopfdruck von überall und kostenoptimiert auf den Weg bringen. Damit dieser Prozess reibungslos abläuft, ist es wichtig, Geschäftspartner oder Lieferanten in den Implementierungsprozess der E-Rechnung mit einzubeziehen, um einen unterbrechungsfreien Geschäftsablauf zu gewährleisten. So können mit Hilfe der Prozessautomatisierung manuelle und unnötig komplexe Prozessschritte über mehrere Stufen hinweg einfacher und effizienter gestaltet werden.

Die E-Rechnung als Digitalisierungsmotor

Unternehmen sollten auf einen Technologiepartner setzen, der das Thema E-Rechnung ganzheitlich und gemeinsam mit ihnen angeht und dabei die Prozesse nicht aus den Augen verliert. Denn bei einer guten Umsetzung entfällt künftig ein hoher Zeitaufwand für manuelle Prüf- und Bearbeitungsschritte. Hilfreich sind dabei erprobte und schlüsselfertige Plattformen, insbesondere für das digitale Dokumentenmanagement und den elektronischen Datenaustausch, sowie die Anbindung an standardisierte und rechtssichere Netze, die alle aktuellen und zukünftigen Anforderungen des Wachstumschancengesetzes erfüllen. Der Vormarsch der E-Rechnung zeigt, dass ein möglichst papierloses Büro und die Automatisierung von Prozessen ein wichtiges Ziel für Unternehmen sein sollte.

Ingo Wittrock

Software, die wirklich greift

WARUM PROZESSORIENTIERTES REQUIREMENTS ENGINEERING UNVERZICHTBAR IST

Kennen Sie das, eine neue Softwarelösung wird den hohen Erwartungen nicht gerecht, obwohl ihr ein umfangreiches Projekt vorausgeht? Die Antwort liegt oft in der Art und Weise, wie sie entwickelt wird: Es wird sich auf Funktionalitäten konzentriert, ohne die Business-Prozesse End-to-End zu berücksichtigen. Was passiert also, wenn in Software-Projekten die fachlichen Abläufe nur oberflächlich betrachtet und Business-Prozesse nicht wirklich erfasst werden? Genau hier setzt PoRE, das prozessorientierte Requirements Engineering an.

Stellen Sie sich vor, Ihre HR-Abteilung steht vor der Herausforderung, täglich hunderte Bewerbungen zu koordinieren – doch mit dem eingesetzten System können die für Sie so wichtigen Daten und Informationen nur zum Teil erfasst und verarbeitet werden. Es fühlt sich an, als würde man einen wertvollen Schatz nur in groben Umrissen sehen, ohne die feinen Details und unternehmensindividuellen Bedürfnisse, die den Rekrutierungsprozess erst lebendig machen, heben zu können. Was wäre, wenn Ihre IT-Lösung nicht nur den Bewerbungsprozess abbildet, sondern ihn lebt? Ein System, das den Herzschlag Ihrer Personalgewinnung kennt – und alle Perspektiven und Anforderungen Ihrer Mitarbeitenden aktiv in den Mittelpunkt stellt.

Wir glauben daran, der Schlüssel zum Erfolg liegt darin, Prozesse in ihrer vollen Ausprägung in den Fokus zu rücken und darüber Anforderungen prozessorientiert zu entwickeln. Während bei traditionellen Vorgehensweisen viele Details und viel Wissen der Fachexperten, oft auch wichtige Schnittstellen unberührt bleiben, heben wir diese Schätze mit einem ganzheitlichen, prozessorientierten Ansatz im Requirements Engineering. Wir werfen den Blick hinter den Vorhang und machen so aus einem Tool die Grundlage für ein

Gesamtpaket, das nicht nur die Effizienz steigert, sondern auch die menschliche Komponente in den Mittelpunkt stellt.

Authentische Dynamik für Ihre Geschäftsprozesse

In vielen Unternehmen dominiert noch immer die projekt- oder funktionsbezogene Sicht auf Anforderungen. Wie im obigen Beispiel, werden insbesondere in IT-Projekten Anforderungen oft auf Projekt- oder Bereichsebene definiert – mit begrenztem Blick auf das Gesamtunternehmen. Entscheidungen, Ziele und Verantwortlichkeiten orientieren sich an Projekt- oder Bereichsstrukturen, während Prozesse eher als Nebenprodukt betrachtet werden. Trotz wachsendem Wunsch nach prozessualem Denken bleibt die Prozessentwicklung in solchen Strukturen oft zweitrangig.

Perspektivwechsel: Prozessorientierte Organisation

In der prozessorientierten Organisation werden Anforderungen ganzheitlich und unternehmensweit betrachtet. Grundlage bildet ein unternehmensweit getragenes Prozessmodell mit:

- Systematisch und vollständig dokumentierten Prozessen bis auf Arbeitsebene,
- eindeutig zugewiesenen Verantwortlichkeiten,
- strategisch getroffenen Entscheidungen mit klarem Prozessbezug,
- konkreten Zielgrößen zu den Prozessen, ausgerichtet an der Unternehmensstrategie.

Das Prozessmodell ist nicht nur Referenz, sondern Ausgangspunkt aller Anforderungen im PoRE.

Anforderungen der Unternehmen – die neue Realität

Unternehmen stehen vor der Herausforderung, steigende Komplexität und Dynamik zu bewältigen. Dafür braucht es ein durchgängiges, prozessorientiertes Anforderungsmanagement, das:

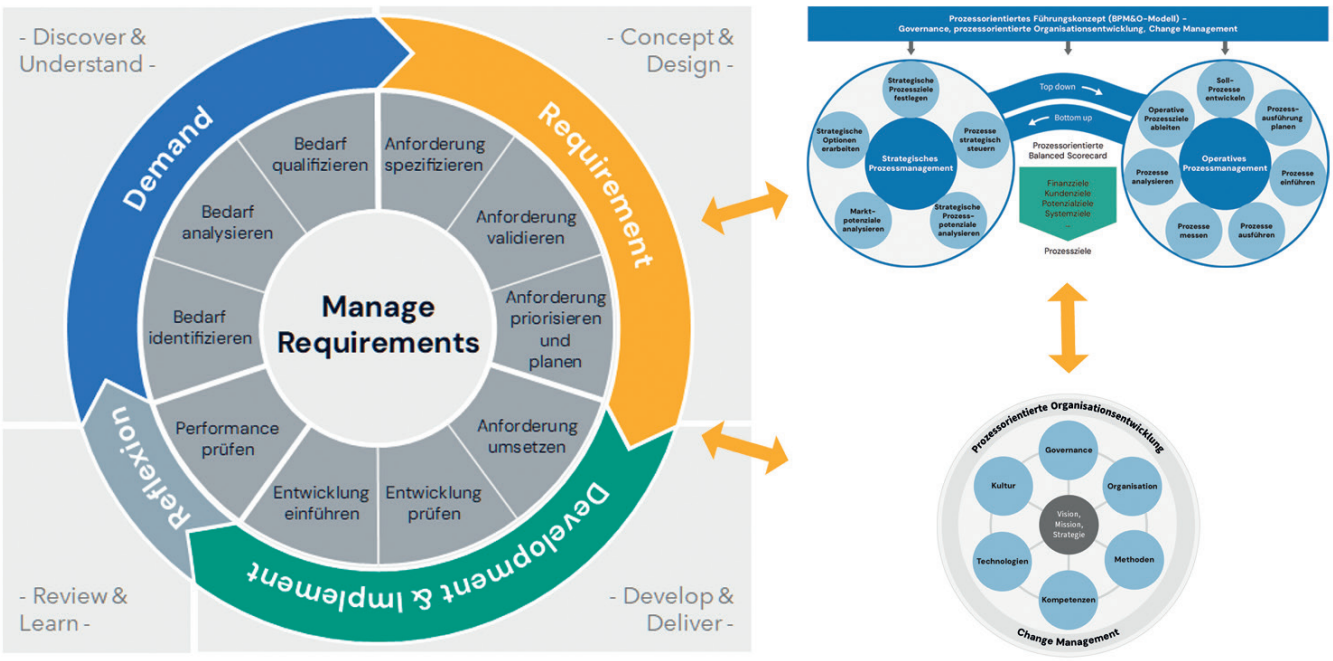
- Anforderungen integriert steuert,
- Schnittstellen, Aufgaben und Verantwortlichkeiten eindeutig definiert,
- Nachvollziehbarkeit (Traceability) sicherstellt,
- Transparenz und Steuerbarkeit über alle Ebenen hinweg gewährleistet.

Ein zentrales Prozessmodell ist der Schlüssel zur Konsistenz und Stabilität in Organisation und IT.

Leitidee der prozessorientierten Organisation

Um diesen Anforderungen gerecht zu werden, folgt die prozessorientierte Organisation einer klaren Leitidee, in der das prozessorientierte Requirements Engineering einen wichtigen Knotenpunkt bildet (Bild 1).

BILD 1: LEITBILD MIT PORE



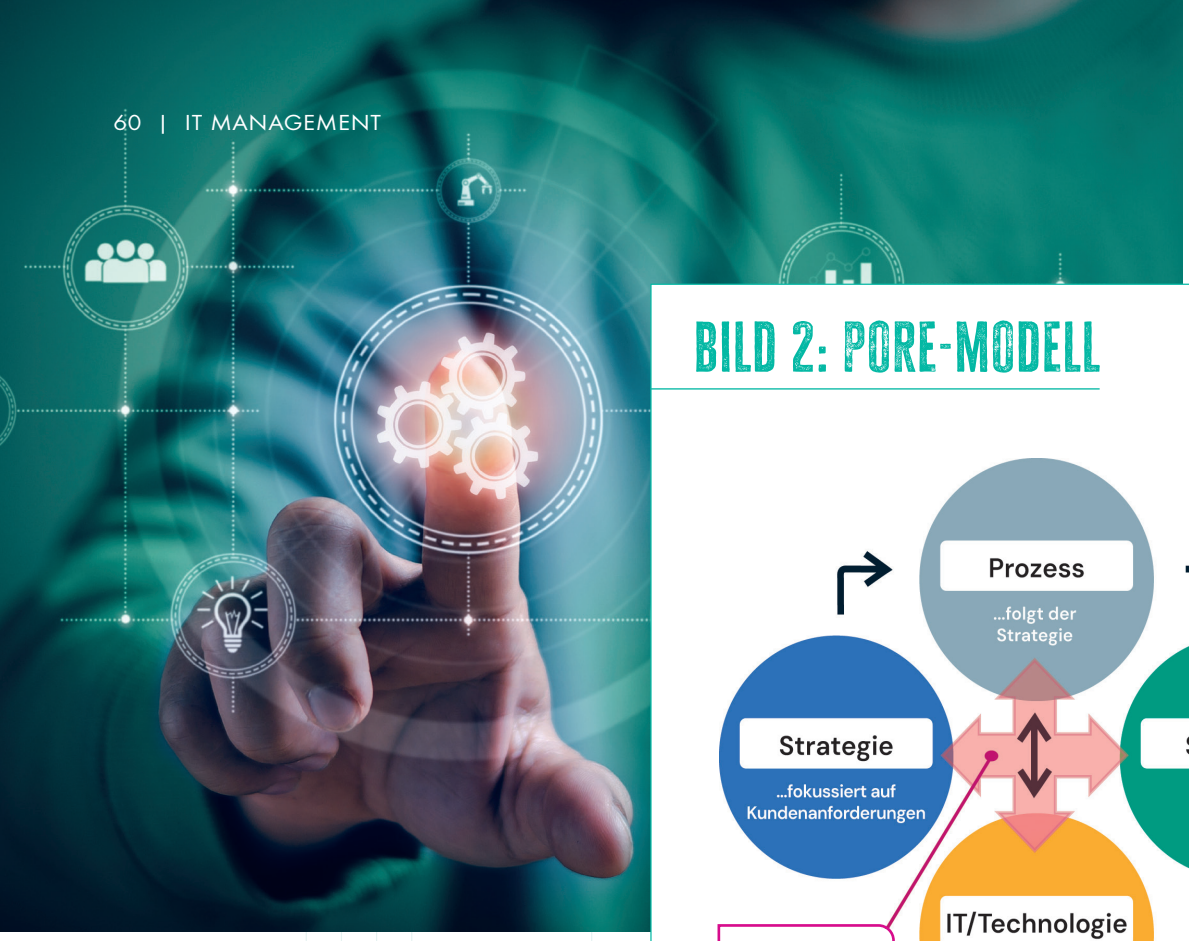


BILD 2: PORE-MODELL

NUR WER ANFORDERUNGEN IM PROZESSZUSAMMENHANG VERSTEHT, KANN UNTERNEHMENS- UND IT-STRATEGIEN WIRKSAM UND ZUKUNFTSSICHER GESTALTEN UND DAMIT ZU EINER NACHHALTIGEN DIGITALISIERUNG BEITRAGEN.

Matthias Böhme, Management-Berater, BPM&O GmbH, www.bpmo.de

Die Leitidee zeigt, IT und Prozesse sind heute untrennbar verbunden – ohne Prozesse keine sinnvolle IT-Unterstützung, ohne IT keine skalierbaren Prozesse.

Schnittstelle und Steuerungsinstrument

PoRE verbindet Strategie, Struktur, Prozess und IT. Es greift auf bewährte Methoden zurück, zum Beispiel:

- Strategisches und operatives Prozessmanagement,
- klassisches und agiles Projektmanagement,
- Software- und Testmanagement,
- Anforderungs- und Change Management. (Bild 2)

Von der Strategie zur Umsetzung

Dieser Ansatz fördert eine durchgängige Top-Down-Ausrichtung – von der Unternehmensstrategie bis zu jeder einzelnen an den Unternehmenszielen ausgerichteten und mit Kennzahlen gemessenen Aufgabe im Prozess. Werden diese Aufgaben mit Hilfe oder durch eine IT-Anwendung ausgeführt, besteht wiederum ein direkter Bezug der eingesetzten IT-Anwendung zur Unternehmensstrategie.

Praxisbeispiele

1. SAP S/4HANA-Einführung mit PoRE

Im Rahmen einer SAP S/4HANA-Transformation hat ein mittelständisches Unternehmen seine IT-Organisation neu strukturiert: Die IT-Abteilung wurde in zwei Verantwortungsbereiche unterteilt – „Design und Development" sowie „Service und Betrieb". Zusätzlich wurde ein drittes, unabhängiges SAP-Team etabliert, das ausschließlich SAP S/4HANA-Themen verantwortet.

Auf Basis des PoRE-Frameworks entwickelte das SAP-Team einen klar definierten Prozess zur Aufnahme, Spezifikation, Umsetzung, Test und Veröffentlichung

von Anforderungen. Dadurch konnten von Beginn an folgende Prinzipien berücksichtigt werden:

- Entwicklung von SOLL-Prozessen, sofern erforderlich,
- Ableitung von Anforderungen auf Basis bestehender Geschäftsprozesse,
- enge Synchronisation zwischen Prozessdesign und SAP-Entwicklung, insbesondere bei Test und Einführung.

Eine Analyse zeigte, dass die ursprünglich separaten Prozesse der drei Teams methodisch ähnlich waren und aufeinander aufbauten. Daher war es naheliegend, die abgeglichenen Prozessschritte zu einem durchgängigen Prozess zusammenzuführen, sowie ein übergreifendes Testmanagement einzuführen.

Das Ergebnis war ein konsolidierter End-to-End-Prozess mit deutlich verbessertem, gegenseitigem Verständnis. Dieser trug wesentlich dazu bei:

- Nachbesserungsaufwände zu reduzieren,
- Anforderungen ganzheitlich und konsistent zu erfassen,
- Effektivität, Effizienz und Qualität in der IT-Bereitstellung nachhaltig zu steigern.

Dieses Beispiel verdeutlicht, wie PoRE in komplexen IT-Umgebungen zur strukturierten und nachhaltigen Umsetzung von Anforderungen beitragen kann.

Wichtiger Baustein der Organisationsentwicklung

Ein deutschlandweit tätiges Bauunternehmen mit über 25 Standorten und mehr als 2.000 Mitarbeitenden entschied sich, seine Organisation grundlegend zu transformieren – weg von einer funktional ausgerichteten Struktur hin zu einer prozessorientierten Organisation. Ziel der Neuausrichtung war es Transparenz, Effizienz und Kundenorientierung nachhaltig zu steigern.

DIE STEUERUNG VON PROZESSANFORDERUNGEN IST DER SCHLÜSSEL FÜR EINE NACHHALTIGE DIGITALISIERUNG.

Danijela Bagaric, Management-Beraterin, BPM&O GmbH, www.bpmo.de

Im Zuge der Neugestaltung zentraler Geschäftsprozesse sowie der Einführung klar definierter Prozessrollen traten zahlreiche Verbesserungspotenziale innerhalb der Organisation zutage. Um diese strukturiert, bereichsübergreifend und zielgerichtet zu bearbeiten, wurde ergänzend zum Projekt- und Prozessmanagement PoRE etabliert.

Der entscheidende Mehrwert lag in der integrierten Ausgestaltung. Anders als in klassischen Anforderungsprozessen wurden hier:

- gezielt die Abhängigkeiten zwischen Prozessen analysiert und berücksichtigt,
- Prozessverantwortliche aktiv in den Anforderungsmanagementprozess eingebunden,
- eine direkte Verbindung operativer Anforderungen mit der übergeordneten Unternehmensstrategie ermöglicht.

Dieses ganzheitliche Anforderungsmanagement schaffte die Grundlage dafür, dass Veränderungen nicht isoliert, sondern im Gesamtzusammenhang bewertet und umgesetzt wurden – ein zentraler Erfolgsfaktor für die agile und nachhaltige Organisationsentwicklung.

Vorteile für Ihr Unternehmen

PoRE als Ansatz integriert verschiedene Management-Systeme und -Methoden:

- Der ganzheitliche Ansatz im strategischen Prozessmanagement richtet die IT systematisch auf die Unternehmensstrategie aus
- Das operative Prozessmanagement nutzt kontinuierliche Verbesserungsmethoden wie KVP, Kaizen und den PDCA-Zyklus
- Change Management berücksichtigt organisatorische und kulturelle Aspekte für einen nachhaltigen Wandel
- Testmanagement sichert die nachhaltige Implementierung und Expansion
- Requirements Engineering setzt strukturierten Umgang mit Anforderungen um

Die Integration des PoRE-Ansatzes steigert den Erfolg in der täglichen Arbeit erheblich. Ein einheitliches Prozessmodell ermöglicht die unternehmensweite Integration von Anforderungen, steuert Risiken und Qualität und reduziert so Komplexität. Die präzise Steuerung von Aufgaben und Datenflüssen sichert die Konsistenz zwischen Schnittstellen. Die zielorientierte Steuerung sorgt für ein transparentes Management, das auf Effektivität, Effizienz, Compliance und Stabilität ausgerichtet ist.

Danijela Bagaric, Matthias Böhme

Digitalisierung ist ein Change

WARUM SCHEITERN TROTZDEM SO VIELE PROJEKTE IMMER AN DEN SELBEN PUNKTEN?

Wenn über Digitalisierung gesprochen wird, scheint für alle klar zu sein, dass damit ein Veränderungsprozess verbunden ist. Auf Nachfrage zeigt sich allerdings auch, dass Digitalisierungs-Projekte immer noch technikzentriert und mit einem klassischen Planungs-Paradigma angegangen werden. Erst wenn die Akzeptanz der Mitarbeitenden in Frage steht, kommt Change Management zur Anwendung.

Unser Verständnis von „Change" ist umfassender und konkret: Change umfasst von Anfang an immer Elemente einer Organisation wie Prozesse, Strukturen, Kultur, Führung und Personalentwicklung, im Rahmen der Mission und der strategischen Ziele eines Unternehmens.

Change braucht immer die Mitwirkung der Betroffenen im Unternehmen, beginnend bei der Entwicklung eines gemeinsamen Zielbilds (Was soll nach der Einführung der IT oder der Digitalisierung anders sein soll als bisher?). Zu klären sind Begriffe, Zusammenhänge im Ökosystem, die erforderliche Flexibilität unter VUCA-Bedingungen und schließlich das Vorgehen im Change-Prozess.

Dass es an derartigen Klärungen mangelt, erkennen wir an den regelmäßig wiederkehrenden Befunden (zum Beispiel: McKinsey, PWC, Standishgroup).

Warum Projekte zu 60-70 Prozent scheitern:

#1 Unklares Ziel
#2 Unklarer Projektauftrag
#3 Unrealistische Pläne

EINIGE UNSERER FRAGEN ZUM CHANGE-/ DIGITALISIERUNGS-CHECK

Welches Bild haben wir?
- Worum geht es in der Veränderung wirklich?
- Welche Hinweise auf Veränderungsnotwendigkeit gibt es woher (externe Impulse, Feedback aus Organisation)?
- Wohin und wie stark/ wie weit sollten wir uns verändern?
- Wo sollten wir neu denken?
- Wo sollten wir ansetzen, worauf konzentrieren?
- Welche Rolle spielt dabei die Digitalisierung?

Wie entwickeln wir eine empowernde Führung?
- Welche Führungskultur (Reifegrad) brauchen wir für eine anpassungsfähige Organisation?
- Was tut Führung, um andere Haltungen zu fördern (Verantwortungsübernahme, Selbstorganisation, Lernen, ...)
- Wie entwickeln wir eine wirksame Führungskultur?
- Wie teilen wir Führungsaufgaben und –rollen im Change?

Wie nutzen wir die vorhandene Intelligenz?
- Welche Sensoren haben wir bzgl. Kunden, Wettbewerb, Markt, eigener Haltung, (Zusammen-)Arbeit und Wirksamkeit?
- Welche Stimme haben die „Jungen"/ die „Querdenker"?
- Welche Informations- und Beteiligungskultur wird gelebt?
- Wie können wir „verstreutes Wissen" besser teilen und nutzen?
- Welche Lern- und Kommunikationskultur braucht es dafür?
- Wie sind Strukturen und Mechanismen anzupassen?

Wie organisieren wir wirksamen Change?
- Haben wir erkannt, welche Strukturen, Prozesse und Rollen hilfreich sind, um den Change umzusetzen?
- Wie passt diese Strategie zur Digitalisierung und wie kann das besser verschränkt werden?
- Wie wollen wir den Change flexibel und wirksam planen, steuern, kommunizieren?
- Welche organisationalen Aufgaben sind anzugehen?
- Womit und wie können wir schnell beginnen (MVPs)?

Wie können wir alle Kräften bündeln?
- Welche Stärken haben wir an Bord - wo ist viel Energie?
- Welche zukunftsrelevanten Stärken müssen wir ausbauen?
- Wie können wir kritische Schwächen ausgleichen?
- Wie können wir Fähigkeiten und Motivationen vernetzen?
- Welche Hindernisse, schädlichen Muster oder Illusionen sind zu erkennen, und wie können wir sie bearbeiten?

Bild 1

#4 Nur anfangs formulierte Risiken

#5 Verleugnung von Problemen nd Schwierigkeiten im Umgang mit Komplexität

#6 Inkonsequenz, etwa in der Anwendung agiler Verfahren

#7 Unsicherheit in der Besetzung und Fluktuation

#8 Mangelnde Stakeholder-Analyse und Kommunikation

#9 Ständige Debatten aufgrund dieser Unklarheiten und Unsicherheiten

Das ist allerdings „Oberflächen-Statistik" und symptomatisch für Verhaltensmuster im Unternehmen. Keiner kommt auf die Idee, dahinter zu schauen - vielmehr werden reflexartig bekannte Ratschläge zur Einhaltung des PM-Kanons wiederholt, was bisher nichts gebracht hat.

Die wirklichen Gründe für nachhaltigen Change

Bei Ergründung der genannten Punkte kommen wir nach Auswertung unserer Erfahrungen zu Fragestellungen, die in Change-Prozessen hilfreich sein können (siehe Bild 1).

Mithilfe solcher Erkenntnisse kann sich eine erste Entscheidung ergeben, was wann in welchem Umfang mit wem als „Change" angepackt werden sollte; daraus lässt sich eine erste Roadmap ableiten.

Gleichzeitig wird deutlich, dass insbesondere mittelständische Unternehmen für ein solches, reflektiertes Vorgehen erfahrene, ganzheitlich denkende Berater brauchen, die nicht nur ihre Produkte, Rezepte und Systeme verkaufen wollen, sondern Change-Prozesse als eine gemeinsame Herausforderung verstehen.

Statt Technologie und Systeme in den Mittelpunkt der Diskussion zu stellen, halten wir es für günstiger, herauszuarbeiten, was für den Kunden eine sinnvolle Wertsteigerung und für die Mitarbeitenden eine deutliche Verbesserung der Arbeitsbedingungen sein kann. Hierzu braucht es die Beteiligung der Beschäftigten mit deren Perspektiven, Erkenntnissen und Lösungsideen. Damit werden auch das Engagement und die Akzeptanz für den Change – quasi nebenher - unterstützt.

Gründe des „Scheiterns"

Wie kann es passieren, dass qualifizierte Projektleiter/-managerInnen, die ihren Projektmanagement-Kanon gelernt haben, die bekannten Erfolgsvoraussetzungen wie zum Beispiel Auftragsklärung oder Stakeholder-Analyse nicht realisieren und Projekte anhand solcher Punkte immer wieder scheitern?

Einige Vermutungen dazu:

#10 **1.** Es wird an dem Grundsatz der einmaligen Auftragsklarheit festgehalten, oder der Grundsatz wird frustriert aufgegeben, weil nicht realisierbar. Wenn man aber den „change-Angang" verinnerlicht hat, geht man davon aus, dass alles im Fluss ist und immer wieder nachgeklärt werden muss und sich der Auftrag erst im Zuge der Projektarbeit konkretisiert. Daher sprechen wir von „iterativem" Vorgehen.

#11 **2.** Eng damit verknüpft ist die so genannte Planungs-Illusion: in einem komplexen und dynamischen Umfeld führt eine lineare Planungs-Logik zwangsläufig zu enormem planerischem Aufwand und zu einem immer größer werdenden Gap zwischen geplantem und realem Zustand und zu Konflikten.

#12 **3.** Zudem funktioniert die Terminsetzung schon wegen des ungeeigneten oder fehlenden Priorisierungsprozesses nicht. In vielen Unternehmen setzt man sich nicht realistisch mit den vorhandenen Kapazitäten, fachlichen Möglichkeiten und Gegebenheiten des Projekt-Portfolios auseinander- und wenn, dann meist ohne Einbeziehung der Betroffenen.

Wir stellen in unserem Vorgehen das Organizational Change Management in den Mittelpunkt, ein Aspekt, der hinter guter Projektorganisation und Konfliktmanagement auf Platz 3 einer evidenzorientierten Studie liegt (Komus u.a., 2015). Es geht darum, in unser Denken und Handeln auch das Ökosystem des Change-Projekts einzubeziehen: das Umfeld im Unternehmen, Kunden, Zulieferer, Banken, Mitbewerber (Häußling et al., 2012; Borgert, 2014, Fachgruppe systemisches PM, 2018).

Einige Hinweise zum Organizational Change Management aus unserer Erfahrung:

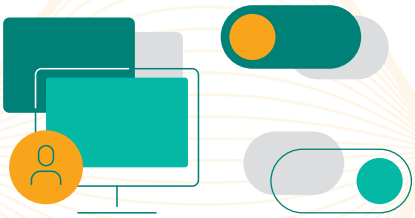
#13 Zielklärungen oder Planungen sollten nur in offener, konstruktiver Auseinandersetzung mit den Betroffenen stattfinden. Es geht darum, sich auf einen machbaren Weg zu einigen, um das Respektieren von Grenzen, um die gemeinsame Klärung von Engpässen.

#14 Für das iterative Vorgehen ist wichtig, dass die nötigen Schritte und Erprobungen mit einem ehrlichen Feedback durchgeführt werden, um daraus Entscheidungen zum weiteren Vorgehen treffen zu können. Dazu ist eine passende Fehler-Kultur zu etablieren, um Lernen zu ermöglichen.

#15 Bezüglich der Stakeholder-Analyse oder Risiko-Analyse wird zum Teil auch mit fehlender Zeit argumentiert. Das sehen wir nicht als Scheiter-Grund - vielmehr ist nicht die Zeit, sondern die mangelnde Verständigung mit dem Auftraggeber über die Notwendigkeit solcher Analysen. Eine wirkungsvolle Unterstützung des PL/PM wäre aus unserer Sicht, ihn fit zu machen in Verhandlungsführung in Verbindung mit der Rollenklärung und der Konfliktklärung.

#16 Oft wird mit der Umständlichkeit oder Ineffektivität einer Methode argumentiert. Daraus ergibt sich auch die Frage, wie geübt der PL/PM in einer Methode ist, welche Varianten oder Alternativen er kennt. Wenn etwa die klassische Stakeholder-Analyse zur Diskussion steht, dann kann im agilen Umfeld alternativ ein mitlaufender Prozess des Checks von projekt- und situationsrelevanten Personen genutzt werden.

#17 Entlang des Prozesses lernen wir mit den beteiligten Personen auch



deren unterschiedliche Wirklichkeitskonstruktionen kennen, die für den Change relevant sein können. Es braucht gutes Zuhören, gegebenenfalls auch einen Perspektivenwechsel, und damit verbunden immer wieder einen Blick auf die unterschiedlichen Dimensionen einer Organisation und ihrer Veränderung.

Kurzum: Zum Change Management gehört ein steter Prozess der Zielklärung, Planung und Organisation mit zunehmendem Erkenntnisgewinn und Entscheidungsfortschritt.

In Ergänzung dazu: es geht auch noch um den „Reload" von Denkmustern, Konzepten und Modellen.

Change-Reload

Es geht uns in einem effektiven Change Management also um „das big picture", um Verstehen, um an den richtigen Stellen ansetzen zu können. Wir haben allerdings erkannt, dass es parallel darum gehen muss, die üblichen Denkmuster, Konzepte und Modelle in der Auseinandersetzung mit Organisation, mit dem Menschen und mit Veränderung ebenfalls zu überwinden – zumindest zu hinterfragen, ob sie noch zeitgemäß sind. Mit dieser Idee sind wir auf den Ansatz von Scharmer, den er in „Theory U" beschreibt (2014), gestoßen. Dabei geht es nicht nur um den Umbau von Denk-Modellen, sondern auch um die Einbeziehung unserer emotionalen Bewertungen. Wir nennen dieses Vorgehen nun in Anlehnung an ihn „Change-Reload" und verändern damit im Rahmen eines WS-Formats im Austausch unter Scheiter-Erfahrenen Denkmuster und Konzepte und damit – zumindest von der Möglichkeit her – auch das Handeln. Wir stellen

BISHERIGE ERKENNTNISSE AUS UNSEREN RELOAD-WS

von der Oberfläche zu den eigentlichen Hintergründen/Ursachen:

Vertrauen auf Gurus, Rezepte & Co	vs.	Mut und Wille zum eigenen Denken
Planungsillusion (Predict and control)	vs.	Iteration/Adaptivität (Sense & respond)
Planungsbetrug (und alle wissen es)	vs.	Mut zur Wahrheit und Konsequenz
Definitionshoheit („Agil heißt: …")	vs.	Gemeinsame Klärung („Was soll Agil für uns (nicht) bedeuten?")
Zuteilung von Information	vs.	Volle Transparenz
Verdächtige Sprüche („Der Mensch steht im Mittelpunkt")	vs.	Gemeinsames Arbeiten und Erleben
Zielbild vorgegeben und beauftragt	vs.	Gemeinsam erarbeitetes Zielbild
Anfängliche Auftragsklarheit als Zustand	vs.	Stete Auftragsklärung als Prozess
Versprechen von inhaltlichen Zielen	vs.	Versprechen von Kommunikation
Verkauf von Beratungs- und Change-Produkten	vs.	Arbeiten an Lösungen für das Kundensystem (und jedes ist anders)

Bild 2

WIR HOFFEN, DASS SIE ANREGUNGEN FÜR IHRE CHANGE-ARBEIT NUTZEN KÖNNEN, UM IHRE PROJEKTE VOR DEM SCHEITERN ZU BEWAHREN.

Dr. Klaus Wagenhals, Gründer, metisleadership, www.metisleadership.com

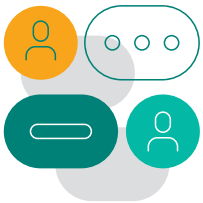
Hypothesen zum Scheitern auf und diskutieren Handlungsoptionen für die jeweiligen Projekte.

Wir haben mittlerweile mit diesem Format mehr als 15 Workshops und Abend-Veranstaltungen für verschiedene Communities und Firmen durchgeführt, immer angepasst an die Fragestellungen der Teilnehmenden. Dabei zeigten sich folgende Widersprüchlichkeiten, die man durchaus als Paradigmenwechsel bezeichnen kann.

Lessons Learned aus den Reload-Workshops

Die bisherigen Erkenntnisse geben Hinweise für Wege aus den bekannten Denk- und Handlungsmustern:

#18 **1.** Besprechen Sie mit dem Auftraggeber die Vorgehensweise für den Change. Beziehen Sie hier schon Vertreter von Betroffenen ein. Entwickeln Sie gemeinsam eine grobe Roadmap, die neben den fachlichen Themen auch die Kommunikation beschreibt: Workshops mit den Usern, World Cafés, Open Spaces, Feedback-Schleifen, Change-Forum mit allen Stakeholdern.



#19 **2.** Denken sie an die Glaubwürdigkeit der Kommunikation und die Wirkung von Botschaften. Begegnen Sie der Gerüchteküche schnell. Wiederholen Sie Informationen – auch wenn Sie ungeduldig werden. Seien Sie in den Inhalten konsistent und in Ihrer Kommunikation verlässlich.

#20 **3.** Laden Sie wichtige Player zur Mitarbeit ein. Setzen Sie Multiplikatoren ein. Achten Sie auf eine saubere Rollenklärung und die Arbeitsbelastung der Beteiligten. Diskutieren Sie die Prioritätensetzung, Umverteilung von Aufgaben, arbeitsorganisatorische Maßnahmen.

#21 **4.** Richten Sie die Schrittfolge und die Taktung auf die Bedürfnisse der Beteiligten aus. Achten Sie durchgehend auf die Orientierung des Prozesses am Zukunftsbild und auf die Transparenz des Prozesses. Entscheiden Sie schnell und nachvollziehbar.

ZUM CHANGE MANAGEMENT GEHÖRT EIN STETER PROZESS DER ZIELKLÄRUNG, PLANUNG UND ORGANISATION MIT ZUNEHMENDEM ERKENNTNISGEWINN UND ENTSCHEIDUNGSFORTSCHRITT.

Dr. Frank Kühn, Consultant, www.kuehn-cp.com

#22 **5.** Achten Sie auf Stimmungen und Energie: Zeigen sich Unzufriedenheiten, gibt es Situationen, in denen die Motivation leidet? Dann sollten Sie eingreifen. Gehen Sie auch Konflikten nicht aus dem Weg und tragen Sie sie konstruktiv aus.

#23 **6.** Führen Sie Kommunikationsformate und Foren ein, mit deren Hilfe ein offener Austausch auch zu Problemen und Fehlern willkommen ist.

#24 **7.** Führen Sie Meetings kurz und ergebnisorientiert durch, überladen Sie sie nicht. Richten sie für spezielle Themen eigene, effektive Arbeitsgruppen ein oder eine „Pilotgruppe", und lösen Sie sie wieder auf, wenn ihr Zweck erfüllt ist.

#25 **8.** Schauen Sie beim Monitoring nicht nur auf den technischen Fortschritt, sondern auch auf den Prozess, die Aufgaben, die Rollen, die Zusammenarbeit im Team, das individuelle Erleben (vgl. Retrospektiven im agilen Umfeld). Vereinbaren Sie Kriterien, auf die Sie gemeinsam achten wollen.

#26 **9.** Behalten Sie das Zielbild im Blick, wenn das neue System und die Anwendung reibungslos laufen, die neuen Prozesse und Strukturen funktionieren, die Kunden und User die neuen Möglichkeiten motiviert und qualifiziert nutzen sollen und überprüfen Sie immer wieder per Feedback-Schleifen.

Wir hoffen, dass Sie Anregungen für Ihre Change-Arbeit nutzen können, um Ihre Projekte vor dem Scheitern zu bewahren.

Dr. Klaus Wagenhals, Dr. Frank Kühn

UNSERE THEMEN

it management

Spezialthema: DSAG

Fokusthema: Digitale Transformation im Zeitalter von KI

Schwerpunktthemen: SAP-Partnerlösungen, ERP, Office 4.0, Lizenzmanagement, Projektmanagement

Die Ausgabe 07/08 2025 erscheint am 11. Juli 2025

UNSERE THEMEN

it security

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

WIR WOLLEN IHR FEEDBACK

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

INSERENTENVERZEICHNIS

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Autoren: Danijela Bagaric, Matthias Böhme, Philipp von der Brüggen, Florian Buzin, Andreas Fuchs, Kai Hambrecht, Sascha Hempe, Sarah-Lee Hofe, Chris Kramar, Dr. Frank Kühn, Martin Landis, Stefan Mesquita, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, David Schahinian, Frank Schnicke, Florian Sippel, Dr. Klaus Wagenhals, Ingo Wittrock

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

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

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

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

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

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

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

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

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

Erscheinungsweise: 6 x pro Jahr

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

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

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

SPOT AN FÜR STARKE IT-LÖSUNGEN

it spotlight

spotlight

IHR EXKLUSIVES BUSINESS-PROFIL AUF

it-daily.net

Präsentieren Sie Ihr Unternehmen, Ihre Marke und Produkte gezielt dem IT-Fachpublikum und steigern Sie Ihre Sichtbarkeit im B2B-IT-Bereich nachhaltig.

KONTAKTIEREN SIE UNS

it sa

HOME OF IT SECURITY

SAVE THE DATE

it-sa Expo&Congress

7.–9. Oktober 2025

Nürnberg, Germany

itsa365.de

NÜRNBERG MESSE

it security

Detect. Protect. Respond.
Mai/Juni 2025

THOUGHT LEADERSHIP

AB **SEITE 8**

SOPHOS

DIE NEUE ROLLE VON CYBER SECURITY

Vom IT-Projekt zur Führungsfrage

Timo Schlüter, Arvato Systems

CYBER INSURANCE ASSESSMENT

Den richtigen Bedarf ermitteln

RANSOMWARE-ATTACKE

Von der Krise zum durchdachten Neustart

LIEFERKETTEN-SICHERHEIT

Schwachstellen mit Zero Trust eliminieren

www.it-daily.net

FESTIVAL SUMMIT EXPO!

Tech Riders

KÖLN, 03-04. JULI 2025

Souverän. Sicher. Zukunftsfähig.

Europas Plattform für digitale Souveränität und IT-Strategie

3.–4. Juli 2025 | Köln

80+ Speaker SUMMIT

50+ Austeller & Partner EXPO!

500+ Teilnehmer FESTIVAL

eco Verband der Internetwirtschaft | VOICE Bundesverband der IT-Anwender e.V. | KI Bundesverband | bvmi Bundesverband IT-Mittelstand e.V. | BSKI Bundesverband für den Schutz Kritischer Infrastrukturen e. V.


Ulrich Ahle
CEO
gaia-x


Max Schrems
Chairman
noyb


Lisa Nöth
Head of Partner Alliances
CLOUDPILOTS


Dr. Christian Temath
Geschäftsführer KI.NRW
KI NRW


Harald Joos
Cloud-Beauftragter
Deutsche Rentenversicherung Bund


Prof. Dr. Dennis-Kenji Kipker
Forschungsdirektor
Cyberintelligence Institute


Dr. rer. nat Michael Förtsch
CEO – Q.ANT GmbH
Q.ANT


Knut Jessen
CIO bei der Privatbank Berenberg in Hamburg
BERENBERG


Hermann Huber
CISO @ Hubert Burda Media
Hubert Burda Media


Hans Pezold
Geschäftsführer Uniper IT GmbH
uniper


Ernst Stöckl-Pukall
Leiter des Referats „Digitalisierung & Industrie 4.0", BMWK


Prof. Wolfgang Prinz
stellv. Institutsleiter
Fraunhofer FIT


Dr. Raphael Zimmer
Referatsleiter @ BSI


Ingo Mommertz
VP Omnichanel IT – Deichmann


Ron Kneffel
Vorstandsvorsitzender CISO Alliance e.V.
CISO ALLIANCE


Andreas Weiss
Geschäftsführer eco – Verband der Internetwirtschaft
eco


Timo Wandhöfer
CISO @ Klöckner & Co
klöckner & co


Richard Clasen
Bereichsleiter für E-Business & Digitales Ökosystem
WÜRTH


Jörg Bienert
Präsident des Bundesverbandes Künstliche Intelligenz e.V.
KI BUNDESVERBAND


Dr. Philipp Rösler
Board Advisor
GCORE


Valentina Kerst
Senior Partner Managerin & Co-Autorin
AI Village


Dr. Swantje Westpfahl
Director @ Institute for Security and Safety GmbH


Dr. Daniel Stadler
Geschäftsführer EIN Quantum NRW & Leiter Technologie und Innovation NMWP
EIN Quantum NRW


Dr. Gerd Niehage
CIO & CTO – Ex Swisscom & ZF


Mathias Nöbauer
CEO von Exoscale und A1 Digital Director Cloud
EXOSCALE


Robin Hermann
Geschäftsleitung
STACKIT


Guido Massfeller
Head of Sovereignity EMEA North
Google


Prof. Dr. Dr. Frauke Rostalski
Mitglied des Deutschen Ethikrats & Lehrstuhlinhaberin an der Universität zu Köln


Guido Breunung
CEO & Pionier für AI und Avatare
aio


Rudolf Dück
CIO Universitätsklinikum Schleswig-Holstein
UKSH Informationstechnologie

Jetzt kostenloses Ticket sichern!

Code: TRDAILY25

EXPO

CLOUDPILOTS | claranet | LINK11 | WIIT THE PREMIUM CLOUD | G DATA CyberDefense | noris network | GCORE | A1 Digital | STACKIT A Brand of Schwarz Digits

ENGINSIGHT | plusserver | DEBIT | Public Cloud Group | Edgeless Systems | ninjaOne | COLOGNE INTELLIGENCE | enclaive | OVHcloud

Seedboxx | HEIMAT | BINARY BUNKER | LANCOM East | HanseSecure CHOOSE THE INTRUDER! | 3decon | privacy provided | QUADRUPED ROBOTICS | GROUNDBREAKER TALENTS

TechRiders Summit – Das Sommerfestival für IT-Entscheider

Inhalt

Vom IT-Projekt zur Führungsfrage

DIE NEUE ROLLE VON CYBER SECURITY

Wie müssen Unternehmen Cyber Security heute angehen? Im Interview spricht Timo Schlüter, Business Owner Cyber Security bei Arvato Systems, über ganzheitliche Security-Strategien und darüber, welche Rolle digitale Souveränität und Künstliche Intelligenz dabei spielen.

it security: *Herr Schlüter, bei Cyber Security handelt es sich um ein dynamisches Handlungsfeld für Unternehmen. Was sind die aktuellen Herausforderungen in diesem Bereich?*

Timo Schlüter: Zum einen hat sich die Cyberkriminalität zu einem hochindustrialisierten Geschäftsfeld entwickelt. Zum anderen steigen die regulatorischen Anforderungen unaufhörlich, was viele Unternehmen operativ einfach überfordert. Zudem haben wir es mit einer stark gewachsenen und diversifizierten IT-Landschaft zu tun – von Multi-Cloud-Umgebungen über vernetzte OT- oder IoT-Anwendungen bis hin zu erweiterten IT-Infrastrukturen aufgrund hybrider Arbeitsmodelle. Diese Landschaft ist schwer zu überwachen und zu schützen, da sich die Angriffsflächen unüberschaubar vervielfachen.

Diese Entwicklungen machen es schwierig, eigene Abhängigkeiten zu erkennen und zu managen, was die digitale Souveränität und flexible Sicherheitsarchitekturen unabdingbar macht.

it security: *Inwiefern ist digitale Souveränität entscheidend für effektive Cyber-Security-Strategien, und welche Maßnahmen können Unternehmen ergreifen, um ihre Souveränität zu wahren?*

Timo Schlüter: Digitale Souveränität bildet das Fundament für wirtschaftliche Resilienz, weil sie es Unternehmen ermöglicht, selbstbestimmte Entscheidungen in Bezug auf ihre IT-Infrastruktur und Datenhaltung zu treffen. Diese Unabhängigkeit ist eine Voraussetzung dafür, Cyberbedrohungen schnell und effektiv zu managen. Um digitale Souveränität zu wahren, sollten Unternehmen zunächst Lock-in-Effekte reduzieren, das heißt, sich nicht ausschließlich an einen Anbieter binden. Hybride Betriebsmodelle, die zum Beispiel eine Kombination aus privaten und öffentlichen Cloud-Diensten nutzen, sind besonders effektiv. Zudem ist eine starke Governance um Daten und Prozesse herum wichtig, die Unternehmen verstehen lässt, wo und wie ihre Daten gespeichert und verarbeitet werden. Konzepte wie Zero Trust, Data Sovereignty Frameworks und Confidential Computing unterstützen dabei, den Datenfluss

> WAS UNTERNEHMEN BRAUCHEN, IST PRAKTISCHE UNTERSTÜTZUNG, UM DEN VORSCHRIFTEN GERECHT ZU WERDEN UND GLEICHZEITIG IHRE SICHERHEIT EFFEKTIV ZU MANAGEN.
>
> **Timo Schlüter, Business Owner Cyber Security, Arvato Systems, www.arvato-systems.de**

innerhalb und außerhalb des Unternehmens zu kontrollieren und zu sichern.

it security: *Ist Cyber Security dann gar keine reine Technologiefrage mehr?*

Timo Schlüter: Definitiv. Eine bloße Fokussierung auf Technologie führt in der Praxis meist zu Silodenken, Insellösungen und unverbundenen Einzelmaßnahmen, die letztlich wirkungslos bleiben. Bei uns steht der Geschäftsprozess im Vordergrund, nicht die Technik. Es geht darum, dass Security businessfähig macht, und nicht nur Daten und Systeme schützt. Damit das gelingt, müssen Unternehmen Cyber Security selbst als Geschäftsprozess verstehen – mit klaren Rollen, KPIs und einem kontinuierlichen Reifegradmanagement. Nur durch eine ganzheitliche Herangehensweise, die Sicherheitsmaßnahmen als integralen Bestandteil der Unternehmensführung sieht und diese kontinuierlich an die sich ändernden Geschäftsprozesse und Bedrohungslagen anpasst, können Unternehmen wirksam und dauerhaft ihre Cyber Security verbessern.

it security: *Angesichts der schnell fortschreitenden digitalen Bedrohungen, wie können Unternehmen ihre Cyber Security-Strategien effektiv aktuell halten?*

Timo Schlüter: Cyber Security lässt sich nicht als abgeschlossenes Projekt verstehen – sie ist ein permanenter, dynamischer Prozess. Die Bedrohungslage verändert sich kontinuierlich und regulatorische Anforderungen nehmen zu. Die Sicherheitsstrategie muss daher fortlaufend überprüft, angepasst und weiterentwickelt werden. Damit das gelingt, braucht es eine ganzheitliche Perspektive. Unternehmen müssen nicht nur ihre technischen Schutzmaßnahmen aktuell halten – etwa durch zeitgemäßes Bedrohungsmonitoring, Schwachstellenmanagement oder automatisierte Reaktionsmechanismen –, sondern diese in eine organisatorisch verankerte Sicherheitsarchitektur mit klaren Verantwortlichkeiten und etablierten Prozessen einbetten. Gleichzeitig sollte Cyber Security auch ein kulturelles Thema sein: Nur wenn Mitarbeitende sensibilisiert sind und Sicherheit als Teil ihres Arbeitsalltags begreifen, kann eine Strategie im Unternehmen tatsächlich wirken. Zudem ist sie regelmäßig in der Praxis zu überprüfen – beispielsweise durch Red Teaming, Krisenübungen oder auch Planspiele zur Notfallreaktion. Wer Cyber Security als lebendigen Bestandteil der eigenen Unternehmensführung versteht, schafft nicht nur mehr Sicherheit, sondern auch die notwendige Resilienz, um in einer zunehmend unsicheren digitalen Welt handlungsfähig zu bleiben.

it security: *Mit welchen Problemen sehen sich Unternehmen demnach bei der Realisierung von Cyber Security konfrontiert?*

Timo Schlüter: Viele Unternehmen wissen oft nicht, wo sie anfangen sollen, oder verlieren sich im Überangebot an Sicherheitstools. Die Herausforderung liegt nicht nur in der Technik, sondern auch darin, Cyber Security ins Business zu übersetzen. Obendrein fällt es Unternehmen schwer, durch den Regularien-Dschungel zu navigieren. Der Mangel an Fachkräften verschärft dieses Problem zusätzlich. Was Unternehmen brauchen, ist praktische Unterstützung, um den Vorschriften gerecht zu werden und gleichzeitig ihre Sicherheit effektiv zu managen. Hier können moderne SOCs als Managed Services helfen, indem sie sowohl die Expertise als auch die kontinuierliche Überwachung abdecken.

it security: *Freund oder Feind – welche Rolle spielt Künstliche Intelligenz im Cyber-Security-Umfeld?*

Timo Schlüter: Künstliche Intelligenz ist sowohl Fluch als auch Segen. Einerseits nutzen Cyberkriminelle KI, um ihre Attacken zu automatisieren, zu personalisieren und zu skalieren. Andererseits bietet sie enorme Chancen für die Verteidigung, indem sie etwa Anomalien frühzeitig erkennt und automatisierte Reaktionen ermöglicht. Grundvoraussetzung für den effektiven Einsatz von KI in der Cyber Security ist die Schaffung einer soliden Datenbasis, etwa durch eine saubere Configuration Management Database (CMDB). Sie hilft dabei, die IT-Infrastruktur zu verstehen und schneller auf Bedrohungen zu reagieren. Doch auch das löst nicht das Problem der Explainability, also der Nachvollziehbarkeit von KI-Entscheidungen. Ohne ein Verständnis dafür, wie KI-Systeme entscheiden, ist es schwer, Vertrauen in die automatisierten Prozesse aufzubauen. Hier müssen wir sicherstellen, dass KI-Systeme transparent und frei von Verzerrungen sind. So lange bleiben Hybrid-Modelle das Mittel der Wahl, da der Mensch im Entscheidungsprozess federführend bleibt – unterstützt durch KI, die Routineaufgaben übernimmt und Vorschläge macht. Die Zukunft könnte jedoch in adaptiven SOCs liegen, in denen KI nicht nur unterstützt, sondern kontinuierlich lernt, Risiken neu bewertet und potenzielle Angriffswege simuliert. Dann wäre proaktives Handeln möglich und Unternehmen wären den Cyberkriminellen stets einen Schritt voraus.

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

IDENTITY & ACCESS MANAGEMENT

VON STATISCHEN ZU DYNAMISCHEN SICHERHEITSMODELLEN

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

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

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

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

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

ZWISCHEN WISSEN UND HANDELN

Cyberangriffe gehören mittlerweile zu den größten Geschäftsrisiken – und zwar branchenübergreifend. Vom internationalen Konzern bis zum mittelständischen Unternehmen: Kein Betrieb ist davor gefeit, Opfer von Datendiebstahl, Ransomware oder Systemausfällen zu werden.

Trotzdem wird Cybersicherheit in vielen Unternehmen noch immer als technisches Randthema behandelt – etwas, das die IT schon irgendwie regelt. Dabei ist längst klar: Wer digitale Geschäftsprozesse verantwortet, trägt auch Verantwortung für deren Sicherheit.

Deshalb müssen sich Führungskräfte fragen lassen: Wie gut sind ihre Systeme geschützt, existiert ein Krisenmanagement, wie priorisieren sie das Thema und welche Verantwortung tragen sie selbst?

Chef, wie hältst du es mit der Cybersicherheit?

UNTERNEHMEN VERSCHENKEN WETTBEWERBSVORTEILE DURCH MANGELNDE KOMMUNIKATION IHRER CYBERSICHERHEIT

Sophos hat mit seiner aktuellen Management-Studie „Chef, wie hältst du es mit der Cybersicherheit?" zum zweiten Mal beleuchtet, wie das C-Level-Management in Deutschland, Österreich und der Schweiz die Cybersicherheit bewertet – in diesem Jahr mit einem Schwerpunkt auf den Einfluss der Cybersicherheit auf Geschäftsbeziehungen.

In der Studie zeigt sich, dass die Befragten mit der bestehenden IT-Sicherheitsinfrastruktur zufrieden sind und diesem Aspekt eine hohe Relevanz beimessen. Gleichzeitig tut man sich aber schwer, hieraus Wettbewerbsvorteile abzuleiten. Und: Trotz der grundsätzlichen Zufriedenheit mit der bestehenden Cybersicherheitsinfrastruktur sind die C-Level-Managements in der DACH-Region insgesamt zurückhaltend, was eine aktive Integration dieses Aspekts in die Unternehmenskommunikation angeht. Lediglich die Schweiz zeigt hier im Vergleich zu Deutschland und Österreich etwas mehr Aktivität.

Auch bei der Frage, wo im Unternehmen C-Level-Verantwortliche künftig verstärkten Bedarf an IT-Sicherheitsmaßnahmen sehen, offenbaren sich Unterschiede in den Einschätzungen der Befragten aus den drei Ländern. In Deutschland werden etwa Zukunftstechnologien weniger oft genannt als in den beiden Nachbarländern.

Cybersicherheit kein Wettbewerbsvorteil?

Das Management bestätigt die hohe Relevanz von Cyberschutz für die Geschäftsbeziehungen – und doch wird der tatsächliche Einfluss als sehr gering bewertet.

Hinsichtlich der Frage, wie die Manager auf einer Skala von eins (sehr wichtig) bis sechs (sehr unwichtig) den Einfluss einer effizienten Cybersicherheitsinfrastruktur auf ihre geschäftlichen Beziehungen zu Kunden und Geschäftspartnern bewerten, sind sich die Befragten in allen drei Ländern überwiegend einig: In Deutschland halten 55 Prozent den Cyberschutz für sehr wichtig für die Businessbeziehungen, in Österreich sagen dies 46 Prozent und in der Schweiz betonen sogar 60 Prozent die Relevanz der implementierten Cybersicherheitsmaßnahmen. Als immerhin wichtig bewerten diesen Aspekt noch 28 Prozent der deutschen, 34 Prozent der österreichischen und 32 Prozent der Schweizer Manager:innen. Dass Cyberschutz gänzlich unwichtig sei, glaubt niemand unter den Befragten.

Bedeutung hoch, tatsächlicher Einfluss niedrig

Gleich bei der nächsten Frage zeigen sich Widersprüche in der Bewertung durch die Chefinnen und Chefs. Bezifferte die sehr deutliche Mehrheit den Einfluss eines effizienten Cyberschutzes auf Geschäftsbeziehungen als wichtig oder sehr wichtig, zeichnet der Realitätscheck ein anderes Bild. Auf die Frage, ob sich das Thema Cyberschutz tatsächlich auf der Ebene der Zusam-

menarbeit mit Kunden ausgewirkt habe, bestätigen knapp 35 Prozent der deutschen, 34 Prozent der österreichischen und 40 Prozent der Schweizer Umfrageteilnehmenden, dass sie ohne wirkungsvollen Cyberschutz in der Tat Kunden oder aber Neugeschäft verloren hätten. Die Mehrheit der Befragten – in Deutschland knapp 55 Prozent, in Österreich 58 Prozent und in der Schweiz 48 Prozent – sagt dagegen, die Cybermaßnahmen des eigenen Unternehmens seien weder in den Beziehungen zu Kunden noch in der Neukundenakquise bislang ein Thema gewesen. Lediglich in der Schweiz erweist sich dieser Aspekt somit als einigermaßen ausgeglichen.

Cyberschutz fehlt in externer Kommunikation

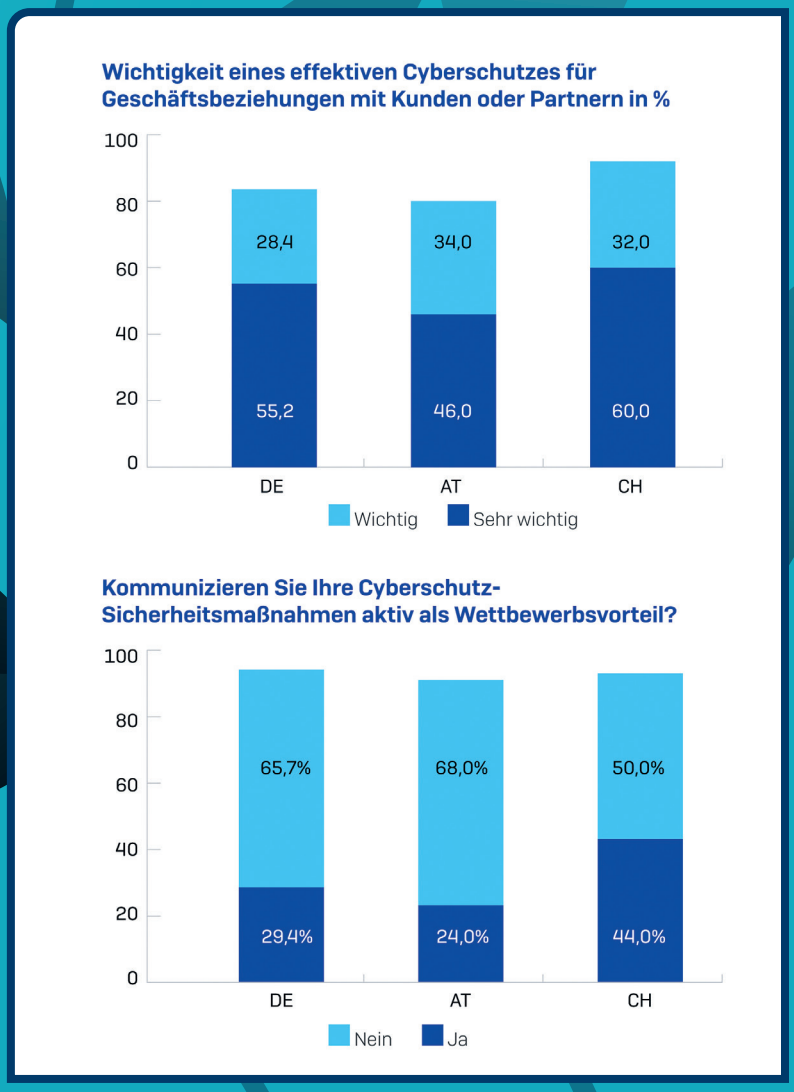
Noch deutlicher als beim Thema Auswirkungen auf Geschäftsbeziehungen zeigt sich eine Diskrepanz hinsichtlich der Kommunikation der Cybersicherheitsinfrastruktur in Richtung Kunden und Geschäftspartner. Nur 29 Prozent der deutschen sowie 24 Prozent der österreichischen Unternehmen kommunizieren ihren Cyberschutz aktiv. In der Schweiz zeigt man sich bei diesem Punkt motivierter, hier sprechen immerhin 44 Prozent über ihren guten Cyberschutz. Bei 14 Prozent findet dieser wichtige Aspekt Eingang in die Marketingkommunikation und bei 10 Prozent der befragten Schweizer Chefinnen und Chefs wird bereits bei der Akquise neuer Mitarbeitender darauf hingewiesen. In Deutschland benennen den Aspekt der Cybersicherheit immerhin noch 8,5 Prozent der Manager:innen im Rahmen der Personalgewinnung, in Österreich ist dieser Punkt mit nur 2 Prozent in dem Zusammenhang kaum von Bedeutung. Hierzulande wie auch in Österreich kommuniziert man, wenn überhaupt, die bestehende und eigentlich gut bewertete IT-Sicherheit des Unternehmens vor allem im Kontakt mit Partnern (Deutschland 14,9 Prozent, Österreich 10 Prozent) oder Kunden (Deutschland 17,4 Prozent, Österreich 12 Prozent).

Mit dem Argument, die IT-Sicherheitsinfrastruktur des Unternehmens verschaffe ihnen keinen Wettbewerbsvorteil bei Kunden oder Geschäftspartnern, binden knapp 66 Prozent der deutschen, 68 Prozent der österreichischen und 50 Prozent der Schweizer Unternehmen diesen Aspekt überhaupt nicht in ihre Kommunikation ein.

Wo sehen Unternehmensführungen in Zukunft Cybergefahren?

Netzwerke, Clouds, Smartphones, Laptops sind als Standards mittlerweile gut im Unternehmen geschützt. Sophos wollte von den Verantwortlichen jedoch auch wissen, welche Bereiche sie für den Schutz sensibler Daten zukünftig als besonders kritisch erachten. Die überwiegende Mehrheit in Deutschland (67,7 Prozent), Österreich (60 Prozent) und der Schweiz (72 Prozent) sieht diesen Bedarf beim mobilen Arbeiten und im Homeoffice. Während hinsichtlich des Spitzenreiters für künftig besonders schützenswerte unternehmensbereiche Einigkeit besteht, zeigen sich schon bei Platz zwei die ersten regionalen Unterschiede.

An zweiter Stelle der sensiblen Sektoren stehen aus Sicht der Managerinnen und Manager die KI-Technologien mit



45,8 Prozent Nennung in Deutschland und 54 Prozent in der Schweiz. Österreich hält Smart Building (intelligente Gebäudetechnik) mit 46 Prozent für wichtiger, hier schafft es KI mit 42 Prozent nur auf den dritten Platz. Das Thema Smart Building rangiert für die befragten deutschen (36,4 Prozent) und Schweizer Unternehmen (38 Prozent) nur an vierter Stelle. Für wichtiger wird in Deutschland die Sicherheit von Firmenwagen erachtet, die mit 37 Prozent der Nennungen hier auf Platz drei rangiert. In Österreich (34 Prozent) und der Schweiz (32 Prozent) landet der Firmenwagen auf Platz fünf der zukünftig vermehrt sicherheitsrelevanten Bereiche.

Unterschiedliche Einschätzung bei Automatisierungstechnologien

Automatisierungen und intelligente Vernetzungen in der Produktion – kurz Smart Factory – verdienen für die Schweizer Verantwortlichen ein höheres Sicherheitslevel. Mit 46 Prozent steht dieser Aspekt bei ihnen nach Remote-Arbeit und KI an dritter Stelle. Die Befragten aus Österreich vergeben hierfür den vierten Platz mit 40 Prozent und Deutschland stuft diesen Faktor in der Befragung noch niedriger ein, mit 35,8 Prozent auf Platz fünf.

Ladetechnologien bei Fahrzeugen werden mit den Plätzen sechs (Deutschland 28,9 Prozent) und sieben (Österreich 30 Prozent, Schweiz 24 Prozent) als eher nicht so anfällig für zukünftige Cybergefahren gesehen. Dass die eigene und IT-gestützte Energieproduktion, wie etwa Solarpaneele auf den Firmendächern, sensible Daten weitergeben könnte, können sich am ehesten die Österreicher vorstellen (32 Prozent), Deutschland sieht mit 28,4 Prozent hier etwas weniger Gefahr und die Schweiz hält das mit nur 17 Prozent für eher unrealistisch.

> UNTERNEHMEN, DIE IM CYBERSCHUTZ GUT UND STABIL AUFGESTELLT SIND, KÖNNTEN IN PUNCTO KOMMUNIKATION DURCHAUS MUTIGER WERDEN.
>
> **Michael Veit,**
> **Cybersecurity-Experte, Sophos,**
> **www.sophos.com**

Virtuelle Welten und Robotik: Unwahrscheinliche Cyberszenarien?

Gefahr durch virtuelle Welten wie Metaverse oder Avatar-Kommunikation laufen für die Deutschen mit 18,4 Prozent auf Platz acht. Für wenig wahrscheinlich halten es die Österreicher mit Platz neun und 12 Prozent. Nur die Schweiz mit 22 Prozent (Platz acht) kann hier ein gewisses Bedrohungspotenzial erkennen.

Dinge wie Google Brillen, Headup-Display-Brillen, Augmented Reality sind wiederum für die Schweizer mit Platz zehn (12 Prozent) wenig wahrscheinlich. Auch Deutschland kann hier keine große Gefahr erkennen (17,9 Prozent, Platz neun). Lediglich die Befragten in österreichischen Unternehmen können sich in diesem Bereich mit 22 Prozent (Platz acht) einen bestimmten Security-Bedarf vorstellen.

Während das Thema Robotik im Büroalltag, wie zum Beispiel Kaffee-Roboter, für deutsche Managerinnen und Manager als potenzielles Sicherheitsrisiko wenig denkbar erscheint (letzter Platz, 11,9 Prozent), hält man das in der Schweiz zu 26 Prozent für gar nicht so unrealistisch. Dazwischen liegt bei diesem Thema Österreich mit 22 Prozent und Platz acht.

Fazit

Chefetagen befassen sich mit dem Thema Cybersicherheit – wenn auch bei einigen Aspekten noch etwas zögerlich. So zeigt sich etwa, dass sich die Befragten ein hohes Maß an Bewusstsein für die wirtschaftlichen Folgen von Cybervorfällen bescheinigen. Auch scheint die Relevanz der Cybersicherheit weiter gestiegen zu sein.

In die strategische Unternehmenskommunikation mit Kunden und Partnern eingebunden ist das Thema hingegen noch bei den wenigsten Unternehmen. Unternehmen, die im Cyberschutz gut und stabil aufgestellt sind, könnten in puncto Kommunikation durchaus mutiger werden und diesen wichtigen Aspekt offensiver als einen Wettbewerbsvorteil kommunizieren und nutzen. „Gutes (Sicheres) tun und darüber reden" darf hier die ganz unbescheidene Devise sein.

Insbesondere in Deutschland zeigt sich, dass Chefinnen und Chefs nach wie vor ein wenig mit Zukunftstechnologien zu fremdeln scheinen. Dies betrifft weniger die klassischen Themen, wie beispielsweise die KI in der Cybersicherheit, sondern eher, was die künftig schützenswerten Unternehmensbereiche betrifft: Hier hat man beispielsweise Firmenwagen richtigerweise sehr im Blick.

Michael Veit

KI IN DER CYBERSECURITY: HYPE ODER ALLHEILMITTEL?

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

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

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

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

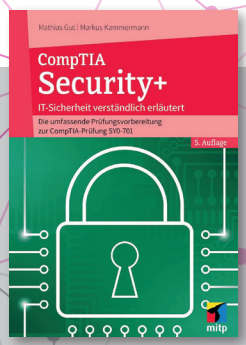
WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 14 Seiten und steht kostenlos zum Downloadbereit.

www.it-daily.net/download

COMPTIA SECURITY+

IT-SICHERHEIT VERSTÄNDLICH ERLÄUTERT



CompTIA Security+:
IT-Sicherheit verständlich erläutert; Mathias Gut, Markus Kammermann, mitp Verlags GmbH & Co.KG, 02-2025

Bedrohungen von Unternehmen durch Angriffe und Sicherheitslücken in den Systemen nehmen laufend zu. Informationssicherheit ist daher ein zentrales Thema in jeder IT-Umgebung. Unternehmen müssen sich gründlich mit der Thematik auseinandersetzen und sich kontinuierlich weiterbilden. Die Zertifizierung CompTIA Security+ ist ein wertvoller Nachweis für praxisnahe und umfassende Kenntnisse zu Themen der Unternehmenssicherheit und die Prüfung deckt die wichtigen Fragestellungen ab.

In der aktuellen Fassung der Prüfung (SYO-701) sind das:

- Generelle Sicherheitskonzepte
- Bedrohungen, Schwachstellen und Abwehrmaßnahmen
- Sicherheitsarchitektur
- Sicherer Betrieb
- Verwaltung und Überwachung von Sicherheitsprogrammen

Die Autoren behandeln umfassend die genannten Themenbereiche und vermitteln Ihnen mit diesem Buch das für die Zertifizierung notwendige Fachwissen. Im Zentrum steht dabei der Aufbau eines eigenen Verständnisses für die IT-Sicherheit. So erhalten Sie die notwendigen Grundlagen, um die Prüfung CompTIA Security+ erfolgreich zu bestehen.

KI revolutioniert das Risiko- und Compliance-Management

NEUE TOOLS FÜR KOMPLEXE AUFGABEN – DYNAMISCH, GRANULAR, IN ECHTZEIT

Heutzutage überfordert die Komplexität sowohl der IT-Infrastruktur selbst als auch die der Angriffe durch Cyberkriminelle die Verantwortlichen. Dazu kommen weitere Anforderungen, wie etwa digitale Prozesse abzusichern, Compliance-Standards einzuhalten und gleichzeitig das Geschäftswachstum zu fördern. Ohne eine KI-basierte Plattform, die dynamische, individuelle und unternehmensspezifische Sicherheitsrichtlinien durchzusetzen hilft, können IT-Security-Verantwortliche nicht den nötigen Beitrag leisten.

CISOs sowie Compliance-Manager kämpfen oft um ausreichende Transparenz über das Risikoniveau im Unternehmen. Häufig fehlt es dafür aber an leistungsfähigen und einheitlichen IT-Sicherheitsplattformen. Mangelhaft integrierte Tools und isolierte Nischenlösungen führen zu falschen Interpretationen von Daten, Fehlkonfigurationen und unnötigen Investitionen. In einer Unternehmensorganisation betreiben zudem verschiedene Akteure IT-Security-, Compliance- und Risiko-Management parallel – mit sich zum Teil überschneidenden Anforderungen oder sogar redundanten Prozessen. So arbeiten oft die ohnehin immer seltener werdenden Fachkräfte unnötig gleichzeitig an denselben Themen.

Angesichts dieser Realität benötigen CISOs eine Cyber-Security-Umgebung, die ohne neue Komplexität leistungsstarke Funktionalitäten bietet:

- eine einheitliche, dynamische und in Echtzeit aktualisierte Übersicht über den aktuellen Risiko- und Compliance-Status;
- Sicherheitsmechanismen, die Risiken und mögliche, auch zukünftige Gefahren automatisch und dynamisch erkennen sowie Richtlinien oder eine System-Härtung automatisch durchsetzen - noch bevor ein Angriff eine Schwachstelle erfolgreich ausnutzen kann; sowie
- Compliance-Mechanismen, die nicht nur Audit-konforme Berichte für alle wichtigen Standards bereitstellen, sondern auch helfen, fehlende Compliance effizient zu bereinigen.

Die Grundlage dafür liefert künstliche Intelligenz, die direkt umsetzbare Hinweise gibt, um potenzielle Gefahren zu erkennen und Sicherheitsrichtlinien dynamisch und automatisiert zu integrieren.

Regeln nach Sicherheitsbedürfnis und Tätigkeitsprofilen

Zentral und grundlegend neu ist nicht nur das proaktive und automatisierte Härten individueller Systeme, sondern auch die Korrelation mit dem Verhalten verschiedener Nutzertypen. Ein IT-Administrationstools zu nutzen, ist bei einem HR-Manager eine verdächtige Anomalie, bei einem IT-Systemadministrator Normalität. KI schafft die Möglichkeit, Aktivitäten abhängig vom individuellen Nutzer-Profil zu bewerten und passende Regeln granular dynamisch und in Echtzeit zu definieren und zu aktivieren.

Die Bitdefender Gravity Zone mit ihrer Proactive Hardening and Attack Surface Reduction (PHASR)-Technologie leistet dies und automatisiert weite Teile des Sicherheits-, Risiko- und Compliance-Managements.

PHASR ist Teil der GravityZone-Plattform von Bitdefender für Risiko- und Compliance-Management, die zudem eine der größten verfügbaren Threat-Intelligence-Datenbanken weltweit verwendet. Überdies fließen die Expertise und Erkenntnisse von IT-Sicherheitsexperten aus ihrem permanenten globalen und aktiven Einsatz gegen die Cyberkriminalität mit in die Produkte und Services ein. So werden die Sicherheit sowie das Risiko- und Compliance-Management eines Unternehmens, unabhängig von Größe und Branche, auf ein bisher unvorstellbares Niveau gehoben. Darüber hinaus kann dem immer bedrohlicher werdenden Wissens- und Fachkräftemangel dank KI erfolgreich begegnet werden. Eine optimale Ergänzung stellt die Kombination dieser Technologie mit Managed Security (MDR)-, Advisory- oder Offensive-Services dar.

www.bitdefender.com/phasr

Bitdefender

Cyber Insurance Assessment

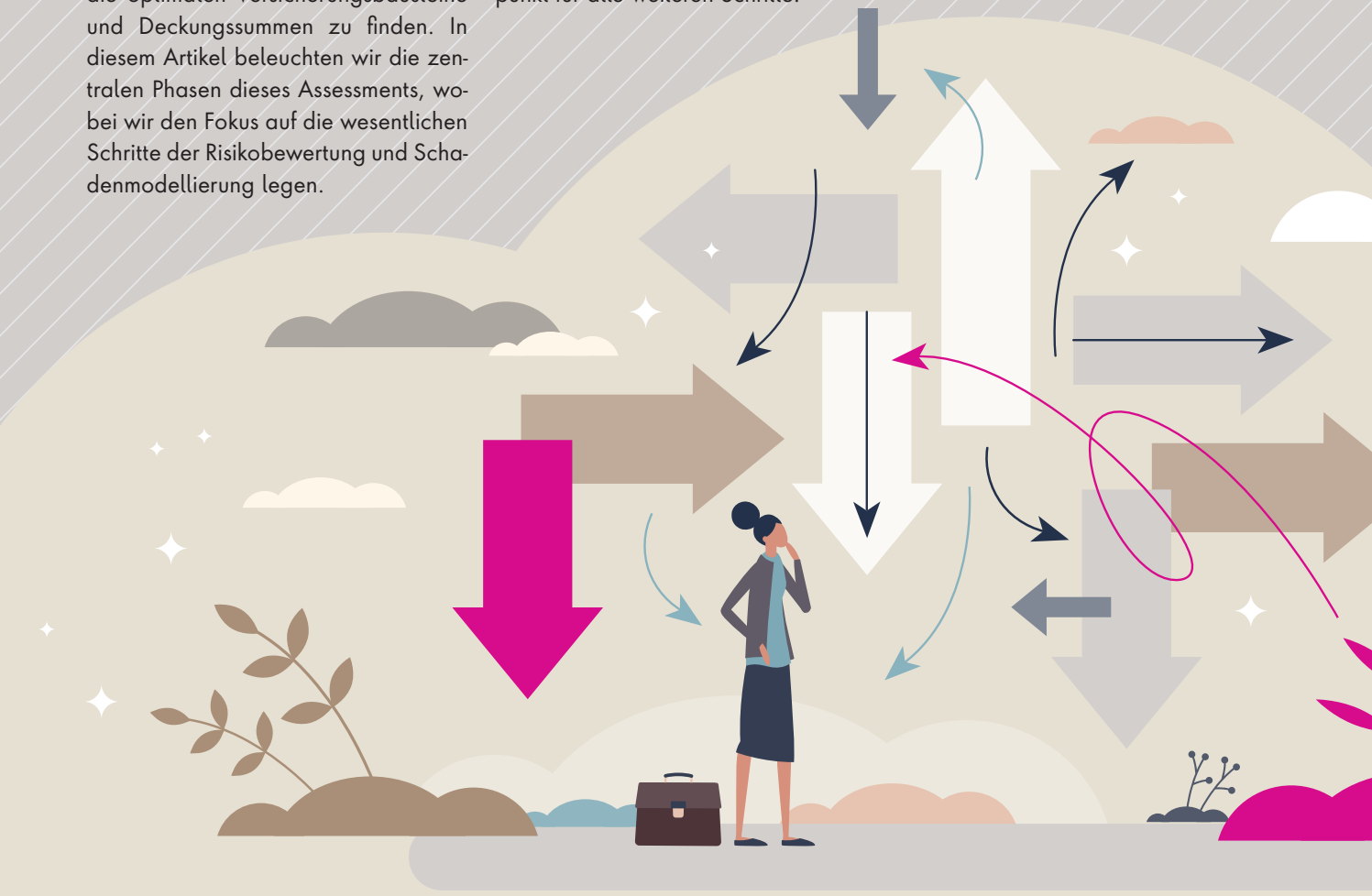
WIE UNTERNEHMEN DEN RICHTIGEN VERSICHERUNGSSCHUTZBEDARF ERMITTELN

Die Digitalisierung bietet Unternehmen immense Möglichkeiten, birgt jedoch auch zahlreiche Risiken. Cyberangriffe gehören mittlerweile zu den größten Bedrohungen für Organisationen jeder Größe. Um sich gegen die potenziellen Schäden abzusichern, setzen immer mehr Unternehmen auf Cyber-Versicherungen. Doch viele tun sich schwer, den richtigen Versicherungsschutz zu bestimmen. Hier hilft ein Cyber-Insurance-Assessment – ein strukturierter Prozess, der dabei unterstützt, die optimalen Versicherungsbausteine und Deckungssummen zu finden. In diesem Artikel beleuchten wir die zentralen Phasen dieses Assessments, wobei wir den Fokus auf die wesentlichen Schritte der Risikobewertung und Schadenmodellierung legen.

PHASE 1: Das Geschäftsmodell verstehen und Cyber-Risiken ableiten

Der erste Schritt eines Cyber-Insurance-Assessments ist immer die Analyse des Geschäftsmodells. Denn die Risiken, denen ein Unternehmen ausgesetzt ist, hängen maßgeblich von seiner Branche, den Geschäftsprozessen und den eingesetzten IT-Systemen ab. Diese Phase bildet die Grundlage für die Risikobewertung und ist der Ausgangspunkt für alle weiteren Schritte.

In dieser Phase wird durch ein interdisziplinäres Team aus IT-Experten, Fachleuten aus den Bereichen Finanzen, Recht und den operativen Einheiten des Unternehmens ermittelt, welche Prozesse, Systeme und Daten am anfälligsten für Cyber-Angriffe sind. Besonders kritisch sind hierbei Geschäftsprozesse wie Zahlungsabwicklungen, Produktionssteuerungen oder der Vertrieb. Aber auch die IT-Sicherheit von Lieferanten und externen Partnern



muss berücksichtigt werden, da Cyber-Risiken nicht nur innerhalb des Unternehmens auftreten können, sondern entlang der gesamten Lieferkette verbreitet werden.

Ziel dieser Phase ist es, ein erstes Risikoprofil des Unternehmens zu erstellen und daraus konkrete Cyber-Szenarien zu entwickeln, die als Grundlage für die folgenden Phasen dienen.

PHASE 2: Reifegrad der IT-Sicherheit und Eintrittswahrscheinlichkeit bewerten

Nachdem die potenziellen Cyber-Risiken identifiziert und analysiert wurden, steht in Phase 2 die Bewertung des aktuellen IT-Sicherheitsniveaus im Mittelpunkt. Hier geht es darum, Schwachstellen in der Sicherheitsarchitektur zu identifizieren und die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs abzuschätzen.

WER SEINE CYBER-RISIKEN NICHT QUANTIFIZIERT, TAPPT IM DUNKELN – NUR EINE BELASTBARE RISIKOBEWERTUNG SCHAFFT DIE GRUNDLAGE, UM DEN VERSICHERUNGSSCHUTZ PASSGENAU AUSZURICHTEN.

Dr. Alexander Dotterweich, Partner Actuarial Risk Modelling Service, PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, www.pwc.de

Bestandsaufnahme der Sicherheitsarchitektur

Der erste Schritt dieser Phase ist die Bestandsaufnahme aller Sicherheitsmaßnahmen, die im Unternehmen derzeit im Einsatz sind. Dies umfasst sowohl technische (Firewalls, Virenschutz, Intrusion Detection Systeme), organisatorische (Richtlinien für Passwörter, Backup-Strategien, Awareness-Programme für Mitarbeiter) als auch physische Sicherheitsvorkehrungen (Zutrittskontrollen zu Serverräumen). Eine gründliche Überprüfung dieser Maßnahmen ist notwendig, um festzustellen, welche Sicherheitslücken existieren und wie diese behoben werden können.

Reifegradbewertung

Im nächsten Schritt erfolgt eine detaillierte Bewertung des Reifegrads der implementierten Sicherheitsmaßnahmen. Unternehmen mit einem höheren Reifegrad weisen eine robustere Sicherheitsinfrastruktur auf und sind in der Regel besser vor Cyberangriffen geschützt. Ein spezieller Fokus liegt hierbei auf der IT-Governance und der Regelkonformität, also der Einhaltung von Standards und Best Practices. Hier kommen auch speziell für kleine und mittlere Unternehmen entwickelte Reifegradkataloge zum Einsatz, die eine schnelle, aber fundierte Einschätzung des Sicherheitsniveaus ermöglichen.

Eintrittswahrscheinlichkeit: Ein mathematisches Modell

Die Eintrittswahrscheinlichkeit eines Cyberangriffs wird schließlich durch ein mathematisches Modell ermittelt, das sowohl die Anzahl potenzieller Angriffsschritte als auch den Sicherheitsreifegrad des Unternehmens berücksichtigt. Je niedriger der Reifegrad der IT-Sicherheit und je größer die Zahl möglicher Angriffspfade, desto höher fällt die Wahrscheinlichkeit eines Angriffs aus. Das Modell hilft dabei, eine fundierte Schätzung der Eintrittswahrscheinlichkeit zu erstellen, indem es die analysierten Daten mathematisch verknüpft.

PHASE 3: Quantifizierung der potenziellen Schäden

In dieser Phase geht es darum, die finanziellen Auswirkungen eines Cyberangriffs genau zu quantifizieren. Nur durch eine detaillierte Einschätzung der potenziellen Schäden können Unternehmen feststellen, wie viel Versicherungsschutz sie benötigen.

Szenario-basierte Schadenanalyse

Der erste Schritt in Phase 3 ist die Szenario-basierte Analyse. Hierbei werden verschiedene Cyber-Angriffsszenarien simuliert, um die direkten und indirekten Kosten eines Angriffs zu ermitteln. Typische Szenarien umfassen beispielswei-

se Ransomware-Angriffe, bei denen Produktionsdaten verschlüsselt und Betriebsabläufe unterbrochen werden, oder Phishing-Angriffe, bei denen sensible Kundendaten gestohlen werden.

Für jedes Szenario werden sowohl die direkten Kosten (wie etwa Kosten für die Wiederherstellung von Daten, Lösegeldzahlungen oder forensische Untersuchungen) als auch die indirekten Kosten (Umsatzverluste, Bußgelder oder Reputationsschäden) ermittelt. Hierbei fließen auch branchenspezifische Erfahrungswerte ein, um insbesondere schwer messbare Schäden wie den Verlust von Kundenvertrauen zu berücksichtigen.

Modellierung der Schadenhöhe

Nach der Analyse der Szenarien werden die möglichen Schadenhöhen mithilfe probabilistischer Modelle wie der Monte-Carlo-Simulation berechnet. Dabei werden Tausende von potenziellen Schadensszenarien durchgespielt, um eine Wahrscheinlichkeitsverteilung zu erstellen, die sowohl häufige kleine Schäden als auch seltene, aber sehr teure Vorfälle umfasst. Die Expected Loss (durchschnittlicher Schaden) sowie die Schäden bei Extremereignissen (etwa bei einem 99%-Quantil) werden dabei ermittelt.

Validierung und Verfeinerung der Schadensberechnungen

Die ersten Berechnungen werden von einem Expertenteam überprüft, um sicherzustellen, dass die ermittelten Schadenhöhen realistisch sind. Insbesondere schwer quantifizierbare Schäden, wie etwa die langfristigen Auswirkungen auf den Ruf eines Unternehmens, werden mithilfe von Erfahrungswerten aus der Praxis ergänzt. Dies ermöglicht eine präzise und realistische Einschätzung der finanziellen Risiken.

ANGREIFER NUTZEN DAS SCHWÄCHSTE GLIED IN DER IT-ARCHITEKTUR AUS. CYBER-ASSESSMENTS NUTZEN SOWOHL BEI DER QUALIFIZIERUNG DER RISIKEN ALS AUCH BEI DER VERBESSERUNG DER REIFE.

Dr. Silvia Knittl, Director, Cyber Security & Privacy, PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, www.pwc.de

PHASE 4: Modellierung der Schadenverteilung

Nachdem die potenziellen Schäden quantifiziert wurden, geht es in Phase 4 um die Modellierung einer Wahrscheinlichkeitsverteilung für die Schäden. Dies ermöglicht eine differenzierte Risikobetrachtung und stellt sicher, dass nicht nur häufige, kleinere Schäden, sondern auch seltene, aber existenzbedrohende Ereignisse abgebildet werden.

Trennung von Häufigkeit und Schwere

Die Schadenverteilung wird in zwei Komponenten unterteilt: Schadenhäufigkeit (wie oft tritt ein Angriff auf?) und Schadenschwere (wie hoch sind die Schäden im Falle eines Angriffs?). Diese Trennung ermöglicht es, die Risikobewertung noch präziser und differenzierter vorzunehmen.

Wahrscheinlichkeitsverteilung und Monte-Carlo-Simulation

Durch die Monte-Carlo-Simulation werden Tausende von potenziellen Schadensverläufen berechnet, um eine realistische Wahrscheinlichkeitsverteilung zu erstellen. Diese gibt Auskunft darüber, wie hoch der zu erwartende Durchschnittsschaden ist und wie sich die Extremereignisse entwickeln könnten. Dabei wird auch berücksichtigt, welche Szenarien den größten Einfluss auf das Gesamtrisiko haben.

Berücksichtigung von Abhängigkeiten

Cyber-Angriffe treten oft nicht isoliert auf. Ein Angriff auf ein System kann in der Regel auch Auswirkungen auf andere Systeme haben, weshalb in der Modellierung die Abhängigkeiten zwischen verschiedenen Schadenarten berücksichtigt werden. Diese Abhängigkeiten werden mithilfe von Copula-Modellen abgebildet, die eine präzise Darstellung der Korrelationen zwischen verschiedenen Schadenarten ermöglichen. Beispielsweise könnte ein Angriff auf die interne IT eines Unternehmens auch Auswirkungen auf die Cloud-Services oder Lieferketten haben.

Nutzen für Versicherungsentscheidungen

Die resultierende Verlustverteilung ist entscheidend für die spätere Versicherungsentscheidung. Sie dient als Grundlage, um zu bestimmen, welche Deckungssumme benötigt wird und welcher Selbstbehalt sinnvoll ist. Darüber hinaus hilft sie dabei, den Fokus entweder auf den Risikotransfer (Versicherung) oder auf präventive Maßnahmen zu legen.

PHASE 5: Handlungsempfehlungen und Implementierung

Nach der detaillierten Analyse in den vorangegangenen Phasen folgt in Phase 5 die Ableitung von Handlungsemp-

fehlungen. Ziel ist es, die gewonnenen Erkenntnisse in konkrete Maßnahmen zu übersetzen, die sowohl das Risikomanagement als auch die Versicherungsstrategie betreffen.

Auswahl der passenden Versicherungskomponenten

Die in den Phasen 2 bis 4 ermittelten Risiken und potenziellen Schäden helfen dabei, die passenden Deckungsbausteine für die Cyber-Versicherung auszuwählen. Dies umfasst die Festlegung der Deckungssumme, der Selbstbehalte und der spezifischen Versicherungspolicen, die auf die individuellen Risiken des Unternehmens zugeschnitten sind. Auch die Haftungsbedingungen werden in diesem Schritt geprüft, um sicherzustellen, dass die Versicherung im Ernstfall umfassenden Schutz bietet.

Gap-Analyse und Verbesserung der Sicherheitsmaßnahmen

Sollte sich herausstellen, dass der Abschluss einer umfassenden Cyber-Versicherung aktuell nicht die beste Lösung darstellt, etwa weil die Prämien zu hoch sind oder keine geeigneten Deckungsbausteine verfügbar sind, empfiehlt sich eine Gap-Analyse. Diese Identifikation von Sicherheitslücken im Unternehmen kann als Grundlage für Verbesserungsmaßnahmen dienen, die im Zuge eines kontinuierlichen Sicherheitsprogramms umgesetzt werden.

Alternative Absicherungsmodelle

In einigen Fällen kann es sinnvoll sein, auf alternative Absicherungsmodelle wie Captives zurückzugreifen – eine Form der Selbstversicherung, bei der ein Unternehmen eigene Rücklagen bildet, um potenzielle Schäden aus Cyber-Angriffen selbst abzudecken. Dieser Ansatz wird besonders für große Unternehmen interessant, die eine hohe Risikofähigkeit besitzen und ihre Versicherungsprämien optimieren möchten.

Fazit

Das Cyber-Insurance-Assessment stellt für Unternehmen eine wichtige Grundlage dar, um ihre Cyber-Risiken zu verstehen und den richtigen Versicherungsschutz zu wählen. Durch die präzise Identifikation von Risiken, die Bewertung der IT-Sicherheit, die Quantifizierung potenzieller Schäden und die Modellierung von Schadenverteilungen erhalten Unternehmen nicht nur ein detailliertes Bild ihrer Bedrohungslage, sondern auch eine fundierte Entscheidungsgrundlage für die Auswahl der passenden Versicherungspolicen.

Dr. Silvia Knittl,
Dr. Alexander Dotterweich

„Hack now, decrypt later“

CYBERSICHERHEIT IM POST-QUANTUM-ZEITALTER

Was bislang wie Science-Fiction klang, rückt rasant näher: Quantencomputer stehen kurz davor, unser Verständnis von Rechenleistung grundlegend zu verändern – und mit ihm die Cybersicherheit. Denn obwohl aktuelle Verschlüsselungen wie AES-256 oder RSA-2048 noch als sicher gelten, könnten sie schon bald von Quantenrechnern mühelos geknackt werden.Damit geraten bestehende IT-Sicherheitsarchitekturen unter massiven Druck.

Superposition trifft auf Sicherheitslücke

Anders als klassische Rechner, die nur zwischen 0 und 1 unterscheiden, arbeiten Quantencomputer mit sogenannten Qubits – sie können beide Zustände gleichzeitig annehmen. Diese „Superposition“ ermöglicht eine exponentielle Steigerung der Rechenleistung. Das Problem: Was heute undenkbar ist, etwa das Knacken komplex verschlüsselter Datenbanken in Echtzeit, wird durch Quantencomputing realistisch.

Laut Studien liegt die Wahrscheinlichkeit, dass gängige Verschlüsselungsverfahren innerhalb der nächsten fünf Jahre gebrochen werden können, bereits bei bis zu 9 Prozent. In zehn Jahren steigt dieses Risiko auf bis zu 33 Prozent.

Diese Entwicklung ist besonders für sicherheitskritische Branchen alarmierend. Im Bankensektor werden Cyberkriminelle immer Interesse an Daten über Bedingungen und Beträge bestimmter strategischer Transaktionen haben. Im Verteidigungssektor sind Details über U-Boote jahrzehntelang gültig. Aber auch im Energiesektor, der Automobilindustrie oder dem Gesundheitswesen ist der Schutz langfristig relevanter Informationen essenziell.

Ein besonders perfides Szenario: die „Store-now-decrypt-later“-Strategie. Dabei sammeln Angreifer bereits heute verschlüsselte Daten, in der Hoffnung, sie in einigen Jahren mit Quantenpower entschlüsseln zu können.

Das Post-Quantum-Zeitalter

Der französische IT-Security-Spezialist Stormshield reagiert schon jetzt auf die kommende Quanten-Ära. Erste Post-Quantum-Kryptografie-Verfahren befinden sich im Proof-of-Concept-Stadium – empfohlen unter anderem von der französischen Sicherheitsbehörde ANSSI.

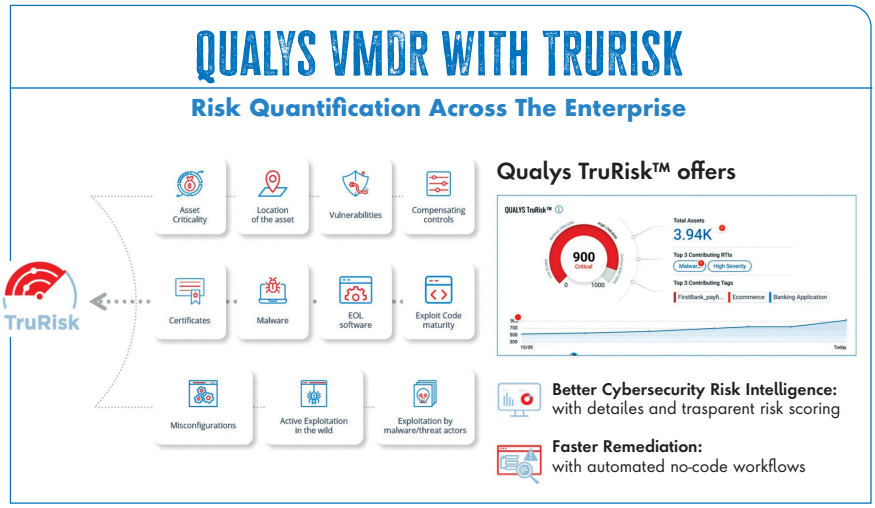
Der Schlüssel: ein hybrider Ansatz. Die bestehende Verschlüsselung (etwa AES oder RSA) bleibt bestehen, wird jedoch ergänzt durch quantensichere Algorithmen wie Crystals-Kyber oder FrodoKEM. Dank des flexiblen IKEv2-Protokolls wird zusätzlich ein sicherer Schlüsselaustausch gewährleistet – selbst für künftige Quantenangriffe.

Gesetzliche Rahmenbedingungen

Auch gesetzliche Rahmenbedingungen erfordern langfristig sichere Datenhaltung – etwa im Gesundheitswesen. Das Gesetz sieht vor, dass eine deutsche Gesundheitseinrichtung (öffentlich oder privat) Ihre Krankenakte mindestens zehn Jahre lang aufbewahren muss. Auf sichere Weise natürlich.

Solange Post-Quantum-Kryptografie-Verfahren nicht vollständig ausgereift sind, empfehlen Behörden wie das BSI oder die ANSSI den hybriden Übergang. Stormshield liefert hierfür eine Lösung, die heutige Sicherheitsstandards mit zukunftsfähiger Kryptografie kombiniert – und damit dem Quantenzeitalter mutig entgegenblickt.

www.stormshield.com/de



Priorisierung als Schlüssel zum Schutz

EFFEKTIVES RISIKOMANAGEMENT IN DER CYBERSICHERHEIT

Die Bedrohungslage in der Cybersicherheit eskaliert. Anfang 2025 verzeichnete die US National Vulnerability Database über 280.000 Schwachstellen, davon 33 Prozent mit hoher bis kritischer Einstufung. 2023 wurden fast 29.000 neue Schwachstellen dokumentiert – ein Anstieg von 3.700 gegenüber dem Vorjahr. Dieser Trend setzt sich fort und zwingt Unternehmen, ihre Sicherheitsstrategie zu überdenken.

Warum eine falsche Priorisierung schadet

Viele Unternehmen behandeln alle Schwachstellen gleich, doch dies führt zu ineffizientem Ressourcenverbrauch und Sicherheitslücken. Ein Finanzunternehmen, das diesen Fehler machte, erlitt unnötige Ausfallzeiten, da geschäftskritische und unwichtige Systeme mit der gleichen Dringlichkeit behandelt wurden. Anstatt Risiken gezielt zu minimieren, waren die IT-Teams überfordert und die wichtigsten Systeme blieben ungeschützt.

Risikomanagement bedeutet nicht, möglichst viele Schwachstellen zu beheben, sondern die richtigen. Ohne eine klare Priorisierung werden nur Symptome behandelt, aber nicht die Ursachen der Bedrohungen.

Schlüsselstrategien für ein wirksames Sicherheitsmanagement

Unternehmen müssen sich auf zwei zentrale Fragen konzentrieren:

#1 Wie hoch ist die Risikotoleranz des Unternehmens?

#2 Welche Systeme sind am kritischsten und welche Folgen hätte eine Kompromittierung?

Eine gemeinsame Sprache für Risiken erleichtert die Priorisierung, verbessert die Kommunikation zwischen technischen Teams und Führungskräften und steigert die Effizienz.

Strukturiertes Vorgehen statt Chaos

In der Automobilproduktion herrschte früher Unordnung und Ineffizienz, bis das Fließband eingeführt wurde. Dieses strukturierte System reduzierte die Produktionszeit und Kosten erheblich. Ein ähnlicher Ansatz ist in der Cybersicherheit erforderlich: Statt reaktiver Ad-hoc-Maßnahmen braucht es wiederholbare, strategische Prozesse zur Risikominimierung.

Risikobasierte Sicherheit umsetzen

Unternehmen sollten nicht nur Schwachstellen beheben, sondern gezielt die wichtigsten Unternehmenswerte schützen. Eine bewährte Methode zur Priorisierung ist die Formel:

➜ Risiko = Wahrscheinlichkeit x Auswirkung

Diese Gleichung hilft, die drängendsten Bedrohungen zu identifizieren und Sicherheitsmaßnahmen gezielt auszurichten.

Die Vorteile einer gemeinsamen Risikostrategie

- **Gezielte Ressourcennutzung:** Kritische Bedrohungen werden priorisiert.
- **Effiziente Prozesse:** Sicherheitsteams arbeiten fokussierter und vermeiden Überlastung.
- **Bessere Zusammenarbeit:** Einheitliche Bewertungsmaßstäbe stärken die Abstimmung zwischen IT und Management.
- **Höhere Widerstandsfähigkeit:** Unternehmen sind proaktiv statt reaktiv.

Fazit: Cybersicherheit als Unternehmenspriorität

Unternehmen müssen ihre Sicherheitsstrategie an den Geschäftszielen ausrichten, um Bedrohungen effektiv zu begegnen. Eine risikobasierte Priorisierung ist der Schlüssel, um Ressourcen sinnvoll einzusetzen, kritische Systeme zu schützen und langfristig widerstandsfähig zu bleiben. Nur mit einer durchdachten Strategie kann Cybersicherheit on einer Herausforderung zur Stärke werden.

Qualys.

Anthony Williams, www.qualys.com

Sicherheitsrisiko Lieferketten

WO LIEGEN DIE SCHWACHSTELLEN?

Die IT-Security beim Zugriff von Externen liegt im Argen. Viele Firmen wurden bereits geschädigt. Wo die Schwachstellen liegen, zeigt eine aktuelle Studie.

In Unternehmen, in denen sonst das interne rollen- und regelbasierte Access-Management zur Königsdisziplin zählt, ist die Verwaltung externer Zugriffe eher lasch. Das ergab eine internationale Befragung vom Ponemon Institut mit Imprivata. In Deutschland beteiligten sich rund 570 Unternehmen und Organisationen. Mehr als die Hälfte gab an, bereits Opfer eines Datenlecks oder einer Cyberattacke gewesen zu sein, die aus der eigenen Lieferkette kam. Was sind die Ursachen?

In komplexen Lieferketten greifen viele externe Dritte und Applikationen tag-

DIE AUFGABE FÜR DIE IT-SICHERHEIT BESTEHT DARIN, SICHERZUSTELLEN, DASS MASSNAHMEN UND TOOLS STRATEGISCH UND KONSEQUENT ANGEWANDT WERDEN – FÜR ALLE PRIVILEGIERTEN ZUGRIFFSANFORDERUNGEN.

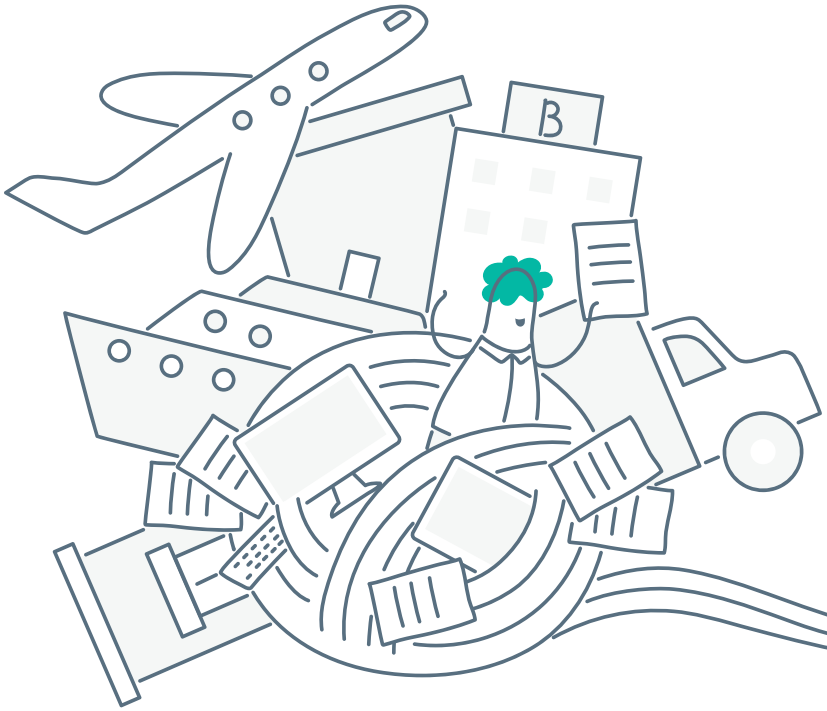
Dirk Wahlefeld, Manager Unimate Tech Services, Imprivata GmbH, www.imprivata.com

täglich mehr oder weniger kontrolliert auf die IT-Ressourcen eines Unternehmens zu. Das Problem für Verantwortliche der IT-Sicherheit beginnt damit, dass sie die Richtlinien für digitale Identitäten, mit denen der Zugriff auf Unternehmens-IT ansonsten geregelt wird, bei Externen disziplinarisch nicht durchsetzen können. Hilfreich wäre eine einheitliche Strategie für die Verwaltung von Zugängen und Berechtigungen für Externe. Doch 58 Prozent der Befragten gaben an, keine derartige Konzeption zu haben.

Ursache weitreichende Zugriffsrechte

51 Prozent der Befragten gaben an, dass ihr Unternehmen in den letzten zwölf Monaten von einer Datenverletzung oder einem Cyberangriff betroffen war, der im Zusammenhang mit der Lieferkette stand. Die Ursache dafür sahen 34 Prozent darin, dass Externen zu weitreichende Zugriffsrechte eingeräumt waren.

Besorgniserregend ist die Tatsache, dass sich 26 Prozent der deutschen Befragten, die von einer Datenschutzverletzung betroffen waren, nicht sicher sind, ob die Ursache für den Security-Vorfall in den Zugriffsrechten Dritter liegt. Diese Gruppe hat demzufolge keine Kenntnis von der Anzahl der externen Anwender und Systeme, die auf ihr Netzwerk zugreifen und mit welchen Berechtigungen sie dies tun.



Dokumentation über Dritte und Zugriffsrechte fehlt

Die gute Nachricht: Immerhin 56 Prozent der Befragten verfügen über eine umfassende Dokumentation aller dritten Parteien mit Zugriff auf das Netzwerk. Diejenigen, die keine Dokumentation haben, nannten zwei Gründe am häufigsten: fehlende Ressourcen für die Überwachung von Dritten (45 Prozent) und keine zentrale Kontrolle über die Beziehungen zu ihnen (37 Prozent). Es fehlt also an einer Transparenz darüber, wer Zugriff hat und was Externe mit ihrem Zugang tun. So ist keine Diagnose möglich, wer für den Schadensfall verantwortlich ist.

Sicherheitsrisiko mit Konsequenzen

Cyberattacken, an denen Dritte aus der Lieferkette beteiligt waren, hatten laut Ponemon-Studie meistens schwerwiegende Folgen. Zu den häufigsten zählten der Verlust oder Diebstahl sensibler und vertraulicher Daten (55 Prozent), Geldstrafen (47 Prozent) und belastete Geschäftsbeziehungen zu den Externen (45 Prozent).

Bei allen operativen Defiziten ist den Verantwortlichen mehrheitlich aber klar, dass sich die Lage verschärfen wird. 68 Prozent der Befragten erwarten, dass die Zahl der Sicherheitsverletzungen durch Dritte in den nächsten zwölf bis 14 Monaten zunehmen oder gleichbleiben wird. Und: 47 Prozent der Befragten bewerten die Zugriffsmöglichkeiten Dritter als die größte Angriffsfläche ihrer IT. Ist das Problem also erkannt?

Sicherheit der Lieferkette wird Priorität

Nur zum Teil: 47 Prozent der Befragten gaben an, dass ihr Unternehmen die Sicherheit des Zugriffs von Externen zur Priorität erklärt haben. Die beiden wichtigsten operativen Maßnahmen sind die Verwaltung der Zugänge (Konten und Berechtigungen) sowie die Überwachung der Aktivitäten externer Anwender und Systeme.

Tatsächlich bejahten sogar 77 Prozent der Befragten, dass ihr Unternehmen über eine Vendor-Privileged-Access-Management-Lösung verfügt. Mit einer VPAM-Lösung lässt sich regeln, wie der Zugriff eines Externen erfolgen darf und welche Rechte er im Netzwerk hat. Allerdings sind nur 52 Prozent dieser Gruppe davon überzeugt, dass ihre VPAM-Lösung den Missbrauch von privi-

WELCHER TEIL IHRES UNTERNEHMENS IST AM MEISTEN FÜR DIE VERWALTUNG UND GEWÄHRUNG DES ZUGANGS ZU DRITTEN UND ANBIETERN ZUSTÄNDIG?

legierten Zugängen Externer wirksam verhindert.

Hoher Aufwand und Komplexität

Die Ursachen, dass trotz VPAM-Lösungen und gutem Willen in Unternehmen die Zugriffe durch Externe nicht ausreichend verwaltet und überwacht werden, liegen darin, dass sich IT-Abteilungen damit überfordert fühlen und die Ressourcen zusätzlich belastet werden. Das gaben 38 Prozent der Befragten an. Die größten Hindernisse sehen sie in der fehlenden Kontrolle oder Steuerung (47 Prozent), der Komplexität der Compliance- und gesetzlichen Anforderungen (59 Prozent) und den unzureichenden Ressourcen oder Budgets (27 Prozent).

Keine Vorab-Prüfung

Fast zwei Drittel der Befragten, 62 Prozent, gaben an, dass ihr Unternehmen die Sicherheits- und Datenschutzpraktiken Dritter nicht bewertet, bevor sie diese in eine Geschäftsbeziehung einbinden, die den Zugriff auf sensible oder vertrauliche Daten ermöglicht.

Anders ist das bei Mitarbeitenden: 62 Prozent der Befragten sagten, dass sie interne Mitarbeitende vor der Vergabe von Zugriffsrechten gründlich überprüfen. Unternehmen scheinen strengere Regeln für die Bewertung interner Benutzer anzuwenden als für Externe.

Mit Zero-Trust Sicherheitslücken schließen

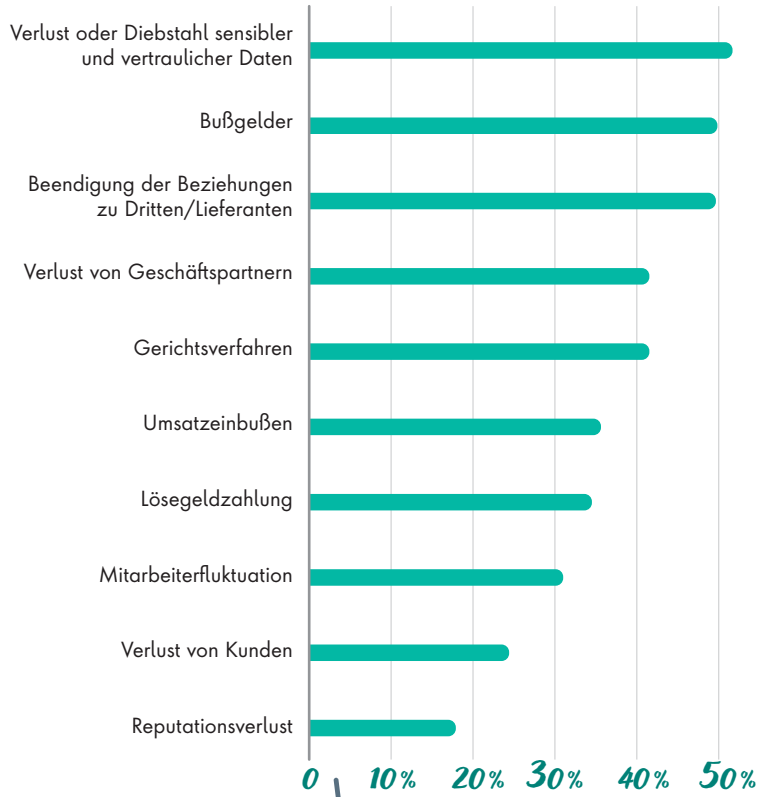
Die Aufgabe für die IT-Sicherheit besteht nun darin, sicherzustellen, dass Maßnahmen und Tools strategisch und konsequent angewandt werden - für alle privilegierten Zugriffsanforderungen. Die Zugriffssicherheit muss sowohl für interne Benutzer als auch für Dritte transparent, dokumentiert und effektiv geregelt werden. Um den Zugriff von Festangestellten und Externen differenziert zu regeln, dienen rollenbasierte Zugangskonzepte, Zero-Trust-Konzepte mit Zugriffsmanagement und Multifaktor-Authentifizierung.

Dirk Wahlefeld

Über die Studie

Das Ponemon Institut befragte Ende 2024 1.942 IT- und IT-Sicherheitsverantwortliche in den USA (733), Großbritannien (398), Deutschland (573) und Australien (238), die mit der Verwaltung von privilegierten Zugängen sowohl von Dritten als auch von internen Benutzern in ihren Organisationen vertraut sind. Die Befragten gehören Unternehmen aus folgenden Branchen an: Gesundheitswesen (11 Prozent), der öffentliche Sektor (23 Prozent), Industrie und Fertigung (32 Prozent) sowie Finanzdienstleistungen (34 Prozent).

FOLGEN EINER SICHERHEITSVERLETZUNG ODER EINES ANGRIFFS



Zero-Trust

VOR DER TECHNOLOGIE KOMMT DIE STRATEGIE

Trotz einer hohen Dunkelziffer an nicht gemeldeten Vorfällen reißt die Flut an Nachrichten über erfolgreiche Cyberangriffe auf Unternehmen und Organisationen nicht ab. So bleibt die Bedrohungslage aus dem Cyberraum auf einem konstant hohen Niveau – eine Erkenntnis, die zahlreiche Cybersecurity-Reports untermauern.

Eine Lehre aus dieser stagnierenden Situation ist die immer noch in der Praxis verbreitete Nutzung klassischer Sicherheitsarchitekturen mit dem Schwerpunkt auf der Perimeter-Verteidigung, bei der leistungsfähige Firewalls zum Einsatz kommen, während der nachgelagerte Bereich der IT-Infrastruktur häufig vernachlässigt wird. Dadurch entsteht oft ein implizites Vertrauensverhältnis im internen Netzwerk zwischen Benutzern, Systemen und Ressourcen. Dies ermöglicht Angreifern, sich nahezu ungehindert lateral im Netzwerk zu bewegen, um ihre schadhaften Ziele zu verfolgen, sobald die Verteidigungslinie des Perimeters überwunden wurde.

Angesichts solcher Risiken ist ein grundlegendes Umdenken unerlässlich. In diesem Zusammenhang stellt Zero-Trust ein vielversprechendes und modernes Sicherheitskonzept dar. Es beruht auf dem Prinzip, dass keinem Nutzer oder System, sei es intern oder extern, automatisch vertraut wird. Stattdessen wird jeder Zugriff auf (kritische) Ressourcen explizit geprüft und auf das notwendige Minimum beschränkt. Diese rigorose Transaktionskontrolle stellt sicher, dass selbst authentifizierte, legitime Nutzer nur auf die für ihre Aufgaben relevanten Daten und Systeme zugreifen können. Darüber hinaus ist eine der Grundannahmen von Zero-Trust, dass ein Angriff bereits stattgefunden haben könnte („assume breach") – sei es durch einen externen Angreifer oder durch einen Insider. Infolgedessen wird das gesamte Netzwerk kontinuierlich überwacht und somit der Handlungsspielraum für Bedrohungsakteure massiv eingeschränkt.

Gezielte Neuausrichtung erforderlich

Neben den aufgezeigten Vorteilen darf nicht unerwähnt bleiben, dass es sich bei Zero-Trust um einen Paradigmenwechsel handelt, welcher erhebliche Aufwände mit sich bringen kann. Zero-Trust erfordert dabei keine vollständige Abkehr von bestehenden Maßnahmen, sondern eine gezielte Neuausrichtung vorhandener Technologien, Prozesse und Mitarbeiter. Viele Unternehmen und Organisationen, die vorrangig auf eine Perimeter-Verteidigung setzen, verfügen bereits über wertvolle Grundlagen für diesen lohnenden Übergang zu Zero-Trust. Organisatorische Strukturen wie Sicherheitsrichtlinien und regelmäßige Überprüfungen sind oft etabliert und bieten eine solide Basis. Auch technische Maßnahmen wie Identitäts- und Zugriffsmanagement, Netzwerksegmentierung oder Endpoint-Protection sind oftmals vorhanden. Diese werden jedoch häufig darauf ausgelegt, den Perimeter zu stärken, anstatt eine durchgängige Vertrauensprüfung sicherzustellen. Entscheidend ist eine klare Strategie, die Zero-Trust konsistent und nachhaltig im Unternehmen oder in der Organisation verankert.

Seit über 50 Jahren steht infodas, ein Airbus Tochterunternehmen spezialisiert auf Cyber und IT, für zuverlässige und vertrauenswürdige Cybersicherheit. infodas bietet neben Hochsicherheitsprodukten gegen den ungewollten Datenabfluss einen ganzheitlichen Beratungsansatz zur Erstellung einer Zero-Trust-Strategie. Gemeinsam mit Ihnen bestimmen wir schützenswerte Ressourcen und Ihr angestrebtes Sicherheitsniveau. Auf dieser Grundlage begleiten wir Sie beim Aufbau der erforderlichen Architektur und unterstützen Sie bei der regelmäßigen Überprüfung der Strategie und dessen Anpassung.

www.infodas.com

infodas
connect more. be secure.

Alles auf Anfang

ECHTZEIT-REPORTAGE: CYBERANGRIFF IM MITTELSTAND

Samstagmorgen, 08:13 Uhr – Das Telefon klingelt. Am anderen Ende der Leitung: ein neuer Kunde, kein Vertrag, keine Service-Level-Agreements – aber mit einem existenzbedrohenden Problem. **Der Verdacht:** Ransomware-Attacke. Keine Zeit für Formalitäten – ich fahre los.

Ich ahne bereits, dass es heftig wird. Weder war das Ausmaß des Angriffs nach dem Erstgespräch abschätzbar, noch kannte ich die Sicherheitslage sowie die vorhandenen Anforderungen, Prozesse und Strukturen.

Strukturierter Einstieg ins Chaos

Als ich ankomme, herrscht auf allen Ebenen Alarmstufe Rot. Die komplette Windows-x86-Plattform des Unternehmens ist lahmgelegt. Alle Dateien verschlüsselt, keine Kommunikation mehr möglich, kein Backup auffindbar. Überall aufgebrachte Gesichter – in den Fluren, im Rechenzentrum, im improvisierten Krisenraum. Admins, LKA-Beamte, Fachbereiche, Geschäftsführung – alle reden durcheinander.

Meine Rolle war mir in den ersten 5 Minuten klar. Ruhe reinbringen, für Struktur sorgen. Ich verschaffe mir Gehör und teile die Akteure nach Verantwortlichkeiten und Handlungsfeldern auf.

Keyuser der Fachbereiche erstellen eine Liste aller geschäftskritischen Applikationen, Administratoren analysieren mögliche Backups und das Management kümmert sich um die Kommunikation mit Presse, Behörden, Lieferanten und Mitarbeiter. Erste forensische Analysen werden durchgeführt.

Das Ergebnis: Der Angriff war gut vorbereitet. Phishing war der Einstieg, monatelang hatten sich die Angreifer im Netz bewegt. Warnsignale wurden übersehen oder falsch interpretiert.

Ein Backup, das keiner auf dem Schirm hatte

Während alle anderen ihre Aufgaben beginnen, schaue ich mir die SAP-Landschaft an. Diese läuft – zum Glück – auf IBM Power-Systemen mit separatem Storage und segmentierter Netzwerkstruktur. **Das Resultat:** Die SAP-Umgebung ist unangetastet.

Doch der Rest der IT ist schwer getroffen. Insbesondere die Backup-Systeme scheinen nicht nur kompromittiert, sondern mutmaßlich gelöscht. Die Stimmung ist auf dem Tiefpunkt.

WER SYSTEME TRENNT, SICHERHEITSTOOLS GANZHEITLICH EINSETZT, PROZESSE INTEGRIERT UND TESTET UND MITARBEITER SENSIBILISIERT, HAT IM ERNSTFALL EINE CHANCE.

Grit Wasmund, Geschäftsführerin, IT-Power Services Deutschland GmbH, www.it-ps.de

Dann der Wendepunkt: Bei der Sichtung der Hardware wird ein älteres Storage-Backupsystem entdeckt, das zwar nicht mehr im produktiven Betrieb genutzt wird, aber noch im Rack unverkabelt verbaut ist. Erleichtert stellen die Admins fest, dass darauf noch Backups vorhanden sind. Das Unternehmen hatte vor kurzem auf ein neues Speichersystem umgestellt, das alte aber nicht gelöscht oder ausgebaut. Es war vom Netzwerk getrennt – und damit für den Angreifer nicht erreichbar.

Ein Paradebeispiel für glückliche Redundanz. Das alte System war quasi ein Cold Backup – ungewollt, in dieser Situation aber rettend.

Clean Room statt Schnellschuss

Statt hektisch alles zurückzuspielen, schlage ich einen methodischen Weg vor. Gemeinsam mit dem Kunden wird eine Clean Room-Infrastruktur aufgebaut. Dort sollen die gesicherten Systeme geprüft und bei Freigabe auf neuer Hardware wieder in Betrieb genommen werden.

Die Wiederanlaufstrategie folgt dabei einer einfachen, aber effizienten Logik: Zuerst werden die betriebsnotwendigen Anwendungen priorisiert – insbesondere ERP, Produktionssteuerung, Kommunikationssysteme. Dann erfolgt eine tiefgreifende Prüfung jeder Applikation auf mögliche Schadsoftware. Nur Systeme, die virenfrei sind und keine Ransomware-Artefakte enthalten, werden überführt.

Die SAP-Systeme auf IBM Power bieten in dieser Situation einen entscheidenden Vorteil. Ihre Sicherheitsarchitektur und die physische Trennung der Infrastruktur sorgen für Integrität. Kein Zugriff der Angreifer, keine Manipulation, keine Verschlüsselung – ein sicherer Anker in der chaotischen Umgebung.

Mittwochmorgen – die neue Welt steht

Immer wieder steht die Frage im Raum, ob man nicht doch auf die Lösegeldforderung reagieren sollte. Doch die Entscheider bleiben standhaft. Keine Kommunikation mit den Angreifern, kein Einlenken, keine Zahlung. Der Wiederanlauf soll mit eigenen Mitteln gelingen.

In den folgenden Tagen arbeiten alle rund um die Uhr mit vollem Einsatz: Rücksicherung der Backups, Neuvergabe sämtlicher User- und Admin-Konten, Segmentierung der Netzwerke, Absicherung aller Managementserver.

Als die Produktion nur 4 Tage nach dem Angriff wieder anläuft, atmen alle durch, kollektive Erleichterung macht sich bereit. **Alle Mühen, aller Einsatz haben sich gelohnt:** ein Gänsehaut-Moment.

In der Krise optimal agieren

Wenn ich heute auf den Einsatz zurückschaue, kann ich die große Anspannung und Verantwortung immer noch körperlich spüren. Man fühlt sich wie in einem falschen Film und stellt sich immer wieder die Frage: Ist das alles nur ein Alptraum oder ein schlechter Scherz?

Welche „Lessons Learned" für das Krisenmanagement nehme ich mit? Zunächst muss eine Person bestimmt werden, die sowohl den Krisenstab leitet als auch den zentralen Workstream „Kommunikation" koordiniert. Dazu gehört die frühzeitige Identifikation und das Briefing weiterer erforderlicher Spezialisten – etwa für Verhandlungsführung, Zahlungsabwicklung oder juristische Fragestellungen.

Zentral für einen Notfalleinsatz ist die Krisenkommunikation. In kürzester Zeit sind zielgerichtete Wordings für alle internen und externen Stakeholder zu erarbeiten – von der Erstinformation über kontinuierliche Mitarbeiter- und Kundenkommunikation bis hin zu Presseinformationen und FAQ-Dokumenten. Parallel sind Zeitpläne, Notfalllösungen und Interimsprozesse zu etablieren.

Bereits im Vorfeld sollten sich Unternehmen auf das Krisenmanagement vorbereiten: zum Beispiel Krisenkommunikations-Handbücher erstellen oder überarbeiten, Notfallübungen durchführen und strategische Beratungsleistungen einbinden – ein entscheidender Faktor, der sich im Ernstfall bezahlt macht.

Lehren für die Zukunft - technische Vorkehrungen

Jedes Unternehmen hat zudem Vorkehrungen zu treffen, die verhindern, dass es überhaupt zu einer Cyberattacke kommt.

Zu einer umfassenden Sicherheitsarchitektur gehören folgende technische Komponenten:

- Konsequentes Nutzermanagement: Benutzerprofile Up-to-Date halten, Segmentierung von Admin- und Benutzerkonten, Pflege auf Applikationsebene.
- Einführen eines zusätzlichen Offline-Backups auf Tape.
- Implementierung eines Tools zur Anomalie-Erkennung inklusive der für ein Funktionieren notwendigen individuellen Unternehmensprozesse.

Lehren für die Zukunft - organisatorische Vorkehrungen

Eine gute organisatorische Vorbereitung umfasst regelmäßige Audits und Security-Analysen. Hier können externe Partner ebenso unterstützen wie bei dem Erstellen und Verteilen einer Informationssicherheitsrichtlinie. Ein absolutes Muss sind regelmäßige Awareness-Schulungen für alle Mitarbeitenden.

Fazit: Wer Systeme trennt, Sicherheitstools ganzheitlich einsetzt, Prozesse integriert und testet und Mitarbeiter sensibilisiert, hat im Ernstfall eine Chance. Und es braucht Menschen mit einem kühlen Kopf, technischer Tiefe - und der Fähigkeit, in Extremsituationen Verantwortung zu übernehmen.

Grit Wasmund

Die häufigsten Passwörter bei Angriffen auf RDP-Ports

NEUE SPECOPS-ANALYSE

Die aktuelle Analyse von Specops zur Nutzung von kompromittierten Passwörtern für Angriffe auf RDP-Ports zeigt einmal mehr: Cyberangriffe sind oft keine Hightech-Operationen, sondern schlicht Fleißarbeit automatisierter Systeme. Es braucht keine ausgeklügelte Hacking-Strategie, wenn nach wie vor Zugangsdaten wie 'admin', '123456' oder 'user' bei öffentlich erreichbaren Remote-Desktop-Ports erfolgreich sind. Für Angreifer bedeutet das: Sie müssen nicht innovativ sein – die Unternehmen machen es ihnen immer noch viel zu leicht.

Passwort-Klassiker

Besonders brisant an den aktuellen Zahlen: Unter den 20 meistversuchten Passwörtern finden sich praktisch ausschließlich Klassiker, die seit Jahren bekannt und auf Sicherheitswarnlisten stehen. Diese Passwörter stehen symbolisch für ein Problem, das viele Unternehmen weiterhin unterschätzen: Es sind nicht nur Zero-Day-Exploits oder hochspezialisierte Attacken, die die IT-Infrastruktur gefährden – oft reicht das digitale Durchprobieren von Standardpasswörtern.

Dabei ist die Methode nicht neu. Brute-Force- oder Credential-Stuffing-Angriffe gehören längst zum Standard-Repertoire von Cyberkriminellen. Neu ist nur, dass es offenbar immer noch genügend Unternehmen gibt, die ihre extern erreichbaren Systeme nicht konsequent dagegen absichern.

Offene RDP-Ports – Einladung zum Angriff

Remote-Desktop-Protokolle (RDP) sind für viele IT-Abteilungen ein praktisches Werkzeug, um auf Systeme zuzugreifen. Aber sobald RDP-Zugänge direkt aus dem Internet erreichbar sind, wird daraus ein massives Sicherheitsrisiko – insbesondere, wenn dabei schwache, bekannte oder kompromittierte Passwörter im Spiel sind.

Die Lösung ist bekannt – und doch in der Praxis oft nicht umgesetzt:

- RDP-Zugänge niemals ungeschützt über das Internet erreichbar machen;
- Absicherung über VPN, Jump-Server oder Geoblocking;
- Starke Passwort-Policies und Passwortfilter einsetzen;
- Multi-Faktor-Authentifizierung verpflichtend aktivieren;
- Unnötige Accounts und RDP-Zugänge konsequent deaktivieren.

Passwortrichtlinien alleine reichen nicht

Ein besonders gefährlicher Irrtum vieler Unternehmen: Sie verlassen sich noch immer auf klassische Passwortrichtlinien, die lediglich Länge und Sonderzeichen fordern. Das führt in der Praxis zu Passwortkonstruktionen wie 'Admin2024!', die technisch komplex wirken, aber in jeder Angriffsliste ganz oben stehen.

Moderne Passwortfilter setzen deshalb gezielt an den bekannten Schwachstellen an. Sie blockieren Standardpasswörter, Namen, Tastaturmuster oder Passwörter aus früheren Leaks. Damit reduzieren Unternehmen das Risiko automatisierter Angriffe erheblich.

IT-Sicherheit beginnt bei den Basics

Die Zahlen von Specops sind kein Beweis für besonders raffinierte Angreifer – im Gegenteil. Sie sind ein Beweis dafür, dass grundlegende Sicherheitsmaßnahmen in vielen Organisationen noch immer nicht konsequent umgesetzt werden.

Dabei ist der Schutz vor solchen Angriffen keine Frage großer Investitionen. Es braucht:

- IT-Hygiene;
- Sensibilisierung;
- technische Mindeststandards.

Das Motto muss lauten: kein extern erreichbarer Login ohne MFA. Kein Passwort ohne moderne Filter. Kein Zugang, der nicht wirklich benötigt wird. Denn wer seine IT-Sicherheit wirklich ernst nimmt, überlässt einfache Passwörter endgültig der Vergangenheit.

Stephan Halbmeier
https://specopssoft.com/de/

Managed-SOCs

UNTERNEHMEN GEGEN RANSOMWARE STÄRKEN

Ob LLM-generierte Schadsoftware oder striktere Richtlinien zur Cybersicherheit – die Rahmenbedingungen werden für Unternehmen nicht einfacher. Im Angebot von Managed Service Providern liegt ein Schlüssel für mehr Resilienz – vorausgesetzt die Tools passen zu den spezifischen Anforderungen und berücksichtigen wichtige Regularien.

Eine Ransomware-Attacke zählt für Unternehmen zu den dunkelsten Stunden in der Firmengeschichte. In vielen IT-Boards ist die Angst vor Schadsoftware dementsprechend hoch – und das zu Recht. Der bitkom ermittelte 2024, dass 60 Prozent der befragten Unternehmen innerhalb eines Jahres mit Ransomware attackiert wurden. Bei einem Drittel entstand durch IT-Ausfälle und Lösegeldforderungen finanzieller Schaden.

FÜR DIE MEISTEN UNTERNEHMEN FÜHRT AN DER ZUSAMMENARBEIT MIT EINEM MANAGED SERVICE PROVIDER (MSP) KEIN WEG VORBEI.

Gerald Eid, Regional Managing Director DACH, Getronics, www.getronics.com/de

Die möglichen Folgewirkungen von Ransomware-Attacken auf Unternehmen haben sich seit Anfang des Jahres nochmals verschärft. Mit dem Inkrafttreten der Cybersicherheits-Richtlinien NIS2 und DORA etablieren sich neue Standards. Verantwortliche müssen sie bei der Gestaltung ihrer Sicherheitsarchitektur berücksichtigen. Zumal auch davon auszugehen ist, dass Behörden und Versicherer bei der Bewertung von Angriffen verstärkt prüfen, ob Risiken sehenden Auges in Kauf genommen worden sind.

Eine realistische Bewertung des Risikos wird daher immer komplexer. Wie Analysen des BSI zeigen, sind LLMs für Cyberkriminelle ein beliebtes Tool bei der Schadcodegenerierung, durch das sie langwierige Trainingsprozesse umgehen können. Eine schlechte Nachricht für Unternehmen – denn damit steigt auch das Risiko für Angriffe.

Framework-gestützte Sicherheitslösungen

Zum Schutz vor Ransomware hat sich in vielen Branchen ein mehrschichtiger Ansatz bewährt. Dazu zählt zum einen der Einsatz von Sicherheitstools wie etwa der Multi-Faktor-Authentifizierung, VPNs und Firewalls. Zum anderen bedarf es einer Unit im Unternehmen, die sich 24/7 mit dem Thema Cyberabwehr beschäftigt. Erst dann kann ein Security Operations Center (SOC) schlagkräftig agieren, um beispielsweise ein lückenloses Alert-Management sicherzustellen, Incident-Response-Pläne zu erstellen und Backup-Strategien umzusetzen. Die lange Aufgabenliste zeigt eines deutlich: nur mit hohem Ressourceneinsatz lassen sich diese Services unternehmensintern umsetzen.

Für die meisten Unternehmen führt an der Zusammenarbeit mit einem Managed Service Provider (MSP) daher kein Weg vorbei. Doch die Auswahl des passenden Dienstleisters ist kein einfaches Unterfangen. Oft fehlt es sowohl an Erfahrungswerten als auch an Messgrößen, mit denen sich die umfangreichen Versprechen von MSPs prüfen lassen. Frameworks wie NIST CBS und MITRE ATT&CK können hier den Unterschied machen. Sie definieren grundlegende Funktionen und Referenzen. Zudem schaffen sie die Schnittstellen zu regulatorischen Standards wie etwa der ISO 27001 oder der DSGVO.

SOC-Teams für einen echten 24/7-Schutz

Für eine effektive Angriffsabwehr braucht es dann noch ein SOC-Team, das 24/7 vor möglichen Incidents schützt. Der Technologieanbieter Getronics setzt hierfür auf ein umfassendes Threat Lifecycle Management, das Endgeräte (EDR) und Netzwerke (NDR) überwacht und den Kunden eine modulare Auswahl von Analytik-Tools offeriert. So können die spezifischen Rahmenbedingungen abgebildet werden, ohne dass unnötige Kosten entstehen. Ein lückenloser Schutz gegen Ransomware macht sich dann bereits ab dem ersten abgewehrten Incident bezahlt.

Gerald Eid

getronics

Digitale Resilienz im Finanzsektor

DORA-VERORDNUNG STÄRKT EUROPÄISCHE FINANZDIENSTLEISTER GEGEN CYBERRISIKEN

Seit dem 17. Januar 2025 ist DORA in Kraft, die EU-Verordnung über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act). Die Verordnung soll im gesamten Finanzsektor die Themen Cybersicherheit, IKT-Risiken und digitale operative Resilienz regeln. Ziel ist es, auf diese Weise den europäischen Finanzmarkt gegenüber Cyberrisiken und Vorfällen der Informations- und Kommunikationstechnologie zu stärken.

Richtig umgesetzt bietet DORA EU-Finanzinstituten und ihren kritischen Serviceprovidern die Möglichkeit, ihre allgemeine Resilienz zu erhöhen. Obwohl die Verordnung in erster Linie auf EU-Finanzinstitute und ihre Drittanbieter (innerhalb und außerhalb der EU) abzielt, wirft ihre Umsetzung wichtige Fragen auf. Konkret geht es um die Auswirkungen auf das Geschäft, die Effizienz und Innovationen für alle Organisationen im weiteren Geschäftsumfeld dieser Finanzinstitute. Besonders relevant sind die Fragen für kleinere Unternehmen, die im Gegensatz zu vergleichbaren größeren Organisationen über weniger Ressourcen verfügen.

Damit DORA erfolgreich sein kann, müssen sowohl direkt betroffene Organisationen als auch kleinere Akteure am Rande der Branche einen Weg finden, die Richtlinie einzuhalten, um zu verhindern, dass sich die Verordnung negativ auf ihre Geschäftsmodelle auswirkt oder Innovationen gar erstickt. Anstatt sich von der Verordnung die Richtung vorgeben zu lassen, sollten Unternehmen sie als treibende Kraft nutzen, um in ihre IT-Managementpraktiken zu investieren und diese zu reformieren. So können sie eine größere Robustheit erreichen und sich gegen die Bedrohung durch Cyberangriffe, Ausfälle und menschliches Versagen wappnen.

DER SCHLÜSSEL ZUM ERFOLG LIEGT IN DER IMPLEMENTIERUNG FORTSCHRITTLICHER ÜBERWACHUNGSSYSTEME UND FUNKTIONSÜBERGREIFENDER REAKTIONSTEAMS.

Effie Bagourdi, Global Head of Service Management, Adaptavist, www.theadaptavistgroup.com

Für eine Kultur der Sicherheit und Widerstandsfähigkeit

In der jüngeren Vergangenheit haben mehrere globale Ereignisse zu einem Wendepunkt für die digitale Resilienz geführt, wie etwa der siebenstündige Ausfall von Meta im Jahr 2021. Dieser war auf einen Fehler bei der routinemäßigen Wartung zurückzuführen, durch den alle Rechenzentren des Unternehmens vorübergehend vom Netz getrennt wurden. Auch der Ausfall von CrowdStrike im Jahr 2024, bei dem Schwachstellen in der IT-Infrastruktur tausender Unternehmen aufgedeckt wurden, hat die digitale Resilienz in den Fokus gerückt.

Auf regulatorischer Ebene etablieren Rahmenwerke wie DORA die digitale Resilienz als eine zentrale geschäftliche Notwendigkeit und bieten Organisationen internationale Standards, die sie befolgen sollten. Innerhalb der Organisationen selbst wird von einer Verschiebung der Prioritäten berichtet. Eine Studie von Adaptavist hat ergeben, dass 86 Prozent der vom CrowdStrike-Ausfall betroffenen Unternehmen nun planen, ihre Schulungen zur Reaktion auf Vorfälle zu verstärken und ihr Risikomanagement für Anbieter zu verbessern.

Unabhängig von den Beweggründen liegt der wahre Maßstab für jede Vorschrift jedoch in ihrer Umsetzung. DORA bietet zwar wichtige Orientierungshilfen, doch Organisationen benötigen die Flexibilität, Resilienzstrategien zu entwickeln, die auf ihre spezifischen betrieblichen Anforderungen zugeschnitten sind. Die einzelnen Haftungsklauseln von DORA stellen jedoch eine Herausforderung dar. Zwar ist es wichtig, Verantwortung zu übernehmen, allerdings besteht bei übermäßigen Strafen

die Gefahr, dass eine Angstkultur entsteht, die die transparente Berichterstattung von Vorfällen behindern könnte. Dies ist jedoch notwendig, um betriebliche Herausforderungen zu meistern.

Anstatt sich von diesen Bestimmungen den Prozess vorschreiben zu lassen, sollten Unternehmen DORA als Chance begreifen – um von Grund auf robuste Resilienz-Praktiken und eine „Resilience-First"-Kultur aufzubauen. In Kombination mit anpassungsfähigen Best Practices wird dies entscheidend dazu beitragen, künftige Ausfälle oder Cybervorfälle großen Ausmaßes und mit weitreichenden Folgen zu verhindern.

Außerdem können sie sich so einen Wettbewerbsvorteil verschaffen, da digitale Resilienz für Partner und Kunden immer mehr an Bedeutung gewinnt.

Die Umsetzung einer effektiven Servicemanagement-Strategie kann Teams dabei helfen, besser zusammenzuarbeiten. Der richtige Ansatz verbessert die Sichtbarkeit und Erkenntnisse durch proaktive Überwachung und ermöglicht es IT-Teams, durch Automatisierung Prozesse und Arbeitsabläufe zu verbessern. Dies wiederum unterstützt Organisationen dabei, sich auf das Wesentliche zu konzentrieren – in der Gewissheit, dass ihre Prozesse einer Prüfung durch die Aufsichtsbehörden standhalten.

Die operative Herausforderung

DORA bietet zwar eine gute Gelegenheit, die operative Basis zu untersuchen und zu stärken, doch die Einhaltung der Vorschriften erfordert von Unternehmen jeder Größe erhebliche Investitionen und Ressourcen. Während größere Institutionen über die Zeit und die Mittel verfügen, um die Richtlinie strategisch nach ihren Vorstellungen umzusetzen, sind kleinere Unternehmen durch enge Fristen und begrenzte Budgets doppelt eingeschränkt. Infolgedessen sind kleinere Unternehmen möglicherweise gezwungen, reaktive Compliance-Maßnahmen zu ergreifen. Damit besteht die Gefahr, dass sie eher danach streben, die schnelle Einhaltung von Vorschriften statt die langfristige betriebliche Effizienz sicherzustellen.

Dies stellt eine große Herausforderung für die internationale Einführung dar, da Länder mit einer starken mittelständischen Wirtschaft dazu neigen, sich für Innovation und Kreativität einzusetzen. Das Potenzial von DORA, dies zu verhindern, könnte zu einem Widerstand führen, wie die verzögerte Einführung von NIS2 in 23 Mitgliedstaaten zeigt.

Daher ist es für kleine Unternehmen unerlässlich, sich anzupassen, über den Tellerrand hinauszuschauen und die Richtlinie proaktiv anzugehen. Nur so können sie die Erfolge größerer Unter-

nehmen erzielen, die regulatorische Anforderungen als Anstoß für strategische Verbesserungen nutzen.

Wie sich DORA erfolgreich umsetzen lässt

Der Aufbau einer Kultur der Resilienz und die Einhaltung von DORA muss nicht zwingend schmerzhaft sein. Wenn man es richtig angeht, können Unternehmen nicht nur Risiken mindern, sondern sich auch einen Wettbewerbsvorteil verschaffen – und das in einer Zeit, in der Resilienz zu einem wichtigen Unterscheidungsmerkmal wird.

Der Schlüssel zum Erfolg liegt in der Implementierung fortschrittlicher Überwachungssysteme und funktionsübergreifender Reaktionsteams, die die Anforderungen erfüllen und eine Reihe potenzieller Betriebsstörungen bewältigen, anstatt Prozesse nur so zu gestalten, dass sie die Mindestanforderungen erfüllen. Unternehmen sollten der Schulung ihrer Teams und ihren Datenschutzpraktiken Priorität einräumen. Dies setzt voraus, dass Unternehmen über Compliance-Checklisten hinausgehen und Resilienz in ihre täglichen Abläufe integrieren.

So ist beispielsweise die obligatorische Meldung von Vorfällen eine der wichtigsten Anforderungen. Organisationen können Rahmenbedingungen für das Vorfallsmanagement einführen, die in Schulungsmodule und Resilienz-Prüfungen integriert werden. So wird sichergestellt, dass die Teams umfassend auf die Melde- und Reaktionsanforderungen von DORA vorbereitet sind. Regelmäßige Schulungen und gemeinsame Übungen verbessern die Reaktionszeiten, reduzieren Störungen und richten die Teams auf Resilienz-Ziele aus.

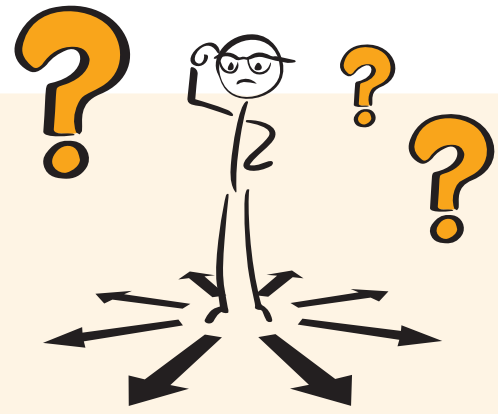
Vorschriften sollten nicht als allgemeine Checkliste mit Geboten und Verboten behandelt werden, sondern vielmehr als Anstoß, kritisch über die eigenen Geschäftsanforderungen nachzudenken. Durch die Berücksichtigung von Bereichen, die möglicherweise nicht in den direkten Geltungsbereich von DORA fallen, wie zum Beispiel rechtliche und betriebliche Funktionen, können Unternehmen einen ganzheitlicheren und zukunftssichereren Ansatz für Resilienz sicherstellen.

Effie Bagourdi

PRO & CONTRA

Wie DORA die Resilienz unterstützt

- Stärkt Frameworks für das IT-Risikomanagement
- Fördert die proaktive betriebliche Resilienz und Wiederherstellungspraktiken
- Reduziert Risiken von Drittanbietern durch robuste Lieferantenstandards
- Stärkt das Vertrauen der Akteure
- Verschafft resilienten Organisationen Wettbewerbsvorteile
- Verbesserte Transparenz durch obligatorische Berichterstattung über Vorfälle



Hindernisse bei der DORA-Implementierung

- Komplexe Prozesse im Zusammenhang mit Risiken können Unternehmen überfordern
- Personelle Engpässe bei obligatorischen Tests/Berichten
- Keine Garantie für eine einheitliche Durchsetzung in den EU-Mitgliedstaaten
- Erhöhung der Komplexität der regionenübergreifenden Compliance
- Einzelne Haftungsklauseln können Transparenz verhindern
- Risiko, dass Vorschriften veralten

Wandel der Cloud-Sicherheitslandschaft

SYSDIG REPORT 2025 ZEIGT ZENTRALE FORTSCHRITTE UND ENTWICKLUNGSPOTENZIALE

CLOUD-NATIVE ARCHITEKTUREN SIND LÄNGST ZUM STANDARD GEWORDEN – MIT IHNEN STEIGEN DIE ANFORDERUNGEN AN SICHERHEIT, TRANSPARENZ UND GOVERNANCE.

Crystal Morin, Cybersecurity Strategist, Sysdig, https://de.sysdig.com/

Cloud-native Architekturen sind längst zum Standard geworden – mit ihnen steigen die Anforderungen an Sicherheit, Transparenz und Governance. Der aktuelle Sysdig Cloud-Native Security and Usage Report 2025 bietet einen datenbasierten Einblick in die Praxis: Millionen von analysierten Container-Workloads und Cloud-Accounts zeigen, wie Unternehmen weltweit ihre Sicherheitsstrategien weiterentwickeln. Besonders auffällig: Während die Cloud-Sicherheitsreife in Bereichen wie Threat Detection, KI-Sicherheit und Runtime Protection zunimmt, bleiben Schwächen beim Identitätsmanagement und der Container-Hygiene bestehen.

KI skaliert – und Sicherheit zieht nach

Die Verbreitung von KI-Workloads ist explodiert: Innerhalb eines Jahres ist ihr Einsatz um 500 Prozent gestiegen. Insbesondere GenAI-Modelle werden immer häufiger in produktiven Umgebungen eingesetzt. Gleichzeitig nimmt die Angriffsfläche ab - der Anteil öffentlich exponierter KI-Workloads ist um 38 Prozent gesunken. Auch Laufzeit-Scans zeigen nur noch vereinzelt kritische Schwachstellen. Dies zeigt: Sicherheitsanforderungen wie Zugriffskontrolle, Netzwerktrennung und Laufzeitschutz werden - zumindest im Bereich KI - zunehmend konsequent umgesetzt.

IAM bleibt Achillesferse der Cloud

Ein zentrales Risiko bleibt das Überprovisionieren von Berechtigungen. Der Report beleuchtet eine andere Perspektive: die Diskrepanz zwischen menschlichen Nutzern und automatisierten Servicekonten. In vielen Organisationen beträgt der Unterschied zehntausende Accounts – zu Lasten der Übersichtlichkeit und Sicherheit. Service-Accounts sind dabei 7,5-mal anfälliger für Sicherheitsvorfälle. Immerhin: Bei Human Accounts gibt es einen klaren Trend zu mehr Governance, etwa durch feinere Rollenzuweisungen und Monitoring.

Angreifer brauchen Minuten – Verteidiger nur Sekunden

Moderne Cloud-Angriffe verlaufen automatisiert und in hohem Tempo. Laut Report gelingt es vielen Security-Teams mittlerweile, dem etwas entgegenzusetzen: Alerts werden in unter fünf Sekunden generiert, Vorfallanalysen innerhalb von vier Minuten abgeschlossen, Reaktionen automatisiert eingeleitet. Möglich wird das durch den Einsatz von Runtime Detection, Policy-as-Code und automatisierten Response-Workflows.

Container-Security: Fortschritte mit Rückschritten

Containerisierte Workloads dominieren Cloud-native Deployments – und deren Absicherung ist entscheidend. Die gute Nachricht: Die Zahl kritischer Schwachstellen zur Laufzeit liegt in vielen Unternehmen unter sechs Prozent. Auch die durchschnittliche Container-Lifetime sinkt, was die Angriffsfläche reduziert. Gleichzeitig wächst jedoch die Größe der Container-Images – teils um das Fünffache. Ein möglicher Nebeneffekt des KI-Booms, der zusätzliche Pakete und Abhängigkeiten mit sich bringt. Hier besteht Nachholbedarf bei der Image-Hygiene.

Fazit: Fortschritt erkennbar, kein Stillstand erlaubt

Der Report zeigt Unternehmen haben zentrale Herausforderungen erkannt – und reagieren mit Tempo, Technologie und Prozessoptimierung. Dennoch bleibt die Cloud ein dynamisches Ziel. Wer dauerhaft sichere, skalierbare Infrastrukturen aufbauen will, muss Risiken kontinuierlich bewerten und Sicherheit als festen Bestandteil des Deployments verstehen. Sonst drohen Infiltration durch Bedrohungsakteuren und Exfiltration sensibler Daten – potenziell innerhalb von Sekunden.

Crystal Morin

Die perfekte XDR-Party

WENN IHRE IT EIN FEST IST – WER SORGT DANN FÜR ORDNUNG?

Stellen Sie sich eine große Party vor: Gäste kommen aus allen Richtungen mit unterschiedlichen Interessen und Bedürfnissen – Freunde, Kollegen und Familie. Einige wollen tanzen, andere reden, manche suchen Snacks oder Drinks. Ohne einen guten Gastgeber, der alles koordiniert, endet die Party im Desaster: Die Musik passt nicht zur Stimmung, das Buffet ist leer, und niemand weiß, wo sich letztendlich die Bar befindet.

Dieser Fachartikel dreht sich natürlich nicht um eine richtige Party. Er nutzt diese aber als Analogie für die moderne IT – und erläutert, wie das ganzheitliche und moderne Sicherheitskonzept von Extended Detection and Response (XDR) als perfekter „Gastgeber" für Ordnung in jeder IT-Infrastruktur sorgt.

Die Gäste:
Vom Endpunkt bis zur Cloud

Widmen wir uns zunächst den Gästen der Party: den Geräten und Systemen in Ihrem Unternehmen – von den Endpunkten über die Server und Firewalls bis hin zu den Cloud-Services, E-Mail-Systemen und Anwendungen. Jeder dieser Gäste bringt dabei seine eigenen Besonderheiten und Kommunikationsweisen mit.

Für den Erfolg der Party entscheidend ist es, dass sich alle Gäste an definierte Regeln halten, miteinander harmonieren und – auch in Einzelfällen – keine Bedrohung für die restliche Gesellschaft darstellen. Ganz gleich, ob man sich untereinander bereits vertraut oder noch fremdelt.

Der Gastgeber: Extended Detection and Response (XDR)

Der Gastgeber der Party ist die eingesetzte XDR-Lösung. Sie empfängt jeden Gast an der Tür, überprüft, ob er eingeladen ist, sorgt dafür, dass niemand unerwünscht eindringt, und achtet darauf, dass sich kein Gast verdächtig verhält.

Im Gegensatz zu klassischen, punktuellen Lösungen wie beispielsweise Endpoint Detection and Response (EDR), die sich ausschließlich auf Endgeräte konzentrieren, integriert XDR die verschiedensten Datenquellen der Gäste in eine zentrale Plattform. XDR als Sicherheitskonzept zielt demnach darauf ab, Cyberbedrohungen über die gesamte IT-Infrastruktur zu erkennen, zu analysieren und darauf schlussfolgernd zu reagieren – und zwar proaktiv, koordiniert, automatisiert sowie unterstützt durch künstliche Intelligenz.

Hinter den Kulissen – was XDR wirklich leistet

Ganzheitliche XDR-Lösungen sammeln kontinuierlich Telemetriedaten aus unterschiedlichsten Datenquellen, normalisieren diese und führen sie in einer zentralen Plattform zusammen. Diese konsolidierten Informationen werden mithilfe fortschrittlicher Analytik, maschinellem Lernen und Verhaltensanalysen ausgewertet, um Muster und Anomalien zu erkennen, die auf potenzielle Bedrohungen in der IT-Infrastruktur hinweisen. Darüber hinaus priorisieren moderne XDR-Plattformen erkannte Bedrohungen, zeigen diese in einem Dashboard auf und unterstützen dabei, komplexe Angriffsketten und Anomalien nachzuvollziehen. So lassen sich jederzeit gezielte und effiziente Reaktionen sicherstellen.

XDR-Lösungen sind darüber hinaus in der Lage, automatisch Gegenmaßnahmen einzuleiten – etwa indem kompromittierte Geräte isoliert, verdächtige IP-Adressen blockiert oder Benutzerkonten vorübergehend gesperrt werden. Durch diese orchestrierten Reaktionen verkürzt sich die Reaktionszeit erheblich, was dabei hilft, potenzielle Schäden für Ihr Unternehmen wirksam einzudämmen. Dabei ermöglichen XDR-Systeme nicht nur reaktive Schutzmechanismen, sondern auch proaktive Sicherheitsmaßnahmen – zum Beispiel durch den Einsatz von Threat Intelligence, die Identifikation von Schwachstellen sowie die kontinuierliche Überwachung auf neue Angriffstechniken.

XDR als Integrations-Allrounder

Wie ein moderner Gastgeber, der sich nicht nur auf seine Intuition verlässt, sondern eingespielte Abläufe und bewährte Dienstleister einbindet, integriert auch das XDR vorhandene Sicherheitssysteme in eine koordinierte Gesamtarchitektur. Bestehende Lösungen wie EDR, SIEM, SOAR oder Firewalls werden nicht ersetzt, sondern angebunden und intelligent vernetzt. XDR sorgt so dafür, dass aus Einzellösungen ein schlüssiges Sicherheitskonzept wird – ohne Systembrüche, aber mit voller Übersicht.

FEATURE VERGLEICH

Technologie	Zweck	Abdeckung	Automatisierung	Reaktion	Stärken
EDR (Endpoint Detection & Response)	Bedrohungserkennung an Endpunkten	Nur Endpunkte	Eingeschränkt	Lokal (z.B. Isolierung)	Tiefe Einblicke in Endgeräte, forensische Analysen
SIEM (Security Information & Event Management)	Zentrale Loganalyse & Korrelation	Breite Logdaten	Gering	Manuell	Breite Datenbasis, langfristige Analyse
SOAR (Security Orchestration, Automation & Response)	Automatisierte Reaktion & Orchestrierung	Tool-übergreifend (SIEM, u.a.)	Hoch	Automatisiert (Playbooks)	Automatisierung repetitiver Aufgaben
XDR (Extended Detection & Response)	Ganzheitliche Bedrohungserkennung & -abwehr	Endpunkte, Netzwerke, Cloud, E-Mails u.a.	Hoch	Integriert, intelligent	Konsolidierte Sicht auf Bedrohungen, reduzierte Komplexität,schnellere, intelligente und automatisierte Reaktion

Ein professioneller Gastgeber denkt auch an die Skalierung. Je mehr Gäste erwartet werden, desto ausgefeilter die Logistik. Genauso flexibel verhält sich XDR: Moderne Lösungen sind modular aufgebaut und skalierbar, sodass sie sowohl in mittelständischen Umgebungen als auch in global vernetzten Konzernen effizient arbeiten. Dank offener Schnittstellen lassen sich bestehende Tools und Datenquellen – ob lokal oder in der Cloud – nahtlos integrieren. So bleibt das Sicherheitskonzept auch bei wachsender Gästezahl durchgängig stimmig, ohne Stolperfallen bei der Integration oder blinde Flecken in der Überwachung.

Wie XDR seine Rolle ausbaut

XDR entwickelt sich zunehmend zur zentralen Plattform moderner Security-Architekturen. Der Trend geht dabei klar in Richtung erweiterter Automatisierung, Kontext-basierter Korrelation von Bedrohungen und dynamischer Response-Mechanismen. Künftige XDR-Generationen werden verstärkt mit Cloud-nativen Architekturen, OT-Systemen und Identity-Plattformen vernetzt sein – inklusive tiefgreifender API-Integration und Echtzeit-Kollaboration mit externen Threat-Intelligence-Feeds.

Zudem wird die Rolle von KI weiter zunehmen: Machine-Learning-Modelle werden nicht nur zur Anomalie-Erkennung beitragen, sondern auch zunehmend Handlungsempfehlungen in Echtzeit geben. Die Roadmap führt XDR damit von einem Analyse- und Reaktionswerkzeug hin zu einer intelligenten, lernenden Steuerinstanz für unternehmensweite Cybersicherheit – resilient, skalierbar und strategisch ausgerichtet.

Mensch & Maschine: Zusammenarbeit statt Ersatz

Eines aber gilt es nicht zu vergessen: Selbst der beste Gastgeber braucht helfende Hände! Auch wenn ein XDR die Security-Teams durch automatisierte Prozesse und intelligente Analysen entlastet, bleibt menschliche Expertise unverzichtbar. Während XDR im Hintergrund die Fäden zieht, Prioritäten setzt und auf verdächtiges Verhalten reagiert, behalten erfahrene Sicherheitsanalysten den Überblick, treffen strategische Entscheidungen und greifen bei kritischen Vorfällen gezielt ein. Wie auf jeder guten Feier ist das Zusammenspiel entscheidend. Im Idealfall stellt dabei die Technik die robuste Struktur bereit, auf die der Mensch mit seiner Intuition, seiner Erfahrung und seinem Gespür aufbauen kann.

AUCH WENN EIN XDR DIE SECURITY-TEAMS DURCH AUTOMATISIERTE PROZESSE UND INTELLIGENTE ANALYSEN ENTLASTET, BLEIBT MENSCHLICHE EXPERTISE UNVERZICHTBAR.

Christian Daum, Business Development Manager Information Security, Controlware, www.controlware.de

Fazit: Erfolgreiche Events sind Teamwork

Controlware unterstützt Unternehmen bei der erfolgreichen Einführung von XDR-Lösungen – von der strategischen Planung über die Integration bis hin zum laufenden Betrieb. Im Mittelpunkt steht dabei die ganzheitliche Verzahnung bestehender Sicherheitskomponenten zu einer effektiven, skalierbaren Architektur. Ergänzend werden mit dem hauseigenen Managed SOC (Security Operations Center) umfassende Services für den Betrieb, die Überwachung und die kontinuierliche Weiterentwicklung der XDR-Umgebung angeboten – für maximale Transparenz, schnelle Reaktionsfähigkeit und nachhaltige Sicherheit. So bleibt Ihre IT auch bei voller Tanzfläche sicher, koordiniert und jederzeit unter Kontrolle.

Christian Daum

Check Point und die Zweischneidigkeit der KI

HINTER DEN KULISSEN EINES CYBERSECURITY-UNTERNEHMENS IM KAMPF MIT UND GEGEN KI

Wie geht ein Cybersecurity-Unternehmen intern mit den Chancen und Risiken der künstlichen Intelligenz um? Während KI die Möglichkeiten in der Cybersicherheit erheblich erweitert, steigt gleichzeitig die Gefahr, Opfer von KI-gesteuerten Angriffen zu werden. Check Point Software Technologies gibt gegenüber IT Security Einblicke in den Umgang mit dieser komplexen Herausforderung.

Wie KI bei Check Point integriert wird

Nataly Kremer ist Chief Product Officer und Head of R&D bei Check Point. Sie ist für den kompletten Produktlebenszyklus verantwortlich und entscheidet welche Produkte und Features entwickelt und wie sie gestaltet werden. Sie erläutert den Ansatz des Unternehmens: „Wir nutzen KI in unserem Backend-Intelligenzsystem, um zu entscheiden, welche potenziellen Bedrohungen bösartig sind und welche nicht, indem wir Tausende von Indikatoren analysieren und eine Entscheidung treffen. Das nennt sich bei uns ThreatCloud AI, das Gehirn all unserer Produkte."

ICH DENKE, KI IST EIN GROSSARTIGER WEG, UM EINFACHHEIT ZU ERREICHEN. ES IST EINE RICHTIGE ABKÜRZUNG.

Nataly Kremer, Chief Product Officer und Head of R&D, Check Point Software Technologies, www.checkpoint.com

Als Teil der Infinity Core Services sammelt und analysiert ThreatCloud AI täglich Big Data-Telemetrie und Millionen von Kompromittierungsindikatoren, sogenannte Indicators of Compromise (IoCs). Die Bedrohungsdatenbank wird von 150.000 angeschlossenen Netzwerken und Millionen von Endgeräten sowie von Check Point Research und Dutzenden von externen Feeds gespeist. Über 50 Engines sind vollgepackt mit KI-basierten Funktionen und Fähigkeiten.

Die Infinity-Plattform wurde mit einigen neuen Funktionen ausgestattet. Dazu gehören „Policy Insights" für KI-gestützte Richtliniendurchsetzung, „Policy Auditor" für die Übereinstimmung mit Unternehmensrichtlinien, und „Infinity Identity" für einheitliche Identitäten. Ein Cloud-Service verwaltet zentralisierte Identitäten, während „Infinity AIOps" Gateway-Überwachung mit proaktiver Fehlervermeidung bietet.

Kremer führt weiter aus: „In den letzten zwei Jahren haben wir begonnen, mehr und mehr generative KI und agentenbasierte KI einzusetzen, die wir in jedes unserer Produkte einbetten, um die Produktivität unserer Admin-Benutzer zu verbessern. Denn sie müssen proaktiver sein und haben mehr Warnmeldungen und Angriffe zu bewältigen."

Wenn Nataly Kremer über Produktentwicklungen redet, spricht sie immer wieder die Themen „Einfachheit" und „Schlichtheit" an. Das sei bei den Produkteinführungen von hoher Bedeutung. Sie sieht in KI einen Weg zu dieser Vereinfachung: „Ich denke, KI ist ein großartiger Weg, um Einfachheit zu erreichen. Es ist eine richtige Abkürzung."

Die kritische Herausforderung bestehe darin, die Verlässlichkeit dieser KI-Systeme ohne Halluzinationen zu gewährleisten, was es von anderen Technologie-Entwicklungen unterscheidet. Das ist gerade bei einem so sensiblen Thema wie der Cybersecurity unabdingbar.

Fokus auf Hybrid-Mesh-Network-Architektur

Ein wesentlicher Entwicklungsschwerpunkt liegt bei Check Point zudem auf der Hybrid-Mesh-Network-Architektur. Diese Technologie vereint verschiedene Netzwerktypen, um maximale Flexibilität und Leistungsfähigkeit zu erzielen. Diese Architektur wird für ein einheitliches Management über On-Premises, Cloud und SASE (Secure Access Service Edge) genutzt. Die integrierte GenAI Productivity ersetzt komplexe manuelle Verwaltungsaufgaben durch

Natural Language und autonome KI-Systeme.

Schutz vor den dunklen Seiten der KI

Auf der anderen Seite arbeitet Check Point daran, Unternehmen vor den Risiken der eigens verwendeten KIs zu schützen. Kremer erklärt: „Wir haben ein Tool, das sicherstellt, dass man keine Anwendung benutzt, die man nicht unterstützen möchte. Es stoppt die Kommunikation sofort, was meiner Meinung nach wichtig ist, da es viele betrügerischen KI-Lösungen gibt. Sie sehen aus wie ChatGPT, sind es aber in Wirklichkeit nicht.

Sie sieht hier eine große Nachfrage: „Ich denke, das ist eine der häufigsten Anfragen von Kunden, die sich vor Gen AI schützen wollen. Ich glaube, CISOs haben das Gefühl, dass sie generative KI einführen müssen, da sie nicht als letzte Organisation ohne diese Technologie dastehen und die damit verbundenen Produktivitätssteigerungen verpassen wollen." Eine automatische Erkennungsfunktion ist notwendig, um präzise zu identifizieren, welche LLM-Modelle wie eingesetzt werden, damit angemessene Schutzmaßnahmen gegen die damit verbundenen vielfältigen Risiken implementiert werden können.

Die realen Gefahren KI-gestützter Cyberangriffe

Während Nataly Kremer und ihr Team die Schutzmaßnahmen und Produktentwicklungen bei Check Point voranbringen, sieht die Threat-Intelligence-Abteilung des Unternehmens bereits die konkreten Bedrohungen, gegen die diese Sicherheitsmechanismen entwickelt werden. Sergey Shykevich, Threat Intelligence Group Manager bei Check Point, bestätigt die Dringlichkeit der von Kremer beschriebenen Maßnahmen anhand realer Bedrohungsdaten.

„Wir sehen mehrere Bereiche, in denen Cyberkriminelle KI einsetzen, um ihre Operationen zu verbessern", erklärt Shykevich. Besonders in der Identitätsfälschung sei KI bereits weit verbreitet.

Ein Beispiel: Während russischsprachige Bedrohungsakteure früher auf menschliche Übersetzer angewiesen waren, nutzen sie heute fortschrittliche KI-Übersetzungstools. „Dadurch wurden all diese Operationen viel effizienter und persönlicher", so Shykevich.

Der Fall FuncSec: Wenn KI Ransomware schreibt

Ein besonders alarmierendes Beispiel entdeckte Check Point mit der Ransomware-Gruppe FuncSec. „Im Dezember war sie die Nummer eins unter den Top-Ransomware-Gruppen, gemessen an der Anzahl der Opfer, die sie auf ihrer Dark-Web-Seite veröffentlichten", erläutert Shykevich.

Bei der Code-Analyse stellten die Experten ungewöhnliche Muster fest: Der Code wirkte ´zu sauber für einen Menschen`. Der Verdacht auf KI-generierte Malware bestätigte sich im direkten Kontakt mit dem Akteur. „Er betrachtete sich nicht als Programmierer", berichtet Shykevich. „Als Entwickler muss er nur die richtigen Tools nutzen - entweder durch andere Personen, die mit der Entwicklung vertraut sind, oder eben generative KI."

> ES GIBT LEIDER NOCH KEINE PERFEKTEN TOOLS, UM ZU ERKENNEN, OB EIN VIDEO ODER EINE AUDIONACHRICHT MIT KI ERSTELLT WURDE.
>
> **Sergey Shykevich, Threat Intelligence Group Manager, Check Point Software Technologies, www.checkpoint.com**

Das Beunruhigende: Trotz technisch einfacher Konzeption ist die Ransomware effektiv. „Sie verschlüsselt die Daten, stört Dienste auf Maschinen, sie funktioniert. Dabei sind die Cyberkriminellen dahinter technisch auf einem ziemlich niedrigen Niveau", betont Shykevich. „Trotzdem konnten sie mithilfe generativer KI eine erfolgreiche, funktionsfähige Ransomware erstellen." Shykevich nennt diese technisch weniger versierten Hacker ´Script Kiddies`. Damit bezeichnet man in der Szene Personen, die nicht über die notwendigen Kenntnisse verfügt, um selbst Programme zu entwickeln, und daher vorgefertigte Skripte und Tools von anderen verwendet, um Computer- und Netzwerke zu hacken oder zu kompromittieren.

Die wachsende Deepfake-Gefahr

Die Identifikation von Deepfakes stellt eine zunehmende Herausforderung dar. Auf die Frage nach Erkennungsmöglichkeiten antwortet Shykevich ehrlich: „Das ist eine schwierige Frage. Es gibt leider noch keine perfekten Tools, um zu erkennen, ob ein Video oder eine Audionachricht mit KI erstellt wurde. Es gibt nichts auf dem Markt, was mit 100-prozentiger Sicherheit feststellen kann, ob es sich um einen Deepfake handelt oder nicht."

BEIM THEMA BEDROHUNGSABWEHR STEHEN WIR ALLE AUF DERSELBEN SEITE. DIESELBE RANSOMWARE GREIFT VIELE LÄNDER IN EUROPA, DEN USA, IM ASIATISCH-PAZIFISCHEN RAUM AN.

Lotem Finkelstein, Head of Threat Intelligence, Check Point Software Technologies
www.checkpoint.com

Bilaterale Bewegungen

Lotem Finkelstein, Head of Threat Intelligence bei Check Point Software, identifiziert Ransomware weiterhin als eine der größten Bedrohungen. Zwei zentrale Risiken bereiten ihm besonders Sorgen: die Sicherheitsrisiken der Remote-Arbeit und die komplexe Verbindung von Cloud- und On-Premises-Umgebungen. „Wir sehen immer mehr Fälle, in denen es eine bilaterale Bewegung zwischen diesen beiden Umgebungen gibt", erklärt Finkelstein. „Das ist besorgniserregend, denn meistens sind diejenigen, die dies tun, auf einem hohen technischen Level."

Für eine effektivere Bedrohungsabwehr fordert Finkelstein daher eine verstärkte internationale Zusammenarbeit. „Hier steht jeder auf derselben Seite. Dieselbe Ransomware greift viele Länder in Europa, den USA, im asiatisch-pazifischen Raum an."

Fazit

Eins ist mittlerweile klar: KI nimmt eine Schlüsselrolle ein, sowohl als Angriffs- als auch als Verteidigungswerkzeug. Sie verändert die Spielregeln der Cybersicherheit auf beiden Seiten fundamental. Die wahre Stärke auf der Seite der Verteidiger liegt aber nicht allein in der Technologie, sondern in der strategischen Verbindung von Entwicklung, Forschung und praktischer Anwendung. Check Point will mit dem ganzheitlichen Ansatz demonstrieren, dass effektive Cybersicherheit im KI-Zeitalter möglich ist.

Lars Becker
www.it-daily.net

IDENTITÄTSBETRUG

IM SPANNUNGSFELD ZWISCHEN SICHERHEIT UND BENUTZERERLEBNIS

Entrust und Docusign haben die Ergebnisse einer gemeinsamen Marktuntersuchung veröffentlicht. Die internationale Studie untersucht die steigenden Kosten von Identitätsbetrug und die Herausforderungen für Unternehmen im Spannungsfeld zwischen Sicherheit und Benutzererlebnis.

Der Bericht „The Future of Global Identity Verification" belegt, dass Identitätsbetrug weltweit und branchenübergreifend eine wachsende Bedrohung darstellt. Mehr als zwei Drittel (69 %) der befragten Unternehmen berichten von einem Anstieg bei Betrugsversuchen. So entstehen Unternehmen mit mehr als 5.000 Mitarbeitern durch Identitätsdiebstahl direkte Kosten in Höhe von durchschnittlich 12 Millionen Euro pro Jahr, wobei die finanziellen Verluste mit zunehmender Unternehmensgröße exponentiell ansteigen.

Mit der Zunahme von KI-gestütztem Betrug werden die Angriffe raffinierter und häufiger. Laut der Studie gaben 51 Prozent der Befragten an, dass Betrug am häufigsten im Zusammenhang mit der Verwendung von Benutzernamen und Passwörtern auftritt – was die Anfälligkeit einfacher, einstufiger Authentifizierungsverfahren unterstreicht. Im Gegensatz dazu berichteten nur 21 Prozent der Unternehmen von Betrugsversuchen gegen die Gesichtsbiometrie mit Lebenderkennung. Fortschrittliche Authentifizierungslösungen reduzieren betrügerische Absichten von Kriminellen bereits proaktiv.

Einsparungen durch tärkere Identitätssicherung

Da sich die Betrugstaktiken rasant weiterentwickeln, investieren Unternehmen zunehmend in fortschrittlichere Sicherheitsmaßnahmen, auch wenn sie Bedenken hinsichtlich der Benutzerfreundlichkeit haben. Obwohl 58 Prozent der Befragten angeben, dass strengere Betrugskontrollen die Verbraucher frustrieren könnten, erkennen die meisten den Nutzen von Investitionen in die Identitätsprüfung (IDV): 70 Prozent sind der Meinung, dass Investitionen in Technologie der beste Weg sind, um finanzielle Risiken durch Identitätsbetrug zu minimieren. 74 Prozent planen, ihre Investitionen in Zukunft zu erhöhen.

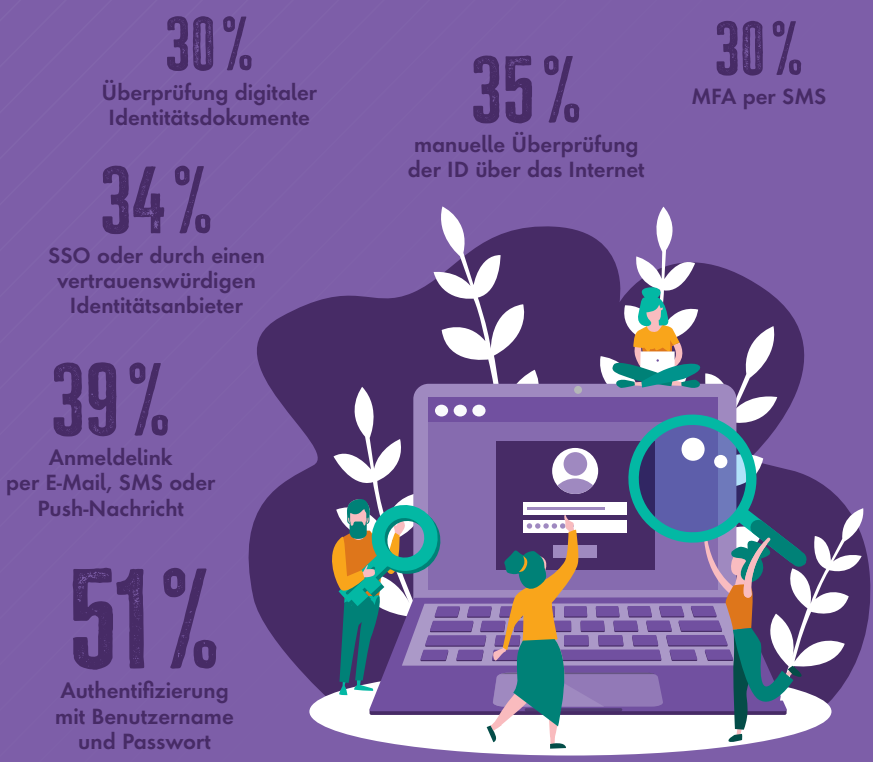
Unternehmen, die in IDV-Lösungen investieren, beziffern ihre Kosteneinsparungen hierdurch auf durchschnittlich 7,5 Millionen Euro pro Jahr.

www.entrust.com

MEHR WERT

The Future of Global Identity Verification

GEBEN SIE BITTE FÜR JEDE ART DER BENUTZERAUTHENTIFIZIERUNG AN, OB BETRUG BEI DIESER TECHNIK HÄUFIGER VORKOMMT



Stärker gemeinsam

SO ARBEITEN IT- UND SICHERHEITSTEAMS EFFEKTIVER ZUSAMMEN

In den letzten Jahren ist die Zusammenarbeit zwischen IT- und Sicherheitsabteilungen immer enger geworden. Dies ist unter anderem auf Veränderungen in den Unternehmensstrukturen (der CIO wird praktisch zum Leiter von IT und Cybersicherheit) und die Konvergenz der benötigten Kompetenzen in beiden Bereichen, IT und Sicherheit zurückzuführen.

Während eine enge Kooperation dieser beiden Teams oft bereits Teil einer modernen Unternehmensstrategie geworden ist, stellt eine gute Umsetzung dieser Philosophie Unternehmen weiterhin vor große Herausforderungen. Die fehlende Abstimmung zwischen beiden Teams bewirkt nicht nur, dass Potenziale nicht vollständig ausgeschöpft werden, sondern sie birgt auch Geschäftsrisiken mit sich. Andererseits reduziert die Zusammenarbeit zwischen IT- und Sicherheitsabteilungen Kommunikationssilos und gleicht die Ziele beider Abteilungen an, wodurch die Arbeitsprozesse im jeweiligen Unternehmen optimiert werden können.

Hier sind einige Möglichkeiten, wie Unternehmen die Kooperation zwischen IT- und Sicherheitsabteilungen optimieren, Ziele aufeinander abstimmen und die Kommunikation untereinander verbessern können.

IT- UND SICHERHEITS-TEAMS BRINGEN ÄHNLICHE KOMPETENZEN MIT. WIR SEHEN EINEN KLAREN TREND, DASS UNTERNEHMEN GEZIELT TALENTE EINSTELLEN, DIE DIE LÜCKE ZWISCHEN BEIDEN BEREICHEN SCHLIESSEN.

Mike Arrowsmith, Chief Trust Officer (CTO), NinjaOne, www.ninjaone.com

Einheitliche Zielstellungen

Der erste Schritt zu einer engeren Zusammenarbeit besteht darin, festzulegen, was jedes Team erreichen möchte. Das klingt einfach, ist aber oft eine große Herausforderung. Es müssen klare und objektive Ziele festgelegt werden, Rollen und Verantwortlichkeiten müssen verstanden werden und alle Teammitglieder müssen wissen, was von ihnen erwartet wird.

Die unterschiedlichen Interessen und Ziele der Abteilungsleiter können eine Herausforderung für die Zusammenarbeit zwischen IT- und Sicherheitsabteilungen darstellen. Für CISOs oder Leiter des Sicherheitsteams sind die Sicherheitslage des Unternehmens und damit zusammenhängende Vorfälle relevant, während für CIOs oder Leiter der IT-Abteilung Produktivität, Innovation und Kosteneffizienz oberste Priorität haben.

Diese Perspektive wandelt sich jedoch zunehmend, da wir immer häufiger sehen, dass CISOs direkt an CIOs berichten, was zu einer engen Abstimmung der Ziele und einer verstärkten Zusammenarbeit führt.

Unabhängig von der Organisationsstruktur ist es für CIOs und CISOs nach wie vor wichtig, eine Reihe von Kennzahlen und messbaren Zielen festzulegen, auf die ihre Teams hinarbeiten, um eine kontinuierliche Abstimmung und klare Erwartungen zu gewährleisten.

Nahtlose Kommunikation für eine optimierte Zusammenarbeit

Eine engere Zusammenarbeit kann durch eine verbesserte Kommunikation zwischen IT- und Sicherheitsabteilungen erreicht werden.

Hier können Planspiele ein nützlicher Ansatz sein. Zusammen mit einer klaren Dokumentation und Berichterstattung machen sie Überschneidungen und Lücken in der IT- und Sicherheitsabdeckung für bestimmte Szenarien sichtbar. Auf der Grundlage dieser Übungen können beide Abteilungen klare Priori-

täten setzen, Einblicke in die Arbeit der einzelnen Teams gewinnen und Lösungen für potenzielle Probleme entwickeln.

Synergien durch gemeinsame Fähigkeiten

Kosteneinsparungen und sich überschneidende Fähigkeiten haben in den letzten Jahren ebenfalls zu einer engeren Abstimmung zwischen IT- und Sicherheitsteams geführt. Durch die schwächelnde Konjunktur und den fortschreitenden IT-Fachkräftemangel suchen Unternehmen nach Personen sowohl mit IT- als auch mit Cybersecurity-Kenntnissen.

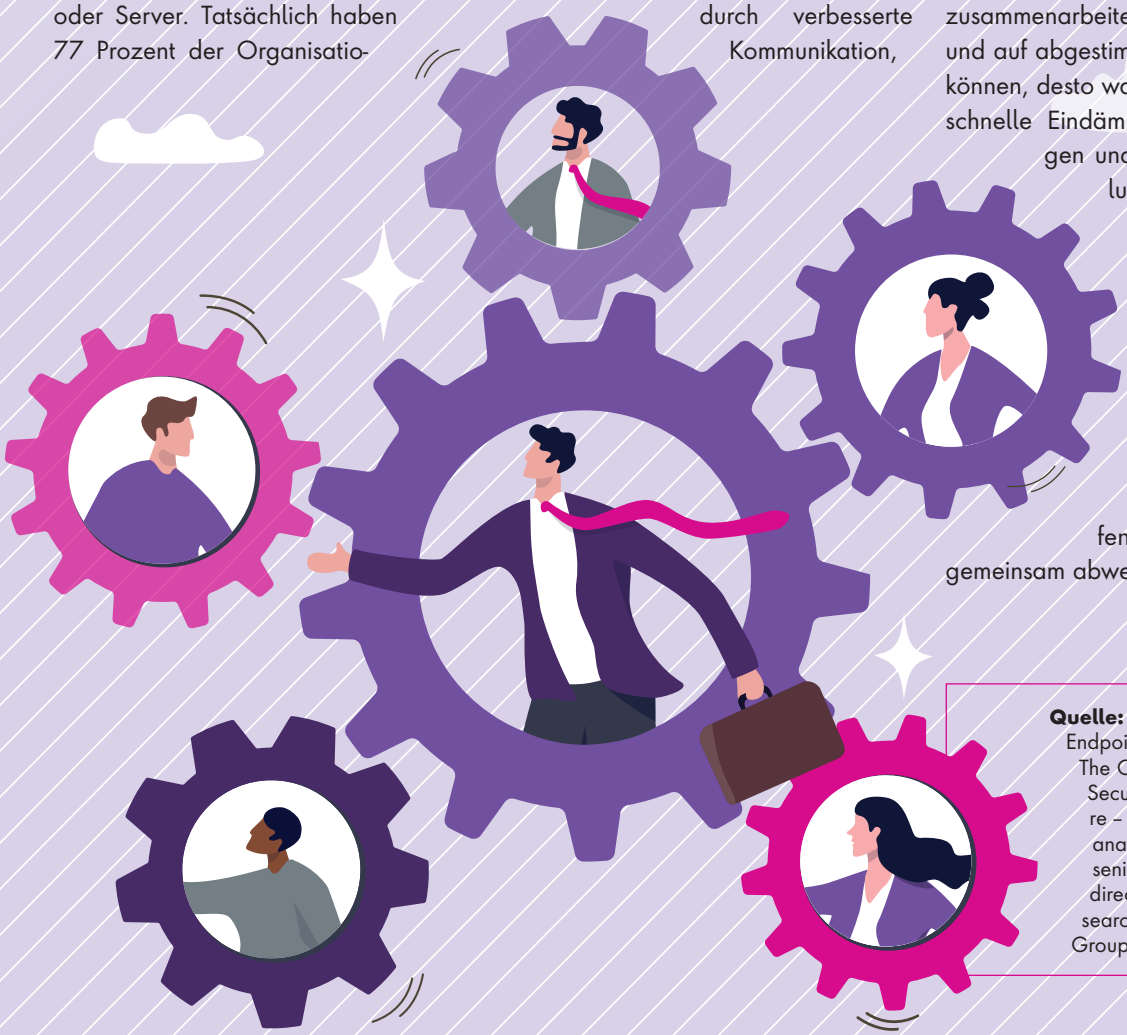
Eine zunehmende Anzahl von Cybersicherheitsvorfällen steht im Zusammenhang mit einem Laptop, Desktop oder Server. Tatsächlich haben 77 Prozent der Organisationen einen Cyberangriff erlebt, der über die Ausnutzung eines unbekannten, nicht verwalteten oder schlecht verwalteten Endpunkts begann. * Die gute Nachricht ist, dass Beschäftigte, die sowohl über IT- als auch über Sicherheitskenntnisse verfügen, wahrscheinlich am geeignetsten für die Verwaltung dieser Endpunkte sowie für die Untersuchung von Sicherheitsverletzungen sind. Durch solche sich ergänzenden Fähigkeiten innerhalb der Teams können Unternehmen Zeit und Ressourcen einsparen und sich besser auf die Erfüllung dieser beiden Funktionen abstimmen.

Dies führt zu einer Konsolidierung der eingesetzten IT- und Sicherheitslösungen und gleichzeitig zu einer allgemeinen Risikoreduzierung durch verbesserte Kommunikation, abgestimmte Strategien und bessere Transparenz in beiden Teams.

Ausblick

Cybersicherheitsvorfälle sind die neue Normalität und diese Situation wird sich in Zukunft weiter verschärfen. Der wahre Maßstab für Erfolg ist nicht das Verhindern von Sicherheitsverletzungen, sondern deren zügige Eindämmung, sobald sie verübt werden. Je besser IT- und Sicherheitsabteilungen zusammenarbeiten, kommunizieren und auf abgestimmte Ziele hinarbeiten können, desto wahrscheinlicher ist eine schnelle Eindämmung von Bedrohungen und somit die Sicherstellung der Geschäftskontinuität von Unternehmen. Für eine solche schnelle Reaktion müssen IT- und Sicherheitsabteilungen zusammenarbeiten, um zügig Entscheidungen zu treffen und Cyberangriffe gemeinsam abwehren zu können.

Mike Arrowsmith



Quelle: *ESG: Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure – Dave Gruber, principal analyst; Gabe Knuth, senior analyst; Bill Lundell, director of syndicated research; Enterprise Strategy Group; May 2023

Insider Threats in den Griff bekommen

EINE FRAGE DER UNTERNEHMENSKULTUR

Cybersicherheit wird oft als rein technisches Problem betrachtet, doch tatsächlich spielen menschliche Faktoren eine entscheidende Rolle. In einer Studie von Proofpoint gaben 72 Prozent der deutschen CISOs an, dass menschliches Versagen die größte Cybersicherheitslücke in ihren Organisationen darstellt. Eine der größten Bedrohungen für die Datensicherheit eines Unternehmens geht nicht von Hackern oder Malware aus, sondern von den eigenen Mitarbeitern, Partnern und Auftragnehmern: Insider Threats sind ein wachsendes Problem, das nicht nur technische Lösungen, sondern auch eine starke Unternehmenskultur erfordert.

Spannungsfeld zwischen Vertrauen und Kontrolle

Unternehmen stehen vor der Herausforderung, ein Gleichgewicht zwischen Vertrauen und Kontrolle zu finden. Einerseits möchten sie ihren Mitarbeitern die Freiheit geben, produktiv und innovativ zu arbeiten. Andererseits müssen sie sicherstellen, dass sensible Daten geschützt bleiben. Dieses Spannungsfeld wird durch die zunehmende Nutzung von Cloud-Diensten und hybriden Arbeitsmodellen zusätzlich aufgeladen. Mitarbeiter arbeiten heute überall: im Büro, zu Hause oder in einem Café. Dabei nutzen sie eine Vielzahl von Geräten, von firmeneigenen Laptops bis hin zu privaten Smartphones.

Ein fiktives Beispiel verdeutlicht dieses Dilemma: Ein Entwickler eines Technologieunternehmens nutzt ChatGPT, um ein Codeproblem zu lösen. Dabei gibt

INSIDER THREATS SIND EIN WACHSENDES PROBLEM, DAS NICHT NUR TECHNISCHE LÖSUNGEN, SONDERN AUCH EINE STARKE UNTERNEHMENSKULTUR ERFORDERT.

Miro Mitrovic,
Area Vice President DACH, Proofpoint,
www.proofpoint.com

er vertrauliche Informationen preis, die später missbraucht werden könnten. Solche Vorfälle – nicht nur aus dem Bereich der Schatten-KI – zeigen, wie wichtig es ist, klare Richtlinien einzuführen und Schulungen abzuhalten, um Mitarbeiter für Risiken zu sensibilisieren. Dabei zeigt sich ein weiteres Problem: Viele Mitarbeiter sehen Sicherheitsrichtlinien als Hindernis an, das ihre Arbeit erschwert. Dies führt dazu, dass sie versuchen, diese Regeln zu umgehen – sei es aus Bequemlichkeit oder Zeitdruck.

Die Frage lautet also: Wie können Unternehmen Sicherheitsmaßnahmen implementieren, ohne die Produktivität ihrer Mitarbeiter zu beeinträchtigen? Die Antwort liegt in einer Kombination aus technologischen Lösungen und einer starken Sicherheitskultur.

Bedeutung einer starken Sicherheitskultur

Eine effektive Sicherheitsstrategie beginnt mit der Unternehmenskultur. Mitarbeiter müssen verstehen, warum bestimmte Sicherheitsmaßnahmen notwendig sind, und sich ihrer Verantwortung bewusst sein. Dies erfordert regelmäßige Schulungen, die nicht nur die technischen Aspekte abdecken, sondern auch ethische Fragen und Best Practices vermitteln. Entsprechend haben mehr als die Hälfte (62 %) der deutschen CISOs 2024 in die Schulung ihrer Mitarbeiter zu Best Practices in der Datensicherheit investiert, was eine Steigerung um 36 Prozent im Vergleich zum Vorjahr bedeutet. Doch Schulungen allein reichen nicht aus. Es geht darum, eine Kultur des Bewusstseins und der Verantwortlichkeit zu schaffen, in der jeder Mitarbeiter – unabhängig von seiner Position – versteht, dass er eine Schlüsselrolle für die Sicherheit des Unternehmens spielt.

Gleichzeitig sollten Unternehmen eine offene Kommunikationskultur fördern, in der Mitarbeiter potenzielle Sicherheitsprobleme melden können, ohne Angst vor Repressalien zu haben. Dies schafft ein Umfeld, in dem Sicherheitsfragen aktiv angegangen werden können, bevor sie zu größeren Problemen führen. Wenn beispielsweise ein Mitarbeiter bemerkt, dass ein Kollege sensible Daten auf eine ungeschützte

Plattform hochlädt, sollte er sich sicher fühlen, dies zu melden, ohne befürchten zu müssen, als „Whistleblower" stigmatisiert zu werden.

Eine solche Kultur erfordert auch ein Engagement der Führungsebene. Führungskräfte müssen nicht nur die Bedeutung von Cybersicherheit betonen, sondern auch selbst als Vorbilder agieren. Wenn Manager beispielsweise selbst Sicherheitsrichtlinien ignorieren oder umgehen, senden sie eine klare Botschaft an ihre Teams: Diese Regeln sind optional. Ein solches Verhalten untergräbt jede Bemühung, eine starke Sicherheitskultur aufzubauen.

Technologische Unterstützung

Technologie allein kann keine Sicherheitskultur schaffen, aber sie kann sie unterstützen. Moderne Data Loss Prevention (DLP)-Lösungen, die auf Verhaltensanalysen und künstlicher Intelligenz basieren, können verdächtige Aktivitäten erkennen und den Kontext liefern, der für fundierte Entscheidungen erforderlich ist. Beispielsweise können solche Systeme erkennen, wenn ein Mitarbeiter ungewöhnlich viele Dateien herunterlädt, und automatisch eine Warnung auslösen. Diese Warnung kann dann nicht nur an das IT-Team gesendet werden, sondern auch direkt an den Mitarbeiter, in Kombination mit einer kurzen Erklärung, warum diese Aktion problematisch erscheint. Auf diese Weise wird der Mitarbeiter nicht nur gewarnt, sondern auch geschult.

Darüber hinaus können adaptive Sicherheitsmaßnahmen implementiert werden, die sich an das Risiko anpassen. Ein Unternehmen kann z.B. einen Mitarbeiter, der gerade gekündigt hat, stärker im Auge behalten, um potenziellen Datenmissbrauch zu verhindern. Wie sich in einer Untersuchung zeigte, waren 87 Prozent der ungewöhnlichen Datei-Exfiltrationen bei Cloud-Nutzern auf ausscheidende Mitarbeiter zurückzuführen. Zudem berichteten 57 Prozent der deutschen Sicherheitsverantwortlichen von einem signifikanten Verlust sensibler Daten, wobei 77 Prozent ausscheidende Mitarbeiter als mitursächlich angaben. Dies unterstreicht die Notwendigkeit präventiver Sicherheitsstrategien zusätzlich.

Ein weiterer Vorteil moderner Technologien ist ihre Fähigkeit, Fehler zu minimieren, ohne die Produktivität zu beeinträchtigen. So können beispielsweise intelligente E-Mail-Systeme verhindern, dass E-Mails mit sensiblen Anhängen an externe Empfänger gesendet werden, indem sie den Absender auffordern, die Empfängeradresse zu überprüfen. Solche kleinen Eingriffe können einen großen Unterschied machen, ohne den Arbeitsfluss zu stören.

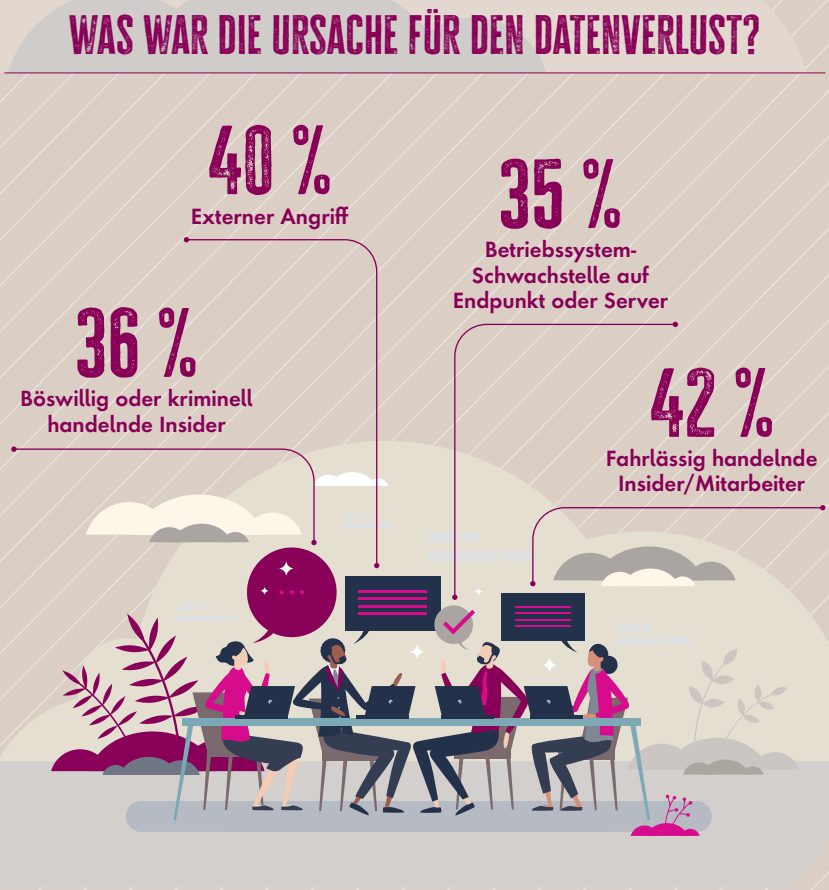
Insider Threats im Kontext von Drittanbietern und Partnern

Ein oft übersehener Aspekt von Insider Threats ist die Rolle von Drittanbietern und Partnern. Viele Unternehmen verlassen sich auf externe Dienstleister, um bestimmte Aufgaben zu erledigen, sei es in der IT, im Kundenservice oder in der Logistik. Diese externen Akteure haben oft Zugang zu sensiblen Daten, sind jedoch nicht immer so gut geschult oder abgesichert wie interne Systeme und Mitarbeiter.

Ein klassisches Beispiel ist ein externer IT-Dienstleister, der Zugang zu den Servern eines Unternehmens hat. Wenn dieser Dienstleister nicht über angemessene Sicherheitsrichtlinien verfügt oder seine Mitarbeiter nicht ausreichend schult, können sensible Daten leicht kompromittiert werden. In einigen Fäl-

len können böswillige Akteure absichtlich Schwachstellen ausnutzen, um Daten zu stehlen oder zu sabotieren.

Um dieses Risiko zu minimieren, sollten Unternehmen strenge Richtlinien für den Umgang mit Drittanbietern einführen. Dazu gehört, dass alle externen Partner vertraglich verpflichtet werden, bestimmte Sicherheitsstandards einzuhalten. Darüber hinaus sollten Unternehmen regelmäßig überprüfen, ob diese Standards tatsächlich eingehalten werden. Moderne DLP-Lösungen können auch hier helfen, indem sie Aktivitäten von Drittanbietern überwachen und ungewöhnliches Verhalten melden.



Proaktive Maßnahmen zur Reduzierung von Insider Threats

Neben der Implementierung moderner Technologien und der Förderung einer starken Sicherheitskultur gibt es weitere Maßnahmen, die Unternehmen ergreifen können, um Insider Threats zu reduzieren:

➤ **Regelmäßige Überprüfung von Zugriffsrechten:** Mitarbeiter sollten nur Zugriff auf die Daten haben, die sie für ihre Arbeit benötigen. Regelmäßige Audits können sicherstellen, dass ehemalige Mitarbeiter oder externe Partner keinen Zugriff mehr haben.

➤ **Etablierung eines robusten Offboarding-Prozesses:** Wenn ein Mitarbeiter das Unternehmen verlässt, sollten alle Zugriffsrechte sofort widerrufen werden. Dies verhindert, dass ehemalige Mitarbeiter weiterhin auf sensible Daten zugreifen können.

➤ **Anonyme Meldekanäle:** Mitarbeiter sollten die Möglichkeit haben, potenziell riskantes Verhalten anonym zu melden. Dies kann dazu beitragen, Probleme frühzeitig zu erkennen und zu beheben.

➤ **Simulation von Insider-Bedrohungen**: Ähnlich wie bei Phishing-Simulationen können Unternehmen Test-Szenarien erstellen, um festzustellen, wie gut ihre Mitarbeiter und Systeme auf Insider Threats vorbereitet sind.

Es gelingt nur mit Mensch und Technologie im Einklang

Insider Threats sind nicht nur ein technisches, sondern auch ein kulturelles Problem. Sie erfordern einen ganzheitlichen Ansatz, der sowohl die technischen als auch die menschlichen Aspekte berücksichtigt. Während moderne Technologien wie DLP-Lösungen und Verhaltensanalysen wichtige Werkzeuge im Kampf gegen Insider Threats sind, ist es letztendlich die Unternehmenskultur, die den Unterschied macht.

Unternehmen, die eine starke Sicherheitskultur fördern, regelmäßige Schulungen anbieten und moderne Technologien einsetzen, sind besser gerüstet, diese Bedrohungen zu bewältigen. Letztendlich geht es darum, ein Umfeld zu schaffen, in dem Sicherheit nicht als Hindernis, sondern als integraler Bestandteil des Geschäftserfolgs gesehen wird. Nur so können Unternehmen das Vertrauen ihrer Mitarbeiter, Kunden und Partner stärken und ihre sensiblen Daten effektiv schützen.

Miro Mitrovic

Quantenresistente Maschinenidentitäten

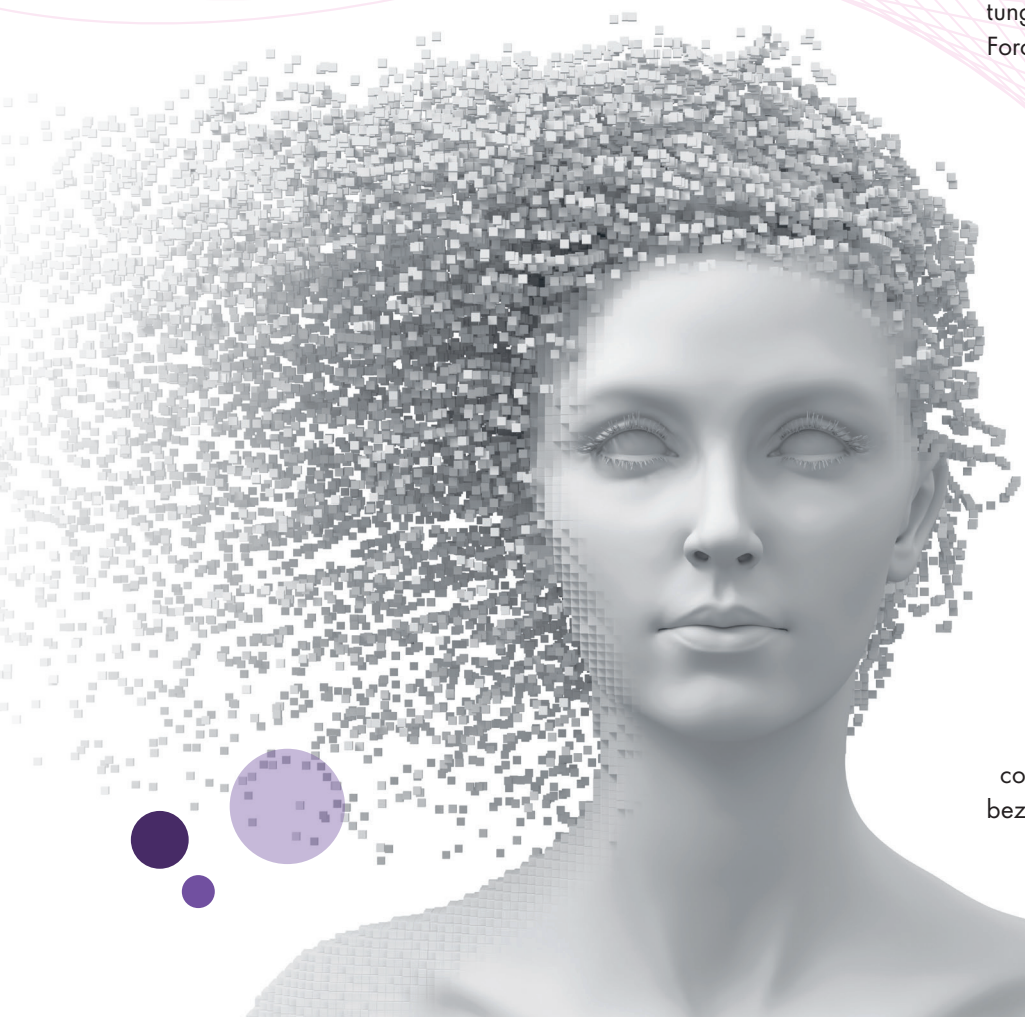
NEUE HERAUSFORDERUNGEN FÜR INDUSTRIE 4.0

Um sämtliche Vorteile einer digitalisierten und vernetzten Industrie 4.0 voll zum Einsatz bringen zu können, müssen Anlagen, Maschinen und IIoT-Geräte auf sicherem Wege untereinander, mit ihren OT- und IT-Systemen sowie mit ihren menschlichen Anwendern interagieren können. Damit ein solcher Datenaustausch gelingen kann, sind sie mit digitalen Identitäten, sogenannten Maschinenidentitäten, ausgestattet. Diese ermöglichen ihnen eine verschlüsselte Kommunikation – auf Basis kryptografischer Schlüssel und digitaler Zertifikate.

Die versandten und empfangenen Daten können so vor unerlaubten Einsichtnahmen und Manipulationen, die vernetzten Anlagen, Maschinen und IIoT-Geräte vor Kompromittierungen, die den Betrieb beeinträchtigen, stören oder sogar gefährden könnten, geschützt werden. Als Algorithmen kommen dabei meist die Kryptographie-Systeme Rivest-Shamir-Adleman (RSA) und Elliptic Curve Cryptography (ECC), die neben Computernetzwerken auch in der Absicherung der Internetkommunikation eine wichtige Rolle spielen, zum Einsatz – bislang mit großem Erfolg. In wenigen Jahren schon dürfte sich das aber fundamental ändern.

Die Kryptographie-Risiken

Bereits Anfang der 2030er Jahre, so die derzeitigen Prognosen, dürften erste Quantencomputer auf dem Markt erhältlich sein, deren Rechenleistung traditionellen Kryptographie-Systemen gefährlich werden könnte. Staatlichen und halbstaatlichen, nach kurzer Zeit sicherlich aber auch kriminellen Akteuren wird dann die enorme Rechenleistung des Quantencomputing für Brute Force-Angriffe zur Verfügung stehen.



Unter Zuhilfenahme des Shor-Algorithmus, eines Quantenalgorithmus, der große Zahlen exponentiell schneller faktorisieren kann als jedes bekannte andere Verfahren, werden sich gerade die derzeit populärsten Algorithmen, wie RSA und ECC, dann deutlich schneller knacken lassen, als es mit traditionellen Rechnern jemals möglich gewesen wäre. Ein Umstand, der für Unternehmen der Industrie 4.0 nicht erst in Zukunft zum Problem werden dürfte. Haben Angreifer doch längst begonnen, den künftigen Einsatz eines Quantencomputers in ihre Planungen mit einzubeziehen.

„Steal now, harvest later" ist längst zum geflügelten Wort geworden – nicht nur unter PQC-Cybersicherheitsexperten. Verschlüsselte Daten der Industrie 4.0 werden heute entwendet, um dann in einigen Jahren entschlüsselt und zur Vorbereitung weiterer Angriffe nutzbar gemacht zu werden – zum Beispiel um Produktionsgeheimnisse zu stehlen, eine Produktionsstraße zu manipulieren oder gleich ganz zum Erliegen zu bringen.

Quantenresistente Algorithmen

Intensiv wird schon seit einigen Jahren an der Entwicklung quantenresistenter kryptografischer Verfahren, als sicheren Nachfolgern von RSA und ECC, gearbeitet. Im vergangenen Jahr hat das National Institute of Standards and Technology (NIST) die drei ersten Standards zur Post Quantum Cryptographie (PQC) genehmigt: die Federal Information Processing Standards (FIPS) 203, 204 und 205. Für jedes Unternehmen, vor allem aber für Unternehmen der Industrie 4.0, wird die langfristige Sicherheit der eigenen Maschinenidentitäten von der raschen Umstellung auf diese neuen Algorithmen abhängen. Das Problem: viele Industrieunternehmen sind, wenn es um ihre PQC geht, noch längst nicht da, wo sie eigentlich schon sein sollten.

Umstellung schreitet nur langsam voran

In Keyfactors The State of Quantum Readiness in 2024-Report äußerten 80 Prozent der befragten IT-Entscheider Zweifel, ob es ihnen gelänge, die Kryptographie von IT, OT, IoT und IIoT ihres Unternehmens auf die anstehenden Risiken und Veränderungen ausreichend vorzubereiten. Laut einer Ponemon Institute-Studie vom vergangenen Jahr schreiten die Vorbereitungen weltweit und branchenübergreifend nur langsam voran. Ganze 27 Prozent der Befragten erklärten, sich noch überhaupt nicht mit Quantenbedrohungen beschäftigt zu haben. Nur 45 Prozent der befragten IT-Entscheider gaben an, dass ihr Unternehmen einen vollständigen Überblick über ihre kryptografischen Assets besitze. Und lediglich 50 Prozent erklärten, die erforderlichen Technologien zu besitzen, die zur Unterstützung der für PQC erforderlichen größeren Schlüssellängen und höheren Rechenleistung erforderlich sind.

DIE SYSTEMATISCHE VORBEREITUNG AUF DAS QUANTENZEITALTER, SIE HAT MIT EINEM MEHR AN TRANSPARENZ ZU BEGINNEN.

Jiannis Papadakis, Director of Solutions Engineering, Keyfactor, www.keyfaktor.com

Der Weg zur Quantenresistenz – Worauf es ankommt

Die systematische Vorbereitung auf das Quantenzeitalter, sie hat mit einem Mehr an Transparenz zu beginnen. Unternehmen müssen ein umfassendes Verständnis ihrer aktuellen kryptografischen Praktiken und Maschinenidentitäten gewinnen. Ein weiterer wichtiger Faktor ist der Ausbau der Flexibilität ihrer Kryptografie – ihre Fähigkeit, in Reaktion

auf neue Schwachstellen oder Standards, die im Einsatz befindlichen kryptografischen Algorithmen schnell und vollständig austauschen zu können. Mit der Notwendigkeit solcher Maßnahmen muss gerechnet werden. Während der Übergangsphase zum Quantenzeitalter beispielsweise, werden wahrscheinlich hybride Lösungen zum Einsatz kommen müssen.

Ein dritter wichtiger Faktor schließlich ist die Automatisierung. Automatisierte Prozesse können die Verwaltung der Infrastruktur und der Lebenszyklen von Zertifikaten drastisch vereinfachen. Ablaufende oder kompromittierte Maschinenidentitäten können rechtzeitig und umfassend erkannt und frühzeitig durch Post-Quantum-fähige Lösungen ersetzt werden. An der Implementierung einer automatisierten Public Key Infrastructure (PKI) samt Certificate Lifecycle Management (CLM) werden Unternehmen mit einer überdurchschnittlich großen Zahl an Maschinenidentitäten deshalb kaum herumkommen.

In 4 Schritten erfolgreich zu einer quantenresistenten Verschlüsselung

#1 Erstellung eines kryptografischen Inventars:
Ermitteln Sie, wo kryptografische Algorithmen verwendet werden, welche Zertifikate und Schlüssel anfällig sind und welche Abhängigkeiten in Ihrer Infrastruktur bestehen.

Verwenden Sie automatisierte Tools zum Scannen von Zertifizierungsstellen (CAs), Servern, Geräten, Quellcode und anderen Assets. Achten Sie darauf, dass bei dieser Bestandsaufnahme auch Ihre Rechneridentitäten berücksichtigt werden.

#2 Vorbereitung auf Krypto-Agilität:
Stellen Sie sicher, dass Ihre PKI hybride Zertifikate unterstützen kann, die sowohl klassische als auch Post-Quantum-Algorithmen nutzen.

Richten Sie Ihre kryptografische Infrastruktur so ein, dass sie sich an künftige Entwicklungen quantenresistenter Standards anpassen kann, und bereiten Sie sich darauf vor, Ihre Rechneridentitäten im Rahmen dieses Übergangs zu aktualisieren.

#3 Automatisierung des Lebenszyklusmanagements von Zertifikaten:
Verringern Sie das Risiko von Zertifikatsausfällen und Sicherheitslücken, indem Sie Ihre Ermittlung, Ausstellung und Erneuerung von Zertifikaten automatisieren.

Halten Sie Schritt mit den sich stetig weiterentwickelnden Sicherheitsstandards. Versetzen Sie Sich in die Lage, kryptografische Richtlinien zügig zu aktualisieren.

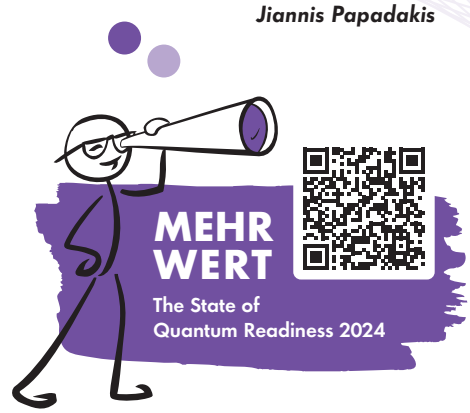
#4 Tests der Post-Quantum-Kryptografie:
Beginnen Sie mit dem Testen von PQC-Algorithmen in kontrollierten Umgebungen, um Leistung, Kompatibilität und etwaige Implementierungsprobleme zu festzustellen und zu bewerten.

Sammeln Sie erste praktische Erfahrungen, noch bevor die PQC-Einführung in vollem Umfang erforderlich ist. So stellen Sie sicher, dass Ihre Maschinenidentitätssysteme mit den neuen PQC-Algorithmen kompatibel sind.

Halten sich IT-Entscheider an diese vier Schritte, sind sie auf einem guten Weg, ihre IT-, OT- und IIoT-Umgebungen fit für

das Quantenzeitalter zu machen. Allerdings – und das muss ihnen klar sein – wird die Umstellung ein langer Prozess sein. In der Regel dauert es 8 bis 10 Jahre, bis quantensichere Algorithmen vollständig in einem Unternehmen implementiert sind. Angesichts der rasanten Fortschritte in der Quantencomputertechnologie – und da Angreifer, wie bereits erwähnt, schon heute im Hinblick auf die baldige Verfügbarkeit des Quantencomputings gezielt Daten stehlen und massenhaft sammeln – haben IT-Entscheider keine Zeit zu verlieren.

Jiannis Papadakis



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:
Mike Arrowsmith, Effie Bagourdi, Lars Becker, Christian Daum, Dr. Alexander Dotterweich, Gerald Eid, Dr. Silvia Knittl, Miro Mitrovic, Carina Mitzschke, Crystal Morin, Jiannis Papadakis, Silvia Parthier, Ulrich Parthier, Michael Veit, Dirk Wahlefeld, Grit Wasmund, Anthony Williams

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0,
Fax: 08104-6494-22

E-Mail für Leserbriefe: info@it-verlag.de
Homepage: www.it-daily.net

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

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

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

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

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

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

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

Erscheinungsweise: 6 x pro Jahr

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

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

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

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

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

CYBERSICHERHEIT AM SCHEIDEWEG

GRÜNDE FÜR DAS CYBERSICHERHEITS-DILEMMA IN UNTERNEHMEN

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

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

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

WHITEPAPER DOWNLOAD

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

IT MANAGEMENT DIGITALEVENT

GENERATIVE AI: ZUKUNFT DER TECHNOLOGIE

MITTWOCH, 04.06.2025 | AB 9UHR

#GenAI

Infos und Anmeldung

Eine Veranstaltung von itmanagement & it-daily.net

IT-EXPERTENWISSEN AUF KNOPFDRUCK

UNSERE

it-daily.net

ONLINE-EVENTS

FÜR DIE DIGITALE ZUKUNFT

JETZT ENTDECKEN!

IMMER AM PULS DER IT