it management

Der Motor für Innovation
Mai/Juni 2024

INKLUSIVE 48 SEITEN
it security

AB SEITE 17
appian

IT-MONITORING

Alles im Blick, alles unter Kontrolle

Alexander Wiedenbruch, USU GmbH

ZIEL

IT-VISION

IT ROADMAP 3.0

15. Mai 2024

Digitalevent

PROZESSE

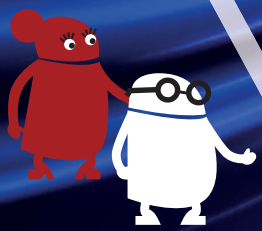
it-daily.net

Mehr erfahren

BUSINESS ANFORDERUNGEN

STRATEGIE

START



#Roadmap2024

Eine Veranstaltung von itmanagement & it-daily.net

MEHR FOKUS

LIEBE LESERINNEN UND LESER,

um ein erfolgreiches Unternehmen zu sein, sollte man immer alles im Blick und alles unter Kontrolle haben. Dass das nicht so einfach ist, merkt man schon an dem Wörtchen „sollte".

Man „sollte" mittlerweile gut auf die Einführung von NIS2 vorbereitet sein, man „sollte" sich mit dem Lieferkettensorgfaltsgesetz auseinandergesetzt haben, man „sollte" sich natürlich auch dringend um sein SAP-System kümmern, die Cyberabwehr aktuell halten oder beispielsweise die Migration in die Cloud vorantreiben.

Die Praxis sieht oft anders aus. Statt all diese Dinge wirklich im Blick zu haben, fehlt der Überblick. Was bleibt? Hilfloses Hände über dem Kopf zusammenschlagen! So endet es zumindest bei mir recht häufig – nicht, weil ich mich um oben genannte Themen kümmern müsste, sondern weil manchmal einfach zu viele Abteilungen zu viele Informationen auf einmal wollen, weil sich Termine und Besprechungen überlagern oder einfach nur der Posteingang überquillt.

Um im Unternehmen zum Beispiel den Überblick zu behalten, wäre die Einführung eines IT-Monitorings eine gute Idee. Für die Einhaltung von NIS2 sollte man sich vielleicht einen Spezialisten ins Team holen.

Und für meinen Arbeitsablauf? Da habe ich gelernt, dass man das wichtigste To-do in eine Fokuszeit legt. Eine Stunde fokussiertes Arbeiten, ohne Ablenkung, ohne Posteingang, ohne Chatfunktion, ohne Smartphone. Ich werde berichten, ob es funktioniert.

Herzlichst

Carina Mitzschke | Redakteurin it management & it security

INHALT

COVERSTORY

THOUGHT LEADERSHIP

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

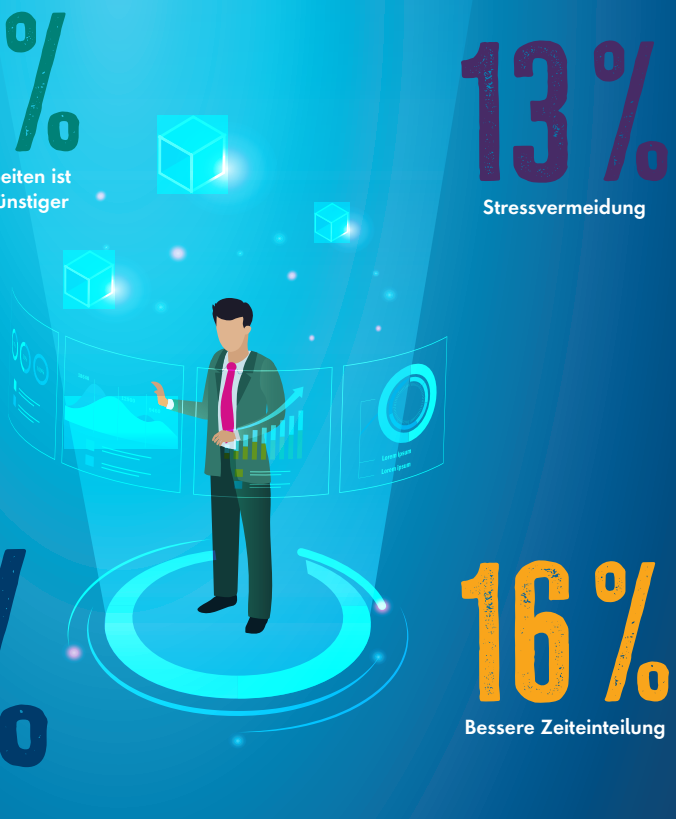
IT MANAGEMENT

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**

GRÜNDE FÜR DAS MEIDEN DES ARBEITSPLATZES



FÜHRUNGSKRÄFTESTUDIE

WIESO MITARBEITENDE DAS BÜRO MEIDEN

Ein Drittel der Führungskräfte stimmt der Aussage zu, dass Mitarbeitende im Homeoffice arbeiten wollen, weil sie nicht gerne ins Büro kommen. Hauptgründe dafür sind lange Arbeitswege und ein schlechtes Arbeitsklima. Zu diesem Ergebnis kommt der Hernstein Management Report, eine repräsentative Befragung von 1.500 Führungskräften in Deutschland und Österreich.

Gute Führungsarbeit kann insbesondere bei einem schlechten Arbeitsklima entgegenwirken. Leadership, welches auf Empathie und Einfühlungsvermögen setzt, kann die Produktivität positiv beeinflussen und die Stimmung im Unternehmen verbessern. Obwohl die befragten Führungskräfte diese Persönlichkeitsmerkmale als wichtig erachten, treffen diese nur bei rund 30 Prozent ihrer eigenen Führungskraft voll zu.

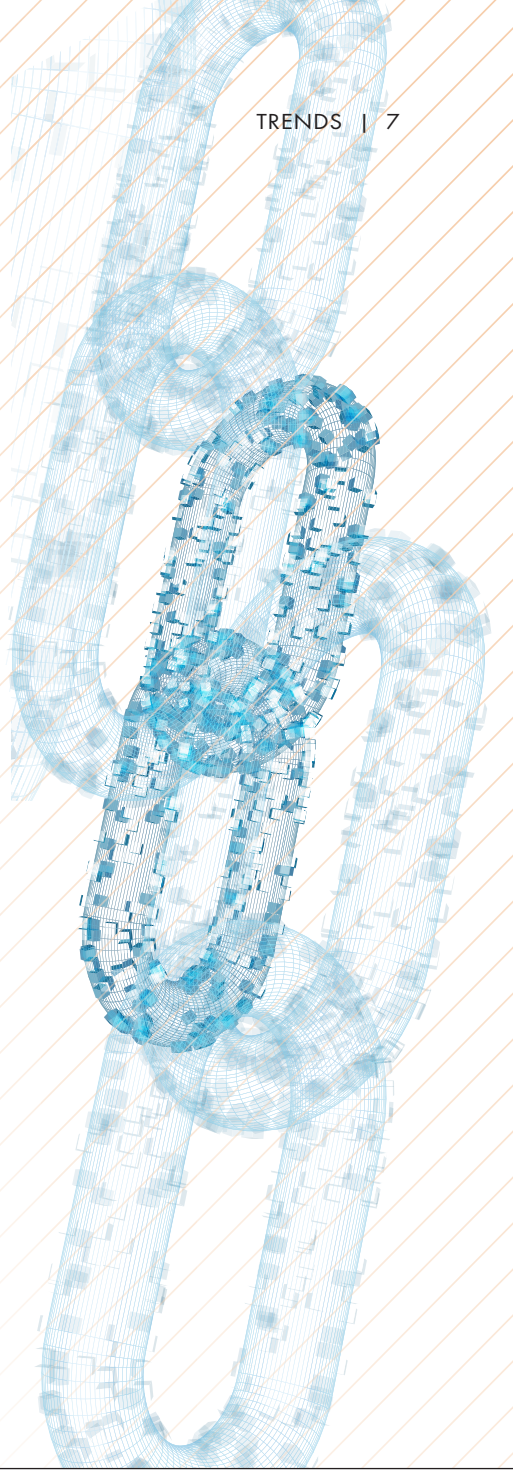
Noch ein interessantes Ergebnis findet sich im aktuellen Report: Leadership und Management werden von den befragten Führungskräften mehrheitlich, genau zu 56 Prozent, als Begriffe mit unterschiedlichen Funktionen gesehen. Dabei steht Management eher für die Sachebene und Leadership für die Beziehungsebene. Die häufigste Assoziation mit Management ist „klare Organisation", die von 37 Prozent der Befragten genannt wird. Mit Leadership wird an erster Stelle menschliches und soziales Verhalten in Verbindung gebracht, und zwar von 21 Prozent.

MEHR WERT
Hernstein Management Report 2024

www.hernstein.at

Blockchain

NUR NISCHENTECHNOLOGIE?



Blockchain-Anwendungen kommen bei weniger als einem Prozent der Unternehmen aus der DACH-Region zum Einsatz. Unternehmen aus der Finanzindustrie, dem Informations- und Kommunikationssektor sowie Beratungsfirmen gehören dabei zu den Unternehmen, die die Blockchain überdurchschnittlich häufig nutzen. So bilden sich insbesondere in den wichtigen Finanzzentren sogenannte Blockchain-Cluster. Das zeigt eine Studie des Zentrums für Europäische Wirtschaftsforschung, der TU München und der Universität Mannheim.

„Unsere Ergebnisse zeigen, dass die Blockchain von unter einem Prozent aller analysierten Unternehmen genutzt wird. Damit ist die Technologie auch 15 Jahre nach ihrer Einführung weiterhin eine Nischentechnologie, wobei die Finanzbranche aber auch ICT- und Beratungsunternehmen Blockchain durchaus stellenweise einsetzen“, sagt Prof. Dr. Hanna Hottenrott, Leiterin des ZEW-Forschungsbereichs „Innovationsökonomik und Unternehmensdynamik“ und Mitautorin der Studie.

Blockchain-Cluster

Die Bildung von Blockchain-Clustern in Finanzzentren habe mehrere Vorteile. Zunächst ermögliche die Nähe zu anderen Unternehmen, die an ähnlichen Technologien arbeiten, den Austausch von Wissen, Ressourcen und mache Kooperationen damit wahrscheinlicher. Auch die geringe Entfernung zu potenziellen Kunden spiele dabei eine wichtige Rolle. Zusätzlich kann die Nähe zu Finanzzentren den Zugang zu Kapital und Investitionen erleichtern. „Insgesamt tragen Blockchain-Cluster dazu bei, die Verbreitung der Blockchain-Technologie zu fördern, indem sie ein Umfeld schaffen, das Innovation, Zusammenarbeit und Wachstum in diesem Bereich unterstützt“, erläutert Prof. Dr. Hanna Hottenrott.

www.zew.de

CYBERBEDROHUNGEN

IMMER MEHR GERÄTE BETROFFEN

Industrieunternehmen in Deutschland sind laut einer aktuellen Analyse des Kaspersky ICS CERT nach wie vor im Visier von Cyberkriminellen: So war mehr als jeder sechste industrielle Computer 2023 von Cyberbedrohungen betroffen (18,3 Prozent).

Cyberbedrohungslandschaft im internationalen Vergleich
Im internationalen Vergleich werden Industrieunternehmen in Deutschland deutlich weniger angegriffen: Während hierzulande 18,3 Prozent der industriellen Computer betroffen waren, waren es weltweit knapp 32 Prozent. Weiterhin zeigt die Analyse regionale Unterschiede in der globalen Bedrohungslandschaft. In der zweiten Jahreshälfte des vergangenen Jahres gab es deutliche regionale Schwankungen im Prozentsatz der industriellen Computer, auf denen schädliche Aktivitäten blockiert wurden. Während in Afrika 38,2 Prozent betroffen waren, lag der Anteil in Nordeuropa lediglich bei 14,8 Prozent.

www.kaspersky.de

EMPFEHLUNGEN ZUM SCHUTZ VON OT-COMPUTERN

- Regelmäßig Sicherheitsanalysen von OT-Systemen durchführen
- Eine kontinuierlichen Schwachstellenbewertung und -sortierung als Grundlage für einen effektiven Schwachstellenmanagementprozess etablieren
- Alle Komponenten des OT-Netzes des Unternehmens rechtzeitig aktualisieren
- Ein ICS Threat Intelligence Reporting liefert detaillierte Informationen über schädliche Kampagnen, die auf Industrieunternehmen abzielen
- EDR-Lösungen einsetzen
- Dedizierte OT-Sicherheitsschulungen für IT-Sicherheitsteams und OT-Personal durchführen

MEHR WERT
ICS Threat Landscape Report

VIELFALT DER ENTDECKTEN MALWARE

(Quelle: Kaspersky – ICS Threat Landscape Report)

22 %
der Kunden sind bereit, auf eine komplett digitale Bankberatung umzusteigen

41 %
der Kunden sind mit der Reaktion ihrer Bank auf Cyberattacken zufrieden

63 %
haben das Gefühl, dass ihre Bank ihr Geld nicht vermehren möchte

Digitale Traditionsbank

AUF DEM WEG ZUM KLASSENBESTEN

Klassische USPs der Traditionsbanken wie die fachlich-fundierte Beratung von Mensch zu Mensch bieten den digital orientierten, zeitknappen Verbrauchern heute keinen ausreichenden Mehrwert mehr.

Das Ziel, digitale Traditionsbank zu werden, die einen agilen, reaktionsschnellen und personalisierten Service per Mobilgerät bietet, rückt somit nur langsam näher. Um Wettbewerbsfähigkeit, Mehrwert und Einzigartigkeit zu erlangen, müssen traditionelle Banken ihre Wettbewerbsvorteile – fundiertes Kundenwissen, Vertrauenskapital und anspruchsvolle Finanzprodukte – noch konsequenter als bislang in die Smartphone-Welt ihrer Kunden transformieren.

Die Wettbewerbsstrategie gehört auf den Prüfstand, da die Traditionsbanken in Sachen Flexibilität und Preisgestaltung nicht mit digitalen Banken oder GAFAM (Google, Amazon, Facebook, Apple und Microsoft)-ähnlichen Anbietern mithalten können. Sie sollten sich stattdessen darauf konzentrieren, Klassenbeste unter ihresgleichen zu werden, solange die Wechselbereitschaft so gering ist wie derzeit.

Gute Kundenarbeit bei Hackerangriffen oder Phishing schützt zudem vor Abwanderung und steigert die Attraktivität für potenzielle Neukunden. Erweiterte Sicherheitsverfahren (Enhanced Digital Security) zählen zu den drei Top-Kriterien für einen Wechsel der Hausbank in Deutschland.

Als vertrauenswürdiger Finanzdienstleister sollten Banken aktiver zum Thema Sicherheit kommunizieren – vorausgesetzt ihre digitale Technologie ist auf dem neuesten Stand und Sicherheitsvorkehrungen werden nicht als Last wahrgenommen.

Das Smartphone wird immer zur Schaltzentrale für das tägliche Leben – auch in Deutschland. Damit entsteht ein enormes Potenzial für hyperpersonalisierte Dienstleistungen auf der Grundlage von Zahlungen und Standortdaten, vorausgesetzt, Technologie und Prozesse sind vorhanden, um die Daten zu verarbeiten.

Umwelt-, Sozial- und Governance-Aspekte (ESG) stellen ebenfalls einen potenziellen Wettbewerbsvorteil für Banken dar.

www.soprasteria.de

Die Mehrwerte des IT-Monitorings

ALLES IM BLICK, ALLES UNTER KONTROLLE

In unserer digitalen Welt ist die IT-Infrastruktur ein kritischer Erfolgsfaktor für jedes Unternehmen. Die ständige Verfügbarkeit und Funktionsfähigkeit von IT-Systemen ist unerlässlich, um Geschäftsprozesse reibungslos zu gestalten, Kundenzufriedenheit zu gewährleisten, den Wettbewerbsvorteil zu sichern und Engpässe zu identifizieren.

IT-Monitoring spielt hierbei eine entscheidende Rolle. Über dessen Bedeutung, Potenziale und Herausforderungen sprachen wir mit Alexander Wiedenbruch, Director R&D & Domain Representative bei der USU GmbH.

it management: *Herr Wiedenbruch, wenn wir über das Thema IT-Monitoring sprechen, wie hoch würden Sie den Verbreitungsgrad in deutschen Unternehmen einschätzen?*

Alexander Wiedenbruch: In der heutigen Geschäftswelt, wo nahezu jedes Unternehmen in irgendeiner Weise IT-Monitoring einsetzt, würde ich den Verbreitungsgrad in deutschen Unternehmen als sehr hoch einstufen. Diese Entwicklung unterstreicht das zunehmende Bewusstsein für die Bedeutung einer nahtlosen Überwachung der IT-Infrastruktur. Trotzdem finden wir in vielen IT-Abteilungen eine Vielzahl nicht integrierter Monitoring-Systeme vor, die historisch mit der IT-Infrastruktur mitgewachsen sind. Es ist nicht unüblich, dass große, international agierende Unternehmen bis zu 10 verschiedene Systeme parallel nutzen. Dies deutet darauf hin, dass zwar ein Bewusstsein für die Notwendigkeit von IT-Monitoring besteht, jedoch oft noch Herausforderungen in Bezug auf die Integration und Konsolidierung bestehen, um eine effiziente und ganzheitliche Überwachung zu gewährleisten. Es besteht also definitiv noch Potenzial für eine breitere Akzeptanz und Implementierung von integrierten IT-Monitoring-Lösungen in deutschen Unternehmen.

it management: *Wie meistern Sie die Herausforderungen, die die immer weiter steigende Komplexität von IT-Systemen und Anwendungen mit sich bringt. Die IT-Infrastruktur wird von Jahr zu Jahr komplexer. Können wir dagegen etwas tun?*

Alexander Wiedenbruch: Die steigende Komplexität der IT-Landschaften stellt zweifellos eine Herausforderung dar. Eine IT-Monitoring-Lösung sollte nach unserer Auffassung speziell dafür konzipiert sein, um diese Komplexität zu beherrschen und das Management von IT-Infrastrukturen zu vereinfachen. Wir nutzen hierfür speziell entwickelte Konnektoren und Tools, um Daten aus allen Bereichen der IT-Landschaft effizient zu erfassen. Dies erlaubt eine ganzheitliche Überwachung des gesamten Systems, die sich vom End-to-End (E2E) Monitoring über Cloud- und Container-Überwachung bis zu individuellen Anwendungen erstreckt. Durch die Integration in bestehende Systeme und die Bereitstellung intelligenter Observability-Funktionen bieten wir unseren Kunden eine nahtlose und effiziente 360-Grad-Überwachungsmöglichkeit. Damit können sie nicht nur die steigende Komplexität bewältigen, sondern auch ihre Geschäftsprozesse und die Einhaltung von Services und Service-Level-Agreements (SLAs) effektiver managen und überwachen. So stellen wir sicher, dass unsere Kunden nicht nur den aktuellen, sondern auch zukünftigen Anforderungen ihrer IT-Umgebungen gewachsen sind.

it management: *Können Sie näher erläutern, was Sie unter einer 360-Grad-Überwachung verstehen? Und wie zielführend ist so ein Ansatz?*

Alexander Wiedenbruch: Unter einer 360-Grad-Überwachung verstehen wir eine umfassende Sicht auf die gesamte IT-Infrastruktur eines Unternehmens, die sich nicht nur auf die Überwachung klassischer Hardwarekomponenten wie Server und Netzwerke beschränkt. Unser Ansatz schließt Software, Applikationen, Datenbanken sowie die gesamte Rechenzentrums- und Gebäudetechnik ein. Dies ist entscheidend, denn auch Faktoren wie die Raumtemperatur, der Energieverbrauch, die Effizienz der Klimatisierung, mögliche Überlastungen oder Störungen in der unterbrechungsfreien Stromversorgung (USV) spielen eine zentrale Rolle für die Serviceverfügbarkeit. Diese ganzheitliche 360-Grad-Betrachtung ist entscheidend für die Fähigkeit, Probleme zeitnah zu identifizieren und zu beheben und bietet so einen echten Mehrwert im

> DIE ZUKUNFT GEHÖRT DEN LÖSUNGEN, DIE NICHT NUR REAKTIV, SONDERN AUCH PROAKTIV AGIEREN KÖNNEN.
>
> **Dr.-Ing. Alexander Wiedenbruch, Director R&D & Domain Representative, USU GmbH, www.usu.com**

Hinblick auf die Servicequalität und -sicherheit.

it management: *Neben der Überwachung ist auch das IT-Service Management von zentraler Bedeutung. Wie unterstützt die Lösung von USU Unternehmen dabei, ihre Effizienz in diesem Bereich zu steigern?*

Alexander Wiedenbruch: Ein wesentlicher Aspekt unserer Lösung ist die Fähigkeit, die Effizienz des Service Managements deutlich zu verbessern. Ein zentrales Problem vieler Unternehmen ist die Flut an Warnmeldungen, die von verschiedenen Monitoring-Tools generiert werden und oft enthalten diese eine hohe Anzahl an False Positives, also Alarme oder Warnungen, die fälschlicherweise ausgelöst wurden, obwohl kein tatsächliches Problem oder keine Bedrohung vorliegt. Unsere Lösung hilft, diese Herausforderungen zu bewältigen, indem sie die Informationen normalisiert, analysiert und nur die relevanten Warnungen hervorhebt. Durch die intelligente Korrelation von Events und die Erstellung von Sammeltickets für ähnliche oder zusammenhängende Probleme können wir die Anzahl der zu bearbeitenden Tickets erheblich reduzieren. Dies ermöglicht IT-Teams, sich auf tatsächliche Probleme zu konzentrieren und vermeidet die Überlastung durch eine Vielzahl von Einzeltickets. Darüber hinaus bietet unsere Lösung eine schnellere Diagnose und Behebung von Problemen, was zu kürzeren Ausfallzeiten und einer verbesserten Servicequalität führt. Bei Bedarf kann das System auch automatisch korrigierende Maßnahmen einleiten oder den zuständigen Personenkreis alarmieren.

it management: *KI ist ja das Hype-Thema in der IT. Wo kann sie den Anwendern im IT-Monitoring helfen und gibt es Best Practices für einen KI-basierten Workflow?*

Alexander Wiedenbruch: Künstliche Intelligenz bietet im Bereich des IT-Monitorings zahlreiche Vorteile, insbesondere bei der frühzeitigen Erkennung potenzieller Probleme und der automatisierten Reaktion darauf. Ein Beispiel dafür ist eine auf KI-Algorithmen basierende dynamische Schwellwertberechnung. Dies ermöglicht es den Verantwortlichen, flexible Schwellwerte für relevante Metriken wie CPU- oder Festplattenauslastung zu konfigurieren, die sich an die tatsächliche Nutzung anpassen. Durch die Nutzung von historischen Daten und selbstlernenden Algorithmen ist ein solches intelligentes Modul in der Lage, Muster zu identifizieren und kontinuierlich Schwellwerte anzupassen. Zum Beispiel wird bei der CPU-Auslastung der Peak am Montagmorgen berücksichtigt, wenn alle Nutzer nach dem Wochenende ihre IT-Endgeräte starten. Dadurch verbessert sich die Qualität der Alarmierung erheblich, was zu weniger Fehlalarmen und einer früheren Erkennung von Anomalien führt.

it management: *Nur das Zusammenspiel zwischen Monitoring, Event Management, Capacity Management, Incident Management und Alarmierungsmodulen garantiert die Vermeidung technischer Ausfälle und sorgt für eine schnelle Fehlerbehebung. Was können Sie Anwendern hier bieten, das über das klassische IT-Monitoring hinausgeht?*

Alexander Wiedenbruch: Wir bieten unseren Kunden ein ganzheitliches Lösungspaket, das weit über traditionelles IT-Monitoring hinausreicht und verschiedene Aspekte des IT-Betriebs abdeckt. Neben der Überwachung der IT-Infrastruktur bieten wir leistungsstarke Event-Management-Funktionen, die eine konsolidierte Sicht auf die gesamte die IT-Landschaft ermöglichen. Darüber hinaus gewährleistet das Capacity Management nicht nur eine Vorhersage und Anpassung von IT-Kapazitäten auf Basis aktueller Trends, sondern ermöglicht auch ein effizientes Rightsizing der Kapazitäten. Dies führt zu einer optimierten Ressourcennutzung, die sowohl den wirtschaftlichen Bedarf als auch die Nachfrage berücksichtigt, wodurch Ausfallzeiten minimiert und die Serviceverfügbarkeit deutlich verbessert werden. Ein weiterer zentraler Bestandteil der Lösung ist das Incident Management zusammen mit der integrierten Alarmierungsfunktion, die operative Teams, Service-Owner und das Management in die Lage versetzt, jederzeit schnell, zuverlässig und wirkungsvoll auf Störungen zu reagieren, egal wo sie sich gerade befinden. Dieses Vorgehen garantiert nicht nur eine Minimierung der Fehlerbehebungszeiten, sondern verhindert auch, dass kritische Systeme und Prozesse beeinträchtigt werden.

it management: *Abschließend, wie sehen Sie die Zukunft des IT-Monitorings und wie bereitet sich USU darauf vor?*

Alexander Wiedenbruch: Die Zukunft gehört den Lösungen, die nicht nur reaktiv, sondern auch proaktiv agieren können. Dank fortschrittlicher Technologien wie KI und maschinellem Lernen werden wir in der Lage sein, noch präzisere Prognosen und automatisierte Reaktionen auf potenzielle Probleme zu ermöglichen, um diese zu verhindern, bevor sie auftreten. USU investiert kontinuierlich in Forschung und Entwicklung, um Lösungen mit diesen Technologien zu erweitern und zu verbessern. Ziel ist es, unseren Kunden nicht nur Werkzeuge zur Überwachung ihrer IT-Infrastruktur zu bieten, sondern sie auch in die Lage zu versetzen, vorausschauend zu handeln und ihre IT-Landschaften effizienter und sicherer zu gestalten.

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

IT-Event-Management 2.0

DIE ZUKUNFT DER IT-ÜBERWACHUNG

In der heutigen Ära der Digitalisierung, ist das IT-Event-Management zu einer entscheidenden Säule innerhalb der IT-Strategien geworden. Der rapide technologische Fortschritt und die zunehmende Vernetzung haben das Management der IT-Infrastrukturen zu einer komplexen Herausforderung gemacht.

Vor diesem Hintergrund suchen Unternehmen nach fortschrittlichen und leistungsfähigen Lösungen für die Überwachung und Verwaltung ihrer IT-Infrastrukturen. Es besteht ein wachsender Bedarf an Werkzeugen und Strategien, um nicht nur auf aktuelle Herausforderungen zu reagieren, sondern auch die Grundlage für zukünftige Innovationen und Verbesserungen zu bieten. Eine proaktive Problemlösung und die Fähigkeit, den Überblick in der Fülle der Informationen zu behalten sowie das frühzeitige Erkennen möglicher Störungen sind dabei von entscheidender Bedeutung. In dieser Situation erweisen sich aktuelle IT-Event-Management-Systeme als praktische Lösungen, die gezielt auf die vielseitigen Anforderungen der heutigen IT-Landschaften eingehen und gleichzeitig Möglichkeiten für zukünftige Innovationen schaffen.

Zentralisierte Überwachung als Schlüssel zur Effizienz

Moderne Lösungen integrieren die Überwachung aller Infrastrukturkomponenten und vorhandenen Monitoring-Lösungen in einem zentralen System. Dadurch wird die Möglichkeit geschaffen, Probleme schnell und präzise zu identifizieren – vom Endgerät über die Anwendung bis hin zur Datenbank – und eine kontinuierliche Überwachung in Echtzeit zu gewährleisten. Dies ermöglicht IT-Teams, ihre Ressourcen effizienter einzusetzen und die Zeit, die für das Abwickeln von False Positives benötigt wird, signifikant zu reduzieren. Die Ergebnisse sind eine verbesserte Effizienz des IT-Betriebs und eine gesteigerte Kundenzufriedenheit und -bindung, da Probleme proaktiv adressiert und gelöst werden können, bevor sie den Benutzer beeinträchtigen.

Die Correlation Engine

In der heutigen Zeit, in der sich IT-Infrastrukturen unaufhaltsamen entwickeln und ständig neu gestalten ist die Correlation Engine zweifellos das zentrale Element moderner IT-Event-Management Lösungen. Sie fungiert als intelligenter Knotenpunkt, der einen Großteil der Datenverarbeitung und -analyse in der IT-Infrastruktur übernimmt. Diese hochentwickelte Technologie ist darauf ausgelegt, eine breite Palette von Datenquellen zu integrieren und zu verarbeiten, darunter Monitoring-Software, Systemmanagement-Tools, Applikationsprotokolle und Netzwerkkomponenten. Ein bedeutender Bestandteil dieses Systems ist die Configuration Management Database (CMDB), die eine umfassende und detaillierte Darstel-

lung der Service-Topologien sowie relevante Service Level Agreements (SLAs) bereitstellt.

Gerade für die Entscheidungssicherheit in der komplexen Welt der IT ist eine Correlation Engine inzwischen unverzichtbar. Durch ihre Fähigkeit zur Standardisierung von Daten und zur Anwendung etablierter Bewertungskriterien ermöglicht sie eine zuverlässige Identifizierung von Zusammenhängen zwischen verschiedenen Ereignissen. Diese Engine kann komplexe Muster erkennen, bestehendes Wissen anwenden und das Überschreiten definierter Schwellenwerte erkennen. Dadurch trägt sie maßgeblich zur frühzeitigen Erkennung potenzieller Störungen bei und beschleunigt die Reaktionszeiten des IT-Service-Managements erheblich.

Gleichzeitig zeichnet sich die Correlation Engine durch ihre hohe Anpassungsfähigkeit aus, die durch flexible Regeln ermöglicht wird. Sie analysiert Events in Echtzeit, erkennt verschiedene Arten von Korrelationen und passt ihre Reaktionen dynamisch an. Dies bedeutet, dass sie Alarme basierend auf der Häufigkeit und Dringlichkeit von Ereignissen auslösen kann, wobei gleichzeitig die Auswirkungen auf die Business Services gemäß den SLAs berücksichtigt werden.

Die Vorteile einer zentralen Event- und Service-Korrelation

➤ Konsolidierte Alarme und Tickets: Durch die Correlation Engine werden Events gefiltert, wodurch Mitarbeitende nur über relevante Ereignisse informiert werden. Für jeden Störfall wird nur eine Benachrichtigung generiert, unabhängig von der Anzahl der eingeflossenen Events. Dadurch entsteht eine effiziente Arbeitsweise, und der IT-Service-Desk wird erheblich entlastet. Die automatische Priorisierung und Sortierung von Tickets trägt zusätzlich dazu bei, dass dringende Angelegenheiten vorrangig behandelt werden können, was wiederum die Reaktionszeiten verbessert und die Kundenzufriedenheit erhöht.

➤ Der Gesamtzustand im Überblick: Eine wesentliche Stärke der Event-Korrelation besteht darin, dass sie den Zustand der IT-Infrastruktur in einer einheitlichen und übersichtlichen Struktur darstellt. Durch Dashboards und Event-Konsolen erhalten verschiedene Akteure, wie Service Owner, Fachabteilungen und das Management, die benötigten Informationen auf einen Blick. Dies ermöglicht es den Mitarbeitenden, Engpässe frühzeitig zu erkennen, Kapazitäten bedarfsgerecht zu planen und Ressourcen effizient einzusetzen. Zudem können auf Basis der korrelierten Events aussagekräftige Berichte erstellt werden, die einen detaillierten Einblick in die Performance bestimmter Services oder die Auslastung von Ressourcen bieten.

➤ Effizienter IT-Betrieb: Eine zentrale Event- und Service-Korrelation trägt signifikant zur Steigerung der Wirtschaftlichkeit des IT-Betriebs bei:

#1 Durch die Reduzierung von manuellen Aufwänden im IT Service Management können Ressourcen effizienter eingesetzt werden, was letztendlich zu Kosteneinsparungen führt.

#2 Die Analyse der Event-Korrelationen ermöglicht es, Optimierungspotenziale im IT-Betrieb zu identifizieren und entsprechende Maßnahmen zur Steigerung der Effizienz einzuleiten

#3 Mitarbeitende profitieren von konsolidierten Darstellungen, die ihnen ermöglichen, Reportings und Performance-Analysen durchzuführen, was wiederum die Produktivität erhöht.

#4 Die Verringerung der Mean Time To Repair (MTTR) führt zu einer Reduzierung der Ausfallzeiten, was sich positiv auf den Geschäftsbetrieb auswirkt und potenzielle Umsatzeinbußen minimiert.

Ganzheitliches IT-Event-Management

Die USU-Lösung bietet vielfältige Anwendungsmöglichkeiten. Sie standardisiert und aggregiert Überwachungsdaten aus allen Infrastrukturkomponenten in einer zentralen Datenbank. Dort werden sie analysiert, bewertet und über benutzerfreundliche Dashboards und Berichte visualisiert. Bei Bedarf initiiert das IT-Event-Management automatisch Korrekturmaßnahmen oder benachrichtigt das relevante Personal.

Fazit

Ähnlich wie Menschen aus Fehlern lernen, kann auch die IT durch den Einsatz von KI und Event-Korrelation optimiert werden. Die Identifizierung von Optimierungspotenzialen und die Verfeinerung der Kapazitätsplanung tragen maßgeblich zur Effizienzsteigerung im IT-Betrieb bei. Die Reduzierung von Tickets und Alarmen schafft Freiräume im IT-Service-Management, um sich auf wesentliche Aufgaben zu konzentrieren und Prozesse sowie Komponenten kontinuierlich zu verbessern. Daher ist die Implementierung eines Next-Generation-Monitorings unverzichtbar, um das Servicemanagement auf ein höheres Niveau zu heben und den stetig wachsenden Anforderungen an die IT-Infrastruktur gerecht zu werden.

Frank Laschet | www.usu.com

KÜNSTLICHE INTELLIGENZ
ALS BUSINESS-BOOSTER FÜR UNTERNEHMEN

INTERIM MANAGER BERICHTEN AUS DER PRAXIS

Elf Interim Manager haben ein gemeinsames Fachbuch über ihre Erfahrungen und Empfehlungen zum Einsatz Künstlicher Intelligenz (KI) in Unternehmen geschrieben. Die Autoren Ulvi Aydin, Klaus Becker, Udo Fichtner, Melanie Heßler, Eckhart Hilgenstock, Falk Janotta, Jürgen Kaiser, Dr. Albert Schappert, Dr. Harald Schönfeld, Klaus-Peter Stöppler und Oliver Strass sind „Führungskräfte auf Zeit", also Manager, die für einige Zeit in Unternehmen geholt werden, um Projekte wie die Einführung von KI voranzutreiben. Die dabei gewonnenen Erkenntnisse haben sie in dem neuen Werk „Künstliche Intelligenz als Business-Booster für Unternehmen" (ISBN 978-3-98674-110-5) auf 380 Seiten zusammengefasst.

„Es gibt keine anderen Führungskräfte als Interim Manager, die im Laufe ihres Berufslebens so viele Unternehmen und so viele verschiedene unternehmerische Herausforderungen kennenlernen", erklärt der Herausgeber Dr. Harald Schönfeld, warum die Autoren besonders geeignet für das Thema sind. Er erläutert den Buchtitel: „Künstliche Intelligenz gilt derzeit als der 'Business-Booster' für Unternehmen, der Märkte umfassend verändert - aufgrund der exponentiellen Entwicklung sogar in einer kaum vorstellbaren Geschwindigkeit." Er verweist auf eine im Buch vorgestellte aktuelle Untersuchung über Topmanager in Deutschland, Österreich und der Schweiz, nach der beinahe zwei Drittel der Führungskräfte fest davon überzeugt sind, dass Künstliche Intelligenz die Produktivität erhöhen wird. Gut die Hälfte der Manager will KI in Zukunft bei wichtigen Entscheidungen im Unternehmen einen hohen Stellenwert einräumen.

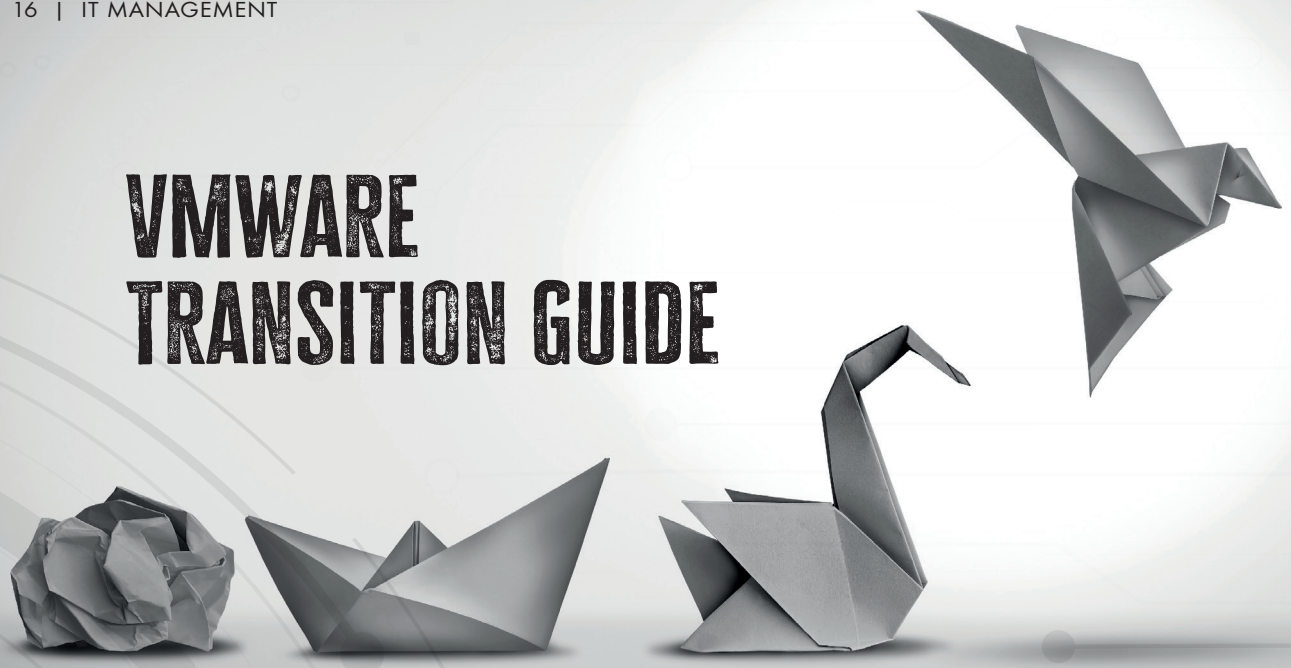
Breites Spektrum der Buchbeiträge

Das Spektrum der Beiträge in dem neuen KI-Buch reicht von der Einführung über die Herausforderungen beim Einsatz über Querschnittsfunktionen wie Marketing, Personalwesen, Controlling und Nachhaltigkeitsmanagement bis hin zu branchenspezifischen Beispielen, aus denen sich viele Erfahrungen für andere Branchen übernehmen lassen. Die Themen im Einzelnen:

- Von Interim Managern lernen (Dr. Harald Schönfeld),
- KI: Geschichte, Anwendungen, Herausforderungen (Eckhart Hilgenstock),
- Die drei Dimensionen Künstlicher Intelligenz (Ulvi Aydin),
- Künstliche Intelligenz – Stolpersteine bei der Einführung im Unternehmen (Falk Janotta),
- Künstliche Intelligenz im Marketing (Melanie Heßler),
- KI & Co. im Personal- und Nachhaltigkeitsmanagement (Udo Fichtner),
- Künstliche Intelligenz im Bauprojektmanagement (Klaus-Peter Stöppler),
- Business Intelligence: Wie KI das Controlling revolutioniert (Jürgen Kaiser, Oliver Strass),
- KI-Anwendungen in die Organisation bringen (Dr. Albert Schappert),
- Die Zukunft der Modebranche (Klaus Becker).

Künstliche Intelligenz als Business-Booster für Unternehmen;
Dr. Harald Schönfeld et al.;
DC Publishing; 03-2024

VMWARE TRANSITION GUIDE



ZUR STÄRKUNG IHRER VIRTUALISIERUNGSSTRATEGIE IN ZEITEN DES WANDELS

In der dynamischen IT-Welt, in der Fortschritt und Umbruch Hand in Hand gehen, ist Veränderung die einzige Konstante. VMware hat sein Produktangebot, seine Lizenzmodelle und seine Verträge mit Partnern einer Reihe umfassender Änderungen unterzogen. Diese sind eine direkte Folge der Übernahme durch Broadcom im November 2023 und der Ausgangspunkt nachwirkender Umstellungen in der VMware Technologiewelt.

Allerdings ist auch jede Änderung gleichzeitig eine neue Chance. Somit ist jetzt für VMware-Kunden und -Partner ein günstiger Moment, ihre Virtualisierungsstrategie noch einmal zu überdenken. Angesichts des Ausmaßes der Umstellungen sollte man als erstes herausfinden, was das konkret für Ihren Geschäftsbetrieb und Ihre Zukunftsplanung bedeutet.

Dieser Leitfaden bietet Ihnen einen Überblick zu den wesentlichen Änderungen und strategischen Alternativen.

Inhalt des eBooks:

- #1 Wie Sie die Folgen der Übernahme durch Broadcom meistern
- #2 Umstellungen in der Lizenzierung, die die VMware-Landschaft auf den Kopf stellen
- #3 Diese Fragen sollten Sie sich stellen
- #4 Für VMware optimierter Speicher, der zudem einen nahtlosen Wechsel ermöglicht
- #5 Unterbrechungsfreie Ablösung von VMware vSAN mit SANsymphony
- #6 Auswahl über VMware vSphere hinaus ermöglichen
- #7 Maximale VMware-Effizienz mit SANsymphony

Das **eBook** umfasst 11 Seiten und steht zum kostenlosen Download bereit

DATA FABRIC TOOLS – DIE TREIBENDE KRAFT

Eine verbesserte Compliance ist für Unternehmen unerlässlich, um Rechtsvorschriften und Branchenstandards einzuhalten, das Risiko von Bußgeldern zu verringern und das Vertrauen der Partner und Kunden zu stärken.

Die Erweiterung des deutschen Lieferketten-gesetzes stellt Unternehmen und die Einhaltung der Compliance-Richtlinien nicht nur vor neue Herausforderungen, sondern auch vor eine kostenintensive Aufgabe.

Die Nutzung neuer Technologien wäre an dieser Stelle hilfreich, doch viele Unternehmen zögern, besonders auf dem Weg zur Prozessautomati-sierung. Data Fabric Tools erweisen sich hier als unverzichtbare Verbündete. Sie fungieren als zentrales Nervenzentrum, das Daten aus unterschiedlichen Quellen sammelt, integriert und aufbereitet, um sie für automatisierte Prozesse nutzbar zu machen.

Bessere Compliance

DIGITALISIERTE UND AUTOMATISIERTE LIEFERKETTEN

Die Verantwortung von Unternehmen endet keineswegs an den physischen Grenzen des Betriebsgeländes. Nach der Erweiterung zum deutschen Lieferkettengesetz im Januar 2024 steht jetzt die nächste Neuerung an: Die EU hat sich im März auf eine deutlich strengere Lieferketten-Gesetzgebung geeinigt. Größere Unternehmen müssen einen Plan erstellen, der die Vereinbarkeit ihres Geschäftsmodells und ihrer Strategie mit dem Pariser Abkommen zum Klimawandel sicherstellt. Künftig tragen sie dabei die Verantwortung für ihre gesamte Geschäftskette.

Der Aufwand auf Unternehmensseite ist erheblich und die neuen Gesetze bergen zahlreiche Herausforderungen – Unternehmer haben zwei Jahre Zeit, um sich an das Gesetz mitsamt den gestiegenen Anforderungen anzupassen. Die neue EU-Regulierung verpflichtet Unternehmen zu umfangreichen ESG- (Environmental, Social und Governance) Reportings, die in manueller Erstellung mühsam, zeitaufwändig und intransparent sein können. Nachweise für die Compliance zu erbringen, wird hier zur kostenintensiven Aufgabe.

Uneinheitliche Systeme und Methoden

In vielen Unternehmen ist die IT-Struktur nicht mehr Compliance-konform: Bis jetzt basieren zahlreiche Randprozesse und Systeme auf Spreadsheet und E-Mail. Das erschwert die Zusammenarbeit mit Lieferanten und die Einhaltung von Governance- und Compliance-Vorschriften enorm. Zudem erfordert die Verwaltung komplexer Beziehungen zu Dienstleistern eine umfassende Due-Diligence-Prüfung. Unternehmen müssen die Einhaltung von komplexen, multidimensionalen Sanktionsprüfungen in Abhängigkeit von zum Beispiel Region, Produktkategorie und Auftragsvolumen sicherstellen und das Geschäftsrisiko minimieren. Hier arbeiten viele unterschiedliche Abteilungen teilweise auf sehr individueller Fallebene zusammen. Bei einer manuellen Bearbeitung sind Fehler vorprogrammiert: Diese Prozesse in uneinheitlichen Systemen sind intransparent und ineffizient.

In vielen Unternehmen gelingt die Überwindung dieser Schwierigkeiten durch die Nutzung moderner Digitalisierungstechnologien, die auch die Orchestrierung und Automatisierung ihrer Prozesse ermöglichen. Neue Technologien vereinfachen die Art und Weise der relevanten Datenerhebung und Berichterstattung. Das spart Personalressourcen für Koordination und Bearbeitung ein. Doch häufig wagen viele Firmen den Schritt erst nach langer Überlegung: Um aktuelle Digitalisierungs- und Automatisierungs-Potenziale zur Abbildung neuer Governance- und Compliance-Regelungen nutzen zu können, muss die Unternehmens-IT neue Technologieplattformen in ihrer Architektur abbilden.

Plattform für Prozessorchestrierung

Die aktuellen Lieferkettengesetze zeigen deutlich, welchen hohen Stellenwert die

digitale Orchestrierung von Prozessen heute hat. Jetzt brauchen Unternehmen die Steuerung von komplexen Aufgaben, deren Automatisierung Abläufe verkürzt und deren Funktionsweise überzeugt. Die Basis hierfür bietet eine Plattform mit hoher Integrationsfähigkeit. Appian dockt an die vorhandenen ERP-Systeme an. Dabei verbinden sich flexibel austauschbare Datenquellen miteinander und schaffen ein einheitliches System. So werden die Prozessvariationen über unterschiedliche Systeme hinweg orchestriert – für mehr Transparenz und Effizienz.

Verbindung von Datenquellen und Prozessoptimierung

Um den Wandel zu beschleunigen, eignen sich vor allem so genannte Data Fabric Tools. Sie sind eine wichtige Komponente bei einer entsprechenden Prozessautomatisierungs-Plattform. Für eine komplexe Automatisierung im großen Maßstab ist eine solide Datenarchitektur erforderlich, die verschiedene Datenquellen miteinander verbindet – denn oft werden die Informationen heute noch immer in Datensilos gelagert, die über die gesamte Organisation verstreut sind.

In diesem Kontext spielt Data Fabric eine zentrale Rolle, denn der Ansatz verknüpft Datenquellen in verschiedenen Systemen miteinander – ob On-Premises oder in Cloud-Umgebungen – und integriert sie in die Prozessabläufe.

Die Datensätze verbleiben dabei in ihren ursprünglichen Systemen. Dank einer virtualisierten Datenebene müssen die Informationen nicht aus ihrem aktuellen Speicherort wie einer Datenbank, einem ERP-System oder einer CRM-Anwendung kopiert werden, wenn mit ihnen gearbeitet werden soll. Der Zugriff auf Echtzeitdaten erlaubt qualitativ bessere und schnellere Entscheidungen – und er entlastet IT-Teams von zeitaufwändiger und kostenintensiver Datenintegrationsarbeit. So lassen sich Geschäftsdaten auf neue und besonders effiziente Weise nutzen.

Die Plattform zur Prozessautomatisierung von Appian kombiniert zudem weitere Technologien, um die entsprechenden Gesamtprozesse zu optimieren und zu automatisieren. Im Einzelnen sind das die Robotic Process Automation (RPA), das Intelligent Document Processing (IDP), die Workflow-Orchestrierung, der Einsatz Künstlicher Intelligenz (KI), aber auch Systemintegration und Geschäftsregeln.

Vereinheitlichte Analyse

Ein weiterer Vorteil ist die vereinheitlichte Analyse. Eine Data Fabric-Lösung verwendet wie beschrieben eine virtualisierte Datenebene, um Daten aus jeder Quelle in ein einheitliches Modell in Kontext oder Verbindung zu setzen. So können Unternehmen eine umfassendere und genauere Sicht auf ihre Prozesse und Kunden sowie die relevanten Märkte bekommen. Mit dem einheitlichen Datenmodell lassen sich aber auch Advanced-Analytics-Prognosen durchführen, die vorher so nicht möglich waren. Data Fabric unterstützt zudem Erkenntnisse in Echtzeit. Die virtualisierte Datenschicht spielt dabei eine wesentliche Rolle, indem sie konsistent Updates sowohl beim Lesen als auch beim Schreiben von Daten an die ursprüngliche Datenquelle und von ihr zurück überträgt. So sind die Informationen immer auf dem neuesten Stand und Entscheidungen lassen sich schneller treffen.

Von zentraler Bedeutung ist die hohe Zuverlässigkeit beim Datenzugriff auf jeder Ebene. Dafür sorgt die Data-Fabric-Architektur – hiermit lässt sich der Zugang selbst auf granularen Ebenen wirksam beschränken.

Effektivere Datennutzung

Eine Data Fabric-Lösung vereinheitlicht den Blick auf Daten aus unterschiedlichen Systemen und erlaubt sogar den Bezug von Informationen eines Systems auf Basis eines Datenfelds auf ein ganz anderes System – rasch und quellenübergreifend. Was früher noch eine umfassende Aufgabe für Data Scientists sowie Entwicklungsteams war, ist heute eine einfache Abfrage in einem Data-Fabric-System. Durch die Verbindung von Daten unter Berücksichtigung eines quellübergreifenden Rechtekonzepts und die Unterstützung agiler Analysen in Kombination mit einer Anwendungsentwicklungsumgebung für Workflows, bietet Data Fabric Unternehmen die Chance, ihre Daten innerhalb von Prozessen effektiver zu nutzen – und vor allem maximale Compliance-Sicherheit zu haben.

Betriebswirtschaftliche Vorteile

Dass die manuelle Bearbeitung Prozesse verlangsamt und erschwert, ist kein Geheimnis – und es besteht ein erhöhtes Risiko menschlicher Fehler. Das kann in Zusammenhang mit verschärften Regularien und Sanktionen fatale wirtschaftliche Folgen haben. Daher bietet eine Prozessautomatisierungsplattform auf Basis einer leistungsfähigen Data Fabric-Komponen-

te betriebswirtschaftliche Vorteile: Dazu gehören die Entwicklungsgeschwindigkeit und Skalierbarkeit, denn eine Data Fabric-Architektur wartet mit konsistenten Funktionen für sämtliche Entwicklungen im Bereich datengesteuerter Anwendungen auf. Ohne einen Data Fabric-Ansatz erfordern hybride Umgebungen komplexe „Data-Engineering"-Fähigkeiten, um die erforderlichen Informationen in entsprechende Anwendungen zu integrieren. Das führt zu Verzögerungen bei der Entwicklung neuer Geschäftsanwendungen. Mit Data Fabric-Technologie können Daten unabhängig von ihrem Standort oder Format leicht abgerufen, verwaltet und analysiert werden. Das hilft auch bei der Skalierung von Daten über Anwendungen hinweg.

Automatisierungsplattform als „Agilitätsschicht"

Die Data Fabric-Tools für die Prozessautomatisierungsplattform von Appian zeichnen sich durch vorgefertigte Konnektoren aus, die Systeme wie CRM, ERP und Datenbankanwendungen miteinander verbinden, ohne dass diese Integrationen von Grund auf neu entwickelt werden müssen. Eine Workflow-Orchestrierung sollte ebenfalls vorhanden sein, um unterschiedlichste Aufgaben nahtlos zwischen Software-Bots und menschlichen Mitarbeitern zu verteilen oder zu koordinieren.

Eine Plattform mit hoher Integrationsfähigkeit für eine systematische Prozessorchestrierung wird als „Agilitätsschicht" an die vorhandenen Systeme angedockt. Unterschiedliche Datenquellen werden miteinander verbunden, die während einer laufenden Migration flexibel austauschbar sind. So orchestriert Appian mit der unternehmenseigenen Plattform die Prozessvariationen systemübergreifend. Das schafft Transparenz und steigert die Effizienz.

Eine über diesen ersten Schritt hinausgehende Prozessautomatisierung hat das Potenzial, die Art und Weise, wie Unternehmen mit Anbietern und Lieferanten kommunizieren, grundlegend zu verändern. Werden die Datenquellen der ERP-Systeme verknüpft und die Prozesse zur Fallbearbeitung automatisiert, entstehen dadurch dynamische Ad-hoc-Arbeitsabläufe. Mit entsprechenden Workflow-Funktionen können Aufgaben und Arbeitsschritte koordiniert werden – und es kann bedarfsweise gegengesteuert oder auch automatisiert und damit die Effizienz erhöht werden.

Die Case Management-Plattform von Appian unterstützt das Erstellen und Verwalten von Geschäftsregeln und bietet den Mitarbeitenden die Möglichkeit, Prozesse schnell an neue Situationen anzupassen. Insgesamt lässt sich die Lösung schnell und flexibel implementieren und nutzen. Das entsprechende User Interface ist auch sofort auf Mobilgeräten verfügbar.

KI und Machine Learning für strukturierte Daten

Bei einer anspruchsvollen Lösung wie einer Automatisierungsplattform sind neue Technologien erfolgsentscheidend. Im Bereich Automatisierung ist das insbesondere Künstliche Intelligenz. Zum Beispiel beim Intelligent Document Processing (IDP). Machine Learning kann unstrukturierte Informationen in strukturierte Daten umwandeln oder auch Dokumente automatisch klassifizieren. Die aktuellen Entwicklungen bei generativer KI und Large Language Models unterstützen die Prozessautomatisierung.

Dabei sollten entsprechend vortrainierte KI-Modelle, die mit unternehmenseigenen Daten spezieller trainiert werden, diese Firmendaten niemals zurück an den KI-Anbieter spielen. Eine solche private KI gewährleistet den Datenschutz und Einhaltung der jeweiligen Unternehmens-Policies.

Mit den geeigneten Methoden lassen sich die Herausforderungen der neuen Compliance-Richtlinien gut bewältigen. Unternehmen können so effizient und transparent agieren sowie ihrer Verantwortung gerecht werden. Digitalisierung und Automatisierung sind zentrale Mittel, um den Anforderungen neuer ESG-Gesetze sowie dem neuen Lieferkettengesetz zu entsprechen und damit letztendlich auch einen Beitrag zu einer nachhaltigeren und gerechteren Welt zu leisten.

Fabian Czicholl

EINE DATA FABRIC-LÖSUNG VEREINHEITLICHT DEN BLICK AUF DATEN AUS UNTERSCHIEDLICHEN SYSTEMEN UND ERLAUBT SOGAR DEN BEZUG VON INFORMATIONEN EINES SYSTEMS AUF BASIS EINES DATENFELDS AUF EIN GANZ ANDERES SYSTEM.

Fabian Czicholl,
Regional Vice President, Appian,
www.appian.com

IT Management & Digitalisierung

BERUFSBEGLEITENDE FERNSTUDIENGÄNGE

Seit 20 Jahren bietet die Hochschule Schmalkalden berufsbegleitende Fernstudiengänge an und wurde für diese schon mehrfach zum TOP-Fernstudienanbieter gekürt (FernstudiumCheck.de). Zum Portfolio gehören der Master-Studiengang „Informatik und IT-Management (M.Sc.)“ und die Bachelor-Studiengänge „Wirtschaftsinformatik und Digitale Transformation (B.Sc.)“ sowie „Wirtschaftsingenieurwesen und Digitalisierung (B.Eng.)“.

Mit einer Kombination aus Präsenz- und Selbststudienphasen sind die Angebote so konzipiert, dass sich Studium, Berufstätigkeit und Privatleben optimal vereinbaren lassen. Pro Semester finden etwa vier Präsenzphasen jeweils von Donnerstag/Freitag bis Sonntag auf dem Hochschulcampus in Schmalkalden oder über den Online-Campus statt. Während dieser Zeiten werden auch die Prüfungen abgenommen, so dass keine Belastungsspitzen am Semesterende zu bewältigen sind. Kleine Jahrgangsgruppen und eine individuelle Betreuung sorgen für hervorragende Studienbedingungen.

Das fünfsemestrige Master-Studium richtet sich an Personen mit einem ersten Hochschulabschluss (Informatik, Wirtschaftsinformatik) sowie einer einjährigen Berufserfahrung. Die Bachelor-Programme stehen Berufstätigen mit traditioneller Hochschulzugangsberechtigung (HZB) sowie auch beruflich Qualifizierten mit nicht-traditioneller HZB offen – und richten sich an Personen, die eine Ausbildung in einem technischen, kaufmännischen oder IT-Beruf absolviert haben und über erste Berufserfahrungen verfügen. Je nach Vorbildung umfassen die Bachelor-Studiengänge sechs bis acht Semester.

www.hsm-fernstudium.de

Die Zukunft der Fertigungsindustrie

NAHTLOSE INTEGRATION VON SAP UND NON-SAP IN DER CLOUD

Im Kern moderner Fertigungsunternehmen befindet sich ein komplexes Netzwerk von SAP-Systemen, das Betriebsabläufe orchestriert, Prozesse optimiert und Wachstum vorantreibt. Ziel der nahtlosen Verzahnung aller Komponenten ist die Maximierung von Effizienz und Produktivität – unverzichtbares Element im unternehmerischen Motor. Doch mit der Weiterentwicklung von Branchen und Technologie stellt sich die Frage: Wie können Hersteller sicherstellen, dass ihre SAP-Landschaften zukünftigen Anforderungen gerecht werden?

Cloud als Antwort

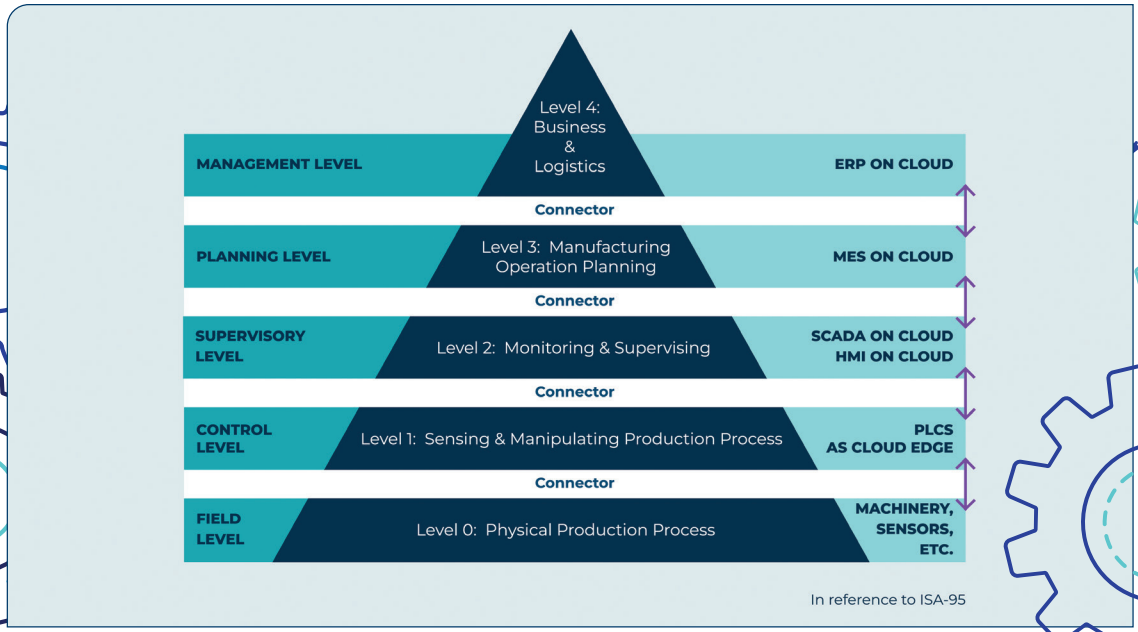
Die Antwort: Mit Cloud Computing. Laut aktuellen Studien von Gartner werden bis zum Ende dieses Jahrzehnts fast 70 Prozent der Unternehmen Cloud-Technologien nutzen. Diese Prognose ist bereits heute am Markt deutlich spürbar. Wir begleiten aktuell mehrere Kunden beim vollständigen Aufbau der Produktions-IT in der Cloud – einschließlich Manufacturing Execution System (MES). Die Cloud bietet Agilität – insbesondere geografisch – Skalierbarkeit und Kosteneffizienz. Ein wesentlicher Katalysator der Cloud-Adaption ist Künstliche Intelligenz (KI). Auch wenn sich KI am Zenit der Erwartungshaltung befindet, ist eines absehbar: Generative KI bedeutet Disruption. Um Teil dieser Bewegung zu sein, ist Cloud Computing als zentrale Komponente der Infrastrukturstrategie notwendig.

SAP im Wandel zu Cloud Native

Auch in der SAP-Welt ist der Wandel von On-Premises zu Cloud-Lösungen unaufhaltsam. Innovative Produkte der SAP – wie modernste KI-Lösungen – sind primär Cloud-Produkte. Doch welche Auswirkungen hat dieser Wandel auf die Schnittstellen der Unternehmens- und Kontrollsysteme der Fertigungsindustrie?

Wenn es um die Beschreibung und Darstellung der Interaktionspunkte und Beziehungen von Systemen in der Fertigungsindustrie geht, wird üblicherweise der international anerkannte Standard ISA-95 herangezogen. Dieser kann neben der Beschreibung der Systemlandschaft auch Aufschluss über die Aktivitäts- und Datenflüsse geben. Dabei werden die Systeme in verschiedene Schichten unterteilt – alle mit deutlicher Tendenz zu Cloud-Lösungen.

So ist es nicht verwunderlich, dass ERP aus der Cloud der neue Standard ist. Auch MES-Systeme werden zunehmend in die Cloud verlagert sowie alle anderen Schichten. SCADA/HMI-Systeme werden mit der Cloud verbunden und PLCs als Cloud-Edge-Geräte konzipiert.



Auch im Field Level zeigt sich, getrieben durch neue Technologien und Standards in der Industrial IoT, ein Wandel. Wir erleben die Verbreitung von IO-Link sowie ein Retrofit vorhandener Systeme, die durch moderne Kommunikations- und Sensortechnik erweitert werden. So kann eine zeitnahe Adaption von KI in Edge-Computing-Umgebung realisiert werden.

Die Cloud-Transformation ist Grundpfeiler zukünftiger Innovationen. Neben Generativer KI betrifft dies vor allem auch zukünftige Integrationsstrategien, um die eingangs beschriebene nahtlose Verzahnung von Prozessen, Applikationen und Ökosystemen zu gewährleisten.

Doch wie wird eine reibungslose Integration unterschiedlicher Anwendungen und Ökosysteme sogar über Multi-Cloud-Umgebungen hinweg realisiert? Die Erwartungshaltung an mögliche Integrationsszenarien aus Geschäfts- und Managementsicht ist eindeutig: nahtlos, medienbruchlos, problemlos. In der Praxis – vor allem technisch – ist die Integration von SAP- und Non-SAP-Systemen, von On-Premise- zu Cloud-Lösungen, häufig eine Herausforderung gewesen. Die Lösung: Maßgeschneiderte Konnektoren für horizontale und vertikale Intersystemkommunikation aus den Baukästen der Cloud Service Provider.

Konnektoren: die Überholspur von Cloud zu Cloud

Viele Unternehmen stehen aktuell vor der konkreten Herausforderung SAP S/4HANA Public und Private Cloud Editions in MES-Systemen zu integrieren.

ERP-Systeme spielen eine zentrale Rolle für Geschäftsprozesse, Ressourcen und Daten, da sie eine effiziente Planung, Steuerung und Kontrolle verschiedener Geschäftsbereiche ermöglichen.

MES-Systeme optimieren Fertigungsprozesse, indem sie Echtzeitdaten aus der Produktion erfassen, analysieren und nutzen, um die Produktivität zu steigern, die Qualität zu verbessern und Betriebskosten zu senken.

FÜR FERTIGUNGSUNTERNEHMEN MARKIERT DIE MIGRATION VON SAP-LANDSCHAFTEN IN DIE CLOUD DEN BEGINN EINER NEUEN ÄRA.

Simon Meraner, Managing Partner, Zoi, www.zoi.tech

Jedes Unternehmen hat spezifische Anforderungen und Prozesse, die bei der Integration zu berücksichtigen sind. Eine One-Size-Fits-All-Lösung ist oft nicht ausreichend.

Maßgeschneiderte Konnektoren schaffen Abhilfe: Sie überbrücken die Kluft zwischen disparaten Systemen und ermöglichen so einen reibungslosen Datenaustausch. Dabei kann die Integrationsstrategie von Kunde zu Kunde variieren und ist stark von der jeweiligen vorherrschenden SAP-Landschaft und dem spezifischen Integrationsszenario abhängig. So kann die Implementierung von Konnektoren mittels SAP Integration Suite auf der Business Technology Platform erfolgen oder bei einem Hyperscaler mit klassischer Abbindung an das SAP-Ökosystem. Nachfolgend einige Möglichkeiten, wie Konnektoren bei der Integration helfen:

Datenmapping und -transformation: Konnektoren bieten Funktionen zum Mapping und zur Transformation von Daten zwischen den verschiedenen Datenmodellen von SAP S/4HANA und MES-Systemen. Sie können dazu beitragen, die Komplexität der Integration zu reduzieren, indem sie die Konvertierung von Daten automatisieren.

Echtzeit-Synchronisierung: Konnektoren leisten den Echtzeit-Datenaustausch zwischen SAP S/4HANA und MES-Systemen, sodass Informationen stets aktuell sind und eine effektive Fertigungsplanung und -steuerung möglich ist.

Flexibilität und Anpassungsfähigkeit: Konnektoren können flexibel an die individuellen Anforderungen und Geschäftsprozesse eines Unternehmens angepasst werden.

Überwachung und Fehlerbehebung: Konnektoren bieten in der Regel Funktionen zur Überwachung des Datenaustauschs und zur Fehlerbehebung. So können Unternehmen Integrationsprozess überwachen und bei möglichen auftretenden Problemen schnell reagieren.

Das Ergebnis? Ein harmonisches Ökosystem, in dem Daten effizient fließen und Entscheidungsträger von Echtzeit-Einblicken profitieren.

SAP on Cloud: Innovation und Wachstum als Ergebnis

Zusammenfassend sind die Vorteile der Transformation von Systemlandschaften in die Cloud vielfältig und der Weg nach vorne ist klar. Für Fertigungsunternehmen markiert die Migration von SAP-Landschaften in die Cloud dennoch den Beginn einer neuen Ära – die sich vor allem durch ihre Flexibilität und Anpassungsfähigkeit auszeichnet. Um diese Vorteile optimal für sich zu nutzen, kann eine Zusammenarbeit mit einer Cloud-Beratung hilfreich sein. Als grundlegende Kompetenzen zeichnen sich hier vorhandene Erfahrung im Umgang mit komplexen SAP-Migrationen, Erfahrung mit Cloud-Anbietern, weitreichendes Verständnis der Fertigungsindustrie sowie ein tiefes technisches Know-how bei der Umsetzung individueller Anforderungen aus. Um den Weg für Innovation und Wachstum zu ebnen, sollten das gemeinsame Ziel stets nahtlose Übergänge und unterbrechungsfreie Betriebsabläufe sein.

Simon Meraner

SAP S/4HANA für HCM

SO KLAPPT DIE TRANSFORMATION REIBUNGSLOS

Mit der Auslieferung von HCM für SAP S/4HANA ist im Herbst 2022 das letzte Modul in die SAP S/4HANA-Architektur für ERP eingezogen. Welche Chancen der Umstieg mit sich bringt und mit welchen Ansätzen sich HCM optimal in die neue Umgebung integrieren lässt, veranschaulicht folgendes konkretes Szenario.

Mit der Verfügbarkeit von SAP HCM für S/4HANA ist grundsätzlich eine Wartungszusage für die sogenannten Core-Themen bis 2040 verbunden. Das gilt insbesondere für die notwendigen gesetzlichen Änderungen in der Abrechnung und die stetig wachsenden Arbeitgeberaufgaben in der Kommunikation mit gesetzlichen Einrichtungen. Die weitere Digitalisierung dieser Prozesse ist damit gesichert. Kunden können dadurch überdies ihre Unternehmensprozesse in einer sogenannten On-Premises-Architektur unterstützen.

Verschiedene Konfigurationsmöglichkeiten

Das SAP HCM wäre nun aber nicht HCM, gäbe es hier nicht diverse Optionen zur zukünftigen Ausrichtung der Architektur im Zusammenhang mit SAP S/4HANA sowohl beim Betriebsmodus (On-Premises, Cloud, Hybrid), bei der SAP-Integration (Stand-alone, Compatibility Mode, integriert) sowie bei der eingesetzten SAP-Software (HCM, Successfactors).

Vorgehensweise bei der HCM S/4HANA-Transformation

Im Folgenden wird auf die Transformation näher eingegangen. Das Standardvorgehen der SAP ist die sogenannte Conversion. Dabei werden alle Einstellungen, Daten und Entwicklungen (so S/4HANA-kompatibel) in die „neue Welt" übernommen. Im Wesentlichen erfolgt hierfür ein Upgrade auf SAP S/4HANA 2022 und im Nachgang die Aktivierung der SAP S/4HANA-Version des SAP HCM über eine sogenannte Business-Funktion. Dieses Verfahren funktioniert sehr gut, belässt allerdings „alles beim Alten".

Sehr viele SAP HCM-Installationen blicken jedoch auf eine lange Historie zurück. Das ist in den Datenbeständen, den

5 GRÜNDE FÜR DEN SDT-ANSATZ BEI DER SAP HCM TRANSFORMATION

#1 Eine selektive Transition kann den Wechsel beschleunigen.

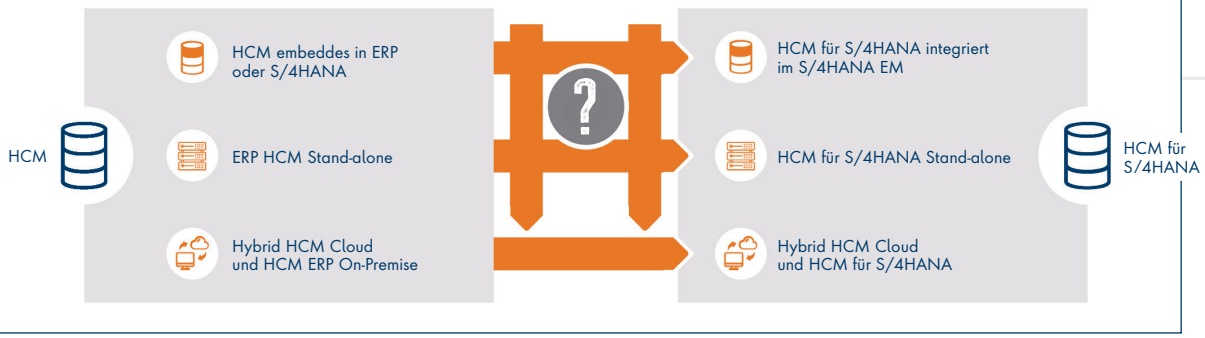
#2 Das Verfahren reduziert das Projektrisiko, im Vergleich zu einer Neuimplementierung.

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

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

#5 Veränderungen der IT-Landschaft (z.B. Systemkonsolidierungen, Prozessauslagerungen) in Cloud-Lösungen können in einem Schritt erfolgen.

TRANSFORMATIONSWEGE ZUM INDIVIDUELLEN HCM FÜR S/4HANA

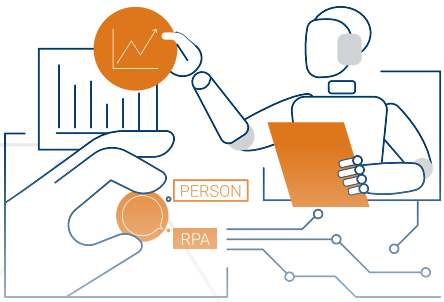


Customizing-Varianten und auch -Entwicklungen zu sehen. Insofern bieten sich neben der Eins-zu-eins-Conversion (Brownfield) weitere Möglichkeiten. Die hiermit verbundenen Chancen beinhalten sowohl Re-Standardisierung und Re-Design der Anwendung als auch eine Reduzierung der vorhandenen Daten, um zum Beispiel inaktive Unternehmen oder nicht mehr gültige Kontierungen. Die Nutzung dieser Chancen, auch in der Kombination aus Anwendung und Daten, ist mit Ansätzen sowohl einer kompletten Neueinführung (Greenfield) als auch einer teilweisen Neuausrichtung, der sogenannten Selective Data Transition (SDT), möglich.

Im Hinblick auf aktuelle, meist komplexe Abrechnungs- und/oder Zeitwirtschaftsszenarien mit hoher Dezentralisierung ist eine komplette Neueinführung sehr zeit- und kostenintensiv. Sie kommt wahrscheinlich nur dann infrage, wenn sich der Betriebsmodus ändert oder die Re-Standardisierung der Anwendung für den neuen Betriebsmodus im Fokus steht. Der SDT-Ansatz ist dagegen eine überzeugende Alternative zur Eins-zu-eins-Conversion.

Philipp von der Brüggen

> MIT DER VERFÜGBARKEIT VON SAP HCM FÜR S/4HANA IST GRUNDSÄTZLICH EINE WARTUNGSZUSAGE FÜR DIE SOGENANNTEN CORE-THEMEN BIS 2040 VERBUNDEN
>
> **Philipp von der Brüggen, CMO, Natuvion, www.natuvion.de**



Mehr Zeit für's Wesentliche

SAP-TRANSAKTIONEN AUTOMATISIEREN OHNE SAP GUI ANZUSTEUERN

In der Regel werden in Unternehmen die meisten SAP-Anwendungen und -Prozesse klassisch per Transaktionsaufruf in der SAP GUI verwendet. Doch die Dateneingabe über die SAP GUI ist grundsätzlich für die meisten Prozesse nicht selbsterklärend und erfordert zeitaufwändige Anwenderschulungen, weil unübersichtliche Eingabemasken gespickt mit technischen Feldern und Menüs vorherrschen. Insbesondere bei komplexen Transaktionen wie der Personalstammdatenpflege ist oft der Frust der Anwender groß und die Einarbeitung eine Herausforderung, da sie Zeit und Ressourcen verschlingt. Wenn darüber hinaus Daten zwischen SAP und anderen Anwendungen ausgetauscht werden, ist sogar meistens manuelle Doppelpflege nötig. Grund: SAP erlaubt von Haus aus keinen einfachen Datenaustausch mit Drittsystemen. All diese Probleme führen zu Fehlern, ineffizienten Geschäftsprozessen und beeinträchtigen somit die Produktivität und Rentabilität eines Unternehmens erheblich.

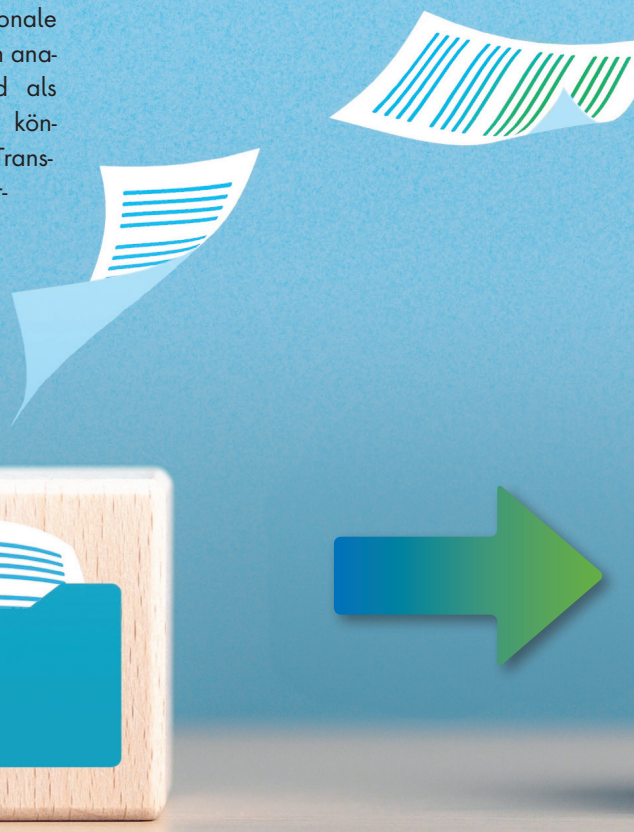
Automatisierung von SAP-Transaktionen

Eine Funktion, die die vollständige Automatisierung von SAP-Transaktionen ermöglicht, ist etwa das Transaction Feature in yunIO, der Schnittstellenlösung zur Prozessintegration von Theobald Software. yunIO ist ein No-Code-Konnektor für die Gestaltung, Automatisierung und Integration von SAP-Prozessen mit einer Vielzahl von (Cloud-) Anwendungen und Plattformen. Das nun integrierte Transaction Feature ermöglicht Anwendern und Powerusern SAP-Transaktionen und -Prozesse außerhalb der SAP GUI anzusteuern und zu automatisieren. Dank dieser Komponente können Unternehmen häufig genutzte SAP-Transaktionen konfigurieren und parametrisieren und somit für den externen Aufruf verfügbar machen. Eine derartige Funktion ist für alle SAP nutzenden Unternehmen relevant, die ihre SAP-Prozesse mit anderen Nicht-SAP Umgebungen integrieren, individualisieren und automatisieren möchten.

Die Bearbeitung von SAP-Transaktionen erfolgt über ein bestimmtes technisches Protokoll, das es ermöglicht, direkt über den yunIO Designer auf SAP zuzugreifen – so, als würde man in der SAP GUI arbeiten. Der Vorteil besteht darin, dass mit diesem Ansatz vertraute transaktionale Prozesse im yunIO Designer einfach analog durchlaufen, gespeichert und als Webservice bereitgestellt werden können. Für solche aufgezeichneten Transaktionen ist es dann nicht mehr erforderlich, diese direkt in SAP auszuführen. Sie können dann über individuell gestaltbare Anwendungen und Oberflächen in der vertrauten Umgebung, zum Beispiel einem Mitarbeiterportal, bereitgestellt werden. Für diejenigen, die selbst über keinen SAP-Zugang verfügen und auch keine tiefergehenden SAP-Kenntnisse besitzen, erweitert sich das Nutzerfeld: Denn die Integration der Schnittstelle verringert auch die Komplexität eines SAP-Prozesses, etwa durch weniger Eingabefelder und individuelle Feldnamen. Zudem kann der Entwicklungsaufwand von SAP-Integrationsprojekten reduziert werden, das heißt: Der Project Owner kommt sehr schnell zu vorzeigbaren Ergebnissen.

Automatisierung mit Schnittstellen in der Praxis

Doch wie sieht die Umsetzung in der Praxis aus? In der HR-Abteilung – eine Ab-



teilung die nur bedingt täglich mit SAP arbeiten muss – existieren beispielsweise wiederkehrende, nicht alltägliche SAP-Transaktionen, die sich optimieren lassen:

1. Personalstammdaten ändern: Die Transaktion PA30 wird dazu genutzt, Stamm- oder Personalakten von Mitarbeitenden zu bearbeiten. Hierzu zählen Personal- und Gehaltsinformationen sowie Arbeitszeiten. Die Bearbeitung in SAP ist komplex und aufwändig. Fehler würden hier nicht nur bei Mitarbeitenden für Frust sorgen, sondern erhebliche Auswirkungen auf Geschäftsprozesse haben, etwa durch falsche Gehaltsabrechnungen oder Arbeitszeiterfassungen. Dank einer Schnittstelle lassen sich Fehlerquellen minimieren, da eine benutzerfreundliche Oberfläche – ein einziges, übersichtliches Eingabeformular – sowie eine einfache Navigation die Bearbeitung spürbar vereinfachen.

2. Onboarding von neuen Mitarbeitern: Auch der Onboarding-Prozess wird einfacher: Grundsätzlich umfasst die genutzte SAP-Transaktion PA40 mehrere Schritte, um die Erfassung und Verwaltung der Personalbasisdaten neuer Mitarbeitender in SAP zu ermöglichen. Der manuelle Prozess ist mühselig, fehleranfällig und besonders zeitaufwändig. Mit der SAP-Integration in die Nintex Automation Cloud wird es einfacher für alle Beteiligten: Die Personalbasisdaten werden außerhalb des SAP-Systems von neuen Mitarbeitenden über ein Webformular oder eine App erfasst. Die Daten werden im Hintergrund automatisiert in die SAP-Transaktion PA40 übertragen.

SCHNITTSTELLEN MIT AUTOMATISIERUNGSFUNKTION ERLEICHTERN DIE WORKFLOWS VON MITARBEITERN, MINIMIEREN FEHLER UND OPTIMIEREN GESCHÄFTSPROZESSE.

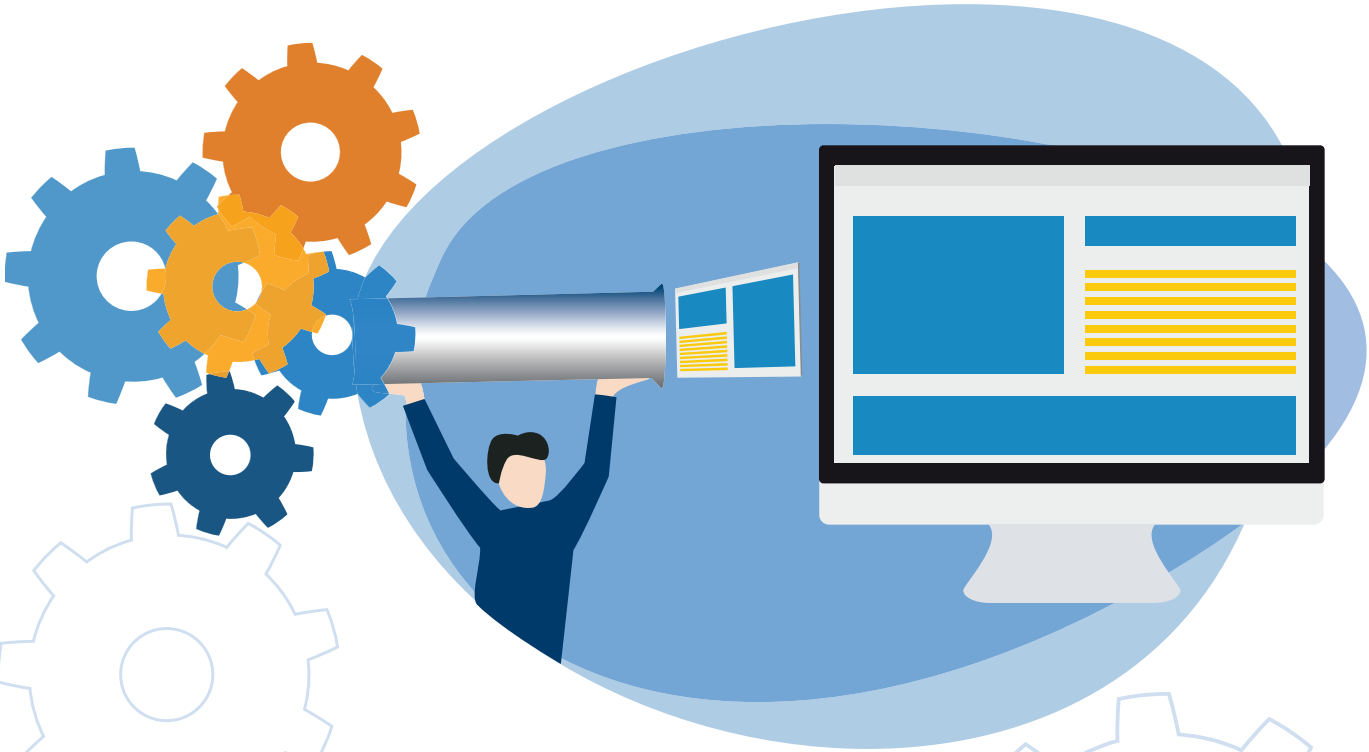
Christian Tauchmann, Software Consultant, Theobald Software GmbH, www.theobald-software.com

3. Auch das Sales-Department profitiert von vereinfachten Prozessen: Hier wird die SAP-Transaktion VA02 zur Bearbeitung von Kundenaufträgen genutzt. Mit ihr werden Auftragsdaten bearbeitet, Auftragspositionen organisiert, Preise und Konditionen verwaltet oder Liefertermine festgesetzt. Kommt es bei einem Kundenauftrag einmal zu einer Zahlungssperre, wird es jedoch kompliziert: Um diese einzurichten sind weiterführende SAP-Kenntnisse notwendig. Denn Anwender müssen mehrere Schritte in der SAP GUI durchlaufen und einen Funktionsbaustein aufrufen, der im Standard verschiedene Felder enthält. Zeitaufwändiger wird es, wenn nur bestimmte Felder oder Feldgruppen geändert werden. Mit der Schnittstelle inklusive Transaction Feature wird die Zahlungssperre in der VA02 aufgezeichnet und über eine übersichtliche PHP-Webseite mit JavaScript aufgerufen. Relevante Informationen sind übersichtlich dargestellt und es besteht Zugriff auf die entsprechenden Felder - eine enorme Erleichterung bei der Einrichtung sowie Aktualisierung beispielsweise von Zahlungssperren.

Fazit

Die Nutzung einer Schnittstelle, wie etwa yunIO von Theobald Software, sorgt für erhebliche Kosteneinsparungen, da keine eigene API für SAP-Transaktionen entwickelt werden muss. So besteht die Möglichkeit, jede Bildschirmtransaktion in SAP über einen Webservice zu steuern. Installation und Handhabung sind sehr einfach gehalten und funktionieren ohne jegliche Programmierung. Mit einer Funktion wie dem Transaction Feature auf No-Code-Basis kann eine Schnittstellenlösung über die Funktionalität des klassischen SAP-Transaktionsrekorders hinausgehen. So können Anwender auch komplexere Transaktionen simpel umsetzen, wie zum Beispiel im HR-Bereich die Personalstammdatenpflege (Transaktion PA30) und das Ausführen von Personalmaßnahmen (PA40) sowie im Sales-Bereich (Transaktion VA02). Innerhalb kürzester Zeit können Nutzer so Anwendungsszenarien umsetzen, die ohne die Software nicht oder nur mit hohem (Entwicklungs-) Aufwand realisierbar wären. Damit birgt das Tool Potenzial, die Art und Weise grundlegend zu verändern, wie Unternehmen SAP zur Prozessautomatisierung einsetzen.

Christian Tauchmann



Testdatenmanagement

MASSGESCHNEIDERTE TESTDATEN IN EINER AWS CODEPIPELINE ERSTELLEN

– TEIL 3 VON 5 –

Diese fünfteilige Artikelserie behandelt das Thema Testdatenmanagement (TDM) in der IT-Landschaft, das eine zentrale Rolle in der Qualitätssicherung von Softwareprodukten spielt. Die Serie beleuchtet verschiedene Aspekte des TDMs, einschließlich bewährter Praktiken, Herausforderungen und innovativer Lösungen.

Um das Verhalten einer Anwendung während der Produktion genau zu bewerten, benötigen Entwickler normalerweise eine Testumgebung, die der endgültigen Produktionsumgebung möglichst nahe kommt. Jedoch wird eine Testumgebung zwangsläufig nicht dasselbe Sicherheitsniveau wie die endgültige Produktionsumgebung haben. Dies stellt ein Problem dar, wenn Testdaten erstellt und später im Testprozess verwendet werden müssen. Tester stehen vor der Entscheidung, ob sie eine Kopie von bereinigten Produktionsdaten verwenden oder möglichst realistische synthetische Testdaten erzeugen sollen.

TDM umfasst verschiedene Aufgaben wie die Bereitstellung von Testdaten, Anonymisierung und Maskierung sensibler Daten, die Bildung von Teilmengen, die Sicherstellung von Datenkonsistenz sowie die Integration in CI/CD-Pipelines. Ein effektives TDM trägt zur Verbesserung der Softwarequalität bei, indem es Tests unter realistischen Bedingungen ermöglicht, potenzielle Probleme frühzeitig erkennt und die Effizienz von Testprozessen steigert.

Die Serie hebt die TDM-Funktionen von IRI Voracity hervor, einer End-to-End Datenmanagementplattform, die Datenerkennung, -integration, -migration und -verwaltung in einem Metadaten-Framework vereint. Die Verwendung von IRI Voracity ermöglicht eine effiziente Bedienung und führt zu Kosteneinsparungen in vernetzten IT-Umgebungen.

Im vorherigen Beitrag wurde die Erstellung von Testdaten in einer GitLab-Pipeline behandelt, wobei sowohl strukturierte Datenmaskierung als auch Datensynthese-Jobs verwendet wurden, um Testdaten zu generieren. Diese wurden dann in API-Tests nach der Bereitstellung eingesetzt. Dieser Artikel hingegen beschäftigt sich mit der Durchführung von Datenmaskierungs-Jobs in der AWS CodePipeline unter Verwendung von SSH-Befehlen. Dies ermöglicht die maßgeschneiderte Generierung von Testdaten im Rahmen des DevOps-Prozesses. Zusätzlich wird die Dateien-API auf einem entfernten Server aufgerufen, was eine alternative Methode zur Erzeugung angepasster Testdaten darstellt.

AWS CodePipeline

Die Amazon Web Service CodePipeline ist ein automatisierter Continuous Delivery-Service (CD), der schnelle und zuverlässige Updates ermöglicht. Es automatisiert den Erstellungsprozess sowie Test- und Bereitstellungsstadien für Codeände-

rungen basierend auf benutzerdefinierten Veröffentlichungsmodellen. Dadurch werden neue Funktionen und Updates zeitnah bereitgestellt und es besteht die Möglichkeit, benutzerdefinierte Plug-ins zu verwenden. Die Automatisierung des Entwicklungs-, Test- und Veröffentlichungsprozesses ermöglicht eine schnelle Bereitstellung neuer Funktionen und erleichtert das Testen von Codeänderungen ohne Verzögerungen.

Gemäß der AWS-Dokumentation ist eine Pipeline ein Workflow-Konstrukt das beschreibt, wie Softwareänderungen einen Freigabeprozess durchlaufen. Die Pipelines bestehen aus Einheiten, die Stufen (Build, Test, Bereitstellung) genannt werden. Jede Stufe besteht wiederum aus einer Reihe von Operationen, die als Aktionen bezeichnet werden. Die Aktionen sind so konfiguriert, dass sie an bestimmten Punkten in der Pipeline ausgeführt werden. Ein Beispiel für eine Aktion wäre eine Bereitstellungsaktion in einer Bereitstellungsstufe, die Code auf einen Berechnungsdienst bereitstellt. Jede Aktion kann seriell oder parallel innerhalb einer Stufe ausgeführt werden. Jede Aktionsart hat einen akzeptierten Satz von Anbietern, das im Feld „Provider" in der Aktionskategorie der Pipeline enthalten sein muss. Die folgenden sind gültige Aktionsarten in CodePipeline:

- Quelle
- Build
- Test
- Bereitstellung
- Genehmigung
- Aufruf

Kombination mit IRI Voracity

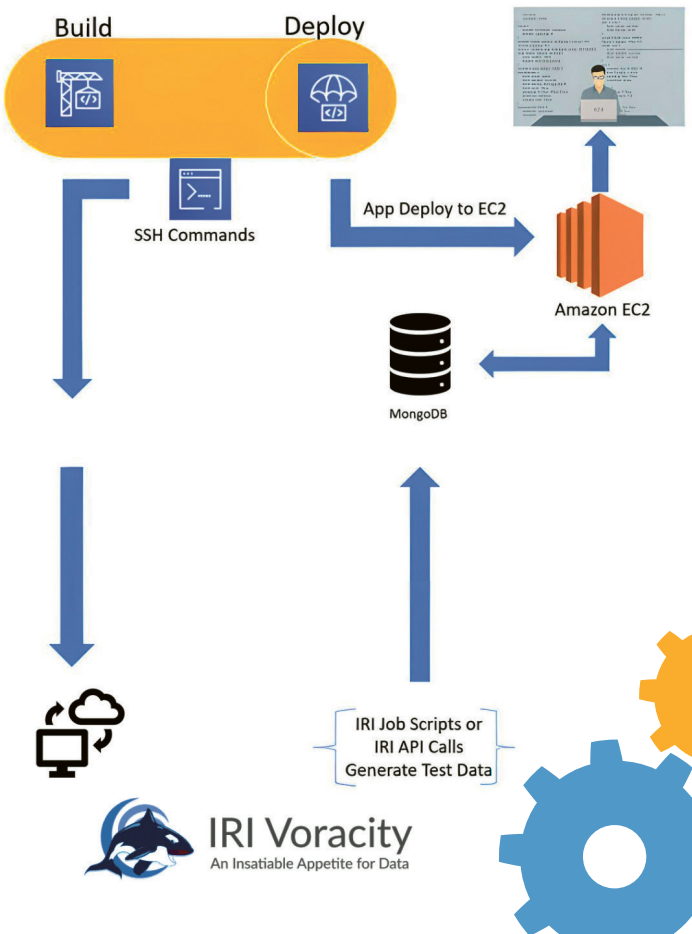
Eine Komponente der IRI Voracity-Datenverwaltungsplattform bietet umfassende Funktionen zur Maskierung sensibler Daten in semi- und unstrukturierten Quellen wie NoSQL-Datenbanken (einschließlich

IRI VORACITY BIETET EINE UMFASSENDE LÖSUNG ZUR AUTOMATISIERUNG VON TESTPROZESSEN UND GENERIERUNG MASSGESCHNEIDERTER TESTDATEN AUS VERSCHIEDENEN QUELLEN.

Amadeus Thomas, Geschäftsführer, JET-Software, www.jet-software.com

DynamoDB), PDFs, Microsoft Word, Text- und Bilddateien (einschließlich Parquet und DICOM). Sensible Informationen in Flat-Files (lokal oder in Buckets wie S3 gespeichert) und RDBs (normalerweise mit C/BLOB-Daten) können ebenso automatisch erkannt und geschützt werden. Durch die Integration in AWS CodePipeline können Testdaten-produzierende Jobs automatisiert ausgeführt werden. Die buildspec.yml-Datei kann dabei an einer beliebigen Anzahl von Orten wie Amazon S3, Amazon ECR, CodeCommit, BitBucket, GitHub und GitHub Enterprise Server gespeichert sein. Durch die Verwendung von SSH können Jobskripte oder API-Routinen nahtlos in der Pipeline ausgeführt werden. Dies verbessert die Effizienz des CI/CD-Prozesses und ermöglicht Entwicklern die Automatisierung verschiedener Aufgaben.

BILD 1: AWS DIAGRAMM



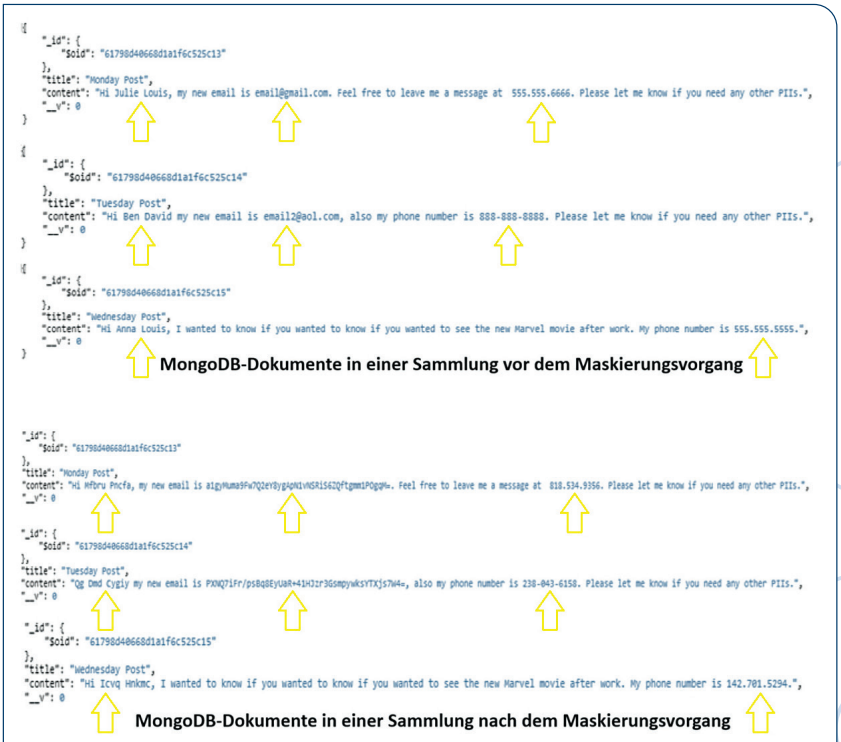


Bild 2: Die sensiblen PII wurden erfolgreich identifiziert und mittels Anonymisierung, Pseudonymisierung und gezielter Datenmaskierung auf Feldebene geschützt.

Ausführen der Build-Stufe

Die Phase der Testdatengenerierung in der Build-Stufe beinhaltet das Ausführen eines IRI Voracity-Jobskripts auf dem Server, auf dem die IRI Voracity Plattform installiert ist. Nach Abschluss dieser Phase zeigt die AWS-Pipeline-Konsole eine erfolgreiche Build-Nachricht an. Ein typischer Ablauf könnte die Verwendung eines Python-Skripts umfassen, das die IRI Voracity-API auf einem Remote-Server aufruft, um JSON-Beiträge zu suchen und zu maskieren, die in einer Sammlung auf einem Test-MongoDB-Cluster in AWS gespeichert sind. Die Protokolldatei der Build-Stufe bestätigt dann die erfolgreiche Herstellung der Verbindung zum Remote-Server und den erfolgreichen Aufruf der IRI Voracity-API. Damit können sensible Informationen (PII) wie Namen, E-Mail-Adressen, Telefonnummern und weiterer Informationen automatisch identifiziert und mithilfe diverser Verfahren auf Feldebene geschützt werden. Nach Abschluss dieser Such- und Maskierungsvorgänge werden die maskierten Dateien in der benutzerdefinierten Sammlung im Cloud-MongoDB-Cluster entsprechend platziert.

Fazit

IRI Voracity bietet eine umfassende Lösung zur Automatisierung von Testprozessen und Generierung maßgeschneiderter Testdaten aus verschiedenen Quellen. Die Testdatenbereitstellung mit IRI Voracity ermöglicht die Erstellung von Datenbanken mit referenzieller Integrität und die Simulation verschiedener Datenformate. Die Automatisierung unterstützt DevOps durch Konsistenz, Geschwindigkeit und Zuverlässigkeit.

Der Artikel zeigt, dass man mit AWS CodePipeline die Ausführung von Testdaten-produzierenden Jobs von IRI Voracity automatisieren kann. Mithilfe von SSH können beliebige Jobskripte oder API-Routinen, die von der Befehlszeile aus ausgeführt werden können, innerhalb der Pipeline ausgeführt werden. Da der Backend-Motor ein ausführbares Programm ist, kann IRI Voracity von der Befehlszeile aus ausgeführt werden. Die Integration von Voracity in den CI/CD-Prozess ermöglicht die nahtlose Automatisierung von Aufgaben wie der Generierung synthetischer Testdaten oder der Maskierung sensibler Daten.

Die Einrichtung einer Pipeline erfordert zwar einige Schritte, aber sie ist ein wertvolles Werkzeug im Entwicklungsprozess. Die Integration von Voracity in den CI/CD-Prozess verbessert die Effizienz und ermöglicht Entwicklern die Automatisierung verschiedener Aufgaben.

Amadeus Thomas

AUSBLICK

Ob es sich um die Generierung synthetischer Testdaten, die Maskierung strukturierter Daten, semistrukturierter oder unstrukturierter Daten handelt, es ist möglich, IRI Voracity Jobskripte in den DevOps-Prozess durch die CI/CD-Pipeline zu integrieren. Mein nächster Artikel wird dies in Azure DevOps demonstrieren.

BUSINESS ANALYSE

EINFACH UND EFFEKTIV

Unternehmen müssen in der Lage sein, sich zu verändern und an die jeweiligen Markt- und Wirtschaftsbedingungen schnell anzupassen. Die Tätigkeit der Business-Analyse und deren organisatorische Verankerung im Demand Management sind wesentliche Erfolgsfaktoren dafür. Die erforderlichen Veränderungen werden erkannt, fachlich gestaltet und umgesetzt. Das Projektportfolio sowie die einzelnen Projekte und Wartungsmaßnahmen werden an den Geschäftserfordernissen ausgerichtet und die Produktivität bei der Umsetzung wird gesteigert. Anzahl und Umfang von Geschäftsanforderungen werden durch frühzeitige Prüfung auf Nutzen, Konsistenz und Wichtigkeit deutlich reduziert. Unnötige Doppelarbeiten und wertvernichtende Projekte werden vermieden. So entstehen Freiräume für strategische Vorhaben.

Wir stellen in diesem Buch Grundlagen und Best-Practices zur Durchführung der Business-Analyse bereit und helfen Ihnen, das Demand-Management bei klassischem und agilem Vorgehen mit Leben zu füllen.

Business Analyse
einfach und effektiv

Inge Hanschke, Daniel Goetze; Carl Hanser Verlag GmbH & Co.KG; 03-2024

Datenschutz, KI und Edge Computing

STRATEGIEN FÜR EINE SICHERE DATENVERWALTUNG

Mit einem zunehmenden Bewusstsein der Verbraucher sowohl für den Wert ihrer Daten als auch deren Bedrohungen war es noch nie so entscheidend für Führungskräfte, die Privatsphäre der Nutzer zu respektieren. Datenverstöße nehmen in einem beispiellosen Tempo zu, wobei im ersten Quartal 2023 weltweit mehr als sechs Millionen Datensätze durch Datenverstöße freigelegt wurden. Des Weiteren machen es Regulierungen wie die DSGVO (Datenschutz-Grundverordnung) der EU und der CCPA (California Consumer Privacy Act) für Unternehmen auch immer dringlicher, sicherzustellen, dass sie angemessene Schutzmaßnahmen für Verbraucherdaten haben. Führungskräfte müssen Transparenz gewährleisten und aufkommende Technologien nutzen, um einen ausgewogenen Ansatz zu finden, der private Daten respektiert und gleichzeitig innovative Dienste bereitstellt.

Auch neue Technologien werden eine entscheidende Rolle spielen, wenn es darum geht, Daten im großen Maßstab zu nutzen. Jede Sekunde generiert jede Person im Schnitt auf der Erde etwa 1,7 Megabyte Daten – ein Trend, der mit jedem Jahr zunimmt. Künstliche Intelligenz (KI) und Edge Computing werden entscheidend sein, um Daten dieser Größenordnung Herr zu werden und gleichzeitig die intelligenten, personalisierten Dienste bereitzustellen, die sich Verbraucher wünschen. Die Zukunft des Datenschutzes ist eng mit diesen aufkommenden Technologien verbunden, wobei Edge Computing dabei hilft zu kontrollieren, wo Daten verarbeitet werden, und KI sowohl Chancen als auch Herausforderungen im Hinblick auf Datenschutz bietet. Techniken wie Anonymisierung, föderales Lernen und homomorphe Verschlüsselung können ebenfalls helfen, den Datenschutz in den Vordergrund zu stellen.

> SOWOHL KI ALS AUCH EDGE COMPUTING WERDEN DIE ART UND WEISE VERÄNDERN, WIE DIE WELT ÜBER DEN SCHUTZ PERSÖNLICHER DATEN DENKT.
>
> **Paul Höcherl, Product Manager ISG, Lenovo, www.lenovo.com**

Für Führungskräfte kann es schwerwiegende finanzielle Strafen und einen Mangel an Verbrauchervertrauen nach sich ziehen, falls sie es versäumen, den Datenschutz zu berücksichtigen. Wenn Unternehmen den Datenschutz ernsthaft wahren wollen, müssen sie eng mit Sicherheitsexperten, Regulierungsbehörden und Drittparteien zusammenarbeiten, um ihren Weg zu planen und Datenschutz in alles, was sie tun, zu integrieren.

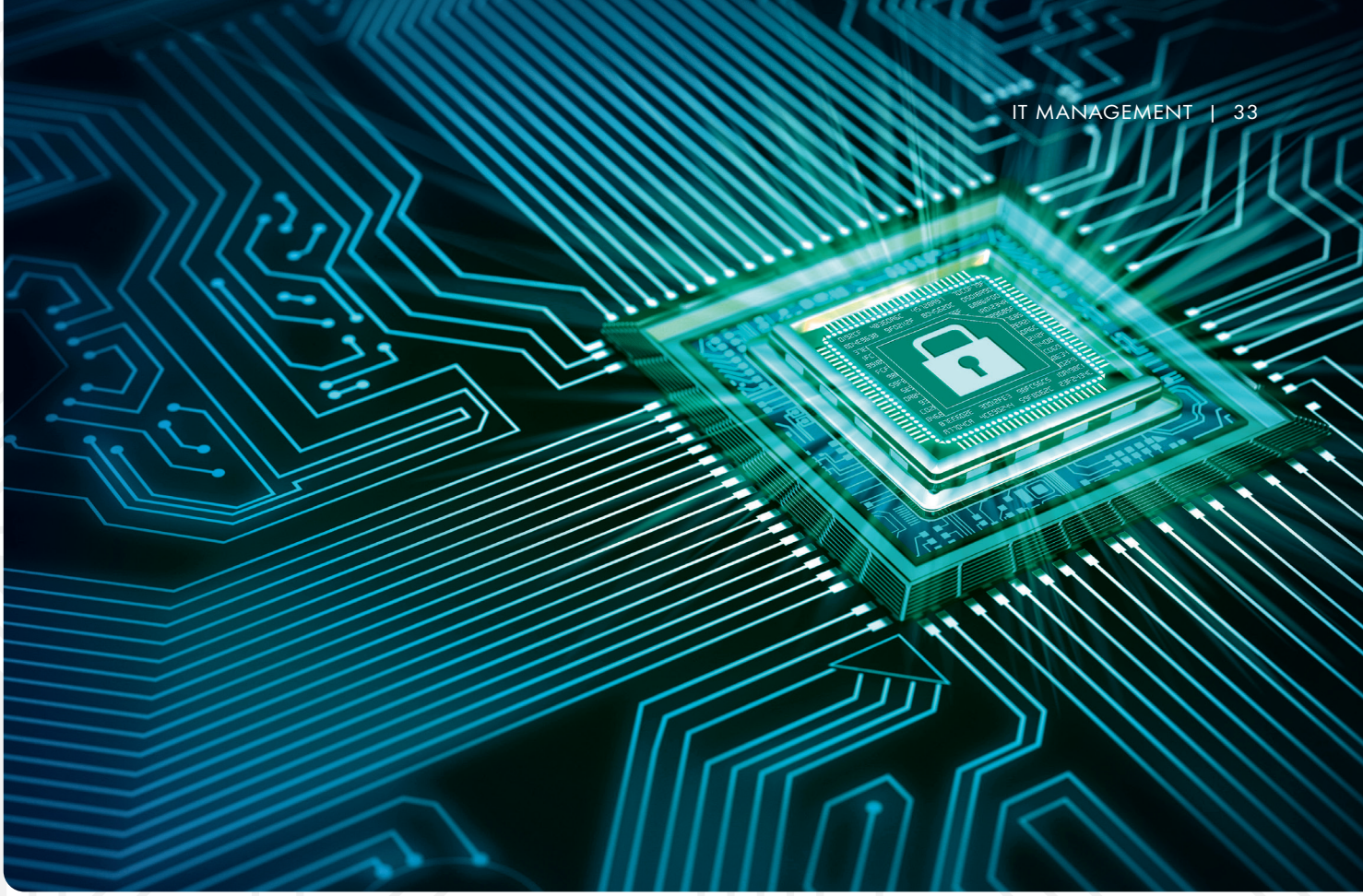
Datenschutz am Netzwerkrand

Sowohl KI als auch Edge Computing werden die Art und Weise verändern, wie die Welt über den Schutz persönlicher Daten denkt. Edge Computing bietet mit seiner dezentralen Verarbeitungsfähigkeit erhebliches Potenzial, den Datenschutz zu verbessern. Indem es Daten näher an der Quelle verarbeiten lässt, bedeutet dies beispielsweise, dass ein Kamerasystem Aufnahmen aufzeichnen kann, aber nur anonymisierte Daten zur Cloud zur Verarbeitung und Speicherung weiterleitet. Durch die Reduzierung der Übertragung und Speicherung potenziell sensibler Daten kann Edge Computing das Risiko von Datenlecks minimieren. Inzwischen setzen auch Unternehmen vermehrt auf Edge Computing-Lösungen. So ergab eine aktuelle Studie von IDC und Lenovo, dass die Ausgaben für Edge Computing im vergangenen Jahr in Deutschland um 20 Prozent gestiegen sind.

Wenn es dann um künstliche Intelligenz geht, sollten Führungskräfte diese mit Bedacht einsetzen. Obwohl sie das Potenzial hat, die Benutzererfahrung oder die Cybersicherheit zu verbessern, indem sie beispielsweise Anomalien erkennt, gibt es auch berechtigte Bedenken hinsichtlich des möglichen Missbrauchs oder der ungewollten Offenlegung sensibler Daten. Generative KI-Systeme haben oft keine Möglichkeit, Informationen zu ‚löschen', was potenziell Probleme im Hinblick auf die langfristige Verwaltung von Daten aufwerfen kann. Entscheider müssen gewährleisten, dass ihre Nutzung von KI robuste Sicherheitsfunktionen umfasst und strenge Datenschutzrichtlinien bei der Identifizierung von Daten durchgesetzt werden.

Der Nutzer an erster Stelle

Transparenz ist entscheidend, wenn es um den Datenschutz von Nutzern geht. Führungskräfte müssen sicherstellen, dass



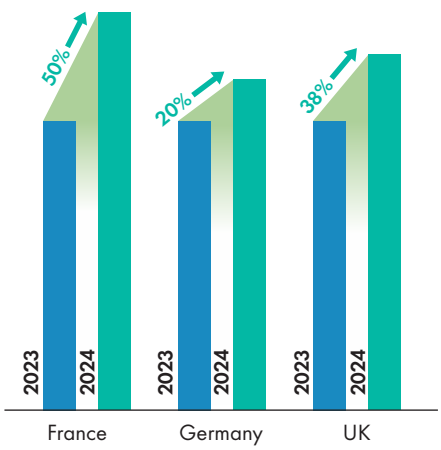
Kunden klar darüber informiert sind, wann ihre Daten erfasst werden und wie sie verwendet werden. Dies ist sowohl für die Einhaltung von Vorschriften als auch für den Aufbau von Nutzervertrauen unerlässlich.

Nicht zu unterschätzen ist außerdem die Aufklärung der Nutzer selbst. Führungskräfte sollten Verbrauchern die Informationen zur Verfügung stellen, die erforderlich sind, damit sie ihre eigenen informierten Entscheidungen über Daten treffen können. Datenschutzrichtlinien müssen transparent sein, und Einzelpersonen müssen ermächtigt werden, auf die Daten zuzugreifen, sie zu korrigieren und die Löschung aller Daten zu beantragen, die die Organisation besitzt. Damit alles reibungslos läuft, müssen klare Datenverwaltungspolicen existieren und regelmäßig angepasst werden, um die Datenschutzverordnungen wie die DSGVO zu erfüllen.

Organisationen mit einem Datenschutz-first-Ansatz

Der Aufbau einer Organisation, die den Datenschutz an erste Stelle setzt, erfordert, dass alle an einem Tisch sitzen – angefangen bei den Mitarbeitern bis hin zu Drittanbieterorganisationen. Um eine Kultur der Datensicherheit zu fördern, ist es wichtig, dass Mitarbeiter über grundlegende Datenschutzpraktiken und Speicherungsrichtlinien informiert sind. Dazu gehört beispielsweise die Verwendung von sicheren Passwörtern auf Dienstlaptops sowie das Erkennen von Anzeichen für Phishing-Angriffe. Dies sollte mit der Planung von Incident-Response und regelmäßigen Audits kombiniert werden, um sicherzustellen, dass die gesamte Organisation darauf vorbereitet ist, mit Vorfällen umzugehen, und dass Mitarbeiter ein vollständiges Verständnis für die Bedeutung der Datensicherheit haben.

EDGE COMPUTING



Um sicherzustellen, dass Daten geschützt sind, müssen auch externe Anbieter sich an die strengsten Datenschutzstandards halten. Cyberkriminelle suchen stets nach dem schwächsten Glied in der Kette, ob es nun ein Rechtsunternehmen, ein Buchhalter oder ein Softwareanbieter ist, und jede Sicherheitslücke eines Drittanbieters wird sich negativ auf jedes Unternehmen auswirken, das ihre Dienste nutzt.

Führungskräfte sollten sicherstellen, dass sie Technologie auf eine Weise einsetzen, die die Bedenken der Benutzer hinsichtlich ihrer Daten respektiert, und darauf abzielen, Datenschutz, Benutzerfreundlichkeit und Innovation in Einklang zu bringen. Der menschliche Aspekt ist entscheidend, wobei transparente Kommunikation Verbrauchern hilft, informierte Entscheidungen zu treffen, und Gespräche mit Drittanbietern zunehmend erforderlich sind, da sich Vorschriften auf der ganzen Welt weiterentwickeln. Die richtigen Technologieentscheidungen bezüglich Datenverwaltung, Anonymisierung und KI sind zentral, um Organisationen zu schaffen, die den Datenschutz an erste Stelle setzen und für die Welt von morgen gerüstet sind.

Paul Höcherl

Navigieren durch die Datenflut

STRATEGIEN FÜR BESSERE DATENINTEGRITÄT

Vielleicht kennen Sie das: Briefe sind unzustellbar, weil Teile der Anschrift fehlen, Ansprechpartner arbeiten gar nicht mehr im Unternehmen, ...

Auf der anderen Seite basieren immer mehr Entscheidungen auf Daten. Business Intelligence und Künstliche Intelligenz benötigen valide Daten für zielführende Ergebnisse. Gartner prognostizierte bereits vor einigen Jahren, dass 2022 85 Prozent der KI-Projekte aufgrund falscher Daten fehlerhafte Ergebnisse liefern.

In vielen Daten- und Applikationsinseln befinden sich redundante Daten. Durch die Digitalisierung und Internet-of-Things fallen zugleich immer mehr Daten an. Unternehmen drohen an der Datenflut zu ersticken. Um Daten effektiv zu nutzen, gewinnt das Thema Datenqualität deshalb immer mehr an Bedeutung.

WIE MISST MAN DATENQUALITÄT?
Datenqualität lässt sich in 9 Dimensionen messen:

Vollständigkeit
Fehlen Daten? Sind bei einer Anschrift zum Beispiel Straße, Hausnummer, PLZ, Ort sowie ein Land vorhanden.

Genauigkeit
Stimmen die Daten mit der realen Welt überein? Gibt es die angegebene Straße mit dieser Hausnummer wirklich?

Validität
Entspricht der Datensatz den formalen Datenrichtlinien? Eine Postleitzahl muss in Deutschland zum Beispiel 5 Stellen umfassen.

Einzigartigkeit
Jeder Datensatz darf nur einmal existieren. Ein Dubletten-Check identifiziert etwa doppelte Kontakte in einer CRM-Software.

Konsistenz
Einhaltung von Datenrichtlinien in Bezug auf mehrere Werte. So ist zum Beispiel für einen Datensatz aus Deutschland eine Ländervorwahl der Telefon-Nr. mit +49 plausibel.

Aktualität
Wie weit klafft der Zeitpunkt der Datenerhebung und der -verwendung auseinander?

Nachvollziehbarkeit
Die Kenntnis, woher die Daten stammen und wer die Daten wie verändert hat.

Klarheit
Anwender verstehen, in welchem Datenfeld sich welche Informationen befinden.

Verfügbarkeit
Wie einfach können Anwender auf die Daten zugreifen?

Data Quality Management, kurz DQM, umfasst alle Maßnahmen eines Unternehmens, seine Daten dauerhaft und im Zeitverlauf zu erhalten.

AUFGABEN UND ZIELE

Quality Management umfasst fünf große Aufgabenbereiche:

#1 Datenanalyse und -bewertung

Eine gründliche Bewertung der Daten legt den Grundstein für die weiteren Schritte im Data Quality Management Prozess. Hierbei werden Datenquellen identifiziert, Datenqualitätsprobleme erkannt und die Priorisierung der zu bearbeitenden Daten festgelegt.

#2 Datenbereinigung und -standardisierung

Nach der Analyse folgt die Datenbereinigung. Dabei werden inkonsistente, fehlerhafte oder veraltete Daten bereinigt und standardisiert. Die Daten werden in einheitlicher Form strukturiert, um die Konsistenz und Genauigkeit zu gewährleisten.

#3 Datenvalidierung und -überwachung

Die Datenvalidierung ist ein wesentlicher Schritt im Data Quality Management. Hierbei werden die Daten auf Plausibilität und Richtigkeit geprüft. Es ist wichtig, die Daten kontinuierlich zu überwachen, um sicherzustellen, dass sie auch langfristig von hoher Qualität bleiben.

#4 Implementierung von Datenqualitätsstandards

Legen Sie Datenqualitätsstandards fest und implementieren Sie diese im Unternehmen.

#5 Schulung und Sensibilisierung der Mitarbeiter

Bieten Sie für Mitarbeiter regelmäßig Schulungen an. Fördern Sie das Verständnis für Data Quality Management und sensibilisieren Sie die Mitarbeiter für ihre Rolle bei der Datenqualität.

HERAUSFORDERUNG UND HÄUFIGE PROBLEME

Viele Unternehmen stehen beim Thema Daten-Qualitätsmanagement vor diesen vier Herausforderungen:

#1 Datenkomplexität und -vielfalt:

In Unternehmen gibt es eine Vielzahl unterschiedlicher Datenquellen und Anwendungen. Das erschwert die Implementierung eines einheitlichen Daten-Qualitätsmanagements.

#2 Datenmigration und -integration:

Werden Daten aus verschiedenen Systemen zusammengeführt, besteht die Gefahr von Inkonsistenzen oder Datenverlust. Datenmigration und -integration sind komplexe Aufgaben, die sorgfältig zu planen sind.

#3 Menschliche Fehler:

Viele Daten werden manuell von Mitarbeitern bearbeitet. Dadurch schleichen sich leicht Fehler ein. Eine umfassende Schulung der Mitarbeiter ist unerlässlich. Plausibilitätsprüfungen in Anwendung helfen menschliche Fehler zu vermeiden.

#4 Daten veralten:

Daten sind ständigem Wandel unterworfen. Unternehmen schließen oder firmieren um. Mitarbeiter scheiden aus. Das erfordert eine regelmäßige Überprüfung und Aktualisierung der Daten.

EFFEKTIVES DQM

Mit diesen Praxistipps optimieren Sie sofort Ihre Datenqualität:

Datenvalidierung und Bereinigung:
Die Grundlage jedes Daten-Qualitätsmanagements ist die Validierung und Bereinigung der Daten. Dabei werden die Daten gemäß der 9 Dimensionen der Datenqualität geprüft, um fehlerhafte Daten zu identifizieren.

Einführung von Datenstandards:
Klare Richtlinien für die Bearbeitung und Speicherung von Daten helfen dabei, dass alle Mitarbeiter dieselben Datenpraktiken befolgen. DQM-Systeme, wie zum Beispiel Syncler, unterstützen diesen Prozess, in dem Sie Fehler sichtbar machen und beheben. Das verbessert die Datenqualität erheblich.

Data Governance: Verantwortlichkeiten festlegen
In vielen Unternehmen ist nicht geregelt, wer für Datenqualität und Datenmanagement verantwortlich ist. Data Governance regelt Zuständigkeiten und Rollen der Beteiligten. So stellen Sie sicher, dass die Datenqualität regelmäßig gemessen und Datenrichtlinien eingehalten werden.

Datenqualität im Alltag:
Datenqualität erreichen Sie nicht durch eine einmalige Aktion, sondern ist ein kontinuierlicher Prozess. Es braucht ein System, um Datenqualität regelmäßig zu messen und Daten automatisiert zu bereinigen.

WER KEIN SYSTEMATISCHES DATENMANAGEMENT AUFBAUT, DROHT IN ZUKUNFT AN DER MASSE UNBRAUCHBARER DATEN ZU ERSTICKEN.

Markus Grutzeck, CRM-Berater, Sellmore GmbH, www.sellmore.de

Schulen Sie die Mitarbeiter:
Die häufigsten Fehler in Daten entstehen durch Anwender. Es ist wichtig, Mitarbeiter für die Folgen schlechter Datenqualität zu sensibilisieren. Bieten Sie deshalb regelmäßige Trainings an.

Datenintegration und -standardisierung:
Durch die Vereinheitlichung der Datenstruktur und -formatierung vermeiden Sie Redundanzen und Inkonsistenzen.

Ein Integrationshub, wie Syncler, verbindet Datenquellen und schafft so kontinuierliche Datenströme. Das vermeidet mehrfache manuelle Datenerfassungen durch Mitarbeiter. Es beschleunigt Prozesse und sorgt für konsistente Daten.

Einbeziehung aller Stakeholder:
Datenqualität ist kein Thema eines kleinen Projektteams, sondern betrifft alle. Nutzen Sie das Feedback von Lieferanten, Kunden und Partnern, um alle Anforderungen zu berücksichtigen. Steigern Sie so die Datenqualität kontinuierlich.

AUSBLICK
Wer kein systematisches Datenmanagement aufbaut, droht in Zukunft an der Masse unbrauchbarer Daten zu ersticken. Dem Databerg Report zufolge ist deutschen Firmen der Inhalt - und damit auch der Wert - von 66 Prozent ihrer gespeicherten Daten („Dark Data") unbekannt. Der Anteil von Daten, die redundant, veraltet oder unbedeutend sind, liegt bei 19 Prozent.

Deshalb ist es lohnend, ein Data-Quality-Management-System aufzubauen. Künstliche Intelligenz hält immer mehr Einzug. Die KI basiert auf korrekten Daten. Sonst liefert die KI fehlerhafte Ergebnisse.

Die Zukunft des Data Quality Management (DQM) konzentriert sich auf die Automatisierung von Prozessen, den Einsatz von Künstlicher Intelligenz (KI) und maschinellem Lernen. So identifizieren und beheben Sie Datenqualitätsprobleme proaktiv. Die Integration von DQM in Echtzeit-Datenströme wird wichtiger, um sofortige Korrekturen und Verbesserungen zu ermöglichen. Die Bedeutung von Datenethik und Datenschutz wächst, da Unternehmen den Wert und die Sensibilität der von ihnen verwalteten Informationen erkennen. Insgesamt wird ein umfassenderer, intelligenterer Ansatz für das Datenmanagement erwartet, der sowohl Effizienz als auch Genauigkeit steigert.

Markus Grutzeck

Fluch oder Segen?

SCAN ME

it-daily.net/ki

Mehr Infos dazu im Printmagazin

itmanagement

und online auf www.it-daily.net

Fit für KI

UNTERNEHMEN MÜSSEN IHRE DATENMANAGEMENTSTRATEGIEN OPTIMIEREN

Auch in diesem Jahr wird das Thema Künstliche Intelligenz (KI) heiß diskutiert. Gerade generative KI verzeichnet weiterhin rasante Fortschritte und findet zunehmend Verwendung. Das stellt besonders Analysten und IT-Führungskräfte vor neue Herausforderungen.

Viele deutsche Unternehmen tasten sich bereits an generative KI und Large Language Models (LLMs) heran und nutzen diese, um ihre Betriebsdaten zu verwalten. Laut dem Denodo Data Gap Report 2023 stoßen sie dabei noch häufig auf Probleme und haben Schwierigkeiten, Prozesse in komplexen Umgebungen zu automatisieren (24 Prozent) oder das zunehmend steigende Datenvolumen effizient zu managen (20 Prozent). Zudem fehlt ihnen oftmals ausreichend qualifiziertes Personal, um mit Herausforderungen wie diesen fertig zu werden (21 Prozent). Gefragt ist daher vor allem eines: zuverlässiges und effizientes Datenmanagement. Ohne eine solide Grundlage in diesem Bereich laufen selbst die fortschrittlichsten KI-Projekte Gefahr, unzuverlässige, mangelhafte oder nicht normgerechte Ergebnisse zu liefern.

Mit der fortschreitenden digitalen Transformation gewinnen somit smarte Datenmanagementstrategien zusehends an Bedeutung. Obgleich viele Unternehmen zwar bereits eine entsprechende Strategie implementiert haben, erfordern unvorstellbare Datenmengen und die uneinheitliche Natur der Daten, die durch KI generiert wurden, einen regelrechten Paradigmenwechsel.

ZUKÜNFTIG WIRD ES SICH AUSZAHLEN, BEREITS HEUTE PROAKTIV VERÄNDERUNGEN IM DATAMANAGEMENT EINGELEITET ZU HABEN.

Otto Neuer, Regional VP und General Manager, Denodo, www.denodo.com

Neues Datenzeitalter erfordert neuen Datenmanagementansatz

Herkömmliche Verfahren im Datenmanagement wie die Batch- oder Stapelverarbeitung in Data Warehouses erweisen sich mittlerweile als unzureichend, um den Anforderungen von Echtzeitdaten-Einblicken gerecht zu werden. Halten Unternehmen jedoch beim Versuch KI zu implementieren an diesen Methoden fest, stehen sie ihrem eigenen Fortschritt häufig im Weg.

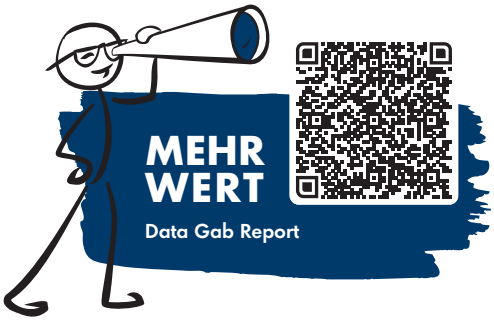
Stattdessen werden Unternehmen, die proaktiv in ein modernes und leistungsfähiges Datenmanagementsystem investieren, besser in der Lage sein das volle Potenzial fortschrittlicher Technologien wie der generativen KI und LLMs auszuschöpfen. Dazu existieren bereits innovative und erprobte Ansätze, die die Schwachstellen herkömmlicher Methoden hinter sich lassen. Zudem ist zu beobachten, dass Unternehmen vermehrt auf Architekturen wie Data Mesh setzen oder Datenkompetenz-Programme für ihre Mitarbeitenden anbieten, um eine datengestützte Entscheidungsfindung zu erleichtern.

Gerade die Vermittlung der Datenkompetenz bei Mitarbeitern ist entscheidend: denn die Komplexität des Datenmanagements in einer KI-basierten Geschäftsstrategie erfordert Erfahrung und kontinuierliches Lernen. Deshalb sollten Unternehmen ihre Mitarbeitenden und Nutzer, die technisch weniger versiert sind, unterstützen und anleiten, um das volle Potenzial der KI im Sinne des Betriebs ausschöpfen zu können.

KI-Integration für eine effizientere Datendemokratisierung

In vielen Fällen können Datenmanagement-Anbieter eine wichtige Stütze für Unternehmen sein, die mit der neuen Datenkomplexität zu kämpfen haben. Dabei erweisen sich vor allem Datenmanagement-Lösungen mit KI-Funktionen als hilfreich, die mit Natural Language Queries ausgestattet und von LLMs unterstützt werden. So sind auch Anwender ohne SQL-Kenntnisse oder Wissen zu Datenspeicherung in der Lage, selbstständig und sicher auf die von ihnen benötigten Daten zuzugreifen.

Zusätzlich können KI-Modelle eingesetzt werden, um Muster in der bisherigen Datenverwendung der Nutzer zu unter-



suchen und anhand dieser Einblicke Anwendern andere relevante Datenquellen empfehlen. Das kann in Form von Vorschlägen wie „Andere Nutzer, die sich diese Datensätze angesehen haben, befanden diese ebenfalls als nützlich" ablaufen. Dieser Ansatz kann nicht nur für Geschäftsanwender, sondern auch für Analysten und Data Scientists zu neuen Datenerkenntnissen führen. All dies trägt dazu bei, den Zugang zu relevanten Daten im gesamten Unternehmen zu verbessern, und hilft letztlich den Unternehmen, ihren Endkunden bessere Dienstleistungen anzubieten.

Ethische Hürden von KI und Datenmanagement meistern

Auch im Hinblick auf ethische Risiken stellt KI die Unternehmen zweifellos vor Herausforderungen. Während GenAI und LLM das Potenzial haben, Betrieben enorme Effizienzgewinne zu bringen, kann es auch unerwartete oder unbeabsichtigte Folgen geben, die gemildert werden müssen. Zwei Aspekte sollten in jedem Fall berücksichtigt werden, um sicherzustellen, dass der Einsatz von KI ethisch vertretbar, robust und in seinen Ergebnissen genau ist:

- Regulierungen: Angesichts des globalen Charakters vieler Organisationen müssen sowohl auf nationaler als auch auf globaler Ebene regulatorische Standards festgelegt werden, unabhängig davon, ob diese von den Regierungen auferlegt oder von den Sektoren freiwillig übernommen werden. Dies ist entscheidend, um Unternehmen und ihre Mitarbeiter bei der ethischen Nutzung von KI zu unterstützen. Während sich die Vorschriften entwickeln, müssen Unternehmen die von ihnen verwendeten Daten überwachen, um Verzerrungen, Ungenauigkeiten oder Urheberrechtsverletzungen in den Ergebnissen von KI-Modellen zu vermeiden.

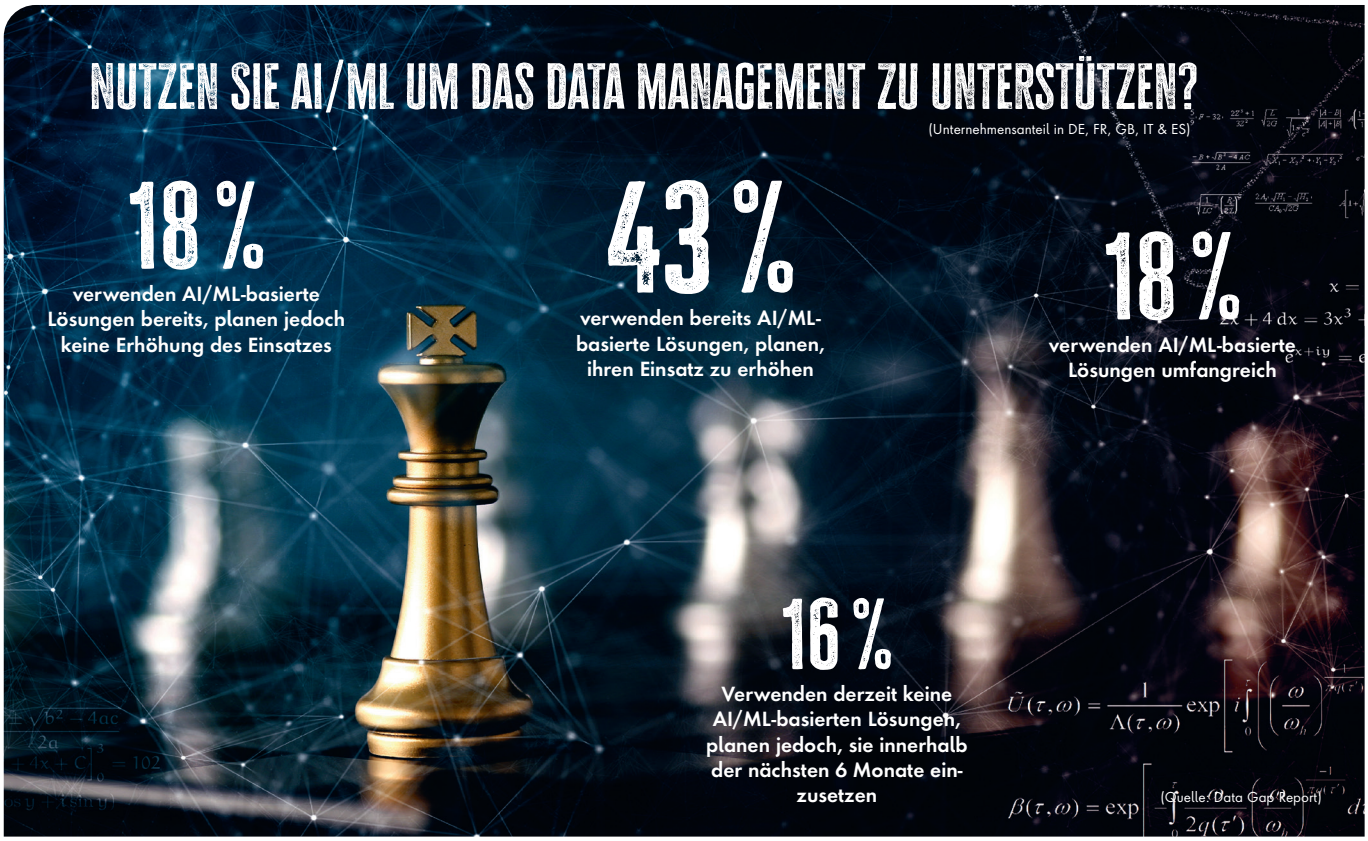
- Zugang: Um zu verhindern, dass unerwünschte Verzerrungen in KI-Modelle einfließen, ist ein möglichst breiter Zugang zu vielfältigen Datenquellen während der Lernphase der KI wichtig. Je größer der Umfang und die Breite der Datenquellen in einem GenAI-Lernmodell ist, desto zuverlässiger arbeitet die KI. Daher sind Datenmanagementplattformen für die nahtlose Datenintegration und -bereitstellung unverzichtbare Komponenten von KI-Architekturen.

Fazit

Die weitere Entwicklung von KI wird maßgeblich durch den Bedarf nach Echtzeit-Daten-Einblicken sowohl für informative als auch operative Zwecke bestimmt. Zukünftig müssen Unternehmen ihre Datenstrategien in Einklang mit den Gegebenheiten der KI bringen und ihren Datenmanagementansatz modernisieren, um Daten zu demokratisieren und eine ethische Nutzung und Output zu gewährleisten.

Seitdem die ersten Chatbots auf Webseiten eingesetzt wurden, hat sich viel getan und weitere spannende Entwicklungen werden folgen. Zukünftig wird es sich auszahlen, bereits heute proaktiv Veränderungen im Datamanagement eingeleitet zu haben.

Otto Neuer



Banking Trends

HERAUSFORDERUNGEN

Es scheint, als ob noch nie derlei viele Aspekte die Gestaltungsmöglichkeiten in der Finanzdienstleistungsbranche beeinflusst haben wie derzeit. Gesellschaftlich, technologisch, regulativ: an allen Ecken warten Herausforderungen auf die Akteure. ibi research erfasst ein aktuelles Stimmungsbild der Branche. Auf Basis einer Status quo-Recherche wurde eine onlinebasierte Experten-Befragung konzipiert, die auf die wesentlichen Trends der nächsten zwei bis drei Jahre in der Finanzdienstleistung abzielt.

Kern der Befragung bilden Untersuchungshypothesen und Szenarien, die auf die zukünftige Situation im Privat- und Firmenkundengeschäft in den genannten Bereichen fokussieren. Angereichert werden diese jeweils um die Beurteilung der Marktpotenziale sowie um die Einschätzung der Bedarfe für die jeweiligen Marktteilnehmer.

Ein breites Themenspektrum zeigt die Vielzahl der Herausforderungen, die Befragungsergebnisse bilden die zum Teil sehr differenzierte Meinungsbildung ab, beispielhaft seien folgende genannt:

#1 Banking of Things: Obwohl Kunden sowohl den Einsatz von Banking of Things erwarten als auch durch Banking of Things wichtige Erkenntnisse über deren Vorlieben und Verhaltensweisen vorliegen würden und infolgedessen Entscheidungen passgenauer getroffen werden können, äußern sich die Experten skeptisch in Bezug auf den tatsächlichen Einsatz und die zu hebenden Geschäftspotenziale.

#2 Cloud Banking: Die Auslagerung in die Cloud wird übergreifend nicht als „Allheilmittel" angesehen, vor allem der Aspekt der Sicherheit bleibt auch in diesem Zusammenhang herausfordernd. Die „eine" richtige Cloud-Strategie gibt es dabei nicht: eine Cloud-Too-Strategie wird von der Hälfte der Befragten präferiert, allerdings bevorzugen gleichzeitig mehr als ein Drittel eine Cloud-First-Strategie.

#3 Generative KI: Für den Einsatz Generativer KI ist die Generierung passender Daten von entscheidender Bedeutung. Die Experten äußern sich skeptisch in Bezug auf das Vorliegen dieser Daten in der Bankbranche. Passend dazu wird davon ausgegangen, dass Kreditinstitute vor allem auf zugelieferte, vortrainierte Basismodelle der Generativen KI von spezialisierten Anbietern zurückgreifen werden.

www.ibi.de

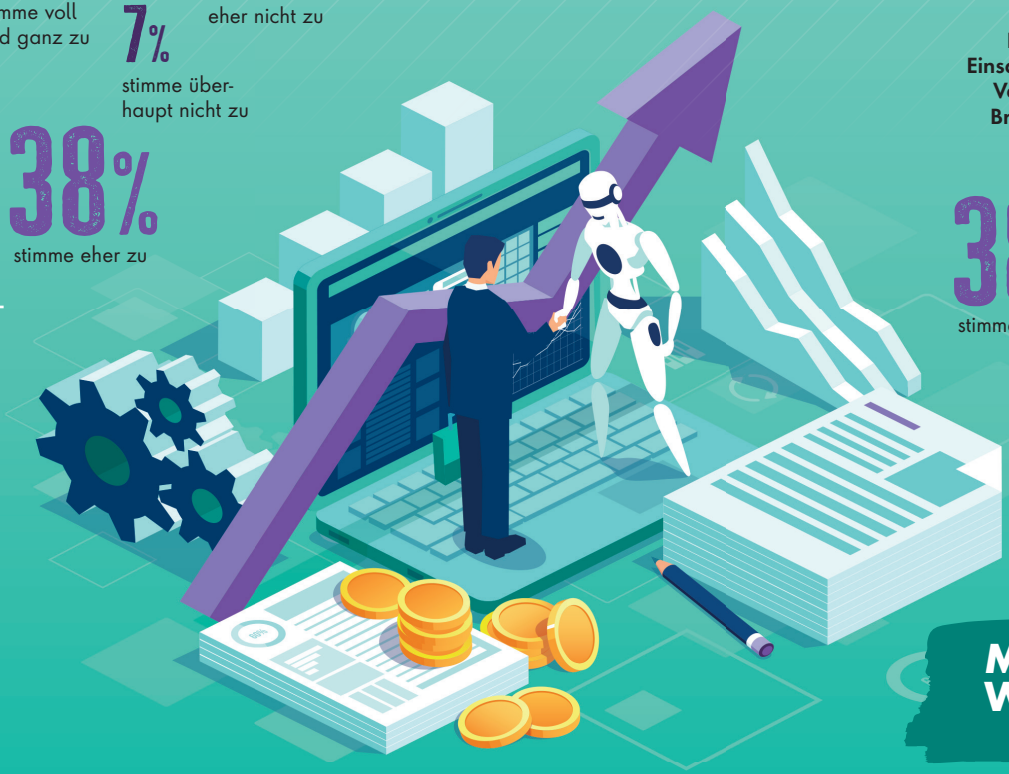
Kreditinstitute verfügen immer noch über umfangreiche, veraltete Informationstechnologie, die für den Einsatz generativer KI ungeeignet ist.

22% stimme voll und ganz zu

16% stimme eher nicht zu

7% stimme überhaupt nicht zu

38% stimme eher zu



Generative KI birgt viele Risiken, daher wird sich der Einsatz in der Finanzbranche im Vergleich zu nicht-regulierten Branchen deutlich verzögern.

38% stimme eher zu

21% stimme voll und ganz zu

16% stimme eher nicht zu

MEHR WERT
Banking Trends 2024

Passgenaue ERP-Abdeckung

DER STANDARD MUSS STANDARD WERDEN

Die passgenaue ERP-Abdeckung der eigenen Abläufe ist für Unternehmen oft ein zentraler Erfolgsfaktor. Doch nicht wenige scheuen die individuelle Anpassung des Standards wie der Teufel das Weihwasser. Sie fürchten höhere Implementierungskosten, erschwerte Wartungen oder eine stärkere Abhängigkeit vom Hersteller. Um Kunden aus dem Dilemma zu helfen, stehen die ERP-Anbieter in der Pflicht: Für sie gilt es, Alternativen zur Anpassung zur Verfügung zu stellen – damit passgenaue Individualität auch im Standard gelingen kann.

Ein besonderer Kniff im Fertigungsprozess, spezielle Individualisierungsmöglichkeiten für Kunden, eine außergewöhnlich effiziente Auftragsabwicklung – es sind die spezifischen Besonderheiten eines Unternehmens, die dieses am Markt einzigartig machen und gegenüber Mitbewerbern auszeichnen. Eine Individualität, die auch die genutzte ERP-Lösung widerspiegeln muss, um ineffiziente Medienbrüche, manuelle Nacharbeiten oder Workarounds zu vermeiden.

In vielen Unternehmen ergeben sich so oft zahlreiche individuelle Anpassungen der ERP-Lösung, sowohl auf Funktionsebene als auch bezüglich der Oberflächen. Für die ERP-User ein Segen, sind sie damit doch in der Lage, ihre täglichen Aufgaben mit bestmöglicher Effizienz zu bearbeiten. Für die IT-Teams hingegen bringen die Anpassungen auch ihre Schattenseiten mit sich: Je mehr Modifikationen am Standard bestehen, desto aufwendiger gestalten sich etwa Wartungs- und Upgrade-Prozesse.

Individualität im Standard

Um die Erforderlichkeit von individuellen Anpassungen am Standard zu reduzieren, gilt es für ERP-Anbieter, die Flexibilität ihrer Lösungen von Grund auf zu erhöhen. Dazu können sie ihre Systeme beispielsweise um umfassende Konfigurationsmöglichkeiten erweitern, die Kunden eine Individualisierung der Lösung ohne Eingriff in deren Programmierung ermöglichen.

Dazu ließe sich zum Beispiel eine dedizierte Prozesssicht bereitstellen, welche die zentralen Abläufe des Unternehmens widerspiegelt und die bei Bedarf auf Konfigurationsbasis verändert werden kann. Erweitert sich etwa das Geschäftsmodell eines Unternehmens durch eine zusätzliche Produktsparte, die neue Freigabe- oder Fertigungsabläufe erfordert, kann dies einfach und schnell in der Prozesssicht angepasst werden, ohne dass ein Eingriff in den Standard der ERP-Software erforderlich wäre. So spiegelt das IT-System zu jedem Zeitpunkt die jeweils aktuellen, individuellen Prozesse des Unternehmens wider – deutlich schneller als durch eine zeitaufwendige Anpassung im Programmcode.

Ein weiterer Vorteil ergibt sich für die einzelnen User: Kundenspezifische Anpassungen am ERP-Standard lassen sich in vielen Fällen wirtschaftlich sinnvoll nur für das Unternehmen als Ganzes realisieren. Gerade Kleinigkeiten, etwa welche Spalten in einer Listenansicht benötigt werden, unterscheiden sich oft stark von Anwender zu Anwender. Konfigurationen in der Oberfläche lassen sich auch auf Ebene einzelner Nutzer realisieren, sodass jeder und jede die Informationen und Elemente erhält, durch die er oder sie mit bestmöglicher Effizienz im System arbeiten kann.

Die Zukunft gehört dem Standard

Angesichts der derzeitigen Herausforderungen der wirtschaftlichen Weltlage ist es für Unternehmen entscheidender denn je, ihre individuellen Stärken mit maximaler Effizienz am Markt auszuspielen – ohne den unerwünschten Bremsklotz übermäßiger Anpassungen. Der spezifische Zuschnitt der ERP-Lösung rein auf Konfigurationsbasis lässt den Standard unverändert und deckt dabei doch das ab, was das Unternehmen einzigartig macht – ein sinnvoller neuer Standard für die ERP-Welt.

Ralf Bachthaler

ES SIND DIE SPEZIFISCHEN BESONDERHEITEN EINES UNTERNEHMENS, DIE ES AM MARKT EINZIGARTIG MACHEN UND SICH AUCH IN DER ERP-LÖSUNG WIDERSPIEGELN MÜSSEN.

Ralf Bachthaler,
Vorstand, Asseco Solutions AG,
www.applus-erp.com

Deutschlands digitale Revolution

DIE E-RECHNUNGSPFLICHT TRITT 2025 IN KRAFT

Deutschland durchläuft aktuell einen bedeutenden Wandel hin zum obligatorischen elektronischen Rechnungsaustausch zwischen Unternehmen. Mit der Zustimmung zum Wachstumschancengesetz im März 2024 ist auch die schrittweise Einführung der E-Rechnungspflicht beschlossene Sache.

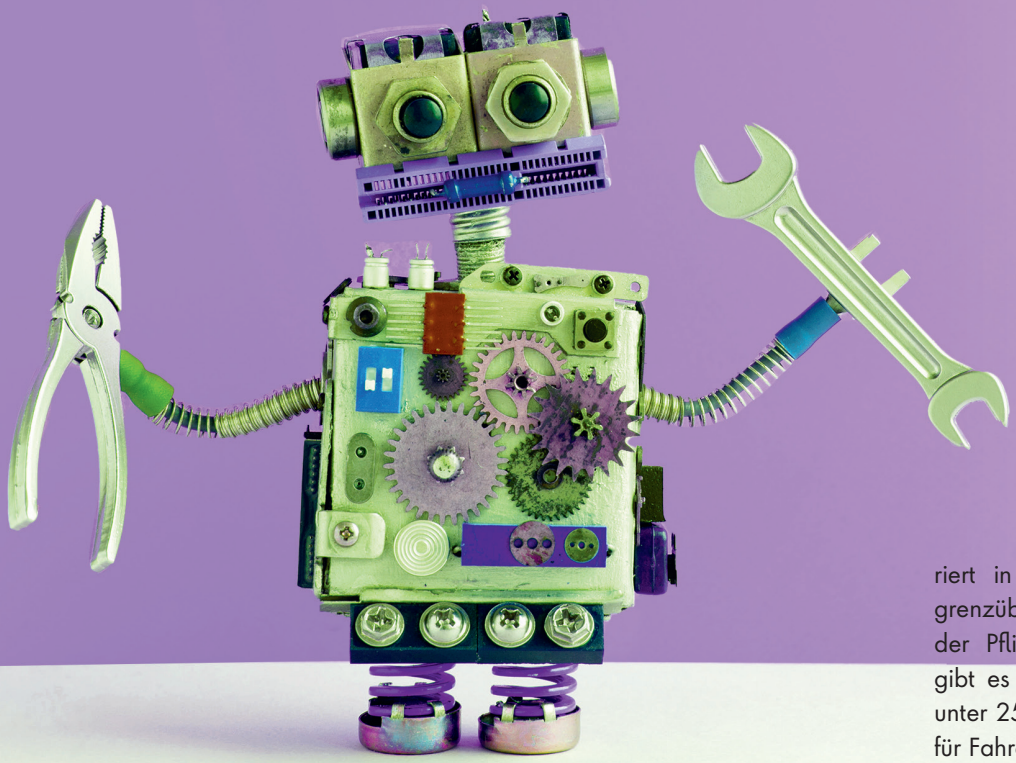
Die Verpflichtung sieht vor, dass deutsche Unternehmen ab dem 1. Januar 2025 in der Lage sein müssen, elektronische Rechnungen in den Formaten der CEN-Norm EN 16931 zu empfangen. Die Möglichkeit für den Rechnungsempfänger, elektronische Rechnungen abzulehnen, entfällt, da der Vorrang von Papierrechnungen nicht mehr gilt.

Ab dem 1. Januar 2027 soll der Versand elektronischer Rechnungen in Deutschland für Unternehmen mit einem Jahresumsatz von mehr als 800.000 Euro endgültig zur Pflicht werden. Ab dem 1. Januar 2028 wird die B2B-Pflicht für das Senden und Empfangen von E-Rechnungen auch auf alle anderen Unternehmen ausgedehnt.

Welche Übergangsfristen und Ausnahmen gelten?

Die Ära der Papierrechnungen neigt sich in Deutschland dem Ende zu. Für bestehende EDI-Rechnungen (Electronic Data Interchange) gilt eine Übergangsfrist von etwa drei Jahren.

- bis 31. Dezember 2026: Papierrechnungen sowie E-Rechnungen in nicht-konformen Formaten dürfen noch ausgetauscht werden, wobei die Priorität der Papierrechnung entfällt.
- bis 31. Dezember 2027: Der Austausch von Papierrechnungen sowie E-Rechnungen in nicht-konformen Formaten ist nur noch für Unternehmen mit weniger als 800.000 Euro Umsatz im Jahr möglich, wobei auch hier die Priorität der Papierrechnung entfällt.
- bis 31. Dezember 2027: Übergangsfrist für bestehende EDI-Verbindungen



Wichtig ist, dass in der Übergangsfrist weiterhin die Zustimmung des Rechnungsempfängers für den Austausch von E-Rechnungen in nicht-konformen Formaten erforderlich ist.

Die E-Rechnungspflicht gilt für B2B-Transaktionen sowie Rechnungen, deren Sender und Empfänger beide umsatzsteuerregistriert in Deutschland sind. Somit sind grenzüberschreitende Rechnungen von der Pflicht ausgenommen. Ausnahmen gibt es darüber hinaus für Rechnungen unter 250 Euro gemäß § 33 UStDV und für Fahrausweise gemäß § 34 UStDV.

Rechnungen an Verbraucher (B2C) sind von der Verpflichtung ausgeschlossen. Darüber hinaus sind auch Rechnungen an öffentliche Auftraggeber (B2G) nicht von dieser Pflicht betroffen, da es für B2G unabhängige Regelungen zur elektronischen Rechnungsstellung gibt.

Wie ist die Empfangspflicht umzusetzen?

Unternehmen müssen bis Januar 2025 sicherstellen, dass sie in der Lage sind, Rechnungen in den rechtskonformen Formaten zu empfangen und auch zu prüfen, ob eingehende Rechnungen diesen Vorgaben entsprechen. Das erforderliche strukturierte Format muss dabei sowohl der CEN-Norm als auch der Liste der entsprechenden Syntaxen gemäß der Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen (ABl. L 133 vom 6.5.2014, S. 1) entsprechen. Aktuell sind dies in Deutschland die Formate ZUGFeRD und XRechnung. Es gibt allerdings unterschiedliche Versionen dieser Formate, von denen nicht alle der CEN-Norm entsprechen. Es ist daher im Zweifelsfall darauf zu achten, immer die aktuellste Version zu nutzen. Die in der Wirtschaft häufig genutzten EDIFACT Formate sind grundsätzlich nicht konform mit der CEN-Norm EN 16931. Eine Ausnahme ist das Format UN/EDIFACT INVOIC D16B; die Syntax befindet sich jedoch nicht auf der Liste der entsprechenden Syntaxen.

Das Format kann auch zwischen Rechnungsaussteller und Rechnungsempfänger vereinbart werden. Voraussetzung ist, dass die richtige und vollständige Extraktion der nach gesetzlich erforderlichen Angaben aus der elektronischen Rechnung in ein EN 16391 konformes Format ermöglicht wird (Interoperabilität).

Zusätzlich dazu müssen Unternehmen festlegen, auf welchem Weg sie E-Rechnungen empfangen. Eine Unterscheidung nach Größe und Art des Rechnungsausstellers ist sinnvoll:

- Eine technische EDI-Schnittstelle zwischen dem IT-System des Rechnungsausstellers und dem IT-System des Rechnungsempfängers (klassisches EDI) ist vor allem bei großen Unternehmen schon vor der geplanten E-Rechnungspflicht üblich und besonders für Geschäftspartner geeignet, mit den viele Rechnungen ausgetauscht werden.

- Webportale (WebEDI) bieten KMU-Lieferanten die Möglichkeit, ein Rechnungsformular über ein webbasiertes Portal auszufüllen, woraus automatisch ein rechtskonformes Rechnungsformat erstellt und an den Empfänger geschickt werden kann.

- E-Mail als klassischer Übertragungsweg bietet sich für Geschäftspartner an, mit denen im Vergleich sehr wenige Rechnungen ausgetauscht werden.

Sobald Unternehmen eine E-Rechnung erhalten, muss diese in die IT-Systeme des Unternehmens übertragen werden, um die weitere Verarbeitung zu gewährleisten. Es ist daher notwendig, sicherzustellen, dass die IT-Systeme die erforderlichen Formate unterstützen. Sollte dies nicht der Fall sein, gibt es zwei Möglichkeiten:

- Die Beauftragung eines internen oder externen Entwicklers oder direkt des Herstellers, der die Verarbeitung der erforderlichen Formate in dem IT-System ermöglicht.

- Die Beauftragung eines EDI- / E-Invoicing-Dienstleisters, um die empfangene Rechnung in Format zu konvertieren, das von dem IT-System des Unternehmens verarbeitet werden kann. Hierfür bieten sich sowohl On-Premises-Converter als auch Software-Service-Dienstleister als Brücke zwischen den Empfangskanälen und den IT-Systemen des Unternehmens an.

Kleinere Unternehmen befürchten oft, dass sie diese strukturierten, maschinenlesbaren Formate nicht persönlich lesen können. Tatsächlich können E-Rechnungen jedoch mit einem entsprechenden Programm menschenlesbar gemacht werden. Dies ist sogar mit gängigen Internetbrowsern und dem Editor-Programm auf Windows möglich.

Was ist zu beachten?

Um die Pflicht zum Versenden elektronischer Rechnungen zu erfüllen, muss sichergestellt werden, dass das IT-System in der Lage ist, Rechnungen in den geforderten Formaten zu erstellen. Auch hier besteht wieder die Möglichkeit die Erstellung der gewünschten Formate direkt im genutzten IT-System zu forcieren oder mithilfe eines Dienstleisters die Umwandlung der Rechnungen in die notwendigen Formate sicherzustellen.

Nachdem die Rechnung im korrekten Format vorliegt, muss sie an den Empfänger übertragen werden. Auch der Rechnungsversand kann wiederum entsprechend der Gegebenheiten über eine technische Schnittstelle (klassisches EDI), ein Webportal (WebEDI) oder per E-Mail erfolgen. In jedem Fall ist sicherzustellen, dass das IT-System, mit welchem die E-Rechnung erstellt wird, in der Lage ist, diese über eine Schnittstelle direkt an die verwendetet Lösung für den Rechnungsausgang zu übermitteln. Diese Möglichkeiten können entweder von dem Unternehmen selbst oder mithilfe eines EDI-Dienstleisters geschaffen werden.

Bei Geschäftsbeziehungen im deren Rahmen viele Rechnungen ausgetauscht werden, wird typischerweise ein Format vereinbart, um den Aufwand der Verarbeitung verschiedener Formate zu reduzieren.

Paula Müller, Rafał Trojanowski
www.comarch.de/e-invoicing

Quellennachweis:

1] BGBl. 2024 I Nr. 108 vom 27.03.2024, Artikel 23: https://www.recht.bund.de/bgbl/1/2024/108/VO.html
2] https://www.comarch.de/produkte/datenaustauch-und-dokumentenmanagement/e-invoicing/e-invoicing-in-deutschland/xrechnung-zugferd/
3] https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Required+syntaxes

IT Service Management Tools

EINSATZ VON GENERATIVER KI

In der heutigen digitalen Landschaft ist das effiziente Management von IT-Services von entscheidender Bedeutung für den reibungslosen Betrieb von Unternehmen. Der Einsatz von Künstlicher Intelligenz (KI) hat sich als eine der vielversprechendsten Methoden erwiesen, um diese Effizienz zu steigern. Insbesondere die Integration von generativer KI in ITSM-Tools eröffnet eine Vielzahl von Möglichkeiten zur Optimierung von Prozessen und Verbesserung der Kundenerfahrung. In diesem Beitrag werden fünf verschiedene Use Cases für den Einsatz von generativer KI in ITSM-Tools sowie deren Vorteile diskutiert.

USE CASE 1: Lösungsvorschläge zu generischen IT-Problemen

Generative KI kann verwendet werden, um automatisch Lösungsvorschläge für generische IT-Probleme zu generieren. Dies ermöglicht eine schnellere Problembehebung und reduziert Ausfallzeiten, da Benutzer nicht auf manuelle Unterstützung warten müssen.

Vorteile:

- Schnellere Problemlösung und Reduzierung von Ausfallzeiten.
- Entlastung des Support-Teams durch automatisierte Bereitstellung von Lösungsvorschlägen.
- Verbesserte Benutzererfahrung durch sofortige Unterstützung bei IT-Problemen.

USE CASE 2: Präzisere E-Mail an Melder formulieren

Eine weitere Anwendung von generativer KI in ITSM-Tools besteht darin, E-Mails in zielgruppengerechter Sprache zu formulieren. Zum Beispiel kann anhand von Stichpunkten eine Rückfragemail an den Melder ausformuliert werden.

Vorteile:

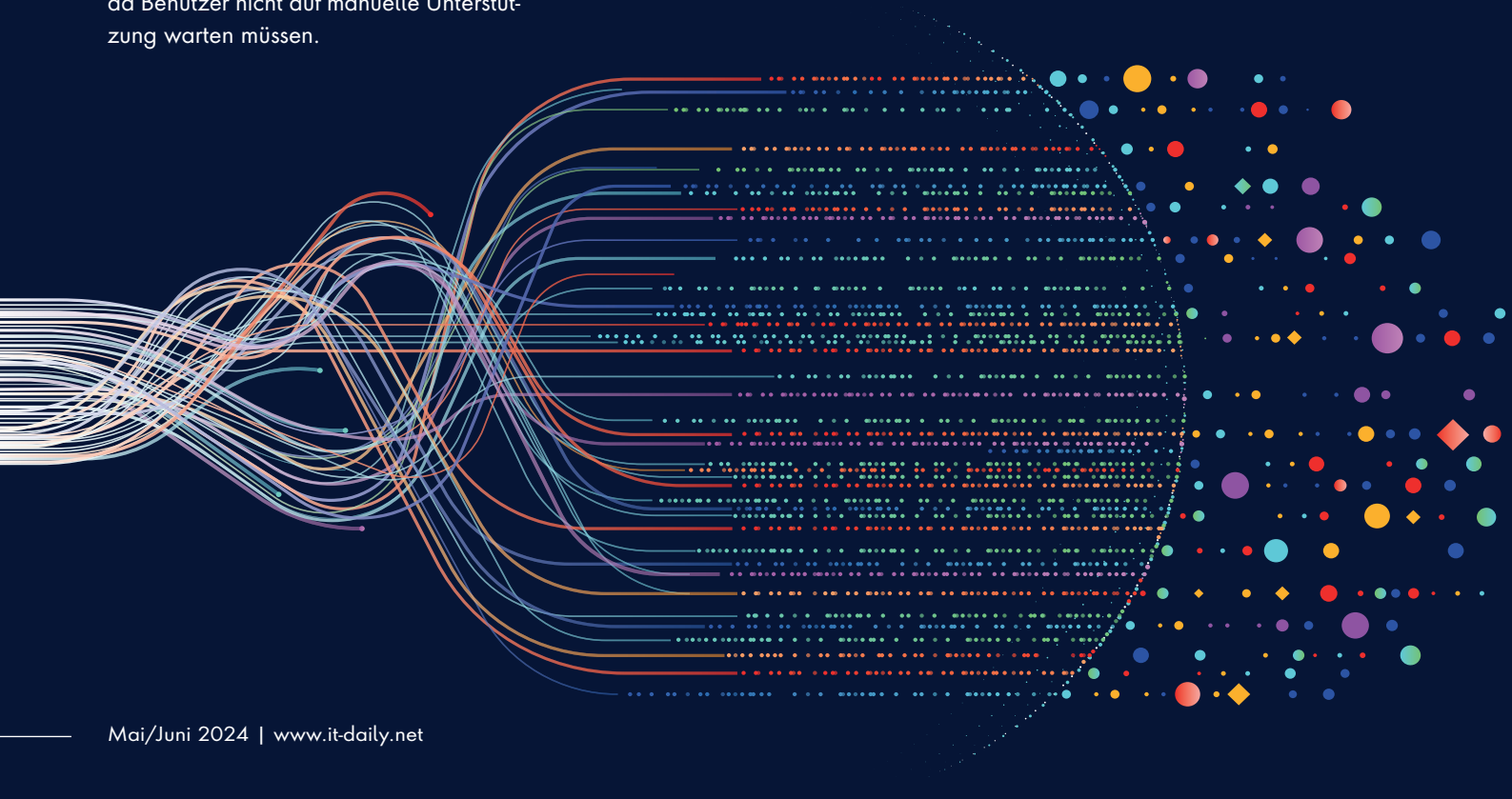
- Präzisere und zielgruppengerechtere Kommunikation
- Reduzierung der Arbeitsbelastung für das Support-Team.
- Verbesserte Benutzerzufriedenheit durch schnelle und präzise Antworten.

USE CASE 3: Incidents automatisch klassifizieren

Die Klassifizierung von Incidents ist ein wesentlicher Schritt im ITSM-Prozess, der die Priorisierung und Zuweisung von Ressourcen beeinflusst. Generative KI kann dabei helfen, Incidents automatisch zu klassifizieren, indem sie auf Basis der Anfrage die Kurzbeschreibung, Kategorisierung, Incidentart, Auswirkung, Dringlichkeit und Bearbeitergruppe ableitet. Dadurch können Incidents schneller und genauer bearbeitet werden.

Vorteile:

- Effizientere Zuweisung von Ressourcen durch automatisierte Incident-Klassifizierung.



- Verbesserte Reaktionszeiten auf Incidents durch schnellere Identifizierung der relevanten Kategorie.
- Optimierung der Ressourcennutzung im Support-Team.

USE CASE 4: Incidents automatisch zusammenfassen

Generative KI kann auch eingesetzt werden, um Incidents automatisch zusammenzufassen. Das System analysiert die Kommunikation zwischen Benutzern und Support-Team und extrahiert relevante Informationen, um eine prägnante Zusammenfassung des Incidents zu erstellen. Dies ermöglicht eine effizientere Eskalation und Weiterleitung von Incidents innerhalb des Support-Teams. Oder auch eine prägnante Zusammenfassung der Lösungsschritte in der Schließmail an den Melder.

Vorteile:

- Schnellere Eskalation und Weiterleitung von Incidents durch prägnante Zusammenfassungen.
- Verbesserte Effizienz im Support-Team durch automatisierte Informationsextraktion.
- Reduzierung von Missverständnissen durch klare und präzise Incident-Zusammenfassungen.

USE CASE 5: Incidents mit eigenen Daten/Wissensdatenbank lösen

Schließlich kann generative KI verwendet werden, um Incidents mithilfe interner Datenbanken oder externen Wissensquellen zu lösen. Das Training eines eigenen Modells kostet Millionen. Ein kosteneffizienter Lösungsansatz ist hier „Retrieval Augmented Generation". Dabei kombiniert man generative KI mit einer Vektorsuche, einer Machine Learning Technik, die aus der Anfrage die Absicht erkennt (semantische Suche). Hier gibt es Standardtools, deren Integration deutlich einfacher ist als das Training oder Feintuning eines eigenen Modells. Das System kann auf vorhandene Informationen zugreifen und basierend darauf Lösungsvorschläge generieren, um Incidents effektiv zu beheben. Dadurch werden Ausfallzeiten minimiert und die Produktivität der Benutzer maximiert.

Vorteile:

- Effiziente Incident-Behebung durch Zugriff auf umfangreiche Wissensdatenbanken.
- Minimierung von Ausfallzeiten durch schnelle Bereitstellung relevanter Lösungsvorschläge.
- teigerung der Benutzerproduktivität durch schnelle Problembehebung.

DIE INTEGRATION VON GENERATIVER KI IN ITSM-TOOLS ERÖFFNET EINE VIELZAHL VON MÖGLICHKEITEN ZUR OPTIMIERUNG VON PROZESSEN UND VERBESSERUNG DER KUNDENERFAHRUNG.

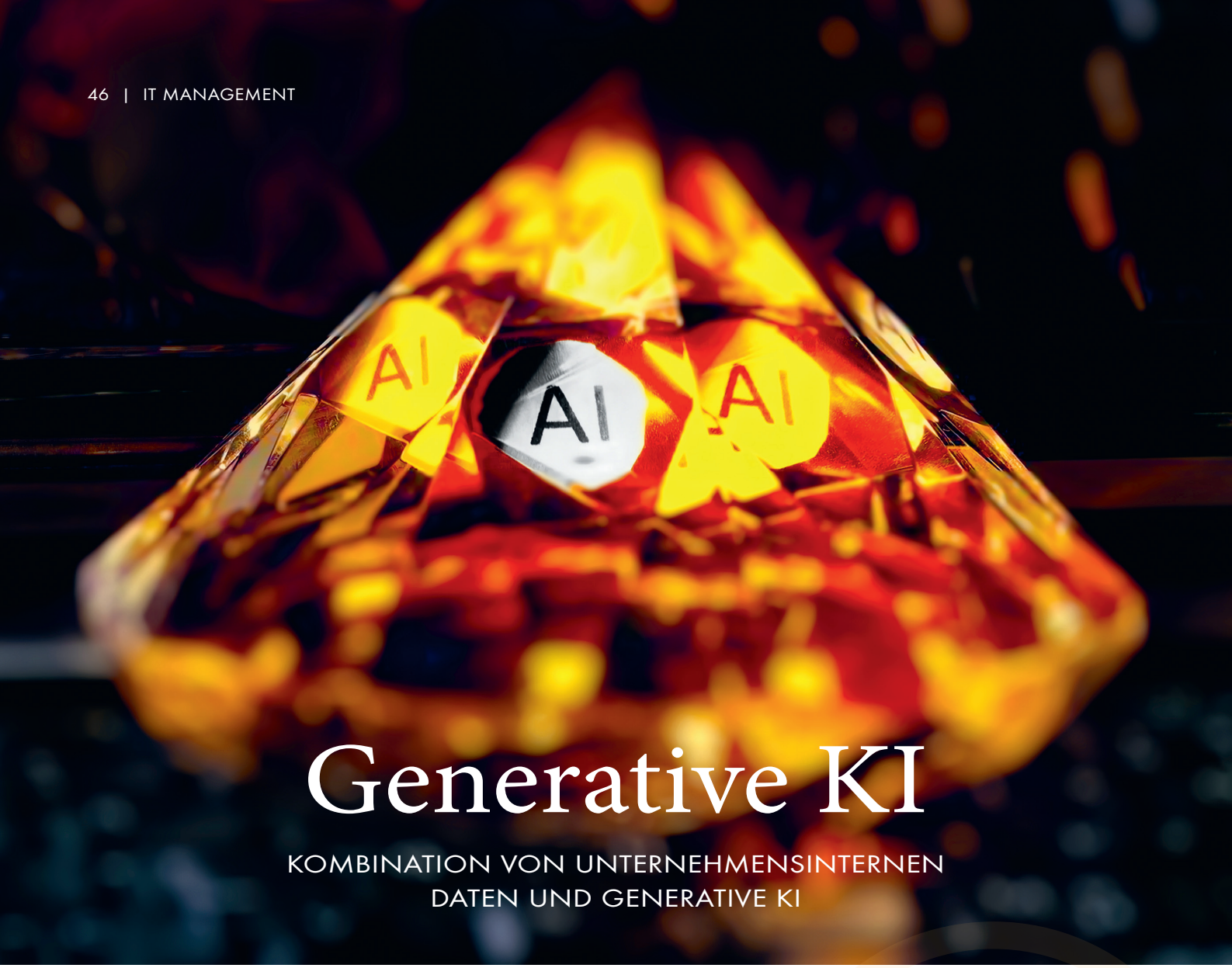
Benjamin da Silva Moreira, Consultancy, TOPdesk Deutschland GmbH, www.topdesk.de

Insgesamt bietet der Einsatz von generativer KI in ITSM-Tools eine Vielzahl von Vorteilen, darunter eine verbesserte Effizienz, schnellere Problembehebung und eine insgesamt bessere Benutzererfahrung. Durch die Automatisierung von Prozessen und die Nutzung von maschinellem Lernen können Unternehmen ihre IT-Services optimieren und ihre Wettbewerbsfähigkeit steigern.

Tool für IT Service Management und KI-Lösungen

TOPdesk ist eine führende Lösung für IT Service Management, um Unternehmen bei der effizienten Verwaltung ihrer IT-Services zu unterstützen. Hier gilt: Die Implementierung großer Changes ist von gestern! TOPdesk wurde entwickelt, IT-Serviceteams dabei zu helfen, kleine, realisierbare Ideen auszuprobieren – Schritt für Schritt. Automatisieren Sie das Zurücksetzen von Passwörtern. Teilen Sie FAQs. Implementieren Sie Self Service. Wissen Sie, was funktioniert und was nicht. Das Ergebnis? Ein sorgloses Serviceteam, das abliefert. Durch die Integration von KI kann die Lösung seine Leistungsfähigkeit weiter steigern und zusätzliche Mehrwerte für Melder schaffen.

Benjamin da Silva Moreira



Generative KI

KOMBINATION VON UNTERNEHMENSINTERNEN DATEN UND GENERATIVE KI

Viele Unternehmen erkennen das Potenzial, das generative KI in Kombination mit unternehmensinternem Know-How ihnen bietet. Doch für viele Mitarbeiter sind die Best Practices und Funktionsweisen noch vollkommen unklar. Dieser Artikel hilft interessierten Unternehmen, die Technik und Prozesse besser zu verstehen.

Stellen Sie sich vor, Sie verfügen über einen Chatbot mit umfangreichem Fachwissen. Dies eröffnet verschiedene Anwendungsfälle, darunter etwa die richtige Anwendung von Normen in der Produktentwicklung. Wenige Abteilungen sind so wissensintensiv wie die Produktentwicklung, weshalb ein schneller Zugriff auf ein internes Know-how entscheidend ist. Ein konkreter Anwendungsfall wäre, dass Mitarbeiter einen spezifischen Wert für eine Kalkulation benötigen, beispielsweise im Zusammenhang mit technischen Regeln für die Trinkwasserinstallation.

Richtige Anwendung von Normen in der Produktentwicklung

In diesem Fall verwendet die KI ausschließlich Informationen aus der Norm, um eine Antwort auf die Frage des Mitarbeiters zu generieren. Um sicherzustellen, dass dieser der Aussage der KI nicht blind vertraut, werden zum Beispiel zusätzlich Verweise auf eine bestehende DIN-Norm eingefügt, so dass Mitarbeiter direkt nachvollziehen können, von welcher Seite der Wert genommen wurde.

Finden von dezentralen Informationen

Für viele Anwendungsfälle liegen die Informationen verteilt in diversen Systemen. Man benötigt also Informationen aus Laufwerken, SharePoint und eventuell einem Tickettool wie Jira. Kombiniert man eine intelligente Enterprise Search mit einer generativen KI, dann kann man die intelligente Suche mit generativer KI kombinieren, so dass die generative KI die Informationen zusammenfasst.

E-Mailverläufe zusammenfassen

Oft genug werden Mitarbeiter irgendwann Teil eines längeren E-Mailverlaufs. Für sie ergibt sich die Möglichkeit, alle E-Mails durchzulesen oder mit Hilfe einer generativen KI sich den Verlauf zusammen zu fassen oder nochmal nachzufragen. Somit haben Mitarbeiter einen deutlich vereinfachten Zugriff auf unternehmensinternes Know-How.

Anfragen reduzieren

Einer der ersten Anwendungsfälle, der in Kombination mit generativer KI genannt wird, ist zumeist der Anwendungsfall des Supports. Support kann einerseits extern, andererseits intern anfallen.

Häufig wird die IT mit technischen Anfragen geblockt, zu denen es eigentlich bereits Antworten in Richtlinien oder Supportdokumenten gibt. Über einen klassischen Chat können Mitarbeiter mit Hilfe von generativer KI die Fragen einfach an die KI stellen. Auf die Frage „Wie kann ich eine Signatur selbst einreichten" wird beispielsweise eine ausführliche Schritt-für-Schrittanleitung generiert. Diese Antwort stammt jedoch nicht aus der „Intelligenz" des KI-Modells selbst, sondern aus einem Confluencedokument, welches nachvollziehbar referenziert wurde.

Suche von Ansprechpartnern und Generierung einer E-Mail

Generative KI kann genutzt werden, um sich E-Mails mit den Feinheiten beziehungsweise der Sprache des eigenen Unternehmens formulieren zu lassen.

Konzept der Abfrage von einem KI-Modell, welches mit eigenen Daten trainiert wurde.

Natürlich kann jedes Onlinetool eine E-Mail vorformulieren. Oftmals fehlen aber konkrete Insights, die eine solche E-Mail wirklich brauchbar machen. Generative KI sucht zunächst nach den richtigen Kontaktdaten und schreibt basierend auf dem beschriebenen Problem anschließend eine E-Mail. Natürlich können Nutzer auch hier die KI bitten Formulierungen anzupassen oder die E-Mail beispielsweise per du zu schreiben.

Anwendungsfälle gibt es genug – aber wie setzt man diese um?

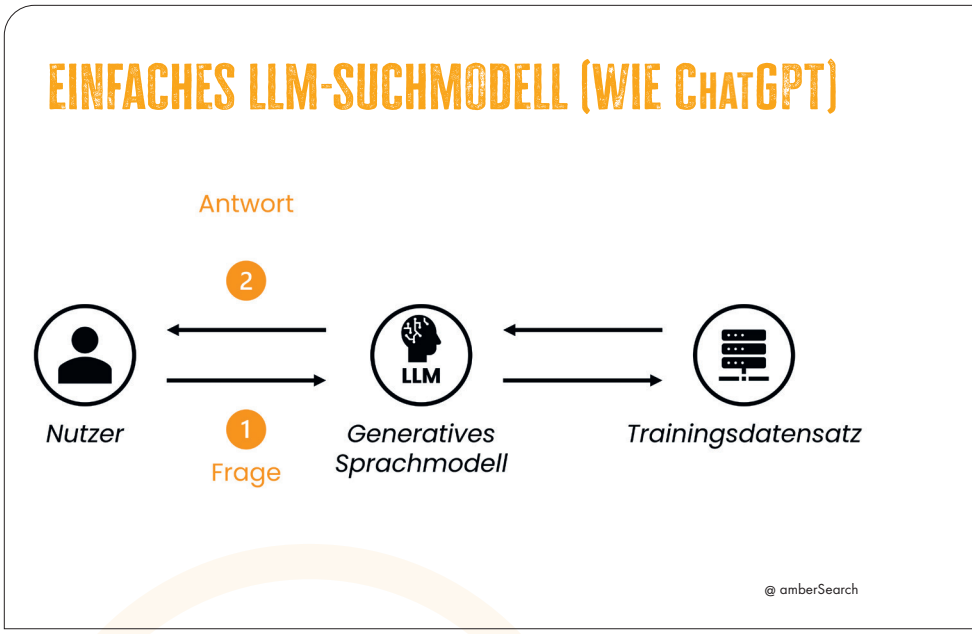
Um solche Anwendungsfälle umzusetzen, gibt es drei Möglichkeiten – aber nur eine ist für Unternehmen wirklich nachhaltig:

1. Man trainiert ein eigenes Sprachmodell (Large Language Modell)
2. Man baut ein Retrieval Augmented Generation System
3. Man kombiniert ein Retrieval Augmented Generation System mit einer intelligenten Suche

#1 Training eines eigenen Sprachmodells

Viele Unternehmen träumen zurzeit vom Sprachmodell mit eigenen Daten. Darum kommt relativ die schnell die Frage auf, warum wir nicht einfach eine KI mit unseren Daten trainieren?

Im Ergebnis hätten Unternehmen ein KI-Modell, welches das Know-How des Unternehmens hätte. Mit diesem Know-How hätten Mitarbeiter Möglichkeiten, sich ihre Fragen schneller und effizienter beantworten zu lassen.



Um ein KI-Modell mit eigenen Daten zu trainieren, bedarf es jedoch einer Menge technischen Know-How's sowie einer Menge Hardwareressourcen. In Summe spricht man schnell über hohe fünf- bis sechsstellige Beträge.

Des Weiteren hat dieser technische Ansatz einige Nachteile:

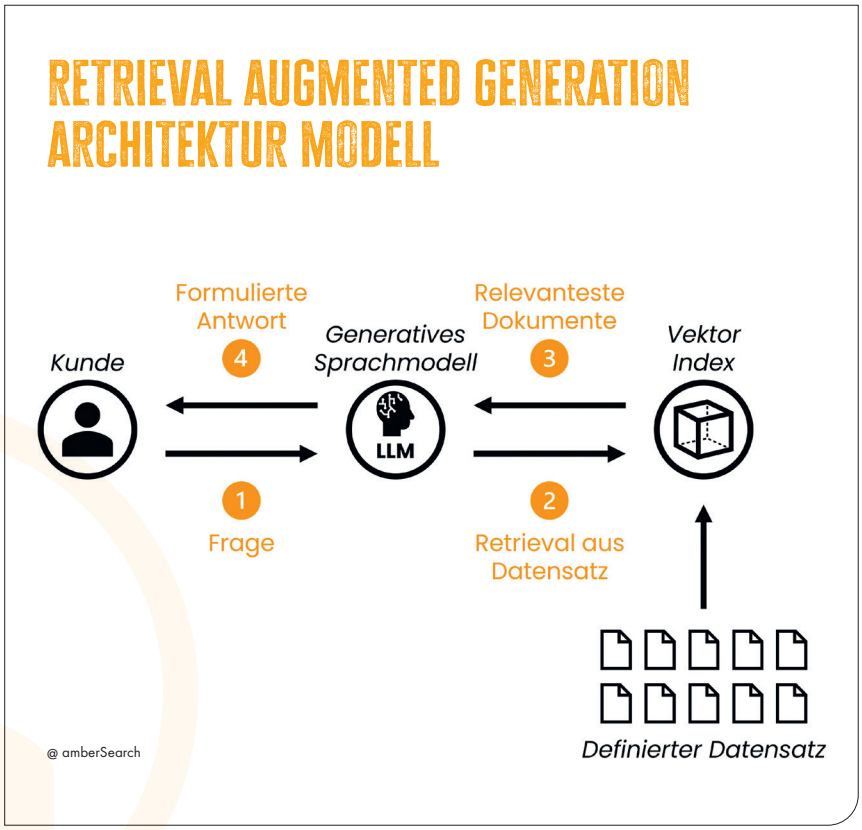
- Zunächst muss definiert werden, welcher Datensatz genutzt wird, um die generative KI zu trainieren.
- Da sich der Datensatz schnell verändert, wird das trainierte KI-Modell auch recht schnell outdated sein.
- Ein KI-Modell alleine kann keine Zugriffsrechte berücksichtigen, daher wird meist ein eher oberflächlicher Datensatz ausgewählt. Dieser enthält meistens zu wenige Informationen, um wirklich konkret genug zu sein, da die wirklich interessanten Informationen Zugriffsbeschränkungen unterliegen und somit nicht zum Training verwendet werden.
- KI-Modelle tendieren dazu, zu halluzinieren, das heißt die Antworten sind nicht zwangsläufig richtig. Kommen die Antworten aus dem KI-Modell selbst (so wäre es bei diesem technischen Ansatz der Fall), dann würde man nicht wissen, woher das KI-Modell die Antwort nimmt – ähnlich wie bei ChatGPT.

#2 Der Retrieval Augmented Generation Ansatz

Mit Hilfe eines Retrieval Augmented Generation Ansatzes könnte man diese Herausforderungen jedoch umgehen. Bei diesem Ansatz wird vor der Generierung

einer Antwort überprüft, welche Daten aus einem bestimmten Datensatz sich am besten eignen, um die Anforderung des Nutzers zu erfüllen. Nur die Dokumente, die als am relevantesten bewertet werden, werden in die Generierung einer Antwort mit einbezogen.

Um ein Retrieval Augmented Generation System aufzubauen, würde man zunächst einen Datensatz definieren. Dieser Datensatz würde anschließend von dem Softwaresystem indiziert beziehungsweise vektorisiert werden.



Beschreibung eines Retrieval Augmented Generations Modells ohne die Anbindung einer Enterprise Search

VIELE UNTERNEHMEN ERKENNEN DAS POTENZIAL, DAS GENERATIVE KI IN KOMBINATION MIT UNTERNEHMENSINTERNEM KNOW-HOW IHNEN BIETET. DOCH FÜR VIELE MITARBEITER SIND DIE BEST PRACTICES UND FUNKTIONSWEISEN NOCH VOLLKOMMEN UNKLAR.

Bastian Maiworm, CRO, amberSearch, https://ambersearch.de/de/

Stellt der Nutzer nun eine Frage, schaut die Software zunächst nach den relevantesten Dokumenten und nutzt diese in Kombination mit der Intelligenz eines KI-Modells, um eine Antwort zu generieren. In diesem Fall wird die Antwort also nicht durch das Know-How des KI-Modell selbst generiert, sondern durch den Kontext, der über den vorab definierten Datensatz gegeben wurde. Die Intelligenz des generativen KI-Modells wird nur genutzt, um die relevantesten Ergebnisse in einer Form aufzubereiten, so dass diese die Frage des Nutzers beantworten. Ein weiterer Vorteil ist, dass ein KI-Modell über diesen Ansatz in der Lage ist zu referenzieren, wo genau welche Information herkommt.

Aber auch dieser technische Ansatz hat einige Herausforderungen, die ungelöst sind:

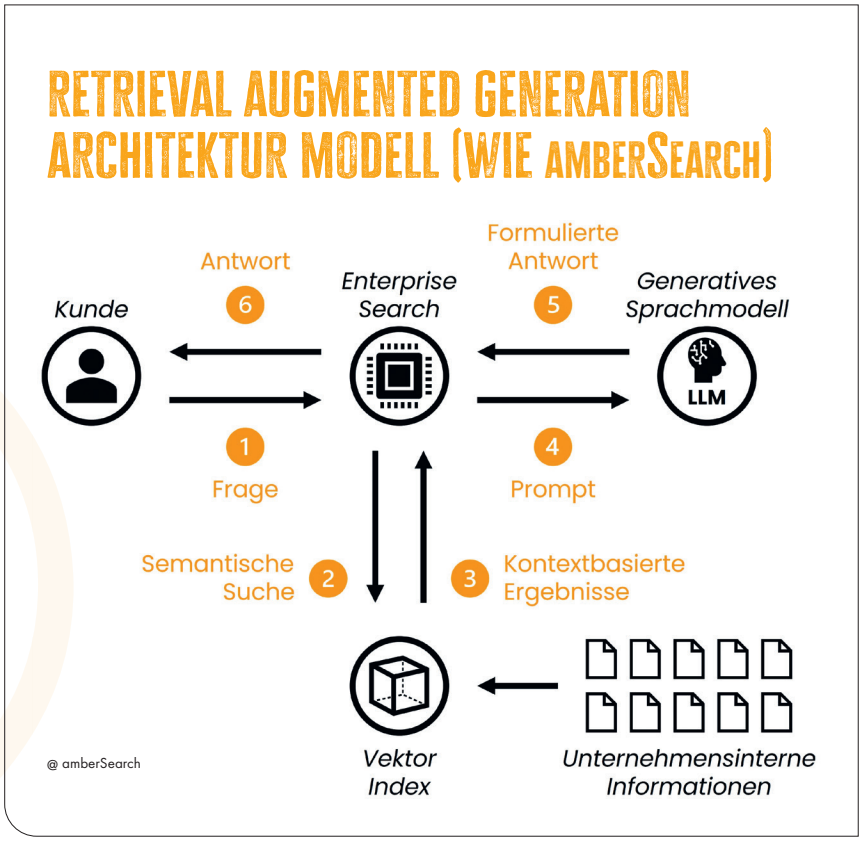
- Über diesen Ansatz kann man diverse Chatbots aufbauen oder definieren. Man würde einfach definieren, dass ein Support-Chatbot alle Informationen vom Support bekommt, ein Onboarding-Chatbot alle Informationen zum Onboarding und so weiter. Das Problem ist, dass man noch keinen „wirklich" übergreifenden Chatbot hat, sondern mehrere spezialisierte Chatbots. Man muss für jeden Anwendungsfall einen statischen Datensatz definieren.

- Auch hier werden keine Zugriffsrechte berücksichtigt.

Kombination eines Retrieval Augmented Generation Systems mit einer Enterprise Search

Um den Datensatz flexibler zu gestalten beziehungsweise um Zugriffsrechte zu berücksichtigen, sollte man auf die Kombination eines Retrieval Augmented Generation Systems mit einer Enterprise Search setzen. Die Enterprise Search, eine Art Google fürs Unternehmen, sucht zunächst alle relevanten Informationen für die Anfrage des Nutzers – unter Berück-

sichtigung der bestehenden Zugriffsrechte. Diese werden dann als Kontext an die generative KI übergeben, die in der Lage ist, diese so aufzubereiten, dass sie die Frage des Nutzers beantworten



Kombination einer Enterprise Search mit generativer KI, um auf einem flexiblen Datensatz die richtigen Antworten zu generieren

Im Gegensatz zum reinen Retrieval Augmented Generation System übernimmt die Enterprise Search die Aufgabe, den jeweils zum Prompt passenden Datensatz flexibel zu definieren. Damit kann man die Herausforderungen mehrerer Retrieval Augmented Generation Systeme und die der Zugriffsrechte lösen.

Eine der Herausforderungen ist es, dass sich die Enterprise Search nur auf ein Thema des Prompts fokussieren kann.

Um aber multidimensionale Prompts lösen zu können, wird ein Multi-Hop Question Answering System benötigt. Dieses ist in der Lage, vor Generierung einer Antwort mehrere Suchanfragen an das System abzusetzen und somit die verschiedenen Dimensionen eines Prompts zu beantworten.

Fazit – Selbst entwickeln oder zukaufen?

Tools wie ChatGPT und Co machen es sehr leicht, solche Systeme – gerade als kleiner Demonstrator - selbst zu bauen. Wer aber eine nachhaltige Lösung möchte, der sollte auf ein richtiges Produkt setzen. Die bereits angesprochenen Aspekte zeigen, dass die Umsetzung einer solchen Lösung durchaus komplex ist und einige Herausforderungen mit sich bringt. Zurzeit gibt es viele Agenturen und Beratungsunternehmen, die mit Unternehmen zusammen Demonstratoren bauen. Was Unternehmen jedoch bedenken sollten ist die Komplexität, die mit der Eigenentwicklung solcher Systeme einhergeht. Um aus einem Demonstrator unter Berücksichtigung der genannten Herausforderungen ein Produktivsystem zu machen, ist einiges an Aufwand nötig.

Bei amberSearch haben wir bereits 2020, also weit vor dem Hype um KI angefangen, ein Produkt zu bauen, welches die angesprochenen Anforderungen für Unternehmen löst.

Bastian Maiworm

Finanzbereich auf Kurs

BRAUCHEN UNTERNEHMEN AUTOMATION ODER KI IN DER FINANZORGANISATION?

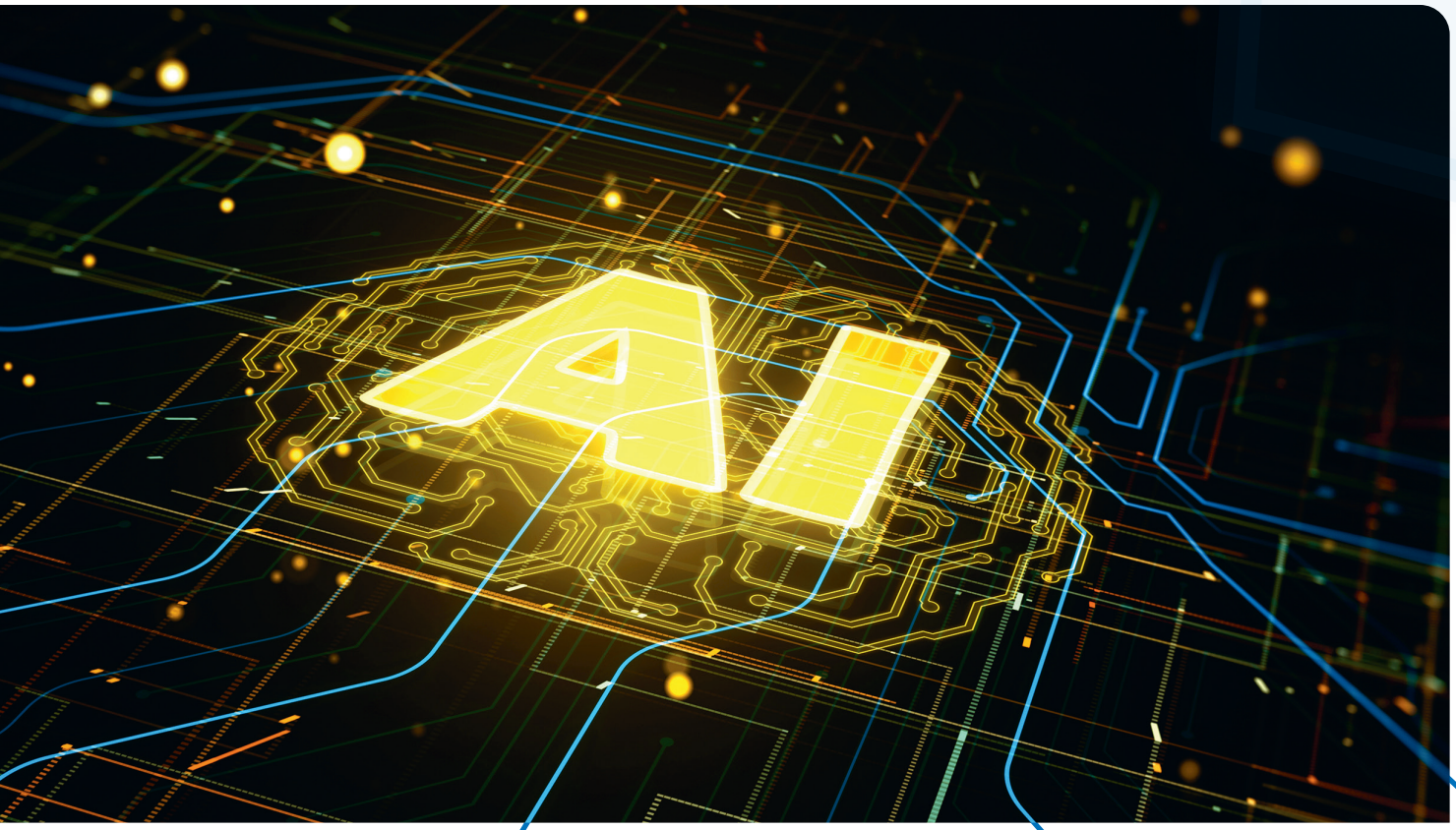
Was machen Unternehmen, wenn etwas Unvorhergesehenes passiert? Sie reagieren. Allerdings trennt sich genau an dieser Stelle die Spreu vom Weizen. Denn eine Reaktion kann entweder adhoc erfolgen oder das Unternehmen ist bereits im Voraus so gut vorbereitet, dass selbst aus überraschenden Ereignissen ein Vorteil gezogen werden kann. Diese positive Art der Reaktion kann nur dann funktionieren, wenn sich die Führungsspitze auf die Daten ihrer Finanzabteilung und des Controllings verlassen können. Noch besser ist es, wenn das F&A in der Lage ist, aufgrund von verlässlichen Prozessen, weitreichender Automation oder dem Einsatz von Künstlicher Intelligenz ein Accounting zu betreiben, das den Kapitänen als Kompass dient.

Spätestens seit dem querliegenden Frachter im Suezkanal, der COVID-19-Pandemie oder den kriegerischen Handlungen in Europa ist klar, dass es nicht so weitergehen kann. Unternehmen kommen ins Schlingern und kämpfen nicht nur mit den veränderten Umständen, etwa Handelsembargos oder der Verlagerung der Mitarbeiter ins Homeoffice. Sie haben vor allem Schwierigkeiten damit, auf Basis von belastbarem Zahlenmaterial gezielt aus der Situation herauszufinden und einen Kurs einzuschlagen, der dem Unternehmen eine Zukunftsperspektive bietet. Allerdings können einige Unternehmen schadlos oder gar gestärkt aus den Krisenszenarien hervorgehen. Ein Blick in Studienergebnisse lässt vermuten, was diese richtiger machen haben als andere.

Navigieren im Nebel

Zu den Fakten: 2020 sah sich, einer BlackLine-Studie zufolge, ein Drittel der Unternehmen (33 Prozent) aufgrund der COVID-19-Pandemie unter erhöhtem Druck, ein exaktes Abbild der Unternehmensleistung zu liefern. Gründe dafür waren mangelnde Agilität und eine hohe Fehlerquote durch noch mehr Druck in der Finanzorganisation. Zu viele Datenquellen, zu wenig Automatisierung im F&A und vor allem zu viel manuelle Prozesse taten ihr Übriges.

Heute, mit den Erfahrungen der letzten turbulenten Jahre, sind die Unternehmen alarmiert. In der jüngsten BlackLine-Studie, die Censuswide Ende 2023 in sieben Märkten (USA, Kanada, Großbritannien,



Frankreich, Deutschland, Australien und Singapur) durchgeführt hat, wurden die C-Level Führungskräfte und Finanzprofis erneut befragt. Rund 30 Prozent der Befragten sehen eine potenzielle Gefahr, dass erneut einschneidende Ereignisse eintreten werden. 34 Prozent rechnen beispielsweise mit dem Risiko einer globalen Finanzkrise, 36 Prozent mit einer großen Cyber-Crime-Krise, 25 Prozent mit einer Pandemie oder 33 Prozent mit weitreichenden geopolitischen Komplikationen. Man könnte annehmen, dass sie aus der Vergangenheit gelernt und ihre Prozesse im F&A neu aufgestellt haben, um in Zukunft besser für Unvorhersehbares gewappnet zu sein.

Kaum dazu gelernt

Doch trotz dieser Erkenntnisse und der verstrichenen Zeit, sind vergleichsweise wenig Unternehmen gut vorbereitet. Auf die Frage, ob sich die Unternehmen strategisch für diverse Krisenszenarien aufgestellt haben, fühlten sich im Falle einer Finanzkrise nur 22 Prozent gut gerüstet, für geopolitische Situationen nur 25 Prozent, für eine Pandemie 24 Prozent und für eine Cyber-Crime-Krise immerhin 35 Prozent.

Einer der Gründe ist in den Zahlen der Studien schnell ausgemacht: die nach wie vor ernüchternde Situation mit der Zuverlässigkeit von Finanzdaten. In der Studie im Jahr 2020 war weniger als ein Drittel (29 Prozent) der Befragten davon überzeugt, dass die Finanzdaten, die sie für Analysen und Prognosen heranziehen, akkurat sind. Die neue Studie von Ende 2023 zeigt, dass 37 Prozent international und 40 Prozent in Deutschland Befragten ihren eigenen Daten nicht vollständig vertrauen. Für die strategische Entscheidungsfindung in einer Zeit von teils desaströsen Ereignissen, ist dies keine gute Grundlage für das F&A und die Führungskräfte.

KI soll es richten?

Nun könnte man meinen, dass KI die Lösung aller Probleme ist. Immerhin wird diese spätestens seit dem öffentlichen Zugang zu ChatGPT in jeglicher Form heiß diskutiert – durchaus kontrovers, aber vielfach auch als Heilsbringer für alles und jeden. Gilt diese rosige Zukunft der KI auch für die Finanzorganisation und die Führung eines Unternehmens? Man ist indifferent: In Deutschland glauben 57 Prozent, dass generative KI und 55 Prozent, dass neue Arten von KI wichtig sind, um die Widerstandsfähigkeit zu erhöhen. Umso erstaunlicher ist, dass nach wie vor die Abhängigkeit von manuellen und veralteten Prozessen, einschließlich der manuellen Datenerfassung, die anfällig für menschliche Fehler ist (22 Prozent in Deutschland) an der Tagesordnung sind.

DURCH KI KÖNNEN UNTERNEHMEN IHRE TRANSAKTIONSFEHLER MASSGEBLICH REDUZIEREN, WAS WIEDERUM ZU ERHEBLICHEN ZEIT- UND KOSTENEINSPARUNGEN FÜHRT.

Ralph Weiss,
Geo VP DACH BlackLine,
www.blackline.com

Nach aktuellem Stand sind rund ein Drittel keine großen Förderer der KI im Finanzumfeld. Beispielsweise glauben in Deutschland 35 Prozent, dass KI nicht mit den Compliance-Regeln einher gehen wird und 32 Prozent bangen sogar um ihren Job durch den Einsatz von KI. Wenn es KI richten soll, sprechen die Studienergebnisse nicht dafür, dass es innerhalb kurzer Zeit passieren wird.

Dank Finanz-Automation und KI in ruhigen Fahrwassern

Die Ergebnisse der aktuellen Studie zeigen, dass noch viel Strecke zurückgelegt werden muss, bis die Finanzorganisation und das Management auf verlässliche Finanzdaten zurückgreifen können oder sogar zukunftsweisende Empfehlungen und Szenarien aus dem Finanzdepartment zu erwarten sind. Was könnten demnach die nächsten logischen Schritte sein? Möglichst umgehend sollte die Digitalisierung, konkret die Eliminierung von manuellen Prozessen im F&A vorangetrieben werden. Das hat mehrere Vorteile: Erstens senkt die Automation die Fehlerquote drastisch, so dass sich Finanzprofis und das Management auf die Finanzdaten verlassen können. Zweitens können Berichte wesentlich schneller und auch zwischen den Berichtsperioden angefertigt werden. Drittens haben die Finanzprofis die benötigten Ressourcen, um die Daten gewinnbringend zu analysieren und für Entscheidungen des Managements individuell an die Situation angepasst aufzubereiten.

Und was ist mit KI? Künstliche Intelligenz kann bereits heute entscheidend helfen. Ein Beispiel ist die Intercompany Predictive Guidance. Sie nutzt künstliche Intelligenz, um die Transaktionsdaten eines Unternehmens zu analysieren. Noch bevor die Transaktionen gebucht werden, sagt die KI voraus, wo mutmaßlich Probleme auftreten und Risiken für die Finanzabschlussprozesse und die Datengenauigkeit bestehen. Durch KI können Unternehmen ihre Transaktionsfehler maßgeblich reduzieren, was wiederum zu erheblichen Zeit- und Kosteneinsparungen führt.

Darüber hinaus ist es vorstellbar, dass die KI den Finanzprofis dabei hilft, große Datenpools aus den eigenen Quellen, vielleicht aber auch aus externen Quellen zusammenzuführen, um daraus Modelle zu generieren. Dieser Schritt ist für die meisten Unternehmen vermutlich noch weiter am Horizont als die Automatisierung. Doch selbst Christoph Columbus wusste nicht genau, was ihn hinter dem Horizont erwartet. Er hatte aber eine Vorstellung und schlug genau darauf seinen Kurs ein.

Ralph Weiss

5G und 6G: Smart vernetzt in die Stadt der Zukunft

WARUM INTERCONNECTION-PLATTFORMEN DAS KERNSTÜCK JEDER SMART CITY SIND

Von autonomen Autos über selbstfliegende Drohnen bis hin zu abrufbereiten Flugtaxis – die Smart City soll in Zukunft jederzeit individuelle Mobilität möglich machen. Schon heute sind dafür neue Konzepte gefragt. Konzepte, die in der Lage sein müssen, Verkehrsflüsse übergreifend, autonom, intelligent und in Echtzeit zu überwachen und zu steuern. Um eine solche Zukunft zu realisieren, sind nicht nur datenbasierte Lösungen notwendig, sondern Netzinfrastrukturen, die Daten besonders schnell und damit möglichst latenzfrei übertragen können. Gerade im Hinblick auf das autonome Fahren bestehen in der Smart City hohe Anforderungen an die Latenz. Um Menschen und Fahrzeuge sicher, schnell und zuverlässig durch die Mobilitätswelt von morgen zu bewegen, müssen smarte Leitsysteme kritische Situationen im Voraus erkennen und den autonomen Verkehr echtzeitlich entsprechend steuern können.

Egal, ob mit smarten Verkehrszentralen oder cleveren Anwendungen, um Städte sauberer, lebenswerter und nachhaltiger zu machen – Services wie diese machen zudem neue Geschäftsmodelle möglich. Laut einer Studie vom eco – Verband der Internetwirtschaft wächst das Umsatzvolumen des deutschen Smart-City-Marktes von 38,5 Milliarden Euro im Jahr 2021 auf 84,7 Milliarden Euro im Jahr 2026. Tendenz steigend, wenn die technologischen Voraussetzungen passen. Beispiel 5G: Zwar schreitet der Ausbau der Infrastruktur voran, aber er ist längst nicht abgeschlossen, wie eine Analyse der Bundesnetzagentur von Oktober 2023 zeigt. 90 Prozent des Bundesgebiets sind erst durch mindestens einen 5G-Netzbetreiber versorgt.

GERADE IM HINBLICK AUF DAS AUTONOME FAHREN BESTEHEN IN DER SMART CITY HOHE ANFORDERUNGEN AN DIE LATENZ.

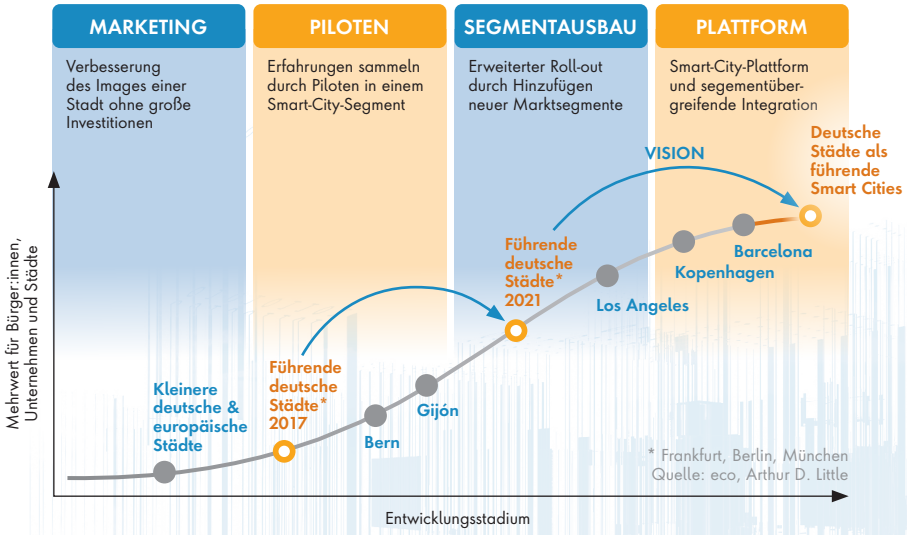
Dr. Christoph Dietzel, Global Head of Products and Research bei DE-CIX, www.de-cix.net

Smart City mit 5G: Daten teilen und verarbeiten

Das zu ändern, lohnt sich: Als vollständiger Technologiestack bietet 5G gegenüber Vorgängerversionen zahlreiche Vorteile. So lassen sich Software-integrierte Funktionen verknüpfen, Services virtualisieren oder Edge-Netzwerke betreiben. Daten lassen sich mit Geschwindigkeiten von bis zu 20 Gbit/s übertragen – und das zuverlässigerer als mit vorangehenden Mobilfunktechnologien. Dabei nutzt 5G nicht nur die verfügbare Bandbreite optimaler als vorangehende Standards aus, sondern erreicht eine Versorgungsdichte von bis zu einer Million Geräte pro Quadratkilometer. Das verbessert die mobile Internetversorgung in einem vollbesetzten Fußballstadion oder während einer Open-Air-Veranstaltung. Zudem ermöglicht es 5G, viele Geräte im Internet der Dinge zu orchestrieren, um Daten zu teilen und in smarten City-Services zu verarbeiten – von der intelligenten Mülltonne bis zur Realtime-Verkehrssteuerung.

Auch anderswo gewährleistet Mobilfunk reibungslose Abläufe. Beispielsweise können Städte Baustellen mit digitalen 3D-Modellen abbilden, um die Arbeiten besser zu planen, zu steuern und zu dokumen-

tieren. Kameras und Sensoren übertragen dabei Bilder und Daten an das Baureferat. Ähnlich funktioniert die Kontrolle der strukturellen Integrität von Brücken mit Hilfe von 5G, um Einstürze zu vermeiden oder im Notfall über Alarmsysteme schnell zu reagieren. Intelligente Energiezähler lassen sich aus der Ferne auslesen. Sensoren messen zudem den Wasserverbrauch oder die Luftverschmutzung. In öffentlichen Gebäuden werden Heizung und Klimaanlage über die gemessene Temperatur und Luftfeuchtigkeit gesteuert, die Belüftung über den Sauerstoffgehalt.



Smart-City-Entwicklungsstadien: Deutsche Städte im internationalen Vergleich

Digitale Zwillinge als 6G-Anwendung der Zukunft

Die Nachfolgeversion des Mobilfunkstandards, die auf den Vorteilen von 5G aufbaut, steht schon in den Startlöchern. 6G wird voraussichtlich Ende dieses Jahrzehnts verfügbar sein, noch leistungsfähiger und effizienter werden sowie zahlreiche neue Funktionen bieten. Laut einer Studie von Capgemini wird 6G noch schneller sein als 5G. Der Standard ermöglicht demnach Datentransfers mit bis zu 1 Tbit/s, Latenzzeiten von 10 bis 100 Mikrosekunden, eine Versorgungsdichte von zehn Millionen Geräten pro Quadratkilometer und eine fünffach effizientere Nutzung des Funkspektrums.

Digitale Zwillinge gelten als 6G-Anwendung der Zukunft. Reale und virtuelle Welt verschmelzen in Simulationen miteinander. Und das nicht nur, um die Verkehrsströme einer kompletten Stadt abbilden und smart steuern zu können, sondern alle Verfahren, Prozesse und Abläufe – von jeder einzelnen intelligenten Fußgängerampel über jede konnektierte Abfalltonne bis hin zur dezentralen Stromproduktion in verteilten Windkraftanlagen, Solarparks und Blockheizkraftwerken. Mobil vernetzt lassen sich Daten im Digital Twin verarbeiten, übergreifend verknüpfen und neue digitale Services realisieren. Zusätzlich integriert 6G unterschiedliche Systeme und Plattformen, von Antennen am Boden bis zu Satelliten im Weltraum, um eine nahtlose Mobilfunkversorgung bereitzustellen. Bis 6G verfügbar ist, soll 5G Advanced in diesem Jahr an den Start gehen. 5G Advanced bildet das Fundament für den künftigen 6G-Technologiestack und erweitert bestehende 5G-Funktionen, um beispielsweise KI-Anwendungen zu integrieren.

Rechenzentrum trifft Mobilfunk

Um Autos, Menschen und Geräte in der Smart City derart zu verbinden, braucht es zum einen eine passende Mobilfunkversorgung. Nur so lassen sich Informationen flächendeckend sammeln und auch smart verarbeiten. Und zum anderen braucht es eine passende Netzinfrastruktur. Nur so lassen sich große Datenmengen realzeitlich und domänenübergreifend austauschen. Für diese Vernetzung sowie zur Bearbeitung und Analyse der Daten für Prognosen, Anpassungen und Optimierungen sind – neben mobiler Konnektivität – immer mehr miteinander vernetzte Rechenzentren notwendig.

Viele Städte sammeln und analysieren ihre Daten bereits zentral auf offenen Cloud-Plattformen. Um große und sich rasch realzeitlich ändernde Mengen an Informationen übertragen zu können, ist eine hochperformante Vernetzung nötig. Eine, die es erforderlich macht, in den kommenden Jahren eine passende Infrastruktur aufzubauen. Das Ziel: Big Data mit geringer Latenz und hoher Bandbreite übertragen zu können. Eine Architektur, die dezentral verteilte Daten derartig übergreifend vernetzt verarbeiten soll, macht Interconnection-Plattformen zum Kernstück jeder Konnektivitätsstrategie einer Smart City. Diese sorgen nicht nur für eine stabilere Internetverbindung durch direkte Interconnection- oder Peering-Dienste, sondern auch für Cloud-Konnektivität durch Cloud Exchanges und Cloud Router. Der Betreiber einer Interconnection-Plattform kann dabei sichere, zuverlässige und leistungsstarke Datenübertragungen gewährleisten.

Performanz maximieren, Latenzzeiten minimieren

Fest steht: Alle Mobil-Applikationen der Smart City können nur so intelligent und leistungsfähig sein, wie es ihnen die Infrastruktur erlaubt, auf der sie betrieben werden. Ohne eine performante Verbindung zu Clouds, Mobil- und Glasfasernetzwerken sowie geographisch verteilten Rechenzentren lassen sich die gewünschten Latenzzeiten und Geschwindigkeiten nicht erreichen. Nur mit einer leistungsfähigen Infrastruktur für den Datenaustausch können 5G- und 6G-basierte Mobilgeräte, Sensoren und Smart-City-Anwendungen ihr volles Potenzial entfalten.

Dr. Christoph Dietzel

MEHR WERT

Cloud Exchanges
https://www.de-cix.net/en/services/directcloud

5G ist nicht gleich 5G

WORAUF ES FÜR UNTERNEHMEN ANKOMMT

Tatsächlich gibt es drei Arten von 5G-Spektrumsbändern: Low-Band, Mid-Band und High-Band. Was bieten die drei 5G-Spektrumsarten und welche Anwendungsfälle machen sie für Unternehmen möglich?

Jedes 5G-Band besteht aus einer zusammenhängenden Gruppe von Funkfrequenzen, deren Geschwindigkeit (Leistung) und Reichweite (Ausbreitung) variieren. Bei 5G-Spektrumsbändern stehen Leistung und Ausbreitung in einem umgekehrten Verhältnis: Bänder mit hoher Ausbreitung haben eine begrenzte Leistung, Bänder mit hoher Leistung haben eine begrenzte Ausbreitung. Was müssen Unternehmen wissen, um die richtige 5G-Lösung für sich zu finden?

ES IST WICHTIGER DENN JE, DASS UNTERNEHMEN SICHERSTELLEN, DASS SICH IHRE EDGE-NETZWERK-LÖSUNGEN NAHTLOS AN JEDE PHASE DER 5G-EINFÜHRUNG ANPASSEN KÖNNEN.

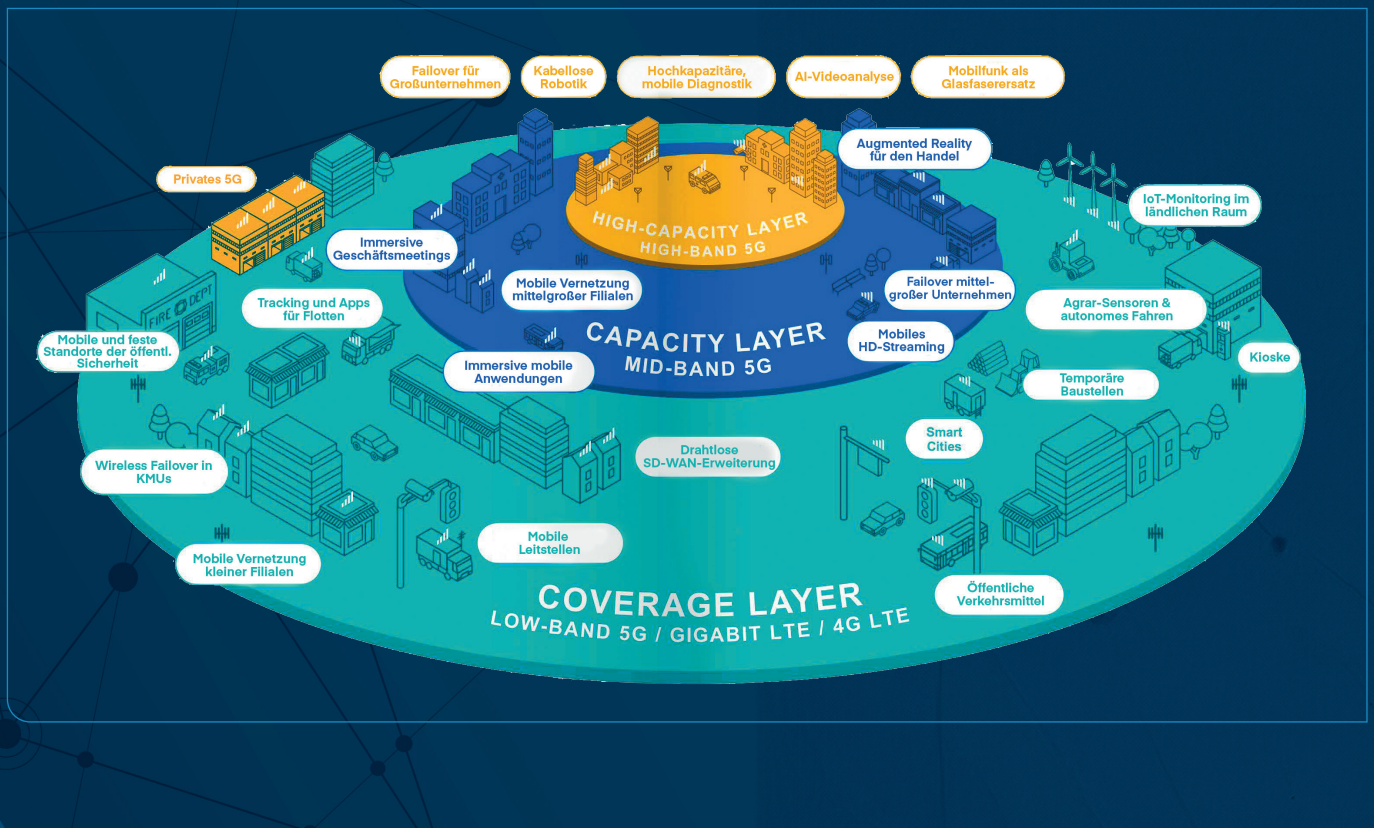
Jan Willeke, Area Director Central Europe, Cradlepoint, www.cradlepoint.com

Low-Band 5G –
Die Versorgungsebene

Neben 4G LTE und Gigabit-Class LTE ist Low-Band 5G Teil der Versorgungsebene. Seit seiner Einführung findet der Mobilfunkdienst in der Versorgungsschicht statt, die das Spektrum unter 2 GHz (meist unter 1 GHz) nutzt. Die Versorgungsschicht hat gute Ausbreitungseigenschaften, aber die geringste Datenkapazität aller Frequenzschichten. Was nicht heißt, dass sie im Vergleich zu anderen Mobilfunktechnologien nicht leistungsfähig ist: Low-Band 5G ist im Schnitt 20 Prozent schneller als 4G. Mit der höchsten Ausbreitung kann das Signal Hindernisse durchdringen und große Entfernungen zurücklegen und hat viele Anwendungen: Konnektivität für öffentliche Verkehrsmittel und Ersthelfer, Flottenverfolgung, IoT-Überwachung, Pop-Up Stores und Verkaufskioske funktionieren hervorragend in der Versorgungsschicht. Viele Anwendungen werden in der Versorgungsschicht gut funktionieren, während andere eine höhere 5G-Leistung benötigen.

Mid-Band 5G –
Die Kapazitätsschicht

Mit 5G wurden zwei neue Frequenzebenen für die Mobilfunkkommunikation eingeführt. Die erste wird als Kapazitätsschicht bezeichnet und arbeitet zwischen 2-7 GHz. Die Kapazitätsschicht bietet deutlich mehr Bandbreite, aber eine geringere Ausbreitung als die Versorgungsschicht, da sie eine stärkere Verdichtung als die Versorgungsschicht erfordert. Diese Schicht wird meist als Mid-Band 5G bezeichnet und gilt für viele als der Sweet Spot von 5G – sie bietet gute Kompromisse zwischen Leistung und Ausbreitung.



Das 5G-Mittelband erweitert die Fähigkeiten und Anwendungsbereiche, die bisher über die grundlegende Versorgungsschicht möglich waren. Ersthelfer können beispielsweise verbesserten Zugriff auf mobile HD-Streaming-Dienste direkt aus ihren Einsatzfahrzeugen erhalten. Ähnlich können Überwachungskamerasysteme, die bisher nur Standardansichten boten, in der Mittelbandschicht aufgerüstet werden und hochauflösende Bilderkennung ermöglichen. Auch der Einsatz von Augmented Reality für Handels- und Sicherheitsanwendungen wird durch die Kapazitätsschicht von 5G erleichtert, was zu effizienteren und interaktiveren Lösungen führt.

High-Band 5G –
Die Hochkapazitätsschicht

Die zweite neue Spektrumsebene, die mit 5G eingeführt wurde, wird als Hochkapazitätsschicht bezeichnet – auch High-Band 5G und mmWave-Spektrum genannt, benannt nach dem Abstand zwischen den Funkwellen. Diese Schicht liegt in der Regel über 24 GHz und kann mit Download-Geschwindigkeiten von bis zu 3 Gbit/s signifikant mehr Daten übertragen, als die Schichten mit niedrigem und mittlerem Spektrum. Diese höheren Frequenzen sind anfälliger für Wetter, Störungen durch Gebäude und hohe Entfernungen. Betreiber haben es jedoch möglich gemacht, dieses Spektrum zu nutzen mit neuen Antennen, dichten Netzwerkarchitekturen und Techniken zur Strahlformung. Diese Technologien wurden in den neuen 5G-Standard integriert und die meisten großen Betreiber werden mmWave in ihre 5G-Rollout-Architektur aufnehmen. Allerdings wird mmWave 5G auf Gebiete beschränkt bleiben, in denen die Übertragungen, die nur in direkter Sichtlinie möglich ist, dichtere Bevölkerungen erreichen können.

Die Ergänzung des 5G-Hochfrequenzbands schafft erheblich mehr Möglichkeiten für Unternehmen. Dieses Frequenzband ist für Anwendungen reserviert, die höchste Leistung erfordern, darunter Videoerkennung mit künstlicher Intelligenz (KI), drahtlose Robotik und drahtloser Glasfaserersatz. Neben zukunftsorientierten Anwendungen wie ferngesteuerten Standorten und Fabriken, die eine vorbeugende Selbstwartung durchführen können, bietet die Hochleistungsschicht Geschäftskontinuität durch die Ausfallsicherung großer Standorte und kann sogar vorübergehend eingesetzt werden, um Sportveranstaltungen oder große Kongresse zu ermöglichen.

MEHR WERT

Sind Sie 5G-Ready?
https://enterprisewanassessment.com/

Die Wahl von 5G –
Flutlicht oder Laserpointer?

Alle 5G-Spektrumsbänder ähneln sich insofern, als sie für verbesserte mobile Breitbanddienste, IoT-Funktionen und einige grundlegende Funktionen für Ausfallsicherheit genutzt werden können, haben aber, wie beschrieben, auch exklusive Anwendungsfälle. Zusammenfassend kann man sich die einzelnen Bänder und ihre Fähigkeiten als Lichtstrahlen vorstellen. Das Low-Band ist vergleichbar mit

einem Flutlicht: Es wirft einen breiten Lichtstrahl, ist aber nicht unbedingt das konzentrierteste und leistungsfähigste Licht. Mid-Band ähnelt dem Strahl einer Taschenlampe, der präziser ist und einen kleineren Radius hat. High-Band ist wie ein Laserpointer mit höchster Präzision, aber einem kleinen Wirkungsradius.

Mit Blick auf die Zukunft werden die Netzbetreiber die Performance von 5G weiter ausbauen, über die bloße Nutzung unterschiedlicher Spektren hinaus. Der Standardansatz wird die Carrier-Aggregation sein – eine Technik, bei der mehrere Mobilfunknetzbetreiber in einem einzigen Kanal kombiniert werden, um die Netzkapazität zu erhöhen. Die Vorbereitung auf die Einführung der verschiedenen Arten von 5G ist entscheidend, um ihre Vorzüge auch nutzen zu können. Es ist wichtiger denn je, dass Unternehmen sicherstellen, dass sich ihre Edge-Netzwerklösungen nahtlos an jede Phase der 5G-Einführung anpassen können.

Jan Willeke

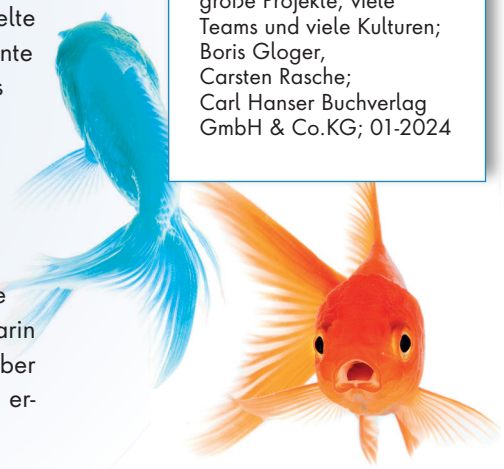
SCRUM THINK BIG

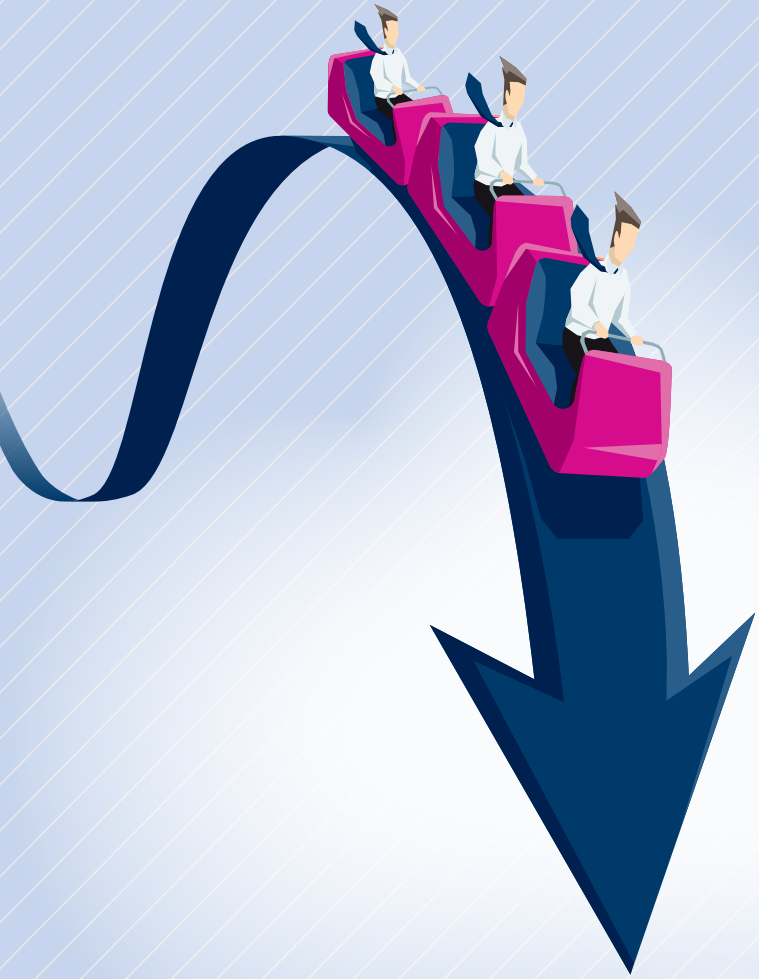
SCRUM FÜR WIRKLICH GROSSE PROJEKTE, VIELE TEAMS UND VIELE KULTUREN

In kleinen Teams hat sich Scrum als Weg für die erfolgreiche Produktentwicklung längst etabliert. Doch jetzt geht es um andere Dimensionen: Unter dem Druck der Digitalisierung wollen Unternehmen die Erfahrungen aus agilen Pilotprojekten auf immer größere Teile der Organisation übertragen. Agile Skalierungsframeworks versprechen schnelle und einfache Lösungen, doch diese vorgefertigten Strukturen führen nicht zum eigentlichen Ziel: dem agilen Unternehmen.

Boris Gloger und Carsten Rasche beschreiben in diesem Buch einen anderen Weg, der auf Praxiserfahrungen basiert. Bei der Skalierung von Scrum geht es nicht um die Multiplikation einer Methode, sondern um einen neuen Blick auf das große Projekt als fraktal skalierte Organisation. Gefragt sind entkoppelte Produktarchitekturen, das konsequente Denken aus Sicht der Kunden, das Projektmanagement- Office als umsichtiger Scrum Master, die Lust auf frische Skills, gestützt durch moderne Infrastrukturen. Und schließlich braucht es eine Führung, die ihre wichtigste Aufgabe darin sieht, Zusammenarbeit über alle Ebenen hinweg zu ermöglichen.

Scrum Think big:
Scrum für wirklich große Projekte, viele Teams und viele Kulturen;
Boris Gloger,
Carsten Rasche;
Carl Hanser Buchverlag GmbH & Co.KG; 01-2024





Wirtschaftlichkeit in der Wolke

DIE CLOUD MUSS NICHT ÜBERTEUERT SEIN

Das Bild von Cloud-basierten Lösungen als technologisch-ökonomische Revolution hat erste Risse bekommen. Immer mehr Unternehmen stellen die anfangs als kosteneffizient angepriesenen Modelle auf den Prüfstand, nicht wenige kehren Hyperscalern und Public Cloud den Rücken zu. Mit Recht, denn wirtschaftlich attraktive Alternativen gibt es schon lange.

Die Misere beginnt mit der wachsenden Beliebtheit. Galt die Cloud zu Anfang noch als der technologische Heilsbringer, der Remote-Work realisierte, fehlende Rechenleistung wett machte und Skalierung neu definierte, entwickelte sich der anhaltende Erfolg schnell zum Problem für Anwender. Was auf den ersten Blick paradox klingt, hat ganz ökonomische Gründe: Der exponentiell wachsende Speicherplatzbedarf ließ die Betriebskosten in die Höhe schnellen. Viele Anbieter von Cloud-Lösungen, die über keine eigene Serverinfrastruktur verfügten, befanden sich hier in der Abhängigkeit von Hyperscalern, die häufig überhöhte Hosting-Gebühren verlangten. Diese Cloud-Anbieter waren dann gezwungen, die aufgeblähten Kosten an ihre Nutzer weiterzugeben. Aus den schlanken und billigen Cloud-Modellen wurden so aufgeblähte Kostenmodelle, die zu einem Umdenken auf Seiten der Nutzer führen muss – eine Entwicklung, die bereits zu beobachten ist. Nüchtern betrachtet führt auf dem wettbewerbsintensiven Markt kein Weg an Cloud-Lösungen vorbei, um die eigene IT-Infrastruktur effizienter zu gestalten und flexibel auf neue Anforderungen zu reagieren. Weil aber Investitionen in die Angebote der Hyperscaler immer unwirtschaftlicher werden, gehen mehr und mehr Anbieter von Cloudbasierten Lösungen gänzlich neue Wege.

In die Cloud, aber sinnvoll

Als Reaktion auf die steigenden Preise der großen Anbieter von weltweiter Serverinfrastruktur, weichen mehr und mehr Anbieter von Cloud-Lösungen auf eine eigene Infrastruktur aus, anstatt sich von den überteuerten Angeboten der Hyperscaler abhängig zu machen. Mit Erfolg: Die Nutzung der eigenen Server führt zu einer größeren Kontrolle über die Systeme und zu großen Einsparungen, die direkt an Endkunden weitergegeben werden können. Daher kann es sich auch für Endkunden sehr schnell rechnen, sich von Cloud-Anbietern abzuwenden, die auf Hyperscaler setzen – wenn die Rahmenbedingungen stimmen. Als Fundament einer erfolgreichen und auf die eigenen Anforderungen abgestimmten Cloud-Strategie kommt es dabei abseits der Platzhirsche auf dem Markt weiterhin auf die Wahl des richtigen Partners als Drittanbieter an. Anstelle der großen, unflexiblen One-fits-All-Lösungen von AWS, Azure und Co. stehen dabei aber Anbieter im Fokus, die auf die spezifischen Bedürfnisse der Unternehmen eingehen und somit auch die Investitionen an die individuellen Anwendungsfälle anpassen können. Ein weiterer entscheidender Vorteil: Anbieter, die ihre eigenen Rechenzentren betreiben, besitzen eine umfassende Kontrolle über ihre Kosten, Lieferketten und Infrastruktur.

Damit sich die Wahl des Cloud-Anbieters, egal, ob Public, Private oder Hyb-

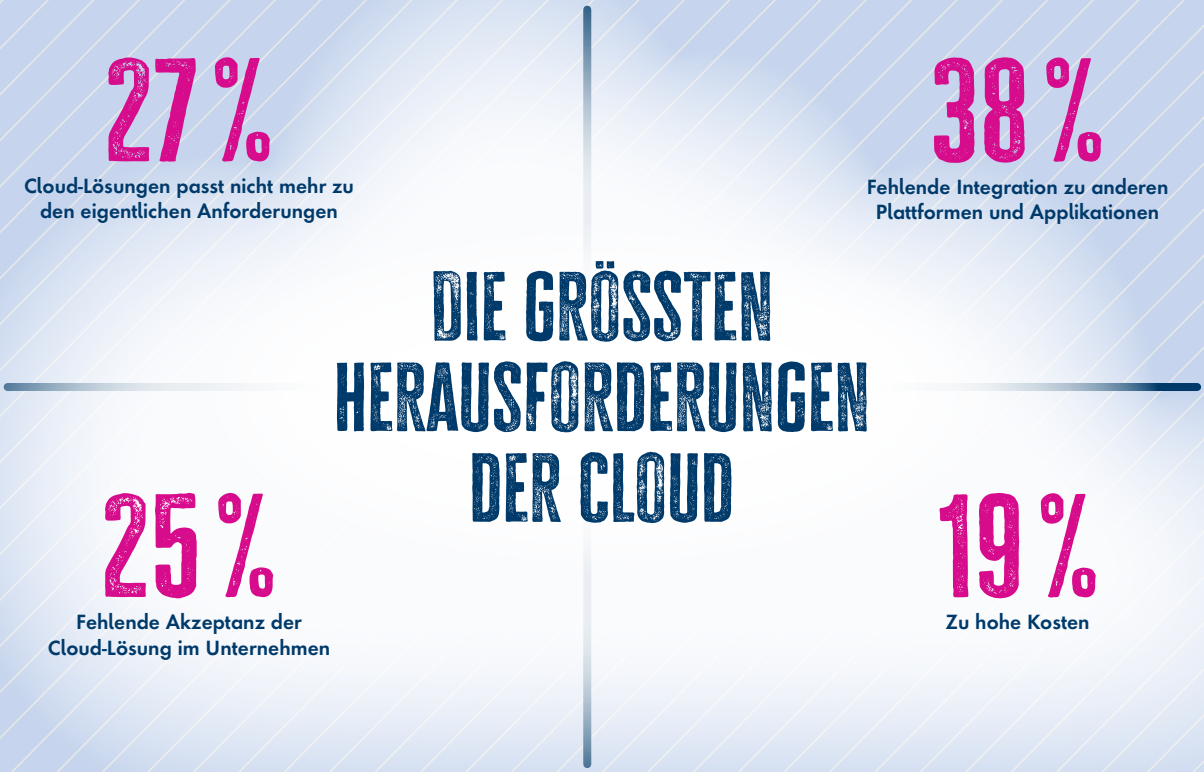
rid, zu einer langfristigen Partnerschaft entwickelt, sollten Unternehmen auf eine transparente und planbare Geschäftsstrategie von potenziellen Partnern achten. Dabei geht es vor allem um die Frage, wie sich die Konditionen bei dem Fall eines Unternehmenswachstums verändern – und wie sich eine Skalierung auf den Preis der Dienste auswirkt. Aber auch die langfristigen Ambitionen der Anbieter spielen eine entscheidende Rolle, um eine Vorstellung von möglichen zukünftigen Fusionen und Übernahmen zu erhalten. Daneben sollte auch eine klar definierte Roadmap zu geplanten Einführungen von Innovationen sowie Wachstumsplänen in die Entscheidungsfindung miteinfließen. Diese Faktoren werden die Kunden in Zukunft beeinflussen. Die Abstimmung der Unternehmenswerte und -strategien mit dem Cloud-Partner ist unerlässlich, um eine nahtlose Kundenerfahrung zu gewährleisten und das Potenzial für unerwartete Überraschungen langfristig zu verringern.

Die Wahl des richtigen Anbieters hat darüber hinaus aber auch grundlegende wirtschaftliche Motive – können Unternehmen ihre IT-Ausgaben mit der richtigen Entscheidung doch erheblich senken, indem sie von Vorteilen wie geringeren Anschaffungskosten, Kostenverteilung und niedrigeren Gesamtbetriebskosten profitieren. All diese Aspekte tragen dazu bei, auf dem Markt wettbewerbsfähig zu bleiben und eine zukunftssichere Strategie umzusetzen.

Das Risiko minimieren

Eine nicht abgestimmte Cloud-Strategie und Anbieter mit den falschen Konditionen können sich zu einer wirtschaftlichen Gefahr entwickeln. Steigende Kosten stoßen dabei nicht selten auch einen Dominoeffekt an, der auf andere Geschäftsbereiche übergreift und zu Budgetkürzungen in Kernbereichen wie Personal oder Marketing führt. Als Konsequenz sind Unternehmen unter Umständen dazu gezwungen, die hohen Kosten an ihre Kunden weiterzugeben. Die Auswahl eines geeigneten Anbieters kann diese Risiken jedoch nahezu eliminieren und helfen, eine erhebliche Kapitalrendite zu erzielen. Im Umkehrschluss müssen Cloud-Anbieter dabei einerseits die Wirtschaftlichkeit der Kunden sicherstellen, andererseits aber auch ganz praktische Aufgaben auf höchstem Niveau meistern – allen voran der umfassende Schutz von Unternehmensdaten. Potenzielle Gefahren wie Cyberangriffe und Datenschutzverletzungen, die zu Datenverlust, finanziellen Schäden und Reputationsverlust führen können, dürfen keine Nebenrolle spielen. Ein Vorteil für Unternehmen: Viele Anbieter verfügen über umfassende IT-Security-Expertise, deren Niveau mit eigenen Inhouse-Ressourcen nur schwer zu erreichen und mit hohen Kosten verbunden ist.

Ein besonderes Augenmerk muss dabei zwangsläufig auf den entstehenden Kosten liegen, die nicht wenigen Unternehmen in Sachen Cloud Computing zu entgleiten drohen. So ergab eine Umfrage des globalen Technologieanbieters Zoho



Die größten Stolpersteine auf dem Weg in die Cloud im Überblick.

Quelle: Die Studie wurde in Auftrag von Zoho von Censuswide durchgeführt, die dafür unter anderem rund 300 deutsche Unternehmen zum Thema "Digitale Transformation" befragt haben.

und dem Marktforschungsinstitut Censuswide unter rund 300 Entscheidungsträgern in Deutschland, dass knapp jede fünfte Firma eigenen Angaben nach zu viel für Cloud Services bezahlt, als es ökonomisch sinnvoll wäre. Ein anderes Problem, das die Studie aufdeckt: 38 Prozent der Befragten haben Probleme mit der Interoperabilität zwischen der gewählten Lösung und anderen Plattformen sowie Applikationen, weil sie die Entscheidungsfindung überstürzt haben. Abhilfe schafft eine solide Implementierungsstrategie, die potenzielle Risiken frühzeitig aufdeckt und sowohl Funktionalität als auch Wirtschaftlichkeit sicherstellt.

Anbieter mit eigener Infrastruktur auf dem Vormarsch

Dropbox, Netflix und Basecamp sind als Anbieter von Cloud-Services einige prominente Beispiele für eine tendenzielle Entwicklung, die sich von den großen Hyperscalern abwendet und die eigenständige Verwaltung eigener Server und Infrastrukturen bevorzugt. Der Umstieg wird auch deswegen für viele Anwender wieder attraktiv, weil sie bei der Datenverarbeitung auf AWS, Azure und anderen großen Anbietern das eigentlich angestrebte Ziel einer Kostensenkung schlicht nicht mehr erreichen. Wird die Cloud damit unwirtschaftlich? Nein, aber der Unterschied zwischen Hyperscalern und Drittanbietern mit einer eigenen Infrastruktur wird immer deutlicher. Die Versprechen der Cloud sind weiterhin ungebrochen – bei der Frage nach dem Wie und Wo sollten Anwender allerdings eine langfristige Planung berücksichtigen und in Sachen der Wirtschaftlichkeit auch Anbieter mit eigener Infrastruktur im Auge behalten.

Sridhar Iyengar

DIE VERSPRECHEN DER CLOUD SIND WEITERHIN UNGEBROCHEN – BEI DER FRAGE NACH DEM WIE UND WO SOLLTEN ANWENDER ALLERDINGS EINE LANGFRISTIGE PLANUNG BERÜCKSICHTIGEN.

Sridhar Iyengar, Managing Director, Zoho Europe, www.zoho.com

Dezentralisierte physische Infrastrukturnetzwerke (DePIN)

DIE LÖSUNG FÜR EUROPAS CLOUD-PROBLEM?

Europa hat ein Cloud-Problem: Die Abhängigkeit von einigen wenigen globalen Anbietern engt den Markt ein, was für europäische Unternehmen hohe Kosten und Datenschutzbedenken mit sich bringt. Diese Situation beeinträchtigt die Wettbewerbsfähigkeit und untergräbt die digitale Souveränität Europas. Eine Lösung ist dringend nötig: Eine dezentrale, europäische Cloud-Infrastruktur, die nicht nur kosteneffizient ist, sondern auch den strengen Datenschutznormen der EU entspricht.

DePIN BIETET EINE VISIONÄRE ANTWORT AUF DIE DRÄNGENDEN FRAGEN DER EUROPÄISCHEN CLOUD-INFRASTRUKTUR.

Dr. Kai Wawrzinek, CEO und Mitgründer, Impossible Cloud GmbH, https://de.impossiblecloud.com/

Dezentralisierte physische Infrastrukturnetzwerke (DePIN) stellen einen vielversprechenden Ansatz dar, um Europas Bindung an die Cloud-Giganten zu überwinden. Indem sie auf Dezentralisierung setzen, zielen DePIN darauf ab, die Abhängigkeiten zu minimieren, die wirtschaftliche und sicherheitsbezogene Risiken für Unternehmen bergen. DePIN könnten der entscheidende Baustein für eine selbstbestimmte, zukunftsfähige digitale Infrastruktur in Europa sein.

Was ist DePIN?

Bislang hat DePIN vor allem in Krypto-Medien Schlagzeilen gemacht – befeuert durch Kursanstiege einzelner Kryptowährungen, die mit dem Sektor in Verbindung gebracht werden. Doch wer DePIN nun als kurzlebigen Krypto-Hype abtut, übersieht das enorme Potenzial, das in dezentralen physischen Infrastrukturnetzwerken schlummert.

DePIN steht für eine radikale Abkehr von herkömmlichen, zentralisierten Cloud-Modellen. Die technische Grundlage bildet eine dezentrale Architektur, die Daten über ein weit verteiltes Netzwerk von Knotenpunkten speichert und verarbeitet. Diese Struktur erhöht einerseits die Ausfallsicherheit, indem sie Single-Point-of-Failure-Risiken reduziert. Andererseits ermöglichen DePIN-Modelle geringere Latenzzeiten, weil die Daten in einem voll ausgebauten Netzwerk kürzere Wege zurücklegen müssen. Nicht zuletzt fördert die Dezentralisierung eine höhere Flexibilität und Skalierbarkeit der Cloud-Dienste, was insbesondere in einer Welt, die von Daten, Echtzeitkommunikation und KI angetrieben wird, von entscheidender Bedeutung ist.

DePIN und DLT: Ein starkes Team

DePIN repräsentiert einen Paradigmenwechsel in der Art und Weise, wie Cloud-Infrastrukturen konzipiert und betrieben werden. Anstatt sich auf zentrale Rechenzentren zu stützen, verteilt DePIN die Datenhaltung und -verarbeitung über ein Netzwerk von Knotenpunkten, die von verschiedenen Akteuren in einem dezentralisierten System betrieben werden. Dieser Ansatz nutzt die Prinzipien von Blockchain- oder anderen Distributed-Ledger-Technologien (DLT), um Transparenz, Sicherheit und Unveränderlichkeit der Daten für alle Netzwerkteilnehmer zu gewährleisten. Bei einer DLT wird jede Transaktion in einem verteilten Hauptbuch (Ledger) aufgezeichnet, das auf mehreren Computern oder Knoten gespeichert ist, was die Daten gegen Manipulation und unautorisiertem Zugriff sichert. Teilnehmer, die Aufgaben im Netzwerk übernehmen (zum Beispiel Transaktionen bestätigen), erhalten für ihre Dienste in der Regel eine Belohnung in Form von Krypto-Token.

In der Welt von DePIN sollen Token indes nicht nur digitale Interaktionen, sondern auch den Aufbau physischer Infrastrukturen incentivieren. Beispielsweise belohnt Filecoin, ein dezentrales Speichernetzwerk, seine Nutzer mit Token für die Bereitstellung von Speicherplatz und das Hosting von Dateien. Beim Helium Network erhalten Teilnehmer dagegen Token für den Betrieb von Hotspots, um eine

drahtlose Netzabdeckung für IoT-Geräte bereitstellen. Die jeweiligen Token können dann gehandelt oder verwendet werden, um Netzwerkdienste zu bezahlen.

Adoptions-Hemmnisse:
Wo bleibt der DePIN-Run?

Doch obwohl Projekte wie Filecoin, Helium und Co. bereits seit längerem auf dem Markt sind, kann von einem Run auf DePIN – zumindest abseits der Krypto-Börsen – noch nicht die Rede sein. Trotz der offensichtlichen Vorteile zögern viele Unternehmen noch, DePIN zu adoptieren. Einige der Gründe hierfür sind:

- Technische Komplexität: Der Übergang zu einem dezentralisierten Netzwerk erfordert oft ein Umdenken in Bezug auf Datenmanagement und -sicherheit. Unternehmen müssen sich mit der neuen Technologie vertraut machen und möglicherweise bestehende Infrastrukturen anpassen.

- Regulatorische Unsicherheit: Da diese Technologien relativ neu sind, gibt es oft noch keine klaren regulatorischen Rahmenbedingungen, was Unternehmen zur Vorsicht mahnt.

- Marktreife: Viele dezentralisierte Lösungen sind noch in den Anfangsphasen ihrer Entwicklung. Ihre Leistung und Zuverlässigkeit müssen sich erst noch in großem Maßstab beweisen.

- Vertrauensfaktoren: In einem dezentralen Netzwerk müssen Unternehmen darauf vertrauen, dass die Daten sicher und jederzeit verfügbar sind, ohne die Kontrolle einer zentralen Autorität.

- Volatilität von Kryptowährungen: Kryptowährungen sind berüchtigt für ihre starken Kursschwankungen, was eine eingeschränkte Planungssicherheit für Teilnehmer in DePIN-Netzwerken bedeuten kann.

Ein Großteil dieser Adoptionshemmnisse wird sich mit der Zeit auflösen. Die Einführung der MiCA-Regulierung (Markets in Crypto Assets) durch die EU und das wachsende Vertrauen in den gereiften Krypto-Markt tragen beispielsweise dazu bei, DePIN-Lösungen für Unternehmen interessanter zu machen.

Cloud Act vs. DSGVO:
Ein Zielkonflikt zwischen USA und EU

Darüber hinaus stärkt DePIN-Technologie die digitale Souveränität Europas. Für europäische Unternehmen eröffnet sie somit neue Möglichkeiten, ihre Abhängigkeit von nicht-europäischen Technologiegiganten zu verringern und gleichzeitig die Datenschutzstandards gemäß der DSGVO einzuhalten. Denn das ist, Stand heute, leider keine Selbstverständlichkeit.

So gibt es einen massiven Konflikt zwischen dem US-amerikanischen CLOUD-Gesetz (Clarifying Lawful Overseas Use of Data Act) und der DSGVO der Europäischen Union. Der Cloud Act erlaubt es US-Behörden, auf Daten zuzugreifen, die von US-Unternehmen gespeichert wurden – selbst, wenn diese Daten außerhalb der USA gespeichert sind. Dies steht im direkten Widerspruch zur DSGVO, die strenge Regeln für den Transfer und die Verarbeitung personenbezogener Daten von EU-Bürgern vorschreibt.

Dieser Umstand unterstreicht das Potenzial von DePIN, Unternehmen eine stärkere lokale Kontrolle und Schutz der in der Cloud gespeicherten Daten ermöglichen. Dabei helfen Techniken wie Geofencing – die Begrenzung von Speicherzugriffen auf definierte geografische Regionen – erlaubt es europäischen Unternehmen, gegenüber extraterritorialen Gesetzen Resilienz zu zeigen.

Ausblick

Keine Frage: DePIN bietet eine visionäre Antwort auf die drängenden Fragen der europäischen Cloud-Infrastruktur. Durch die Förderung von Dezentralisierung, Datensouveränität und nicht zuletzt des Wettbewerbs hat DePIN das Potenzial, die Landschaft der digitalen Dienste in Europa nachhaltig zu verändern. Die weitere Entwicklung und Integration in Europas digitale Ökosysteme wird entscheidend sein, um die digitale Souveränität langfristig zu stärken und eine innovative, sichere und unabhängige digitale Zukunft für Europa zu gestalten. Eine Zukunft, in der jedermann exzellente Cloud-Dienste zu einem Bruchteil der heutigen Kosten genießen kann.

Dr. Kai Wawrzinek

Unternehmen fit für die Zukunft machen

GESCHÄFTSPROZESS- UND CHANGE-MANAGEMENT VERZAHNEN

Oft entwerfen Unternehmen am „grünen Tisch" Geschäftsprozesse in ihrer Organisation neu. Dann funktioniert deren Einführung meist nicht so reibungslos wie geplant, denn: Wenn sich die Abläufe und Strukturen ändern, muss sich auch das Verhalten der Mitarbeiter ändern. Das gilt es beim Neugestalten der Prozesse zu beachten.

„Wir müssen unsere Geschäftsprozesse auf den Prüfstand stellen und ein gezieltes Geschäftsprozessmanagement betreiben." Diese Aussage hört man seit einigen Jahren gehäuft von Top-Managern, da sich die Rahmenbedingungen des wirtschaftlichen Handelns ihrer Unternehmen immer schneller und fundamentaler wandeln. Als Beleg hierfür seien die Stichworte Corona, Ukraine-Krieg, Klimawandel, Energiekrise, Lieferengpass, Fachkräftemangel, Inflation, multipolare Weltordnung und Künstliche Intelligenz genannt.

Ziel: Das Unternehmen zukunftsfit machen

Von einem Neugestalten der Geschäftsprozesse – meist auch mit Hilfe der Digitaltechnik – versprechen sich die Unternehmensführer in der Regel unter anderem:

- kürzere Durchlaufzeiten,
- weniger Fehlerquellen und
- eine effizientere Nutzung der Ressourcen

also letztlich niedrigere Kosten auf allen Ebenen und mehr Gewinn sowie eine höhere Qualität und Kundenzufriedenheit.

FÜR EINE STÄRKERE VERZAHNUNG VON GESCHÄFTSPROZESS-MANAGEMENT UND CHANGE-MANAGEMENT IST EINE CHANGE-MANAGEMENT-QUALIFIZIERUNG DER PROZESS-MANAGER/-BERATER SOWIE DER FÜHRUNGSKRÄFTE UND DER MITARBEITER, DIE EINE SCHLÜSSELROLLE SPIELEN, UNVERZICHTBAR.

Prof. Dr. Georg Kraus,
Inhaber, Kraus & Partner,
www.kraus-und-partner.de

Das Unternehmen soll hierdurch also „zukunftsfit" gemacht werden.

Im Unternehmensalltag erweist sich das Geschäftsprozessmanagement jedoch als ein sensibles Thema – auch weil die Mitarbeiter mit dem Neugestalten der Geschäftsprozesse meist Vokabeln wie „Kostensenkung", „Personalabbau", „Automatisierung", „Outsourcing" und einen erhöhten Veränderungsdruck assoziieren. Demzufolge reagieren sie reserviert auf entsprechende Initiativen der Unternehmensleitung. Das gilt auch für die Führungskräfte. Denn auch sie befürchten: Wenn die Prozesse bereichs- und funktionsübergreifend optimiert werden, wird auch so manche Führungsposition obsolet. Zudem wird das Alltagshandeln der verbleibenden Führungskräfte einer stärkeren Kontrolle unterworfen. Also sperren auch sie sich nicht selten mental gegen ein modernes, professionelles Geschäftsprozessmanagement, selbst wenn sie dessen strategische Notwendigkeit und betriebswirtschlichen Nutzen durchaus sehen.

Ziel: Alle ziehen am selben Strang

In der Vergangenheit beschränkte sich das Geschäftsprozessmanagement in vielen Unternehmen weitgehend auf ein Re-Design der Prozesse oder auf Prozessoptimierungen in einzelnen Unternehmensbereichen – so als seien diese autonome Einheiten. Dabei werden heute zumindest die Kernleistungen der Unternehmen auch im Gefolge der fortschreitenden Digitalisierung meist in einer funktions- und bereichsübergreifenden Team- und Projektarbeit erbracht.

Durch diese fragmentarische Heran- und Vorgehensweise stieg die Zahl der Schnittstellen; zudem wurde die funktions- und bereichsübergreifende Zusammenarbeit diffiziler. Entsprechend groß ist heute noch der Bedarf an Abstimmung und Koordination, weshalb viele Fach- und Führungskräfte einen großen Teil ihrer Arbeitszeit in Meetings verbringen.

Dieses Manko möchte ein modernes, professionelles Geschäftsprozessmanagement beheben, und zwar indem die für

DAS CHANGEMANAGEMENT-BERATUNGSDREIECK

den Kunden Wert schöpfenden Prozesse identifiziert und mit der Strategie des Unternehmens in Verbindung gebracht werden. Hieraus werden dann Optimierungsvorschläge abgeleitet, die anschließend umgesetzt werden. Dabei sorgen Prozesskennzahlen für eine Transparenz der Qualität und Kosten. Sie ermöglichen zudem eine zeitnahe Reaktion, wenn das Erreichen der Ziele gefährdet ist.

Eine zentrale Rolle spielen dabei die Prozessmanager oder -berater. Ihre Aufgaben variieren von Unternehmen zu Unternehmen. In der Regel sind sie jedoch verantwortlich für:

- das Aufsetzen neuer Projekte,
- das Re-Design der Geschäftsprozesse,
- deren Einführung in der Organisation und
- das kontinuierliche Führen, Planen, Überwachen, Steuern und Verbessern der Prozesse – mit den Führungskräften.

Die Mitarbeiter: Erfolgsfaktor und Hemmschuh

Der wichtigste Erfolgsfaktor und zugleich Hemmschuh beim Neugestalten und Weiterentwickeln der Geschäftsprozesse sind die Mitarbeiter. Sie müssen eine hohe Veränderungsfähigkeit und -bereitschaft zeigen. Deshalb hängt der Erfolg eines professionellen, strategischen Geschäftsprozessmanagements weitgehend davon ab, inwieweit es gelingt, die Betroffenen von der Notwendigkeit einer Änderung der Abläufe und Strukturen zu überzeugen.

An diesem Punkt zeigen viele Unternehmen Entwicklungsdefizite. Oft erfolgt das Re-Design der Prozesse und das Planen des künftigen Projektverlaufs am „grünen Tisch". Nicht ausreichend berücksichtigt wird, dass das Unternehmen beim Umsetzen auf die Mitarbeit der Betroffenen angewiesen ist. Folglich werden auch die Grundprinzipien für das Gestalten jedes Change-Prozesses nicht ausreichend berücksichtigt und fließen in das Projektdesign ein. Hierdurch sinkt die Wahrscheinlichkeit, dass die initiierten Veränderungsprozesse erfolgreich umgesetzt werden. Deshalb werden im Folgenden die wichtigsten Change-Management-Prinzipien, die es beim Geschäftsprozessmanagement zu beachten gilt, kurz vorgestellt.

Wichtige Geschäftsprozessmanagement-Prinzipien

#1 Die betroffenen Mitarbeiter/ Führungskräfte beteiligen

Abläufe in Unternehmen funktionieren dann sicher, wenn die beteiligten Menschen diese verinnerlicht und Routine im Umgang mit ihnen entwickelt haben. Dann destabilisieren auch kleinere Störungen das System nicht, was die Qualität sichert. Sollen jedoch Prozesse neu gestaltet werden, dann ist dieses Beharrungsvermögen eher hinderlich. Deshalb sollten die verantwortlichen Führungskräfte und die wichtigen Schlüsselpersonen in die Analyse der aktuellen Situation und in das Neugestalten der Prozesse einbezogen werden. Das stellt sicher, dass ihr Erfahrungs- und Expertenwissen ausreichend berücksichtigt wird. Außerdem haben die Beteiligten weniger das Gefühl, dass ihnen etwas übergestülpt wird. Deshalb identifizieren sie sich stärker mit dem Neuen.

#2 Freiräume für Reflexion und Dialog schaffen

Bei jedem Geschäftsprozessmanagement-Projekt stehen die Beteiligten unter einem hohen Zeit- und Arbeitsdruck. Zu kurz kommt deshalb oft die gemeinsame Reflexion über

- das bereits Erreichte,
- die noch offenen Aufgaben und
- die bestehenden Blockaden/ Schwierigkeiten.

Solche Reflexionsrunden sollten fest institutionalisiert werden, denn sie stärken den Zusammenhalt des „Kernteams" und sorgen dafür, dass seine Mitglieder dieselbe „Sprache" sprechen und am selben Strang ziehen – unter anderem, weil der Gedanken- und Erfahrungsaustausch zu einer Sensibilisierung für die Sichtweisen der Kollegen führt und einen Abgleich mit der eigenen Sicht ermöglicht. Dieser Austausch sollte abseits des operativen (Alltags-)Geschäfts erfolgen.

#3 Die Kommunikation über die Veränderungen planen

Bevorstehende Veränderungen bewirken Unsicherheiten bei den Mitarbeitern und diese führen zur bekannten Gerüchteküche, wenn ein Informationsvakuum besteht. Und hieraus resultieren Reibungs-

verluste und Produktivitätseinbußen. Um diese zu vermeiden, sollte in einem Kommunikationskonzept geplant werden, „wer was wann und auf welche Weise an wen kommuniziert". Und werden Informationen aus guten Gründen zurückgehalten? Dann sollte dies auf Basis einer expliziten Entscheidung und im Bewusstsein der möglichen Folgen geschehen.

#4 Widerstände und Konflikte berücksichtigen und nutzen

Ein Neugestalten (und Automatisieren) von Geschäftsprozessen verursacht Widerstände. Diese Widerstände sind immer emotional bedingt und werden meist verschlüsselt artikuliert. Deshalb sollten die Verantwortlichen mit den „Widerständlern" den persönlichen Dialog suchen, um herauszufinden, was die realen Ursachen sind. Diese sollten dann in einer sachlichen Atmosphäre bearbeitet werden, so dass Vereinbarungen über das weitere Vorgehen möglich sind. Das entschärft die Situation.

#5 In Systemen denken Bitte noch etwas verlängern

Komplexe Veränderungsprozesse, die sich in zahlreiche (Teil-)Projekte, die sich wechselseitig beeinflussen, untergliedern, können nicht mit linearen Denkansätzen umgesetzt werden. Hierfür ist ein Denken in Systemen, also vernetzten Strukturen, nötig. Dieses Denken geht davon aus, dass das Verhalten des Einzelnen von seinem sozialen System beeinflusst wird und er dessen Entwicklung wiederum beeinflussen kann. Dies berücksichtigt ein systemischer Beratungsansatz, weshalb er keine isolierten Problemlösungen entwirft.

#6 Den Schlüsselpersonen die nötigen Kompetenzen vermitteln

Bei jedem Veränderungsprozess gibt es Phasen der Unsicherheit. In ihnen müssen die Führungskräfte ihren Mitarbeitern Orientierung und Halt bieten, auch wenn sie selbst Unsicherheiten plagen; entsprechendes gilt für die Prozessmanager/-berater. Deshalb sollten sie mit den Besonderheiten von Veränderungsprozessen vertraut sein und wissen, dass in ihnen an sie teils andere Anforderungen als in „stabilen Zeiten" gestellt werden. Außerdem sollten sie die Methoden und Instrumente des Change-Managements beherrschen, damit sie die Veränderungen gestalten können. Diese Fähigkeiten müssen die Unternehmen den Schlüsselpersonen in ihrer Organisation vermitteln – auch weil „stabile Zeiten" heute eher die Ausnahme sind. Deshalb hat sich das Change-Management zu einer Kernkompetenz von Führungskräften entwickelt.

#7 Das Prozessdenken in der Unternehmenskultur verankern

Der Einstieg in ein prozessorientiertes Denken und Handeln erfordert in vielen Unternehmen einen Wandel der Unternehmenskultur. Diese Kultur definiert sich aus bewussten und unbewussten Haltungen und Werten, die für die Mitarbeiter wichtig sind, und deren Missachtung für sie oft ein Tabubruch ist. Beim Verändern der Unternehmenskultur spielen die Führungskräfte die zentrale Rolle, weil sie für ihre Mitarbeiter Vor- und Leitbilder sind. Folglich muss mittels entsprechender Maßnahmen des Change-Managements daraufhin gearbeitet werden, dass sich im Handeln der Führungskräfte die veränderte Unternehmenskultur zeigt und sie sich in der Organisation etabliert.

#8 Mit Coaching die Nachhaltigkeit sichern

Wie bereits erwähnt, ist die Rolle des Prozessmanagers/-beraters in Unternehmen nicht fest definiert. Auf alle Fälle sollte es in der Organisation jedoch eine Person oder Institution geben, die für das Geschäftsprozessmanagement verantwortlich ist. Weitere wichtige Aufgaben sind:

- das Coachen der Prozesseigner/-verantwortlichen,
- das Organisieren der Weiterbildung zum Thema Prozess und
- das Etablieren eines Wissensmanagements, um aus Erfahrungen zu lernen.

Um diese Aufgaben professionell wahrzunehmen, benötigen die Verantwortlichen eine hohe Kompetenz in Sachen Change-Management.

Die nötige Change-Management-Kompetenz vermitteln

Eine stärkere Verzahnung von Geschäftsprozess-Management und Change-Management lässt sich auf verschiedene Art und Weise erreichen. Dabei ist jedoch eine Change-Management-Qualifizierung der Prozessmanager/-berater sowie der Führungskräfte und der Mitarbeiter, die eine Schlüsselrolle spielen, unverzichtbar. Entsprechende Aus- und Weiterbildungen werden in verschiedenen Umfängen angeboten – vom dreitägigen Einstiegsseminar bis zur einjährigen berufsbegleitenden Fortbildung. Für die Prozessmanager/-berater bietet sich Letzteres an, weil der Erwerb der nötigen Kompetenz auch mit einem Sammeln von Erfahrung und einer persönlichen Entwicklung verbunden seine sollte. Deshalb sollte bei der Wahl der Ausbildung auf einen hohen Praxisbezug und eine ausreichende Transfermöglichkeit auf das eigene Aufgabenfeld geachtet werden.

Prof. Dr. Georg Kraus

it management

AUSGABE 07-08/2024
ERSCHEINT
AM 1. JULI 2024

UNSERE THEMEN

Projektmanagement
Finance Spezial
KI & Digitalisierung

it security

AUSGABE 07-08/2024
ERSCHEINT
AM 1. JULI 2024

UNSERE THEMEN

Blockchain
Verschlüsselung
IAM & PAM

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: Ralf Bachthaler, Philipp von der Brüggen, Fabian Czicholl, Dr. Christoph Dietzel, Markus Grutzeck, Paul Höcherl, Sridhar Iyengar, Prof. Dr. Georg Kraus, Frank Laschet, Bastian Maiworm, Simon Meraner, Carina Mitzschke, Paula Müller, Otto Neuer, Silvia Parthier, Ulrich Parthier, Benjamin da Silva Moreira, Christian Tauchmann, Amadeus Thomas, Rafat Trojanowski, Dr. Kai Wawrzinek, Ralph Weiss, Jan Willeke

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.

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. 31.
Preisliste gültig ab 1. Oktober 2023.

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, +49-1523-6341255, mann@it-verlag.de

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

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

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

Erscheinungsweise: 6 x pro Jahr

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

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

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

e3mag.com

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

SNP Transformation World

Winning together

Bereits zum 10. Mal lädt Sie SNP nach Heidelberg zur Transformation World ein, eine der größten SAP-Partnerkonferenzen in Europa und interaktive Plattform zum Austausch und Erkenntnisgewinn auf höchstem Niveau. Teilnehmende können sich dieses Jahr wieder auf ein außergewöhnliches Programm mit zahlreichen Praxisberichten führender deutscher und internationaler Unternehmen, mehr als 100 Vorträge rund um die Modernisierung von Systemen und Geschäftsprozessen und hochkarätige Keynote-Speaker sowie auf ein spannendes Rahmen- und Abendprogramm freuen.

Sichern Sie sich jetzt einen der begehrten Plätze!

SNP Transformation World 2024: Winning together
19. – 20. Juni in Heidelberg

Jetzt anmelden!

it security

Detect. Protect. Respond.
Mai/Juni 2024

THOUGHT LEADERSHIP

AB SEITE 10

ninjaOne.

CYBERSICHERHEIT

Eine digitale Souveränität schaffen

Arved Graf von Stackelberg, DriveLock

VON KRITIS ZU NIS2

Kritische Infrastrukturen absichern

DER EINFLUSS VON KI

Digitale Sicherheitslandschaft im Wandel

ARGUSAUGEN DER NEUZEIT

Managed Detection and Response

WE SECURE IT

13. und 14. November 2024

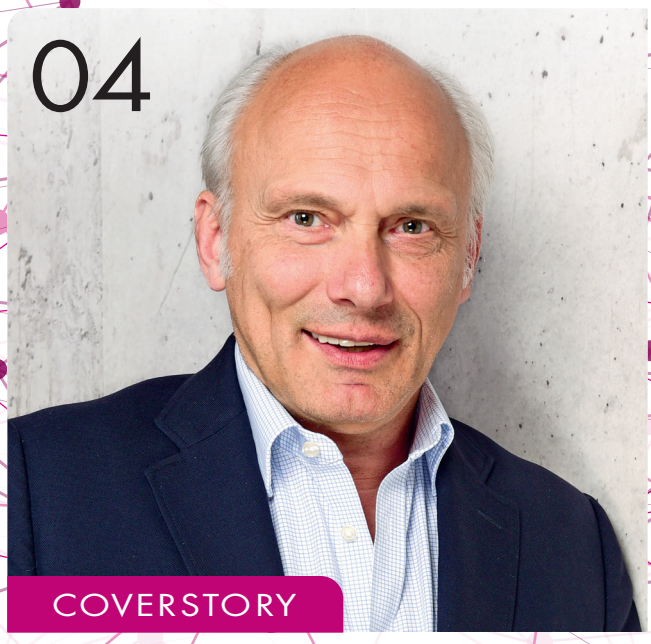
Digitalevent

SAVE THE DATE

it-daily.net

#WesecureIT2024

Eine Veranstaltung von itsecurity & it-daily.net



Inhalt

COVERSTORY

THOUGHT LEADERSHIP

SPEZIAL NIS2

IT SECURITY

Cybersicherheit

DIGITALE SOUVERÄNITÄT IN DEUTSCHLAND UND EUROPA SCHAFFEN

Cyberbedrohungen nehmen zu und mit ihnen die Zahl der Vorschriften und Maßnahmenkataloge, die die IT-Sicherheit in der gesamten Europäischen Union erhöhen sollen. Dazu gehört zum Beispiel die EU-weite NIS2-Regelung für kritische Infrastrukturen (KRITIS), die aktuell in aller Munde ist und im Oktober dieses Jahres in nationales Recht umgesetzt wird. Wir sprachen mit Arved Graf von Stackelberg, CEO bei DriveLock.

it security: *Herr Stackelberg, welche Herausforderungen sehen Sie konkret für Unternehmen in Deutschland im Bereich Cybersecurity?*

Arved Stackelberg: Neben der bereits erwähnten NIS2-Regelung gibt es auch weitere Regelungen, die die Sicherheit und Resilienz erhöhen sollen. Diese sind zum Teil schon in Kraft oder werden es bald sein, wie die DSGVO, das Patientendatenschutzgesetz im Gesundheitswesen oder die geplante DORA-Verordnung (Digital Operational Resilience Act) für den Finanzsektor. Es kommt bei NIS2 noch eine Besonderheit dazu: Wegen der Klassifizierungsmethode sind von der Regelung auch Organisationen betroffen, die zuvor nicht als KRITIS eingestuft wurden und somit noch keine Erfahrung mit Sicherheitsvorschriften auf diesem Niveau haben. Die Entwicklungen der letzten Jahre lassen darauf schließen, dass in Zukunft weitere Gesetze, Verpflichtungen und Regelungen auf Unternehmen und Organisationen jeder Art, Branche und Größe kommen werden. Hier wird es für Unternehmen zunehmend schwieriger, all diese neuen, für Fachfremde unübersichtlichen und strengeren Anforderungen zu erfüllen.

Von staatlicher Seite kommen leider nicht nur mehr Gesetze, sondern auch Cyberbedrohungen. Die geopolitischen Entwicklungen haben vermehrt staatlich gesteuerte Hackerangriffe zur Folge, sei es im Sinne der Wirtschaftsspionage oder als Angriffsmittel. Zudem stehen wir bei Cybercrime allgemein noch am Anfang von dem, was alles mithilfe von KI möglich ist – von glaubwürdigeren Texten für Phishing Emails dank KI-Sprachmodellen bis hin zu Deep Fakes oder mittels KI automatisierten Angriffen im großen Umfang. Gleichzeitig steigt die Skrupellosigkeit der Hacker, denn es geraten auch immer mehr gemeinnützige Organisationen (NGOs) ins Visier, wie etwa zuletzt „Water for the Planet".

Dass 99,8 Prozent der Wirtschaft aus KMU besteht, erschwert die Lage zusätzlich. Denn ebenso wie NGOs und öffentliche Einrichtungen müssen diese meist mit sehr viel weniger Ressourcen Herausforderungen stemmen. Cybersecurity stellt somit für viele Organisationen und Institutionen eine immense Mammutaufgabe dar.

Zusammengefasst durchleben wir sehr volatile Zeiten. Komplexität sowie Kritikalität der Angriffe nehmen in vielerlei Hinsicht zu. Das erhöht umso mehr den Bedarf an Sicherheitslösungen, die gleichermaßen effektiv, umfassend, ressourcenschonend und anwenderfreundlich sind.

it security: *Sie malen uns damit ein recht düsteres Bild für die Zukunft von IT-Sicherheit. Welchen Lösungsweg schlagen Sie als Sicherheitsexperte vor?*

IT-SICHERHEIT MUSS DAS SICHERE DIGITALE ARBEITEN ERMÖGLICHEN UND DARF DER DIGITALISIERUNG NICHT IM WEG STEHEN.

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

Arved Stackelberg: Nein, düster sehe ich die Zukunft überhaupt nicht. Im Gegenteil: Ich bin optimistisch, aber nicht naiv. Es gibt in der Cybersicherheit keine eierlegende Wollmilchsau, die im Alleingang alle Daten und Systeme zu 100 Prozent schützt. Daher setzen wir bei DriveLock ganz stark auf Zusammenarbeit. Unsere Vision ist es, europäische Best-of-Breed-Hersteller in unsere HYPERSECURE Platform zu integrieren, um gemeinsam eine Cybersicherheitsantwort für Europa zu haben. Ganz nach dem Motto: Sicherheit aus Deutschland und Europa für die Welt.

Aus unserer Perspektive ist es wichtig, dass Security-Anbieter den Konkurrenzgedanken zum Wohl der Kunden beiseitelegen und sich zusammentun, um eine Plattform-Allianz mit komplementären Lösungen zu bilden. An solch einer Plattform arbeiten wir gemeinsam mit anderen Security-Anbietern, damit Organisationen umfassende Lösungen erhalten, die den gesamten Lebenszyklus von Daten und Systemen lückenlos absichern und dabei ressourcenschonend sowie einfach zu bedienen sind. Erst wenn die Sicherheit ihrer Systeme und Daten in trockenen Tüchern ist, können sich Behörden, der deutsche Mittelstand und KRITIS-Unternehmen im großen Stil ihrer Digitalisierung zuwenden und ihre Position im internationalen Wettbewerb stärken.

IT-Sicherheit muss der Komplexität der Rahmenbedingungen zum Trotz einfach und schnell verfügbar sein. Sie soll das sichere digitale Arbeiten ermöglichen und darf der Digitalisierung nicht im Weg stehen. Das ist das gemeinsame Grundverständnis, das uns mit unseren Plattform-Partnern verbindet.

Wichtige Punkte in diesem Zusammenhang sind Vertrauen und digitale Souveränität: Beim Aufbau unserer Plattform arbeiten wir ausschließlich mit Partnern, deren Lösungen in Deutschland oder Europa entsprechend zertifiziert und damit qualitätsgeprüft sind. Lokale Lösungen sind elementar. Die geopolitischen Entwicklungen der letzten zwei Jahre haben verdeutlicht, dass die Unabhängigkeit vom EU-Ausland die wirtschaftliche Resilienz stärkt.

Daher setzen wir, als deutsches Unternehmen, bei unserer Plattform-Allianz auf lokale Partner aus Deutschland und der EU, um die digitale Souveränität und digitale Resilienz in Europa zu fördern.

it security: *Welchen Lösungs-Bereich deckt DriveLock in dieser Security-Allianz ab?*

Arved Stackelberg: Unsere HYPERSECURE Platform ist wie eine schlagkräftige Counter-Force aus spezialisierten Abwehrkräften, die in ihrer jeweiligen Disziplin zu den Besten zählen. Die Kombination der verschiedenen Elemente – von Endpoint Protection über Verschlüsselung bis hin zu Security Awareness – schafft Synergien, sodass Cyberattacken dort bleiben, wo sie hingehören: außen vor.

Damit bieten wir Organisationen mehrschichtige Sicherheit nach dem Zero-Trust-Prinzip. Die Lösung ist Cloud-basiert und somit sofort verfügbar mit niedrigen Investitions- und Betriebskosten. So können auch Organisationen, die keine großen Budgets haben oder unter dem Fachkräftemangel in der IT-Sicherheit leiden, mit ihren verfügbaren Ressourcen ganz einfach effektive Cybersecurity umsetzen. Zudem sind die DriveLock-Lösungen Device Control und Application Control nach Common Criteria EAL3+ zertifiziert. Diese international anerkannte Zertifizierung in Kombination mit der Entwicklung und dem technischen Support unserer Lösungen aus Deutschland helfen Unternehmen dabei, gesetzliche und sonstige (Compliance-)Vorgaben einzuhalten.

it security: *Das klingt vielsprechend. Können Sie uns weitere deutsche Security-Anbieter nennen, die dieser Plattform-Allianz beigetreten sind?*

Arved Stackelberg: Natürlich! Wir haben erst kürzlich eine strategische Partnerschaft mit Enginsight geschlossen, das seine SIEM-Software ebenfalls inhouse entwickelt. Das Unternehmen aus Jena teilt mit uns die Vision, dass Security-Lösungen speziell auf die Bedürfnisse von Mittelstand, Behörden und KRITIS-Unternehmen zugeschnitten sein sollten für hohen Cyberschutz und langfristige digitale Souveränität in Deutschland und Europa. Diese Partnerschaft ermöglicht es Kunden unserer Unternehmen, ihre Sicherheitsstrategien zu stärken und auf Herausforderungen proaktiv zu reagieren. Dadurch verbessern sie ihre Widerstandsfähigkeit gegenüber Cyberbedrohungen nachhaltig und können anspruchsvolle Sicherheitsstandards wie NIS2, TISAX, ISO27001 und den BSI-Grundschutz erheblich leichter einhalten.

Dieses Jahr werden weitere Partner unserer Plattform-Allianz beitreten. Wir setzen sehr hohe Maßstäbe an uns selbst und an unsere Technologie-Partner, um unserem Anspruch – Unternehmen und Organisationen jeder Größe eine hocheffiziente, umfassende und ressourcenschonende Cybersecurity-Plattform bereitzustellen – gerecht zu werden.

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

Tick, tack – die Zeit wird knapp

NIS2-VORBEREITUNGEN

Die Network and Information Systems Directive 2 (NIS2) der europäischen Union soll bis 17. Oktober dieses Jahres in nationales Recht umgesetzt werden. Aktuell ist der deutsche Gesetzgebungsprozess noch immer in der Phase des Referentenentwurfs. Somit fehlt es betroffenen Organisationen wenige Monate vor Ablauf der Frist immer noch an Orientierung und konkreten Anforderungen, um sich umfassend vorzubereiten. Zudem wird die Umsetzung des kommenden Gesetzes für zahlreiche Unternehmen Neuland: Denn angesichts der steigenden Cyberbedrohungen fallen auch Einrichtungen unter NIS2, die zuvor nicht zu den kritischen Sektoren gehörten und somit keine rechtlich vorgegebenen Sicherheitsvorschriften dieser Art erfüllen mussten. Die Verzögerung beim Gesetzesentwurf stellt sie vor die Herausforderung, sich weitgehend „im Blindflug" auf die neue Regelung einzustellen und vorzubereiten.

Welche Informationen zu NIS2 liegen aktuell vor?

Die EU reagiert mit der NIS2-Richtlinie auf die wachsenden Bedrohungen im Cyberspace – sei es durch technologische Innovationen bei den Angriffsmethoden oder neuen Zielen und Vorgehensweisen als Folge von geopolitischen Entwicklungen. NIS2 dient dazu, ein einheitliches und hohes Niveau an Cybersicherheit in der gesamten EU zu etablieren und somit die Cyberresilienz und -souveränität der Union zu fördern.

Konkret sind Unternehmen und Organisationen betroffen, die

- mehr als 50 Mitarbeitende haben,
- über 10 Millionen EURO Umsatz machen oder
- von der Regierung als kritische Organisation eingestuft werden.

Diese Definition umfasst fast 40.000 Organisationen in 18 Sektoren in Deutschland, die von B2B-IT-Dienstleistern bis hin zur Trinkwasserversorgung, Lebensmittelverarbeitung oder Forschung reichen und in die Kategorien wichtige bzw. wesentliche Einrichtungen eingeordnet werden – zudem kann es Sonderfälle bei besonderer Kritikalität geben. Die Pflichten und Sanktionen variieren je nach Größe und Leistungsfähigkeit. Ähnlich wie bei der Datenschutzgrundverordnung gibt es auch hier Meldepflichten bei Verstößen: innerhalb von 24 Stunden, 72 Stunden sowie einen Monat nach Kenntniserlangung. Die Meldungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) müssen die Ursache, den Schweregrad, die gegebenenfalls grenzüberschreitenden Auswirkungen sowie die ergriffenen Maßnahmen aufführen.

Außerdem werden Personen aus der Geschäftsführung oder Chief Information Security Officer zur Verantwortung gezogen. Sie müssen regelmäßig an Cybersicherheits-Schulungen teilnehmen und sind verpflichtet, die Einhaltung und Durchführung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit (Artikel 21) zu überwachen. Das Ziel ist es, Sicherheitsvorfälle zu verhindern oder ihre Auswirkungen zu minimieren. Dazu lassen sich die Maßnahmen grob in zwei Kategorien unterteilen:

#1 Die Gefahrenanalyse stellt den ersten Schritt dar und umfasst die vollständige Bestandsanalyse physischer und digitaler Gefahrenquellen – von Brand oder Diebstahl bis hin zu Zero Day Exploits oder Phishing Mails. Eine solide Analyse muss den Stand der Technik berücksichtigen. Da sich Technologien jedoch kontinuierlich weiterentwickeln, sind laufende Evaluierungen unumgänglich.

#2 Der zweite Teil beinhaltet Lösungen und Konzepte, die Sicherheitsvorfälle verhindern oder deren Auswirkungen minimieren. Bei deren Umsetzung müssen die betroffenen Organisa-

tionen zudem die Verhältnismäßigkeit der Maßnahmen ermitteln anhand des Ausmaßes der Risikoexposition, der Größe der Einrichtung und der Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen sowie der Schwere möglicher Auswirkungen für Wirtschaft und Gesellschaft. Auch sollen Einrichtungen bei der Wahl ihrer Lösungen den aktuellen Stand der Technik und, sofern möglich, europäische oder internationale Normen (z. B. ISO 27001/2) berücksichtigen.

Zum Warten verurteilt?
Was Unternehmen jetzt hilft

Auch wenn es noch keinen spezifischen Gesetzesentwurf gibt, können betroffene Organisationen bereits jetzt schon nützliche Schritte für ein aktives Risikomanagement umsetzen.

In der Tabelle sind die im Artikel 21 erwähnten Risikomanagementmaßnahmen gelistet und auf entsprechende kritische Security Controls gemappt, um einen ersten Überblick zu erhalten.

Die genannten kritischen Security Controls sind Bestandteil bewährter Regelungen und Standards, an denen sich betroffene Einrichtungen orientieren können, um optimal vorbereitet zu sein. Einige Beispiele dafür sind:

- IT-Grundschutz des BSI
- BSI-Gesetz
- Cybersecurity Framework von NIST (National Institute of Standards and Technology)
- CIS Critical Security Controls

Entsprechende Security Controls stehen sowohl einzeln oder in gebündelter Form über Plattformlösungen zur Verfügung. Organisationen mit geringen Ressourcen erhalten mit einer Cloud-basierten Security-Plattform mehrschichtige Cybersicherheit, die sofort verfügbar, wirtschaftlich effizient und mit niedrigen Investitions- und Betriebskosten verbunden ist. Vor allem öffentliche Einrichtungen oder Unternehmen aus dem Klein- und Mittelstand können so mit minimalem Aufwand ganz einfach und schnell ein hohes Sicherheitsniveau realisieren und gleichzeitig gesetzliche Anforderungen erfüllen. Bei der Wahl sollten Organisationen auch darauf achten, ob der Security-Anbieter bereits wichtige Zertifizierungen erfüllt. Beispielsweise sind die DriveLock-Lösungen Device Control und Application Control nach Common Criteria EAL3+ zertifiziert. DriveLock bietet Kunden bereits heute eine Vielzahl dieser Security Controls, die dazu beitragen, die Integrität, Verfügbarkeit und Vertraulichkeit von Systemen und Daten zu gewährleisten.

Fazit

Organisationen müssen nicht erst auf einen konkreten Gesetzesentwurf zur NIS2-Richtlinie warten, um sich darauf vorzubereiten. Sie können bereits jetzt mithilfe vorhandener Modelle und Best Practices ihre Cybersicherheit stärken und aktuelle sowie kommende Richtlinien einhalten.

www.drivelock.com

NIS-2 MASSNAHME	KATEGORIE ODER TOOL
Konzepte für Risikoanalyse und Informationssicherheit	**Sicherheitsrichtlinien / Inventory**
Bewältigung von Sicherheitsvorfällen	**Incident Management**
Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen	**Prevention & Detect**
Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	**Disaster Recovery & Business Continuity**
Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern	**Supply Chain / API / Endpoint Protection**
Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung	**Zero Trust Security / Application Control / Device Control**
Konzepte und Verfahren für den Einsatz von Kryptografie und ggfs. Verschlüsselung	**Data Loss Prevention / Verschlüsselung**
Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit	**Security Awareness**
Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen	**Access Control**
Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	**Risk & Compliance**

EINSTIEG IN ETHICAL HACKING

PENETRATION TESTING UND HACKING-TOOLS FÜR DIE IT-SECURITY

Dieses Buch richtet sich an IT-Sicherheitsexperten und alle, die es werden wollen. Um die Systeme von Unternehmen vor Cyberangriffen zu schützen, müssen Sie wie ein Angreifer denken. Spüren Sie Sicherheitslücken in Webanwendungen und Netzwerken auf, hacken Sie Passwörter und nutzen das schwächste Glied in der Sicherheitskette, um in Systeme einzudringen: den Menschen.

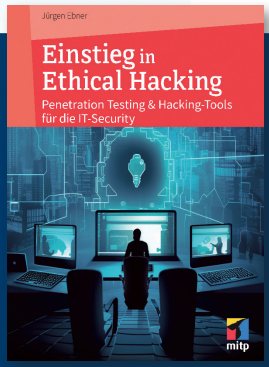
Penetration Testing mit Kali Linux

Richten Sie eine sichere Testumgebung mit Kali Linux ein und lernen Sie die Bandbreite der mitgelieferten installierbaren Hacking-Tools kennen: OpenVAS, Medusa, Metasploit, John the Ripper, Armitage, Netcat und viele mehr.

Lernen Sie, wie ein professioneller Penetration Test abläuft und welche Richtlinien eingehalten werden müssen, um Ihre Auftraggeber zufriedenzustellen und legal sowie ethisch zu hacken.

Aus dem Inhalt:

- Hacking Labor einrichten
- Linux-Grundlagen
- Einführung in Kali-Linux
- Port- und Schwachstellen-Scan
- Passwörter hacken
- Netzwerkverkehr ausspähen
- Active-Directory-Hacking
- Webhacking
- Social Engineering



Einstieg in Ethical Hacking: Penetration Testing und Hacking-Tools für die IT-Security

Jürgen Ebner (Autor), mitp Verlags GmbH & Co.KG; 03-2024

SICHER & EFFIZIENT

Unternehmen sind von der Zuverlässigkeit ihrer Technologie abhängig, daher steht die Sicherheit der Systeme und Daten an vorderster Front.

Schwachstellen in Software und Systemen werden schnell von Hackern ausgenutzt, um Daten zu stehlen, das System zu beschädigen oder das Unternehmen handlungsunfähig zu machen. Die Vielzahl an Bedrohungen und die ständig wachsende Komplexität von IT-Infrastrukturen erfordern einen proaktiven Ansatz und eine ständige Wachsamkeit.
In diesem Kontext gewinnt das Vulnerability Management, also das Schwachstellenmanagement, als eine effiziente Sicherheitsstrategie immer mehr an Bedeutung.

Das Konzept des risikobasierten Schwachstellenmanagements zielt darauf ab, Ressourcen dort einzusetzen, wo sie am dringendsten benötigt werden. Statt sich auf die Behebung jeder einzelnen Schwachstelle zu konzentrieren, werden die Schwachstellen priorisiert und nach ihrem potenziellen Risiko für das Unternehmen bewertet. Auf diese Weise können Unternehmen ihre begrenzten Ressourcen optimal nutzen und sich gezielt gegen diejenigen Schwachstellen verteidigen, die das größte Risiko für ihre Geschäftsprozesse darstellen.

Vulnerability Management

RISIKOBASIERTES SCHWACHSTELLENMANAGEMENT ALS EFFIZIENTE SICHERHEITSSTRATEGIE

Auch das stärkste IT-System ist nur so stark wie seine schwächste Sicherheitslücke. Bedauerlicherweise nimmt die Anzahl solcher Lücken stetig zu – in den letzten zehn Jahren hat sich diese sogar mehr als verdreifacht. Die Praxis zeigt uns, dass viele Unternehmen erst dann auf potenzielle Einfallstore in ihren IT-Systemen aufmerksam werden, wenn es bereits zu spät ist und diese schon ausgenutzt wurden. Solche Nachlässigkeiten haben oft kostspielige Auswirkungen und führen im schlimmsten Fall zu langfristigen Schäden, die sich nur schwer reparieren lassen. Die Frage lautet also: Wie können IT-Verantwortliche die Schwachstellen ihrer Systeme rechtzeitig erkennen und beseitigen? Und was genau unterscheidet eine Bedrohung von einer Schwachstelle und einem Risiko?

Schwachstellen aufdecken, einschätzen und eliminieren

Schwachstellenmanagement, auch als Vulnerability Management bekannt, bezeichnet den kontinuierlichen Prozess der Identifizierung, Kategorisierung und Behebung von IT-Sicherheitslücken. Es ist ein wesentlicher Bestandteil der Sicherheitsarchitektur jedes Unternehmens, da die frühzeitige Erkennung und Behebung von Schwachstellen Datenverlust, Betriebsstörungen und Reputationsschäden abwenden kann.

Für ein effektives Vulnerability Management müssen Unternehmen zunächst eine klare Unterscheidung zwischen Bedrohung, Schwachstelle und Risiko treffen. Eine Bedrohung im IT-Kontext ist alles, was ein Asset beschädigen oder zerstören oder das digitale System negativ beeinflussen kann. Eine Schwachstelle ist eine spezifische Schwäche oder Lücke in einem Programm, System oder Prozess, die ein Angreifer ausnutzen kann, um in die Infrastruktur einzudringen. Ein Risiko ist die Wahrscheinlichkeit oder das Ausmaß des potenziellen Schadens, der durch die Ausnutzung einer Schwachstelle entstehen kann.

Ein Risiko ergibt sich aus der Kombination von Bedrohungen und Schwachstellen. Da es nahezu unmöglich ist, jede Lücke in einer IT-Umgebung zu beseitigen, müssen IT-Sicherheitsbeauftragte Prioritäten setzen. Die wichtigste Frage, die sich dazu stellt, lautet: „Welche Schwachstellen sind besonders riskant und sollten daher vorrangig beseitigt werden?" Ein solches risikobasiertes Vulnerability Management ist Teil einer proaktiven Cybersicherheitsstrategie, die darauf abzielt, Schwachstellen auf Basis ihres individuellen Risikopotenzials zu bewerten und die Bedrohungen zuerst anzugehen, die am dringendsten zu beheben sind. Denn kein Unternehmen

72 %
DER KMU GEBEN DER VERBESSERUNG IHRER SICHERHEITSMASSNAHMEN OBERSTE PRIORITÄT

EIN RISIKOBASIERTES VULNERABILITY MANAGEMENT IST TEIL EINER PROAKTIVEN CYBERSICHERHEITSSTRATEGIE, DIE DARAUF ABZIELT, SCHWACHSTELLEN AUF BASIS IHRES INDIVIDUELLEN RISIKOPOTENZIALS ZU BEWERTEN UND DIE BEDROHUNGEN ZUERST ANZUGEHEN, DIE AM DRINGENDSTEN ZU BEHEBEN SIND.

André Schindler, General Manager EMEA, NinjaOne, www.ninjaone.de

kann zu jeder Zeit sicherstellen, dass sämtliche Einfallstore zuverlässig versiegelt sind.

Die vier Schritte des Schwachstellenmanagements

Im Rahmen des Vulnerability Managements besteht das Ziel darin, Kontrolle über die Anfälligkeiten eines IT-Systems zu gewinnen. Dies erreichen die verantwortlichen Teams durch die Anwendung etablierter Best Practices. Doch dabei handelt es sich nicht um ein einmaliges Event, sondern um einen laufenden Prozess, der Sicherheitslücken identifiziert und bewertet, um dann Maßnahmen zur Risikominderung einzuleiten. Dieser umfasst die folgenden vier Schritte:

#1 Lokalisierung und Identifikation: Zuerst müssen alle Schwachstellen in der IT-Umgebung festgestellt werden. Dabei sind Fragen zu klären wie: Welche Art von Sicherheitslücke liegt vor? Wo befindet sie sich? Hier können spezielle Tools und Techniken zum Einsatz kommen, wie zum Beispiel Penetrationstests, Schwachstellenscanner und Codeüberprüfungen.

#2 Bewertung: Die Risikobewertung entscheidet über die Priorisierung. Für jede identifizierte Schwachstelle wird das Worst-Case-Szenario bestimmt, das auf das Unternehmen zukommen könnte, wenn diese durch einen Angreifer ausgenutzt wird. Auf Grundlage dieser Szenarien können die identifizierten Schwachstellen kategorisiert und priorisiert werden. Eine geeignete IT-Dokumentationssoftware hilft dabei, die gewonnenen Informationen zu dokumentieren, um später wieder darauf zurückgreifen zu können und möglicherweise auch im Verlauf noch wichtige Erkenntnisse zu gewinnen.

#3 Überwachung und Bekämpfung: Dieser Teil des Prozesses erfolgt kontinuierlich, denn auch neu auftretende Sicherheitslücken müssen entdeckt werden – und zwar durch proaktive Überwachung. Die Schwachstellen mit der höchsten Priorität werden zuerst beseitigt. Je nach Art der Sicherheitslücke können unterschiedliche Maßnahmen erforderlich sein, zum Beispiel ein Geräteneustart, die Installation eines Patches oder die Einrichtung eines Workarounds, bis eine Lösung verfügbar ist.

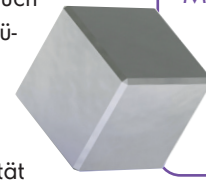
#4 Überprüfung und Bestätigung: Vertrauen ist gut, Kontrolle ist besser. Aus diesem Grund besteht der letzte Schritt im Vulnerability Management darin, zu überprüfen, ob die durchgeführten Maßnahmen erfolgreich waren und die identifizierten Schwachstellen tatsächlich behoben wurden. Dies kann durch erneute Scans, Tests und Audits erfolgen. Diese Phase dient auch dazu, Compliance-Anforderungen zu erfüllen und zu dokumentieren, dass das Unternehmen seine Sorgfaltspflicht in Bezug auf die IT-Sicherheit erfüllt hat.

Tools für das Schwachstellenmanagement: Vorzüge und Alternativen

Spezielle Vulnerability-Management-Lösungen bieten alle vier oben genannten Schritte in einem benutzerfreundlichen Paket an. Doch auch ohne diese ist es möglich, effektiv mit Schwachstellen umzugehen. Eine entsprechende Software – ob spezialisiert oder als Teil einer Unified-IT-Management-Plattform – sollte die folgenden Funktionen umfassen:

28 %

DER BEFRAGTEN FACHLEUTE BETONEN, WIE WICHTIG ES IST, DAS SCHWACHSTELLENMANAGEMENT UND DIE PATCH COMPLIANCE IM KOMMENDEN JAHR ZU VERBESSERN



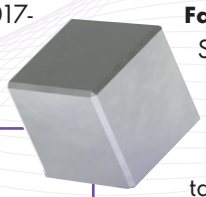
- **Abdeckung:** Die Stärke von Tools für das Schwachstellenmanagement liegt in ihrer Fähigkeit, eine breite Palette von Sicherheitslücken aufzudecken. Führende Lösungen bieten einen umfassenden Überblick über alle Schwachstellen in einer IT-Umgebung. Sie erleichtern die Risikobewertung und unterstützen bei der Implementierung geeigneter Schutzmaßnahmen und der Sicherung wichtiger digitaler Daten. Hier gilt: je mehr, desto besser.

- **Automatisierung:** Ein weiterer signifikanter Vorteil einiger Tools ist die Möglichkeit der Automatisierung vieler Aufgaben innerhalb des Vulnerability Managements. Das verantwortliche Team spart Zeit und Mühe, da die entsprechende Lösung regelmäßige und konsistente, automatisierte Überprüfungen auf Schwachstellen ermöglicht. Gerade in Zeiten des akuten Fachkräftemangels ist die Entlastung der IT-Teams ein wichtiger Faktor. Automatisierungen können außerdem bei der Behebung von Sicherheitslücken hilfreich sein, sie erleichtern Wartungsaufgaben und reduzieren aktiv Risikofaktoren.

- **Berichterstattung:** Reporting-Funktionen bieten einen transparenten Überblick über die aktuelle Sicherheitslage und erleichtern die Nachverfolgung von Verbesserungen. Sie ermöglichen es außerdem, den Status von Schwachstellen und die Wirksamkeit der Maßnahmen zur Risikominderung zu verfolgen. Berichte dienen darüber hinaus dazu, die Einhaltung gesetzlicher Anforderungen zu belegen und zu dokumentieren, dass ein Unternehmen die nötigen Schritte zur Verbesserung der IT-Sicherheit unternommen hat und sich Compliance-konform verhält.

Proaktives Schwachstellenmanagement

Common Vulnerabilities and Exposures (CVEs - zu deutsch: allgemeine Schwachstellen und Gefährdungen) spielen eine zentrale Rolle im Schwachstellenmanagement und gehören daher auf die Agenda eines jeden IT-Teams. Dabei handelt es sich um eine standardisierte Kennung, die einer bestimmten Schwachstelle zugewiesen wird und so zu einem eindeutigen Bezugspunkt wird. Fachleute für Cybersicherheit können CVEs verwenden, um Schwachstellen in verschiedenen Systemen und Plattformen zu diskutieren, mit anderen zu teilen und gemeinsam an Lösungen zu arbeiten. Als eindeutige Kennziffer bieten sie eine gemeinsame Basis und sorgen dafür, dass alle Beteiligten genau wissen, um welche Sicherheitslücke es im konkreten Fall geht. Einige CVEs erlangten bereits traurige Berühmtheit: Die berüchtigte CVE-2017-0144, auch bekannt als EternalBlue, deckte beispielsweise 2017 Schwachstellen im SMB-Protokoll von Microsoft auf, was zu dem weltweiten WannaCry-Ransomware-Angriff führte. CVE-2014-0160, der Heartbleed-Bug von 2014, betraf die kryptografische Softwarebibliothek OpenSSL.



26 %
DER FESTGESTELLTEN NEUEN SCHWACHSTELLEN WAREN KEINE VÖLLIG NEUEN BEDROHUNGEN

CVEs spielen eine Schlüsselrolle bei der proaktiven Identifizierung und Behebung von Schwachstellen, denn durch die Bereitstellung einer standardisierten Referenz können Cybersicherheitsprofis effizient kommunizieren, Informationen über Bedrohungen austauschen und gemeinsam an einer Lösung arbeiten – idealerweise bevor Schäden entstehen. Und auch im Falle eines akuten Cybersecurity-Vorfalls sind die Kennziffern unerlässlich: Sicherheitsteams können sie nutzen, um die Art der Sicherheitslücke zu verstehen, ihren Schweregrad einzuschätzen und gezielte Maßnahmen zu ergreifen. Beispiele wie die Datenpanne bei Equifax (CVE-2017-5638) und die Apache Struts-Schwachstelle zeigen immer wieder, wie die Ausnutzung bereits bekannter Einfallstore zu erheblichen Datenschutzverletzungen führen kann. Unternehmen müssen also stets auf dem aktuellsten Stand bleiben und die Vernetzung mit Gleichgesinnten kann dabei helfen, Angreifern einen Schritt voraus zu sein.

Fazit

Sicherheit in der digitalen Welt erfordert ständige Wachsamkeit. Während einige Cyberattacken unerwartet aus dem Nichts auftauchen und Unternehmen regelrecht überrollen, können IT-Teams anderen Angriffen durchaus vorbeugen, indem sie ihre Hausaufgaben gründlich machen. Ein proaktives, risikobasiertes Schwachstellenmanagement sollte dabei ganz oben auf der Agenda stehen. Die Umsetzung in der Praxis gelingt mit klar strukturierten Prozessen, professionell ausgestatteten Teams und durchdachten Hilfsmitteln an den richtigen Stellen. Mit diesem Handwerkszeug machen Unternehmen das Vulnerability Management für sich zu einer effektiven Methode, um sich vor Sicherheitsverletzungen zu schützen und das Risiko eines folgenschweren Cyberangriffs zu reduzieren.

André Schindler

Phi·shing

/'fɪʃɪŋ/

Substantiv, Neutrum [das]

englisch phishing, zu: fishing = das Fischen;
die ph-Schreibung als häufig gebrauchte Verfremdung im Hackerjargon für f wohl nach englisch-amerikanisch phreaking = das Hacken (zu: freak, Freak).

Beschaffung persönlicher Daten anderer Personen (Passwort, Kreditkartennummer o. Ä.) mit gefälschten E-Mails oder Websites.

Wettbewerbsvorteile nutzen!

HOHE RELEVANZ VON CYBERSICHERHEIT

Sophos veröffentlicht einen neuen, aktuellen Teil seiner Management-Studie „Chef, wie hältst du es mit der Cybersicherheit" für Deutschland, Österreich und die Schweiz. Die Studie ist eine Fortsetzung einer Befragungsreihe aus 2022 und wurde im ersten Quartal dieses Jahres erneut vom Marktforschungsinstitut Ipsos im Auftrag von Sophos durchgeführt.

Relevanz von Cyberschutz

Hinsichtlich der Frage, wie sie 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 in der überwiegenden Mehrzahl einig: In Deutschland halten Manager zu 55 Prozent Cyberschutz für sehr wichtig für die Business-Beziehungen, in Österreich sagen dies 46 Prozent und in der Schweiz betonen sogar 60 Prozent die Relevanz der implementierten Cybersicherheitsmaßnahmen.

Bedeutung hoch, tatsächlicher Einfluss niedrig?

Gleich bei der nächsten Frage zeigt sich aber eine Diskrepanz in der Bewertung durch die Chefs. Bezifferte die sehr deutliche Mehrheit den Einfluss eines effizienten Cyberschutzes auf Geschäftsbeziehungen als mindestens wichtig, zeichnet der Realitätscheck ein scheinbar anderes Bild. Auf die Frage, ob sich das Thema Cyberschutz tatsächlich auf der Ebene der Zusammenarbeit mit Kunden ausgewirkt habe, bestätigen knapp 35 Prozent der deutschen, 34 Prozent der österreichischen und 40 Prozent der Schweizer Umfrage-Teilnehmenden positiv, dass sie ohne wirkungsvollen Cyberschutz in der Tat Kunden verloren hätten. Die Mehrheit der Befragten dagegen sagt, die Cybermaßnahmen des eigenen Unternehmens seien weder in den Beziehungen zu Kunden noch in der Neukunden-Akquise bislang ein Thema gewesen. Lediglich in der Schweiz erweist sich dieser Aspekt somit als einigermaßen ausgeglichen.

Kein Wettbewerbsvorteil, keine Kommunikation

Noch deutlicher als beim Thema Auswirkungen auf Geschäftsbeziehungen zeigt sich hinsichtlich der aktiven Kommunikation der Cybersicherheitsinfrastruktur in Richtung Kunden und Geschäftspartner eine Diskrepanz. Nur insgesamt gut 29 Prozent der deutschen sowie 24 Prozent der österreichischen Unternehmen kommunizieren ihren Cyberschutz aktiv an Kunden und Geschäftspartner. In der Schweiz tun dies mit immerhin 40 Prozent deutlich mehr.

Wettbewerbsvorteile sehen und nutzen

„Ich bin überzeugt, dass viele Unternehmen, die eine wirksame, moderne Cybersicherheitsinfrastruktur im Einsatz haben und darüber nicht kommunizieren, Chancen ungenutzt lassen. Wer etwa vernetzte und intelligente Schutztechnologien verwendet, oder auch externe Expertise im Rahmen eines Cybersecurity as a Service-Modells (CSaaS) nutzt, hat entscheidende Elemente einer zeitgemäßen, proaktiven Sicherheitsstrategie implementiert. Dies kann angesichts der sich verschärfenden Bedrohungslage ein Wettbewerbsvorteil sein. Oder anders gesagt: Wer bei der Cybersicherheit gut aufgestellt ist, schafft Vertrauen für sich selbst und alle Partner. Darüber sollte man reden," sagt Michael Veit, Security Experte bei Sophos.

www.sophos.de

KOMMUNIZIEREN SIE IHRE CYBERSCHUTZ-SICHERHEITS-MASSNAHMEN AKTIV ALS WETTBEWERBSVORTEIL? (Deutschland)

66 %

NEIN,

der Cyberschutz verschafft uns keinen Wettbewerbsvorteil in der Zusammenarbeit der Kunden

29 %

JA,

wir kommunizieren unseren Cyberschutz und die sichere Zusammenarbeit bei Kunden aktiv

EIN SCHRITT HIN ZU MEHR SICHERHEIT

Die NIS2-Richtlinie („The Network and Information Security (NIS) Directive") ist am 16. Januar 2023 in Kraft getreten. Mit ihr wurden die Anforderungen an die Cybersicherheit für Unternehmen verschärft, denn sie erweitert die Cybersicherheitsanforderungen und auch die Sanktionen, um das Sicherheitsniveau der europäischen Mitgliedsstaaten zu verbessern und aufeinander abzustimmen.

Bis Oktober 2024 müssen die EU-Mitgliedstaaten die Richtlinie nun in nationales Recht überführen. Bis dato waren von der KRITIS-Gesetzgebung vorwiegend größere Institutionen betroffen, nun weitet sich die Richtlinie auch auf kleinere Organisationen aus. Damit wird das Thema Cybersicherheit zu einem Hauptthema in der Chefetage.
Mehr dazu in unserem Spezial.

NIS2-Compliance

LEITFADEN FÜR DIE EINHALTUNG

Um die Einhaltung der NIS2-Richtlinie sicherzustellen, ist es für Organisationen essentiell, ein tiefgreifendes Verständnis der erforderlichen Maßnahmen und Schritte zu entwickeln.

Die NIS2-Richtlinie zielt darauf ab, ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU zu gewährleisten. Im Folgenden finden Sie einen Leitfaden, um Ihre Organisation auf den Weg zur NIS2-Compliance zu führen.

#1 Verstehen der NIS2-Anforderungen

Zunächst ist es wichtig, die spezifischen Anforderungen der NIS2-Richtlinie zu verstehen. Dazu gehört die Kenntnis darüber, welche Arten von Organisationen betroffen sind, und die spezifischen Sicherheits- und Meldemaßnahmen, die implementiert werden müssen. Die Richtlinie erweitert den Anwendungsbereich auf mehr Sektoren und Typen von Diensten, was bedeutet, dass mehr Unternehmen als zuvor ihre IT-Sicherheitsmaßnahmen evaluieren und gegebenenfalls anpassen müssen.

#2 Risikobewertung und -management

Eine gründliche Risikobewertung ist der Grundstein für jede Sicherheitsstrategie. Identifizieren Sie die Risiken für Ihre IT-Systeme und Daten und bewerten Sie deren potenzielle Auswirkungen auf Ihre Organisation. Basierend auf dieser Bewertung sollten Sie ein Risikomanagementprogramm entwickeln, das darauf abzielt, diese Risiken zu mindern und die Resilienz Ihrer Systeme zu stärken.

#3 Technische und organisatorische Maßnahmen

Um den Anforderungen der NIS2-Richtlinie gerecht zu werden, müssen Organisationen angemessene technische und organisatorische Maßnahmen ergreifen. Dazu gehören die Sicherung von Netzwerken und Informationssystemen, der Schutz vor Cyberangriffen, die Gewährleistung der Datensicherheit und die Implementierung von Notfallplänen. Es ist wichtig, regelmäßige Überprüfungen und Aktualisierungen dieser Maßnahmen durchzuführen, um ihre Effektivität zu gewährleisten.

#4 Incident-Management und Meldewesen

Ein effektives Incident-Management-System ist für die Einhaltung der NIS2-Richtlinie unerlässlich. Organisationen müssen in der Lage sein, Sicherheitsvorfälle schnell zu erkennen, zu melden und darauf zu reagieren. Darüber hinaus erfordert die Richtlinie, dass bestimmte Arten von Sicherheitsvorfällen an die zuständigen nationalen Behörden gemeldet werden. Die Entwicklung eines robusten Incident-Response-Plans ist hierbei entscheidend.

#5 Bewusstsein und Schulung

Die Sensibilisierung und Schulung von Mitarbeitern spielen eine entscheidende Rolle bei der Sicherung von Netz- und Informationssystemen. Stellen Sie sicher, dass alle Mitarbeiter über die Risiken informiert sind und wissen, wie sie zur Sicherheit der Organisation beitragen können. Regelmäßige Schulungen und Awareness-Kampagnen können dabei helfen, eine Kultur der Cybersicherheit in Ihrer Organisation zu fördern

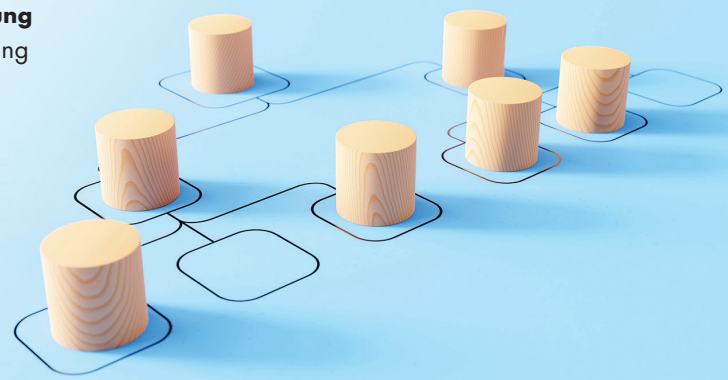
#6 Überprüfung und kontinuierliche Verbesserung

Die Einhaltung der NIS2-Richtlinie ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess. Technologien entwickeln sich weiter, und Cyberbedrohungen werden immer ausgefeilter. Daher ist es wichtig, die Sicherheitsmaßnahmen regelmäßig zu überprüfen und zu aktualisieren. Dies beinhaltet auch die Überprüfung der Compliance-Maßnahmen, um sicherzustellen, dass sie weiterhin den Anforderungen der Richtlinie entsprechen.

Fazit

Die Einhaltung der NIS2-Richtlinie erfordert eine umfassende Strategie, die Risikomanagement, technische und organisatorische Maßnahmen, Incident-Management, Mitarbeiterbewusstsein und kontinuierliche Verbesserung umfasst. Durch die Befolgung dieser Schritte können Organisationen nicht nur die Compliance sicherstellen, sondern auch ihre allgemeine Cybersicherheitsstruktur stärken.

Ulrich Parthier



Im Zeichen von NIS2

MIT ZERO TRUST- UND MIKROSEGMENTIERUNG GEGEN CYBERANGRIFFE

Cyberangriffe gehören zu den größten Bedrohungen für Unternehmen. In Deutschland bewegte sich die Zahl neuer Schadsoftware-Varianten, die für Cyberangriffe genutzt werden, im Jahr 2022 laut Bundesamt für Sicherheit in der Informationstechnik (BSI) im niedrigen dreistelligen Millionenbereich. 2016 war europaweit mit der ersten NIS-Richtlinie („Network and Information Security") eine gesetzliche Grundlage für den Schutz von bestimmten Netzwerken und Systemen vor Cyberangriffen geschaffen worden.

Seit Januar 2023 ist mit NIS2 die nächste, umfassendere Version in Kraft – mit einem deutlich größeren Kreis betroffener Unternehmen und Branchen. Das heißt: Ab Herbst 2024, wenn das deutsche Umsetzungsgesetz in Kraft tritt, gelten strengere Anforderungen an Sicherheitsvorkehrungen. Erklärtes Ziel ist die Stärkung der Resilienz kritischer Infrastrukturen in der EU.

Netzwerktransparenz sichern

Wie lassen sich unter diesen neuen Umständen Angriffe abwehren, Transparenz in das Netzwerk bringen und Compliance gewährleisten? Das gelingt durch die Umkehr von einem negativen in ein positives Sicherheitsmodell. Diesen Ansatz hat Akamai als einer der weltweit größten Anbieter für die Bereitstellung, Beschleunigung und Cyberschutz von Online-Anwendungen und -Inhalten in seinem „Zero Trust"-Sicherheitskonzept realisiert.

Grundannahme ist, dass alle Nutzer und Geräte schädlich sein könnten. Das bedeutet: Sie müssen als legitim verifiziert werden. Konkrete Sicherheitslösungen müssen sämtliche Signale für den Fall identifizieren können, dass ein Nutzer untypisch handelt, oder sich Anomalien zeigen. Das erschwert es Hackern mit Hilfe von Schadsoftware Schwachstellen auszunutzen.

Zero-Trust-Modell braucht Mikrosegmentierung

Das Zero-Trust-Modell sollte durch die Aufteilung des Netzwerks in separate Bereiche – die Mikrosegmentierung – ergänzt werden. Sie verhindert die ungebremste und unerwünschte Ausbreitung von Schadsoftware. Als unverzichtbares Workflow-Tool unterstützt die Mikrosegmentierung die Unternehmen bei der Anwendung der Zero-Trust-Netzwerkprinzipien maßgeblich.

Fit für das nächste Audit

Mithilfe von Akamai Guardicore Segmentation lassen sich Abhängigkeiten zwischen Ressourcen grafisch zuordnen – unerlässlich für die Gruppierung von Mikroperimetern und Erstellung genauer Richtlinien. Protokolle erfassen sämtliche Transaktionen in Echtzeit im Verlauf. So ermöglichen sie eine kontinuierliche Validierung und sorgen dafür, dass Unsicherheiten und Risiken umfassend eliminiert werden.

Hierfür sammelt Akamai Guardicore Segmentation Informationen über die IT-Infrastruktur und generiert eine dynamische Karte, mit der Sicherheitsteams alle relevanten Aktivitäten in Echtzeit einsehen können. In Kombination mit KI-basierten Sicherheitsrichtlinien-Workflows ermöglichen diese Einblicke die Erstellung von Segmentierungsrichtlinien für einzelne IT-Assets. Die Akamai Guardicore Segmentation bietet zudem mehrere Methoden, um Schadsoftware zu erkennen und zu blockieren, darunter eine Threat Intelligence Firewall, Reputationsanalyse sowie einen Service zur Auffindung von Schwachstellen, Anomalien und Data Breaches.

Akamai selbst nutzt diese Lösung für Compliance-Audits – mit Erfolg. Seit 2017 ist das Unternehmen in der Kategorie ‚Content Delivery Network' beim BSI gelistet. Dabei muss das Unternehmen in externen Audits nachweisen, dass es Technik auf dem neuesten Stand für die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der kritischen Systeme vorhält.

Philipp Merth | www.akamai.de

„Cybersecurity wird Chefsache“

RISIKOMANAGEMENT IM FOKUS

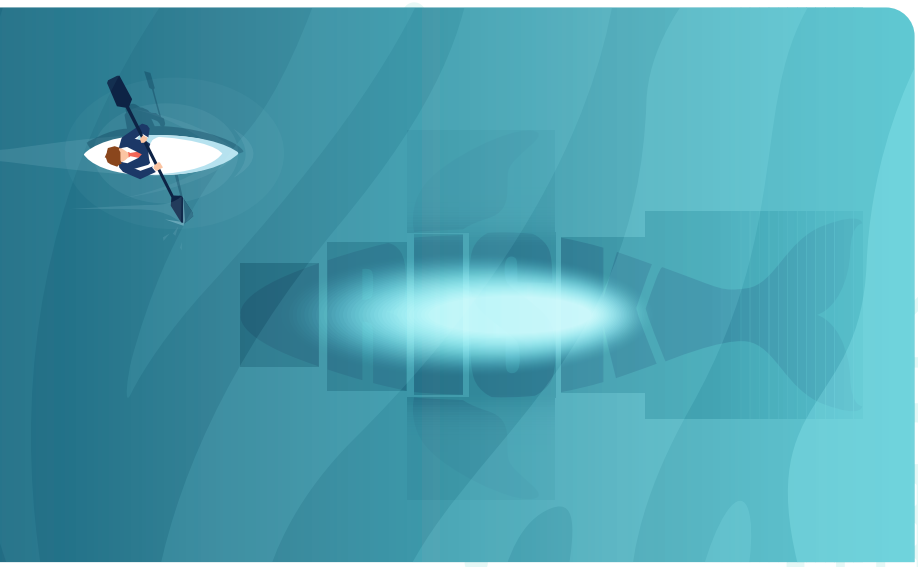
Mit Inkrafttreten der EU-Richtlinie NIS2 und Verabschiedung des nationalen Rechtes bis Oktober 2024 sind in Deutschland 15-mal mehr Unternehmen als bisher zu umfassenden Informationssicherheits-Maßnahmen verpflichtet. Was als erstes zu tun ist und warum auch diejenigen Unternehmen reagieren sollten, die gar nicht unter die Richtlinie fallen, erklärt Cybersecurity-Experte Florian Goldenstein im Interview.

it security: *Herr Goldenstein, Sie beraten Unternehmen rund um die Cyber-Sicherheit. Welchen Stellenwert nimmt NIS2 im Moment ein?*

Florian Goldenstein: Bei ungefähr der Hälfte aller Anfragen, die wir im Moment bekommen, geht es um NIS2. Das Thema steht bei vielen ganz oben auf der Agenda, und das ist auch gut so. Denn statt der rund 2.000 KRITIS-Unternehmen müssen ab Oktober 2024 fast 30.000 Unternehmen vernünftige Maßnahmen für Informationssicherheit nachweisen. Auch die, die bisher einen Bogen gemacht haben.

it security: *Welche neuen Pflichten ergeben sich durch NIS2?*

Florian Goldenstein: Alle Unternehmen in Deutschland, die unter NIS2 fallen, müssen sich binnen drei Monaten beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als zuständige Aufsichtsbehörde registrieren. „Erhebliche Sicherheitsvorfälle“ müssen die Unternehmen außerdem in Zukunft innerhalb von 24 Stunden sogar an Feiertagen an das BSI melden. Als erheblich gilt dabei alles, was eine Bedrohung oder einen finanziellen Schaden nach sich ziehen kann. Die Geschäftsleitung wird dazu verpflichtet, sich regelmäßig zu Cybersicherheit und Risikomanagement schulen zu lassen. Sie ist in Zukunft ganz klar dafür verantwortlich, dass alle Mindestanforderungen erfüllt sind. Mit NIS2 wird Cybersecurity damit zur Chefsache.



it security: *War das bisher noch nicht der Fall?*

Florian Goldenstein: Die neue Richtlinie sieht vor, dass die Organe der Geschäftsleitung bei Pflichtverletzungen in Haftung genommen werden können. Es wird also in Zukunft nicht mehr möglich sein, Sicherheitsvorfälle oder nur mangelnde Vorkehrungen unter den Teppich zu kehren. Und die vorgesehenen Strafen für Unternehmen sind empfindlich: bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes bei wesentlichen Einrichtungen. Deshalb empfehle ich dringend, jetzt die nötigen Hausaufgaben zu erledigen.

it security: *Und was steht da ganz oben auf der To-Do-Liste?*

Florian Goldenstein: Jedes Unternehmen, das unter die neue Richtlinie fällt – egal ob Konzern oder mittleres Unternehmen– sollte sich dringend mit dem Risikomanagement auseinandersetzen. Einerseits ist das der Kern von NIS2. Andererseits kann ich nur dann die technischen und organisatorischen Voraussetzungen für eine hohe Informationssicherheit schaffen, wenn ich auch die Schwachpunkte kenne. An welchen Stellen haben Dritte Zugriff auf mein Netzwerk? Wurde der Graben um meine sichere Zone tief genug gezogen? Für wen lasse ich die Zugbrücke herunter? Und was muss auf dem Ausweis stehen, damit jemanden durchs Tor kommt? Auch kleine Schritte in Richtung Resilienz sind wichtig. Nur reicht es nicht mehr zu sagen: „Cyber-Risiko interessiert mich nicht, die letzten 30 Jahre hat alles funktioniert und wird es auch die nächsten 30 Jahre.“

it security: *Was beinhaltet ein gutes Risikomanagement nach NIS2?*

Florian Goldenstein: Da geht es zunächst um ganz grundlegende Dinge wie Risikoanalyse, Bewertung und Festlegung von Maßnahmen. Zu den organisatorischen Anforderungen aus der NIS2 Richtlinie gehören zum Beispiel die Lieferkettensicherheit, Backup- und Notfallmanagement, Awareness und Cyberhygiene sowie die Sicherheit bei Erwerb, Entwicklung und Wartung von IT. Das Zauberwort hier heißt übrigens Wartung: Veraltete IT-Systeme verstoßen zukünftig gegen NIS2! Die technischen Anforderungen reichen von Kryptografie über Personal- und Zugriffskontrollen bis hin zu Multifaktor-Authentifizierung. Der Faktor Mensch spielt dabei eine große Rolle – wer „p@sswort" als Passwort verwendet und auf Links in Phishing-Mails klickt, muss besser geschult werden.

it security: *Aber für die Unternehmen, die nicht unter NIS2 fallen, ist das alles weiterhin kein Thema?*

Florian Goldenstein: NIS2 wird auch Konsequenzen für Unternehmen haben, die eigentlich nicht unter die Regelung fallen. Denn oft sind es Zulieferbetriebe für betroffene Unternehmen – und die wiederum müssen laut Gesetz die Sicherheit ihrer Lieferkette sicherstellen. Also ist es sehr wahrscheinlich, dass sie ähnlich wirksame Cybersecurity-Maßnahmen auch bei ihren Geschäftspartnern erwarten. Ansonsten könnte eine jahrelange Zusammenarbeit im Extremfall abrupt enden.

it security: *Bereits ab Oktober soll das nationale Recht gelten. Ist Panik angesagt?*

Florian Goldenstein: Wilder Aktionismus bringt niemandem etwas. Aber Abwarten und Nichtstun ist ebenfalls keine Option. Denn obwohl die Richtlinie noch nicht in nationales Recht überführt wurde und die Politik immer noch an Details arbeitet: NIS2 wird sicher kommen. Das bedeutet nicht, dass zum Oktober überall die gesamte Organisation eines Unternehmens umgekrempelt sein muss. Wer jetzt beginnt, am Risikomanagement zu arbeiten – zum Beispiel durch die Festlegung von Maßnahmen zur Risikominderung – bereitet sich auf jeden Fall gut vor.

ES WIRD IN ZUKUNFT NICHT MEHR MÖGLICH SEIN, SICHERHEITSVORFÄLLE ODER NUR MANGELNDE VORKEHRUNGEN UNTER DEN TEPPICH ZU KEHREN.

Florian Goldenstein, Head of IT-Security & CISO, Konica Minolta Business Solutions Deutschland GmbH, www.konicaminolta.de

it security: *Zusätzlich zum Zeitdruck bereitet der Personalmangel vielen Unternehmen Probleme. Was ist Ihr Rat?*

Florian Goldenstein: Es muss nicht immer das eigene Team sein, das sämtliche Aufgaben inhouse bewältigt. Mit Know-how, Kapazitäten und Technologie von außen können auch kleine und mittelständische Unternehmen in kurzer Zeit fit für NIS2 werden – auch ohne riesige Security- und Compliance-Abteilung. Unser Team hat für jede der genannten Mindestanforderungen eine Lösung im Portfolio. Wir unterstützen zum Beispiel mit Workshops zur Risikoanalyse, bei der Einführung eines ISMS oder bei Sicherheitschecks. Außerdem planen wir gemeinsam mit unseren Kunden IT-Projekte und bieten Managed Services zur Entlastung der IT-Abteilungen an.

it security: *Warum braucht Europa überhaupt eine weitere Cybersicherheits-Richtlinie?*

Florian Goldenstein: Brauchbare gesetzliche Vorschriften zur IT-Sicherheit gibt es noch gar nicht so lange. Nach dem Hacker-Angriff auf den Deutschen Bundestag 2015 wurde relativ kurzfristig das IT-Sicherheits-Gesetz verabschiedet, ein Jahr später hat die EU die erste NIS-Richtlinie erlassen. Das steht für die „Sicherheit von Netz- und Informationssystemen". Es folgten die KRITIS-Verordnung sowie mehrere Änderungen in den folgenden Jahren. Was aber bisher fehlte, sind einheitliche Regelungen für alle Unternehmen, die im Krisenfall weiterarbeiten müssen, die Verankerung der Verantwortung bei der Geschäftsleitung und verbindliche Pflichten. NIS2 beinhaltet das alles. Warum das wichtig ist, zeigt die Statistik: 58 Prozent der Unternehmen in Deutschland wurden 2023 Opfer von Cyberkriminalität – und 100 Prozent der befragten österreichischen Unternehmen haben im selben Jahr Cyberangriffe verzeichnet.

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

Von KRITIS zu NIS2

SO ÄNDERT SICH DIE SECURITY-PRAXIS KRITISCHER INFRASTRUKTUREN

Über 205 Milliarden Euro Schaden durch Cyberangriffe allein im vergangenen Jahr zeigen die Notwendigkeit einer robusten Cybersecurity-Strategie. Die NIS2-Richtlinie der EU weitet die Anforderungen für Unternehmen stark aus.

Laut dem Wirtschaftsschutzbericht 2023 des Digitalverbandes Bitkom entstand in diesem Jahr in Deutschland durch Cyberkriminalität ein Schaden von mehr als 205 Milliarden Euro. Die Experten erkennen zudem eine Professionalisierung: Sechs von zehn Cyberangriffen stammen aus der organisierten Kriminalität, eine Verdopplung seit 2021. Die Angriffe richten sich immer häufiger auf KRITIS-Unternehmen. Hier verzeichnet der Bitkom den größten Anstieg.

DIE UMSETZUNG DER NIS2-RICHTLINIE ERFORDERT VON DEN BETROFFENEN UNTERNEHMEN EINE SORGFÄLTIGE PLANUNG.

Daniel Graßer, Senior Director of Security Services, plusserver GmbH, www.plusserver.com

Diese Unternehmen aus kritischen Infrastrukturen erbringen wichtige Dienstleistungen zur Versorgung der Allgemeinheit. Ein Ausfall würde zu erheblichen Versorgungsengpässen, Gefährdung der öffentlichen Sicherheit und ähnlichen Folgen führen. Deshalb gelten für sie besondere Anforderungen an eine möglichst sichere und zuverlässige Abwehr von Cyberangriffen.

Die bisherige Definition der KRITIS-Unternehmen ist vergleichsweise eng, längst nicht alle Unternehmen eines Sektors zählen dazu. Experten gehen von etwa 1.700 KRITIS-Unternehmen in Deutschland aus. Im Herbst 2024 wird sich die Zahl der Unternehmen mit besonderen Anforderungen an Cybersecurity jedoch erhöhen, und zwar auf etwa 29.000. Der Grund ist die NIS2-Richtlinie (Network and Information Security Directive 2) der Europäischen Union, die ab Oktober auch in Deutschland gelten soll.

Hier gibt es allerdings noch eine Hürde: Der Gesetzgeber muss seine Hausaufgaben erledigen und bis spätestens Oktober 2024 ein NIS2-Umsetzungsgesetz beschließen. Leider ist im Moment nicht absehbar, ob es das Gesetz durch alle Institutionen schafft und nicht wie das Online-Zugangsgesetz in letzter Sekunde im Bundesrat scheitert. Trotzdem sollten Unternehmen in bestimmten Sektoren davon ausgehen, dass die Richtlinie früher oder später für sie gilt – und sich entsprechend vorbereiten.

Für diese Branchen gilt die NIS2-Richtlinie

NIS2 ersetzt den eingeführten Begriff KRITIS-Unternehmen durch eine deutlich erweiterte Zweiteilung: die „wichtigen Einrichtungen" und die „besonders wichtigen (wesentlichen) Einrichtungen". Letztere besitzen zudem eine Untergruppe der „kritischen Anlagen", zu denen die bisherigen KRITIS-Unternehmen gehören.

Wichtige Einrichtungen sind Unternehmen bestimmter Branchen mit mindestens 50 Mitarbeitenden oder einem Umsatz ab zehn Millionen Euro und einer Bilanzsumme ab zehn Millionen Euro. Besonders wichtige Einrichtungen sind dagegen Unternehmen wichtiger Branchen mit mindestens 250 Mitarbeitern oder einem Umsatz ab 50 Millionen Euro und einer Bilanzsumme ab 43 Millionen Euro.

Die betroffenen Branchen werden in den beiden Anhängen der Richtlinie definiert, unter anderem gehören Sektoren

wie Energie, Transport und Verkehr, Finanz-/Versicherungswesen, Gesundheitswesen, Wasserwirtschaft und Telekommunikation dazu. Der Unterschied zwischen den Gruppen betrifft nicht die Pflichten, sondern die Höhen von Geldstrafen und die Häufigkeit von Prüfungen. Kritische und besonders wichtige Unternehmen müssen damit rechnen, häufig aktiv geprüft zu werden.

Das fordert die Richtlinie von Unternehmen

Generell sollen Unternehmen und öffentliche Verwaltungen geeignete technische und organisatorische Maßnahmen der Cybersecurity umsetzen. Dazu gehört die Sicherung von Netzwerken und Systemen sowie die Implementierung von Sicherheitsrichtlinien. Alle Maßnahmen müssen dem Stand der Technik entsprechen. In der Praxis bewirkt dieses Kriterium den Einsatz der aktuellen Best-Practices der IT-Security und ist damit ein „Moving Target". Die Unternehmen müssen also regelmäßig ihre Security-Maßnahmen überprüfen und an die Anforderungen anpassen.

Ein wichtiges Element der NIS2-Richtlinie ist die Meldepflicht: Unternehmen müssen erhebliche Zwischenfälle innerhalb von 72 Stunden an die nationalen Behörden melden. Das erlaubt ihnen, schnell auf Bedrohungen zu reagieren und die Auswirkungen zu verringern. Unter einem erheblichen Zwischenfall versteht die EU-Kommission dabei alles, was Betreiber oder Nutzer eines IT-Systems stark beeinträchtigt und größeren materiellen oder immateriellen Schaden verursacht.

Die Umsetzung der NIS2-Richtlinie erfordert von den betroffenen Unternehmen eine sorgfältige Planung. Verantwortlich dafür ist die Geschäftsführung, die auch für Verstöße haftet. Sinnvoll zur Umsetzung ist eine Stabsstelle mit einem angemessen ausgestatteten Projektteam. Dann kommt zunächst eine Bestandsaufnahme der Situation und anschließend die Planung von eventuell noch fehlenden Maßnahmen.

Informationssicherheitsmanagement nach ISO

Größere Unternehmen sollten spätestens jetzt die Einführung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001 und der entsprechenden Folgenormen angehen. Kleinere Unternehmen können auf den Grundschutzkatalog des BSI zurückgreifen, der kompatibel zur ISO-Norm ist. Zudem gibt es inzwischen eine Vielzahl an branchenspezifischen Sicherheitsstandards (B3S). Sie erlauben es Unternehmen, ihre Sicherheitsmaßnahmen entsprechend den Branchenanforderungen zu definieren und bringen Rechtssicherheit.

Zu den wichtigen Maßnahmen gehört die Einführung eines Incidentmanagements, das sich um die Prävention, Erkennung und Bewältigung von Sicherheitsverfahren kümmert. Dabei sollten alle Systeme mit einem Identity & Access Management geschützt werden, wozu auch der Einsatz von Multi-Faktor-Authentifizierung und einem abgesicherten Single-Sign-On gehört. Die Kommunikation geschieht natürlich mithilfe von sicheren Tools und Transportverschlüsselung.

Ein wichtiges Element für Unternehmen der kritischen Infrastrukturen ist ein Business Continuity Management, das nicht nur aus Backups und Disaster Recovery besteht, sondern auch Vorkehrungen für ein Krisenmanagement umfasst. Denn wenn ein schwerer Security-Vorfall eintritt, muss ein Notfallplan greifen, der Durcheinander und überflüssige Datenverluste vermeidet. Dazu gehört auch die Vorbereitung von Notfallkommunikation, also beispielsweise gesicherte und von der sonstigen Infrastruktur getrennte Systeme, die auch bei einem schweren Cyberangriff funktionieren.

Umsetzung der Richtlinie ist aufwändig

Der Aufwand zur Umsetzung der NIS2-Richtlinie ist vor allem für Unternehmen groß, deren IT-Ressourcen begrenzt sind. Deshalb ist es hilfreich, externe Berater und Lösungsanbieter zu verpflichten, um alle Anforderungen zu erfüllen. Externe Dienste wie Penetrationstests, Security Operations Center (SOC) oder Advanced Threat Protection helfen Unternehmen, ihre Verteidigungslinien zu stärken und potenzielle Schwachstellen zu identifizieren und zu schließen.

Ein SOC erweitert die rein technischen Maßnahmen, die von NIS2 vorgesehen sind. Hier sind Security-Experten im Einsatz, die dabei helfen, sicherheitsrelevanten Ereignissen vorzubeugen oder diese zu bewältigen. Dazu überwacht das SOC zentral Hard- und Softwarekomponenten sowie -prozesse. Es analysiert und bewertet Sicherheitsrisiken, schafft Transparenz und erkennt zielgerichtete Angriffe wie Ransomware oder Malware – rund um die Uhr an 365 Tagen.

Ein eigenes SOC ist für viele Unternehmen allerdings nicht zu leisten. Deshalb bieten Cloudprovider und Security-Dienstleister „SOC as a Service". Dabei übernimmt der Dienstleister mit einem eigenen Team und Plattformen für SIEM (Security Information and Event Management) und EDR (Endpoint Detection & Response) das Monitoring der Infrastruktur. Diese Form der Angriffserkennung schützt Unternehmen und sorgt für Compliance zur NIS2-Richtlinie.

Daniel Graßer

Cyberkriminelle überall

da tut Hilfe not

Mehr Infos dazu im Printmagazin

itsecurity

und online auf **www.it-daily.net**

Mittelständische Industrie

BEVORZUGTES ZIEL FÜR CYBERKRIMINALITÄT

Die Konvergenz von IT und OT führt zu einer Verschmelzung der Netzwerke. Dies eröffnet neue Angriffsvektoren und erfordert eine umfassende Sicherheitsstrategie, die beide Bereiche abdeckt. Ungesicherte Netzwerkverbindungen ermöglichen Lauschangriffe, Datenmanipulation und Überlastung, was zu Ausfällen führen kann. Sowohl interne als auch externe Akteure können Netzwerke gefährden. Insider-Bedrohungen, durch Mitarbeiter oder Lieferanten, sind eine ernstzunehmende Herausforderung. Das Internet der Dinge (IoT) erweitert die Angriffsfläche, und die Sicherheit von IoT-Geräten und -Netzwerken ist entscheidend, um unbefugten Zugriff zu verhindern. Insgesamt erfordert die Netzwerksicherheit eine ganzheitliche Herangehensweise, die technische, organisatorische und menschliche Aspekte berücksichtigt.

Als globaler Marktführer vertraut die Süddeutsche Gelenkscheibenfabrik (SGF) auf die 20-jährige Erfahrung von macmon NAC im Bereich der Netzwerksicherheit. Die SGF, gegründet im Jahr 1946, ist ein anerkannter Partner der weltweiten Automobilindustrie und in verschiedenen industriellen Anwendungen tätig. Bei SGF hat man die wachsende Gefahr für die Sicherheit ihrer IT- und OT-Netzwerke erkannt, denn in einer digitalen Welt entscheiden – immer öfter – die besten Security-Strategien über die Resilienz und Zukunft von Unternehmen.

Thomas Schuster, Systemadministrator, SGF, weist auf die Berührungspunkte zwischen IT- und OT-Sicherheit hin: „In unserem Industrieunternehmen arbeiten wir schon seit Jahren an gemeinsamen Lösungen, denn je mehr IT in der OT verbaut ist, desto enger muss die Zusammenarbeit sein. Schon im Entscheidungsprozess wird die IT von der OT informiert und wir klären bereits vor der Bestellung von Neuanschaffungen für die Produktion die Fernwartungsmöglichkeiten, beziehungsweise die benötigte Konnektivität."

Besonderheiten bei der Absicherung des OT-Netzwerkes

Generell muss die OT-Sicherheit eine absolute Ausfallsicherheit gewährleisten, denn Nichts ist für einen Produktionsbetrieb betriebswirtschaftlich schädlicher als Verzögerungen oder sogar der Ausfall von Produktionsanlagen. Dazu Schuster: „Hier hat sich bei uns bewährt, dass eine Maschine immer ein eigenes VLAN erhält – somit müssen wir derzeit eine große Anzahl von über 250 Netzen verwalten."

Eine komplexe Herausforderung bei der Belden´s macmon NAC durch die Identifikation der Endgeräte für Übersicht und Kontrolle sorgt. Das bestätigt Thomas Schuster: „Gerade bei Maschinenverlagerungen,-erweiterungen, und -umbauten steht uns die NAC-Lösung hilfreich zur Seite. Oft werde ich von den Entwicklern von Speicher programmierbaren Steuerungen (SPS) gefragt, warum ein ganz bestimmtes Endgerät nicht kommunizieren kann. Hier ist es unerlässlich, dass ich schnell herausfinde, wo das gesuchte Gerät physisch angesteckt ist. Außerdem muss ich fallweise wissen, ob es nicht oder eventuell sogar falsch angesteckt ist. So kann ich kurzfristig und zuverlässig unseren Entwicklern weiterhelfen."

www.macmon.eu

macmon NAC bietet Sicherheit und Kontrolle für IT- OT-Netzwerke:

- #1 Transparenz und Überblick: Sofortiger Netzwerküberblick über alle Geräte.
- #2 Sichere Authentifizierung: Granulare Zugriffskontrolle für autorisierte Geräte und Benutzer.
- #3 Automatische Visualisierung: Komfortable Darstellung des Netzwerks.
- #4 Steuerung der Zugänge: Präzise Kontrolle darüber, wer ins Netzwerk gelangt.
- #5 Identifizierung von Geräten: Effiziente Überwachung aller Geräte im Netzwerk.
- #6 Hochflexibles Gästeportal: Einfache und sichere Zulassung von Gast- und Mitarbeitergeräten.
- #7 Technologiepartnerschaften: Zusammenarbeit mit IT- und OT-Sicherheitslösungen.

macmon intelligent einfach

SPITZENBRANCHEN

MIT HOHEM API-AUFRUFVOLUMEN UND HOHEM BOT-TRAFFIC (AUSZUG)

7%
Technologie

18%
eCommerce und Retail

(Quelle: Imperva)

18%
Banking und Finanzwesen

5%
Service Provider, Transportwesen, Gesundheitsbranche

Keine Sicherheit ohne wirkungsvollen API-Schutz

API REPORT 2024

APIs (Application Programming Interfaces) haben in modernen IT-Infrastrukturen eine Schlüsselrolle inne: Diese Schnittstellen sind essenziell für die Kommunikation von Anwendungen untereinander und um Systeme reibungslos zu integrieren. Darüber hinaus erleichtern sie den Zugriff auf externe Ressourcen wie Datenbanken, Dateien und Webdienste, ohne dass eine vollständige Neuprogrammierung erforderlich ist. Letztendlich bilden sie also die Grundlage dafür, dass Nutzer mühelos auf Funktionen wie die Abfrage von Wetterdaten auf ihren Smartphones zugreifen oder Einzelhändler ihren Lagerbestand in Echtzeit überwachen können.

Im Jahr 2023 machten APIs laut des neuesten Berichts von Imperva über 71 Prozent des gesamten Internetverkehrs aus. Mit durchschnittlich 1,5 Milliarden Aufrufen pro Jahr auf Unternehmenswebsites sind APIs zu einem zentralen Bestandteil der digitalen Landschaft geworden. Doch gleichzeitig stellen sie eine beträchtliche Angriffsfläche für Cyberkriminelle dar.

Störungen wichtiger Geschäftsprozesse

Dem Bericht zufolge zielen 27 Prozent der Angriffe auf APIs darauf ab, die Business Logic von Unternehmen zu untergraben. Das führt zur potenziellen Störung wichtiger Geschäftsregeln und -prozesse wie etwa der Preisberechnung oder der Benutzerverwaltung.

19 Prozent der Angriffe auf APIs waren das Werk sogenannter „Bad Bots". Diese automatisierten Systeme haben das Ziel, Webseiten mit schädlichen Absichten anzugreifen. Unter den weltweit betroffenen Branchen waren vor allem Finanzdienstleister (20 Prozent) Ziel solcher Angriffe. 2023 entfielen 68,8 Prozent aller Bot-Aktivitäten in Deutschland auf Bad Bots, womit die Bundesrepublik international an der Spitze steht.

Besondere Risiken durch Schatten-APIs

Ein erhebliches Sicherheitsrisiko für Unternehmen stellen insbesondere Schatten-APIs dar, da sie oft Überbleibsel aus früheren Softwareversionen sind. Zwar sind sie möglicherweise noch für Tests neuer Funktionen nutzbar, doch sie sind auch anfällig für Manipulationen und Missbrauch durch böswillige Akteure.

Darüber hinaus können auch veraltete API-Endpunkte erhebliche Probleme verursachen, da sie keine Updates oder Patches mehr erhalten und somit anfällig für bekannte Sicherheitslücken sind, die in neueren Versionen behoben wurden. Wenn diese veralteten Endpunkte nicht erkannt und außer Betrieb genommen werden, steigt das Risiko von Daten-Kompromittierung. Daher ist es für Sicherheitsteams unerlässlich, die Systeme regelmäßig zu überprüfen, um solche potenziellen Risiken zu vermeiden.

Eine weitere Gefahr sind nicht authentifizierte Endpunkte. Diese werden von Entwicklern geschaffen, um den Entwicklungsprozess zu beschleunigen. So wird während der Entwicklungsphase der Funktionalität der Vorzug vor der Sicherheit gegeben, um Zeit zu sparen. Obwohl sich die Systeme im Laufe der Zeit weiterentwickeln, bleiben diese APIs oft ohne angemessene Sicherheitsmaßnahmen erhalten, was ein großes Risiko für Unternehmen darstellt. So könnten Daten unbefugten Benutzern zugänglich gemacht werden, was Hackern dann die Möglichkeit gibt, das System zu manipulieren. Regelmäßige Audits der Systeme durch Sicherheitsteams sind daher unerlässlich.

Schwachstellen

Neben den genannten Risiken gibt es noch weitere kritische Sicherheitslücken und Angriffsvarianten: An erster Stelle steht die so genannte „Broken Object Level Authorization" (BOLA), auch bekannt als „Insecure Direct Object Reference" (IDOR). Diese entstehen dadurch, dass APIs über ihre Endpunkte Objektidentifikatoren preisgeben, was zu großen Problemen bei der Zugriffskontrolle auf Objektebene führt. So können Angreifer API-Daten ohne entsprechende Autorisierung manipulieren oder darauf zugreifen. Durchschnittlich sind 1,6 API-Endpunkte dem Risiko eines BOLA-Missbrauchs ausgesetzt.

Angreifer können auch API-Konten übernehmen (API Account Takeover, ATO), indem sie Schwachstellen in API-Authentifizierungsprozessen ausnutzen, um sich unberechtigten Zugriff auf Benutzerkonten zu verschaffen. Laut des Berichts zielten im Jahr 2023 45,8 Prozent aller von Imperva registrierten ATO-Angriffe auf API-Endpunkte ab. ATO-Angriffe können mit Hilfe von Advanced Bot Protection-Lösungen abgewehrt werden.

Ein weiteres Problem stellen Distributed Denial of Service (DDoS)-Angriffe auf API-Webseiten dar. Dabei entfielen 27,9 Prozent aller DDoS-Angriffe auf API-Webseiten des Finanzsektors, gefolgt vom Unternehmenssektor mit 18,5 Prozent und Telekommunikations- und Internetdienstleistern mit 9,8 Prozent.

Effektiven Schutz bietet nur ganzheitlicher Ansatz

Die Herausforderungen für die Sicherheit von APIs sind breit gefächert und anspruchsvoll, und sie überschreiten oft die Grenzen herkömmlicher Schwachstellen in Anwendungen. Darüber hinaus sind API-Interaktionen überaus dynamisch und die gewaltige Menge an legitimen Anfragen macht ihren Schutz zu einer großen Herausforderung. Daher sind generische Lösungen dafür häufig nicht ausreichend. Es ist entscheidend, dass Unternehmen sich auf konkrete Aktionen konzentrieren, um die Sicherheit ihrer APIs zu stärken:

ES BEDARF EINES INTEGRIERTEN ANSATZES, UM APIS EFFEKTIV ZU SCHÜTZEN.

Stephan Dykgers, AVP DACH, Imperva, www.imperva.com/de

➤ Unternehmen sollten zunächst eine umfassende Identifizierung, Klassifizierung und Katalogisierung aller APIs, Endpunkte, Parameter und Payloads durchführen. Anschließend sind diese kontinuierlich zu überwachen, um das API-Inventar stets aktuell zu halten. Dadurch erhalten die Verantwortlichen Einblick in potenzielle Risiken und können festlegen, welche sensiblen Daten geschützt werden müssen.

➤ Es ist unerlässlich, risikoreiche und sensible APIs zu erkennen und zu sichern. Hierfür sollten Unternehmen spezifische Risikobewertungen durchführen, die sich auf API-Endpunkte konzentrieren, die anfällig für fehlerhafte Autorisierung und Authentifizierung sowie unangemessene Datenexposition sind.

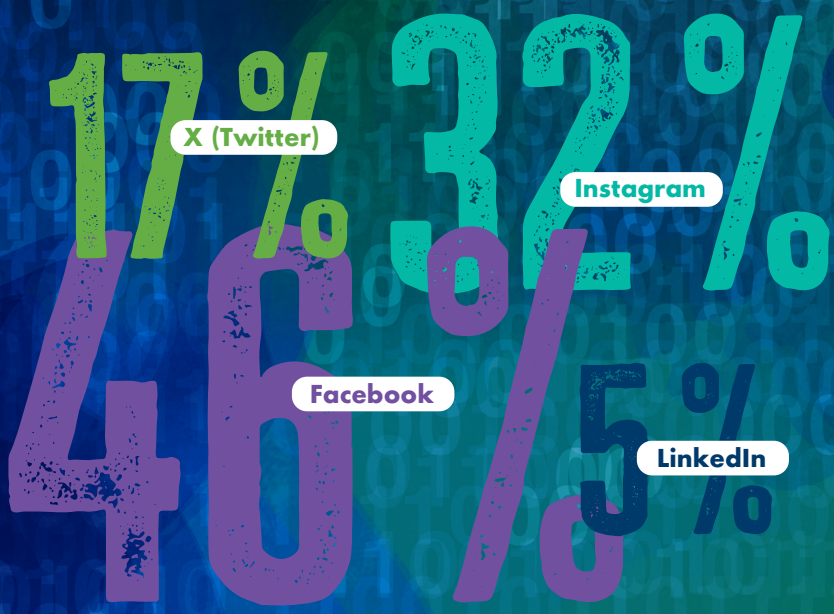
➤ Empfehlenswert ist es außerdem, ein leistungsstarkes Überwachungssystem für API-Endpunkte zu implementieren, um verdächtige Verhaltensweisen und Zugriffsmuster aktiv zu erkennen und zu analysieren.

➤ Schließlich sollten Unternehmen einen umfassenden Ansatz zur API-Sicherheit verfolgen, der API-Sicherheit, Web Application Firewall (WAF), Bot-Schutz und Schutz vor Distributed Denial of Service (DDoS) umfasst. Nur durch eine ganzheitliche Strategie können Sicherheitsteams Bedrohungen, die von exponierten APIs ausgehen, effektiv erkennen und beseitigen.

Zusammenfassend ist es unerlässlich für Unternehmen, die Bedrohungen durch Angriffe auf APIs ernst zu nehmen, da andernfalls geschäftskritische Infrastrukturen gefährdet sind. Zusätzlich können Angriffe auf APIs zu erheblichen Folgekosten führen, darunter Betrugsfälle, Datendiebstähle und ein Verlust des Kundenvertrauens. Herkömmliche Sicherheitsmaßnahmen allein sind daher nicht ausreichend. Es bedarf eines integrierten Ansatzes, um APIs effektiv zu schützen. API Security von Imperva beispielsweise erkennt und klassifiziert sensible Daten sowie sämtliche öffentliche, private und Schatten-APIs. So werden Security-Teams in die Lage versetzt, ein umfassendes Sicherheitsmodell zu implementieren.

Stephan Dykgers

WELCHE EXECUTIVE-PROFILE SIND AM EHESTEN GEFÄHRDET?



GEFÄHRLICHER TREND

BETRUG DURCH FAKE-PROFILE VON FÜHRUNGSKRÄFTEN

Betrugsversuche in der Form von Spammails begegnen vielen Menschen alltäglich, doch auch die sozialen Medien werden vermehrt von Cyberkriminellen heimgesucht. Eine besonders tückische Gefahr geht von einem Trend aus, der in letzter Zeit vermehrt beobachtet werden kann: gezielt erstellte Fake-Profile von Firmen-Führungskräften auf Facebook, Instagram und LinkedIn.

Diese Masche kann für Betrüger sehr lukrativ sein: Sie können sensible Daten stehlen und durch Erpressung oder Verkauf dieser Informationen enorme Profite erzielen. Dass leitende Angestellte und Personen von öffentlichem Interesse bevorzugte Ziele für Angreifer sind, liegt allerdings nicht ausschließlich am hohen potenziellen Wert der Beute. Kriminelle können die Bekanntheit und den Status einer Zielperson ausnutzen, um arglose Nutzer zu täuschen. Wenn diese mit dem Fake-Profil interagieren, gelingt es den Betrügern in vielen Fällen ihre Opfer zu manipulieren und ihnen Betriebsgeheimnisse, persönliche Daten oder sogar Geld zu entlocken.

So funktioniert die Betrugsmasche

Durch das Imitieren einer Führungskraft, ist es Angreifern oft möglich, potenzielle Geschäftspartner oder Mitarbeiter des hochrangigen Angestellten direkt zu kontaktieren ohne Verdacht auf sich zu ziehen. Sie versuchen Vertrauen aufzubauen, und Opfer dazu zu bringen, Informationen preiszugeben oder sogar Geld zu überweisen. Ein Vorteil dieser Vorgehensweise: Die Cyberkriminellen müssen – anders als bei anderen Cyberattacken – in der Regel keine Sicherheitsmechanismen wie Firewalls, Spamfilter, und Antivirenprogrammen überwinden. Sie nutzen die Tatsache aus, dass soziale Medien eine schnelle und einfache Kontaktaufnahme ermöglichen. Sollte die Täuschung erfolgreich sein, haben sie nun die Möglichkeit Daten und Ressourcen direkt vom Opfer übermittelt zu bekommen.

Betrüger brauchen ein Auge fürs Detail

Die erfolgreiche Durchführung von Identitätsfälschung auf Social-Media-Plattformen erfordert detailgetreue Arbeit. Um nicht verdächtig zu wirken, agieren die Betrüger bei der Ausspähung ihrer Ziele mit großer Sorgfalt. Es geht nicht nur darum Fotos und Lebensläufe zu kopieren. Sie müssen auch darauf achten, den Schreibstil und Post-Rhythmus des zu fälschenden Accounts möglichst genau nachzuahmen. Der Kauf massenhafter Bot-Follower zu günstigen Preisen ist ein weiteres attraktives Werkzeug für die Cyberkriminellen, um Glaubwürdigkeit vorzutäuschen. Die vermeintlich große Anhängerschaft eines Accounts kann auf den ersten Blick Vertrauen erwecken und dafür sorgen, dass Nutzer bei dem Versuch einer Kontaktaufnahme zunächst keinen Betrug vermuten.

Die Rolle der KI

Die jüngsten Fortschritte auf dem Gebiet der generativen Künstlichen Intelligenz eröffnen Bedrohungsakteuren die Möglichkeit, mit Leichtigkeit Bilder und Videos zu erstellen, die dazu dienen, digitale Identitäten mit einer verblüffenden Realitätsnähe auszustatten.

Das Gute an diesem technischen Entwicklungssprung ist, dass die Errungenschaften in den Bereichen von KI und ML ebenso strategisch eingesetzt werden können, um solche betrügerischen Aktivitäten aufzudecken.

www.bluevoyant.com

Managed Detection and Response

DREI ARGUMENTE FÜR MDR

DANK MDR KÖNNEN IT-VERANTWORTLICHE AUF EXTERNE SPEZIALISTEN UND IHRE AKTIVE UNTERSTÜTZUNG SETZEN.

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

Traditionelle Sicherheitsmaßnahmen leisten einen wichtigen Beitrag zum IT-Grundschutz. Inzwischen reichen diese aber bei weitem nicht mehr aus, um die gezielten Attacken der hochprofessionellen Cyberkriminellen auszuschließen. An einer mehrstufigen Abwehr und externer menschlichen Expertise für das Security-Management sowie an Analyse und Reaktionen auf Angriffe kommt kein Unternehmen mehr vorbei.

Klassische Endpoint Detection and Response (EDR), Network Detection and Response (NDR), gezielte Sicherheitsschulungen, Anti-Phishing-Trainings und nicht zuletzt der gesunde Menschenverstand wehren die meisten Cyberangriffe ab. Allerdings nur, wenn genügend qualifiziertes Personal vorhanden ist, welches die von diesen Technologien generierten Alarme auswerten, priorisieren und verfolgen kann. Oft bleibt ein unvermeidbares Restrisiko durch anspruchsvolle Infiltrationen in eine Unternehmens-IT, von denen bereits eine Einzige fatale Folgen haben kann. Komplexe hybride IT-Infrastrukturen aus Cloud -Plattformen, privaten Endgeräten aller Couleur, Notebooks oder Internet-of-Things-Hardware bieten eine höchst unübersichtliche und große Angriffsfläche. Zudem ist das schwächste Glied der Abwehr, der Mitarbeiter, in aller Regel das Ziel anspruchsvollerer Phishing-Attacken mit Hilfe generativer Künstlicher Intelligenz, die sich zunehmend auch Large-Language-Modellen bedient.

Hilfe von außen

Das Eindringen von Hackern in die Unternehmens-IT lässt sich niemals ausschließen. Im Gegenteil, man muss inzwischen davon ausgehen, dass dies längst erfolgt ist, ohne erkannt zu werden. Es bedarf daher einer mehrstufigen Abwehr, die sich sowohl auf die mögliche Prävention, aber vor allem auf das Erkennen und Eindämmen von Angriffen fokussiert. Und aufgrund von Fachkräftemangel, Komplexität und Wissenslücken braucht es die komplementäre Unterstützung durch Experten von außen.

Managed-Detection-and-Response (MDR)-Dienste, oft auch als Managed SOC bezeichnet, bieten die notwendige Erweiterung der vorhandenen Abwehrmaßnahmen. Sie liefern eine umfassende Sichtbarkeit der Cyberrisiken für eine agile Abwehr. Vor allem aber können IT-Verantwortliche dank MDR auf ein Team von hocherfahrenen Spezialisten, ihre proaktive Analyse und aktive Unterstützung im Falle eines erkannten Angriffs setzen. Sie nutzen aktuelle Technologien, die für ein Unternehmen oft außer Reichweite sind, und erkennen Anomalien, die ansonsten unerkannt bleiben.

Drei Argumente sprechen für die Notwendigkeit von Managed Detection and Response:

Kontrollierte Sicherheit: Externe Experten in weltweit verteilten Security Operation Centers (SOC) stehen rund um die Uhr an sieben Tagen in der Woche bereit. Sie beobachten nicht nur die allgemeine Angriffslage, sie überwachen kontinuierlich die IT-Sicherheit Ihrer Kunden und agieren proaktiv angesichts möglicher Bedrohungen.

Kontinuierliche Erkennung: MDR hat die dynamisch wachsende Angriffsfläche durch Anwendungen, Infrastruktur und zunehmende Cloud-Nutzung im Blick. Aufgrund einer darauf aufbauenden Analyse identifizieren und bewerten Experten proaktiv potenzielle Risiken. KI-Technologien in Verbindung mit Threat Intelligence erkennen Anomalien am Verhalten digitaler Assets, die auf einen Cyberangriff hinweisen können.

Gezielte Gegenmaßnahmen: Eine wirksame Reaktion beruht nicht nur auf dem Alarm, sondern auf einer konkret umsetzbaren Strategie zur Abwehr und zum Eindämmen eines Angriffes. Der menschliche Blick und Erfahrung sind zentral, um echte Risiken von Fehlalarmen zu unterscheiden, Informationen im Kontext zu analysieren und die Abwehr anhand vorab festgelegter Abläufe zu initiieren. Ein solcher Ansatz stärkt zugleich die zukünftige Abwehr.

Jörg von der Heydt
www.bitdefender.de

Bitdefender

Argusaugen der Neuzeit

WIE MANAGED DETECTION AND RESPONSE (MDR) EINE WICHTIGE LÜCKE SCHLIESST

Ransomware-Attacke hier, Lieferkettenangriff da – IT-Verantwortliche wissen manchmal gar nicht mehr, wohin sie ihren Blick zuerst richten sollen, um jedes Einfallstor unter Kontrolle zu bringen. Und nach Feierabend wird es sowieso schwierig. Im Interview zeigt Michael Haas, Vice President Central Europe bei WatchGuard Technologies, wie MDR-Services in solchen Situationen zum Retter in der Not werden.

it security: *Herr Haas, im Herbst 2023 hat WatchGuard einen eigenen MDR-Service vorgestellt. Wie sieht die Strategie dahinter aus?*

Michael Haas: Das ist recht schnell erklärt: Bereits bevor WatchGuard im Jahr 2020 Panda Security als Spezialisten im Bereich Endgerätesicherheit akquiriert hat, gab es im spanischen Bilbao ein eigenes Security Operations Center (SOC). Dieses übernahm als eine separate Geschäftseinheit unter dem Namen Cytomic – mittlerweile WatchGuard Orion – für große Unternehmen wie beispielsweise den Telekommunikationskonzern Telefónica dedizierte Aufgaben im Rahmen der Angriffserkennung und -abwehr und tut dies auch weiterhin. Der Grundstein für das hochprofessionelle MDR-Angebot, von dem unsere Partner und deren Kunden heute profitieren, wurde somit bereits vor vielen Jahren gelegt. Zuletzt haben wir das Portfolio weiter ausgebaut, wobei wir konkret die Bedürfnisse mittelständischer Unternehmen im Blick hatten. Hier haben wir in den letzten Jahren massiv investiert – sowohl technologisch als auch personell.

it security: *Was bedeutet das konkret? Wie groß ist die Mannschaft?*

Michael Haas: Seit 2020 wurden zahlreiche Mitarbeiter und Mitarbeiterinnen eingestellt, die jetzt rund um die Uhr damit beschäftigt sind, die gegenwärtigen Bedrohungsszenarios konsequent zu überwachen. Das Eliteteam aus IT-Sicherheitsexperten arbeitet auf Basis fortschrittlichster Technologien – unterstützt von Künstlicher Intelligenz. Dieses Gesamtpaket haben wir 2023 in ein „as a Service"-Angebot gegossen – allein dafür kamen über 100 neue Kollegen und Kolleginnen dazu. Von unseren Partnern wird dieses Engagement extrem gut angenommen. Schließlich können sie nun souverän auf die steigende Nachfrage nach 24/7-Überwachung reagieren, ohne in den eigenen Reihen den enormen finanziellen, fachlichen und zeitlichen Aufwand, der mit dem Aufbau eines eigenen SOC einhergeht, stemmen zu müssen.

it security: *Der Service läuft also über die WatchGuard-Partner?*

Michael Haas: In der Regel ja, konkret über Partner, die sich als MSP (Managed Service Provider) positionieren. Der Grund liegt nah: Diese sind gemeinsam mit den Kunden an vorderster Front, sollten die Alarmglocken im WatchGuard SOC einmal schrillen. So kann bei Bedarf gegebenenfalls sofort und fachkundig eingegriffen und reagiert werden, um Schaden fernzuhalten. In der aktuellen Situation, die von einem massiven Fachkräftemangel im Markt geprägt ist, ist dies meist die zielführendste Konstellation. Denn in der Realität sieht die Lage doch immer häufiger so aus: Unternehmen, vor allem im KMU-Bereich, verfügen selbst nicht über die entsprechenden Personalkapazitäten und/oder Expertenkenntnisse, um wirklich umfassenden Schutz sicherstellen zu können. Wer das Thema IT-Sicherheit für seine Firma jedoch nicht gänzlich abschreiben will, begibt sich auf die Suche nach einem geeigneten Dienstleistungspartner. Der Bedarf wird zunehmend größer, was es für die immer zahlreicheren Managed Service Provider natürlich auch nicht einfacher macht, schließlich wächst das Fachpersonal in deren Reihen ebenfalls nicht auf Bäumen. Genau hier schließt der MDR-Service eine ent-

scheidende Lücke. Wie der Wächter Argus aus der griechischen Mythologie hat unser SOC die einschlägige Gefahr für unsere Partner und deren Kunden jederzeit verlässlich im Blick. Im Gegensatz zum antiken Vorbild lassen sich unsere Cyberexperten aber nicht durch ein Schlaflied oder sonstige Ablenkung einlullen, sondern bleiben pausenlos in Bereitschaft.

it security: *Also gezielte Arbeitsteilung für noch besseren Schutz?*

Michael Haas: Vollkommen richtig. Der skalierbare und an die jeweiligen Bedürfnisse anpassbare Service fügt sich stringent in unser „Unified Security"-Konzept ein und bereichert dieses um fortschrittliche Funktionen zur Gefahrenerkennung und -abwehr. Neben der 24/7-Überwachung aller Ereignisse am Endpunkt gehört auch die proaktive Suche nach Angriffsindikatoren zum Leistungsumfang. Zudem erfolgt bei einem validierten Vorfall eine sofortige Benachrichtigung des jeweiligen Partners – mit wichtigen Informationen zu betroffenen Rechnern oder verwendeten Taktiken. Auf Wunsch rufen wir aber auch direkt beim Kunden an, schließlich geht es im Ernstfall um jede Minute. In dem Zusammenhang bieten wir zudem zahlreiche Optionen zur Angriffsbehebung. So unterstützt das WatchGuard-Team beispielsweise dabei, die Spuren eines Angriffs einzudämmen und zu entfernen, Daten wiederherzustellen, Schwachstellen zu patchen und zusätzliche Kontrollen zu installieren, egal ob im Hintergrund oder unmittelbar. Das entscheiden letztlich die Partner.

it security: *Wie reagieren diese auf das neue Angebot?*

Michael Haas: Absolut positiv, zumal es ja die unterschiedlichsten Varianten gibt, den MDR-Service im Rahmen individueller Dienstleistungspakete auszuspielen. Dazu vielleicht ein Beispiel: Die MTF Solutions AG, die seit 2021 zur Schweizer Swisscom gehört, war einer unserer ersten Partner im deutschsprachigen Raum, die schon in der Beta-Phase mit dem WatchGuard SOC zusammengearbeitet haben. Als MSP bietet das Unternehmen den Kunden Sicherheitsleistungen in drei verschiedenen Ausprägungen. Das Bronze-Level umfasst initial die Analyse der IT-Systeme. Sobald etwas Ungewöhnliches entdeckt wird, erhält der Kunde von MTF die Information und kann selbst aktiv werden. Darauf greifen insbesondere größere Organisationen zurück, die ein eigenes Security-Team haben, das dann passende Maßnahmen ergreift. Im Silber-Status überwacht MTF nicht nur, sondern übernimmt auch die Problemlösung. Und das Gold-Paket subsummiert schließlich das gesamte Leistungsspektrum von Überwachung, Reaktion und Recovery in 24/7-Bereitschaft – ein Angebot, das mittlerweile immer mehr MTF-Kunden in Anspruch nehmen. Gerade im Hinblick auf die lückenlose Überwachung von Endpoints können wir dem Partner in diesem Konstrukt eine nicht zu unterschätzende Last abnehmen. Es ergibt sich eine Win-win-Situation für alle Beteiligten. Unser kontinuierlicher Invest in ein hochmodernes SOC trägt sich. IT-Dienstleister profitieren von hochkarätiger MDR-Funktionalität zum wettbewerbsfähigen Preis und Endkunden erhalten erstklassige und umfassende Sicherheit, die der virulenten Bedrohungslage Stand hält. Und darauf kommt es ja am Ende an. Aus diesem Grund werden wir unsere „Argusaugen" künftig auch noch deutlich weiter ausrichten.

it security: *Was genau bedeutet das für Ihre zukünftige Planung?*

Michael Haas: In Kürze wird zum MDR-Service mit Fokus auf Endgerätesicherheit auch noch ein Angebot im Bereich Network Detection and Response (NDR) hinzukommen. Hierbei geht es darum, Netzwerkanomalien in hochautomatisierter Form zu bekämpfen. Bisher war NDR aus Kostengründen ja meist nur großen Konzernen vorbehalten. Das werden wir gemeinsam mit unseren Partnern zukünftig ändern und adäquat zu MDR entsprechende Funktionalität auch für den Mittelstand anbieten. Details dazu verraten wir bald.

it security: *Herr Haas, vielen Dank für das Gespräch!*

IT-DIENSTLEISTER PROFITIEREN VON HOCHKARÄTIGER MDR-FUNKTIONALITÄT ZUM WETTBEWERBSFÄHIGEN PREIS UND ENDKUNDEN ERHALTEN ERSTKLASSIGE UND UMFASSENDE SICHERHEIT, DIE DER VIRULENTEN BEDROHUNGSLAGE STAND HÄLT.

Michael Haas, Vice President Central Europe, WatchGuard Technologies, www.watchguard.de

Computer Vision

KI-SCHLÜSSEL-TECHNOLOGIE FÜR MEHR PRODUKTIVITÄT

Der Einsatz von Computer-Vision-Technologie, die auf KI basiert, nimmt deutlich Fahrt auf und wird die Produktivität in zahlreichen Branchen steigern. Dies zeigt eine neue Studie im Auftrag von Panasonic Connect Europe. Im Durchschnitt rechnen die befragten Entscheidungsträger mit einer Produktivitätssteigerung von 42 Prozent in den ersten drei Jahren nach der Bereitstellung der Technologie. Die größten Auswirkungen erwartet das verarbeitende Gewerbe mit Produktivitätssteigerungen von bis zu 52 Prozent.

Computer Vision ist ein Bereich der Künstlichen Intelligenz, der es Computern und Systemen ermöglicht, aus digitalen Bildern aussagekräftige Informationen abzuleiten. Das „Auge" der KI beobachtet, identifiziert, klassifiziert und rückverfolgt Bilder. Die gesammelten Informationen wandeln sie schließlich in nutzbare Daten um, die Menschen oder eine ergänzende KI abfragen und nutzen können.

Vielfältige Anwendungsmöglichkeiten

Die Befragten gaben an, dass die Computer-Vision-Technologie bereits in einer Vielzahl von Abteilungen und Anwendungen eingesetzt wird. Praktische Tätigkeiten wie Reparaturen und Wartung, Überwachung von Produktionslinien und Qualitätskontrollen überwiegen dabei leicht gegenüber dem Einsatz in den Bereichen Sicherheit und Gesundheitsschutz. Anwendungen in der Logistik und in der Lieferkette sind ebenso beliebt wie Echtzeit-Projektionsmapping und Personenverfolgung. Dies verdeutlicht das breite Spektrum an relevanten Anwendungsfällen für die Computer-Vision-Technologie.

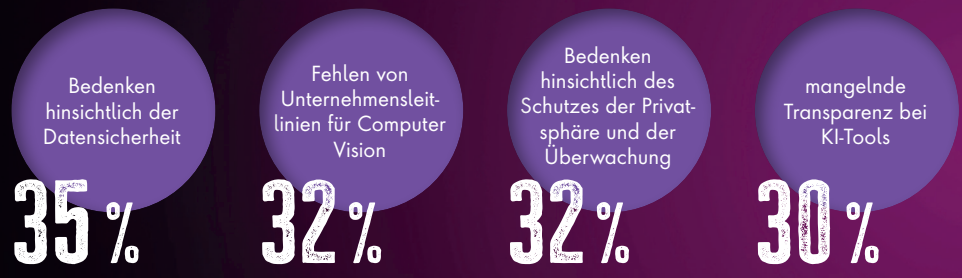
Fehlende Fähigkeiten hemmen den Einsatz

Die größten Hindernisse für den Einsatz der Technologie stellen der Mangel an externer fachlicher Unterstützung (37 Prozent) und die Aufrechterhaltung von Computer-Vision-Kenntnissen im Unternehmen (33 Prozent) dar. Unternehmen sind zudem für die potenziellen ethischen Bedenken beim Einsatz von KI-gestützten Computer-Vision-Anwendungen sensibilisiert. Die größten Vorbehalte gibt es in Bezug auf Datensicherheit (35 Prozent), dicht gefolgt von Bedenken hinsichtlich des Datenschutzes und der Überwachung, mangelnden Unternehmensrichtlinien und der Befürchtung, den Arbeitsplatz zu verlieren – alle auf einem Niveau von 32 Prozent.

„Die Studie zeigt deutlich, dass die Computer Vision-Technologie nicht nur ein Konzept, sondern schon Realität ist. Sie führt in Unternehmen bereits zu erheblichen Produktivitäts- und Betriebssteigerungen", sagt Margarita Lindahl, Head of AI bei Panasonic Connect Europe.

https://eu-connect.panasonic.com

Was sind die wichtigsten ethischen Hindernisse für den Einsatz von Computer Vision in Ihrem Unternehmen?



KI in der SAP-Security

POTENZIALE UND GRENZEN DES MASCHINELLEN LERNENS

VIELES IST KEINE ROCKET SCIENCE, SONDERN NUMERISCHE AUSWERTUNG UND ANALYSE.

Ralf Kempf,
CTO, Pathlock Deutschland,
www.pathlock.de

Eine aktuelle Umfrage des führenden IT-Security-Spezialisten Pathlock zur SAP-Security bestätigt, dass das Thema KI auch in der deutschsprachigen SAP-Community rasant an Bedeutung gewinnt – es aber kaum jemand wirklich versteht. Ralf Kempf, CTO von Pathlock Deutschland, erklärt, warum weder Mensch noch Maschine die alleinige Lösung sind.

„Wie haltet ihr es denn mit künstlicher Intelligenz?" – eine Frage, die uns derzeit immer mehr Kunden stellen, weil sie medial allgegenwärtig ist. Nüchtern betrachtet ist dies zunächst ein trendiges „Buzzword", unter dem sich aber fast niemand Konkretes vorstellen kann. Vieles darunter Gefasste, etwa das autonome Fahren, ist dabei keine Rocket Science, sondern eine Vorstufe von KI, die numerische Bildauswertung.

Grenzen künstlicher Intelligenz

Ein System wird mit vielen Informationen gefüttert, wie etwas normal ist oder nicht. Es kann dann aufgrund numerischer Analyse, bei der die Informationen so verdichtet werden, dass sie wieder abgefragt werden können, in der Regel gute Links-rechts-Entscheidungen automatisieren. Aber eben nur in der Regel: Ein autonomes Fahrsystem weiß, dass es bei einem Stoppschild anhalten muss. Wenn aber Schnee das Schild bedeckt, ist einem menschlichen Fahrer trotzdem bewusst, vor einer Kreuzung vorsichtig zu sein. Das autonome System wird jedoch einfach weiterfahren.

Das lässt sich vereinfacht auf die Grenzen künstlicher Intelligenz in der SAP-Security übertragen. Von einem rein neuronalen Netzwerk geleitet zu werden, könnte zu sehr merkwürdigen Ergebnissen führen. Wenn wir zugleich feststellen, dass auch in Ausschreibungen zunehmend die Frage nach KI gestellt wird, bestätigt dies, dass der mediale Hype oft von jenen befördert wird, die nicht wissen, wie diffizil das Thema ist, und es laufend überstrapazieren. Wir haben es aber nicht mit einer Art göttlichen Lösung zu tun, die ad hoc alles von selbst erledigt und den Menschen überflüssig macht.

Vielmehr ist KI eine hochinteressante Entwicklung und hat eine absolute Daseinsberechtigung. Wie aber am Beispiel des autonomen Fahrens erkennbar, ist es eben doch nicht ganz so einfach. Während der Analyst allein überlastet und die KI in vielen Fällen noch regelrecht dumm ist, gibt es einen bewährten Weg der Mitte, die Vorstufe von künstlicher Intelligenz: maschinelles Lernen – die numerische Analyse und UEBA (User and Entity Behavior Analytics).

User and Entity Behavior Analytics

Für ein Security-Baselining muss UEBA zunächst Daten aus verschiedenen Quellen sammeln, sie auswerten und lernen, was ein normales Verhalten von Nutzern und Entitäten ist. Gesammelt und korreliert wird dabei etwa, auf welche Systeme und Daten wann und von wo gewöhnlich zugegriffen wird, welche typischen Betriebssysteme und Anwendungen genutzt werden und welche Entitäten miteinander kommunizieren.

Danach ist das System in der Lage, durch kontinuierliche Analyse der Daten in Echtzeit Anomalien aufzuspüren. Maschinelles Lernen und intelligente Algorithmen optimieren fortlaufend die Erkennungsverfahren. Findet UEBA Anomalien, alarmiert es gemeinhin die für die IT-Sicherheit verantwortlichen Stellen. Dies funktioniert am besten mit vordefinierten Algorithmen, wie wir sie in unserer Software bereitstellen. Und spätestens hier kommt wieder der Mensch ins Spiel: Denn bevor ein autonomes System eventuell fälschlicherweise die Notbremse zieht, sollte alles, was UEBA als anormal identifiziert, letztlich von einem Analysten überprüft werden.

www.pathlock.com

pathlock

Technik und Kultur

GEMEINSAM FÜR MEHR CYBER-SICHERHEIT

Kriminelle erbeuten 25 Millionen US-Dollar von einem Unternehmen, indem sie unter Einsatz von KI dessen CFO imitieren – dieser Deepfake-Fall in Hongkong ging vor wenigen Wochen durch die Presse. Er dürfte nicht der letzte seiner Art gewesen sein. Wieder einmal zeigte sich unheilvoll das Gewaltpotenzial, welches sich hinter den neuen Techniken der Künstlichen Intelligenz verbirgt.

Cyberkriminelle und Hacktivisten wissen sich deren Fähigkeiten in höchst kreativer Weise zu bedienen: Phishing-Mails werden unter Einsatz KI-gestützter Gestaltung noch originalgetreuer, die Kanäle durch automatisiertes Social Engineering präziser gewählt, und die Quantität der Angriffe wächst weiter: Laut Bundeskriminalamt steigen sowohl die durch Cyberkriminalität entstandenen Schäden stark an als auch die aus dem Ausland heraus begangenen Taten. Branchenübergreifend sind alle gleichermaßen betroffen: Kleinunternehmen, Mittelständler wie auch Großkonzerne. Im besonderen Fokus der Cyberkriminellen stehen der öffentliche Sektor und kritische Infrastrukturen.

Deshalb wird es immer wichtiger, Hard- und Software sowie physische als auch virtuelle Zugänge zu schützen. Dies muss von zwei Seiten aus angegangen werden: technische Minimierung von Angriffsflächen durch Umsetzung von SOAR-Konzepten (= Security Orchestration, Automation and Response) durch UEM-Plattformen auf der einen Seite und Sensibilisierung der „Schwachstelle Mensch" auf der anderen.

Plattformen für Unified Endpoint Management bilden sämtliche Aufgaben der IT-Administration zentral mit Hilfe unterschiedlicher Module ab. Sie sind dadurch ein ideales Werkzeug zur Prävention. Angriffsflächen lassen sich mit ihnen minimieren und Schwachstellen klein halten beziehungsweise schnell schließen, wenn Updates verfügbar sind.

Microsoft Defender über UEM steuern

Über ein UEM-System können IT-Admins verschiedene Antivirenlösungen und Verschlüsselungsmethoden zentral verwalten. So beinhaltet die ACMP Suite von Aagon ein eigenes Modul (Defender Management) für die zentrale Steuerung des Microsoft Defenders auf allen Clients in der Netzwerkumgebung. Seit einiger Zeit bereits hat sich der Defender auf die vordersten Plätze unter den Antivirus-Systemen vorgearbeitet und ist zudem kostenlos im Betriebssystem enthalten. Das UEM-System liefert hierbei voreingestellt aussagekräftige Reports über den Defender-Status, Scan-Historien, neueste Bedrohungen sowie Infos zum nächsten anstehenden Scan. Es bietet zudem eine Möglichkeit für Abfragen der genutzten / nicht genutzten Konfigurationsprofile.

UNTER DEM SCHLAGWORT „HUMAN CENTERED SECURITY" WERDEN MASSNAHMEN ZUSAMMENGEFASST, DIE FÜR DIE RISIKEN, DIE VOM EINZELNEN USER AUSGEHEN, SENSIBILISIEREN SOLLEN.

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

Regelmäßig wird nach Funden, Bedrohungen und Updates gescannt – mit sofortigem Statusbericht. Das UEM-System liefert einen Überblick aller gefundenen Bedrohungen, fehlgeschlagenen Updates und sonstigen Ereignisse. Die Anzeige der Ereignisse lässt sich konfigurieren, veraltete lassen sich filtern, sortieren oder löschen. Aus einem Ereignis kann der Admin direkt aus der UEM-Konsole zum betroffenen Client navigieren. Zudem hat dieser die Möglichkeit, Quarantänedateien einzusehen, wiederherzustellen, Aktionen auf ihnen auszuführen sowie sie automatisiert nach Ablauf eines definierten Zeitraums zu löschen.

Das verlorengegangene Notebook

Das ACMP BitLocker Management integriert die Verwaltung des Microsoft BitLockers in die Konsole der Aagon-Lösung und ergänzt dessen Funktion um zentrale Verwaltung und Überblick der Festplattenverschlüsselungen, Statusabfragen von Schlüsselschutzvorrichtungen, Überblick über BitLocker-fähige

Clients sowie Monitoring- und Reporting-Funktionen für aussagekräftige Analysen. Das erhöht die IT-Security und schützt sensible Informationen zuverlässig vor Datendiebstahl.

Schwachstellenmanagement

Ein Schwachstellenmanagement spürt zudem kritische Sicherheitslücken in der Netzwerkumgebung auf, legt vom IT-Administrator voreingestellte und automatisierte Reaktionsroutinen fest und beseitigt Risiken mithilfe CVSS- und CVE-zertifizierter Handlungsempfehlungen. Die dafür notwendigen Sicherheits-Scans werden so geplant und durchgeführt, dass die einzelne Arbeitskraft vor ihrem PC davon nichts mitbekommt und auch nicht beeinträchtigt wird. Schließlich beinhaltet das UEM-System von Aagon Module für Windows Update Management, Managed Software und Desktop Automation, die sich an das Schwachstellenmanagement anschließen bzw. darauf reagieren.

Automatisierung der Cyber-Sicherheit durch SOAR

Für das gebündelte Erkennen, Priorisieren und Beheben möglicher Sicherheitsprobleme hat sich seit einiger Zeit der Terminus SOAR (Security Orchestration, Automation and Response) etabliert. Darunter versammeln sich alle Funktionen, die darauf abzielen, durch Standardisierung und Priorisierung automatisiert und damit effizient auf erkannte Bedrohungen zu reagieren. Genau dies ist mit einer UEM-Lösung möglich.

Reine SOAR-Werkzeuge sind oft auf Enterprise-Umgebungen hin zugeschnitten und decken Schwachstellen über die ganze Bandbreite möglicher Sicherheitslücken ab: Clients, Server, Firewalls etc. Für viele Mittelständler ist ein solcher Ansatz zu aufwändig und teuer. Angesichts der Tatsache, dass die Endpoints ohnehin Haupteinfallstor für Cyber-Attacken sind, liegt es nahe, ein SOAR-Konzept mit der vorhandenen UEM-Lösung umzusetzen. Sie enthält bereits die drei grundlegenden SOAR-Bausteine: Case- und Workflow-Management, Aufgabenautomatisierung sowie eine zentrale Methode, um Bedrohungsinformationen (Threat Intelligence) aufzurufen, zu durchsuchen und zu teilen.

Das UEM-System kann damit bereits viel. Nicht zu seinen Aufgaben zählt es dagegen, Schulungen zum Verhalten der Beschäftigten anzubieten oder durchzuführen. Was zur „Schwachstelle Mensch" als zweitem Ansatzpunkt für Prävention führt. Durch fortschreitende Technik, den Anstieg von Mobile Work und ungünstige äußere Umstände wie steigende Arbeitsdichte und Informationsflut sind Unternehmen auch weiterhin nicht davor gefeit, dass viele Sicherheitslücken sich durch den Menschen erst öffnen.

Phishing-Mails: nur einmal unaufmerksam geklickt

Unter dem Schlagwort „Human Centered Security" werden deshalb Maßnahmen zusammengefasst, die für die Risiken, die vom einzelnen User ausgehen, sensibilisieren sollen. Es geht darum, Verhaltens- und Denkmuster in der IT-Sicherheit zu ändern und herauszufinden, wann und unter welchen Umständen menschliches Verhalten Sicherheitsrisiken provoziert. Diese gilt es in der Folge strategisch, technologisch und psychologisch zu vermeiden.

Instrument dafür sind spezielle Schulungen, die Verhaltensgrundsätze wie den Umgang mit Zugangsdaten sowie Hardware, Erkennungskriterien von Phishing-Mails und grundsätzliche mit dem Datenschutz verbundene Inhalte lehren. Denn insbesondere durch KI sind Phishing-Mails heute so raffiniert, dass eben doch immer wieder jemand darauf hereinfällt und aus Unaufmerksamkeit den fatalen Button klickt.

Ergebnis dieser Sensibilisierung soll es sein, dass die vermittelten theoretischen Verhaltensweisen auch wirklich eingehalten und nicht, gesteuert durch Emotionen, kognitive Diversität sowie Verzerrungen, unterminiert werden. Damit – und durch UEM-Technologie – ist dann schon viel gewonnen auf dem Weg zu höherer Cyber-Security.

Sebastian Weber

HackGPT

DIGITALE SICHERHEITSLANDSCHAFT IM WANDEL: DER EINFLUSS VON KI

Die Technologie der künstlichen Intelligenz (KI) hat eine Revolution in zahlreichen Branchen ausgelöst, nicht zuletzt in der Welt der Cybersicherheit. Während KI-Systeme, insbesondere ChatGPT und ähnliche Modelle, beeindruckende Effizienzsteigerungen in der Datenverarbeitung und im Kundenservice ermöglichen, haben sie zugleich eine neue Dimension der Cyberkriminalität eröffnet. Dies zwingt Sicherheitsexperten dazu, ihre Schutzstrategien grundlegend zu überdenken.

Die Ambivalenz von KI in der Cybersicherheit

Die Einführung von KI in die Cybersicherheit hat das Potenzial, Netzwerksicherheitssysteme zu stärken, indem sie Bedrohungen schneller identifiziert als traditionelle Methoden. Diese Technologien bringen jedoch auch Risiken mit sich, da sie ebenso von Cyberkriminellen genutzt werden können, um ausgeklügelte Angriffe zu orchestrieren.

Generative KI-Modelle, die Inhalte wie Texte, Bilder und Videos mit verblüffender Authentizität erzeugen, eröffnen neue Wege für Kreativität und Produktivität. Gleichzeitig birgt diese Fähigkeit das Risiko, gefälschte Inhalte und Medien (Deepfakes) zu erstellen, die für

Betrug und Desinformation eingesetzt werden können.

Neue Angriffsvektoren und Sicherheitsherausforderungen

Mit der fortschreitenden Entwicklung der KI ergeben sich für Cyberkriminelle neue Angriffsstrategien. Von der Generierung überzeugender Phishing-E-Mails bis hin zur Erstellung von bösartigem Code ermöglicht KI eine bisher unerreichte Personalisierung und Effizienz in Cyberangriffen.

KI-Modelle erleichtern Cyberkriminellen die Forschung und Informationsbeschaffung über potenzielle Ziele. Durch die Analyse großer Datenmengen können Angreifer maßgeschneiderte Phishing-Kampagnen entwickeln, die selbst aufmerksame Nutzer täuschen können. Zudem ermöglicht KI die schnelle Entwicklung und Anpassung von Malware, wodurch auch weniger technisch versierte Kriminelle gefährliche Angriffe durchführen können.

Verteidigungsstrategien im KI-Zeitalter

Um der wachsenden Bedrohung durch KI-gestützte Angriffe zu begegnen, ist eine Evolution der Sicherheitsstrategien unerlässlich. Fortschrittliche Authentifizierungsmethoden, wie Multi-Faktor-Authentifizierung und passwortlose Systeme, bieten einen starken Schutzschild gegen viele Formen von Cyberangriffen.

Eine ausgefeilte Customer Identity and Access Management (CIAM)-Strategie ist entscheidend, um gegen die raffinierten Angriffsmethoden gewappnet zu sein. Durch die Kombination von Sicherheit und Benutzerfreundlichkeit bieten moderne CIAM-Systeme wie die von Nevis einen robusten Rahmen für den Schutz digitaler Identitäten.

DIE DYNAMISCHE NATUR DER KI-GESTÜTZTEN CYBER-BEDROHUNGEN ERFORDERT EINE KONTINUIERLICHE ANPASSUNG UND AKTUALISIERUNG DER SICHERHEITSSTRATEGIEN.

Gregory Guglielmetti,
Chief Product Officer, Nevis Security AG,
www.nevis.net/de

Security Operation Centers (SOCs) bieten mithilfe einer KI-gestützten Kundenidentitätsplattform wie Nevis die Möglichkeit, zentral auf schnell veränderliche Bedrohungslagen zu reagieren, indem sie wichtige Bedrohungsintelligenzsignale und Informationen zur Verfügung stellen. Darüber hinaus ist Nevis auch in bestehende Bedrohungsintelligenz- und FRIP-Systeme integrierbar, um Risikosignale zu verstärken und Cyberattacken gezielt abzuwehren – bevor sie Schaden anrichten können.

Fortgeschrittene KI-Anwendungen in der Cyberabwehr

Die fortschreitende Entwicklung von KI bietet nicht nur Angreifern neue Werkzeuge, sondern stärkt auch die Verteidigungslinien der Cyberabwehr. Machine Learning und KI-Systeme werden zunehmend eingesetzt, um Muster in Datenverkehr und Nutzerverhalten zu erkennen, wodurch Anomalien und potenzielle Bedrohungen schneller identifiziert werden können. Diese Technologien unterstützen auch bei der Analyse von Schwachstellen in Software und Netzwerken, um präventive Maßnahmen zu ergreifen, bevor diese ausgenutzt werden können.

Anpassung an die dynamische Bedrohungslandschaft

Die dynamische Natur der KI-gestützten Cyberbedrohungen erfordert eine kontinuierliche Anpassung und Aktualisierung der Sicherheitsstrategien. Sicherheitsexperten müssen nicht nur aktuelle Trends in der Cyberkriminalität verfolgen, sondern auch die Entwicklung neuer KI-Modelle und Techniken berücksichtigen, um proaktiv Gegenmaßnahmen zu entwickeln.

Neben der Implementierung fortschrittlicher Technologien ist die Aufrechterhaltung einer soliden Sicherheitshygiene entscheidend für den Schutz gegen KI-gestützte Angriffe. Dazu gehören regelmäßige Sicherheitsaudits, die Schulung von Mitarbeitern im Umgang mit digitalen Ressourcen und die Etablierung von Richtlinien für eine sichere Nutzung von KI-Tools.

Ein neues Zeitalter der Cybersicherheit

Die Integration von KI in die Cybersicherheit markiert den Beginn eines neuen Zeitalters, in dem die Grenzen zwischen technologischer Innovation und Sicherheitsrisiken zunehmend verschwimmen. Während KI enorme Chancen für die Verbesserung der Cyberabwehr bietet, erfordert sie auch eine sorgfältige Abwägung der Risiken und eine verantwortungsvolle Steuerung. Die Zukunft der Cybersicherheit wird maßgeblich davon abhängen, wie wir diese leistungsstarken Werkzeuge nutzen, um eine sichere und resiliente digitale Welt zu schaffen.

Gregory Guglielmetti

DIE ZUKUNFT VON KI

WERT UND SICHERHEIT

Künstliche Intelligenz (KI) und Automatisierung haben das Potenzial, nahezu unbegrenzte Veränderungen in der Geschäftsdynamik herbeizuführen. Dabei sollten Produkthersteller KI mit Vorsicht und Strategie angehen und Wert und Sicherheit über Entwicklungsgeschwindigkeit stellen

Verantwortungsvolle Implementierung

Vier Veränderungen, die sich zukünftig in vier Schlüsselbereichen ergeben könnten:

#1 Kunden integrieren KI direkt in ihre Automatisierungen

Wenn wir über das Potenzial der KI-gesteuerten Automatisierung nachdenken, besteht das ultimative Ziel darin, die Kraft der Innovation direkt in die Hände der Kunden zu legen. Wir sehen eine Zukunft, in der die Nutzer nicht nur Konsumenten sind, sondern aktive Gestalter. Dieser Trend markiert einen entscheidenden Schritt in der Weiterentwicklung der Unternehmensstrategien, da KI nicht mehr nur als eigenständiges Werkzeug betrachtet wird, sondern als integraler Bestandteil automatisierter Abläufe und deren Optimierung.

#2 Deutliche Verbesserung der Kundenerfahrungen

Bei jedem neuen Automatisierungstool gibt es eine Lernkurve. Traditionell stellt dies eine Barriere zwischen dem Benutzer und einer optimalen Produktivität dar. Mit KI können wir neue Lernprozesse finden, die diese Kurve abflachen und den gesamten Prozess viel angenehmer und benutzerfreundlicher gestalten.

#3 Einsatz von KI zur Optimierung interner Abläufe

KI hat einen transformativen Einfluss auf Unternehmen. Durch die Einbindung von KI-Tools in unsere Arbeitsabläufe haben wir eine neue Ära der Präzision und Effizienz eingeläutet. Es geht nicht darum, weniger Mitarbeiter zu haben, sondern mit den Mitarbeitern mehr und effizienter zu arbeiten. Das Ziel ist es, das Wachstum und die Resilienz durch Fokussierung zu beschleunigen.

#4 Anwendungen von KI in Produktfunktionen

Die Automatisierung richtet sich an ein breites Spektrum von Anwendern: von Fachleuten aus der Wirtschaft über Entwickler bis hin zu IT-Experten und Lösungspartnern. Aktuelle Automatisierungstools werden eingesetzt, um Prozessdokumentation zu übernehmen, Prozesse zu bestimmen und zu überwachen, an Workflow-Designs mitzuarbeiten und vieles mehr. Für fast alle diese Aktivitäten können KI-Funktionen integriert werden, um die Effizienz der Benutzer durch die Nutzung von relevantem Kontext zu optimieren.

www.nintex.de

Identity Access Management

5 BEST PRACTICES ZUR VERBESSERUNG IHRER IT-SECURITY

Identity Access Management (IAM) ist die Verwaltung von Benutzern, Konten und Berechtigungen in Systemen und Anwendungen. Das Ziel ist, diese Berechtigungen auf ein Minimum zu beschränken und rechtzeitig zu entziehen, sobald sie nicht mehr benötigt werden. So können Gefahren wie Privilege Creep (User sammeln mit der Zeit zu viele Berechtigungen an) und Lateral Movement (Hacker bewegen sich anhand der Zugriffsrechte eines gekaperten Benutzerkontos im System weiter) verhindert werden. Allerdings: was genau ein solides IAM-Konzept beinhaltet und wie es umzusetzen ist, bleibt Unternehmen selbst überlassen.

Diese 5 IAM Best Practices bringen Ordnung ins Chaos

#1 Scopes festelgen & Richtlinien definieren

Im ersten Schritt muss festgestellt werden, in welchen Bereichen das IAM-System zur Anwendung kommt: Welche Personen und Gruppen sollen damit verwaltet werden (Angestellte, externe Mitarbeiter, Kunden) und welche Ressourcen (Apps, Cloud-Dienste, Datenbanken, Netzwerke)? Definieren Sie Richtlinien, die für bestimmte Personen, Ressourcen und Gruppen gelten. Klassifizieren Sie Informationen und Dateien („vertraulich", „streng vertraulich", „öffentlich") und bestimmten Sie, wer auf welche Dateien Zugriff haben darf und wer nicht.

#2 Role-based Access Control

Anstatt Usern jede Berechtigung individuell zu erteilen, sollte die rollenbasierte Zugriffskontrolle (engl. Role-based Access Control, RBAC) zur Anwendung kommen. Dabei werden Personen anhand von Attributen (Standort, Abteilungszugehörigkeit, Position) unterschiedlichen Gruppen zugeordnet und erhalten dann auf Grund dieser Zugehörigkeiten bestimmte Berechtigungen. Das spart nicht nur Zeit, sondern reduziert auch die Fehlerquote, die bei der Einzelvergabe entsteht.

#3 Least-Privilege-Prinzip

Das Prinzip der geringsten Privilegien (engl. Principle of Least Privilege, POLP) gibt vor, dass User nur auf jene Informationen, Dateien und Ordnern Zugriff erhalten dürfen, die sie für ihre Arbeit benötigen, und das zu jeder Zeit. Das heißt, Berechtigungen müssen sofort wieder entzogen werden, wenn sie nicht mehr benötigt werden (etwa bei Abteilungswechsel oder wenn eine Person aus dem Unternehmen ausscheidet). Das verhindert nicht nur eine Überberechtigung von Benutzern, sondern reduziert auch die Gefahr von verwaisten Benutzerkonten, die ebenfalls ein Sicherheitsrisiko darstellen.

WAS GENAU EIN SOLIDES IAM-KONZEPT BEINHALTET UND WIE ES UMZUSETZEN IST, BLEIBT UNTERNEHMEN SELBST ÜBERLASSEN.

Helmut Semmelmayer, VP Revenue Operations, www.tenfold-security.com

#4 User Access Reviews

Bei einem User Access Review werden in regelmäßigen Abständen die Zugriffsrechte aller Benutzer überprüft und gegebenenfalls entfernt, um Privilege Creep und verwaisten Benutzerkonten vorzubeugen.

#5 Workflows automatisieren

Um das Least-Privilege-Prinzip umzusetzen und regelmäßige Access Reviews durchzuführen, sowie zur Berechtigungsvergabe mittels Rollen, müssen IT-Administratoren einen beachtlichen Anteil ihrer wertvollen Zeit und ihres Fachwissens aufwenden. Dabei lassen sich Tätigkeiten wie Useranlage, Berechtigungsvergabe, Passwort- und Datenänderungen mit geeigneten IAM-Tools einfach automatisieren. Das spart nicht nur Zeit und Tickets, sondern reduziert auch die Fehlerquote, die bei manueller Berechtigungsvergabe entsteht.

Helmut Semmelmayer

Foto: AD/stock.adobe.com

Digitale Identitäten im Wandel

SICHERHEIT UND AUTONOMIE IN DER VERNETZTEN WELT

– TEIL 2 VON 2 –

Im ersten Teil des Artikels (it security 3-4, Seite 34 oder online) sind wir in die Ansätze des Identitäts- und Zugriffsmanagements und deren Entwicklung hin zu selbstbestimmten Identitäten eingestiegen. Mit diesem Ansatz verändert sich die Art und Weise, wie wir über die digitalen Identitäten denken. Der Endnutzer speichert hier die Verifiable Credentials (VCs) in einer Wallet-App. Im Vergleich zu traditionellen Identitäts- und Zugriffsmanagementansätzen erhält der Nutzer also deutlich mehr Autonomie. Gleichzeitig ergeben sich neue Fragen hinsichtlich der Sicherheitsaspekte von selbstbestimmten Identitäten.

Sicherheit durch Kryptographie

Bei selbstbestimmten Identitäten ist es essenziell, dass diese bestimmte Sicherheitseigenschaften aufweisen, um als vertrauenswürdig zu gelten. Ein wesentliches Merkmal ist die Signatur der ausstellenden Partei (Issuer). Diese stellt sicher, dass die ausgestellten VCs hinsichtlich ihrer Integrität überprüfbar sind und Manipulationen zuverlässig erkannt werden können. Das bedeutet, dass weder der Nutzer noch andere Parteien die Inhalte der VCs unbemerkt ändern können.

Darüber hinaus trägt die Signatur zur Authentizität der VCs bei. Sie ermöglicht es der prüfenden Partei (Verifier), sicherzustellen, dass die Credentials tatsächlich vom angegeben Issuer ausgestellt wurden. Da in der Regel keine direkte Kommunikation zwischen dem Verifier und dem Issuer stattfindet, gibt es für die Glaubwürdigkeit der Signierschlüssel verschiedene Mechanismen: Diese können beispielsweise in vertrauenswürdigen Listen wie der EU Trusted List geführt oder dezentral in einer Blockchain registriert werden. In allen Fällen ist das Vertrauen in die VCs stark abhängig von der Governance

der jeweiligen Liste oder des Systems, die die Schlüssel verwalten.

Im Kontrast zu traditionellen Identitätsmodellen, die auf einem Identity Provider (IDP) basieren, zeichnen sich selbstbestimmte Identitäten durch ihre langfristige Gültigkeit und universelle Einsatzfähigkeit aus, da sie keine spezifische Zielgruppe (Audience) adressieren. Dies ermöglicht es, dieselben Credentials für verschiedene Dienste und Zwecke zu verwenden. Allerdings bringt das auch die Herausforderung mit sich, dass einmal geteilte Daten potenziell vielfach kopiert werden können. Um zu gewährleisten, dass die Credentials ausschließlich der Inhaber der Identität nutzen kann, wird beim Vorzeigen der Credentials meist ein Nachweis erstellt, der bestätigt, dass sie kryptografisch an den Inhaber gebunden sind. Diese sogenannten Verifiable Presentations (VP) sind maßgebend für die Sicherheit selbstbestimmter Identitäten.

Die Erstellung des VPs erfolgt zumeist durch eine zusätzliche Signatur der VCs mit einem privaten Schlüssel, dessen öffentlichen Gegenpart bereits die ausgestellten VCs enthalten. Dieser Prozess stellt sicher, dass der Inhaber der VCs den VP unmittelbar an sich bindet, was die Authentizität und die sichere Nutzung der VCs zusätzlich unterstreicht. Darüber hinaus haben VPs ähnliche Eigenschaften wie die Identitätsdaten, die ein IDP nach erfolgreicher Authentifizierung zu einem Dienstleister sendet: Sie haben eine sehr kurze Laufzeit, gelten nur für eine bestimmte Audience und beinhalten weitere Attribute, um sich vor unberechtigten Zugriffen zu schützen. Zudem nutzen sie Ende-zu-Ende verschlüsselte Transportmedien wie HTTPS für die Datenübertragung.

Schlüsselmanagement als Best Practices

Die in selbstbestimmten Identitäten verwendeten Schlüssel lassen sich an spezifische Geräte binden, um das Sicherheitsniveau weiter zu erhöhen. Ein zentraler Bestandteil dabei ist das Key Management, insbesondere im Kontext von Cloud-Lösungen. Hierbei wird empfohlen, die Schlüssel der Nutzer und die der laufenden Systeme getrennt zu halten (Key Isolation). Dies verhindert, dass Unbefugte die Schlüssel im Falle eines Sicherheitsvorfalls kompromittieren. Zu diesem Zweck kommen Komponenten wie Hardware Security Modules (HSM) und Trusted Execution Environments (TEE) zum Einsatz. In diese sicheren Umgebungen werden die Daten zur Signatur übermittelt, während die Schlüssel selbst in dieser geschützten Umgebung verbleiben, damit sie niemand extrahieren kann.

Ein ähnliches Konzept mit Key Isolation gilt auch für die Nutzer: Die Erstellung von VPs lässt sich ausschließlich mit dem eigenen Smartphone durchführen. Das bedeutet, dass kopierte oder gestohlene VCs ohne das entsprechende Gerät nutzlos sind. Diese Gerätebindung trägt maßgeblich dazu bei, die Sicherheit und Integrität der VCs und VPs zu gewährleisten und stellt einen weiteren Schutzmechanismus gegen unbefugten Zugriff und Missbrauch dar.

Zusätzlicher Schutz

Ein weiterer entscheidender Aspekt im Kontext selbstbestimmter Identitäten ist die Sicherheit der Wallets, die die VCs speichern. Um zu gewährleisten, dass nur der legitime Inhaber Zugriff auf diese Wallet-App hat, kommen Sicherheitsmechanismen wie PIN-Codes und biometrische Verfahren zum Einsatz. Diese Sicherheitsfeatures sind von grundlegender Bedeutung, da sie eine zusätzliche Schutzschicht darstellen. Selbst wenn ein Smartphone verloren geht oder gestohlen wird, verhindern sie, dass unbefugte Personen Zugriff auf die in der Wallet gespeicherten VCs erhalten. Die Verwendung von PINs oder biometrischen Daten wie Fingerabdruck- oder Gesichtserkennung schützt die Wallet-App und die darin enthaltenen sensiblen Informationen vor unberechtigtem Zugriff.

Ich habe mein Passwort vergessen: Was nun?

Traditionelle Identitätsmanagementsysteme bieten häufig die Möglichkeit, Authentifizierungsdaten wie Benutzernamen per E-Mail zuzusenden und Passwörter zurückzusetzen. Diese Funktion erleichtert die Wiederherstellung des Zugangs zu VCs, die IDPs speichern. Das Konzept der selbstbestimmten Identitäten sieht solche Funktionen in der Regel nicht vor, da es keine zentralen IDPs gibt und die VCs jeweils lokal in der Wallet-App gespeichert sind. Das bedeutet, dass herkömmliche Wiederherstellungsmethoden nicht funktionieren. Jedoch bieten die meisten Wallet-Apps eine Backup-Funktion an, die es Nutzern ermöglicht, VCs zu exportieren und mittels Verschlüsselung auf anderen Speichermedien wie Cloud-Services oder lokalen Datenträgern wie Festplatten und USB-Sticks zu sichern.

MEHR WERT

Digitale Identitäten in Deutschland und Europa

Digitale Identitäten (Teil 1 von 2)

Es ist allerdings zu beachten, dass sich VCs, die beispielsweise durch HSM an ein spezifisches Gerät gebunden sind, nicht einfach auf andere Geräte übertragen lassen. Solche VCs muss der Issurer dem Nutzer beim Verlust oder der Migration auf ein neues Smartphone erneut ausstellen. Daher ist eine sorgfältige Abwägung erforderlich, welche VCs an ein Gerät gebunden und welche exportierbar sein sollten. Diese Entscheidung basiert auf dem notwendigen Vertrauensniveau der jeweiligen VC. Beispielsweise müssen staatliche elektronische Identitätsnachweise (eIDs) an Geräte gebunden werden, um ein hohes Vertrauensniveau zu gewährleisten. Für die VCs für Anwendungen mit geringeren Sicherheitsanforderungen, wie Campuszugänge oder Mitgliedschaftsnachweise, ist hingegen auch eine exportierbare Gestaltung möglich. Dies unterstreicht deutlich die Notwendigkeit, Sicherheit und Nutzerfreundlichkeit, die auf dem Schutzbedarf des jeweiligen Anwendungsfalls basiert, abzuwägen.

Umdenken erforderlich

Der Übergang von traditionellen Identitätsmanagementsystemen, die sich auf zentrale IDPs stützen, hin zu selbstbestimmten Identitätsmodellen markiert einen bedeutenden Wandel in der Art und Weise, wie wir über digitale Sicherheit und Datenschutz denken. Die Vorteile dieser neuen Modelle, einschließlich erhöhter Kontrolle und Flexibilität für die Nutzer, sind klar – ebenso wie die Herausforderungen, insbesondere in Bezug auf die Verwaltung der Credentials.

SELBSTBESTIMMTE IDENTITÄTEN GEWINNEN ZUNEHMEND AN BEDEUTUNG UND STEHEN AUF EINER STUFE MIT TRADITIONELLEN IDENTITÄTS- UND ZUGRIFFSVERWALTUNGSSYSTEMEN.

Hakan Yildiz,
IT Architekt, Accenture GmbH,
www.accenture.com

Die Sicherheit der digitalen Identitäten, sei es in traditionellen Systemen oder für selbstbestimmte Identitäten, beruht auf robusten Authentifizierungsmechanismen und vertrauenswürdigen Governance-Strukturen. Während traditionelle Systeme die Wiederherstellung von Zugangsdaten durch standardisierte Prozesse wie Passwortrücksetzungen ermöglichen, erfordern selbstbestimmte Identitätsmodelle neuartige Lösungen wie sichere Wallet-Apps und durchdachte Wiederherstellungsstrategien.

Besonders in Europa ist der Ansatz von selbstbestimmten Identitäten sehr beliebt. Das liegt vor allem an den zahlreichen Mitgliedstaaten und dem Bestreben, einen Authentifizierungs- und Autorisierungsmechanismus zu etablieren, der den Zugang zu Dienstleistern in allen Mitgliedstaaten ermöglicht. Derzeit gibt es mehrere Projekte, die dieses Ziel verfolgen, einschließlich der Large Scale Pilots für digitale Identitäten. Darüber hinaus entspricht die Autonomie für Endnutzer auch den europäischen Werten und dem Vorhaben, Abhängigkeiten von großen ausländischen Technologieunternehmen zu verringern. Ein weiterer Aspekt ist der Datenschutz: Der dezentralisierte Ansatz erschwert das Profiling von Nutzern deutlich. Aus diesen Gründen gewinnen selbstbestimmte Identitäten zunehmend an Bedeutung und stehen auf einer Stufe mit traditionellen Identitäts- und Zugriffsverwaltungssystemen. Für die Akzeptanz der Nutzer ist jedoch ein prinzipielles Umdenken mit Blick auf digitale Identitäten notwendig.

Hakan Yildiz

Distributed Denial of Services

BEDROHUNGSLANDSCHAFTEN IM ERSTEN QUARTAL 2024

Cloudflare hat im ersten Quartal 2024 mit automatisierten Abwehrmaßnahmen bereits 4,5 Millionen DDoS-Angriffe abgewehrt – eine Menge, die 32 Prozent aller DDoS-Angriffe entspricht, die im Jahr 2023 abgewehrt wurden.

HTTP-DDoS-Attacken stiegen um 93 Prozent im Jahres- und 51 Prozent im Quartalsvergleich. DDoS-Angriffe auf der Netzwerkebene(L3/4-DDoS-Angriffe) stiegen um 28 Prozent gegenüber dem Vorjahr und 5 Prozent gegenüber dem Vorquartal.

Insgesamt haben die Cloudflare-Systeme im ersten Quartal 10,5 Billionen HTTP-DDoS-Angriffe abgewehrt. Außerdem bekämpften ihre Systeme mehr als 59 Petabyte an DDoS-Angriffs-Traffic allein auf Netzwerkschicht.

Unter diesen DDoS-Angriffen auf der Netzwerkebene überschritten viele die Rate von 1 Terabit pro Sekunde und zwar fast wöchentlich. Der bisher größte im Jahr 2024 abgewehrte Angriff ging von einer Mirai-Variante des Botnetzes aus. Dieser Angriff erreichte 2 Tbit/s und richtete sich gegen einen asiatischen Hosting-Provider.

www.cloudflare.com

Data Security Posture Management

AM ENDE GEHT ES IMMER UM DATEN

Daten sind im Fokus von Cyber-Kriminellen und sollten deshalb auch im Zentrum der IT-Sicherheit stehen. Diesem Ansatz folgt das Konzept des Data Security Posture Management. Es zielt auf einen effektiven Schutz sensibler Informationen, bringt die herkömmliche IT-Security aber an ihre Grenzen.

Sie versuchen Schadsoftware einzuschleusen, Passwörter zu knacken, oder Mitarbeiter zu täuschen: Cyber-Kriminelle wenden die unterschiedlichsten Taktiken an und kombinieren sie miteinander. Aber egal, welche Einfallstore sie suchen und welche Wege sie einschlagen – am Ende geht es ihnen meist um dasselbe, nämlich an sensible Unternehmensdaten zu gelangen. Sie sind der Zweck ihrer kriminellen Aktivitäten.

Deshalb sollte der Schutz der Unternehmensdaten auch im Mittelpunkt der IT-Sicherheit stehen. Natürlich müssen Einfallstore geschlossen und die Wege dorthin versperrt werden, aber Dreh- und Angelpunkt sollten immer die Daten selbst sein. Dieser Notwendigkeit trägt das neuartige Konzept des Data Security Posture Management (DSPM) Rechnung. Es rückt die Daten ins Zentrum der IT-Security und fordert eine ganzheitliche Absicherung über alle Speicherorte und Kanäle hinweg. Damit bietet es Unternehmen das Fundament, um ihre sensiblen Informationen effektiv vor internen und externen Bedrohungen zu schützen und die Einhaltung von Datenschutzvorschriften zu gewährleisten.

Fünf Kernaufgaben

Um DSPM umzusetzen müssen Unternehmen sich fünf Kernaufgaben widmen:

#1 Daten erkennen,
#2 klassifizieren,
#3 priorisieren,
#4 schützen und
#5 monitoren.

Zweck der Datenerkennung, auch als Data Discovery bezeichnet, ist es, erst einmal herauszufinden, welche Daten bei einem Unternehmen im Umlauf sind und wo sie sich befinden. Logischerweise kann nur geschützt werden, was auch bekannt ist. Wenn alle Daten erfasst sind, müssen sie klassifiziert, also in unterschiedliche Kategorien eingeteilt werden. Darauf basierend können Unternehmen dann einen angemessenen Schutz für jede Kategorie definieren und dabei die sensibelsten Daten mit Priorität schützen.

Zum konkreten Schutz der Daten können Unternehmen Richtlinien aufsetzen, die dafür sorgen, dass sie nicht in einer Art und Weise verwendet werden können, die sie einem Risiko aussetzen. Das kann beispielsweise bedeuten, dass Daten einer bestimmten Kategorie nicht in öffentliche Clouds hochgeladen, auf USB-Sticks gezogen oder ausgedruckt werden dürfen. Mit einem Monitoring müssen Unternehmen die Einhaltung dieser Richtlinien schließlich kontinuierlich überwachen.

Komplexe Systemlandschaften und heterogene IT-Sicherheit

Bei der Ausführung dieser Schritte sind Unternehmen mit einigen Herausforderungen konfrontiert. Eine davon sind die inzwischen äußerst komplexen Systemlandschaften. Unternehmensdaten befinden sich heute buchstäblich überall und bewegen sich durch Kanäle wie Internet, Cloud- und Unternehmensanwendungen, E-Mails und seit neuestem auch verstärkt generativen KI-Tools. Alle diese Daten zuverlässig aufzuspüren ist ohne technische Unterstützung praktisch unmöglich. Dasselbe gilt für die Klassifizierung der Daten. Ihre schiere Menge und die Tatsache, dass sie permanent weiterverarbeitet werden und auch ständig neue Daten hinzukommen, machen die Klassifizierung zu einer echten Sisyphusarbeit, die von Menschen gar nicht mehr bewältigt werden kann.

Beim Schutz der Daten stellen die heterogenen IT-Security-Landschaften eine Herausforderung dar. Unternehmen haben in der Regel viele separate, nicht integrierte Insellösungen im Einsatz. Das ist ineffizient, weil diese verschiedenen Lösungen alle ihre eigenen Managementoberflächen mit individueller Logik mitbringen. Sicherheitsteams müssen deshalb mit viel Administrationsaufwand für jede Lösung ein komplett eigenes Policy Management betreiben. Es birgt auch Risiken, weil die Teams dabei

meist keine identischen Sicherheitsrichtlinien etablieren und durchsetzen können, wodurch kein ganzheitlicher Schutz möglich ist. Darüber hinaus können beim Zusammenspiel von Insellösungen gefährliche Blind Spots und zusätzliche Angriffsvektoren entstehen.

Ganzheitliche Data-Security-Lösungen

Mit herkömmlichen IT-Sicherheits-Tools können Unternehmen kein effektives Data Security Posture Management umsetzen. Dafür sind die erforderlichen Aufgaben zu umfassend und zu komplex. Unternehmen benötigen moderne Data-Security-Lösungen, die Automatismen ermöglichen und einen hohen Integrationsgrad aufweisen.

Solche Lösungen nutzen beispielsweise fortschrittliche Künstliche Intelligenz und Machine Learning für die Erkennung und Klassifizierung von Daten. Sie scannen sämtliche Systeme wie Fileserver, Cloudspeicher, Notebooks und Desktop PCs und klassifizieren die gefundenen Daten mithilfe selbstlernender KI-Modelle. Sie können Beispiele von Unternehmen für schützenswerte Daten analysieren und finden dann selbstständig ähnliche Daten in der gesamten Systemlandschaft. Den Security-Teams entsteht dadurch kein nennenswerter Zusatzaufwand.

Moderne Data-Security-Lösungen vereinen unterschiedliche Security-Technologien, wie zum Beispiel Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), Secure Web Gateway (SWG) und Zero Trust Network Access (ZTNA). Dies ermöglicht die Durchsetzung von Sicherheitsrichtlinien über die komplette System-Landschaft hinweg.

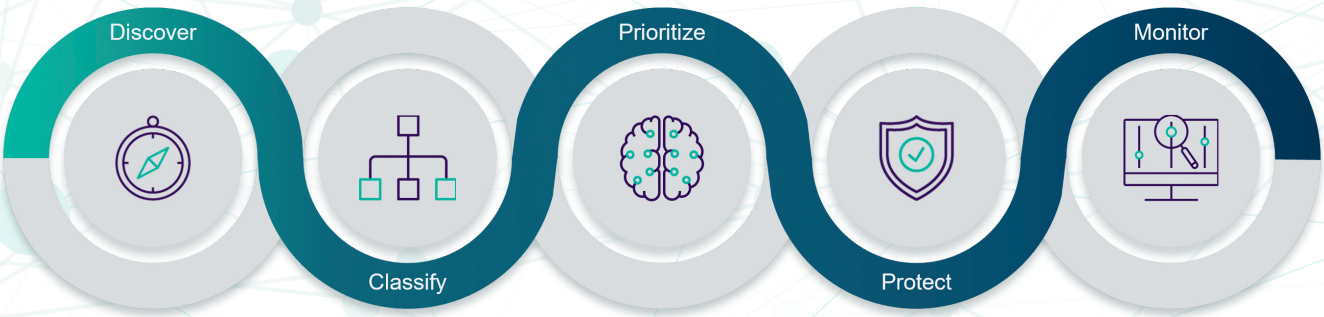
Nicht zuletzt zeichnen sich solche Lösungen durch Risiko-adaptive Ansätze aus, die dem Zero-Trust-Gedanken folgen. Sie geben jedem Mitarbeiter Zugang zu den Daten, die ihm anvertraut sind, analysieren riskantes Verhalten und reagieren darauf mit Maßnahmen, die dem konkreten Kontext angemessen sind. Der Versand bestimmter Daten beispielsweise per E-Mail wird nicht automatisch unterbunden, sondern abhängig vom jeweiligen errechneten Risikowert des Nutzers erlaubt oder blockiert. Der Versand wird nur dann blockiert, wenn sich aus dem Gesamtbild ein erhöhtes Risiko ergibt. Auf diese Weise verhindert das System den Abfluss von Daten, ohne die Produktivität der Mitarbeiter unnötig einzuschränken.

Fabian Glöser

DATA SECURITY POSTURE MANAGEMENT RÜCKT DIE DATEN INS ZENTRUM DER IT-SECURITY UND FORDERT EINE GANZHEITLICHE ABSICHERUNG ÜBER ALLE SPEICHERORTE UND KANÄLE HINWEG.

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

DATA SECURITY POSTURE MANAGEMENT



Data Security Posture Management erfordert die Erkennung, Klassifizierung, Priorisierung, den Schutz und die Überwachung von Daten.

Quelle: Forcepoint

Souveränität der Informationstechnologien

ANTIZIPATION, ÜBERWACHUNG UND INNOVATION

Der Verteidigungs- und Sicherheitssektor hat in vielerlei Hinsicht besondere Anliegen. Doch selbst unter Berücksichtigung der Besonderheiten (Vorschriften, Kontakte, die Länge der Entscheidungszyklen) bei der Entwicklung von Cybersicherheitsangeboten unterscheiden sich die Herausforderungen und Probleme, mit denen der Bereich konfrontiert ist, nicht so sehr von denen zahlreicher ziviler Branchen.

Der ständige Wandel der Cybersicherheit

Ein gutes Beispiel ist der Vergleich zwischen der zivilen und militärischen Luftfahrt, die in dasselbe Spektrum fallen. Die Verteidigungs- und die nationale Sicherheitsindustrie haben sehr langfristige Programme und unterliegen äußerst strengen Anforderungen an die betrieblichen Sicherheitsbedingungen. Während der Laufzeit eines Programms werden sukzessiv neue Entwicklungen in den Bereichen Konnektivität, multimedialer Austausch von Informationen mit dem Boden und Telekommunikation implementiert, die alle ein höheres Maß an Cybersicherheit erfordern. Gleiches gilt für die zivile Luftfahrt, bei der die Lebenszyklen der Flugzeuge ähnlich und regelmäßige Upgrades der Ausstattung erforderlich sind (Cockpit, Kabine, Konnektivität).

Demnach führt die Lebensdauer solcher Programme zu einer technologischen Lücke zwischen dem Beginn der Flugzeugproduktion und dessen Nutzung. Vor 30 Jahren beispielsweise wurde der Aspekt der Kybernetik bei der Entwicklung von Flugzeugen nicht berücksichtigt, da die Verbindung zum Boden nur minimal war. Heute ist jedes Flugzeug – ob zivil oder militärisch – ein Technologiekonzentrat aus einer ganzen Reihe von digitalisierten, gestützten und vernetzten Prozessen. Der hypervernetzte Charakter des Luftfahrtsektors geht mit einer Zunahme des Cyberrisikos Hand in Hand. Das Hinzufügen eines zusätzlichen Anschlusses zu einem Gerät ist vergleichbar mit dem Hinzufügen einer weiteren Haustür: Es erhöht das Risiko des Eindringens.

Um ein weiteres Beispiel zu nennen: Zusätzlich zur Gewährleistung einer Grundkonnektivität werden auch die Bereiche Verteidigung und nationale Sicherheit zunehmend interoperabel. Das ist das Ziel des deutschen BOS-Digitalfunknetzes (BOS = Behörden und Organisationen mit Sicherheitsaufgaben) mit aktuell 5.000 Basisstationen, die bereits 99,2 Prozent der Fläche Deutschlands abdecken. Dieses Netz ist das Rückgrat der operativen Kommunikation im Sicherheits- und Katastrophenschutzbereich und verbindet die Akteure der verschiedenen Dienste miteinander.

DIE NEUEN VORSCHRIFTEN UND RICHTLINIEN TRAGEN AKTIV ZUM SCHUTZ GEGEN DIE RISIKEN VON GEOPOLITISCHEN, INDUSTRIELLEN ODER KOMMERZIELLEN ANGRIFFEN UND SPIONAGE BEI.

Uwe Gries, Country Manager DACH, Stormshield, www.stormshield.com

Bei diesem industriellen Großprojekt mit seinen äußerst kritischen Kommunikationsvorgängen wurden Cyberrisiken natürlich von Anfang an berücksichtigt. Dadurch sollen Störungen, Denial-of-Service-Vorfälle oder sogar das Ausspähen des Netzes während sensibler Vorgänge vermieden und so die Verfügbarkeit, Integrität sowie Vertraulichkeit der Daten gewährleistet werden.

Strategien für die Zukunft

Zu den Herausforderungen der Cybersicherheit, die sich aus der Innovation ergeben, zählen zudem die noch weitgehend unbekannten Aspekte der Quanteninformatik. Die Auswirkungen eines Quanten-Cyberangriffs sind angesichts der potenziell beispiellosen Rechenleistung, die diese Superpositionstechnologie bietet, noch ungewiss. Obwohl einige glauben, dass solche Risiken erst in Jahrzehnten Realität werden, müssen wir unbedingt jetzt damit beginnen, uns darauf vorzubereiten. Genau deshalb berücksichtigen Branchenspezialisten diese Risiken bereits heute in ihren Strategien.

All diese technologischen Entwicklungen machen deutlich, wie wichtig die Cybersicherheit der Systeme ist. Angesichts der steigenden Komplexität und der wachsenden Bedrohung wird sie zunehmend zu einer großen Herausforderung und einer zentralen betrieblichen Notwendigkeit statt nur zu einer Belastung, wie sie Hersteller in diesem Sektor traditionell wahrnehmen.

Goldene Regel für Verteidigung und Sicherheit

In einem sich schnell verändernden technologischen Umfeld gelten für Hersteller, die im Verteidigungs- und Sicherheitsumfeld ein Höchstmaß an Schutz gewährleisten wollen, die drei folgenden goldenen Regeln.

Erstens: Cyberrisiken durch eine schrittweise Verbesserung des Sicherheitsniveaus aller Netz- und Kommunikationsinfrastrukturen sowie sämtlicher IT-Ausrüstungen am Boden und an Bord von Fahr- oder Flugzeugen aller Art vorbeugen.

Zweitens: Eine ständige Überwachung der Entwicklung von Bedrohungen und der auf dem Markt verfügbaren Lösungen für ihre Bekämpfung. Hier spielt die technologische und industrielle Aufklärung, die von vielen Regierungen häufig für wirtschaftliche Zwecke eingesetzt wird, eine wichtige Rolle.

Und schließlich: Innovation im Bereich der Cybersicherheit. Glücklicherweise gibt es in Europa viele lokale Spitzentechnologie-Unternehmen, die über das notwendige Fachwissen verfügen und neben der staatlichen Finanzierung eine Rolle bei der Förderung der Innovation spielen.

Cybersicherheit mit der Unterstützung der öffentlichen Hand

Während die Verteidigungs- und Sicherheitsexperten dieses Dreiergespann von Maßnahmen (Antizipieren, Überwachen, Innovieren) anwenden, regulieren die Behörden die Cybersicherheit, um sie zu einer unabdingbaren Voraussetzung zu machen. Die durch neue Vorschriften wie den neuen IPSec-DR-Referenzrahmen und die NIS2-Richtlinie auferlegten Pflichten sind keine bloße Checkliste: Sie tragen aktiv zum Schutz gegen die Risiken von geopolitischen, industriellen oder kommerziellen Angriffen und Spionage bei.

Die Vorschriften werden weiterentwickelt, um unsere gesamte Wirtschaft auf neue Risiken vorzubereiten, die durch unsere mittlerweile hypervernetzten Umgebungen entstehen. Letztendlich ist das gemeinsame Ziel: die Souveränität unserer Informationstechnologien zu gewährleisten und einen einwandfreien Schutz unserer Infrastrukturen zu garantieren, um Güter und Menschen zu schützen, die unser Land ausmachen. Im Militärumfeld ist dies auch das Ziel des neuen Operationsplans Deutschland (OPLAN DEU).

In dieser Hinsicht stehen die Verteidigungs- und die Sicherheitsindustrie an vorderster Front, da sie eine entscheidende Rolle bei der Aufrechterhaltung der öffentlichen Ordnung und der nationalen Sicherheit spielen. Wenn die nationale Sicherheit und die Verteidigung ins Visier genommen werden, stehen das reibungslose Funktionieren des Staatsapparats und letztlich unserer Volkswirtschaften auf dem Spiel. Durch die Implementierung von Cybersecurity in den Lösungen für das Sicherheits- und Verteidigungssystem und – was noch wichtiger ist – durch eine europäische (souveräne) Form der Cybersicherheit werden wir in der Lage sein, Bedrohungen zu antizipieren und zu innovieren. So wird ein technologischer Vorsprung vor aufstrebenden Bedrohungsakteuren bewahrt, die in einer Cyberumgebung mit zahlreichen Angriffspunkten äußerst aktiv und möglicherweise sogar kriegerisch tätig sind.

Uwe Gries

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:
Stephan Dykgers, Fabian Glöser, Daniel Graßer, Gregory Guglielmetti, Jörg von der Heydt, Philipp Merth, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, André Schindler, Helmut Semmelmayer, Sebastian Weber, Hakan Yildiz

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. 31.
Preisliste gültig ab 1. Oktober 2023.

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, +49-1523-6341255, mann@it-verlag.de

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

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

Erscheinungsweise: 6 x pro Jahr

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

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

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

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

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

RANSOMWARE PROTECTION

26. Juni 2024

Digitalevent

#RansomwareProtection

Mehr erfahren

Eine Veranstaltung von itsecurity & it-daily.net

swissbit®

fido CERTIFIED L1 FIDO2

Made in Germany

iShield Key Pro

Mehr als nur ein FIDO-Stick!

Skalierbar, erweiterbar und anpassbar:

- Unterstützung von FIDO2, HOTP, TOTP, PIV
- Zutrittskontrolle
- Optimal zur Umsetzung von NIS-2-Anforderungen

swissbit.com/ishield-key