INKLUSIVE 80 SEITEN
it security

# it management

Der Motor für Innovation
September/Oktober 2024

THOUGHT LEADERSHIP
AB SEITE 16
appian

TRANSFORMATION AUF SAP S/4HANA

## Denn sie wissen, was sie tun

Patric Dahse, Natuvion

BLACKLINE
SAP Clean Core
ab Seite 22

zscaler
Managed Services
ab Seite 42

SOPHOS
Cybersecurity-Ökosystem
ab Seite 44


itsa EXPO CONGRESS
PLAY HARD.
PROTECT SMART.
HOME OF IT SECURITY
JETZT GRATIS-TICKET SICHERN!
22. – 24. Oktober 2024
Nürnberg, Germany
itsa365.de/itsa-expo-besuchen
NÜRNBERG MESSE



**Ulrich Parthier** **Carina Mitzschke** **Lars Becker**

# HERAUSFORDERUNGEN DER IT

LIEBE LESERINNEN UND LESER,

Gehören Sie auch zu den Unternehmen, deren dringlichstes Problem mal nicht die IT-Security oder SAP-Migration ist? Dann finden Sie sich wahrscheinlich den Einrichtungen zugehörig, deren Fokus aktuell auf NIS2 liegt. Mit der Einführung der NIS2-Richtlinie steht Europa vor einem Paradigmenwechsel in der Cybersicherheit und somit vor großen Herausforderungen. Bis zu Beginn der diesjährigen **it-sa (22. – 24.10.2024)** in Nürnberg, sollten diese Herausforderungen allerdings gemeistert worden sein. Gespräche über NIS2 werden auf der Messe allgegenwärtig sein. Ebenso wie digitale Identitäten und KI-Einsatz, wird auch dieses Thema in unserem it-sa Spezial im Supplement it security von großer Bedeutung sein.

Übrigens sind auch wir wieder live vor Ort. Besuchen Sie uns auf unserem Stand, **Halle 6-208**!

Im Oktober steht aber nicht nur die it-sa an, sondern auch der **DSAG-Jahreskongress**. Neben der kontinuierlichen Zunahme an Cyberbedrohungen, wächst auch die Datenmenge, die Unternehmen verarbeiten und analysieren müssen. SAP unterstützt Anwender dabei, stellt sie aber auch vor neue Probleme – Schlagwort S/4HANA-Migration. Lösungsansätze und neue Strategien dazu, finden Sie in unserem DSAG-Spezial im it management.

Auch wir haben uns neuen Herausforderungen gestellt: Zum einen gibt es seit Juni eine englische Version unserer Online-Plattform it-daily.net. Nebenher modernisieren wir auch unsere technische Infrastruktur und setzen neue Tools ein, um die User Experience für Sie weiter zu verbessern. Zum anderen wird es erstmals neben dem normalen PDF der Printausgabe eine Interactive Edition geben, die mehr Interaktion durch audio-visuelle Inhalte mit den Lesern ermöglichen soll. Sie finden die interaktiven Versionen von it management und it security auf it-daily.net.

Viel Spaß beim Lesen dieser Ausgabe!
Ihr Redaktionsteam



# INHALT

## COVERSTORY

**10** **Transformation auf SAP S/4HANA**
Denn sie wissen, was sie tun

**12** **Einer für alle**
One Data Transformation Approach

## THOUGHT LEADERSHIP

**16** **Erfolg trotz Ungewissheit**
Agile Unternehmensführung mit KI-gestütztem Sales & Operations Planning

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

## DSAG-SPEZIAL

**22** **SAP Clean Core & Standardisierung**
Clean Core Strategie als Business-Booster nutzen

**26** **SAP S/4 und RISE with SAP**
Turbo für die digitale Transformation

**28** **RISE with SAP**
Tipps zur Lizenzoptimierung in der Cloud

**30** **DSAG-Jahreskongress 2024**
Dreiklang der Zukunft

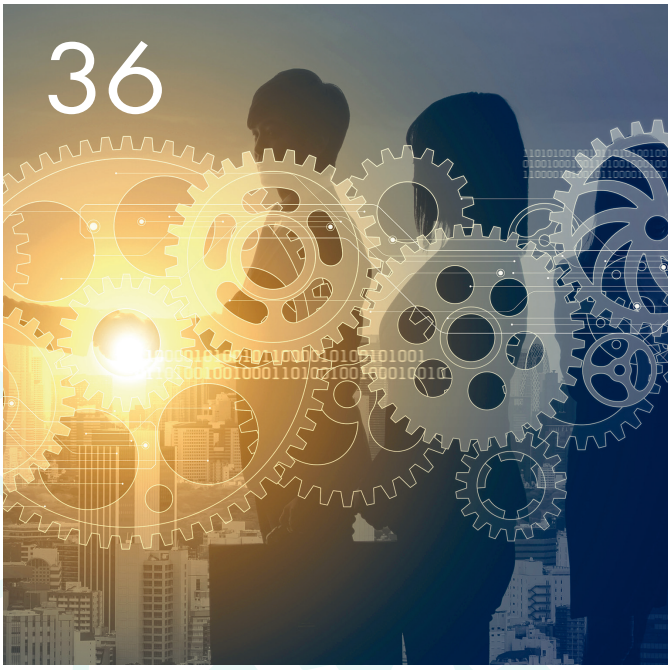
**32** **Workflows für alle S/4HANA-Ausprägungen**
Flexible SAP-Add-Ons

**34** **Synergien freisetzen**
Integration von Onlinemarktplätzen

**36** **Best-of-Breed-Ansatz**
Die wachsende Bedeutung der SAP-Daten- und Prozessintegration

**38** **Fundierte Entscheidungen treffen**
Mit einer Roadmap erfolgreich zum Ziel

**40** **Schlanke und effiziente SAP Brownfield Conversion**
Migration für mittelständische Unternehmen





## IT MANAGEMENT


**42** **Von reaktiver zu proaktiver Sicherheit durch KI**
Neuer Trend in der Cybersecurity

**44** **Cybersecurity-Ökosystem**
Neue Strategien und die Verantwortung der Chefs

**46** **Logistik goes digital**
Digitale Datenintegrationssysteme für mehr Zuverlässigkeit

**48** **IT-Servicemanagement**
Ein Relikt des letzten Jahrhunderts?

**50** **Synergie der Superkräfte**
Wie Edge und Cloud gemeinsam glänzen

**52** **Cloud Computing**
Ein Muss für die Digitale Transformation

**54** **Testdatenmanagement (Teil 5 von 5)**
Durchführen von Tests mit Datenbank-Teilmengen

**58** **SQL, NoSQL, Vektor oder Multimodell?**
Wann und wofür man welche Datenbank braucht

**61** **Die E-Rechnung kommt**
Fünf Best Practices für die Umstellung

**64** **Cloudkostenoptimierung & FinOps**
Wohlfühlen in der Endlosschleife



**Inklusive 80 Seiten it security**

**GUT ZU WISSEN**

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

**WAS WAREN AUS IHRER SICHT DIE TOP-3-EINFLUSSFAKTOREN DER GESTIEGENEN BEDROHUNGSLAGE?**


# CYBER SECURITY

## DIGITALISIERUNG VERSCHÄRFT DIE BEDROHUNGSLAGE

Das Risiko von Unternehmen, Opfer eines Cyber-Angriffs zu werden, bleibt weiterhin hoch. Das ist eines der Ergebnisse der neuen Lünendonk-Studie 2024 „Von Cyber Security zu Cyber Resilience – eine komplexere Bedrohungslage erfordert neue Ansätze."

Die Komplexität der Cyber-Abwehrmaßnahmen nimmt immer weiter zu, da Cyber-Bedrohungen zunehmend sowohl von innen als auch von außen kommen. 71 Prozent der Unternehmen sehen ein erhöhtes Risiko, Opfer einer Ransomware- und/oder Phishing-Attacke zu werden. Diese Gefahr wird durch die technologischen Entwicklungen rund um Künstliche Intelligenz (KI), mit der sich die Qualität der Phishing-Attacken enorm verbessern wird, noch zusätzlich verstärkt. Auch hat die Gefahr durch Insider Threats, also der absichtlichen Weitergabe von Daten oder geistigem Eigentum durch Mitarbeitende, laut der Studie enorm zugenommen: Während zu Beginn des Jahres 2023 noch 37 Prozent der Unternehmen hierdurch eine hohe Bedrohung wahrnahmen, steigt dieser Wert 2024 auf 65 Prozent.

„Durch die zunehmende Vernetzung und immer mehr eingesetzte Software wird die Angriffsfläche für Cyber-Attacken stetig größer und ihre Abwehr immer komplexer. Gleichzeitig gehen Hacker nicht zuletzt durch KI-Unterstützung immer professioneller vor", fasst Mario Zillmann, Partner bei Lünendonk & Hossenfelder, die Entwicklungen zusammen.

Aber auch die verstärkte Nutzung von Cloud-Technologien führt zu einer Verschärfung der Bedrohungslage: 58 Prozent der Befragten sehen in der Cloud-Nutzung ein erhöhtes Cyber-Sicherheitsrisiko. Die befragten Unternehmen identifizieren hier vor allem Handlungsfelder in den Bereichen Datenverschlüsselung und Datenschutz (86 %) sowie Identity & Access Management (85 %). Demgegenüber stehen aber auch 42 Prozent der Studienteilnehmenden, nach deren Einschätzung die Nutzung von Cloud Services zu einer Verbesserung des Security-Levels geführt hat.

**Steigende Investitionen in Sicherheitsmaßnahmen**

Um der Bedrohungslage entgegenzuwirken, investieren Unternehmen weiterhin in ihre Cyber-Sicherheit. 45 Prozent der befragten Unternehmen planen, ihre Ausgaben für Cyber Security um fünf bis zehn Prozent im Jahr 2024 zu erhöhen. Da ein Großteil der Befragten die fortschreitende Digitalisierung als Hauptgrund für die gestiegene Bedrohung sieht, investieren 77 Prozent verstärkt in das Vulnerability Management, um so Schwachstellen in Softwareprodukten frühzeitig zu erkennen und schnell zu beheben.

***www.luenendonk.de***


**AKTUELLE STUDIE**

Die Studie „Von Cyber Security zu Cyber Resilience – Eine komplexere Bedrohungslage erfordert neue Ansätze" entstand in fachlicher Zusammenarbeit mit KPMG und steht ab sofort unter **www.luenendonk.de** zum kostenfreien Download bereit.

# Cybersecurity-Budgets

## EFFIZIENTERE CYBERABWEHR DANK GENAI?

IT-SiG 2.0, BSIG, KRITIS-DachG, NIS2-UmsuCG – allein die Umsetzung von Regulierungsvorschriften für eine bessere Cybersicherheit bindet Ressourcen und Mittel bei Behörden, die sie ebenso dringend für den Ausbau der digitalen Verwaltung benötigen. Hinzu kommt nun eine neue Bedrohungslage, ausgelöst durch den verstärkten Einsatz von generativer Künstlicher Intelligenz (GenAI) durch Cyberkriminelle. Drei Viertel der Fach- und Führungskräfte in deutschen Behörden bestätigen, dass sie mit einer verschärften Situation zu tun haben.

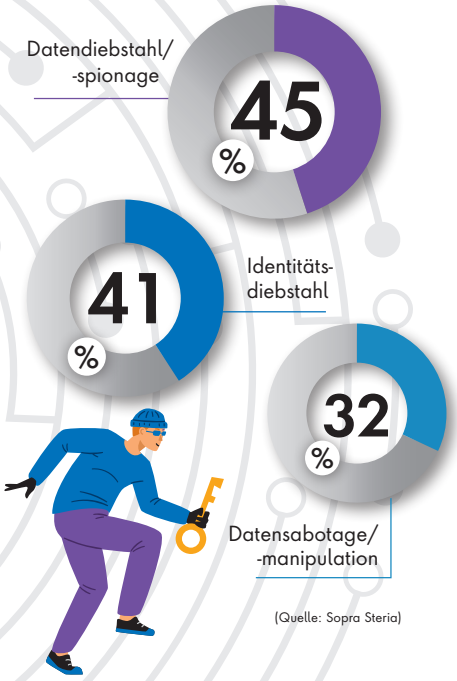
Die Verwaltungen in Deutschland wissen somit, dass sie handeln müssen, werden allerdings durch begrenzte Mittel oder fehlendes Personal gebremst. 70 Prozent nennen fehlende personelle Ressourcen im IT-Bereich, 65 Prozent fehlendes Cybersecurity-Know-how und 50 Prozent die niedrigen Budgets als Hindernisse für eine bessere Cybersecurity, so eine aktuelle Studie von Sopra Steria. Die Angaben liegen deutlich über denen von Unternehmen aus dem Finanzsektor und der verarbeitenden Industrie.


Cybersecurity im Zeitalter von KI

### KI für die Cyberabwehr

Als Effizienz- und Qualitätshebel steht Behörden der Einsatz von zunehmend intelligenter Technologie zur Verfügung. Genauso wie Angreifer für Phishing-Attacken oder das Eindringen in Behördennetzwerke verstärkt auf Sprachmodelle wie FraudGPT setzen, können Behörden legale Versionen dieser Technologien für sich nutzen. „Verwaltungen können beispielsweise Warnmeldungen von KI-Lösungen vorprüfen lassen und so die Zahl von Fehlalarmen reduzieren. Darüber hinaus haben sich GenAI-Tools bereits bei aufwendigen Risikoanalysen bewährt, oder sie helfen im Compliance Monitoring“, so Dr. Barbara Korte, Squad Lead AI @ Cyber Security bei Sopra Steria.

**Welche Szenarien werden infolge der Nutzung von KI durch Cyberkriminelle in den nächsten 12 Monaten am stärksten zunehmen?**




(Quelle: Sopra Steria)

Elf Prozent der befragten Verwaltungen nutzen KI-unterstützte Systeme bereits für die Cybersicherheit. Zum Vergleich: In der Privatwirtschaft ist es etwa jedes dritte Unternehmen. Auf dem Gebiet besteht somit großes Potenzial für die öffentliche Verwaltung, sich effizienter aufzustellen und die Qualität ihrer Cybersecurity-Maßnahmen zu steigern.

***www.soprasteria.de***

# METAVERSE

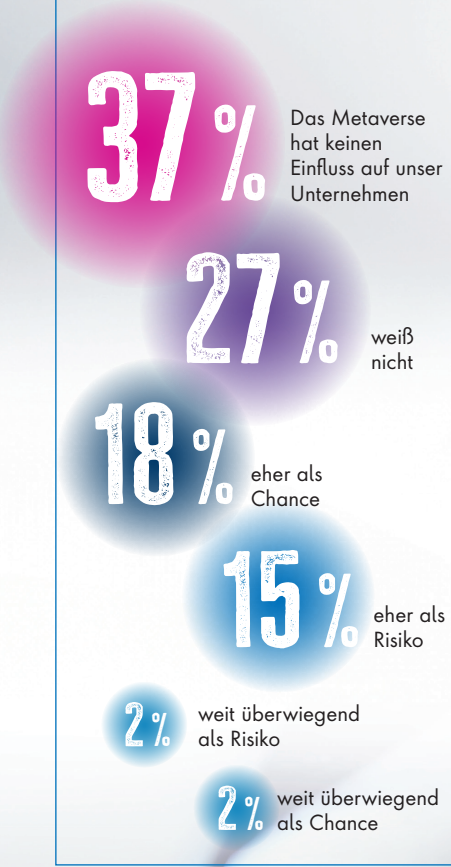
## CHANCE ODER RISIKO?

Beim Metaverse steht die deutsche Wirtschaft noch auf der Bremse. Die Unternehmen sehen in vielen Branchen und Bereichen Einsatzmöglichkeiten, zögern aber, selbst aktiv zu werden.

Jedes zehnte Unternehmen (10 Prozent) gibt an, dass das Metaverse das eigene Geschäftsmodell bedroht, 15 Prozent fühlen sich durch das Metaverse sogar in ihrer Existenz gefährdet. Dennoch will die große Mehrheit (83 Prozent) erst einmal abwarten, welche Erfahrungen andere Unternehmen mit dem Metaverse machen. Das sind Ergebnisse einer repräsentativen Befragung von 605 Unternehmen ab 20 Beschäftigten in Deutschland im Auftrag des Digitalverbands Bitkom.

Als wichtigster Vorteil des Metaverse für die Wirtschaft gilt ganz allgemein eine Verbesserung der Zusammenarbeit innerhalb des Unternehmens (44 Prozent). Die Möglichkeit, neue Produkte oder Dienstleistungen zu entwickeln (43 %), bestehende Angebote anzupassen (12 %). 39 Prozent sagen, dass man im Metaverse auf neue Arten mit Kunden interagieren kann, 15 Prozent, dass dadurch Zugang zu völlig neuen Kundengruppen geschaffen wird. 36 Prozent denken, dass das Metaverse einen nachhaltigeren Ressourceneinsatz ermöglicht und 11 Prozent sehen als Vorteil des Metaverse ein verbessertes Unternehmensimage.

**SEHEN SIE DAS METAVERSE EHER ALS CHANCE ODER ALS RISIKO FÜR IHR UNTERNEHMEN?**




Quelle: Bitkom

### Mehr Anwendungen und Standards gewünscht

Als größte Herausforderung rund ums Metaverse gilt den Unternehmen ein wahrgenommener Mangel an praktischen Anwendungen (76 Prozent). Vor zwei Jahren lag der Anteil noch bei 66 Prozent. 43 Prozent sehen keinen Nutzen für das eigene Unternehmen, 14 Prozent investieren schon in andere Zukunftstrends. Aber auch mit Blick auf die Technologie gibt es Bedenken. Drei Viertel (73 Prozent) halten sie noch nicht für ausgereift, 55 Prozent beklagen ungenügende Standardisierung und für 10 Prozent fehlen externe Dienstleister. Hinzu kommen regulatorische Herausforderungen. So beklagen 67 Prozent Anforderungen an den Datenschutz, 44 Prozent rechtliche Unsicherheiten und einen unklaren Rechtsrahmen sowie 36 Prozent Anforderungen an die IT-Sicherheit.

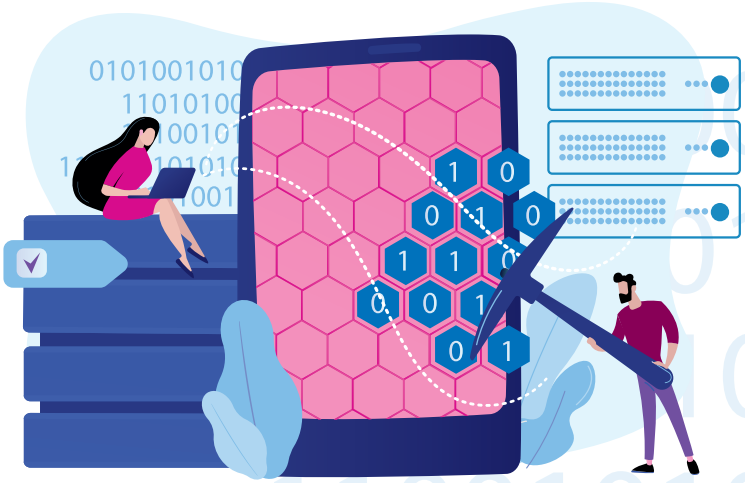
### Das Metaverse ist schwer zu verstehen

Für viele ist problematisch, dass sie das Metaverse noch nicht richtig fassen können. 86 Prozent der Verantwortlichen in den Unternehmen räumen ein, dass es ihnen schwerfällt, den Entwicklungen zu folgen. Drei Viertel (76 Prozent) finden es verwirrend, dass so viele unterschiedliche Anwendungen als Metaverse bezeichnet werden. Und 60 Prozent haben schlicht Probleme, sich das Metaverse vorzustellen. Rund einem Fünftel (19 Prozent) der Befragten macht das Metaverse Angst.

***www.bitkom.org***


**MEHR WERT**

**Wegweiser in das Metaverse**



# Data Mining

## DIE GEHEIMNISSE VON DATENMASSEN

Wenn Daten das Öl des 21. Jahrhunderts sind, sitzen die meisten Unternehmen auf riesigen Vorkommen, die sie allein nicht mehr fördern können. Um aus den wachsenden Datenmassen wirklich wertvolle Erkenntnisse zu gewinnen, brauchen sie effiziente Analysen – wie Data Mining.

Data Mining fasst als Oberbegriff verschiedene Methoden, statistische Prinzipien und Algorithmen zusammen, um Muster und Trends in großen Datenmengen zu erkennen. Diese spezielle Art der Datenanalyse hilft Unternehmen, komplexe Sachverhalte besser zu verstehen, fundierte Entscheidungen zu treffen, Vorhersagen zu machen oder Empfehlungen auszusprechen. Im Kern umfasst das Verfahren vier grundlegende Schritte:

**1. Daten sammeln und aufbereiten:** In einem ersten Schritt werden strukturierte und unstrukturierte Daten aus verschiedenen Quellen wie Datenbanken, Sensoren, dem Internet oder Dokumenten zusammengeführt. Um einen vollständigen und konsistenten Datenpool zu erhalten, müssen die gesammelten Daten anschließend bereinigt werden, was etwa das Entfernen von Duplikaten oder das Ergänzen von fehlenden Werten umfasst.

**2. Daten transformieren:** Im nächsten Schritt werden die zuvor gesammelten Rohdaten in ein für die Analyse geeignetes Format gebracht, das als Grundlage für das spätere Data Mining dient. Dazu gehört etwa die Skalierung der Daten auf einen gemeinsamen Wertebereich, die Umwandlung in eine standardisierte Form und die Erzeugung neuer Features, die bessere Einblicke und Ergebnisse ermöglichen.

**3. Data Mining:** Beim eigentlichen Data Mining kommen Algorithmen und Analysetechniken zum Einsatz, um Muster und Beziehungen in den aufbereiteten Daten zu entdecken. Gängige Techniken sind dabei etwa die Klassifikation, also die Einteilung der Daten in vordefinierte Kategorien, und das Clustering, das ähnliche Daten in Gruppen zusammenfasst. Aber auch das Lernen von Assoziationsregeln, die Vorhersage von Werten auf Basis des Inputs und die Anomalie-Erkennung kommen in diesem Schritt zum Tragen.

**4. Bewertung und Visualisierung:** Abschließend werden entdeckte Muster hinsichtlich ihrer Aussagekraft und Nützlichkeit bewertet. Für eine optimale Präsentation der Ergebnisse eignen sich neben schriftlichen Berichten besonders Diagramme oder Dashboards, um Entscheidungsträgern die Interpretation und Nutzung der oft komplexen Ergebnisse zu erleichtern.

„Data Mining hat bereits in Zeiten von Big Data immer mehr an Bedeutung gewonnen, mit neuen KI-Funktionen zeigt sich allerdings erst das gesamte Potenzial", erklärt Gregor Bauer, Manager Solutions Engineering CEUR bei Couchbase. „Die Grundlage zur Gewinnung wertvoller Insights sind daher leistungsfähige Datenmanagement-Plattformen, die Künstliche Intelligenz, Menschen und Daten zusammenbringen."

***www.couchbase.com***

# Transformation auf SAP S/4HANA

## DENN SIE WISSEN, WAS SIE TUN

Die SAP-Gemeinde stellt sich seit geraumer Zeit die Frage, wie die Transformation auf SAP S/4HANA am besten glücken kann und was es braucht, um den Umzug auf das neue System optimal zu gestalten. Viele Unternehmen schauen denjenigen über die Schulter, die die Transformation bereits durchlaufen haben, um deren Best Practices bei der eigenen Transformation anzuwenden.

Doch sind diese Best Practices und Erfahrungen Einzelner einfach replizierbar? Darüber hat Ulrich Parthier, Herausgeber IT-Management, mit Patric Dahse, CEO von Natuvion, gesprochen.

**Ulrich Parthier:** *Die Transformation auf SAP S/4HANA ist ein hoch aktuelles Thema und es scheint keine leichte Aufgabe zu sein. Immerhin hat SAP seinen Kunden schon mehrfach Hilfestellung gegeben, um endlich die alten Versionen auf End of Life zu setzen. Wie sehen Sie als einer der großen Transformationsdienstleister die aktuelle Lage?*

**Patric Dahse:** Eine SAP S/4HANA Transformation ist kein Spaziergang. Die Altsysteme laufen seit vielen Jahren, sind teilweise in einem extremen Ausmaß individualisiert, schlecht dokumentiert und die Daten sind oft dürftig gewartet. Deswegen haben viele Unternehmen ihre Transformation mit sehr unterschiedlichen, teils unbefriedigenden Ergebnissen durchlaufen. Das zeigt unsere Untersuchung sehr deutlich. Mit 28 Prozent hat über ein Viertel ihr gesetztes Budget zu 10 Prozent überschritten, weitere 24 Prozent haben das Budget sogar um 20 Prozent überzogen. In puncto Zeitüberschreitung ist es bemerkenswert, dass 70 Prozent der Unternehmen ihr Transformationsprojekt um 20 Prozent und mehr überschreiten, bei 45 Prozent sind es sogar 30 Prozent und mehr Zeitüberschreitung. Das kostet nicht nur Geld, es behindert Unternehmen dabei, möglichst schnell mit optimierten Prozessen zu arbeiten.

Alarmierend ist zudem, dass 43 Prozent die Ziele ihrer Transformation nur teilweise oder überhaupt nicht erreicht haben. Wenn ein Unternehmen also nach Best Practices für die eigene Transformation sucht, muss es die anderen 57 Prozent oder einen erfahrenen Spezialisten finden und befragen.

MEHR WERT

Transformationsstudie 2024

**Ulrich Parthier:** *Lediglich 57 Prozent an zufriedenen Unternehmen nach einer Transformation empfinde ich als ein ernüchterndes Ergebnis. Was haben diese Unternehmen richtig gemacht und was ist bei den 43 Prozent schiefgelaufen?*

**Patric Dahse:** In unserer neuen Studie sehen wir, dass die bestehende Situation beispielsweise nicht zu den gesteckten Zielen und ebenfalls nicht zu bereitgestellten Budgets passt. Die meisten entscheidenden Fehler passieren gleich am Anfang, also bei der Planung der Transformation. Diesen Umstand wollten wir genauer untersuchen und haben explizit danach gefragt, wer in der Anfangsphase beteiligt ist. Mit über 37 Prozent sind die Transformationen von der IT-Abteilung am häufigsten initiiert, gefolgt von der Geschäftsführung (29%) und den Finanzen- und Controlling-Spezialisten (24%). Am weiteren Entscheidungsprozess beteiligt sind 44 Prozent die IT-Abteilung, 31% die Geschäftsführung und 26% Finanzen und Controlling. Es besteht kein Zweifel darüber, dass alle Gruppen wichtige Stakeholder in einer Transformation sind, aber nur selten befinden sich erfahrene Transformationsexperten darunter. Das führt dazu, dass sich Fehler in der Startphase exponentiell im gesamten Projektverlauf ausweiten. Ein Resultat ist, dass nur etwas mehr als 13 Prozent der Studienteilnehmer den Zeitplan ihrer Transformation eingehalten haben, was im schlimmsten Fall zu

### ÜBER DIE TRANSFORMATIONSSTUDIE 2024

Im Rahmen einer strukturierten Befragung haben Natuvion und NTT Data Business Solutions 1.259 Führungskräfte in 15 Ländern nach den Erfahrungen aus ihrer letzten IT-Transformation befragt. Die granulare Befragung zahlt auf drei Hauptbereiche ein, damit Unternehmen ihre Transformation besser planen und auf Basis von Best Practices durchführen können: Welche Herausforderungen im Rahmen ihrer Transformation haben die Befragten überrascht? Was würden sie heute anders machen? Haben sie ihre Ziele erreicht, und falls nicht, warum?

Produktionsverzögerungen, Ausfällen und zu einer höheren finanziellen Belastung für die Transformation führen kann.

**Ulrich Parthier:** *Das klingt nach einem Transformations-Management-thema. Was genau sollte das Management vor einer Transformation wissen und welche Herausforderungen sollte es angehen?*

**Patric Dahse:** Wir haben die Befragten dieses wie letztes Jahr gebeten, ihre größten Herausforderungen bei der Planung zu nennen – mit teilweise überraschenden Ergebnissen. Beispielsweise die Komplexität des Gesamtprojekts, letztes Jahr noch mit 41 Prozent auf Platz 1, sank bei der diesjährigen Befragung mit 34 Prozent auf Platz 3. Die Komplexität wurde vom „fehlenden oder ungenügenden Transformations-Know-how" der Mitarbeitenden überholt. Das „fehlende Transformations-Know-how" legte dabei um ganze 6 Prozent zu. Bei der Frage, was im Transformationsprozess am überraschendsten war, antwortete rund ein Drittel mit „Ressourcenknappheit" und „fehlende Erfahrung der Mitarbeitenden mit komplexen Projekten dieser Art". Dies verdeutlicht, dass bei IT-Transformationen kompetente Berater und Mitarbeiter echte Mangelware sind und sich die Situation merklich verschärft.

**Ulrich Parthier:** *Was also raten Sie den Unternehmen und vor allem dem Management?*

> DIE VORBEREITUNG IST DER ENTSCHEIDENDE SCHLÜSSEL ZUM TRANSFORMATIONSERFOLG.
>
> **Patric Dahse, CEO, Natuvion, www.natuvion.com**

**Patric Dahse:** Eine Transformation hat laut unserer Analyse weniger technische Gründe als viel mehr echte Business-Ziele. Die häufigsten Gründe für den Transformationsprozess sind die organisatorische Anpassung mit 36 Prozent, die Einführung neuer Technologien mit 27 Prozent, der Kauf oder die Verschmelzung von Unternehmen oder Unternehmensteilen mit 26 Prozent sowie die Einführung neuer Geschäftsmodelle mit 26 Prozent. Es geht also nicht um ein technisches Update, sondern viel mehr um eine strategische Ausrichtung des Business – und das braucht eine angemessene Zeit, sowohl in der Vorbereitung als auch in der Umsetzung.

Im gleichen Atemzug sollte erwähnt werden, was die Befragten im Transformationsprozess besonders überrascht hat. Fast ein Drittel der Befragten nannte 2023 wie auch 2024 „Probleme mit der Datenqualität". Das sogenannte Housekeeping, also das Kennen, Konsolidieren und Ausmisten der Datenbestände, ist ein entscheidender Schritt in der Vorbereitung einer Transformation, der insbesondere bei großen Unternehmen ohne leistungsstarke Spezial-Tools nicht zu bewerkstelligen ist.

Was ich dem Management von Anfang an rate? Eine sehr gute Vorbereitung inklusive einer realistischen Einschätzung des internen Know-hows, des Zeitrahmens, des verfügbaren Budgets und der Ziele, die durch die Transformation erreicht werden sollen. Die Vorbereitung ist der entscheidende Schlüssel zum Transformationserfolg.

**Ulrich Parthier:** *Vielen Dank für das ausführliche Gespräch Herr Dahse.*

# Einer für alle

## ONE DATA TRANSFORMATION APPROACH

Digitale Transformationen können je nach Systemanbieter, Laufzeit des Altsystems, dem Ziel des Wechsels oder den Anforderungen an die neue Lösung höchst anspruchsvoll sein. Was wäre, wenn jegliche Art von Transformation unter dem Dach einer zentralen Plattform erfolgen würde? Der „One Data Transformation Approach" verfolgt genau dieses Konzept – herstellerunabhängig und hoch flexibel in den Transformationsmethoden.

Wettbewerbsfähigkeit ist für die meisten Unternehmen das A&O und um diese zu erreichen oder beizubehalten, müssen sie sicherstellen, dass sie auf dem neuesten technologischen Stand sind. Ein wichtiger Teil dieser Verbesserungsprozesse ist der Austausch alter Systeme gegen moderne Technologien. Wenn es sich dabei um Kernapplikationen oder führende Systeme handelt, sind meist aufwendige Transformationen nötig. Denn neue Systeme sind mehr als nur eine überarbeitete Softwareversion. Sie beinhalten neue, optimierte Prozesse, die auf das gesamte Datenmanagement im Unternehmen Einfluss haben können.

**Große Würfe der Software- und Systemanbieter**

Um ihre Innovationen im Markt zu verankern, müssen Softwarehersteller die Architektur ihrer Software weiterentwickeln, teils sogar komplett neu designen. Das hat Auswirkungen auf die anwendenden Unternehmen, da Datenstrukturen und Prozesse, die in der alten Software verankert sind, in vielen Fällen nicht einfach übernommen werden können.

Um von den neuen Funktionen, Prozessen und Möglichkeiten in den Applikationen zu profitieren, müssen der Aufbau und die Struktur der Daten umfangreich reorganisiert werden. Ein Beispiel: Noch vor einigen Jahren wurden Informationen über Kunden, Geschäftspartner, Lieferanten oder Mitarbeiter in verschiedenen Applikationen mehrfach erfasst. Das Problem: Die Konsistenz dieser Daten konnte nicht sichergestellt werden. Hatte ein Kunde beispielsweise den Standort gewechselt, war nicht gewährleistet, dass die Adressänderung in jeder einzelnen Applikation erfolgte. Um die Konsistenz dieser verteilten Daten unternehmensweit herzustellen, stellten Unternehmen auf das zentrale Stammdatenkonzept um, das als Basis für die komplette EDV dient. Das Resultat: Alle Applikationen rufen die Stammdaten von einer einzigen zentralen Stelle ab und arbeiten so immer mit dem gleichen Datenbestand.

Dieses sehr vereinfachte Beispiel lässt erahnen, was es bedeutet, wenn man komplexe Applikationen auf ein neues Konzept migrieren möchte. Bei derartigen Transformationen existieren vielfältige Anforderungen, die es zu beachten gilt. Dazu gehören Antworten auf Fragen wie: Welche Datenbestände und in welcher Tiefe habe ich Informationen in meinen Altsystemen? Welche Daten sind wertvoll und welche will ich mitnehmen? Welche Daten kann oder muss ich aus regulatorischen Gründen löschen oder archivieren? Welche Möglichkeiten bietet mir das neue System und welche Daten sind dafür nötig? Möchte ich die Migration nutzen, um gleichzeitig andere Herausforderungen zu lösen, wie beispielsweise eine Datenreduzierung, Qualitätserhöhung der Daten oder die Nutzung von Künstlicher Intelligenz (KI)?

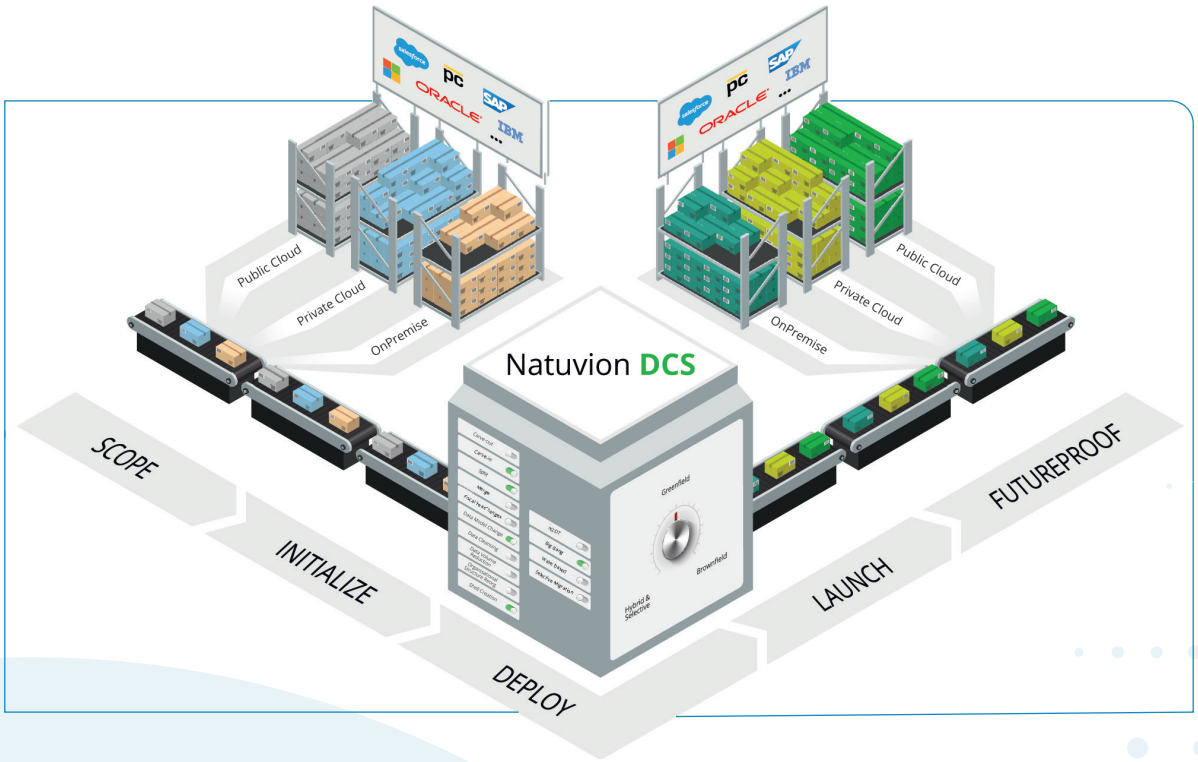
MIT DEM ONE DATA TRANSFORMATION APPROACH PROFITIEREN UNTERNEHMEN VON EINER WEITAUS BREITEREN OPTIONSVIELFALT EINER TRANSFORMATION.

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

Transformationen der Kernsysteme avancieren bei mittelständischen und großen Unternehmen zu gewaltigen Projekten, die teils Jahre der Vorbereitung, Durchführung und Nacharbeit in Anspruch nehmen. Passieren Fehler bereits in der Vorbereitung oder wird auf die falsche Migrationsstrategie gesetzt, verlängert sich das Projekt drastisch. Nicht selten müssen Unternehmen im Transformationsprojekt mehrere Schritte zurückgehen, um diese Fehler zu korrigieren. Ergo ist ein systematisches Vorgehen mit einer intensiven Planung für das gesamte Transformationsprojekt erfolgskritisch.

**Datenmigration – Green, Brown oder bunt?**

Im Laufe der Jahre haben sich unterschiedliche Ansätze zur Datenmigration etabliert. Der Greenfield-Ansatz beispielsweise geht davon aus, dass das Unternehmen eine neue Applikation einführt und mit den Daten und Prozessen auf der „grünen Wiese" komplett neu beginnt. Dieser Ansatz kann der beste sein, bedeutet aber einen sehr hohen Aufwand und erfordert, große Teile der Historie über Bord zu werfen.




Mit dem Brownfield-Ansatz gehen Unternehmen den umgekehrten Weg. Bei dieser Methode übernimmt das Unternehmen alle bestehenden Daten und macht diese lediglich passend. Der Nachteil: Einige moderne Funktionen in den neuen Applikationen können unter Umständen nicht genutzt werden, weil die Daten nicht an die Prozesse angepasst sind.

Bei der selektiven Datenmigration nimmt man mit, was man braucht, und ermöglicht ebenfalls die Nutzung aller neuen Funktionen. Dazu werden Daten und deren Struktur so umgebaut, dass sie von den neuen Systemen und Funktionen genutzt werden können.

**Systemalter beeinflusst Migrationsmethode**

Bereits am Anfang eines Projekts lässt sich anhand bestimmter Eckdaten ableiten, welcher Weg mutmaßlich der vielversprechendste sein könnte. Dieser hängt oft mit dem Alter der Systeme zusammen, wie die aktuelle Transformationsstudie von Natuvion und NTT Data Business Solutions zeigt: Je älter die Systeme sind, desto häufiger wird Greenfield oder die selektive Datenmigration genutzt - je jünger, desto häufiger kommt der Brownfield-Ansatz zum Einsatz.

Der Markt an Migrationsberatern ist groß und reicht von Spezialisten für bestimmte Branchen oder Softwareanbietern bis hin zu Beratungshäusern, die nichts anderes tun als Daten und Systeme von A nach B zu migrieren. Daher findet man in Transformationsprojekten nicht selten mehrere Beratungsunternehmen mit unterschiedlichen Kernkompetenzen. Diese Vorgehensweise erfordert jedoch ein hohes Maß an Koordination und Steuerung, um das gesteckte Ziel im Zeit- und Budgetrahmen zu erreichen.

**Viele Köche oder all in one?**

Der „One Data Transformation Approach" verfolgt einen konträren Ansatz. Der Transformations- und Systemumzugsexperte Natuvion hat mit diesem Verfahren unter intensiver Einbindung des Natuvion DCS (Data Conversion Server) eine flexible Migrationsplattform entwickelt, die alle Migrationsmethoden (Greenfield, Brownfield, Selective, Hybrid) unter einem Dach möglich macht.

Dabei ist es unerheblich, von welcher Quell-Technologie auf welche Ziel-Technologie (SAP, Oracle, Salesforce, Infor, etc.) gewechselt werden soll oder welche Bereitstellungsplattform (On Premises, Public Cloud oder Private Cloud) genutzt wird. Mit dem „One Data Transformation Approach" haben Unternehmen vor allem die Möglichkeit, die Transformation mit weiteren Projekten zu verbinden, die ohne diesen Ansatz separat und meist aufwendiger umgesetzt werden müssten. Damit profitieren Unternehmen von einer weitaus breiteren Optionsvielfalt einer Transformation – unabhängig davon, ob sie im Rahmen ihrer Transformation ein neues Hauptbuch einführen, ihr Fiskaljahr ändern, Änderungen am Datenmodell vornehmen oder sich dazu entscheiden, ihre Transformation in Wellen oder nahezu ohne Downtime durchzuführen. Mit dem One-Data-Transformation-Ansatz bekommen Organisationen die Methodik, Werkzeuge und Erfahrung für ein sehr großes Aufgabenspektrum an die Hand.

Es ist davon auszugehen, dass Softwarefunktionen in Zukunft weniger entscheidende Erfolgsfaktoren sind. Viel mehr werden ein großes Angebot an innovativen Plattformen und vor allem KI entscheidend zur Veränderung und zum Erfolg beitragen. Erfolgskritisch sind allein die Daten und deren Verfügbarkeit. Daher gilt es die Daten schnell, einfach und sicher auf jeder neuen Plattform verfügbar zu machen.

***Philipp von der Brüggen***
***www.natuvion.com***

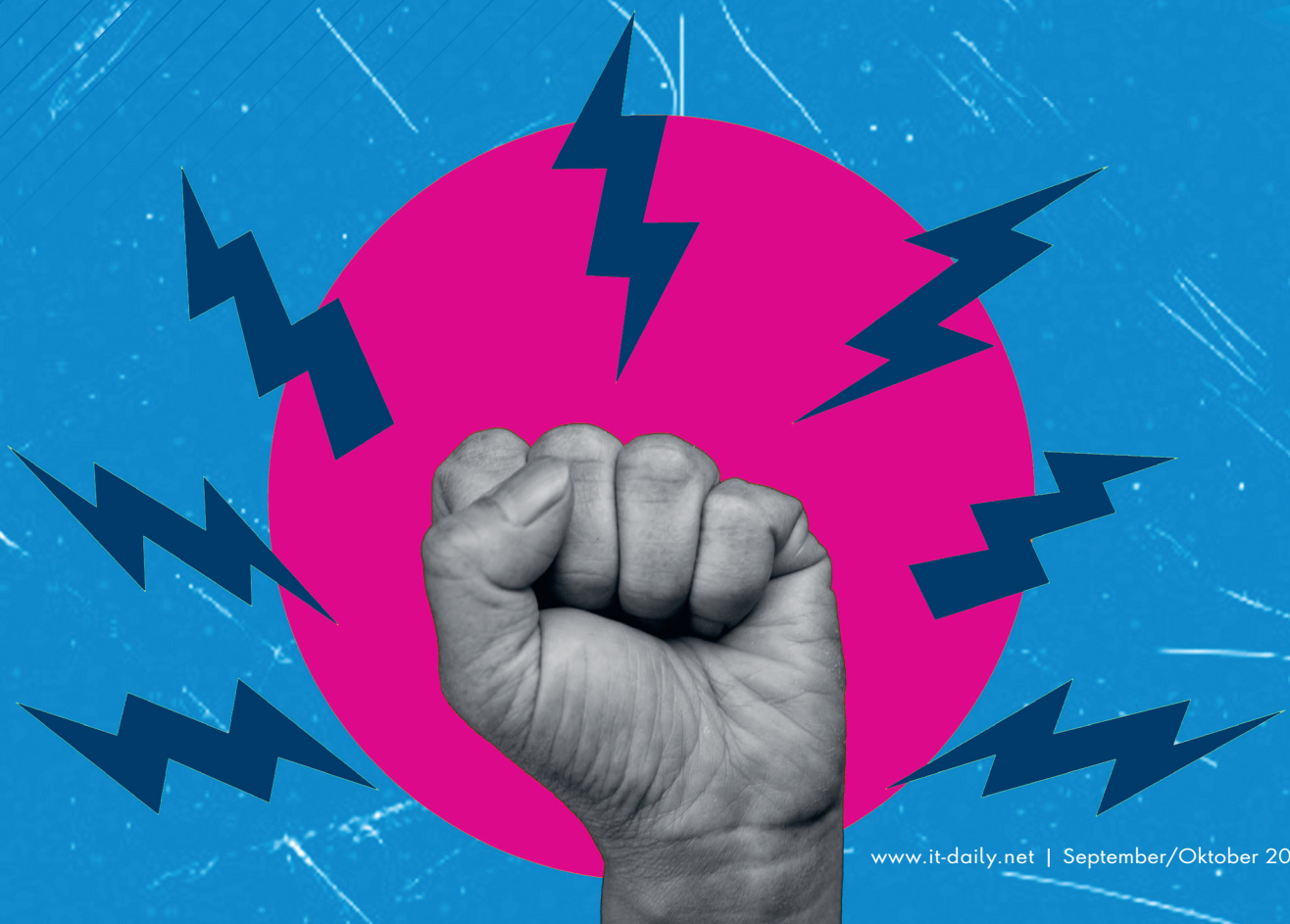
# A leader is one who knows the way, goes the way, and shows the way.

John C. Maxwell

# ÜBERRASCHUNGS-RESISTENT

**Die globale Wirtschaft steht vor beispiellosen Herausforderungen. Seit Jahren, besonders aber seit 2020, erschüttern Krisen und unvorhersehbare Ereignisse die Geschäftswelt. Die Liste der Störfaktoren scheint endlos. In diesem Chaos zeigt sich deutlich: Altbewährte Methoden und starre digitale Lösungen reichen nicht mehr aus. Unternehmen brauchen neue, flexible Ansätze, um Plötzlichkeit zu managen.**

**Doch wie können sie sich anpassen und ihre Strategien neu ausrichten, um in einer Welt voller Überraschungen erfolgreich zu sein?**



# Erfolg trotz Ungewissheit

## AGILE UNTERNEHMENSFÜHRUNG MIT KI-GESTÜTZTEM SALES & OPERATIONS PLANNING

In den letzten Jahren haben komplexe internationale Lieferketten und unterbrochene Handelsströme die Wirtschaft immer wieder vor schwerwiegende Herausforderungen gestellt. Vor allem seit 2020 befinden sich viele Unternehmen im Krisenmodus: Eine globale Pandemie, die Havarie der Ever Given im Suez-Kanal, Krieg auf dem europäischen Kontinent, zunehmende Handelsspannungen zwischen den USA und China – diese und andere Ereignisse haben gezeigt, wie sensibel Lieferketten sind und was passieren kann, wenn sie unterbrochen werden. Unvorhersehbare Situationen benötigen neue Lösungen, die noch nicht existieren, damit Unternehmen weiterhin am Markt erfolgreich bleiben können. Ein statistisches Forecasting – also Vorhersagen aus der Vergangenheit abzuleiten – ist nicht mehr zielführend, um Angebot und Nachfrage mit der Unternehmensstrategie in Einklang zu bringen.

Wir befinden uns bereits in einer hochgradig digitalisierten Welt. Wieso stellen unerwartete Situationen dann trotzdem einen so hohen Störfaktor dar? Die digitalen Lösungen, die heute eingesetzt werden, sind oft zu starr und ohne Erfahrungswerte, um auf solche nie vorher eingetretene Situationen agil reagieren zu können. Oft bleibt eine Abstimmung zwischen vielen Abteilungen über das Verfahren zur weiteren Planung unerlässlich. In den letzten Jahrzehnten haben Unternehmen ihre Investitionen in digitale Vermögenswerte zwar massiv gesteigert, jedoch ist dabei die Produktivität nicht gestiegen. Die Investitionsstrategien müssen also überdacht werden – die Zukunft erfordert eine Unternehmenssteuerung, die den Mehrwert innerhalb der Wertschöpfungskette neu definiert.

**Verknüpfung von Menschen und Prozessen**

Das moderne Unternehmen ist ein Zusammenspiel zwischen Menschen, Daten, Assets und Technologien. Je größer das Unternehmen, desto schwerer ist es, sie alle zu koordinieren. Neue Produkt-Launches, Marketingkampagnen, Produktionsplanung unter Berücksichtigung von Wartungsintervallen – die Optimierung von Vertriebs- und Produktionsprozessen umfasst viele Unternehmenssegmente. Komplexe und schwer nachvollziehbare Prozesse sind Sand im Getriebe eines Unternehmens.

Vor allem im Bereich der Geschäftsplanung ist es herausfordernd, messbare

Werte und Ergebnisse aus einem komplexen Zusammenwirken zu ziehen. Dabei ist es essenziell, dass die relevanten Mitarbeitenden solche Ergebnisse für ihre Entscheidungen vorliegen haben. Dafür müssen alle Abteilungen verknüpft werden: Produktmanagement, Vertrieb, Zulieferer, Produktion, Marketing, Finanzen, Unternehmensleitung. Sie alle nutzen eine Vielzahl von Tools, daher ist eine koordinative Unterstützung gefragt, zum Beispiel in Form von künstlicher Intelligenz. Gleichzeitig müssen getroffene Maßnahmen stets nachvollziehbar bleiben.

**Der Missing Link:**
**Sales & Operations Planning**

Um dieses Beziehungsgeflecht zu entwirren und den Mitarbeitenden verlässliche Entscheidungsgrundlagen zu bieten, braucht es ein Bindeglied. Dieses Bindeglied muss es ermöglichen, Angebot und Nachfrage optimal aufeinander abzustimmen – und zwar agil. Hier kommt Sales & Operations Planning (S&OP) ins Spiel.

S&OP ist ein fortschrittlicher strategischer Geschäftsprozess, der Vertriebsprognosen mit operativen Plänen in Einklang bringt, um eine effektive Ressourcenallokation zu gewährleisten, sodass Unternehmensziele erreicht werden. Dieser Ansatz kann die Leistungsfähigkeit der KI nutzen, um die Genauigkeit von Prognosen zu verbessern, Entscheidungsprozesse zu optimieren und die funktionsübergreifende Zusammenarbeit zu fördern.

Technologische Lösungen im Bereich S&OP, wie beispielsweise eine Data Fabric, legen ein Layer zwischen die einzelnen Unternehmensbereiche und der Basis an Tools und Datenbanken. Sie decken das gesamte Spektrum an Unternehmensanwendungen ab – vom Produktreview bis zum Executive Meeting.

**Viele Schritte für ein S&OP – wenige für die Mitarbeitenden**

Wie ein S&OP in der Praxis funktioniert, lässt sich an den drei folgenden Anwendungsbeispielen konkretisieren:

➤ Die Abteilung Produktmanagement plant ein neues Produkt-Release. Das entsprechende Planungstool informiert die Vertriebs-, Marketing und Lager-Teams darüber, den Bestand der aktuellen Produktversion abzuverkaufen, um die Kapitalbindung am schwerer verkäuflichen Altbestand zu minimieren.

➤ Die Marketingabteilung bereitet eine große Werbekampagne vor. Auch hier übermittelt das Planungstool im Vorfeld den Teams von Sales, Supply Chain, Logistik und Produktion entsprechende Informationen, damit sie auf die abzusehende Spitze im Nachfragevolumen optimal reagieren können.

➤ Ein Lieferant meldet Lieferprobleme. Über eine entsprechende Anwendung im Planungstool werden die Aufgaben an die betroffenen Abteilungen delegiert, damit sie Entscheidungen darüber treffen können, ob etwa ein alternativer Lieferant oder ein schnellerer und kostenintensiverer Transportweg die bessere Wahl für das weitere Vorgehen ist.

Je nach Position, in der sie sich in dem System bewegen, erhalten die Mitarbeitenden individuell relevante Erkenntnisse. Dabei aggregiert die S&OP-Prozessanwendung nicht nur Daten, sondern bringt durch die Implementierung von KI neue und maßgeschneiderte Logiken ein. Dieser Prozess ermöglicht die Erzeugung von Bestands-, Vertriebs-, Logistikanalysen und andere Statusberichte aller relevanten Prozesse und hält alle relevanten Stakeholder informiert.

Im nächsten Schritt erfolgt die Erstellung von Prognosen, die auf den gesammelten Daten basieren. Sie sind nicht statisch, sondern werden regelmäßig dynamisch überprüft und angepasst, um auch spontane Veränderungen im Markt oder in der Nachfrage zu berücksichtigen. Das ermöglicht es jedem Anwender und jeder Anwenderin, mit minimalem Aufwand einen smarten und ganzheitlichen Überblick über alle für den jeweiligen Prozess relevanten Informationen zu erhalten und vereinfacht die üblicherweise schwierige Abstimmung zwischen Unternehmensteilen.

Integriert in eine End-to-End-Prozessautomatisierungsplattform, wie die Appian Plattform, wird so die Durchführung der gesamten Prozesskette im Unternehmen für ein effizientes S&OP ermöglicht. Zentral ist hier das Zusammenspiel von Mensch und KI. So erhält zum Beispiel ein Bedarfsplaner von der KI die Warnung zu einer Anomalie im Forecast. Die Entscheidungshoheit liegt jedoch beim Menschen – dieser kann im Bedarfsfall manuell eine Anpassung des Forecasts vornehmen.

**Vorteile der Verbindung von S&OP und KI**

Die Integration von KI in den Prozess einer Sales & Operations Planung bietet zahlreiche Vorteile. Zunächst einmal ermöglicht sie eine deutlich verbesserte Prognosegenauigkeit. KI-Algorithmen können große Datenmengen analysieren

und Muster erkennen, die für menschliche Planer oft nicht erkennbar sind. Dies führt zu präziseren Vorhersagen des Kundenbedarfs und ermöglicht eine effektivere Bestandsplanung. Unternehmen können so ihre Lagerbestände optimieren, was zu einer Reduzierung des gebundenen Kapitals und einer Verbesserung der Liquidität führt.

Ein weiterer Vorteil von S&OP mit KI ist die Möglichkeit zur Szenarioplanung und -analyse. KI-gestützte Systeme können verschiedene „Was-wäre-wenn"-Szenarien durchspielen und deren Auswirkungen auf die gesamte Lieferkette simulieren. Diese Vorgehensweise ermöglicht es Unternehmen, besser auf jede Art von Eventualität vorbereitet zu sein und flexibler auf Marktveränderungen zu reagieren. Die Fähigkeit, schnell und fundiert auf Veränderungen zu reagieren, kann einen entscheidenden Wettbewerbsvorteil darstellen.

S&OP IST EIN FORTSCHRITTLICHER STRATEGISCHER GESCHÄFTSPROZESS, DER VERTRIEBSPROGNOSEN MIT OPERATIVEN PLÄNEN IN EINKLANG BRINGT, UM EINE EFFEKTIVE RESSOURCENALLOKATION ZU GEWÄHRLEISTEN.

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

Zudem wird sichergestellt, dass alle Unternehmensbereiche informiert gehalten werden und für nötige Entscheidungen die dafür relevanten Informationen per Aufgabenkoordinierung den Organisationseinheiten bereitgestellt werden.

**Kollaboration vereinfachen, Transparenz steigern**

Die Implementierung technologischer Lösungen mit KI für S&OP führt auch zu einer verbesserten funktionsübergreifenden Zusammenarbeit. Traditionell arbeiten verschiedene Abteilungen wie Vertrieb, Produktion und Finanzen oft in Silos, was zu Ineffizienzen und Fehlplanungen führen kann. KI-gestützte Systeme fördern die Zusammenarbeit, indem sie eine einheitliche Datenbasis schaffen und Prozesse automatisieren. Dies ermöglicht eine bessere Abstimmung zwischen den Abteilungen und führt zu kohärenten Planungsentscheidungen.

Darüber hinaus helfen die technologischen Lösungsansätze mit KI im Bereich des S&OP, eine erhöhte Transparenz und Sichtbarkeit in der gesamten Lieferkette zu schaffen. Moderne Prozessautomatisierungsplattformen ermöglichen es Stakeholdern, den aktuellen Status verschiedener Planungs- und Betriebsfragen einzusehen, einschließlich der Verantwortlichkeiten und erwarteten Lösungsfristen. Diese Transparenz fördert das Verantwortungsbewusstsein und ermöglicht eine schnellere Problemlösung.

Ein weiterer wichtiger Aspekt ist die Möglichkeit zur automatisierten Ausnahmebehandlung und Problemlösung. KI-Systeme können Abweichungen vom Plan schnell erkennen und entsprechende Maßnahmen einleiten. Das kann von der automatischen Anpassung von Produktionsplänen bis hin zur Benachrichtigung relevanter Entscheidungsträger reichen. Diese Fähigkeit zur proaktiven Problemlösung minimiert Unterbrechungen und verbessert die Gesamteffizienz des S&OP-Prozesses.

**Prozessexzellenz durch KI-gestütztes S&OP**

Die Auswirkungen eines effektiven S&OP-Prozesses mit KI auf die Unternehmensleistung sind beachtlich. Forschungen zeigen, dass Unternehmen mit einem gut implementierten S&OP-Prozess ein oder zwei zusätzliche Prozentpunkte beim EBIT erzielen im Vergleich zu Unternehmen, die dies nicht haben. Ebenso sind ihre Frachtkosten und Kapitalintensität 10 bis 15 Prozent niedriger und sie haben 40 bis 50 Prozent weniger Vertragsstrafen und entgangene Umsätze bei ihren Kunden. Zudem können sie die Produktivität ihrer Planer um 10 bis 20 Prozent steigern.

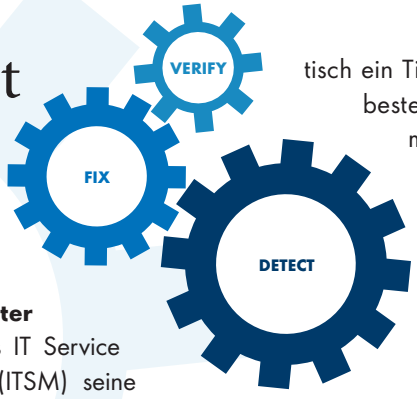
All diese Potenziale schreien förmlich nach der Implementierung eines S&OP. Der praktischen Umsetzung waren bislang durch komplexe Datenanbindungen über Drittsysteme und technische Limitierungen in der Abbildung von Prozessvariationen oft enge Grenzen gesetzt. Ein mit KI technologisch gestütztes S&OP macht das Angehen dieser komplexen Problemstellung endlich möglich und hilft, große Effizienzen zu heben. Es ermöglicht eine präzisere Prognose, eine verbesserte funktionsübergreifende Zusammenarbeit, eine erhöhte Agilität und letztendlich eine Steigerung der Unternehmensleistung.

In einer zunehmend komplexen und volatilen Geschäftswelt wird dies zu einem entscheidenden Faktor für den Unternehmenserfolg und die Wettbewerbsfähigkeit. Mit einem Partner wie Appian lässt sich so Prozessexzellenz erzielen, um in einer sich ständig wandelnden und weiterentwickelnden Geschäftswelt erfolgreich zu bleiben.

***Fabian Czicholl***

# IT Service Management

## WIE MAN SCHWACHSTELLEN EFFIZIENT PRIORISIERT UND BEHEBT




Die zunehmende Masse an Schwachstellen können die meisten Unternehmen nicht mehr bewältigen – aufgrund des Mangels an Personal, Ressourcen und Know-how. Tools für ein risikobasiertes Schwachstellenmanagement (RBVM) helfen hier bei der Einschätzung welche Verwundbarkeiten mit welcher Priorität zu bearbeiten sind. Doch wie lassen sich die Aufgaben effizient auf die beteiligten IT-Teams verteilen und umsetzen?

**it-sa Expo&Congress**

Besuchen Sie uns in **Halle 7–610**

**ITSM als Booster**

Hier spielt das IT Service Management (ITSM) seine Stärken aus, in dem es Security, Operations und Entwickler eng aneinander bindet: Das RBVM-Tool übermittelt Informationen zu Schwachstellen mit hohem Risiko-Score automatisch an Ivanti Neurons for ITSM. Dessen Incident Management Modul verbindet die aktuellen Events mit dem Asset und Configuration Management. Die IT erhält so ein klares Lagebild, welche Server, Clients oder Switches Schwachstellen aufweisen.

Je nach Bewertung und aktiver Ausnutzung steuert die ITSM-Lösung automatisch ein Ticket für das Aufspielen eines bestehenden Patches an den Administrator. Ist ein solcher Patch noch nicht verfügbar, erhält das Developer-Team per ITSM den Auftrag zu dessen Entwicklung.

Mit Hilfe dieser fortschrittlichen DevSecOps-Integration durch das ITSM-System als zentralem Management-Hub lässt sich die Behebung von Schwachstellen weitgehend automatisiert starten und deutlich effizienter durchführen. Danach geht auch das Feedback zur behobenen Schwachstelle automatisch von Dev über ITSM zum RBVM, um den Vorgang abzuschließen.

***www.ivanti.com***

# DIE GENERATIVE KI IST DA!

## GEKOMMEN UM ZU BLEIBEN

Generative KI ist in der Lage Texte, Bilder, Videos oder andere Daten mithilfe von Modellen zu erzeugen. Diese lernen die Muster und die Strukturen der eingegebenen Trainingsdaten und erzeugen dann neue Daten mit ähnlichen Merkmalen.

Anwendungsgebiete gibt es quasi in allen Bereichen und somit natürlich auch in der IT. Entscheidend ist, welchen Nutzen und welche Vorteile sie bringt. Dazu stellen sich die Fragen nach dem Wie, Wo und Wann – also den typischen W-Fragen.

Im neuen, frischen Look konzentrieren wir uns auf die praktischen Anwendungen von KI und lassen dabei ethische Debatten oder Spekulationen über Jobverluste außen vor. Unser eBook bietet Trends, Anwendungen, praxisnahe Tipps und Expertenwissen. Ideal für alle, die die Zukunft der KI gestalten wollen.

**AUS DEM INHALT:**

- KI in der Produktion
- Eine IT-Welt ohne Apps oder dooch nicht?
- IT Servicemanagement Tools
- Effiziente Datenkontrolle in der KI-Ära
- Generative KI? Aber sicher!


Das eBook umfasst 46 Seiten und steht zum **kostenlosen** Download bereit.

# HYPERCONVERGED INFRASTRUCTURE (HCI)

## VMWARE-ALTERNATIVEN BRINGEN SICH IN STELLUNG

Die Server-Giganten erneuern ihr VMware-Bündnis, doch HPE plant einen eigenen Hypervisor-Move. Was bedeutet das für die Zukunft von Hyperconverged Infrastructure?

Kürzlich haben die drei führenden Server-OEMs Dell, Lenovo und HPE ihre Verträge mit VMware verlängert, die zuvor ausgelaufen waren. Dadurch können sie weiterhin Hyperconverged-Systeme und Server mit vorinstalliertem VMware-Stack verkaufen. Dies war ein notwendiger Schritt, da diese OEMs keine eigenen Hypervisoren besitzen, um ihre HCI-Lösungen zu unterstützen. Auf der HPE Discover wurde jedoch eine KVM-basierte Eigenentwicklung von HPE erwähnt, die auf Unternehmens- und Rechenzentrumslösungen abzielt.

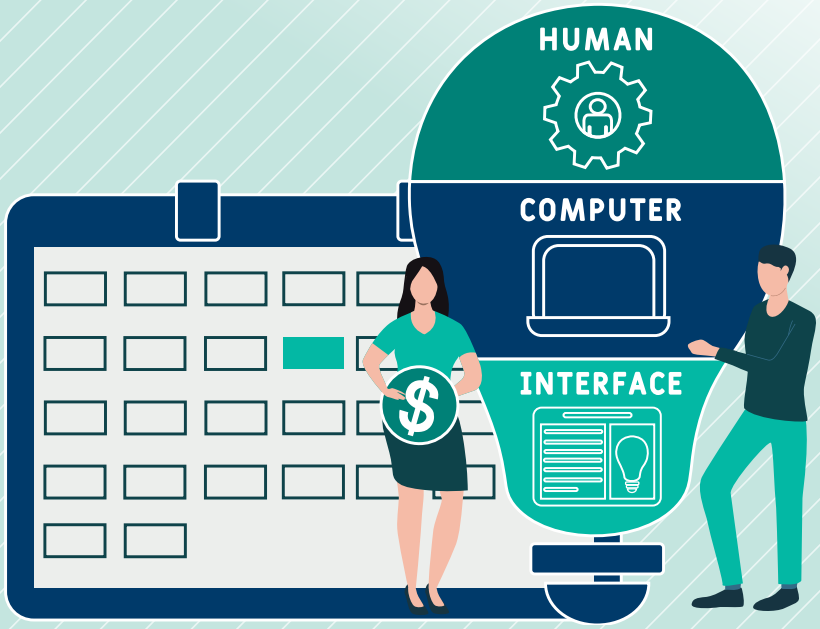
Nach der Übernahme von VMware hat Broadcom das Lizenzmodell für VMware-Produkte geändert und somit die Preise erhöht. Für Kunden, die nach Alternativen suchten, ist dies keine gute Nachricht, da sie nun mehr für integrierte HCI-Lösungen zahlen müssen. Darüber hinaus zweifeln viele Kunden nach der Übernahme an der zukünftigen Unterstützung und Weiterentwicklung von VMware-Produkten, was entscheidende Faktoren für weitere Investitionen in HCI sind. Viele Kunden suchen daher aktiv nach Alternativen für ihre Edge-Daten- und KMU-Anwendungsfälle.

**Der Markt für HCI wächst weiter**

Der Markt für Hyperconverged Infrastructure (HCI) ist in den letzten zehn Jahren kontinuierlich gewachsen und wächst weiter. Es gibt viele aktive Installationen, und sowohl die OEMs als auch Broadcom/VMware sind daran interessiert, diese aktiven Verträge nach ihrem Auslaufen zu verlängern. Der Markt ist jedoch in Bewegung geraten, und Wettbewerber wollen die Gelegenheit nutzen, um End-of-Life-Server mit ihren eigenen Installationen zu ersetzen. Viele Kunden sind nach der Preiserhöhung offen für alternative Lösungen und suchen aktiv danach. Dies betrifft alle Branchen und Unternehmensgrößen, insbesondere aber viele KMUs und den Bereich Edge-Computing, wo hyperkonvergente Systeme kleinere Zweigstellen abdecken.

**Kunden haben drei Alternativen**

Kunden mit VMware-basierten HCI-Systemen haben im Wesentlichen drei Möglichkeiten: Sie können bei VMware bleiben, sich dem neuen Lizenzmodell anpassen und die höheren Preise zahlen. Alternativ können sie zu einer anderen Appliance eines HCI-Anbieters mit einem integrierten Stack wechseln, was günstiger sein könnte. Drittens können sie zu einer alternativen softwaredefinierten Lösung wechseln, die auf neuen oder vorhandenen Servern installiert werden kann. Diese Lösungen umfassen einen Hypervisor, ein fortschrittliches virtuelles Netzwerk und eine Speichersoftwareschicht. Analysten beobachten bereits einen deutlichen Anstieg des Interesses an solchen Speicher- und Rechenarchitekturen.




**Positionierung**

Für VMwares Konkurrenten ist dies eine erstklassige Gelegenheit, Kunden zu gewinnen, die Alternativen für ihre End-of-Life-HCI-Systeme suchen. Gartner schätzt, dass VMwares Konkurrenten ihren Marktanteil von derzeit 30 Prozent auf 60 Prozent im Jahr 2029 erhöhen werden. Eine vielversprechende Option sind softwaredefinierte Lösungen, die direkt auf neuen oder vorhandenen Servern installiert werden können. Diese Lösungen bieten nicht nur Optionen für Kunden, sondern auch für Hardware-Partner, die mit einem günstigeren Software-Stack niedrigere Paketpreise anbieten können. Partnerschaften wie die zwischen StorMagic und HPE sowie Lenovo existieren bereits.

***Tobias Pföhler | www.stormagic.com***

# DSAG SPEZIAL

**Transformation ist der entscheidende Erfolgsfaktor in der Geschäftswelt. Der DSAG-Jahreskongress 2024, vom 15. bis 17. Oktober in Leipzig, greift dieses Thema unter dem Motto „Dreiklang der Zukunft: Anwender, SAP und Partner als Taktgeber der Transformation" auf. Im Mittelpunkt stehen die digitale Transformation, Cloud-Technologien und KI. SAP treibt mit „RISE with SAP" und „GROW with SAP" zudem die Cloud-Migration voran. Darum geht es auch auf den folgende Seiten des DSAG Spezials.**

# SAP Clean Core & Standardisierung

## CLEAN CORE STRATEGIE ALS BUSINESS-BOOSTER NUTZEN

Technologische Veränderungen sind von jeher eine Herausforderung, vor allem dann, wenn sie komplexe Unternehmensarchitekturen betreffen. In diesem Zusammenhang hat der Einzug der Cloud-Technologie nicht nur die Art und Weise wie heute gearbeitet wird verändert, sondern vor allem die unternehmensinternen Prozesse. Wenn ein Software-Konzern, wie die Walldorfer SAP, die technologische Basis von on-premises-Strukturen auf eine Cloud-Strategie umstellt, löst dieser Technologiewechsel nicht nur innerhalb des Unternehmens einen großen Wandel aus, sondern vor allem kundenseitig. Die Kunden müssen ebenfalls umdenken und sich von liebgewonnenen Individualisierungen ihrer SAP-Umgebung trennen. Ulrich Parthier, Herausgeber it management, sprach mit Ralph Weiss, GEO VP DACH bei BlackLine, darüber, welche Herausforderungen der Wechsel von SAP in die Cloud für Unternehmen mit sich bringt und wie das Clean-Core-Prinzip helfen kann.

**Ulrich Parthier:** *Dass die Cloud eine Zukunftstechnologie ist, steht außer Frage. Aber warum tun sich so viele Unternehmen schwer, SAP in die Cloud zu folgen, schließlich ist S/4HANA kein neues Thema?*

**Ralph Weiss:** Das liegt an den zahlreichen individuellen Anpassungen, die Unternehmen über die Jahre vorgenommen haben, um die mächtige SAP-Plattform an die Bedürfnisse des eigenen Unternehmens anzupassen. Zu Zeiten von on-premises ging das, aber inzwischen hat sich die Situation geändert und die Cloud ist die führende Technologie. Das hat dazu geführt, dass SAP seit Jahren verschiedene Systeme am Leben halten muss, was komplexe Herausforderungen mit sich bringt. SAP will das logischerweise ändern und in Zukunft ausschließlich auf die Cloud setzen.

> CLEAN CORE HILFT DEN UNTERNEHMEN, IHRE EFFIZIENZ ZU STEIGERN UND EINE NACHHALTIGE IT-INFRASTRUKTUR AUFZUBAUEN.
>
> **Ralph Weiss, Geo VP DACH, BlackLine, www.blackline.com**

Das Konzept der Cloud-Technologie ist aber anders als bei on-premises. Es basiert auf einem möglichst breiten Standardangebot, an das sich Speziallösungen über Schnittstellen anbinden lassen. Das führt dazu, dass die Unternehmen etablierte Prozesse und Strukturen hinterfragen und an die neuen Rahmenbedingungen anpassen. Das ist nicht leicht, denn in vielen Unternehmen ist SAP das führende System, dem alles untergeordnet ist. Deshalb fällt der Wechsel so schwer, denn er ist komplex.

**Ulrich Parthier:** *Müssen die SAP-Kunden dann beim Umzug in die Cloud Abstriche machen?*

**Ralph Weiss:** Davon ist nicht auszugehen. Was ich aktuell beobachte, ist etwas anderes. In vielen Unternehmen sind zu on-premises-Zeiten geradezu flickenteppichähnliche IT-Landschaften entstanden. Das hat es schwer gemacht, Daten zusammenzuführen und nutzbar zu machen. In den Studien, die BlackLine jedes Jahr durchführt, wurde beispielsweise immer wieder beklagt, dass die Vielzahl der Datenquellen ein enormes Fehlerrisiko mit sich bringt. Cloud-Lösungen dagegen sind so konzipiert, dass Daten – einfacher als früher – über Schnittstellen

integriert werden. Auch SAP hat eine Integration Suite, die bei der Vernetzung der Cloud-Systeme hilft.

? **Ulrich Parthier:** *Und was verbirgt sich hinter dem Clean-Core-Trend, der von SAP derzeit forciert wird?*

**Ralph Weiss:** Im Grunde ist der Name selbstredend. In der SAP-Cloud sollte es keine individuellen Zusatzprogrammierungen innerhalb des SAP Core mehr geben – sprich alles ist clean. Der Core ist das Herzstück der SAP-Plattform, das mit Lösungen aus der Partnerlandschaft ergänzt werden kann, wie beispielsweise mit BlackLine. Sprich, das Clean-Core-Prinzip ist keine Begrenzung von SAP, sondern eher eine Erweiterung. Aber nicht durch individuelle Programmierungen, die aufwendig gepflegt werden müssen, sondern mithilfe einer Partnerlandschaft.

Unsere Lösung beispielsweise ist direkt an die SAP Cloud angebunden und ergänzt SAP um wertvolle Accounting-Funktionen, was die Komplexität des Monatsabschlusses und die Intercompany-Beziehungen reduziert. Durch den gesicherten Datenaustausch zwischen den Systemen sind die Daten sowohl aktuell als auch nicht mehr redundant und das macht sie schlussendlich so wertvoll.

? **Ulrich Parthier:** *Und wie kann ich mir die Umsetzung einer Clean-Core-Strategie in einem Unternehmen konkret vorstellen – unabhängig vom Monatsabschluss oder den Intercompany-Prozessen?*

**Ralph Weiss:** Zunächst müssen die Unternehmen sich entscheiden, welche Prozesse standardisiert und welche individuell sein sollen. Die Herausforderung besteht darin, ein Gleichgewicht zwischen Standardisierung und den spezifischen Business-Interessen einzelner Bereiche oder Regionen zu finden. Im Zentrum steht die SAP Cloud, die es ermöglicht,

**Christian Straub,**
**Head of Customer Advisory S/4HANA & Finance und Co-Head Solution Advisory, Middle & Eastern Europe, SAP**

„Wir arbeiten schon sehr lange und vertrauensvoll mit BlackLine auf Basis einer Solution-Extension-Partnerschaft zusammen. Die BlackLine-Lösungen ergänzen uns hervorragend im Bereich Accounting und Controlling."

Erweiterungen zu entwickeln und zu betreiben, ohne den Kern der SAP-Plattform zu beeinträchtigen. Das bietet Flexibilität und die Möglichkeit, Innovationen wie KI, IoT und maschinelles Lernen zu integrieren. Und das zeigt, dass das Clean-Core-Prinzip einer Öffnung von SAP gleichkommt – allerdings ohne das Herzstück selbst zu verändern.

? **Ulrich Parthier:** *Und welchen konkreten Mehrwerte ergeben sich daraus für die SAP-Kunden?*

**Ralph Weiss:** Zum einen eine größere Agilität, denn weil die Anpassungen außerhalb des Produktkerns vorgenommen werden, sind die Updates konfigurierbarer Standardsoftware unkomplizierter und weniger risikobehaftet. Das bringt geringere Betriebskosten mit sich und senkt den Wartungs- und Support-Aufwand. Dank des Vorhandenseins einer breiten Partnerlandschaft können die Kunden heute und erst recht in Zukunft beliebig viele Funktionen ergänzen, quasi andocken. BlackLine beispielsweise versetzt die Unternehmen in die Lage ein Continuous Accounting durchzuführen. Das entlastet die Finanzabteilung, sorgt für akkurate Finanzdaten in Echtzeit und erhöht die Resilienz von Unternehmen.

? **Ulrich Parthier:** *Das sind die konkreten Vorteile für die Kunden. Und was haben Sie oder andere SAP-Partner davon?*

**Ralph Weiss:** Clean Core ist ein Wachstumsgenerator. Durch die Trennung von Standardplattform und individuellen Erweiterungen werden Unternehmen in die Lage versetzt, schnell und kosteneffizient auf neue Technologien und Marktveränderungen zu reagieren. Da Partnerlösungen jetzt bei der SAP noch stärker im Fokus sind als in der Vergangenheit, tun auch wir oder andere SAP-Partner uns leichter, mit den Unternehmen ins Gespräch und ins Geschäft zu kommen.

? **Ulrich Parthier:** *Das hört sich vielversprechend an. Realität oder Wunschdenken?*

**Ralph Weiss:** Das ist keinesfalls Wunschdenken, auch wenn die Übergangsphase im Moment viele Unternehmen vor Herausforderungen stellt. Schlussendlich hilft Clean Core den Unternehmen, ihre Effizienz zu steigern und eine nachhaltige IT-Infrastruktur aufzubauen. Diese Strategie bietet sowohl den Partnern als auch den Unternehmen eine klare Orientierung, wie sie sich in einer schnelllebigen digitalen Wirtschaft behaupten können und Clean Core ermöglicht es den Unternehmen, den digitalen Wandel anzuführen, statt abgehängt zu werden.

! **Ulrich Parthier:** *Herr Weiss, wir danken Ihnen für das Gespräch.*

# ZUKUNFT DER IP-NETZE

## VIRTUALISIERTE, SOFTWARE-DEFINIERTE, INTELLIGENTE SYSTEMLÖSUNGEN UND -ANWENDUNGEN

Die Technik der IP-Netze entwickelt sich weiter, was besonders durch die Entstehung des Internet of Things (IoT) beeinflusst wurde. Eine fundamentale Bedeutung besitzt hierbei die Virtualisierung von Netzfunktionen, kurz NFV (Network Function Virtualization). Dank NFV ist die Nutzung von VNFs (Virtual Network Functions) in IP-Netzen möglich, was zur Entstehung einer neuen Generation programmierbarer IP-Netze führt und auch als Network Slicing bekannt ist.

Grundlage hierfür sind die Konzepte des SDN (Software Defined Networking), welche in der Umsetzung zu einem Software-Defined IoT (SD-IoT) führen. Das Netz fungiert somit zunehmend als Akteur im digitalen Raum, wobei das Thema Sicherheit eine herausragende Rolle spielt und es neuer Sicherheitsansätze bedarf, wie zum Beispiel den Einsatz der Blockchain-Technologie und moderner kryptografischer Methoden.

Dieses Buch bietet Ihnen eine systematische Darstellung der für die IP-Netze der Zukunft relevanten Konzepte und ihren Anwendungen anschaulich mit über 300 Bildern illustriert.

Das Buch ergänzt das Standardwerk „Technik der IP-Netze. Internet-Kommunikation in Theorie und Einsatz" und eignet sich nicht nur als Lehrbuch für Studierende unterschiedlicher Fachrichtungen und für Neueinsteigende, sondern auch für Praktiker. Im Buch sind die relevanten Quellen ins Internet verlinkt, sodass es auch als „Informations-Hub" für das Selbststudium dienen kann.


**Zukunft der IP-Netze:**
Virtualisierte, software-definierte, intelligente Systemlösungen und -anwendungen;
Anatol Badach, Erwin Hoffmann;
Carl Hanser Verlag GmbH & Co. KG; 11-2025

**Aus dem Inhalt:**

- aufs Ganze unter Berücksichtigung der Details – stellt die Weiterentwicklung der IP-Netze und damit auch des Internets fundiert und zugleich praxisorientiert dar.
- Software-Defined-Systemlösungen und -Anwendungen – erläutert diese anhand umfangreicher Beispiele.
- Blick in die Zukunft – vermittelt ein Verständnis für die Weiterentwicklung des Internets und seiner Sicherheitsaspekte.

# Fertigungsindustrie

## WARUM UNTERNEHMEN SCHON HEUTE AUF SAP DM SETZEN SOLLTEN

**MEHR WERT**
**Mehr zu SAP DM sowie zu hybriden Enterprise-Architekturen, erfahren Sie hier:**

Durch die rasante Digitalisierung wird das Optimieren von Produktionsprozessen immer wichtiger. Echtzeit-Prognosen und die nahtlose Integration von Produktionsanlagen helfen ihnen dabei, ihre Effizienz zu steigern und frühzeitig potenzielle Schwachstellen zu erkennen.

Ausgangspunkt dafür ist ein modernes Manufacturing Execution System (MES) – etwa das cloudbasierte SAP Digital Manufacturing (SAP DM). Dieses wird bis spätestens 2030 den Vorläufer SAP Manufacturing Execution (SAP ME) endgültig ersetzen. Für Unternehmen lohnt es sich daher, frühzeitig einen Blick auf die neue Lösung zu werfen.

**Das volle Potenzial nutzen**

Der Grundsatz bei SAP DM: Digital first! Konsequenterweise wird das System auf der SAP Business Technology Platform (SAP BTP) betrieben. SAP stellt dadurch sicher, dass es sich leicht mit anderen Business-Systemen kombinieren lässt und Unternehmen so Produktion und Management standortübergreifend miteinander vernetzen können. Der Fokus auf die Cloud erhöht die Skalierbarkeit und ermöglicht dem Management Echtzeit-Analysen.

Insgesamt bietet SAP DM zahlreiche Features, die Fertigungsbetriebe nutzen können, um ihre digitale Transformation voranzutreiben. Über eine standardisierte Schnittstelle offeriert es beispielsweise eine leichtgängige Datenübernahme aus dem SAP ERP. Mit dem Production Operation Dashboard (POD) – einem integrativen Bestandteil von SAP DM – können Nutzer zudem jederzeit alle relevanten Auftrags- und Materialinformationen einsehen sowie Rückmeldungen durchführen. Alerts informieren Mitarbeitende vorgelagerter Prozesse dabei schnell über Qualitätsprobleme oder fehlendes Material.

Die integrierte KI erkennt Qualitätsabweichungen automatisch via Kamera und unterstützt so die Qualitätssicherung signifikant. SAP DM besitzt zudem eine Planungsheuristik, mit der Produktionsplanende den zukünftigen Kapazitätsbedarf leichter abschätzen können. Ein besonderer Schwerpunkt liegt auf der Personaleinsatzplanung, die unter anderem die Qualifikationen und Zertifizierungen der Mitarbeitenden berücksichtigt.

Um eine einfache Automatisierung – hin zur Industrie 4.0 – zu garantieren, offeriert SAP DM auch einen Production Process Designer (PPD). Userinnen und User können damit in einer Low-Code-Umgebung automatisierte Prozesse gestalten.

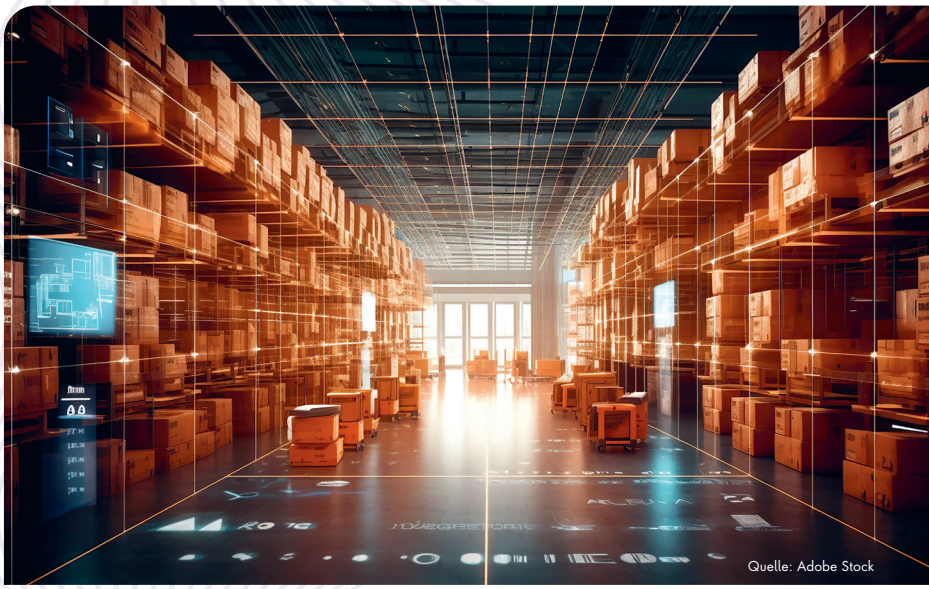
Für mehr Nachhaltigkeit sorgt eine integrierte Live-Daten-Verarbeitung auf Basis von Manufacturing Data Objects (MDO). Diese ermöglichen die Erstellung von Ad-Hoc-Reports über die integrierte SAP Analytics Cloud (Embedded SAC), um etwa Transparenz im Energiemanagement herzustellen.

**SAP DM: Ein Fazit**

Für ein modernes Industrie-4.0-Konzept liefert SAP DM sehr interessante Hilfestellungen: Da es sich um eine cloudbasierte Lösung handelt, ermöglicht sie produzierenden Unternehmen so etwa eine schnellere Integration ihrer Produktionsabläufe über mehrere Standorte hinweg.

Außerdem ermöglicht es den Aufbau hybrider Enterprise-Architekturen. Die SAP BTP sorgt für eine nahtlose Anbindung von Drittsystemen und somit für eine bessere Kommunikation zwischen verschiedenen Systemen und Maschinen. Dies ist eine der zentralen Erfolgsfaktoren für eine erfolgreiche Digitalisierung.

***Thomas Baier, Kai Roßnagel***
***www.mhp.com***



**Mit SAP DM das Digitalisierungspotenzial in der Fertigung nutzen**

Quelle: Adobe Stock

# SAP S/4 und RISE with SAP

## TURBO FÜR DIE DIGITALE TRANSFORMATION

Die Migration nach SAP S/4HANA und das RISE with SAP-Programm sollen Unternehmen dabei helfen, ihre Geschäftsprozesse zu transformieren und in die Cloud zu verlagern. Die Umstellung bedeutet gleichzeitig eine große Herausforderung, da sie nicht nur technische, sondern auch organisatorische und strategische Aspekte umfasst. Der Einsatz von Software und künstlicher Intelligenz (KI) kann diesen Prozess unter anderem durch einen selektiven Ansatz bei der Datenmigration und Automatisierung von Testverfahren erheblich erleichtern und beschleunigen.

**Datenbereinigung und -migration mit KI-Unterstützung**

Der Einsatz von KI bei der Analyse, Bereinigung und Konsolidierung kann die Genauigkeit und Konsistenz der Daten verbessern. Komplexe Datenmigrationsprozesse lassen sich automatisieren, indem Datenstruktur und -anforderungen von SAP S/4HANA analysiert und bestehende Daten entsprechend umgewandelt werden. KI dient zudem dazu, Geschäftsprozesse auszuwerten und zu optimieren, was zu einer effizienteren Implementierung und Nutzung von SAP S/4HANA führt. Auch für Mitarbeitende bedeutet der Einsatz von Software und KI eine Entlastung bei komplexen und ressourcenintensiven Projekten: Routineaufgaben können automatisiert werden – somit reduziert sich auch die Fehlerquote.

Die Planung des gesamten Projektes und das Risikomanagement profitieren ebenfalls: Unternehmen können ihre Projektplanung auf präzise Vorhersagen und Empfehlungen, basierend auf historischen Daten und Best Practices, stützen. Risiken, die während der Migration auftreten können, werden identifiziert, bewertet und Maßnahmen vorgeschlagen.

**Erfolgreiche SAP S/4HANA-Migration**

Unternehmen sollten von Beginn an auf den Einsatz spezieller Transformationssoftware setzen und keine Risken eingehen: Negativbeispiele gibt es seit dem Start der S/4-Migrationswelle genügend, mit einer KI-gestützten Softwareplattform und einem selektiven Migrationsansatz lassen sie sich vermeiden.

Am Anfang steht die gründliche Analyse der bestehenden Systemlandschaft und das Definieren der Migrationsziele; ein detaillierter Migrationsplan wird erstellt. Vor der Migration werden die Daten analysiert und bereinigt und eine automatisierte Datenmigration folgt – softwarebasiert geht das schnell und risikominimiert. Auch die wichtigen und umfassenden Tests werden von End-to-end-Lösungen für IT- und Geschäftstransformationen abgedeckt: Sie stellen einen reibungslosen Ablauf für die migrierten Daten und Prozesse sicher. Die Migrationsergebnisse werden überprüft und validiert – das verschafft Projektleitern mehr Sicherheit bei der Umsetzung.

**Fazit**

Die Migration zu SAP S/4HANA und die Teilnahme an RISE with SAP sind bedeutende Schritte zur digitalen Transformation. Bei der Umsetzung haben es Unternehmen mit komplexen Prozessen zu tun – sorgfältige Planung, eine klare Strategie und der Einsatz von KI-gestützter Software sind der Schlüssel zum Erfolg. Durch die Automatisierung von Datenmigration und -bereinigung, die Optimierung von Geschäftsprozessen und das effektive Projektmanagement können Verantwortliche die Herausforderungen der Migration erfolgreich bewältigen und die Vorteile von SAP S/4 und RISE with SAP voll ausschöpfen!

***www.snpgroup.com***

tangro®

xSuite
It's simple. It's digital.

# Intelligente Automatisierung für E-Invoicing und P2P-Prozesse

## Werden Sie Gipfelstürmer

- Digitale, KI-gestützte Rechnungsverarbeitung
- Versand, Annahme und Verarbeitung von E-Rechnungen
- Durchgängige Auftrags-, Bestell- & Rechnungsprozesse
- Revisionssichere Archivierung
- Einhaltung von Compliance

Webinare zum Thema

**DSAG**
**15.-17.10.24**
**Leipziger Messe**
**Halle 3**

**SAP® Certified**
Integration with RISE with SAP S/4HANA Cloud

info@xsuite.com

www.xsuite.com

# RISE with SAP

## TIPPS ZUR LIZENZOPTIMIERUNG IN DER CLOUD

SAP-NUTZERLIZENZEN SIND EIN WESENTLICHER BESTANDTEIL DER MIT S/4HANA VERBUNDENEN KOSTEN.

**Christian Achenbach, Senior Product Marketing Manager, USU Software AG, www.usu.com**

SAP bezeichnet sich als „The Cloud Company" und hat innerhalb weniger Jahre sein Angebot an Cloud-basierten Lösungen stark erweitert. Mit der Einführung der SAP S/4HANA Cloud Public Edition und insbesondere RISE with SAP untermauerten die Walldorfer ihren Cloud-first Ansatz.

Wenn Sie als ECC-Bestandskunde eine Migration zu SAP Cloud unter Nutzung des RISE-Programms in Erwägung ziehen, sollten Sie zuvor einige Faktoren sorgfältig prüfen, um den bestmöglichen Nutzen ziehen zu können. Denn zweifelsohne hat RISE with SAP erhebliche Auswirkungen, die nicht übersehen werden dürfen.

- Beendigung der ECC-Wartung bis 2027-2030
- Gestoppte ECC-Innovationen
- Jährliche Erhöhung der Wartungsgebühr um 5 Prozent.

**Was ist eigentlich RISE with SAP?**
RISE mit SAP zielt darauf ab, die Cloud-Migration für Kunden zu vereinfachen und sie auf dem Weg zu einem „intelligenten" Unternehmen individuell zu unterstützen. Das Angebot umfasst mehr als nur die Umstellung auf SAP S/4HANA, sondern bietet fünf Kernelemente:

**#1** SAP S/4HANA Cloud
**#2** Business Process Intelligence (BPI)
**#3** SAP Business Technology Platform (SAP BTP)
**#4** Zugang zum SAP Business Network sowie verschiedene
**#5** integrierte Tools und Services.

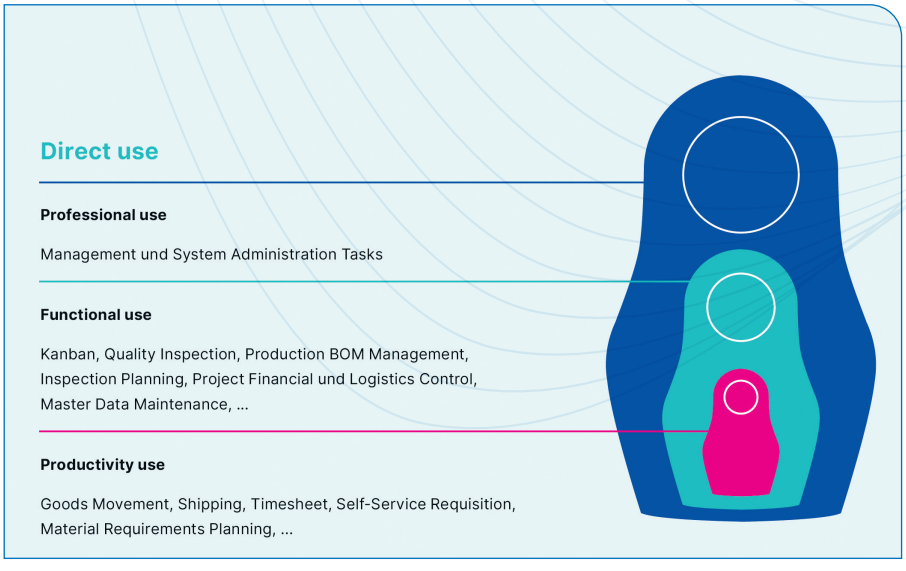
RISE mit SAP funktioniert auf Abonnementbasis mit einem Service Level Agreement (SLA), welches die Komponenten zu einem einzigen Paket zu einem Festpreis bündelt. SAP übernimmt den Betrieb der Lösung und die Fehlerbehebung.

Für das Hosting der Infrastruktur stehen SAP oder Hyperscaler wie Google Cloud, Amazon Web Services oder Microsoft Azure zur Verfügung. Laut SAP können mit RISE with SAP die Gesamtbetriebskosten im Vergleich zu einer SAP S/4HANA-Implementierung vor Ort um bis zu 20 Prozent gesenkt werden, einschließlich der Migrationskosten.

**RISE with SAP, SAP S/4HANA Cloud – was ist der Unterschied?**
RISE with SAP ist darauf zugeschnitten, Unternehmen beim Übergang in die Cloud mit einer Fülle von Innovationen und Lösungen zu unterstützen. Die SAP S/4HANA Cloud, die sowohl als Public- als auch als Private-Cloud-Option verfügbar ist, bildet einen der Eckpfeiler.

RISE mit SAP bietet zwar eine umfassende Cloud-Lösung, ist aber keine Voraussetzung für die Nutzung der Cloud-Angebote von SAP. Unternehmen können auf SAP S/4HANA Cloud, Public Edition, und SAP S/4HANA Cloud, Private Edition, auch ohne „RISE" zugreifen.

Darüber hinaus gibt es seit Anfang 2023 GROW with SAP, das sich insbesondere an Neukunden im Mittelstand richtet. Über GROW können sich Unternehmen für die SAP S/4HANA Cloud Public Edition entscheiden, bei der die Infrastruktur und die Softwarefunktionen des Cloud-ERPs von SAP-Kunden gemeinsam genutzt und direkt von SAP verwaltet werden.




**Nutzertypen-Modell unter SAP S/4HANA On-Premises**

**Das neue FUE-Modell – Chance oder Kostenfalle?**

Vielleicht kennen Sie noch die verschiedenen Nutzertypen bei SAP S/4HANA on-prem? SAP unterscheidet hier sechs Anwendungsszenarien: Developer Use, Professional Use, Functional Use und Productivity Use (als die wichtigsten Use Types), sowie Engine Use und Technical Use.

Das neue FUE-Modell bei RISE mit SAP ist anders. Mit RISE with SAP S/4HANA Cloud hat SAP einen Schritt in Richtung Benutzerlizenzierung gemacht, der das Lizenzmanagement erleichtern soll.

Anstatt eine exakte Anzahl bestimmter Nutzerlizenztypen zu erwerben, können SAP-Kunden sogenannte FUEs (Full Use Equivalents) erwerben. FUEs ist eine fiktive Zahl, die der theoretischen Anzahl von Personen entspricht, die dazu berechtigt sind, auf den vollen Funktionsumfang der Lösung zuzugreifen.

Personen mit weniger Berechtigungen werden berücksichtigt, indem der entsprechende FUE mit Hilfe eines Umrechnungsfaktors berechnet wird:

**1 FUE =**

**1 SAP S/4HANA für Advanced Use**
**5 SAP S/4HANA für Core Use**
**30 SAP S/4HANA für Self-Service Use**

Das FUE-Modell bietet die Option, Nutzerlizenzen für verschiedene Nutzungsarten einzusetzen. Bei einem RISE with SAP-Vertrag muss die Beziehung zwischen den verschiedenen Nutzungsarten nicht festgelegt werden. Laut SAP bietet es große Flexibilität, da Einsparungen ohne Rekonfigurationsrechte oder Vertragsneuverhandlung erzielt werden können.

Das FUE-Modell ist in verschiedenen Stufen erhältlich. Beispiel:

1001-2000 Benutzer: 164€/FUE/Monat (Private Edition) oder 135€/FUE/Monat (Public Edition).

Eine solide Analyse der zuvor genannten Nutzerlizenzen ist dringend erforderlich, um keine unnötigen Kosten zu verursachen. Eine Preisgestaltung ohne kontextbezogene Analyse der zugewiesenen Lizenztypen kann die Höhe der erworbenen FUEs drastisch beeinflussen.

In der Tabelle finden Sie ein Beispiel für eine SAP-Umgebung mit 1.000 Nutzern vor und nach der Lizenzoptimierung.

| Lizenz | Anzahl an Lizenzen ohne Optimierung | Anzahl an Lizenzen nach Optimierung | Gewichtung | FUE ohne Optimierung | FUE nach Optimierung |
|---|---|---|---|---|---|
| Developer Access | 10 | 10 | 0,5 | 20 | 20 |
| Advanced Use | 355 | 154 | 1 | 355 | 154 |
| Core Use | 545 | 345 | 5 | 109 | 69 |
| Self Service | 90 | 491 | 30 | 3 | 17 |
| Summe | 1000 | 1000 | | 487 | 260 |

Wie Sie sehen, konnten 227 FUE eingespart werden, während die Anzahl der Nutzer beibehalten wurde. In unserem obigen Beispiel von 1.000 Lizenzen betrugen die erzielten Einsparungen 30.645 Euro pro Monat (Public Edition).

SAP-Nutzerlizenzen sind ein wesentlicher Bestandteil der mit S/4HANA verbundenen Kosten. Bevor Sie auf S/4HANA migrieren, sollten Sie also unbedingt Ihre aktuellen Lizenzen sorgfältig überprüfen, um sicherzustellen, dass sie für die tatsächliche Systemnutzung optimiert sind.

**Fazit**

Die Verwaltung von SAP-Lizenzen stellt viele Kunden vor große Herausforderungen. Standardverträge von RISE with SAP beinhalten eine Lizenzierung, die auf Berechtigungen (Authorization) anstelle der Nutzung (Usage) basiert.

Dies hat Auswirkungen auf den Preis: die berechtigungsbasierte Lizenzierung ist durchschnittlich 50 – 150 Prozent teurer als die nutzungsbasierte Lizenzierung.

SAP-Kunden haben dennoch Einflussmöglichkeiten auf die Konditionen und den Umfang der gewünschten SAP-Produkte. Entscheidend ist, dass Sie das SAP-Angebot verstehen und aktiv managen. So können Sie die für sich besten Optionen finden.

Mit einer SAP-zertifizierten SAP-Software-Optimierungslösung und Expertise können wir Ihnen dabei helfen, Ihre ECC-Lizenzen zu optimieren, und Ihr ideales S/4HANA-System auf der Grundlage der tatsächlichen Nutzung und Berechtigungen anzupassen. Überlassen Sie das Steuer nicht Ihrem Software-Anbieter, sondern behalten die Kontrolle.

***Christian Achenbach | www.usu.com***

# DSAG-Jahreskongress 2024

## DREIKLANG DER ZUKUNFT

In der sich ständig verändernden Geschäftswelt ist die Transformation das bestimmende Thema. Aber kein erfolgreicher Wandel ohne ein konstruktives Miteinander. Dementsprechend steht der Jahreskongress 2024 vom 15. bis 17. Oktober 2024 in Leipzig unter dem Motto „Dreiklang der Zukunft: Anwender, SAP und Partner als Taktgeber der Transformation". Die digitale Transformation im Hinblick auf die Cloud und auf die künstliche Intelligenz sind die bestimmenden Themen.

**Digitale Transformation und Anwender**

SAP hat mit RISE with SAP und GROW with SAP zwei zentrale Lösungen für die digitale Transformation im Portfolio. Mit den Angeboten soll die Migration zu Cloud-ERP-Lösungen forciert werden. Zudem wurde SAP Migration & Modernization als neues SAP-Programm gelauncht, das finanzielle Anreize bietet für den Wechsel in die Cloud. Dennoch gibt es Diskussionsbedarf bezüglich der S/4HANA Cloud-Strategie von SAP. Konkret fordern die Anwenderunternehmen praxisrelevante Use Cases und eine offene Integration, die auch On-Premises funktioniert.

**Digitale Transformation und Partner**

Ein weiterer Taktgeber der digitalen Transformation sind die Partner. Sie spielen eine zentrale Rolle im SAP-Ökosystem und unterstützen die Anwenderunternehmen bei deren digitaler Transformation. Gleichzeitig treiben sie ihre eigene Transformation voran. Sie müssen selbst den Blick nach vorn richten, um ihre Kunden angemessen betreuen zu können. Wie die gemeinsame Umfrage von DSAG und ASUG von 2023 zeigt, funktioniert die Zusammenarbeit zwischen allen Beteiligten im SAP-Ökosystem gut und 76 Prozent der befragten Unternehmen sind mit ihren Partnern zufrieden.

**Digitale Transformation und künstliche Intelligenz**

Neben der Cloud nimmt die künstliche Intelligenz eine immer wichtigere Rolle ein. Große KI-Modelle werden komplett neue Anwendungen ermöglichen und bestehende Geschäftsmodelle sowie die Wertschöpfung in allen Industrien deutlich verändern. SAP hat die Bedeutung dieser wegweisenden Technologie erkannt und arbeitet daran, das Portfolio entsprechend anzupassen. Jetzt müssen praxiserprobte Anwendungsbeispiele, angemessene und transparente Preismodelle sowie entsprechende Lizenz- und Nutzungsbedingungen auf die Agenda.

Mehr als 5.500 Teilnehmende werden zu der Veranstaltung erwartet.

***www.dsag.de/jahreskongress***

gambit

# DIE REISE PLANEN?

## NEE, ICH STEIGE EINFACH INS NÄCHSTBESTE FLUGZEUG UND SCHAUE MAL, WO ICH LANDE.

Überlassen Sie Ihre Reise nach SAP S/4HANA lieber nicht dem Zufall. Erreichen Sie Ihre gesteckten Ziele und starten Sie mit unserer Roadmap!

Setzen auch Sie jetzt auf unser strukturiertes und bewährtes Vorgehensmodell und legen Sie die Basis für Ihre Implementierung.

Buchen Sie jetzt einen 30-minütigen Kennenlerntermin und sprechen Sie mit uns über Ihre Ziele.

# Workflows für alle S/4HANA-Ausprägungen

## FLEXIBLE SAP-ADD-ONS: FREIHEIT BEI DER WAHL DES BETRIEBSMODELLS

Beim kommenden, unausweichlichen Umstieg auf SAP S/4HANA stehen für SAP-Anwenderunternehmen einige Grundsatzentscheidungen an: Greenfield- oder Brownfield-Migration? On-Premises, in der Cloud oder ein hybrider Ansatz als Betriebsmodell? Und wenn Cloud, welche Ausprägung: Public oder Private?

Nicht zuletzt ist SAP zwar das Kernstück der Unternehmens-IT, aber beileibe nicht die einzige Software. Zusatzlösungen für SAP, die zum Beispiel Einkauf und Buchhaltung unterstützen, gibt es viele. Was bedeutet dies nun für anstehende Migrationen? Unternehmen haben genug mit den Grundsatzfragen des Umstiegs zu tun, sie sollten sich nicht auch noch damit auseinandersetzen müssen, ob ihre bestehende Unternehmenssoftware den Wechsel auch mitmacht.

**Maximale Flexibilität**

Am besten also, wenn Lösungen für Beschaffung und Rechnungsverarbeitung so konzipiert sind, dass sie alle SAP-Deployment-Modelle unterstützen und dokumentenbasierte Prozesse in der alten ECC-Welt ebenso wie in der neuen S/4HANA-Welt automatisiert und digitalisiert abbilden – wie bei den Softwarelösungen des Herstellers xSuite Group.

Die größten Herausforderungen bei Softwareprojekten im Bereich automatisierter Rechnungs- und P2P-Abläufe liegen daher auch in der Integration der Prozesse, der Skalierbarkeit der eingesetzten Lösungen sowie in einer reibungslosen Unterstützung der S/4HANA-Migration. Nur so bleibt maximale Flexibilität bei einer Migration gewährleistet oder bei der Wahl des passenden SAP-Bereitstellungsmodells.

> UNTERNEHMEN HABEN GENUG MIT DEN GRUNDSATZFRAGEN DES UMSTIEGS ZU TUN, SIE SOLLTEN SICH NICHT AUCH NOCH DAMIT AUSEINANDERSETZEN MÜSSEN, OB IHRE BESTEHENDE UNTERNEHMENSSOFTWARE DEN WECHSEL AUCH MITMACHT.
>
> **Mehrnaz Lotfali-Shirazi, Product Manager, xSuite Group GmbH, www.xsuite.com**

**Cloud-Modelle**

Folgende zwei Betriebsmodelle der neuen SAP-Generation sollte man kennen: Die S/4HANA Cloud Private Edition ist eine Variante der SAP S/4HANA Cloud, welche die Vorteile der Cloud mit einem hohen Maß an Kontrolle und Individualisierung (wie es On-Premises-Systeme bieten) verbindet. Der Zugriff ist sowohl über das klassische SAP GUI als auch über das SAP Fiori Launchpad möglich. Kunden haben Zugriff auf den Konfigurationsleitfaden, der es ihnen ermöglicht, das System weitgehend nach ihren spezifischen Anforderungen anzupassen.

SAP bietet für die private Edition jährliche Upgrades an. Unternehmen können diese nach eigenem Zeitplan durchführen, solange sie innerhalb der Mainstream-Wartungszeiträume bleiben. Die Edition unterstützt sowohl Greenfield- als auch Brownfield-Ansätze sowie selektive Datenmitnahmen aus bestehenden Systemen. Sie lässt sich außerdem gut in andere SAP-Lösungen und die SAP Business Technology Platform (BTP) integrieren – Ausgangspunkt für eine integrierte IT-Landschaft, die sowohl cloud-basierte als auch on-premises Lösungen umfasst.

Die S/4HANA Cloud (Public) demgegenüber wird von SAP als standardisiertes Multi-Tenant-SaaS-Angebot bereitgestellt. Das bedeutet, SAP verwaltet die Infrastruktur, Plattform und Software. Zielgruppe sind mittelständische Unternehmen und Neukunden. Der Zugriff erfolgt ausschließlich über das SAP Fiori Launchpad, Kunden haben keinen Zugriff auf den Konfigurationsleitfaden. Statt der ArchiveLink-Schnittstelle, erfolgt die Archivierung über den Content Management Interoperability Service (CMIS). Updates werden vierteljährlich von SAP durchgeführt, Add-ons können über die SAP Business Technology Platform (BTP) angebunden werden.

**SAP BTP und der Clean Core**

Die SAP BTP ist eine Integrationsplattform, auf der SAP-Kunden und -Partner Add-ons und Individualisierungen ihres ERP-Systems entwickeln und betreiben

können. Für SAP ist sie das kommende Fundament für Geschäftsprozesse und ideal für Unternehmen, die Teile ihrer Prozesse in die Cloud auslagern möchten.

Das heißt, benutzerdefinierte Prozesse werden auf die SAP BTP verlagert und nur die Standardprozesse verbleiben auf dem ERP-Kern. Add-on-Lösungen auf der Business Technology Platform ermöglichen somit auch eine einfache Anbindung an SAP S/4HANA, wobei das SAP-System zu 100 Prozent im Clean Core bleibt. Durch die damit verbundene geringere Komplexität sollen Stabilität, Zuverlässigkeit und Agilität des Kern-ERPs gewährleistet werden. Automatisierte Upgrades und die Vermeidung manueller Prozesse, agile Einsteuerung von Innovationen und Anpassung an geschäftliche Anforderungen sorgen für gesteigerte Effizienz.

Innovationen und zusätzliche Funktionalitäten bereitstellen – genau dies ermöglicht die SAP BTP mit einem modularen, entkoppelten Ansatz: Das Kernsystem konzentriert sich auf wesentliche Funktionen, während nicht zum Kern gehörende Services durch Auslagerung auf die BTP ergänzt werden. Indem Hersteller ihre Spezialanwendungen also über die Plattform bereitstellen (wie xSuite), tragen sie mit bei zu einer möglichst reibungslosen S/4HANA-Migration.

xSuite hat den Weg in die Public Cloud als Modell der Zukunft aus gutem Grund eingeschlagen und die Entwicklung darauf ausgerichtet. Sowohl die Rechnungsverarbeitungslösung als auch das Lieferantenportal (Business Partner Portal) des Herstellers werden bereits über die SAP BTP bereitgestellt.

**Cloudbasierte Lieferantenkommunikation**

Das Business Partner Portal ist eine Plattform für den Austausch von Daten und Dokumenten im Procure-to-Pay-(P2P)Prozess. Der Einkauf sendet Bestellungen wie gewohnt aus seinem SAP-System, und der Lieferant kann sie sofort im Portal einsehen. Von dort aus können alle Arbeitsschritte und die gesamte Kommunikation vollständig digital innerhalb des Portals stattfinden. Der Lieferant kann Folgedokumente – zum Beispiel Auftragsbestätigungen, Lieferscheine oder Rechnungen – auf Basis der Bestellung generieren. Alle Informationen werden bequem an das SAP-System des Bestellers zurückgegeben – ein maximaler Automatisierungsgrad wird erreicht.

**Rechnungsbearbeitung auf der SAP BTP**

xSuite nutzt die Plattformtechnologie zur Bereitstellung des Kernprodukts xSuite Invoice. Der Workflow übernimmt die vollständige Digitalisierung und Automatisierung der Rechnungseingangsbearbeitung. Die Lösung unterstützt Unternehmen beim E-Invoicing, holt also auch eingehende XML-Rechnungen ab, liest ihre Inhalte aus und übergibt die relevanten Informationen automatisch in die entsprechenden Felder des ERP-Systems. Die Rechnungsverarbeitung unterstützt alle am Markt gängigen Rechnungsformate und die Einbindung von E-Rechnungs-Portalen und -Netzwerken (zum Beispiel Peppol).

Weil sich die Lösung zugleich für jedes S/4HANA-Betriebsmodell eignet – SAP S/4HANA Cloud , Cloud Private Edition und für On-Premises-Installationen – haben Anwenderunternehmen den Rücken frei für ihre kommende Migration. Die ist schließlich Herausforderung genug.

***Mehrnaz Lotfali-Shirazi***

# Synergien freisetzen

## WIE DIE IMPLEMENTIERUNG VON SAP BTP DIE INTEGRATION VON ONLINEMARKTPLÄTZEN TRANSFORMIEREN KANN

Ob Retail oder Manufacturing – Unternehmen stehen bei umfangreichen SAP-Integrationen oft vor derselben Herausforderung: eine Lösung für die nahtlose Integration verschiedener Systeme zu finden. Für unsere Kunden der Retail-Industrie stellt die Integration von Onlinemarktplätzen in die vorherrschende SAP-Landschaft die größte Herausforderung dar. Ziel ist es, Geschäftsprozesse über die eigenen Unternehmensgrenzen hinaus zu harmonisieren und automatisieren. Dieses Vorhaben kann exemplarisch für viele ähnlich gelagerte Integrationsszenarien anderer Industrien verstanden werden. Die erfolgreiche Bewältigung dieser komplexen Aufgabe erfordert nicht nur technisches Know-how, sondern auch ein tiefes Verständnis der branchenspezifischen Anforderungen und Geschäftsprozesse.

Bis heute ist SAP PI/PO eine der am häufigsten verwendeten Lösungen für die Integration von Unternehmensanwendungen. Mit der Einstellung von SAP PI/PO im Jahr 2027 müssen viele Kunden neue Lösungen für ihre bestehenden Systeme finden. Hier bietet die SAP Business Technology Platform (BTP) eine vielversprechende Alternative. Sie ermöglicht es, typische Altlasten und Integrationsprobleme zu überwinden, die bei der Nutzung mehrerer nicht standardisierter Anwendungsschnittstellen auf verschiedenen Plattformen immer wieder auftreten.

### Herausforderungen einer heterogenen Systemlandschaft

Nachfolgende Hürden haben sich im Laufe der Zeit aus der Praxis herauskristallisiert:

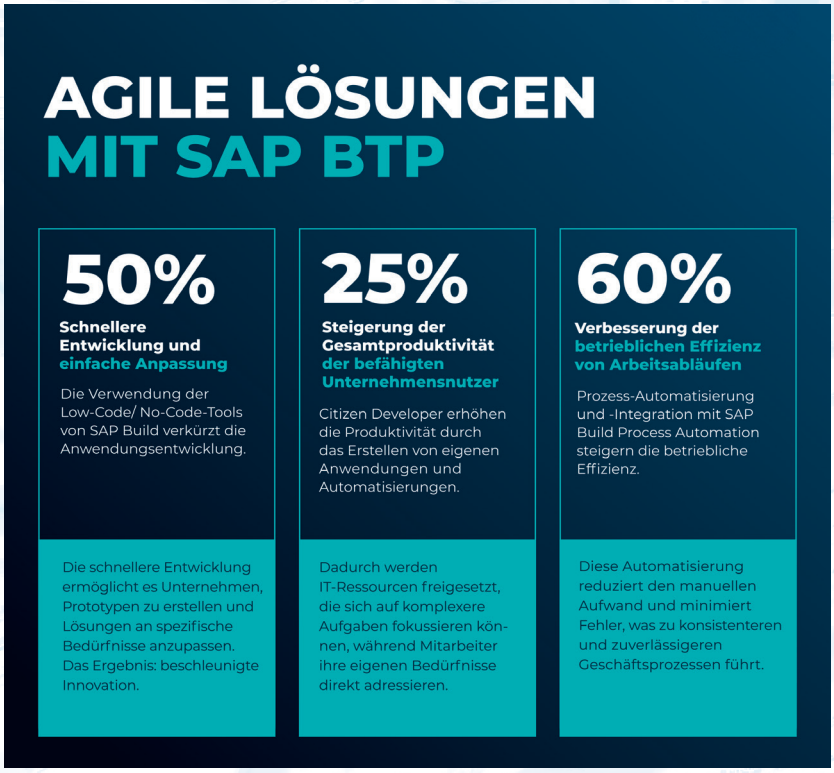
**#1 Schwer kalkulierbares Budget:** Über die Jahre ist beim Kunden eine heterogene Systemlandschaft mit Vor-Ort-, Cloud- und Drittanbietersystemen gewachsen. Dies erschwert die Vorhersage von Zeit- und Ressourcenaufwand für Support und Entwicklung, was zu Budgetüberschreitungen und Gewinneinbußen führen kann.

**#2 Notwendigkeit, Personal in verschiedenen Standards für Datenaustausch zu schulen:** Separat entwickelte Austauschmechanismen erfordern Schulungen in verschiedenen Standards, was steigende Kosten für Systementwicklung und -support sowie Personalwachstum nach sich zog. Der Mangel an Standardisierung verursachte zudem Inkonsistenzen in der Systementwicklung und -unterstützung.

**#3 Schwierigkeit bei der Kontrolle von Datenflüssen:** Unternehmen kämpfen mit Verzögerungen, Dateninkonsistenz und doppelter Arbeit aufgrund von redundantem Datenaustausch auf verschiedenen Plattformen.

**#4 Dateninkonsistenz:** Aus Gesprächen mit Kunden wissen wir, dass redundante Datentransfers zu Inkonsistenzen führen können, mit dem Ergebnis, dass falsche Daten für Entscheidungen herangezogen werden.

**#5 Ineffiziente Nutzung von IT-Ressourcen:** Mehrere Transferprozesse auf verschiedenen Plattformen führten zu einer ineffizienten Nutzung von IT-Ressourcen, da unterschiedliche Abteilungen nicht kompatible Systeme nutzten.



**#6 Sicherheit:** Datentransfers mit externen Anbietern bergen Risiken für Cyberangriffe, Datenschutzverletzungen, Systemausfälle und den Verlust sensibler Geschäftsinformationen – eine komplexe Herausforderung, die wir mit unserem Know-how zu vermeiden wissen.

Es wird deutlich, dass nicht standardisierte Austauschprozesse auf verschiedenen Plattformen zu zahlreichen Problemen führen. Die SAP Integration Suite vereinfacht den Integrationsprozess durch die Bereitstellung eines einzigen Systems für die Erstellung von Datenflüssen, Tests, Einführung und Überwachung. Dadurch wird die Komplexität bei der Verwaltung mehrerer Systeme für verschiedene Integrationsszenarien reduziert. Dieser Ansatz minimiert die Notwendigkeit von individueller Programmierung im SAP-Kern und nutzt stattdessen Side-by-Side-Erweiterungen auf der BTP.

**Vorteile der SAP BTP**

**#1 Clean-Core-Strategie:** Die Clean-Core-Strategie von SAP zielt darauf ab, die Integration und Erweiterung von SAP-Systemen Cloud-konform zu gestalten. Sie sorgt für optimale Stammdatenqualität und eine verbesserte Governance von Geschäftsprozessen. Unsere Erfahrungen zeigen, dass ein Clean Core zu einer besseren Wartbarkeit führt und Herausforderungen wie unvorhersehbare Budgets und Dateninkonsistenz reduziert.

**#2 Standardisierung:** Die SAP Integration Suite bietet einen standardisierten Ansatz für die Entwicklung und Wartung von Systemen. Sie erleichtert die Berechnung und Planung des Entwicklungs- und Supportbudgets und ermöglicht eine zentrale Verwaltung aller Austauschprozesse.

**#3 Zentrale Entwicklung und Verwaltung:** Mit der SAP Integration Suite können alle Austauschprozesse zentral entwickelt und verwaltet werden.

DER EINSATZ DER SAP INTEGRATION SUITE KANN UNTERNEHMEN HELFEN, IHRE GESCHÄFTSPROZESSE ZU HARMONISIEREN UND ZU AUTOMATISIEREN.

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

Dies reduziert die Notwendigkeit, Personal in verschiedenen Datenaustauschstandards zu schulen, und senkt somit die Kosten für Systementwicklung und -support sowie das Personalwachstum.

**#4 Verbesserte Datenqualität und -kontrolle:** Mit der SAP Integration Suite lassen sich Datenflüsse besser kontrollieren, Verzögerungen und doppelte Arbeit vermeiden und die Datenqualität verbessern. Eine visuelle Darstellung der Prozesse fördert die Kommunikation zwischen IT und Geschäft und beschleunigt Entscheidungsprozesse.

**#5 Optimierte IT-Ressourcennutzung:** Durch die Nutzung einer zentralen Plattform werden IT-Ressourcen effizienter genutzt. Vorgefertigte Integrationen sparen Zeit und Ressourcen und decken eine breite Palette von Integrationsszenarien ab, wie etwa Cloud-to-Cloud, Cloud-to-On-Premises und On-Premises-to-On-Premises.

**#6 Erhöhte Sicherheit:** Integrierte Sicherheitsfunktionen schützen vor Cyberangriffen und verringern die Risiken von Datenschutzverletzungen, Systemausfällen und dem Verlust sensibler Geschäftsinformationen.

**SAP Integration Suite**

So wurde deutlich, dass die Implementierung der SAP Integration Suite über die SAP Business Technology Platform (BTP) eine bedeutende Chance für Unternehmen darstellt, die Herausforderungen der Integration heterogener Systeme zu meistern. Unsere Kunden der Retail-Industrie agieren in einem Umfeld, das durch einen hohen Grad an Dynamik gekennzeichnet ist. Die Dauer der Integration bzw. die Umsetzung von Anpassungen zwischen dem eigenen SAP-System und Onlinemarktplätzen wirkt sich kritisch auf den Umsatz aus. Insbesondere hier kann die Integration Suite ihre Stärken gegenüber PI/PO ausspielen. Die bewährte SAP PI/PO-Lösung hat lange Zeit gute Dienste geleistet, doch nun sollten sich Unternehmen auf die zukünftigen Anforderungen einstellen.

Um den Schritt in eine neue Ära zu wagen, kann ein Technologiepartner eine entscheidende Rolle spielen. Anforderung sollten – neben einer langjährigen Migrationserfahrung – überzeugende Referenzen ebenso wie eine umfassende Cloud-Expertise sein, um die Transformation reibungslos zu gestalten und maßgeschneiderte Lösungen zu konzipieren, die exakt auf die Bedürfnisse des jeweiligen Unternehmens abgestimmt sind. Dies gilt besonders für Unternehmen, die vor der Herausforderung stehen, ihre bestehenden Systeme in eine moderne, zukunftsfähige, Cloud-basierte Architektur zu überführen.

**Das Ergebnis**

Der Einsatz der SAP Integration Suite in Verbindung mit der Unterstützung durch erfahrene Technologiepartner kann Unternehmen helfen, nicht nur aktuelle Integrationsprobleme zu überwinden, sondern auch ihre Geschäftsprozesse zu harmonisieren und zu automatisieren – ein Ziel das branchenübergreifend an Bedeutung gewinnt. So werden sie in die Lage versetzt, ihre IT-Landschaften zu optimieren, Synergien frei zu setzen und somit den vollen Mehrwert aus ihren technologischen Investitionen zu ziehen.

***Simon Meraner***

# Best-of-Breed-Ansatz

## DIE WACHSENDE BEDEUTUNG DER SAP-DATEN- UND PROZESSINTEGRATION

Die Migration in die Cloud wird für viele deutsche Unternehmen zeitnah zu einem relevanten Thema. Deutschland ist ein SAP dominierter Markt und es gilt die Migration von ECC zu S4/HANA umzusetzen. Der Aufbau einer cloudbasierten Infrastruktur ist ein entscheidender Schritt, um den globalen Anforderungen und aktuellen Marktgegebenheiten gerecht zu werden. Im Rahmen der Migration gilt es, alle relevanten Stakeholder miteinzubeziehen. Nur so lässt sich sicherstellen, dass sämtliche Anforderungen vollständig berücksichtigt werden. Unternehmen müssen Zeitpläne, Budgets und Verantwortlichkeiten klar definieren, um gleichzeitig ein effektives Risikomanagement aufzustellen.

Ein Schlüsselelement der Planungsphase ist die Auswahl der passenden Migrationsstrategie. Es ist wichtig, die richtige Balance zwischen den Anforderungen des Unternehmens und den technischen Möglichkeiten zu finden. Deutsche Unternehmen tendieren aus Gewohnheit zu einer One-Stop Lösungen – also Komponenten aus einer Hand zu beziehen. Mit Blick auf maximale Effizienz und die Reduzierung von Kostenfaktoren sollten Unternehmen jedoch über den Tellerrand hinausschauen. Mit einer Best-of-Breed-Strategie wählen sie Lösungen genau nach Bedarf und mit Blick auf den Unternehmenserfolg. Keine Sorge – die Erstellung eines detaillierten Konzepts für den Aufbau und die Verlagerung in die Cloud kann mehrere Iterationen durchlaufen, bevor die Migration abschließend umgesetzt wird.

**Daten sind der Schlüssel zur Unternehmensoptimierung**

Die Migration bietet Unternehmen eine resiliente Infrastruktur und verbessert Unternehmensprozesse entscheidend. Um Unternehmensprozesse zu optimieren und ihre Effizienz zu steigern, ist eine optimale technische Basis entscheidend und die Vorteile der IT-Optimierung resultieren somit in verbesserten Unternehmensprozessen. Damit gewinnt auch die Prozessintegration zunehmend an Bedeutung, um Prozesse und Systeme nahtlos zusammenzuführen und Wettbewerbsvorteile zu generieren. Ein häufiges Problem, vor dem Unternehmen stehen, ist der

Mangel an Echtzeit-Zugriff auf komplexe SAP-Daten und die Zusammenführung mit der individuellen Frontend-Lösung. Durch eine Prozessintegration in Echtzeit lässt sich die Genauigkeit zwischen den zwei Systemen sicherstellen, Fehler eliminieren und die Datenintegrität insgesamt verbessern. Zudem lässt sich das Hin- und Herpendeln zwischen SAP und der Frontend-Plattform erheblich reduzieren.

Optimierte und automatisierte Preisfindungs- und Angebotsprozesse sind hier ein interessantes Beispiel für viele globale Unternehmen. Vertriebsmitarbeiter stehen vor der Herausforderung, nur ungenauen Zugang zu Preis- und Bestandsdaten zu haben. Dies führt oft zu Fehlern, Margenverlust und verlängerten Zeiten für die Angebotserstellung. Gleichzeitig beeinträchtigen Unstimmigkeiten zwischen den SAP-Daten und der Frontend-Lösung die Zufriedenheit der Mitarbeiter und Kunden.

Eine Echtzeit Prozessintegration kann dieses Problem lösen. Der Echtzeit-Zugriff auf SAP-Daten und Prozesse sowie die Zusammenführung dieser Daten mit der Frontend-Plattform ermöglichen es dem Vertrieb, effizient auf vollständige und korrekte Informationen zuzugreifen. Dadurch können sie schneller auf Kundenanfragen und -wünsche reagieren. Auf diese Weise können die Teams effizienter und effektiver Umsätze generieren, ohne Kompromisse bei der Übersicht oder Genauigkeit ihre Daten eingehen zu müssen.

Gleichzeitig verfügt auch das Kundenservice-Team über vollständige und aktuelle Daten und kann die Kommunikation und den Service erheblich beschleunigen und verbessern. Unternehmen bieten so intern als auch extern eine bessere Nutzererfahrung und tragen damit zu mehr Loyalität unter Mitarbeitern und Kunden bei – entscheidend für den Unternehmenserfolg und die Bindung von Kunden und Fachkräften.

Gleichzeitig schaffen Unternehmen mit der Prozessintegration in Echtzeit eine optimale Grundlage für die Nutzung von Künstlicher Intelligenz, denn hier ist die Datenbasis entscheidend, um das voll Potential der KI auszunutzen und Unternehmensprozesse weiter zu optimieren.

DURCH EINE PROZESSINTEGRATION IN ECHTZEIT LÄSST SICH DIE GENAUIGKEIT ZWISCHEN DEN ZWEI SYSTEMEN SICHERSTELLEN, FEHLER ELIMINIEREN UND DIE DATENINTEGRITÄT INSGESAMT VERBESSERN.

**Gerald Schlechter,**
**CSO und Gründer von enosix**
**www.enosix.com**

**Zugriff auf SAP-Daten und Geschäftsprozesse in Echtzeit**

Unternehmen erlangen Echtzeit-Zugriff auf ihre Daten durch die Freigabe von SAP-Daten und die Nutzung von benutzerdefinierter Logik und Variantenkonfiguration ganz ohne Programmieraufwand. Bestehende SAP-Daten und Geschäftslogiken, die Unternehmen sich über Jahre im Backend aufgebaut haben, werden für die Frontend-Lösung virtualisiert. Dies wird durch Bereitstellungsservices unterstützt, um sicherzustellen, dass die Integrationen mit SAP nahtlos sind und der übergreifenden Strategie zur Unternehmensskalierung folgen.

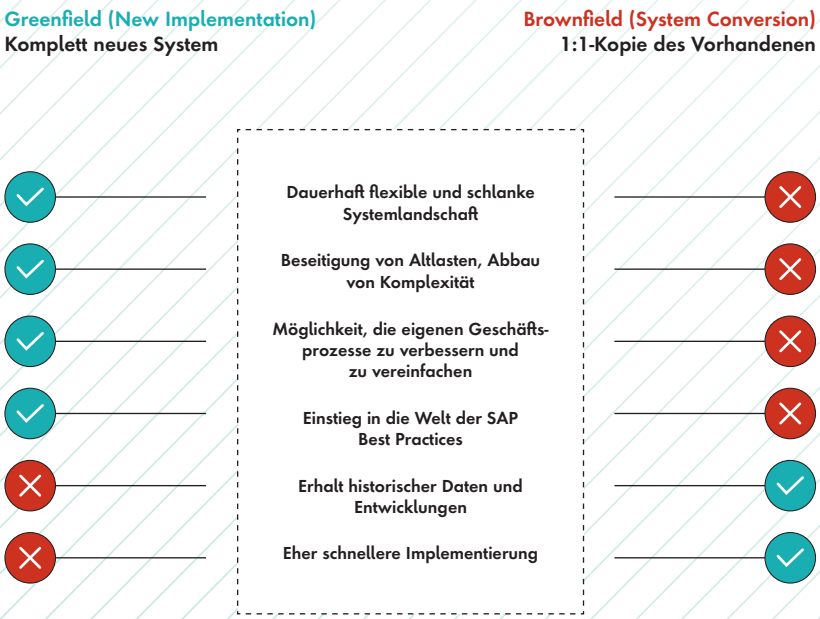
Ein Schlüsselelement hierbei ist der Packaged Integration Process (PIP). Dieser ermöglicht eine nahtlose SAP-Integration, ohne dass sie von qualifiziertem SAP-Personal entworfen oder programmiert werden muss. Eine nahtlose Low-Code-Integration ermöglicht eine bidirektionale Datenintegration zwischen den Systemen über eine API-Plattform, ohne dass Daten gespeichert oder dupliziert werden müssen. Der Echtzeit-Zugang zu SAP-Daten in der Frontend-Lösung erfolgt über eine Plattform, die eine bidirektionale, virtualisierte Datenintegration ermöglicht, indem sie komplexe Geschäftslogiken von SAP nutzt. Nutzer können über eine virtuelle Ansicht in ihrer Frontend-Lösung aus ihren SAP ECC- oder S/4HANA-ERP-Systemen heraus Echtzeit-Anfragen in jeder der Asset-Management-Anwendungen erstellen und unterstützen. Die Echtzeit-Integration des Variantenkonfigurationssystems verbessert zudem den Informationsaustausch zwischen den Produkt-Stakeholdern innerhalb des Unternehmens und ermöglicht schnelle Reaktionen auf Kundenanforderungen.

Obwohl eine solche Prozessintegration langwierig und aufwendig erscheinen mag, reduziert die Verwendung vorgefertigter Komponenten die Entwicklungszeit erheblich und ermöglicht eine schnelle Implementierung. Die Zeit bis zur Wertschöpfung lässt sich so im Vergleich zu einer internen Erstellung von Integrationen oder bei der Zusammenarbeit mit einem Systemintegrator signifikant reduzieren.

Ein vorgefertigtes Bedarfsdaten-Mapping beschleunigt die Implementierung zusätzlich. Mit solchen Lösungen können Frontend-System beispielsweise für Auftragsfreigaben und Versandinformationen Daten in Echtzeit mit hundertprozentiger Genauigkeit nutzen. Dabei ist die Integration in 70 Prozent der Zeit und bei reduzierten Kosten im Vergleich zu herkömmlichen Integrationsmethoden umsetzbar. Vorhandene Integrationssysteme sind oft kostspielig und stellen ein hohes Risiko dar, das Projekt aus Unternehmenssicht nicht erfolgreich umzusetzen, was sie ineffizient macht sowie die Sichtbarkeit der Daten behindert.

Mit diesem Ansatz gewinnt der Best-of-Breed-Ansatz auch für deutsche Unternehmen zunehmend an Bedeutung.

***Gerald Schlechter***




**Bei der Entscheidung zwischen Greenfield und Brownfield sollten Unternehmen ihre strategische Ausrichtung, ihre Geschäftsziele und technologischen Anforderungen berücksichtigen.**

# Fundierte Entscheidungen treffen

## MIT EINER ROADMAP ERFOLGREICH ZUM ZIEL

Noch immer stehen viele Unternehmen vor der Herausforderung, auf SAP S/4HANA umzusteigen. Das näher rückende Wartungsende von SAP ECC erhöht Tag für Tag den Handlungsdruck auf ECC-Kunden, der gewählte Weg auf SAP S/4HANA sollte aber gut überlegt sein. Jede Implementierung muss sorgfältig geplant und vorbereitet werden, um maximalen Mehrwert zu liefern – am besten mit einem Roadmap-Vorprojekt.

Einfache Lösungen gibt es nicht. Allgemeingültige leider auch nicht. Der Übergang zu SAP S/4HANA erfordert eine detaillierte Analyse und Berücksichtigung vieler Kriterien und individueller Voraussetzungen und Anforderungen. Diese reichen von der aktuellen IT-Landschaft und dem strategischen Nutzen der Umstellung bis hin zu den Kosten, Risiken und der Belastungsgrenze der eigenen Organisation.

### Ist die Konservierung des Status quo das Ziel?

Manche Unternehmen haben klare Vorstellungen von der passenden Migrationsstrategie. In meiner beruflichen Praxis habe ich zahlreiche SAP-ECC-Systeme untersucht, die 20 oder sogar 30 Jahre alt waren. Diese Systeme wurden immer wieder umgebaut, angepasst und gepatcht. Oft handelte es sich um klassische „Pain-Point-ERP-Systeme" – Systeme, bei denen eine einfache Schmerztherapie nicht mehr ausreicht.

Ein Beispiel für diesen „Pain": In einem Unternehmen passten nur noch 65 Prozent der damals implementierten Prozesse zu den aktuellen Geschäftsanforderungen – 35 Prozent hingegen nicht mehr. Das bedeutet für die Umstellung nach SAP S/4HANA: Eine 1:1-Brownfield-Conversion wäre hier eher kontraproduktiv, weil Bestehendes zementiert wird. Eine Greenfield-Neuimplementierung erscheint dagegen als die bessere Option, um die Prozesse grundlegend zu überarbeiten, zu modernisieren und zu optimieren.

In anderen Unternehmen ist ein solcher Neustart auf den ersten Blick nicht notwendig. Die Prozesse sind weitestgehend harmonisiert, das System ist gut wartbar und bereits an die neuen Spielregeln der SAP im Bereich Entwicklung angepasst. In solchen Fällen kann eine Brownfield-Conversion durchaus sinnvoll sein, um die bestehende Infrastruktur zu bewahren und die Investitionen der Vergangenheit zu schützen.

Allerdings – und das ist die Frage, die sich alle stellen sollten, die die Umstellung noch vor sich haben – sollten Unternehmen stets genau prüfen, in welche der beiden Unternehmens-Kategorien sie eher fallen. Auch wenn auf den ersten Blick vieles dafürspricht, kann eine Brownfield-Conversion – und damit eine Konservierung des Status quo – die Chancen auf Weiterentwicklung und Optimierung verspielen.

### SAP S/4HANA: Weit mehr als nur ein IT-Upgrade

Man kann es nicht oft genug sagen: Der Übergang zu SAP S/4HANA ist kein rein technisches IT-Projekt. Natürlich lässt sich die Umstellung auch kurz vor dem Wartungsende Ende 2027 von einer „Conversion Factory" innerhalb weniger Monate umsetzen. Doch die mit der Umstellung

verbundenen Chancen für das Unternehmen lassen sich so nicht voll ausschöpfen.

Die grundlegende Neugestaltung von Prozessen, der Zugang zu den SAP Best Practices oder zu neuen Technologien wie Künstlicher Intelligenz sowie die neuen Prinzipien für eine flexible SAP-Architektur können nur mit einer Neuimplementierung zur Gänze erschlossen werden. Wer SAP S/4HANA als Chance für eine weitreichende Modernisierung und als Katalysator für die Digitalisierung begreift, sollte mehr als nur ein IT-Upgrade anstreben.

Richtig ist: Die Entscheidung für den richtigen Ansatz – insbesondere also Greenfield oder Brownfield – ist komplex und weitreichend. Sie sollte daher nicht nur auf der Ausgangssituation, wenigen Parametern oder gar einem Bauchgefühl beruhen. Vielmehr müssen Unternehmen ihre strategische Ausrichtung, ihre Geschäftsziele und technologische Anforderungen berücksichtigen. Business und Technologie müssen in jedem SAP-S/4HANA-Projekt Hand in Hand gehen.

**Roadmap: Die Basis für fundierte Entscheidungen**

Damit ein Unternehmen eine passende Entscheidung treffen kann, ist eine Vorstudie mit einem SAP-Partner in jedem Fall zu empfehlen. Ein Roadmap-Programm hilft dabei, die individuellen Anforderungen, die strategischen und operativen Ziele sowie mögliche Herausforderungen zu analysieren und zu bewerten. Am Ende steht eine gesicherte Empfehlung für die Implementierung, die langfristig den meisten Mehrwert bringt.


Ein Roadmap-Programm umfasst in der Regel mehrere zentrale Punkte:

#1 Eine Analyse der strategischen Ziele und der langfristigen Ausrichtung.

#2 Die Untersuchung der Prozesslandschaft mit Blick auf SAP-S/4HANA-Standardabdeckungsgrad und -Potenziale.

#3 Eine Konzeption und Festlegung der Zielsystemarchitektur unter SAP S/4HANA.

#4 Eine Identifikation und das Management potenzieller Risiken des Projekts.

#5 Eine Kostenanalyse und Aufwandsabschätzung.

#6 Eine Bewertung der verschiedenen Migrationsszenarien und deren Machbarkeit.

#7 Eine Planung und die Strukturierung des Migrationsprojekts.

In Strategie-Interviews mit dem Top-Management zum Beispiel werden bei GAMBIT zu Beginn einer Vorstudie entscheidende Fragen geklärt, die für die Passgenauigkeit der späteren Umsetzung maßgeblich sind. Dies umfasst die Ziele des Unternehmens sowie individuelle Anforderungen und Pain Points, die gelöst werden sollen.

In weiteren Schritten werden die Unternehmensprozesse detailliert untersucht: Unsere SAP-Experten nutzen dazu entweder vorhandene Dokumentationen unserer Kunden oder ihr eigenes Prozesshaus, das sich an den SAP Best Practices orientiert. In Workshops mit der IT und den Fachbereichen erfolgt ein Abgleich der aktuellen Prozesse mit den Best Practices anhand entsprechender Übersichten.

Ein Demosystem – eine so genannte Fully Activated Appliance – ermöglicht es Unternehmen darüber hinaus, SAP S/4HANA schon zu einem sehr frühen Zeitpunkt live zu erleben und verschiedene Szenarien zu testen. Das System enthält vorkonfigurierte Best Practices sowie Demoszenarien mit beispielhaften Stamm- und Bewegungsdaten.

WER SAP S/4HANA ALS CHANCE FÜR EINE WEITREICHENDE MODERNISIERUNG UND ALS KATALYSATOR FÜR DIE DIGITALISIERUNG BEGREIFT, SOLLTE MEHR ALS NUR EIN IT-UPGRADE ANSTREBEN.

**Philipp Fischer,**
**SAP-Projektmanagement, GAMBIT**
**www.gambit.de**

**Der entscheidende Unterschied**

„Die Welt ist im Wandel." Dieses Zitat aus dem Roman „Der Herr der Ringe" trifft auch auf die Digitalisierung und die damit einhergehenden und notwendigen Veränderungen in Unternehmen zu. Sich dem Wandel nicht zu stellen, wäre fatal. In der heutigen dynamischen Geschäftswelt müssen Unternehmen agil und anpassungsfähig bleiben. Der richtige Weg zu SAP S/4HANA kann daher den Unterschied zwischen stagnierendem Tagesgeschäft und zukunftsorientiertem Erfolg ausmachen.

Der Umstieg auf SAP S/4HANA bietet enorme Chancen, birgt jedoch auch Herausforderungen, wenn Projekte nicht sorgfältig aufgesetzt und vorbereitet werden. Eine gewissenhafte Planung und fundierte Entscheidung auf der Basis eines strukturierten und erprobten Roadmap-Programms sind daher entscheidend für den langfristigen Erfolg.

***Philipp Fischer***

# Schlanke und effiziente SAP Brownfield Conversion

## MIGRATION FÜR MITTELSTÄNDISCHE UNTERNEHMEN

Die Migration von SAP ECC zu SAP S/4HANA ist für viele mittelständische Unternehmen (KMU) essenziell, um wettbewerbsfähig zu bleiben und zukünftigen Geschäftsanforderungen gerecht zu werden. Mit dem Support-Ende für SAP ECC im Jahr 2027 wird die Zeit nun knapp, um die Migration vorzubereiten und durchzuführen.

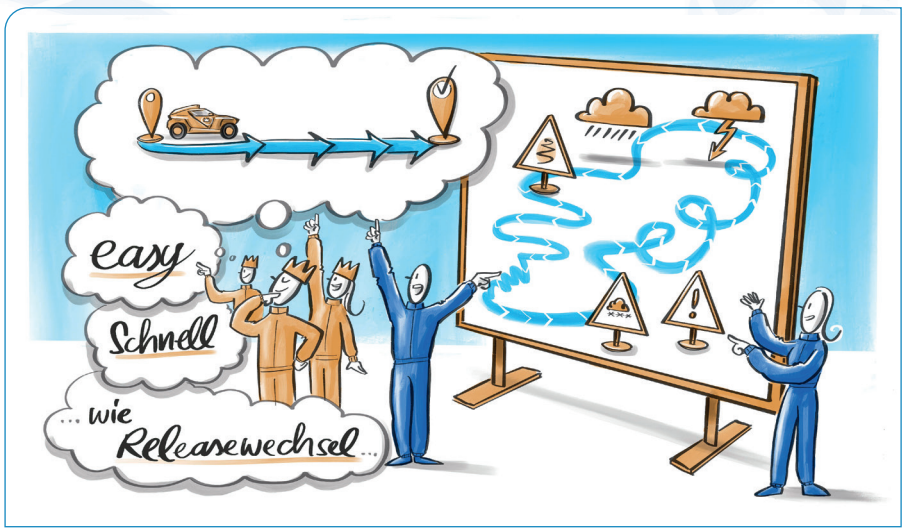
Viele KMU entscheiden sich derzeit dazu, die Transformation möglichst schlank und die Auswirkungen auf ihre Organisation möglichst gering zu halten. Mögliche Innovationen können nach der Transformation identifiziert und gehoben werden.

**Wie migriert man mit möglichst geringem Aufwand auf S/4HANA?** SPIRIT/21 hat einen schlanken und kosteneffizienten Ansatz zur SAP Brownfield Conversion entwickelt, der sich durch eine präzise Anpassung an die spezifischen Bedürfnisse jedes Unternehmens auszeichnet.

Unser Ansatz basiert auf der SAP Activate Methodik, die eine strukturierte und effiziente Projektdurchführung ermöglicht. Die Migration zu SAP S/4HANA beginnt mit wenigen, effizienten Assessment-Workshops, in denen wir weitgehend toolbasiert eine Handlungsempfehlung erstellen. Diese Analysen stimmen wir auf die fachlichen und technischen Anforderungen unserer Kunden ab und bieten eine klare Roadmap für die Umstellung.

Ein zentraler Aspekt unserer Methode ist die Minimierung von Risiken. Dies erreichen wir, in dem wir identifizieren, welche Umfänge in Vorprojekte verlagert werden können und welche Arbeitspakete direkt im Hauptprojekt bearbeitet werden. Ein Beispiel für notwendige Vorprojekte ist die technische Umstellung auf Unicode, die bei der Migration auf SAP S/4HANA zwingend erforderlich ist. Das neue Hauptbuch wiederum ist nicht unbedingt ein Vorprojekt, es sei denn, spezielle Anforderungen bestehen.

Dieser selektive Ansatz ermöglicht eine schlanke und effiziente Projektgestaltung.




Nach der Vorprojektphase, in der alle technischen Voraussetzungen für das Hauptprojekt geschaffen wurden, verfolgen wir einen Ansatz mit minimalen Sandbox-Iterationen. Diese Iterationen passen wir an die Komplexität der Geschäftsprozesse des Kunden an, um Zeit und Ressourcen optimal zu nutzen. Nach jedem Conversion-Prozess bewerten wir die Ergebnisse und entscheiden über die Notwendigkeit weiterer Sandbox-Iterationen in der Post Conversion Phase.

Ein weiterer wesentlicher Bestandteil unserer Methodik ist der effiziente Umgang mit Custom Code. Hierbei werden alle klar als obsolet identifizierbaren Umfänge gelöscht, sodass möglichst nur relevanter Code im SAP S/4HANA System verbleibt. Alle anderen Umfänge werden zunächst übernommen und, falls nötig, in einer zweiten Iteration tiefer betrachtet. Diese Maßnahme reduziert deutlich die Transformationskosten.

Bei der Migration sind Risiken wie kostspielige Archivierungen und unzureichende Datenmigration zu berücksichtigen, die zu Verzögerungen führen können. Besonders bei der Einführung neuer Module wie CVI/Business Partner sind Anpassungen notwendig. Ein häufiges Problem sind Inkonsistenzen in den Kundendaten. Ein Fall aus der Praxis zeigte, dass während der Migration Formatierungsprobleme in Kundendaten zu einer Datenbereinigung führen können. Durch unseren Best-Practice-Ansatz stellen wir eine effiziente und fortlaufende Datenvalidierung mit unserer Toolbox sicher, um Migrationsfehler zu vermeiden. Der Best-Practice-Ansatz umfasst daher die Datenanalyse, Datenbereinigung und kontinuierliche Validierung, um schnell und kos-

BEI DER MIGRATION SIND RISIKEN WIE KOSTSPIELIGE ARCHIVIERUNGEN UND UNZUREICHENDE DATENMIGRATION ZU BERÜCKSICHTIGEN, DIE ZU VERZÖGERUNGEN FÜHREN KÖNNEN.

**Dr. Björn Stark, SAP Project Manager, SPIRIT/21 GmbH, www.spirit21.com**

tengünstig die Migration und die Datenintegrität und Qualität zu gewährleisten.

Als Beispiel sei hier ein Kunde beschrieben, dessen veraltetes SAP ECC-System wir erfolgreich auf SAP S/4HANA modernisiert haben. Mit unserem Knowhow konnten wir eine nahtlose Migration auf SAP S/4HANA erreichen. Die Ist- und Soll-Analyse zeigte, dass das Unternehmen auf Unicode umstellen musste, während das neue G/L direkt in das Hauptprojekt integriert wurde. Dank unseres Change-Managements konnten alle Stakeholder den Mehrwert der Umstellung nachvollziehen.

Oder der Kunde, der in der ersten Welle das Backend-System auf S/4HANA umstellte und in der zweiten Welle die Fiori Apps einführte, um die SAP GUI zu ersetzen. Diese Strategie schonte Ressourcen und gewährleistete eine effiziente Umstellung.

Durch die signifikanten Ergebnisse unseres Brownfield-Ansatzes konnte ein anderer Kunde den Mehrwert der SAP S/4HANA RISE-Cloud in Folgeprojekten nutzen und von neuen, innovativen Technologien profitieren. Dazu gehören die Einführung von Green Ledger, Carbon Footprinting, sowie KI-gestützter Automatisierung.

Mit unserem Ansatz machen wir Unternehmen fit für die Zukunft, über 2027 hinaus. Unsere Methodik stellt sicher, dass technische Herausforderungen bewältigt werden, ohne das operative Geschäft zu beeinträchtigen. Durch gezielte Schulungen und starkes Change-Management sorgen wir für eine erfolgreiche Umstellung. Die Brownfield Conversion ermöglicht es, mit den neuesten Entwicklungen Schritt zu halten und die S/4HANA-Transformation so effizient und kostengünstig wie möglich zu gestalten.

***www.spirit21.com***

# Von reaktiver zu proaktiver Sicherheit durch KI

## NEUER TREND IN DER CYBERSECURITY

Angesichts der zunehmenden Datenflut stehen Unternehmen vor neuen Herausforderungen in Punkto Sicherheit. Nicht nur das Volumen an täglich neu generierten Informationen stellt ein Problem dar, sondern auch deren Vielfalt. In den Fokus der Aufmerksamkeit rücken dadurch unstrukturierte Daten, die beispielsweise durch E-Mails, KI-Anwendungen, soziale Medien oder auch Sensoren von IoT-Geräten generiert werden. Unternehmen müssen sich den Überblick über die unterschiedlichsten Datenströme zurückerobern, um deren Sicherheit garantieren zu können. Laut Kevin Schwarz, Head of CTO in Residence bei Zscaler rückt dabei nicht nur Zero Trust weiter in den Mittelpunkt, sondern auch die künstliche Intelligenz (KI).

**it management:** *Herr Schwarz, Sie sind gerade zurück von der jährlichen Zscaler Anwenderkonferenz Zenith Live. Welche Sicherheitstrends wurden dort diskutiert?*

**Kevin Schwarz:** Wir sehen derzeit eine Reihe von übergeordneten Strömungen, die sich auf die Sicherheit von Unternehmen auswirken. Data Governance muss mit Sicherheit Hand in Hand gehen, wenn immer mehr Daten erfasst, verarbeitet und analysiert, aber eben auch vorgehalten werden. Hinzu kommt der fortwährende Bedarf an Cloud-nativen Lösungen, der von einer zunehmenden Nachfrage nach Automatisierung beflügelt wird. In diesem Zuge wird DevSecOps eine noch wichtigere Rolle spielen. Eine Thematik die viel diskutiert wurde, ist die Transformation von Netzwerkumgebungen. Dort sehen wir eine erhöhte Nachfrage nach Network-as-a-Service, die auch neue Sicherheitsansätze erforderlich macht.

**it management:** *Lassen Sie uns einen Blick auf die Netzwerktransformation werfen. Warum spielt hier der Sicherheitsaspekt eine Rolle?*

**Kevin Schwarz:** Das klassische Netzwerkperimeter-Modell verliert derzeit rasch an Bedeutung. Anwendungen wandern in die Cloud, Mitarbeitende greifen von überall aus darauf zu und die Konvergenz von IT/OT mit der Anbindung über Mobilfunknetze geht mit neuen Anforderungen an die Sichtbarkeit weiterer Datenströme einher, um diese auch überwachen zu können. Cloud-Fabrics, die als Service angebunden werden, lösen die klassischen Netzwerke nach und nach ab. Was jahrzehntelang intern an Hardware vorgehalten wurde, verliert durch neue Formen der Konnektivität an Bedeutung und erfordert Sicherheit als Plattformansatz, die auf Basis von Cloud-basierten Zero Trust-Lösungen für alle Kommunikationskanäle lückenlos greift.

**it management:** *Zero Trust ist demnach weiter auf dem Vormarsch durch neue Anwendungsfälle?*

**Kevin Schwarz:** Zero Trust greift heute nicht nur für die Absicherung des User-Datenverkehrs, sondern die Prinzipien der Least Privileged Zugriffsrechte erlangen auch für Workloads oder die Absicherung von IoT-/OT-Geräten an Bedeutung. Gerade in OT-Umgebungen, die zwar oft von der klassischen IT segmentiert sind, fehlt eine granularere Sichtbarkeit über die vorhandenen Geräte und Kommunikationsströme. Durch die Akquisition von Airgap kann ein „Network of One" geschaffen werden, welches verhindert, dass Clients auf den Geräten in der Produktion installiert werden, die Produktionsabläufe potenziell unterbrechen könnten. Zscaler kann hierdurch nun eine Segmentierung des East-/West-Traffics abdecken, die für die Digitalisierung von Produktionsstätten relevant wird.

**it management:** *Wie kommt bei Sicherheitsunternehmen wie Zscaler die künstliche Intelligenz zum Tragen?*

**Kevin Schwarz:** KI verrichtet schon heute wichtige Dienste, um KI-gesteuerte Angriffe zu erkennen. Wenn die Angreifer aufrüsten und beispielsweise ihre Phishing-Angriffe durch Zuhilfenahme von GenAI-Tools noch personalisierter gestalten, so dass der einzelne User noch weniger Chancen hat, diese zu erkennen, müssen auch die Abwehrmechanismen auf diese Technologien setzen. Dabei verrichtet die KI sehr gute Dienste bei der Korrelation der immensen Datenmengen, um Anomalien effizienter und schneller zu erkennen. Mit Breach Predictor geht Zscaler den Schritt von der reaktiven zur proaktiven Sicherheit.

**it management:** *Können Sie diesen Mechanismus der proaktiven Vorhersage von Angriffen genauer erläutern?*

**Kevin Schwarz:** Zscaler Breach Predictor warnt Organisationen, wenn Faktoren in der IT Umgebung zusammentreffen, die auf potenzielle Cybervorfälle hindeuten und löst darauf aufbauend nicht nur einen Alarm aus, sondern schlägt die zu tätigenden Schritte vor und oder blockiert die verdächtigen Transaktionen. Durch die Übernahme von Avalor ist Zscaler in der Lage, umfangreiche externe Datensätze in die Analyse möglicher Angriffsszenarien einzubeziehen. Diese Übernahme ist wichtig, da jede Sicherheitsplattform meist nur Auskunft darüber geben kann, was sie selbst verarbeitet und/oder erarbeitet. Aufbauend auf den angepassten Datenmodellen kann die KI in der Zero Trust Exchange-Plattform ihre Stärken ausspielen und eben die Aktionen der Angreifer durch Analyse über verschiedenste Datenquellen hinweg vorhersagen. Werden also erste Warnzeichen von bekannten Angriffsmustern in einer Umgebung aufgespürt, wird die Wahrscheinlichkeit der nächsten Schritte prognostiziert und Gegenmaßnahmen vorgeschlagen, so dass proaktive Abwehr erfolgt.

**it management:** *Und was genau verbirgt sich hinter der Aussage: „Fighting AI with AI"?*

**Kevin Schwarz:** Wir verstehen darunter den Einsatz künstlicher Intelligenz zur Erkennung von KI-gesteuerten Angriffen, die in der Zscaler Cloud und in externen Quellen erkannt wurden. Durch die intelligente Analyse des gesamten Netzwerkdatenverkehrs und der Korrelation von Verhaltensmustern mit schädlichen Aktivitäten lässt sich die Angriffswahrscheinlichkeit vorhersagen. Durch die Benachrichtigung der IT-Abteilung können Sicherheitsvorfälle unterbunden und dadurch Betriebsbeeinträchtigungen, die Kosten von Angriffen oder Imageschäden abgefedert werden. Die KI kommt zur Risikomitigierung zum Einsatz und beugt Schäden durch KI-basierte Angriffe vor.

**it management:** *Warum sind solche modernen Maßnahmen heute nötiger denn je?*

**Kevin Schwarz:** Die Angreifer waren schon immer erfinderisch. Letztlich müssen sie nur einmal erfolgreich sein, um Schaden in einem Unternehmen anzurichten, wohingegen die Abwehr kontinuierlich lückenlos greifen muss angesichts sich stetig wandelnder Angriffsmuster. Die jüngsten Vishing-Angriffe - Voice Phishing - haben verdeutlicht, dass Anwender viel mehr hinterfragen müssen, wem oder was sie eigentlich noch vertrauen können. Hier wird deutlich, dass die Vielzahl an Datenschätzen, die im Internet über Unternehmen auffindbar sind, auch jederzeit gegen sie verwendet werden können. Unternehmen tun gut daran, die Souveränität über ihre Daten zurückzuerlangen.

ZSCALER BREACH PREDICTOR WARNT ORGANISATIONEN VOR POTENZIELLEN CYBERVORFÄLLE, SCHLÄGT DIE ZU TÄTIGENDEN SCHRITTE VOR UND ODER BLOCKIERT DIE VERDÄCHTIGEN TRANSAKTIONEN.

**Kevin Schwarz,**
**Head of CTO in Residence, Zscaler,**
**www.zscaler.de**

**it management:** *Was ist Ihr letzter Tipp zum Thema Datensicherheit?*

**Kevin Schwarz:** Der Schutz kritischer Datenbestände gewinnt weiter an Bedeutung. Daher ist es für Unternehmen zu empfehlen, sich jetzt mit den einzelnen Datenströmen und der Klassifizierung von kritischen Daten zu befassen. Wenn wir eins feststellen können durch das Thema AI und GenAI ist es, dass die Segmentierung auf Datenebene mehr und mehr in den Fokus gerät.

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

THANK YOU

# Cybersecurity-Ökosystem

## NEUE STRATEGIEN UND DIE VERANTWORTUNG DER CHEFS

Dass Cybersecurity bei der Vielfalt der Angriffsarten und der Intensität keine einfache Sache mehr ist, müsste mittlerweile jedem Unternehmen klar sein. Doch wie genau sieht die Gefahrenlage aus und mit was müssen Unternehmen bei einer Cyberattacke rechnen? Was genau braucht es, um die zunehmend komplexen und vernetzten IT-Strukturen und die wertvollen Daten vor Cyberangriffen zu schützen? Darüber sprechen der Herausgeber von it management Ulrich Parthier und der Sophos Director Channel Sales für Sophos EMEA Central Stefan Fritz.

? **Ulrich Parthier:** *Behörden wie das BSI oder Organisationen wie der Bitkom warnen von immer komplexeren Angriffen und fordern Unternehmen und Organisationen intensiv auf, sich gegen die Cybergefahren zu schützen. Ich gehe davon aus, dass Sie diese Meinung teilen?*

**Stefan Fritz:** Ja, die Warnungen von offiziellen Stellen und auch aus der Sicherheitsbranche sind berechtigt. Dem immer noch zunehmend professionellen Verhalten der Cyberkriminellen und den Folgen eines Angriffs kann nur mit einer ausgefeilten Sicherheitsstrategie begegnet werden. Unsere Forensik-Teams und weltweite Studien bestätigen das hohe Gefahrenpotenzial für jede Art von Unternehmen und Organisation.

? **Ulrich Parthier:** *Wenn man Ihren letzten State of Ransomware Report liest, wird gleich am Anfang über einen leichten Rückgang der Ransomware-Angriffe berichtet. Heißt das, dass sich die Lage entspannt?*

**Stefan Fritz:** Es gibt einen leichten Rückgang der Cyberattacken mit Ransomware im Vergleich zur Vorjahresstudie. Wir reden hier aber von einem sehr hohen Niveau. 2022 wurde 66 Prozent aller weltweit befragten Unternehmen mit Ransomware angegriffen, 2023 waren es nach wie vor 59 Prozent – sprich noch deutlich mehr als die Hälfte. Das ist aber nicht der springende Punkt. Mittlerweile werden in nahezu allen Fällen die Backups in Mitleidenschaft gezogen, sodass Unternehmen kaum noch in der Lage sind, daraus ihre Systeme wiederherzustellen. Nur 68 Prozent der im vergangenen Jahr angegriffenen Unternehmen konnten aus den Backups die Daten und Systeme wiederherstellen, 2022 waren es noch 73 Prozent. Dieser Umstand führt dazu, dass Unternehmen dazu neigen, die Erpressungssummen zu bezahlen und diese haben sich um mehr als das 2,5-fache auf durchschnittlich 3,0 Millionen Dollar erhöht.

? **Ulrich Parthier:** *Aber dafür gibt es ja zum Glück Cyberversicherungen.*

**Stefan Fritz:** So einfach ist es leider nicht, denn es ist heutzutage sehr schwer, überhaupt einen Versicherungsschutz zu bekommen und wenn, dann werden seitens der Versicherung extrem hohe Ansprüche an die getroffenen Security-Maßnahmen gestellt. Auch in diesem Bereich haben wir in unserer aktuellen Studie einige Daten erhoben. Über 70 Prozent der befragten privatwirtschaftlichen Unternehmen gaben an, eine Cyberversicherung zu haben. Hingegen nur 19 Prozent der angegriffenen Unternehmen bezahlten die Lösegeldsumme über die Versicherung. Das gibt zu denken.

? **Ulrich Parthier:** *Lassen Sie uns einen Blick auf die Verantwortlichkeiten rich-*

*ten. In der Vergangenheit war Cybersecurity hauptsächlich eine Aufgabe der IT. Es scheint jedoch Verschiebungen hin zum Management zu geben. Welche Verantwortlichkeit treffen Sie bei Ihren Kunden an?*

**Stefan Fritz:** Richtig, die Security wird aus strategischer Sicht mehr zum Managementthema – je nach Unternehmensgröße, Unternehmensstruktur und Branche ein wenig unterschiedlich in der Ausprägung. Das ist auch richtig so, denn die Schäden, die einem Unternehmen durch Cyberangriffe entstehen, sind ein Managementthema, sowohl wirtschaftlich als auch aus Reputationsperspektive. Einen Ruck in Richtung Managementverantwortlichkeit gibt es auch durch Gesetze und Vorgaben wie NIS2. Dass jetzt die Geschäftsleitung persönlich im Falle eines Cyberangriffs haftbar gemacht werden kann zeigt klar, welche Wertigkeit von Politik und Gesetzgeber in eine gute Cyberresilienz gelegt wird. Allerdings zeigen unsere Erhebungen in DACH, dass im vergangenen Jahr trotz der teils existenzbedrohenden Angriffe und trotz der neuen Gesetze die Security erst bei 16 Prozent der deutschen Unternehmen Chefsache ist.

**Ulrich Parthier:** *Wird das Verantwortungsbewusstsein im Management weiterhin ansteigen?*

**Stefan Fritz:** Ich denke ja, und das nicht nur wegen des Zwangs durch neue Gesetze. Der Anteil der Cyberresilienz an einem erfolgreichen Business ist mittlerweile derart hoch, dass das Management dieses strategische Thema zunehmend beachten wird.

**Ulrich Parthier:** *Lassen Sie uns über Schutzmöglichkeiten sprechen, was vermutlich im Detail auch weiterhin ein Thema des CSO, CTO oder der IT-Abteilung bleiben wird. Verfolgt man die breit gefächerten Aspekte der Cybersecurity, scheint es eine Mammutaufgabe zu sein, einen wirksamen Schutz zu etablieren und vor allem aufrechtzuerhalten.*

> EINE SECURITY WIE FRÜHER, DIE HAUPTSÄCHLICH AUS EINEM VIRENSCHUTZ UND EINER FIREWALL BESTAND, IST HEUTE BEI WEITEM NICHT WIRKSAM GENUG, UM EINEN ANGEMESSENEN SCHUTZ ZU BIETEN.
>
> **Stefan Fritz, Director Channel Sales für Sophos EMEA Central, Sophos, www.sophos.de**

**Stefan Fritz:** Die Security ist ein hoch komplexes Thema und bei der Steigerung der Komplexität, ist kein Ende in Sicht. Das liegt unter anderem daran, dass die Angreifer ihre Taktiken sehr schnell weiterentwickeln, sehr professionelle Netzwerke an Cyber-Crime-Spezialisten betreiben und auf der anderen Seite immer mehr Unternehmen digitalisiert beziehungsweise untereinander vernetzt sind.

Eine Security wie früher, die hauptsächlich aus einem Virenschutz und einer Firewall bestand, ist heute bei weitem nicht wirksam genug, um einen angemessenen Schutz zu bieten. Und die heute verfügbare Vielfalt an Security-Maßnahmen und Tools ist schier unendlich und nur von Spezialisten zu beherrschen – die nebenbei gesagt, insbesondere im Mittelstand Mangelware sind.

**Ulrich Parthier:** *Und die Lösung beziehungsweise Alternative für dieses Problem ist?*

**Stefan Fritz:** Immer mehr Unternehmen verstehen, dass sie die Vielfalt der Security mit eigenen Ressourcen und Budgets nicht mehr stemmen können. Im Grunde müssten auch mittelständische Unternehmen äquivalent zu Konzernen ein Security Operation Center (SOC) einrichten, um adäquat geschützt zu sein. Das kostet aber enorm viel Geld und personelle Ressourcen.

Die Alternative ist ein Security-Ökosystem, das unter einer Plattform alle Aspekte der Security zusammenführt. Einzelne Security-Komponenten sind unter einem Dach vereint, intelligent vernetzt und durch Services und menschliche Security-Experten ergänzt. Ein weiterer wichtiger Teil des Ökosystems sind die entscheidenden Telemetriedaten, die wir selbst aber auch von Dritten sammeln und auswerten. Ergänzt wird das Ökosystem durch Lösungen und Dienste von Partnerunternehmen, wie beispielsweise Tenable mit ihrer Cloud-fokussierten Security. Im Grunde ist dieses Ökosystem sogar noch mehr als ein SOC, jedoch managebar, leicht skalierbar und vor allem den budgetären und personellen Ressourcen im Mittelstand angepasst. Und es ist darauf zugeschnitten, dass es ein mittelständisches Unternehmen selbst oder durch einen unserer Partner betrieben werden kann.

**Ulrich Parthier:** *Die Plattform beziehungsweise das Ökosystem machen die Security also einfacher?*

**Stefan Fritz:** Exakt, und nicht nur einfacher, sondern auch wirksamer. Indem Unternehmen und Organisationen wie in vielen anderen Bereichen der IT auch, den Betrieb und die Services an spezialisierte externe Partner geben, wird die benötigte Cyberresilienz zur Realität. Man würde ja auch keine eigene Public Cloud aufbauen, um Cloud-Services nutzen zu können.

**Ulrich Parthier:** *Vielen Dank Herr Fritz für das Gespräch und die Einblicke in die Security-Strategien von heute und morgen.*

# Logistik goes digital

## DIGITALE DATENINTEGRATIONSSYSTEME FÜR MEHR ZUVERLÄSSIGKEIT

Wesentlicher Bestandteil wirtschaftlichen Wachstums ist der globale Handel. Welche Folgen eine Unterbrechung des Warenaustauschs hat, mussten viele Länder während der Corona-Krise schmerzlich erfahren. Die internationalen Lieferketten sind inzwischen wieder in Schwung gekommen, stattdessen erschweren Wirtschaftssanktionen den weltweiten Handel. Immer mehr zeigt sich, wie wichtig die Digitalisierung von Logistikprozessen ist.

Laut Statista werden über 90 Prozent der weltweit gehandelten Güter mit Schiffen transportiert. Die Bedeutung der maritimen Wirtschaft ist dabei sowohl für die globalisierte Welt als auch für Deutschland enorm: Allein 2021 beförderte der Seegüterverkehr in Deutschland knapp 289 Millionen Tonnen. Es bietet sich also an, die Digitalisierung der Hafenlogistik genauer unter die Lupe zu nehmen und daraus Schlüsse für andere Logistikstrukturen zu ziehen.

Die IT-Landschaft von Warenumschlagsplätzen, wie Häfen, Bahnhöfe, Flughäfen oder Logistikzentren, sind mit einem lebendigen Nervensystem vergleichbar. Hier interagiert eine Vielzahl hochentwickelter Technologien, Plattformen und Akteure miteinander, um Prozesse möglichst smart zu koordinieren. Im Zentrum des Systems steht die Vernetzung der digitalen mit der physischen Welt – von der Produktion über die Lieferung bis hin zum Kunden. Die Vernetzung der Daten bildet dabei die Grundlage für den Austausch der Waren.

**Die zentralen Zukunftsaufgaben**

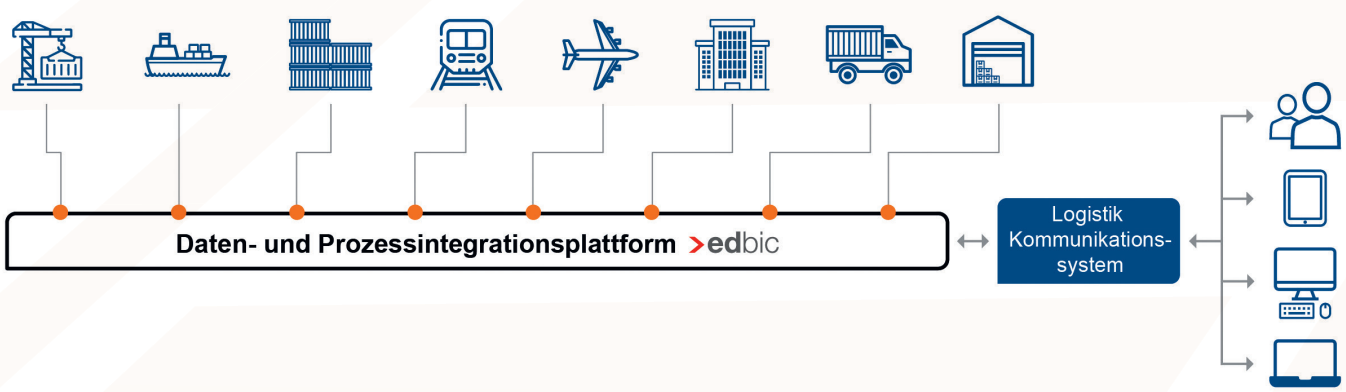
In der maritimen Wirtschaft spielen sogenannte Port Community Systeme (PCS) eine wichtige Rolle. Sie sind eine Art Gehirn, das den Informationsaustausch zwischen den verschiedenen Hafenbeteiligten orchestriert. Als ausführende Hände fungieren die sogenannten Terminal Operating Systems (TOS), denn sie sind für die Bewegung von Containern und Ressourcen verantwortlich, haben aber auch überwachende und steuernde Funktionen.

Darüber hinaus gibt es Zollsysteme, die einen reibungslosen Fluss der Zollformalitäten gewährleisten sollen. Sie sind auch mobil nutzbar, damit die verschiedenen Akteure jederzeit auf Informationen zugreifen und am Logistikprozess partizipieren können. In vielen Häfen, aber auch Bahnhöfen, Flughäfen und Logistikzentren setzt man heutzutage auf moderne Sensoren-Technologie, die über das Internet of Things (IoT) an die anderen Systeme angebunden ist und eine Echtzeitüberwachung und Steuerung physischer Güter ermöglicht. Damit sind die IT-Strukturen internationaler Häfen nicht nur auf die aktuellen Herausforderungen ausgerichtet, sondern auch darauf, zukunftsweisende Technologien zu integrieren und nachhaltige Lösungen für den weltweiten Warenverkehr zu unterstützen. Die nahtlose Integration der verschiedenen Systeme und enge Zusammenarbeit der Beteiligten sind unerlässlich, um dieses komplexe Technologienetzwerk harmonisch zu gestalten. Hilfreich dabei sind zentrale Daten- und Prozessintegrationsplattformen, wie beispielsweise edbic von compacer.

**Daten- und Prozessintegration**

Eine solche Daten- und Prozessintegrationsplattform ist das Rückgrat einer Logistiklandschaft. Sie ermöglicht die umfassende Koordination der Prozesspartner, optimiert logistische Abläufe, minimiert Fehler, verbessert die Effizienz der Lieferkette und sorgt für ein neues Maß an Prozessagilität.

## DIGITALISIERUNG, AUTOMATISIERUNG UND INTEGRATION



**Vier elementare Aspekte sind dabei wichtig:**

## #1 Datenintegration

**Datenkonsistenz:** Eine Integrationsplattform wie edbic sorgt dafür, dass Daten konsistent und in Echtzeit zwischen den verschiedenen Systemen ausgetauscht werden. Damit wird sichergestellt, dass alle beteiligten Parteien auf aktuelle und präzise Informationen zugreifen können.

**Interoperabilität:** Durch die Integration unterschiedlicher Datenformate und -quellen entsteht eine reibungslose Interaktion zwischen den verschiedenen Akteuren und Systemen.

## #2 Prozessintegration

**Effizienzsteigerung:** Eine Integrationsplattform ermöglicht die Automatisierung von Geschäftsprozessen und reduziert damit die Anzahl manueller Prozesse.

**Echtzeitüberwachung:** Abläufe können in Echtzeit überwacht und bei Bedarf verändert werden.

## #3 Flexibilität und Skalierbarkeit

**Anpassungsfähigkeit:** Integrationsplattformen sind flexibel und können sich ändernde Anforderungen und Technologien anpassen. Das ermöglicht es, mit den sich weiter entwickelnden Technologien Schritt zu halten.

**Skalierbarkeit:** Die Skalierbarkeit hilft, das Wachstum eines Logistikknotens zu steuern und der steigenden Anzahl beteiligter Parteien gerecht zu werden.

## #4 Sicherheit und Compliance

**Datensicherheit:** Eine Daten- und Prozessintegrationsplattform trägt zur Datensicherung bei, indem sie für einen sicheren Datenaustausch sorgt und sensible Informationen schützt.

**Compliance:** Die Plattform hilft bei der Einhaltung gesetzlicher und spezifischer Vorschriften, insbesondere im Hinblick auf den Datenaustausch und die Verarbeitung von Informationen.

Von diesen Funktionen profitieren beispielsweise folgende Systeme, die angeschlossen werden können:

- **Zollsysteme:** Integration mit Zollbehörden; elektronischer Datenaustausch für Import- und Exportdokumente, Zolldeklarationen und Zollabfertigung.
- **Terminal Operating System (TOS):** Integration mit TOS für die Verwaltung von Hafenoperationen, Containerbewegungen und Lagerhaltung sowie Echtzeitüberwachung von Schiffs- und Containerbewegungen und Lagerbeständen.
- **Reedereisysteme:** Integration mit den Systemen von Reedereien zur Koordination von Schiffsankünften, Abfahrten und Containerbewegungen und den Austausch von Frachtinformationen und Dokumenten mit den Reedereien.
- **Transport Management System (TMS):** Unterstützt bei der Planung, Ausführung und Optimierung von Transportprozessen und beinhaltet Funktionen wie Routenplanung, Frachtkostenkalkulation, Tracking und Tracing von Sendungen, sowie Frachtraumverwaltung.
- **Behördliche Systeme:** Integration von Behördensystemen, um verwaltungsmäßige Genehmigungen, Inspektionen und andere regulatorische Anforderungen zu unterstützen, inkl. Daten über Umweltauflagen und Sicherheitsstandards.
- **Finanzsysteme:** Integration mit Finanzsystemen für die automatisierte Abwicklung von Zahlungen, Gebühren und Rechnungen im Zusammenhang mit Logistikaktivitäten.
- **Transport- und Verkehrssysteme:** Integration mit Systemen für den Straßen- und Schienenverkehr, um die nahtlose Verbindung zwischen den Verkehrsträgern zu gewährleisten, inkl. Echtzeitüberwachung von Transportbewegungen und Lieferungen.
- **Warehousing-Systeme (WMS):** Integration mit Lagerverwaltungssystemen für die Überwachung von Lagerbeständen und -bewegungen sowie die Automatisierung von Prozessen.

LOGISTIKORGANISATIONEN SOLLTEN SCHNELLSTMÖGLICH IN SMARTE INTEGRATIONS-TECHNOLOGIEN INVESTIEREN SOWIE IN EINE DIGITALISIERUNG IHRER VERWALTUNGSPROZESSE.

**Volker Hettich, Head of Business Development, compacer GmbH, www.compacer.com**

**Fazit**

Logistikorganisationen, egal ob es sich um Häfen, Speditionen, Flughäfen oder Umschlagsbahnhöfe handelt, sollten schnellstmöglich in smarte Integrations-Technologien investieren sowie in eine Digitalisierung ihrer Verwaltungsprozesse. Durch das Zusammenspiel dieser Systeme an einer zentralen Stelle (Single-Window) in einer Daten- und Prozessintegrationsplattform, wird der bürokratische Aufwand reduziert, die Effizienz der Lieferkette gesteigert, die Handelsabwicklung beschleunigt sowie Kosten minimiert. Zudem bilden diese Struktur und Daten die Basis für weitere zukunftsweisende Veränderungen.

***Volker Hettich***

# IT-Servicemanagement

## EIN RELIKT DES LETZTEN JAHRHUNDERTS ODER NOCH IMMER RELEVANT?

**MEHR WERT**
TOPdesk Buyer's Guide: Die ideale ITSM-Lösung für Ihre Organisation

IT-Servicemanagement entstand bereits in den 80ern und ist somit keine neue Disziplin. Die Frage nach seiner heutigen Relevanz ist daher durchaus berechtigt. Aber tatsächlich sind die Prinzipien des ITSM heute aktueller denn je. Wir verraten Ihnen, warum wir das so sehen.

**Warum ist ITSM nach wie vor relevant?**

ITSM wurde in einer Zeit entwickelt, als Organisationen weltweit immer technisierter wurden und die Informationstechnologie Einzug in nahezu alle betrieblichen Prozesse erhielt. Heute erleben wir erneut eine Ära rascher technologischer Fortschritte – KI, Cloud Computing und andere Innovationen verändern unseren Arbeitsalltag tiefgreifend. Um mit diesen Veränderungen Schritt zu halten und die neuen Prozesse effektiv in die Organisation einfließen zu lassen, braucht es ein strukturiertes, sicheres und transparentes Vorgehen. Dies lässt sich mittels ITSM optimal steuern.

Ein weiterer wichtiger – wenn nicht der wichtigste – Grund für die Notwendigkeit von ITSM ist die Usability. Hier hat sich die Erwartungshaltung in den letzten Jahren stark verändert: Unternehmen wie Amazon, Zalando und Netflix haben erkannt, dass zufriedene Kunden hohe Umsätze garantieren – und bieten ihren Nutzern daher erstklassigen Service und intuitive Touchpoints. Dies führt zu steigenden Serviceerwartungen bei Mitarbeitern und Kunden. Ohne ITSM-Tool sind diese kaum zu erfüllen. Mithilfe einer smarten Lösung hingegen können die Erwartungen sogar übertroffen werden! Dies sorgt für exzellenten Service, begeisterte Melder und zufriedene Servicedesk-Mitarbeiter.

**Risiken des Verzichts auf ITSM**

Was passiert, wenn Organisationen keine Lösung fürs IT-Servicemanagement einsetzen? Da ein ITSM-Tool unter anderem eine solide Basis für die Implementierung neuer Technologien und Innovationen darstellt, verlieren Unternehmen ohne ITSM-Lösung einen Teil ihrer Flexibilität, Agilität und letztendlich ihrer Wettbewerbsfähigkeit.

Vor allem aber im Arbeitsalltag der IT-Abteilungen zeigen sich deutliche Defizite, wenn keine passende Softwarelösung zum Einsatz kommt:

**#1 Ressourcenverschwendung:** Ohne standardisierte Prozesse und eine transparente Übersicht werden Ressourcen ineffizient genutzt.

**#2 Erhöhte Betriebskosten:** Ineffiziente Abläufe führen zu höheren Kosten.

**#3 Verzögerungen bei der Servicebereitstellung:** Mangelnde Optimierung führt zu längeren Bereitstellungszeiten und unzufriedenen Mitarbeitern.

Ohne die im ITSM integrierten Verfahren und Kontrollen wird auch die IT-Sicherheit geschwächt. Dies erhöht das Risiko von Datenlecks, Datenschutz-Verletzungen und Cyberangriffen.

**Braucht Ihre Organisation eine IT-Servicemanagement-Lösung?**

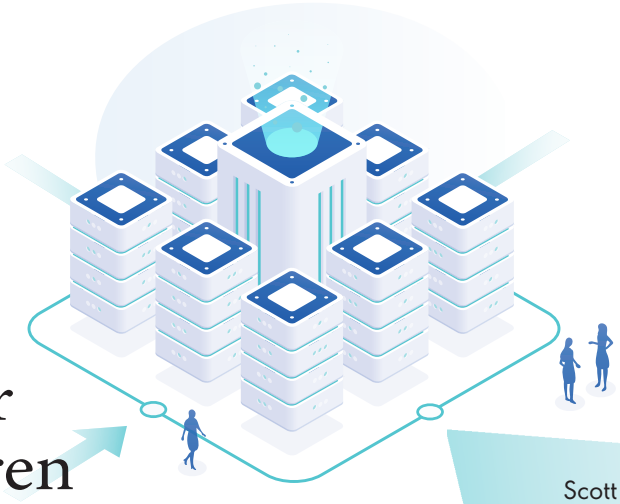
Wenn Sie eine der folgenden Fragen mit „Ja" beantworten, sollten Sie sich Gedanken über die Einführung oder Aktualisierung einer ITSM-Lösung machen:

- Ist der Erfolg Ihrer Organisation von einer möglichst fehlerfreien IT abhängig?
- Gibt es ungeplante Ausfallzeiten oder Verzögerungen bei Ihren IT-Services?
- Wollen Sie immer alle Aspekte der IT-Sicherheit und Compliance im Blick behalten?
- Benötigen Sie verlässliche Reportings, um zu erkennen, wie leistungsfähig Ihre IT ist und wo es Verbesserungsmöglichkeiten gibt?
- Möchten Sie den Nutzern Ihres Helpdesks den bestmöglichen IT-Service bieten?

***Dominik Hagen***

> OHNE DIE IM ITSM INTEGRIERTEN VERFAHREN UND KONTROLLEN ZUR INFORMATIONSSICHERHEIT WIRD AUCH DIE IT-SICHERHEIT IHRER ORGANISATION GESCHWÄCHT.

**Dominik Hagen, Business Development Manager, TOPdesk Deutschland GmbH, www.topdesk.de**



# Wachsende Kapazität europäischer Rechenzentren

## MARKT BLEIBT TROTZDEM UNTERVERSORGT

Nach Analysen von Savills wird die Kapazität von Rechenzentren in Europa bis 2027 um 21 Prozent auf etwa 13.100 Megawatt (MW) ansteigen. Damit entspricht der erwartete Kapazitätszuwachs dem jährlichen Energiebedarf von mehr als einer halben Million Haushalte. Die Internet-Bandbreitennutzung in Europa wird voraussichtlich allerdings noch wesentlich stärker wachsen, nämlich um 31 Prozent bis 2030. Die Lücke zwischen der vorhandenen und der nachgefragten Rechenzentrenkapazität wird sich also vergrößern.

Der europäische Markt für künstliche Intelligenz wird voraussichtlich mit einer jährlichen Rate von 15,9 Prozent bis 2030 wachsen und damit ein wichtiger Treiber für den Anstieg der Nachfrage nach Rechenzentren sein.

Nach Angaben des internationalen Immobilienberaters sollen in den nächsten vier Jahren 94 neue europäische Rechenzentrumsprojekte mit einer Gesamtleistung von rund 2.800 MW realisiert werden.

Scott Newcombe, EMEA Head of Data Centres bei Savills, kommentiert: „Trotz der hohen Anzahl an neuen Rechenzentren, die bis 2027 voraussichtlich gebaut werden, wird der Markt in ganz Europa wahrscheinlich weitgehend unterversorgt bleiben. Angesichts der prognostizierten Ausweitung der Internet-Bandbreitennutzung muss sich die Kapazität der europäischen Rechenzentren bis 2027 verdreifachen und eine Leistung von rund 22.700 MW erreichen, so dass nach wie vor eine erhebliche Angebots-/Nachfragelücke besteht."

***www.savills.de***

# Synergie der Superkräfte

## WIE EDGE UND CLOUD GEMEINSAM GLÄNZEN

Digitale Daten sind vielseitig und aus dem Alltag nicht mehr wegzudenken. Entscheidend sind jedoch nicht nur die Daten selbst, sondern auch ihre Verarbeitung. Diese unterliegt je nach Verwendungszweck der Daten unterschiedlichen Ansprüchen und kann in einigen Fällen eine Herausforderung sein – beispielsweise bei besonders großen Datenmengen, bei sensiblen Informationen oder bei unmittelbar nach der Erhebung benötigten Erkenntnissen.

**Stärken und Alleinstellungsmerkmale**

Während die Datenverarbeitung beim Edge-Computing dezentral am Rand des Netzwerks und damit nah am Ursprungsort der Daten stattfindet, nutzt Cloud-Computing zentrale Rechenzentren, die über ein Netzwerk mit dem Ort der Datenentstehung verbunden sind. Sowohl Edge- als auch Cloud-Computing bieten jeweils einzigartige Vorteile bei der Lösung technologischer Herausforderungen. Die Kombination der beiden Technologien entfaltet ihr volles Potenzial, indem sie die Stärken beider Ansätze vereint und die Leistung, Sicherheit und Latenz der IT-Infrastruktur optimiert.

Ein wichtiges Alleinstellungsmerkmal der Cloud ist die nahezu unbegrenzte Skalierbarkeit. Je nach Bedarf können Ressourcen erweitert oder reduziert werden. Die Edge hingegen hat eine festgelegte, begrenzte Kapazität, die durch die genutzte Hardware, die physischen Gegebenheiten auf dem Betriebsgelände und den Verwendungszweck der Infrastruktur bestimmt wird.

Durch die Nähe zum Ort der Entstehung der Daten ist die Edge allerdings dafür prädestiniert, große Datenmengen fast ohne Verzögerung zu speichern und zu verarbeiten. Sie ist dabei nicht auf die Übertragungsraten des Internets angewiesen. Beim Cloud-Computing gelangen die Daten über eine Internetverbindung in (mindestens) ein Rechenzentrum, das in den meisten Fällen in einiger Entfernung zum Ursprungsort der Daten steht.

Dabei ist die Entfernung zur Datenquelle und zu weiteren möglichen Speicherorten ein Teil des Sicherheitskonzepts. Rechenzentrumsbetreiber wie der Cloud Provider WIIT, verhindern mit Georedundanz beispielsweise, dass verschiedene Speicherorte vom selben Stromausfall oder derselben Naturkatastrophe betroffen sind. Doch auch die Speicherung in der Edge hat Vorteile hinsichtlich der Sicherheit von sensiblen Daten und geistigem Eigentum, da sie in diesem Fall das Betriebsgelände nicht verlassen müssen und der Edge-Betreiber jederzeit die Hoheit über die Daten behält.

Ein weiterer Vorteil der Speicherung und Verarbeitung in der Nähe des Ursprungsortes ist die minimale Latenz. Je nach Größe der zur Verfügung stehenden Edge kann sie als kleines, isoliertes Rechenzentrum fungieren, das umgehend auf lokale Ereignisse reagieren kann.

**Synergie der jeweiligen Vorteile nutzen**

Fügt man die jeweiligen Vorteile von Edge und Cloud zusammen, profitieren die Anwender von einer flexiblen und skalierbaren IT-Infrastruktur, die sowohl Echtzeitanwendungen als auch umfangreiche Datenanalysen unterstützt. Das Zusammenspiel beider Technologien kann für die Erweiterung der Kapazität der Edge dienen oder Daten verdichten und bereinigen, die danach für die Speicherung und Verarbeitung in eine Cloud-Infrastruktur übergehen. Bei einem Pre-Processing der Daten kann die Edge beispielsweise persönliche oder vertrauliche Informationen entfernen oder pseudonymisieren, die ein Unternehmen aufgrund von Compliance-Anforderungen nicht in die Cloud verlagern darf. Diese Vorverarbeitung, die beispielsweise bei der Forschung und der Entwicklung neuer Produkte und Technologien Anwendung findet, trägt gemeinsam mit den umfassenden Schutzmaßnahmen der Cloud dazu bei, Cyberangriffe und Industriespionage abzuwehren.

**Das gebündelte Potenzial in Aktion**

Speziell in der Forschung ist eine Verarbeitung in der Edge oft notwendig. Vor allem die Datenmengen, die bei Experimenten in der angewandten Forschung entstehen, sind häufig so groß, dass ein direkter Transfer in die Cloud kaum umsetzbar ist. Eine Vorverarbeitung filtert und verdichtet die Daten bereits an der Quelle, wodurch sich der Transfer in die Cloud auf relevante und verarbeitbare Daten beschränkt. Die geschickte Kombination von Cloud und Edge reduziert nicht nur die Bandbreitenanforderungen und Speicherkosten, sondern ermöglicht gleichzeitig eine schnellere Analyse und Reaktion auf die Ergebnisse.

Die Kombination von Edge- und Cloud-Computing kann auch zu einer Reduzierung von Energiekosten führen. Durch den Einsatz intelligenter, gesteuerter Systeme im Gebäude- und Energiemanagement lässt sich die Energiezufuhr in Gebäudekomplexen nachhaltig und effizient regulieren. Intelligente Stromnetze, die auf Datenbasis Entscheidungen treffen und an die Cloud angebunden sind, senken Betriebskosten und ermöglichen die Erstellung digitaler Reports. Diese Reports unterstützen die Fernsteuerung und -wartung über die Cloud-Infrastruktur rund um die Uhr. Eine Edge-Lösung stellt dabei sicher, dass nur relevante Daten zur Optimierung von Energieflüssen in die Cloud übertragen werden.

**Die Entwicklung zum Lebensretter**

Der Einsatz intelligenter Systeme und Künstlicher Intelligenz (KI) nimmt in vielen Industriebereichen rasant zu. Auch im Zusammenhang mit Edge- und Cloud-Computing bietet KI enormes Potenzial, beispielsweise im medizinischen Bereich. Dort stellt Edge-Computing seine „klassischen" Vorteile unter Beweis: Das Pre-Processing pseudonymisiert und schützt Patientendaten, bevor die großen Datenmengen, die beispielsweise ein Krankenhaus generiert, zur Speicherung in die Cloud kommen. Zudem schafft die minimale Latenz bei der Datenverarbeitung in der Edge die besten Voraussetzungen dafür, dass Ärzte in zeitkritischen Situationen effektiv helfen und sogar Leben retten können.

Der Einsatz von KI auf einer Edge, die als kleines, vom Internet isoliertes Rechenzentrum fungiert, kann die unterstützende Rolle des Edge-Computings noch weiterentwickeln. Die KI kann medizinischen Bilddaten effizient analysieren und in Echtzeit relevante Muster und Zusammenhänge, Anomalien und potenzielle Krankheitsherde erkennen. Mit diesen Erkenntnissen und der Fähigkeit, auf Grundlage der erhobenen Daten und Echtzeitinformationen Empfehlungen zu geben, kann eine KI eine wertvolle Entscheidungshilfe für die medizinischen Fachkräfte sein. Gleiches gilt für den Bank- und Finanzsektor, in dem künstliche Intelligenz zur Erkennung von Betrug und Geldwäsche beitragen kann, sowie zahlreiche weitere Bereiche, in denen Mustererkennung und die intelligente Analyse gespeicherter Daten einen Mehrwert bieten.

FÜGT MAN DIE JEWEILIGEN VORTEILE VON CLOUD UND EDGE ZUSAMMEN, OPTIMIEREN DIE ANWENDER LEISTUNG, SICHERHEIT UND LATENZ DER IT-INFRASTRUKTUR.

**Christoph Herrnkind, CEO, WIIT AG, www.wiit.cloud/de/**

**Cloud und Edge greifen nahtlos ineinander**

Die Fachkräfte, die in diesen Anwendungsbeispielen mit der Edge arbeiten, können sich darauf verlassen, dass die Daten, auf die sie zugreifen, das Betriebsgelände nicht verlassen. Die unterschiedlichen Speicherorte wirken sich dabei nicht auf ihre Arbeitsabläufe aus, da sie sowohl für die lokalen Daten als auch bei der Arbeit mit Anwendungen und Workloads in der Cloud durchgängig dieselben Management- und Automatisierungstools nutzen. Cloud- und Edge-Provider wie die WIIT AG führen beide Umgebungen unter einer gemeinsamen Administrations-Oberfläche zusammen. So profitieren Unternehmen und Organisationen vom nahtlosen Zusammenspiel beider Technologien und können den maximalen Nutzen aus ihren digitalen Daten und deren Verarbeitung ziehen.

***Christoph Herrnkind***

# Cloud Computing

## EIN MUSS FÜR DIE DIGITALE TRANSFORMATION VON KMU

Für die Wettbewerbsfähigkeit und Effizienz von kleinen und mittelständischen Unternehmen bleibt die Digitalisierung, insbesondere durch eine gute Netzwerkinfrastruktur und Cloud-Computing, trotz wirtschaftlicher Unsicherheiten entscheidend.

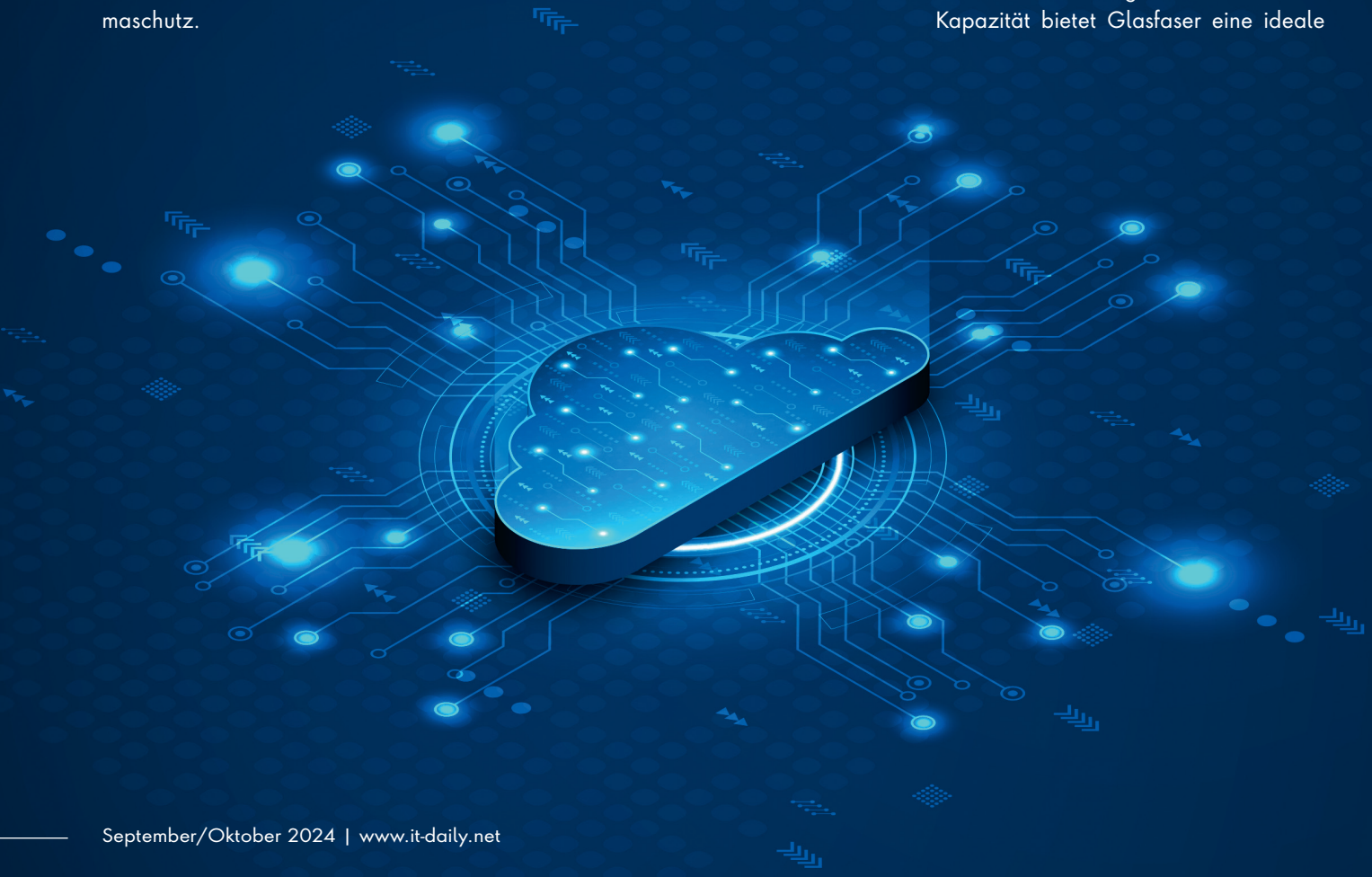
Zuletzt machte die Digitalisierung der deutschen Wirtschaft nur geringe Fortschritte. Diese Entwicklung kann zum Teil auf die anhaltende Krisensituation zurückgeführt werden, in der sowohl die Wirtschaft als auch die Gesellschaft mit Inflation, Problemen in den Lieferketten, der Energiekrise und anderen Unsicherheiten konfrontiert sind. Dies bestätigt der Digitalisierungsindex 2023 des Bundesministeriums für Wirtschaft und Klimaschutz.

Kleine und mittelständische Unternehmen (KMU) sind das Rückgrat der deutschen Wirtschaft. Sie machen einen Großteil der Unternehmen in Deutschland aus und tragen erheblich zur wirtschaftlichen Stabilität und Beschäftigung bei. Dennoch stehen sie häufig vor besonderen Herausforderungen, wenn es um die Digitalisierung geht. Dies betrifft sowohl finanzielle als auch personelle Ressourcen. Die notwendigen Investitionen lohnen sich aber, denn die Digitalisierung bietet KMU die Möglichkeit, ihre Geschäftsprozesse zu optimieren, Kosten zu senken und ihre Wettbewerbsfähigkeit zu steigern.

Moderne IT-Services wie Cloud und Edge Computing bieten erhebliche Entlastungen und Kosteneinsparungen, die für KMU von großem Vorteil sein können. Unternehmen, die jetzt aktiv in die Digitalisierung investieren, können eine Vorreiterrolle sichern und sich klar von der Konkurrenz abheben.

**Bedeutung der Digitalisierung**

Die Netzwerkinfrastruktur bildet das Fundament der Digitalisierung, da sie für den Austausch von Daten sowohl innerhalb des Unternehmens als auch mit Kunden, Partnern und anderen Interessensgruppen von zentraler Bedeutung ist. Ein Glasfaseranschluss stellt eine zukunftssichere Lösung für die digitale Infrastruktur dar. Aufgrund seiner hohen Kapazität bietet Glasfaser eine ideale



Basis für aktuelle und künftige Bandbreitenanforderungen. Mit der Verlegung von Fiber to the Home (FTTH) bis in die Gebäude steht dort unmittelbar die gesamte Bandbreitenkapazität zur Verfügung. Die optische Übertragung mittels Licht sorgt dafür, dass Glasfaser nicht so stark von Dämpfung betroffen und weniger anfällig für elektromagnetische Störungen ist, im direkten Vergleich zu DSL über Kupferkabel.

Darüber hinaus bietet Glasfaser größere Bandbreitenreserven als andere Übertragungsmedien und ermöglicht deutlich größere Entfernungen zwischen den Netzknoten. Zudem ist die Technologie energieeffizienter als kupferbasierte Alternativen. Gleichzeitig bietet eine Glasfaserleitung stabile und hochverfügbar hohe Datenraten im Down- und Upload.

Diesen Anforderungen sind DSL-Anschlüsse nicht gewachsen, da ihre Standards keinen symmetrischen Datenverkehr mit den erforderlichen Übertragungsraten unterstützen. Der Upload stellt insbesondere im Unternehmensumfeld ein entscheidendes Maß für die Leistungskraft eines Netzwerkanschlusses dar. Ein schneller Upload ermöglicht es etwa, große Datenmengen schnell in die Cloud zu laden, was die Effizienz von Backups und die Verfügbarkeit von Daten verbessert.

Auch bei der Nutzung von Videokonferenz-Tools und Remote-Arbeitsplätzen ist eine stabile und schnelle Upload-Geschwindigkeit entscheidend für die Übertragungsqualität von Video und Audio, was die Zusammenarbeit und Kommunikation verbessert.

**Flexibilität und Kosteneffizienz dank der Cloud**

Cloud-Computing ist ein zentrales Element der digitalen Transformation. Es ermöglicht Unternehmen, IT-Ressourcen wie Speicherplatz, Rechenleistung und Anwendungen über ihr Netzwerk und mithilfe der Cloud zu nutzen, anstatt in kostenintensive eigene Hardware und Software zu investieren. Stattdessen zahlen sie nur für die tatsächlich genutzten Ressourcen, was die IT-Kosten erheblich senken kann. Auch sind Cloud-Dienste flexibel und skalierbar, was besonders in Zeiten von Wachstumsphasen oder saisonalen Schwankungen von Vorteil ist.

EINE GUTE NETZWERK-INFRASTRUKTUR IST FÜR VIELE KMU DAS FUNDAMENT DER DIGITALISIERUNG.

**Süleyman Karaman,**
**Geschäftsleiter Geschäftskunden,**
**Deutsche Glasfaser Business GmbH,**
**www.deutsche-glasfaser.de/business/**

Eine moderne Telefonanlage aus der Cloud bietet Unternehmen zusätzlich die Möglichkeit, Kosten und Energie einzusparen. Im Vergleich zu herkömmlichen Telefonanlagen reduziert sich der Aufwand für Aufbau, Betrieb und Wartung erheblich, während das Telefonieren weiterhin von jedem Standort aus problemlos möglich ist. Ein weiterer Vorteil einer Cloud-Telefonanlage ist die hohe Benutzerfreundlichkeit und Flexibilität.

**Integration der Technologie im Unternehmen**

Für KMU stellt die Integration von Cloud-Computing eine vielversprechende Möglichkeit dar, ihre digitale Transformation voranzutreiben. Dabei sollten sie einige wesentliche Punkte beachten. Unternehmen sollten zunächst ihren spezifischen Bedarf ermitteln und analysieren, welche Prozesse und Anwendungen von einer Verlagerung in die Cloud profitieren können.

Mit Cloud-Computing können Mitarbeiter von überall auf Unternehmensdaten und Anwendungen zugreifen. Dies fördert die Mobilität und ermöglicht flexible Arbeitsmodelle, die in der heutigen Arbeitswelt immer wichtiger werden.

Viele Cloud-Anbieter investieren stark in Sicherheitsmaßnahmen und erfüllen strenge Datenschutzanforderungen. Für KMU kann es schwierig sein, das gleiche Sicherheitsniveau mit eigenen Mitteln zu erreichen. Die Auswahl eines geeigneten Cloud- und Edge-Computing-Anbieters ist entscheidend. KMU sollten auf Anbieter setzen, die flexible und skalierbare Lösungen anbieten und gleichzeitig hohe Sicherheitsstandards erfüllen.

Die Einführung neuer Technologien erfordert oft eine Umstellung der Arbeitsprozesse und eine entsprechende Schulung der Mitarbeiter. Investitionen in die Qualifizierung des Personals sind daher unerlässlich. Es kann zudem sinnvoll sein, zunächst mit kleineren Pilotprojekten zu starten, um die neuen Technologien zu testen und Erfahrungen zu sammeln, bevor sie im gesamten Unternehmen implementiert werden.

**Ausblick**

Die digitale Transformation durch Cloud-Computing und eine robuste Netzwerkinfrastruktur ist für KMU unerlässlich, um ihre Wettbewerbsfähigkeit in einer zunehmend digitalisierten Welt zu sichern. Trotz wirtschaftlicher Unsicherheiten und den Herausforderungen der aktuellen Krisensituation müssen KMU die Digitalisierung als Chance begreifen, ihre Geschäftsprozesse zu optimieren, Kosten zu senken und ihre Marktstellung zu stärken. Der Einsatz von Glasfasertechnologie bietet eine stabile und zukunftssichere Basis, während Cloud-Computing flexible, kosteneffiziente und sichere IT-Lösungen bereitstellt. Wer jetzt in die digitale Transformation investiert, langfristig erfolgreich am Markt bestehen.

***Süleyman Karaman***


# Testdatenmanagement

## DURCHFÜHREN VON TESTS MIT DATENBANK-TEILMENGEN IN EINER JENKINS CI/CD-PIPELINE

**– TEIL 5 VON 5 –**

Diese fünfteilige Artikelreihe beschäftigt sich intensiv mit dem Thema Testdatenmanagement (TDM) und dessen bedeutender Rolle bei der Sicherstellung der Softwarequalität. Die Serie beleuchtet verschiedene Aspekte des TDMs, darunter bewährte Methoden, Herausforderungen und innovative Lösungen.

Entwickler benötigen eine Testumgebung, die der Produktionsumgebung möglichst ähnlich ist, um das Verhalten einer Anwendung während des Betriebs realistisch bewerten zu können. Allerdings erreicht eine Testumgebung niemals das gleiche Sicherheitsniveau wie die finale Produktionsumgebung, was ein Dilemma bei der Erstellung und Nutzung von Testdaten darstellt. Tester müssen entscheiden, ob sie bereinigte Kopien von Produktionsdaten verwenden oder realistische synthetische Testdaten erstellen.

TDM umfasst eine Vielzahl von Aufgaben, wie die Bereitstellung von Testdaten, Anonymisierung und Maskierung sensibler Daten, Erstellung von Teilmengen (Data Subsetting), Sicherstellung der Datenkonsistenz und Integration in Continuous Integration (CI) und mit Continuous Delivery (CD) Pipelines. Eine effektive TDM-Strategie verbessert die Softwarequalität, indem sie realistische Testbedingungen schafft, potenzielle Probleme frühzeitig erkennt und die Effizienz der Testprozesse erhöht.

Die Artikelserie hebt die TDM-Funktionen von IRI Voracity hervor, einer umfassenden Datenmanagementplattform, die Datenerkennung, -integration, -migration und -verwaltung in einem Metadaten-Framework vereint. Der Einsatz von IRI Voracity ermöglicht eine effiziente Datenhandhabung und führt zu Kosteneinsparungen in vernetzten Big Data IT-Umgebungen.

Dieser Jenkins-Beitrag ist der letzte Teil einer Artikelreihe zur Nutzung der IRI Testdatenmanagement-Software. Diese Software maskiert, synthetisiert oder teilt Daten in Teilmengen auf, um sichere

und referenziell korrekte Testdaten für DevOps in CI/CD-Umgebungen bereitzustellen. Die vorherigen Artikel demonstrierten die Erstellung von Testdaten mit IRI-Software und deren Einsatz in GitLab, AWS CodePipeline und Azure DevOps.

**Optimierung des Testdatenmanagements mit Jenkins**

Continuous Integration-Tools wie Jenkins bieten erhebliche Vorteile für Anwender, wenn sie mit Aufgaben zur Testdatengenerierung, wie etwa Subsetting, kombiniert werden. In einer CI/CD-Pipeline, in der Anwendungssoftware regelmäßig erstellt und implementiert wird, ist es entscheidend, dass auch der Datenbankzugriff und die Datenverarbeitung gründlich getestet werden.

Stellen Sie sich vor, eine Website muss getestet werden, die die letzten Einkäufe der Benutzer in einem Online-Shop anzeigt. Um sicherzustellen, dass die Website korrekt auf die Datenbank zugreift und die Daten abruft, ist es erforderlich, in allen Phasen der CI/CD-Pipeline realistische Testdaten zu verwenden. Durch die Integration von Subsetting- und Maskierungsjobs in die CI/CD-Pipeline können realistische und gleichzeitig geschützte Datensätze generiert und zusammen mit dem Anwendungscode bereitgestellt werden. Dies sorgt für aussagekräftige Testdaten in jeder Testphase der Pipeline.

EINE EFFEKTIVE TDM-STRATEGIE VERBESSERT DIE SOFTWAREQUALITÄT, INDEM SIE REALISTISCHE TESTBEDINGUNGEN SCHAFFT, POTENZIELLE PROBLEME FRÜHZEITIG ERKENNT UND DIE EFFIZIENZ DER TESTPROZESSE ERHÖHT.

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

**Technische Skizzierung**

Zuerst muss eine VM-Instanz erstellt und entsprechend konfiguriert werden, wobei die Firewall aktiviert wird, um HTTP/S-Traffic zuzulassen, damit der Jenkins-Server Benachrichtigungen für Push-Ereignisse von GitHub empfangen kann. Sobald die Instanz erstellt ist, wird Jenkins und Git installiert. Nach der Installation muss die Netzwerkschnittstelle konfiguriert werden, um auf Jenkins zugreifen zu können mittels einer hinzugefügten Firewallregel. Hier muss dann die Portnummer 8080 und der Quell-IP-Bereich angegeben werden, damit man auf Jenkins von der externen IP-Adresse der VM-Instanz zugreifen kann.

Um die CI/CD-Pipeline nicht manuell oder nach einem Zeitplan auszuführen, wird der Jenkins-Server so konfiguriert, dass er Webhooks verwendet und auf Push-Ereignisse im GitHub-Repository reagiert. Nach der Erstellung eines Benutzerkontos und der Installation der Standard-Jenkins-Plugins kann eine CI/CD-Pipeline erstellt werden. In der Konfiguration der Pipeline wird der Build-Trigger auf „GitHub hook trigger for GITScm polling" gesetzt. Es wird empfohlen, eine Jenkinsfile im Projekt-Repository zu verwenden, da dies mehr Freiheit bei der Verwaltung innerhalb der IRI Workbench, die GUI zur Konfigurierung der Testdaten bietet.

Die Pipeline wird konfiguriert, um ein Pipeline-Skript (Jenkinsfile) aus SCM (Source Code Management) zu verwen-

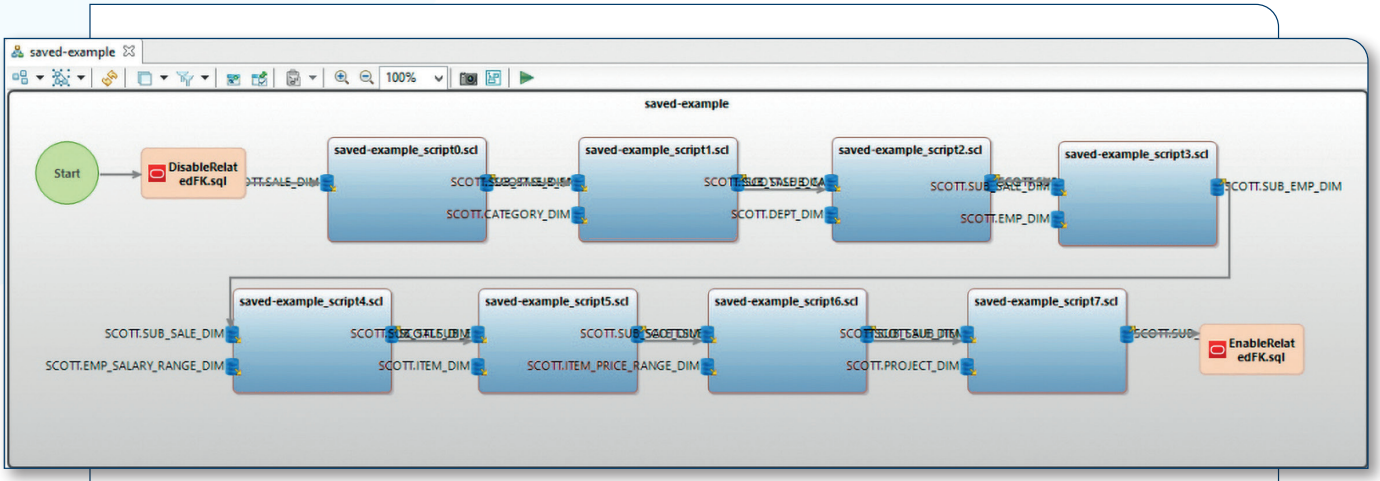



**Bild 1: Data Subsetting: Das Erstellen von Teilmengen ist nützlich für Software- oder Datenbanktests, die nicht die Ressourcen oder Risiken einer Produktionskopie erfordern. Es bewahrt die nötige Geschäftslogik und sorgt, kombiniert mit Datenbereinigung und -maskierung, für sichere und saubere Testdaten.**

den. Die SCM-Option wird auf Git gesetzt und die Repository-URL des Projekts angegeben. Nach dem Speichern der Einstellungen wird die Pipeline bei Push-Ereignissen im Git-Repository ausgelöst. Für die Bereitstellung von Testdaten wird ein einfacher Subsetting-Job in der IRI Workbench erstellt, der aus der CI/CD-Pipeline ausgeführt wird.

In Bild 2 ist das zugrunde liegende IRI-Aufgabenskript für ein Kommandozeilen-Subsetting-(Batch-)Programm zu sehen. Dieses Beispielskript erzeugt eine Teilmenge der Tabelle CHIEFS und wendet eine Maskierungsregel (formatbewahrende Verschlüsselung) auf die Spalte NAME an, um personenbezogene Daten zu schützen.

**Auslösen der Jenkins-Pipeline aus der IRI Workbench**

Da die IRI Workbench die Git-Versionskontrolle unterstützt, können IRI-Projekte aus der Workbench heraus committed und gepushed werden. Bei einem Push-Ereignis wird die Jenkins-Pipeline durch GitHub-Webhooks benachrichtigt. Dies ermöglicht es, die Jenkins-Pipeline direkt aus der IRI Workbench auszulösen.

Bild 2

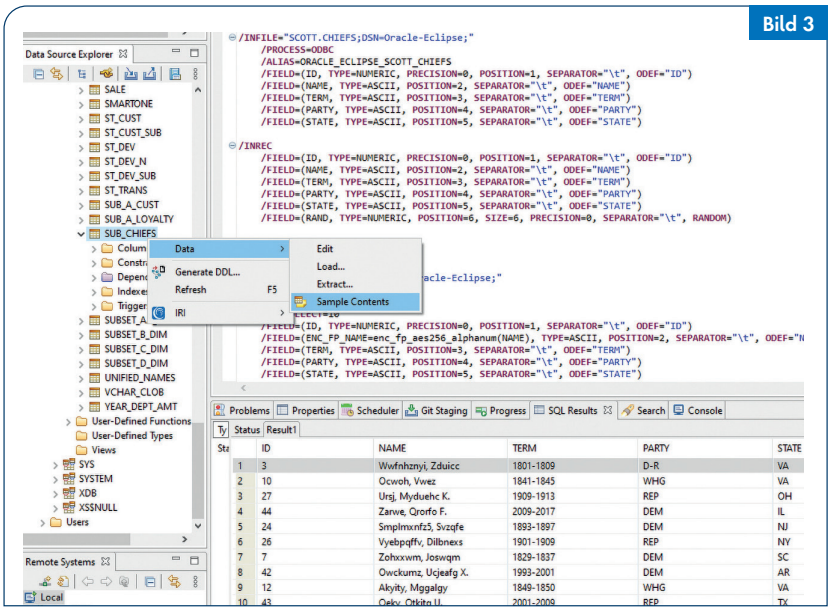
```
/INFILE="SCOTT.CHIEFS;DSN=Oracle-Eclipse;"
    /PROCESS=ODBC
    /ALIAS=ORACLE_ECLIPSE_SCOTT_CHIEFS
    /FIELD=(ID, TYPE=NUMERIC, PRECISION=0, POSITION=1, SEPARATOR="\t", ODEF="ID")
    /FIELD=(NAME, TYPE=ASCII, POSITION=2, SEPARATOR="\t", ODEF="NAME")
    /FIELD=(TERM, TYPE=ASCII, POSITION=3, SEPARATOR="\t", ODEF="TERM")
    /FIELD=(PARTY, TYPE=ASCII, POSITION=4, SEPARATOR="\t", ODEF="PARTY")
    /FIELD=(STATE, TYPE=ASCII, POSITION=5, SEPARATOR="\t", ODEF="STATE")

/INREC
    /FIELD=(ID, TYPE=NUMERIC, PRECISION=0, POSITION=1, SEPARATOR="\t", ODEF="ID")
    /FIELD=(NAME, TYPE=ASCII, POSITION=2, SEPARATOR="\t", ODEF="NAME")
    /FIELD=(TERM, TYPE=ASCII, POSITION=3, SEPARATOR="\t", ODEF="TERM")
    /FIELD=(PARTY, TYPE=ASCII, POSITION=4, SEPARATOR="\t", ODEF="PARTY")
    /FIELD=(STATE, TYPE=ASCII, POSITION=5, SEPARATOR="\t", ODEF="STATE")
    /FIELD=(RAND, TYPE=NUMERIC, POSITION=6, SIZE=6, PRECISION=0, SEPARATOR="\t", RANDOM)

/SORT
    /KEY=(RAND)

/OUTFILE="SCOTT.SUB_CHIEFS;DSN=Oracle-Eclipse;"
    /PROCESS=ODBC
    /CREATE
    /OUTCOLLECT=10
    /FIELD=(ID, TYPE=NUMERIC, PRECISION=0, POSITION=1, SEPARATOR="\t", ODEF="ID")
    /FIELD=(ENC_FP_NAME=enc_fp_aes256_alphanum(NAME), TYPE=ASCII, POSITION=2, SEPARATOR="\t", ODEF="NAME")
    /FIELD=(TERM, TYPE=ASCII, POSITION=3, SEPARATOR="\t", ODEF="TERM")
    /FIELD=(PARTY, TYPE=ASCII, POSITION=4, SEPARATOR="\t", ODEF="PARTY")
    /FIELD=(STATE, TYPE=ASCII, POSITION=5, SEPARATOR="\t", ODEF="STATE")
```

Bild 3




Wenn die Jenkins-Pipeline gestartet wird, läuft der Teilmengen-Job in der Kommandozeile und erstellt eine Tabelle namens SUB_CHIEFS. Anschließend können die Ergebnisse im IRI Workbench eingesehen werden. Aus dem nächsten Bild geht hervor, dass eine Untertabelle namens SUB_CHIEFS erstellt und mit zehn Datensätzen aus der CHIEFS-Tabelle gefüllt wurde. Die Werte in der Spalte NAME wurden ebenfalls verschlüsselt.

**Zusammenfassung**

Das Erstellen von Teilmengen ist nützlich für Test- und Entwicklungszwecke, denn Entwickler möchten möglicherweise mit Produktionsdaten in einer Testumgebung arbeiten, können oder wollen jedoch nicht die Ressourcen für eine vollständige Kopie der Produktionsdatenbank bereitstellen. Daher ist es sinnvoll, eine kleinere Kopie der Datenbank mit intakter referenzieller Integrität zu haben. Durch die Integration von Maskierungsmethoden im Teilmengenprozess werden realistische Daten erstellt, bei denen personenbezogene Daten bereinigt wurden.

Da eine Anwendung während der Testphasen eines DevOps-Prozesses Testdaten benötigt, ist es sinnvoll, das Erstellen von Teilmengen in die CI/CD-Pipeline zu integrieren. Dadurch wird ein umfassender Prozess geschaffen, in dem die Testdaten/Datenbanken zusammen mit dem Anwendungscode erstellt und bereitgestellt werden können, um aussagekräftige Testdaten für die Testphasen der Pipeline bereitzustellen.

***Amadeus Thomas***

# STORYTELLING: DIGITAL – MULTIMEDIAL – ARTIFICIAL

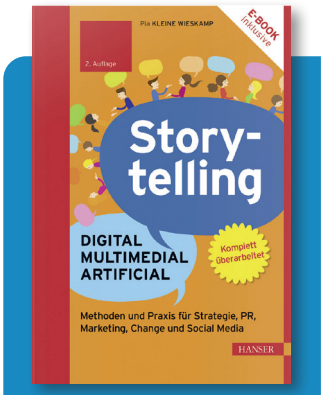
## METHODEN UND PRAXIS FÜR STRATEGIE, PR, MARKETING, CHANGE UND SOCIAL MEDIA

Mittlerweile haben alle Kommunikationsbereiche erkannt, dass Storytelling das mächtigste Mittel zur authentischen Zielgruppenansprache ist. Geschichten bewegen uns, wecken Emotionen und gute Storys bleiben langfristig in Erinnerung.

Dieses Buch regt zum Nachdenken an, liefert Lösungen und lässt Storytelling-Praktiker zu Wort kommen, die bereits erfolgreich umgesetzte Storys präsentieren. Experten erläutern aus der Praxis ihres Berufsalltags heraus, was Storytelling bedeutet und wie sie es als Methode ein- und umsetzen.

**Aus dem Inhalt:**

- Storytelling im Unternehmen
- Sustainable Storytelling
- Streaming
- Storytelling im Metaverse
- Tools und Checklisten




**Storytelling: Digital – Multimedial – Artificial**
Methoden und Praxis für Strategie,PR, Marketing, Change und Social Media
Pia Kleine Wieskamp;
Carl Hanser Verlag GmbH & Co.KG; 03-2024

# SQL, NoSQL, Vektor oder Multimodell?

## WANN UND WOFÜR MAN WELCHE DATENBANK BRAUCHT

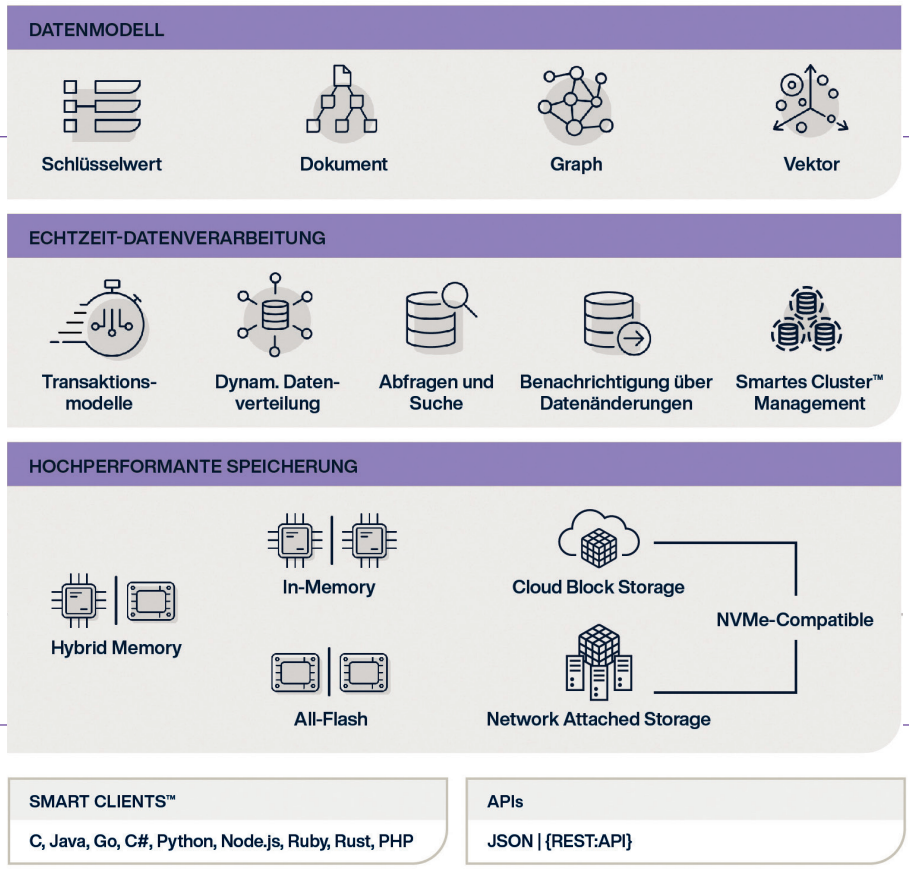
Unternehmen werden von Daten geradezu geflutet. Innovative Datenbanktechnologien versprechen, diese leichter und schneller nutzbar zu machen. Doch was genau können die Neuen besser als ihre traditionellen Vorgänger?

Über viele Jahre dominierten relationale SQL-Datenbanken die Unternehmens-IT. Inzwischen hat sich ein ganzer Reigen neuer Technologien dazu gesellt, darunter Schlüsselwert-, Dokumentendaten-, Graph- und Vektorspeicher. Welche Stärken diese innovativen Systeme mitbringen und welcher Datenbanktyp wo am besten eingesetzt wird, beleuchtet dieser Beitrag.

**SQL-Datenbanken: Integer und konsistent**

Eine relationale oder SQL-Datenbank speichert Daten in strukturierten Tabellen, bestehend aus Zeilen und Spalten. Sie nutzt die SQL-Syntax (Structured Query Language) für Abfragen und Analysen. Die Relationen zwischen den über mehrere Tabellen verteilten Informationen definieren eindeutige Werte, sogenannte Schlüssel. Damit Anwendungen überhaupt Daten in die Datenbank schreiben können, muss das Datenbankschema bereits zu Beginn der Entwicklung feststehen und im weiteren Verlauf unverändert bleiben. Zudem gilt es, alle Daten vor dem Speichern zu normalisieren, also in Kategorien zu organisieren und gemäß den Tabellen zu strukturieren.

## STRUKTUR EINER MULTIMODELL-REALTIME-DATENBANK




Realtime-Multimodell-Datenbanken punkten mit hoher Performance und Skalierbarkeit.

**Merkmale und Anwendungsbereiche von SQL-Datenbanken**

Relationale Datenbanken folgen dem AKID-Prinzip: Atomarität, Konsistenz, Isolierung und Dauerhaftigkeit. Atomarität bedeutet, dass eine Transaktion entweder vollständig oder überhaupt nicht ausgeführt wird. Tritt an einer Stelle des Transaktionsprozesses ein Fehler auf, macht das System alle bisher vorgenommenen Änderungen rückgängig. Zusätzlich halten Regeln und Validierungen das System stets in einem konsistenten Zustand. Isolation gilt als erfüllt, wenn Transaktionen unabhängig voneinander ausgeführt werden und sich die Ergebnisse parallel ablaufender Transaktionen nicht beeinflussen. Das Ergebnis einer vollständig abgeschlossenen Transaktion speichert die Datenbank permanent – selbst nach einem Systemfehler oder Neustart. Damit ist Dauerhaftigkeit gewährleistet.

JEDES DATENBANKSYSTEM HAT IN DER UNTERNEHMENS-IT SEINE BERECHTIGUNG. DAS MAXIMUM AN FLEXIBILITÄT BIETEN AKTUELL JEDOCH MULTIMODELL-DATENBANKEN

**Behrad Babaee,**
**Principal Solutions Architect, Aerospike,**
**www.aerospike.com**

In relationalen Systemen unterliegt die Datenmodellierung strengen Regeln. Das Ergebnis sind Datenschemata, die oft nur schwer zu ändern sind. Gleichzeitig erlaubt diese rigide Vorgehensweise, eine Vielzahl unterschiedlicher Abfragetypen effizient auszuführen. Durchaus ein Vorteil in komplexen Umgebungen, in denen anfangs nicht absehbar ist, welche Abfragen die Geschäftsbereiche benötigen werden. Back-Office-Anwendungen für Finanzen, Controlling oder Buchhaltung können daher von relationaler Datenmodellierung profitieren. Allerdings führt dieser Ansatz unter Umständen auch dazu, dass die Datenbank für Abfragen optimiert wird, welche nie ausgeführt werden. Eine solch unnötige Optimierung bringt erheblichen Mehraufwand mit sich und macht eine SQL-Datenbank weniger skalierbar, langsamer und teurer im Betrieb.

**NoSQL-Datenbank: Flexibel und skalierbar**

Bei nicht-relationalen NoSQL-Datenbanken verantworten Entwickler die optimale Gestaltung des Datenschemas. Daher

lässt sich dieses optimal auf die Anforderungen der Geschäftsbereiche zuschneiden – speziell angepasst auf jeden Use Case. Im Vergleich zu traditionellen Datenbanken sind NoSQL-Systeme damit effizienter, skalierbarer und flexibler und verarbeiten zudem auch halb-strukturierte und unstrukturierte Daten.

**Unter die NoSQL-Datenbanken fallen sehr unterschiedliche Speichersysteme:**

#1 **Schlüsselwertspeicher** legen jeden Datensatz als Wert mit einem einzigartigen Schlüssel ab, über welchen sich Informationen gezielt abfragen lassen.

#2 **Dokumentendatenspeicher** sind ein spezieller Typ von Schlüsselwertspeichern, die Dokumente im Format JSON- oder XML als Wert ablegen. Bei den Dokumenten handelt es sich im Wesentlichen um verschachtelte Datenstrukturen. Diese haben den Vorteil, dass sich die Datenmodellierung auf den jeweiligen Use Case genau zuschneiden lässt – sowohl für strukturierte als auch für halbstrukturierte Daten.

#3 **Graphspeicher** speichern Daten als Knoten und Kanten. Damit lassen sich Beziehungen zwischen Datenpunkten sehr gut herstellen.

#4 **Spaltenorientierte Systeme** speichern einen Datensatz in einer Spalte ab und nicht in Zeilen. Sie sind daher äußerst effizient bei spaltenbasierten Aggregationen.

Jede NoSQL-Datenbank verwendet ihre eigene Abfragesprache, was die Kombination verschiedener Systeme erschweren kann. Häufig ist jedoch zusätzlich SQL als Abfragesprache möglich, daher auch der Name „not only SQL".

**Vorteile und Einsatzgebiete nicht relationaler Datenbanken**

NoSQL-Systeme priorisieren hohe Verfügbarkeit, kurze Antwortzeit, Skalierbarkeit und Flexibilität. Hierfür replizieren sie Daten automatisch über mehrere Server, Rechenzentren oder Cloud-Ressourcen hinweg. Dabei wird eine kontinuierliche Verfügbarkeit gewährleistet und die Latenz für die Nutzer minimiert. Durch ihre verteilte Struktur sind NoSQL-Systeme inkrementell skalierbar, sehr kosteneffizient und bieten praktisch unbegrenztes Wachstumspotenzial. Bemerkenswert: NoSQL-Systeme sind in der Lage, Konsistenz und Verfügbarkeit auszubalancieren. Hat die Verfügbarkeit Priorität, passt das System die Konsistenzprotokolle entsprechend an.

Ihre vereinfachten Datenmodelle kommen ohne Relationen aus. Das lässt NoSQL-Systeme Daten schneller verarbeiten, abrufen und effizienter speichern.

Sie sind daher ideal für Anwendungen, die größte Datenmengen – Stichwort Big Data – speichern sowie Real-time-Verarbeitung und geringe Latenzzeiten benötigen. Typisch dafür sind Online-

Shops/eCommerce, Advertising Technology (AdTech), Customer360-Betrachtungen und der Gamingbereich.

**Auf dem Vormarsch: Vektordatenbanken**

Mit KI und Big Data hat eine dritte Kategorie Einzug in den Unternehmensalltag gehalten: Vektordatenbanken. Sie sollen das Speichern mehrdimensionaler Vektoren vereinfachen, üblicherweise in Form von geordneten Listen oder Zahlenfolgen. Während viele Datenbanken Vektoren speichern können, ist deren effizientes Durchsuchen eine Herausforderung. Vektordatenbanken ermöglichen dies durch eine schnelle Ähnlichkeitssuche. Damit lassen sich verwandte Elemente schnell und einfach finden.

Vektordatenbanken sind hoch-performant, weil sie sich spezieller Algorithmen und Optimierungen bedienen. So meistern sie selbst komplexe Zusammenhänge wie kontextbezogene Bild- und Texterkennung oder die Suche nach ähnlichen Assets in Millisekunden. Sie eignen sich besonders für personalisierte Empfehlungssysteme oder KI-/ML-Anwendungen, die mit semantischem Informationsabruf und Langzeitgedächtnis arbeiten. Weitere Einsatzbereiche sind die Gesichtserkennung oder die Aufdeckung von Anomalien wie in der Betrugserkennung.

**Multimodell: In einer Datenbank vereint**

Die meisten Unternehmen betreiben unterschiedliche Datenbanksysteme parallel. Damit nutzen Firmen die jeweiligen Vorteile und begrenzen die Auswirkungen der Nachteile. Doch viele parallel betriebene Systeme sind aufwändig zu warten und im Betrieb kostenintensiv. Die Alternative: eine Multimodell-Datenbank.

Diese Datenplattformen integrieren relationale und nicht-relationale Datenbankmodelle in einem einzigen System, einige erlauben sogar Vektorsuche. Sie ermöglichen so das Speichern, Verwalten und Abfragen unterschiedlicher Datentypen innerhalb einer einzigen Datenbank – mit dem Ergebnis einer effizienteren und flexibleren Datenverarbeitung.

Sie sind zudem äußerst flexibel auf den jeweiligen Bedarf anpassbar, skalieren horizontal wie vertikal. Außerdem ermöglichen sie eine ganzheitliche Sicht auf verschiedenste Daten, indem sie Datensilos ablösen. Das erleichtert nicht nur die Datenintegration, sondern verbessert auch die Zusammenarbeit zwischen Abteilungen oder Anwendungen.

**Fazit**

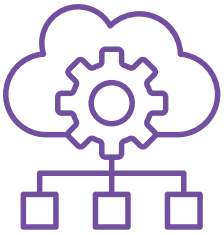
Ob SQL, NoSQL oder Vektor: Jedes Datenbanksystem hat in der Unternehmens-IT seine Berechtigung. Das Maximum an Flexibilität bieten aktuell jedoch Multimodell-Datenbanken.

***Behrad Babaee***

## ÜBERSICHT VERSCHIEDENER DATENBANK-TYPEN

| Typ/Merkmale | SQL | NoSQL | Vektor/Vektorsuche |
|---|---|---|---|
| **Datentyp** | strukturiert | strukturiert, halb-strukturiert, unstrukturiert | strukturiert, halb-strukturiert, unstrukturiert - als multidimensionale Vektoren organisiert |
| **Datenbank-Schema** | vorab zu definieren | flexibel und anpassbar | flexibel und anpassbar |
| **Vorteile** | Integrität und Konsistenz | Performance, Skalierbarkeit, Verfügbarkeit und Flexibilität | erfasst eine Vielzahl an Merkmalen und Details unabhängig vom Datentyp |
| **Geeignet für Big Data** | Nein | Ja | Ja, ideal für KI/ML |
| **Realtime-Datenverarbeitung** | Nein | Ja | Ja |
| **Häufige Anwendungsbereiche** | Finanzwesen, Buchhaltung, Controlling, etc. | eCommerce, AdTech, Customer360, Gaming, etc. | Betrugserkennung, Chatbots, virtuelle Assistenten, personalisierte Empfehlungssysteme. |

Multimodell-Realtime-Datenbanken integrieren die unterschiedlichen Datenbanktypen in einer Plattform.



**Das Maximum an Flexibilität für die Unternehmens-IT bieten aktuell Multimodell-Datenbanken**

Quelle: Easy Software

# Die E-Rechnung kommt

## FÜNF BEST PRACTICES FÜR DIE UMSTELLUNG

Elektronische Rechnungen ersetzen in deutschen Unternehmen immer stärker die lästigen Papierrechnungen. Im B2B-Bereich sind sie ab Januar 2025 sogar Pflicht. Unternehmen jeder Größe und Branche haben bei der Umstellung auf E-Invoicing deshalb noch einiges auf der To-do-Liste.

Die Uhr tickt. In Deutschland steht eine umfassende Pflicht zur elektronischen und strukturierten Rechnungsstellung im B2B-Verkehr bevor. Bereits im vergangenen Jahr hat der Zug in Richtung E-Invoicing, angetrieben durch das europäische Wachstumschancengesetz, Fahrt aufgenommen. Was damals noch in der Schwebe stand, hat der Bundesrat im März 2024 beschlossen. Ab Januar 2025 müssen alle deutschen Unternehmen in der Lage sein, elektronische Rechnungen zu stellen und zu empfangen. Ziel ist es, die Effizienz, Transparenz und Nachhaltigkeit im Geschäftsverkehr zu verbessern.

Die gute Nachricht: Laut einer Bitkom e.V. Studie erstellen bereits 72 Prozent der befragten Unternehmen mindestens die Hälfte ihrer Rechnungen digital (Stand: 2022). Allerdings: Nur etwas mehr als die Hälfte greift dabei auf ein strukturiertes Format zurück, das eine automatisierte, elektronische Weiterverarbeitung der Rechnung ermöglicht. Die übrigen stehen noch ganz am Anfang und vor der Herausforderung, ihre Rechnungsprozesse bis zum Jahresende grundlegend umzustellen, um die neuen gesetzlichen Anforderungen zu erfüllen.

### Zwei Standards für mehr Maschinenlesbarkeit

Eine der größten Herausforderungen besteht tatsächlich in der Maschinenlesbarkeit. Unternehmen müssen sicherstellen, dass die elektronische Rechnung sowohl auf der Seite des Absenders als auch auf der Seite des Empfängers gleich „interpretiert" wird. Um als elektronische Rechnung zu gelten, muss das Rechnungsdokument als maschinenlesbarer Datensatz vorliegen. Die Lösung des Problems: Die Einigung auf einen einheitlichen E-Rechnungsstandard, der alle notwendigen Elemente einer Rechnung in strukturierter Weise enthält. Zwei Formate von Rechnungstypen sind ab 2025 gesetzlich vorgeschrieben: XRechnung und ZUGFeRD.

➤ Die XRechnung stellt den deutschen Standard für elektronische Rechnungen an die öffentliche Verwaltung dar. Gleichwohl steht dieses Rechnungsformat ab 2025 auch zur Rechnungsstellung im B2B-Bereich zur Verfügung. Als Transport-Medium zum Rechnungsversand und -empfang setzt die XRechnung in gewohnter Manier auf die E-Mail. Die entsprechende XML-Datei befindet sich im Anhang. Das Rechnungsformat hat jedoch eine Besonderheit: Die Darstellung der Rechnungsinhalte übernimmt das verarbeitende Datenmanagementsystem (DMS). Der Rechnungsempfänger muss sich also nicht durch unübersichtliche XML-Dateien kämpfen, sondern erhält über eine Visualisierungslösung ein lesbares Dokument.

➤ ZUGFeRD ist das zweite Format, das Unternehmen ab 2025 für die Rechnungs-

stellung zur Verfügung steht. Das Rechnungsformat hat sich seit seiner Einführung im Jahr 2014 sowohl im B2B- als auch im Business-to-Government-Bereich etabliert. Das hybride Datenformat kombiniert ein PDF-Dokument als sichtbare Komponente für den Nutzer mit einem XML-Teil für die strukturierten Rechnungsdaten. Rechnungen dieser Art benötigen keine bilaterale Abstimmung. PDF versteht heute nahezu jedes rechnungsverarbeitende System. Dies gilt auch, wenn der ausländische Rechnungsempfänger das darin enthaltene XML gar nicht verarbeiten kann.

**Was müssen Unternehmen jetzt tun?**
Wohl die wichtigste Frage in Sachen E-Rechnungspflicht lautet: Beginnt das Unternehmen bei Null oder verfügt es bereits über ein Managementsystem, das alle Anforderungen erfüllt?

UNTERNEHMEN MÜSSEN SICHERSTELLEN, DASS DIE ELEKTRONISCHE RECHNUNG SOWOHL AUF DER SEITE DES ABSENDERS ALS AUCH AUF DER SEITE DES EMPFÄNGERS GLEICH „INTERPRETIERT" WIRD.

**Christoph Nordmann, Head of Communication, easy software AG**
**www.easy-software.com**

## #1 Überblick dank Ist-Analyse

Egal wie die Antwort auf diese Frage lautet, grundsätzlich ist es von Vorteil, wenn Unternehmen eine interne Bestandsaufnahme durchführen. Eine Ist-Analyse der Rechnungsverarbeitung verschafft einen klaren Überblick über alle Prozesse und Beteiligten und dient als Grundlage für die weitere Planung. Je nach Stand des Unternehmens kann es sinnvoll sein, einen Projektleiter zu bestimmen, der über die notwendigen finanziellen und zeitlichen Ressourcen verfügt. Um alle relevanten Bedürfnisse und Anforderungen zu berücksichtigen, empfiehlt es sich, gemeinsam mit den betroffenen Abteilungen (Einkauf, Controlling, Rechtsabteilung und IT) eine erste Übersicht zu erstellen. Dies hilft sowohl eine neue Software in die IT-Infrastruktur zu integrieren und bestehende Prozesse zu digitalisieren als auch bestehende Systeme auf ihre Compliance-Tauglichkeit zu prüfen.

## #2 Anforderungskatalog erstellen

Der Anforderungskatalog bildet die Entscheidungsgrundlage für eine neue Softwarelösung. Darin werden Ziele, Anforderungen, Benutzerrollen und Berechtigungen klar definiert. Die Projektverantwortlichen erstellen eine Liste der Erwartungen an die digitale Rechnungsverarbeitung unter Berücksichtigung der Vor- und Nachteile sowie der spezifischen Funktionalitäten des bestehenden Prozesses. Das Resultat ist eine Checkliste, die den weiteren Entscheidungsverlauf erleichtert. Unternehmen, die bereits ein DMS verwenden, können hier aufatmen. Denn in der Regel unterstützen die Systeme bereits die gängigen E-Rechnungsstandards wie XRechnung oder ZUGFeRD. Das erleichtert die Umsetzung der E-Rechnungspflicht erheblich.

# TIMELINE ZUR E-RECHNUNGSPFLICHT


Quelle: easy software AG

## #3 Technische Spezifikationen definieren

Anders sieht es in Unternehmen aus, in denen ein solches modernes Rechnungsmanagementsystem fehlt. Für sie gilt es, im nächsten Schritt gemeinsam mit der IT-Abteilung die technischen Rahmenbedingungen zu klären. Dabei sollten sie technische Spezifikationen, das IT-Budget und die Integration in die bestehende IT-Infrastruktur berücksichtigen. Zur Orientierung dienen die folgenden Fragen:

- Wie lässt sich die Lösung an bestehenden ERP- und CRM-Systemen anknüpfen?
- Wie gestaltet sich die Integration mit Monitoring- und Archivsystemen wie Microsoft Dynamics 365 BC?
- Soll die Lösung in der Cloud sein?
- Welche Schnittstellen zum internen E-Mail-System sind nötig?

## #4 Auswahl der Lösung

Spätestens hier stehen Unternehmen vor der grundlegenden Entscheidung zwischen einer selbstentwickelten Lösung oder einer kommerziellen Software. Bei sehr spezifischen Anforderungen innerhalb des Unternehmens, kann es Sinn machen, Ressourcen wie Entwickler, Infrastruktur und Zeit in eine „Make-Lösung" zu investieren.

Doch gerade kleinere und mittlere Unternehmen, die nicht über die notwendige spezialisierte IT-Abteilung verfügen, profitieren von der bewährten Software eines Anbieters. Sie ist in der Regel schneller einsatzbereit und auf lange Sicht kosteneffizienter. Externe Dienstleister kümmern sich dabei um die Pflege und kontinuierliche Weiterentwicklung der Anwendung, einschließlich neuer Funktionen und Sicherheitsupdates. Zudem helfen erfahrene Anbieter, die sich ständig ändernden gesetzlichen Anforderungen zu erfüllen.

## #5 Onboarden von Mitarbeitern und Partnern

Unabhängig davon, ob Unternehmen eine neue Software einführen oder ihre bestehende Lösung anpassen, ist die offene Kommunikation mit den Mitarbeitenden entscheidend. Vor allem wenn Veränderungen wie die Umstellung der Rechnungsverarbeitung nicht nur den Einkauf, sondern auch andere Abteilungen betreffen. Hier sind Schulungen und Weiterbildungen gerade in der Anfangsphase essenziell. Viele Softwareanbieter bieten ein umfangreiches Schulungsangebot an. So erlernen die Verantwortlichen den Umgang mit der neuen Software sowie die gesetzlichen Anforderungen der E-Rechnung. Interne Ansprechpartner sind darüber hinaus während der Umstellungsphase bei Fragen und Problemen sehr hilfreich.

Genauso wichtig ist die Kommunikation mit den Geschäftspartnern im Hinblick auf die E-Rechnung. Unternehmen sollten ihre Lieferanten und Kunden frühzeitig über ihre Pläne und neue Workflows informieren.

An der elektronischen Rechnungsstellung führt kein Weg vorbei. Durch frühzeitige Vorbereitung und strategische Planung können Unternehmen nicht nur die Herausforderungen wie Umstellungs- und Investitionsaufwand meistern, sondern auch zukünftig von erheblichen Vorteilen profitieren. Denn die Effizienzvorteile von E-Invoicing liegen auf der Hand. Es reduziert Fehlerquellen, entlastet die Mitarbeitenden und spart bis zu 50 Prozent der Kosten. So gesehen, ist die E-Rechnung für Unternehmen nicht nur Pflicht, sondern kann sich auch zur Kür entwickeln.

***Christoph Nordmann***

# Cloudkostenoptimierung & FinOps

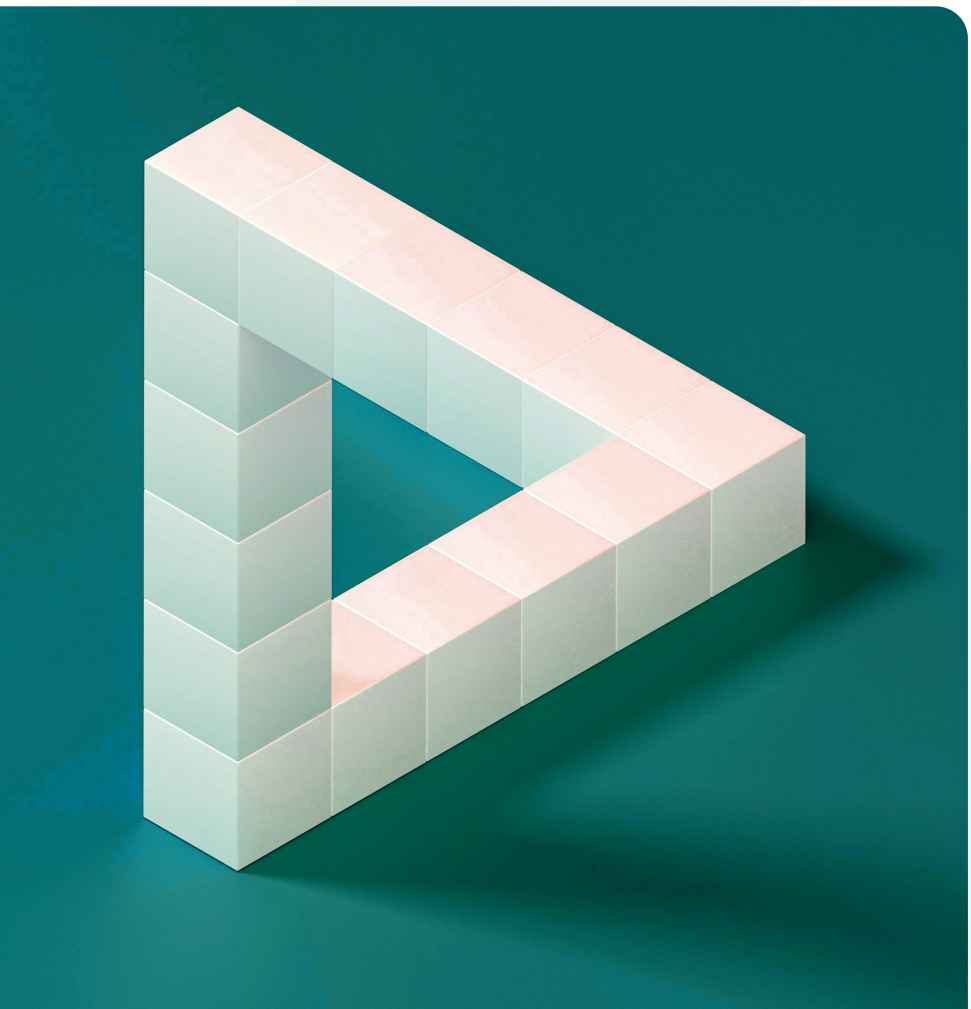
## WOHLFÜHLEN IN DER ENDLOSSCHLEIFE

Die Cloud-Nutzung in Unternehmen steigt und damit auch die Ausgaben. Wie sieht es aber mit dem ROI aus? FinOps versucht darauf eine Antwort zu liefern. Doch wer das Cloud Financial Management als isolierte und einmalige Maßnahme betreibt, erreicht nur bedingt echte Optimierung.

Unabhängig davon, ob sich IT-Ressourcen On-Premise, in einer Hosting-Umgebung, einem Rechenzentrum oder in der Cloud befinden – der Wunsch nach einer effektiven und effizienten Ressourcennutzung in Unternehmen ist groß. Immer wieder starten IT-Verantwortliche Initiativen, um die steigenden IT-Ausgaben, wenn schon nicht zu reduzieren, so doch wenigsten auf betriebswirtschaftlich „gesunde Beine" zu stellen. Die Cloud mit ihrer hohen Flexibilität hinsichtlich Nutzungs- und Preismodellen schafft hier oft mehr Komplexität als Transparenz und lässt die Kosten weiter explodieren.

**Betriebsmodell für die Cloud**

Laut State of the Cloud Report 2024 von Flexera geben 29% der Unternehmen weltweit pro Jahr bereits mehr als 12 Mio. US-Dollar für die Public Cloud aus. Selbst im Mittelstand fließen bei rund einem Drittel mehr als 1,2 Mio. US-Dollar in die Wolken. Die Cloud-Ausgaben zu managen hat höchste Priorität und FinOps gilt als das Modell, um dieses Ziel zu erreichen. Schon jetzt verfügt die Hälfte der Unternehmen über ein dezidiertes FinOps-Team. Die Analysten bei Gartner gehen im Magic Quadrant for Software Asset Management Managed Services (2023) sogar davon aus, dass Unternehmen mit FinOps-Praktiken bis 2026 rund 30% mehr Einsparungen bei ihren Cloud-Infrastruktur- und Plattformdiensten (CIPS) erzielen als Unternehmen ohne FinOps.



Quelle: Unsplash/ cdd20; CC0-Lizenz

Die Idee hinter FinOps: Wer versteht, wie Cloud-Ressourcen die Kosten beeinflussen, kann sie effektiver managen. Der Ansatz umfasst nicht nur klar definierte Prozesse und Governance-Richtlinien. IT- und Cloud-Teams sollen auch enger mit dem Einkauf und der Finanzabteilung zusammenarbeiten, um Cloud-Initiativen auf ihren Mehrwert zu prüfen und die Cloud-Strategie im Unternehmen auf einen gemeinsamen Nenner zu bringen. Das setzt unwillkürlich einen Wandel in der Unternehmenskultur voraus.

Der Erfolg von FinOps hängt jedoch von zwei Faktoren ab: Zum einen handelt es sich bei der Cloud-Kostenoptimierung nicht um eine einmalige Aktion, sondern einen fortlaufenden Prozess. Zum anderen darf FinOps nicht isoliert von anderen IT-Managementkonzepten im Unternehmen stattfinden.

**Eine unendliche (FinOps)Geschichte**

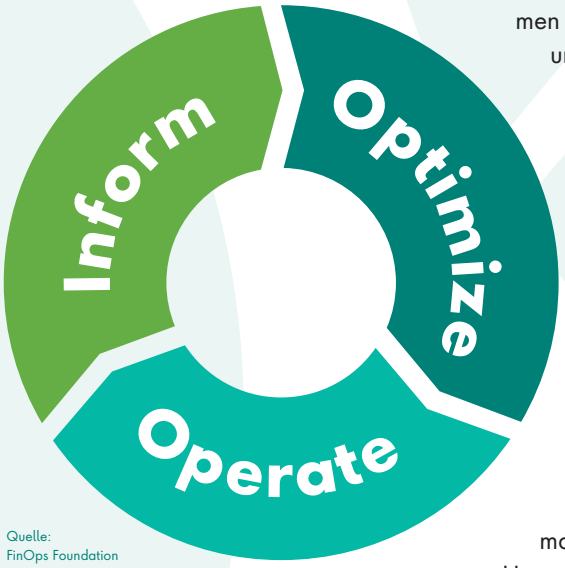
Das FinOps Framework ist nach der FinOps Foundation in drei Phasen unterteilt. In der ersten Phase geht es darum, echte Transparenz im Cloud-Estate herzustel-

len und eine genaue Inventur aller Cloud-Services und -Assets vorzunehmen („Inform"). Ziel ist, eine Kosten-Nutzen-Analyse für jede einzelne, identifizierbare Einheit (z. B. Cloud-Instanz) zu erstellen. In der zweiten Phase lassen sich dann auf dieser Basis, Verbesserungs- und Einsparungspotentiale identifizieren („Optimize"). Das kann das Herunterfahren von Workloads nach Geschäftsende, die konsequente Verfolgung von Schatten-IT bzw. Rogue SaaS oder die Neuverhandlung mit Cloud-Anbietern beinhalten. In der dritten Phase geht es schließlich darum, alle getroffenen Maßnahmen im laufenden IT- und Cloud-Betrieb kontinuierlich zu überprüfen, anzupassen und zu automatisieren („Operate").

DIE IDEE HINTER FINOPS: WER VERSTEHT, WIE CLOUD-RESSOURCEN DIE KOSTEN BEEINFLUSSEN, KANN SIE EFFEKTIVER MANAGEN.

**Wolfgang Schuster,**
**Executive Advisor, Flexera**
**www.flexera.de**

Foto: Wolfgang Schuster




Quelle:
FinOps Foundation

Hier zeigt sich bereits die zyklische Natur von FinOps: Es ist ein nie endender Prozess, der kontinuierliche Ressourcen und Maßnahmen erfordert. Und während bestimmte Optimierungen ein Plateau erreichen können, beginnt der Zyklus mit der Einführung neuer IT-Assets, Services oder Technologien wieder von Neuem.

Dabei ist es egal, ob Unternehmen ihre Cloud-Reise vor zehn Jahren oder vor zehn Monaten begonnen haben. Sie alle stehen immer wieder vor einer steilen Lernkurve, sobald neue IT-Assets integriert werden sollen. Häufig gehen Unternehmen zu Beginn auf Nummer sicher und stellen mehr Ressourcen zur Verfügung als in der Praxis nötig sind. Erst wenn erste Erfahrungswerte hinsichtlich der Nutzung und Auslastung vorliegen, lassen sich wichtige Anpassungen (Rightsizing) vornehmen.

Besonders schön zeigt sich dieses Phänomen aktuell beim Run auf GenAI. Das Angebot an „intelligenten" Services, Features oder Tools ist massiv gewachsen und stößt bei Unternehmen auf hohes Interesse. Laut Flexera-Umfrage nutzt bereits ein Viertel der Unternehmen (25%) Cloud-GenAI-Services ausgiebig für das tägliche Arbeiten. Weitere 38% experimentieren mit der KI. IT-Verantwortliche stehen bei der Einführung der neuen Anwendungen gleich in mehrfacher Hinsicht vor einer Lernkurve. Denn wie alle neuen IT-Assets setzen auch ChatGPT, Microsoft Copilot & Co. zunächst einmal hohe Investitionen voraus, die es kontinuierlich auf ihren ROI zu überprüfen gilt.

**Besser im Team: ITAM und FinOps**

Kosten allein sind keine gute Grundlage für IT-Investitionsentscheidungen. Hinzu kommt, dass die Cloud-Kostenoptimierung weit über die Grenzen von IaaS- und PaaS-Ressourcen und -Services hinausreicht. So fallen beispielsweise für Software in der Cloud – sprich SaaS – in der Regel hohe Ausgaben an, die jedoch in den frühen Phasen des FinOps-Lebenszyklus gerne und oft übersehen werden.

Gerade bei SaaS sind Kosten und Lizenzen eng miteinander verknüpft. Dementsprechend gilt es auch beide Aspekte bei einer geplanten Optimierung zu berücksichtigen. FinOps-Teams sind keine Spezialisten für komplexe Lizenzierungen und Nutzungsrichtlinien. Und was nach FinOps kosteneffektiv erscheint, kann aus Sicht des Lizenzmanagements verheerende Folgen nach sich ziehen.

Gefragt ist daher ein ganzheitlicher Ansatz oder hybrider Ansatz, der das IT-Asset-Management (ITAM) und damit die Verwaltung und Dokumentation aller Soft- und Hardwarebestände eines Unternehmens sowie deren Verhältnis zueinander berücksichtigt. Hybrides ITAM und FinOps kombiniert das Know-how zweier zentraler IT-Disziplinen, um Cloud-Kosten im Kontext ihrer Lizenzen sowie ihrer Bereitstellungsmodelle, ihrer Nutzung und ihres technischen Mehrwerts ganzheitlich zu bewerten. Oder anders gesagt: Die Kosten beziehen sich nicht mehr nur auf die Cloud-Ressourcen, auf denen eine Anwendung läuft, sondern auch auf die Anwendungen selbst. Damit gewinnen Unternehmen Einblick in die „echten" Kosten der Cloud und eine Total Cost of Ownership (TCO).

Die Erwartungen in FinOps als Bändiger der Cloud sind hoch. Wer den Ansatz jedoch isoliert praktiziert und als einmalige Aufgabe abtut, untergräbt das Potential des Frameworks. Dass FinOps richtig umgesetzt die Cloud-Kosten senkt, ist im Übrigen belegt. Laut State of the Cloud-Report waren nach einem Rekordhoch in 2022 (32%) die unnötigen Cloud-Ausgaben für IaaS und PaaS im letzten Jahr erstmals tendenziell rückläufig (27%).

***Wolfgang Schuster***

it management

AUSGABE 11-12/2024
ERSCHEINT
AM 4. NOVEMBER 2024

## UNSERE THEMEN

Innovationen 2025
IT Servicemanagement
IT & Nachhaltigkeit

it security

AUSGABE 11-12/2024
ERSCHEINT
AM 4. NOVEMBER 2024


## UNSERE THEMEN

Innovationen 2025
Schatten IT
Cyberversicherungen

**WIR WOLLEN IHR FEEDBACK**

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

## INSERENTENVERZEICHNIS

***it management***


| | |
|---|---|
| BlackLine GmbH (Teaser) | U1, 22 |
| Zscaler Germany GmbH (Teaser) | U1, 42 |
| Sophos Technology GmbH (Teaser) | U1, 44 |
| NürnbergMesse GmbH | U2 |
| USU Software AG | 7 |
| noris network AG | 9 |
| it verlag GmbH | 14 |
| ivanti (Advertorial) | 19 |
| MHP Management- und IT-Beratungs GmbH (Advertorial) | 25 |
| xSuite Group GmbH | 27 |
| Gambit Consulting GmbH | 31 |
| Consilio GmbH | 41, 49 |
| Next Experts GmbH | 57 |
| E3 / B4B Media | U3 |
| ZOI TechCon GmbH | U4 |


## 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:*** Christian Achenbach, Behrad Babaee, Thomas Baier, Lars Becker, Philipp von der Brüggen, Fabian Czicholl, Philipp Fischer, Dominik Hagen, Christoph Herrnkind, Volker Hettich, Süleyman Karaman, Mehrnaz Lotfali-Shirazi, Simon Meraner, Carina Mitzschke, Christoph Nordmann, Silvia Parthier, Ulrich Parthier, Tobias Pföhler, Kai Roßnagel, Gerald Schlechter, Wolfgang Schuster, Dr. Björn Stark, Amadeus Thomas

***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, +49 152-3634 1255, mann@it-verlag.de

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

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

***Erscheinungsweise:*** 6 x pro Jahr

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

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

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


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

# SAP BTP
# KOMPLEXITÄT RUNTER, INNOVATION RAUF

Mit **Zoi** als **Cloud-Pionier** holen Sie das **Maximum** aus der SAP Business Technology Platform.

**60%**

Agilere Workflows durch Prozessautomatisierung und -integration

**25%**

Steigerung der Mitarbeiterproduktivität dank Citizen Development

**50%**

schnellere Time-to-Market durch Low-Code- und No-Code-Tools

SAP Gold Partner

**50+** erfolgreiche SAP on Cloud Projekte

Zertifizierter **SAP Expert Partner**

**Full Service** von Start bis Ziel

Mehr erreichen mit weniger Aufwand: **LET'S GET IN TOUCH!**

zoi.tech

it security

Detect. Protect. Respond.
September/Oktober 2024

THOUGHT LEADERSHIP

AB **SEITE 10**

ninjaOne.

NIS2

# Intelligentes Risikomanagement

Ralf Kempf, Pathlock Deutschland GmbH

DriveLock
Ganzheitliche Sicherheit
**ab Seite 14**

ASOFTNET
IT-Security | Security Operation Center | IT-Forensik
KI-basiertes SOC
**ab Seite 20**

BELDEN | macmon intelligent einfach
Industrie 4.0-Sicherheit
**ab Seite 24**

NIS2-RICHTLINIE

Dank Fahrplan stressfrei zum Ziel

DIGITALE SOUVERÄNITÄT

Management digitaler Identitäten


itsa EXPO CONGRESS
PLAY HARD.
PROTECT SMART.
HOME OF IT SECURITY
JETZT GRATIS-TICKET SICHERN!
22. – 24. Oktober 2024
Nürnberg, Germany
itsa365.de/itsa-expo-besuchen
NÜRNBERG MESSE

# Inhalt


## COVERSTORY

**4** **Cybersicherheit**
Intelligentes Risikomanagement

**6** **Threat Detection weitergedacht**
Passgenauer Einsatz von KI

## THOUGHT LEADERSHIP

**10** **Mobile Device Management**
Sicherheit für unterwegs

## IT SECURITY

**14** **DriveLock Hypersecure Platform**
Ganzheitliche Sicherheit

**16** **Absicherung komplexer E-Mail-Infrastrukturen**
Individuelles Routing

**17** **E-Mail-Sicherheit**
Gemeinsam stark

## IT-SA SPEZIAL

**20** **KI-basiertes Security Operations Center**
Schutz vor digitalen Bedrohungen

**24** **Industrie 4.0-Sicherheit**
Moderne IT-Schutzkonzepte

**28** **Datenrisiken beim Einsatz von GenAI**
So lassen sie sich vermeiden

**32** **Management digitaler Identitäten**
Digitale Souveränität

**36** **Kein Platz für Ermüdungserscheinungen**
Clevere Lösungen für Security in KMUs

**40** **Das modern SOC**
Bestmöglicher Schutz

**44** **NIS2 ist da**
Fahrplan zur Umsetzung

**48** **Attributdaten haben oder nicht haben**
Hype um die Wallet

**50** **Krieg der KIs**
Risiken minimieren

**52** **Managed Security Service**
Einfacher geht´s nicht

**54** **Multi-Faktor-Authentifizierung**
Warum es ohne nicht mehr geht

**56** **Excel war gestern**
Krisensicher dank zentralem BCM

**62** **Passwortlose Authentifizierung**
Was bedeutet sie für das PAM?

## IT SECURITY

**66** **Cyber Resilience Act**
Darauf müssen Hersteller achten

**68** **IT-Sicherheitsteams unter Cyberstress**
Verbesserte Cybersicherheit

**70** **KRITIS-Unternehmen müssen jetzt handeln**
Systeme zur Angriffserkennung

**72** **Der SD-WAN-Transformationsguide**
Reibungslose Migration

**74** **Gekaperte Router entfesseln DDoS-Tsunami (Teil 1)**
Wenn Core-Router gefährlich werden

# Cybersicherheit

## INTELLIGENTES RISIKOMANAGEMENT IN ZEITEN VON NIS2

Ralf Kempf, CEO des IT-Security- und GRC-Spezialisten Pathlock Deutschland und SAP Evangelist, gibt Einblicke, wie die neue Europäische Cybersicherheitsdirektive immer mehr Unternehmen und deren Management in die Pflicht nimmt und warum NIS2 auch als Chance gesehen werden muss, sich resilient und vor allem ganzheitlich aufzustellen.

**it security:** *Hallo Herr Kempf, können Sie uns eine „Wasserstandsmeldung" zur Situation deutscher Unternehmen angesichts neuer Herausforderungen der Cybersecurity geben?*

**Ralf Kempf:** Tatsächlich haben viele Unternehmen den Eindruck, ihnen stehe sicherheitstechnisch das Wasser bis zum Halse – oder schon darüber. NIS2 macht ihnen bewusst, dass sie in der Vergangenheit sozusagen nicht mal einen ordentlichen Schwimmkurs absolviert haben. Die Einschätzung der CISOs in Bezug auf Unternehmenssicherheit und NIS2 ist, dass sie darauf nicht vorbereitet sind. Die Mehrheit sieht Anwendungssicherheit als blinden Fleck ihrer IT-Sicherheitsstrategie.

**it security:** *Und wie konnte es so weit kommen?*

Ralf Kempf: Zunächst, so die CISOs, weil Security-Tools oftmals kaum Erkenntnisse liefern, mit denen Vorstände Geschäftsrisiken verstehen und Bedrohungen adressieren können. Die Kluft dieser Technologie- und Kommunikationslücken wird angesichts steigender Bedrohungen immer breiter, trotz eigentlich probater Lösungen wie Security Dashboards.

**it security:** *Das beweist doch eigentlich den klaren Bedarf, oder?*

**Ralf Kempf:** Schon, aber frappierend ist, dass trotzdem fast nichts passiert. Die Erkenntnis führt weder zu einer überfälligen Priorisierung der IT-Sicherheit noch zu dringend nötigen Maßnahmen. Unser Eindruck: Unternehmen wissen nicht, wie und wo sie anfangen sollen, den Herausforderungen komplexer IT-Systeme und hybrider SAP-/Non-SAP-Landschaften inklusive neuer Cloud-Applikationen zu begegnen.

Es hilft aber nicht, untätig zu bleiben in der Hoffnung, die Flut von Herausforderungen werde abziehen oder es treibe eine Insellösung vorbei, die etwa NIS2-Compliance ad hoc herbeizaubert. Der laxe Umgang mit Erkenntnissen zeigt auch, wie sich selbst CISOs von aktuellen Buzzwords beeindrucken lassen und eine ganzheitliche Absicherung aus dem Auge verlieren.

**it security:** *Welche Buzzwords meinen Sie?*

**Ralf Kempf:** Nehmen wir zwei, die die aktuelle Diskussion beherrschen und oft in falscher Sicherheit wiegen: Die Cloud ist kein Allheilmittel und ersetzt keine Firewall, sie eröffnet gar neue Angriffsvektoren, derer man sich bewusst sein muss. Und KI hat ganz sicher die Spielregeln für Cybersicherheit verändert, aber darf nicht als pauschale Universallösung oder -bedrohung missverstanden werden.

**it security:** *Okay, aber ist NIS2 nicht auch ein Buzzword?*

**Ralf Kempf:** Nein, sie ist in ihren Konsequenzen eindeutig unverzichtbar für eine europaweite Resilienz. Sie forciert, dass Cybersecurity zum wesentlichen Teil der Unternehmenskultur wird, und zwar als Chefsache. Wer sie vernachlässigt, setzt sein Unternehmen künftig nicht nur erhöhter Angriffsgefahr aus, sondern auch enormen Bußgeldern. Also klare Empfehlung: das Thema priorisieren, Umsetzungsfristen im Auge behalten und die richtigen Partner ins Boot holen.

**it security:** *Von welchem Zeitrahmen sprechen wir hier?*

**Ralf Kempf:** Einem äußerst engen, Unternehmen sollten keine Zeit mehr verlieren, denn die Direktive weitet Cybersicherheit auf mittelständische, allein in Deutschland geschätzte 30.000 Unternehmen aus. Und eines steht fest: Im Oktober wird NIS2 in Kraft treten. Selbst wenn sich die Umsetzung hier verzögert: Wer das Thema nicht sofort angeht, wird es nicht rechtzeitig schaffen. Und Unternehmen, die nicht mal geklärt haben, ob sie betroffen sind, könnten versucht sein zu folgern, dass auch kein Handlungsbedarf besteht. Eine gravierende Fehleinschätzung.

**it security:** *Inwiefern gravierend?*

**Ralf Kempf:** Nun, wichtige Vorgaben werden sofort greifen, etwa die verpflichtende Registrierung beim BSI. Und die Sanktionen: Falls danach ein sicherheitsrelevanter Vorfall eintritt, dessen Folgen auf eine Nichterfüllung der Compliance-Auflagen hindeuten, kann es ausgesprochen teuer werden.

> WER NIS2 VERNACHLÄSSIGT, SETZT SEIN UNTERNEHMEN KÜNFTIG NICHT NUR ERHÖHTER ANGRIFFSGEFAHR AUS, SONDERN AUCH ENORMEN BUSSGELDERN.
>
> **Ralf Kempf, CEO, Pathlock Deutschland GmbH, www.pathlock.de**

**it security:** *Was ist also als Erstes zu tun?*

**Ralf Kempf:** Zunächst sollten Unternehmen prüfen, ob sie zum engen oder zum erweiterten Geltungsbereich gehören. Viele werden indirekt betroffen sein, etwa weil sie KRITIS-Unternehmen beliefern. Auch sie müssen künftig Standards zur Absicherung der Lieferkette erfüllen und nachweisen. NIS2 wird als sogenanntes Artikelgesetz viele andere wie das Energiewirtschaftsgesetz ändern und erweitern. Diese sind mitzuprüfen.

**it security:** *Und wenn klar ist, dass man dazugehört?*

**Ralf Kempf:** Fast alle wünschen sich dann eine exakte Angabe umzusetzender Maßnahmen. Man sollte sich aber nicht vorschnell für Lösungen entscheiden, die pauschal die Beseitigung aller Herausforderungen ohne Berücksichtigung von Unternehmensspezifika anbieten. Natürlich ist der Handlungsdruck groß und der Markt wird erwartbar mit Allheilmitteln aufwarten, die aber oftmals wenig effizient oder zielführend sind.

**it security:** *Was raten Sie stattdessen?*

**Ralf Kempf:** Sich statt vieler Insellösungen die richtige Expertise zu suchen und das Projekt schnellstmöglich ganzheitlich und passgenau voranzutreiben. Und zu berücksichtigen, welche Lösungen, Software und etablierten Maßnahmen sich im Unternehmen bereits vorfinden. Da jedes anders ist, gibt es für dieses individuelle Vorgehen kein universelles Rezept, aber ein paar probate Tipps.

Viele NIS2-Vorgaben sind eng an die ISO 27001 angelehnt. Große Unternehmen sollten sich bei der Implementierung eines Information Security Management Systems daran orientieren, kleinere können auf den kompatiblen Grundschutzkatalog des BSI zurückgreifen.

Grundlegende NIS2-Vorgaben sind: ein Incident Management zur Vorbeugung, Erkennung und Bewältigung von Security-Vorfällen, ein Identity- & Access Management und ein Business Continuity Management, das nicht nur Backups und Disaster Recovery vorsieht, sondern auch Krisenmanagement wie Notfallpläne.

**it security:** *Aber womit sollte man anfangen, gibt es keine Art Roadmap?*

**Ralf Kempf:** Im Grunde folgt der Weg zur Compliance einem etablierten Muster: der Ermittlung des Ist-Zustandes, um interne IT-Strukturen zu dokumentieren und den Bedarf an zusätzlichen Anschaffungen und Dienstleistungen im NIS2-Kontext zu ermitteln. Auf Basis der initialen Analyse wird ein internes Kontrollsystem samt Prüfvorgaben definiert und ein sicher konfigurierter optimaler Soll-Zustand.

In der System-Härtung wird dann immer weiter auf den Soll-Zustand hingearbeitet, indem man Schwachstellen behebt und neue Prozesse etabliert. Um hier Zeit zu gewinnen, bietet sich agiles Projektmanagement an. Schließlich muss das Erreichte kontinuierlich gehalten und mittels präventiver und detektiver Kontrollen überprüft werden – und zwar in Echtzeit. Permanente Überwachung in Echtzeit ist eine zentrale NIS2-Forderung.

**it security:** *Haben Sie noch ein kurzes Fazit für uns?*

**Ralf Kempf:** Klar ist, dass Unternehmen die NIS2-Umsetzung nicht allein stemmen sollten. Dienste wie Security Operations Center oder unsere neu entwickelte Lösung „Threat Intelligence" helfen, die Abwehr zu verbessern und potenzielle Schwachstellen in Sekunden zu identifizieren und zu schließen.

Letztlich wird kein Unternehmen IT Security ohne einen ganzheitlichen Ansatz effektiv gestalten können. So sind alle gut beraten, sich kontinuierlich mit der Verbesserung ihrer IT-Sicherheit zu befassen, und die ist nicht nur in kritischen Infrastrukturen relevanter denn je.

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

THANK YOU

# Threat Detection intelligent weitergedacht

## PASSGENAUER EINSATZ VON KI

Während das Buzzword KI in Sicherheitsszenarien vor allem als Gefahr sich rasant entwickelnder Angriffsvektoren wahrgenommen wird, werden ihre Chancen und Möglichkeiten als weitere Verteidigungslinie oftmals falsch eingeschätzt. KI ist kein undifferenziertes Allheilmittel, kann jedoch die IT-Security verbessern, wenn sie strategisch und wissensbasiert eingesetzt wird.

Threat Intelligence ist eine Erweiterung etablierter Threat-Detection-Lösungen, um die Detektion durch die Anwendung von Machine Learning zu präzisieren und angepasst auf identifizierte Risikosituationen automatisierte Reaktionen zu erlauben. Bislang folgten als Reaktion auf ein erkanntes Risiko zwei Schritte: zunächst die Bewertung der Situation und dann das Ergreifen von Maßnahmen. So verstrich wertvolle Zeit durch unterbesetzte Security Operations Center, fehlendes Know-how oder komplexe Bewertungsprozesse, bis Gegenmaßnahmen ergriffen werden konnten – wobei gerade die Reaktionszeit der entscheidende Faktor bei der Schadensbegrenzung ist.

**Schutz in Echtzeit und rund um die Uhr**

Die Integration automatisierter Prozesse als zusätzliche Sicherheitsebene kann dieses Dilemma entschärfen, indem Zugriffe auf kritische Transaktionen kontextspezifisch eingeschränkt oder sogar vollständig blockiert, einzelne Datenfelder attributbasiert maskiert, weitere Downloads verhindert oder User mit kritischem Verhalten vom System abgemeldet werden. Und zwar vollautomatisch, in Echtzeit und rund um die Uhr.

Durch diese unverzüglichen Reaktionen im Falle einer als Risiko eingestuften Situation werden hochsensible Informationen unmittelbar und zielgenau geschützt. Dabei ist das zugrundeliegende Regelwerk vollständig konfigurierbar und je nach Anwendungsfall individuell anpassbar. Threat Intelligence erweitert die Threat Detection durch die Nutzung Künstlicher Intelligenz um einen strategischen Schritt, damit schnellstmöglich Maßnahmen zur Schadensbegrenzung oder -vermeidung ergriffen werden können. Maschinelles Lernen unterstützt dabei die Vorqualifizierung von Events durch den Einsatz verschiedener Methoden.

THREAT INTELLIGENCE IST NICHT NUR TECHNISCHES HILFSMITTEL, SONDERN EIN INTEGRALER BESTANDTEIL DER STRATEGISCHEN SICHERHEITSPLANUNG EINES UNTERNEHMENS.

**Raphael Kelbert, Product Management, Pathlock Deutschland GmbH, www.pathlock.de**

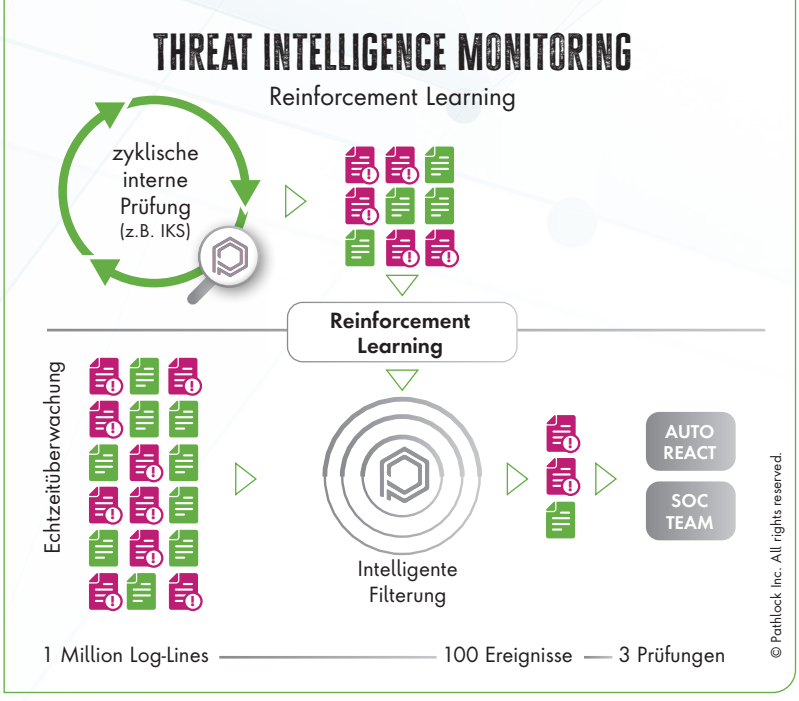
**Verbesserte Bedrohungsdetektion durch Maschinelles Lernen**

Threat Intelligence verbessert also die Fähigkeiten der Bedrohungserkennung und erlaubt (teil-)automatisierte Reaktionen im Anwendungskontext. Hierbei kommen Reinforcement Learning und User and Entity Behavioral Analytics (UEBA) als innovative Ansätze zum Einsatz.

Reinforcement Learning hilft, Ereignisse besser zu bewerten, indem es Informationen aus verschiedenen Quellen wie zyklischen internen Audits in die Echtzeit-Risikoanalyse integriert. Beispielsweise werden Aufrufe von Programmen mit potenziellen Codeschwachstellen oder Aktionen privilegierter Benutzer automatisch mit höherer Kritikalität bewertet als andere. So können relevante Ereignisse identifiziert und detailliert analysiert werden, um die IT-Sicherheitssysteme kontinuierlich zu verbessern. Eine Empfehlung, wie stark die Kritikalität dabei gegenüber einer unkritischen Aktivität erhöht wird, ist anwendungsfallspezifisch vorgeschlagen, lässt sich allerdings auch individuell nach Kundenanforderung redefinieren.

**Automatisierte Verhaltensanalyse**

User and Entity Behavioral Analytics (UEBA) erkennt Anomalien im Verhalten von Benutzern und Systemen. Es kann ungewöhnlich hohe Transaktionsvolumina oder das plötzliche Auftreten seltener Transaktionen aufspüren. Wenn beispielsweise ein Benutzer, der normalerweise nur Einkaufsbestellungen bearbeitet, plötzlich umfangreiche Finanztransaktionen durchführt, deutet dies auf eine potenzielle Bedrohung




oder betrügerische Aktivität hin. UEBA identifiziert solche ungewöhnlichen Verhaltensmuster und leitet sofort Maßnahmen ein, um Risiken zu minimieren und die Systemintegrität zu gewährleisten.

Der kombinierte Einsatz von Reinforcement Learning und UEBA ermöglicht es, Bedrohungen nicht nur schneller zu erkennen, sondern auch präziser zu bewerten, so dass effektiv darauf reagiert werden kann. Und dies unabhängig davon, ob die nachfolgende Reaktion auf das Security Event automatisiert, teilautomatisiert oder manuell erfolgt.

**Fundierte Entscheidungen mit Threat Intelligence**

Zusätzlich zur verbesserten Detektion durch Maschinelles Lernen bietet Threat Intelligence die Möglichkeit, Security Events automatisiert zu Incidents zusammenzufassen und im Kontext darauf zu reagieren. Die Zusammenfassung erfolgt nach Faktoren wie der Kritikalität, der Datenquelle, dem Event-Typ oder der Event-Kategorie, die in beliebiger Kombination verwendet werden können und als Pattern zur Incident Creation gesichert werden. Durch die Berücksichtigung des Zeitraums beim Erstellen von Incidents ist es möglich, beispielsweise täglich alle Events eines Patterns in einem Incident zu sammeln.

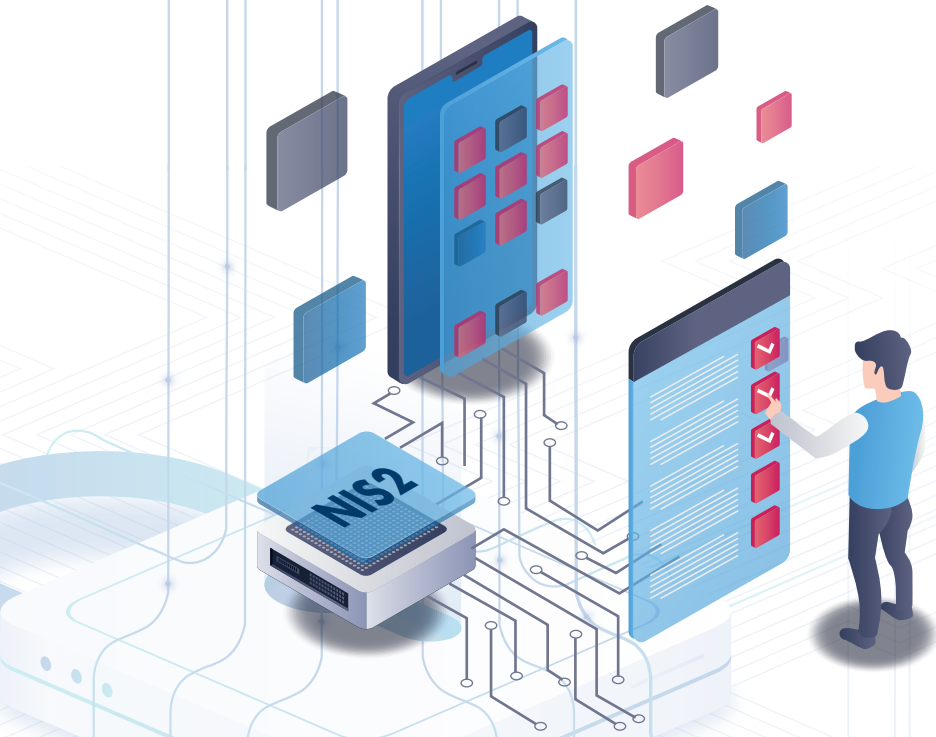
Jedem Incident Creation Pattern lassen sich Aktionen zuordnen, wobei definiert werden kann, ob eine Aktion automatisiert, teilautomatisiert oder manuell – im Rahmen eines Reviews – ausgeführt werden soll. Zu den verfügbaren Aktionen zählen die Funktionen der Dynamic Access Control zur attributbasierten Zugriffs- und Ansichtsbeschränkung, das automatisierte Ausplanen von Batch-Jobs, das Abmelden und/oder Sperren von Benutzern sowie das Entfernen von Benutzer-Rollen.

Threat Intelligence ist dabei nicht nur technisches Hilfsmittel, sondern ein integraler Bestandteil der strategischen Sicherheitsplanung eines Unternehmens. Durch die Nutzung von KI-gestützter Bedrohungsanalyse können CISOs und deren Security Teams fundierte Entscheidungen treffen und Sicherheitsmaßnahmen gezielt priorisieren. Dies führt zu einer besseren Ressourcenallokation und ermöglicht es, präventive Maßnahmen zu ergreifen. Die strategische Einbindung von Threat Intelligence verbessert so nicht nur die Reaktionszeit, sondern stärkt auch ein ganzheitliches Sicherheitsbewusstsein im Unternehmen.

**KI und der Schlüsselfaktor Mensch**

Künstliche Intelligenz als strategisches Werkzeug eingesetzt, entlastet Security-Analysten, indem es ohne manuelles Eingreifen Security Events automatisch analysiert und zusammenfasst. Durch das Filtern und die Nutzung komplexer Zusammenhänge und Kontextinformationen bietet KI besser qualifizierte Ergebnisse, sodass manuelle Qualifikationsschritte reduziert werden. Die Analysten haben dabei stets die Option, Automatismen auszuschalten und auf manuelle Tätigkeiten umzustellen, um jeden Einzelfall individuell zu bewerten. Der Einsatz von KI dient somit als unterstützendes Tool, ermöglicht eine fokussierte Bearbeitung relevanter Themen, spart Zeit und erhöht die Effizienz, damit hoch qualifiziertes Personal weiterhin sinnvoll dort eingesetzt werden kann, wo die menschliche Expertise unverzichtbar bleibt.

***Raphael Kelbert***




# NIS2-CHECKLISTE

## IN 10 SCHRITTEN ZUR EINHALTUNG DER NIS2-RICHTLINIE

NIS2 kommt, das steht fest. Mit der Zunahme von Cyberbedrohungen haben Regierungen auf der ganzen Welt Gesetze und Vorschriften eingeführt, die dazu beitragen sollen, dass Unternehmen zum einen sich selbst, aber auch Ihre Kunden und Geschäftspartner schützen. Eine dieser Vorschriften ist die NIS2-Richtlinie, die EU-Unternehmen zur Einhaltung strenger Cybersicherheitsstandards verpflichtet. Im Oktober 2024 tritt die Novellierung des NIS-Gesetzes, NIS 2.0, in Kraft, die Unternehmen mit zusätzlichen Anforderungen an die Informationssicherheit konfrontiert.

Als EU-Unternehmen ist es nun wichtig zu verstehen, was die NIS2-Richtlinie ist und wie sie sich auf Ihr Unternehmen auswirkt.

NIS steht für „Network and Information Security". Bereits seit 2016 gibt es die Richtlinie zu NIS1. Diese reguliert die notwendigen Maßnahmen für Unternehmen und Organisationen, die als KRITIS (Betreiber kritischer Infrastrukturen) eingestuft wurden. Das wir nun anders werden mit NIS2. Mit NIS2 sind weit mehr Unternehmen betroffen, als das mit NIS1 der Fall war.

Die folgende Checkliste soll Ihnen daher einen Schritt-für-Schritt-Leitfaden liefern, wie Sie die NIS2-Richtlinie einhalten und sicherstellen können, dass Ihr Unternehmen geschützt ist. Sie dient als nützliche Grundlage, um sicherzustellen, dass Ihre Organisation die erforderlichen Maßnahmen zur Verbesserung der Cybersicherheit und zur Einhaltung der EU-Vorschriften ergriffen hat. Erfahren Sie hier, wie Sie die NIS2-Richtlinie umsetzen und die digitale Resilienz Ihres Unternehmens stärken können.


**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 8 Seiten und steht kostenlos zum Download bereit.
**www.it-daily.net/Download**

# MOBIL & SICHER

**Smartphones und Tablets sind im Arbeitsalltag unverzichtbare Werkzeuge geworden, gewähren sie doch schnell und unkomplizierten Zugriff auf benötigte Daten, Kontakte oder Tools. Doch mit dem Zugriff von außerhalb des firmeneigenen Netzwerkes, wachsen die Sicherheitsrisiken für Unternehmen. Gerade mobile Geräte geraten immer mehr in den Fokus von Cyberkriminellen. Eine Möglichkeit diese Herausforderung effektiv zu meistern, bietet das Mobile Device Management.**

**Mit den richtigen Lösungen lässt sich der Schutz mobiler Geräte unkompliziert in bereits bestehende Sicherheitskonzepte integrieren und ermöglicht so eine sichere und produktive mobile Arbeitsumgebung.**

# Mobile Device Management

## SICHERHEIT UNTERWEGS SOLLTE WEDER KOMPLEX NOCH TEUER SEIN

Flexibilität und Sicherheit in Einklang zu bringen, stellt Unternehmen dank der mobilen Arbeitswelt vor große Herausforderungen. Wir sprachen mit Andé Schindler, General Manager bei NinjaOne über die Nutzung mobiler Geräte im beruflichen Umfeld, über deren Risiken und welche Vorteile Mobile Device Management bringen.

**it security:** *Mobile Geräte sind heutzutage in der modernen Arbeitswelt allgegenwärtig. Welche Rolle spielt Mobile Device Management da?*

**André Schindler:** Am modernen Arbeitsplatz ist die Nutzung mobiler Geräte, ob firmeneigen oder privat, eher die Regel als die Ausnahme. Diese Geräte ermöglichen es, jederzeit und überall effizient zu arbeiten. Allerdings können unzureichend oder gar nicht verwaltete mobile Geräte zu Frustration führen. Sei es durch die Unfähigkeit, auf benötigte Anwendungen und Ressourcen zuzugreifen, oder durch Verzögerungen bei der Behebung technischer Probleme. Das wirkt sich negativ auf die Teammotivation aus und ist darüber hinaus ein unnötiger Zeitfresser. Zudem erhöhen unverwaltete mobile Devices die Angriffsfläche der jeweiligen Organisation. Und erhebliche zusätzliche Sicherheitsrisiken braucht in Zeiten wachsender Cyberbedrohungen wirklich niemand.

**it security:** *Welche Risiken sind konkret mit unverwalteten mobilen Geräten verbunden?*

DAS PASSENDE TOOL REDUZIERT KOMPLEXITÄT UND KOSTEN, INDEM ES EINE KONSOLIDIERTE SICHT AUF ALLE ENDPUNKTE BIETET.

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

**André Schindler:** Unverwaltete mobile Geräte können verschiedene Risiken bergen. Dazu gehören beispielsweise schwache oder gar nicht vorhandene Passwörter, das Herunterladen von Apps aus unsicheren Quellen, das Abschalten von Verschlüsselung und die Nutzung öffentlicher WLAN-Netze. All diese Faktoren können die Sicherheit eines Unternehmens erheblich gefährden. IT-Teams benötigen daher Sichtbarkeit und ausreichende Kontrolle über die mobilen Geräte der Nutzer. Nur so können sie gewährleisten, dass sie richtig konfiguriert, compliant und sicher sind. Es ist jedoch auch wichtig, dass die IT-Teams die Benutzerfreundlichkeit und Produktivität nicht beeinträchtigen - hier kommen die MDM-Tools ins Spiel.

**it security:** *Was muss ein solches Tool können, um wirklich einen Nutzen zu bieten?*

**André Schindler:** Um möglichst effizient arbeiten zu können und sich nicht in einem Wust an Einzellösungen wiederzufinden, setzen Unternehmen idealerweise auf eine zentrale Plattform zur Verwaltung aller Endgeräte. So können die jeweiligen IT-Teams die wichtigsten Features innerhalb eines Tools nutzen: eine vollständige Bestandsverfolgung, einfache Bereitstellung und Verwaltung von Konfigurationen sowie Remote Support. Wichtig ist, dass die eingesetzte Lösung die gewünschte Sicherheit bietet. Das gelingt, indem sie IT-Teams die Möglichkeit gibt, Richtlinien zu erstellen und durchzusetzen, Anwendungen zu verwalten und Geräte aus der Ferne zu sperren oder zu löschen. Kurz gesagt: Das passende Tool reduziert Komplexität und Kosten, indem es eine konsolidierte Sicht auf alle Endpunkte bietet. IT-Teams sollten außerdem auf einfache Implementierung, intuitive Nutzung und userfreundliche Oberflächen sowie ein umfassendes Schulungsangebot und die konstruktive Verwertung von Feedback zur kontinuierlichen Weiterentwicklung der Lösung achten.

**it security:** *Können Sie uns ein konkretes Beispiel dafür geben, wie*

*MDM die Sicherheitslage von Unternehmen verbessern kann?*

**André Schindler:** Ein konkretes Beispiel ist die Möglichkeit, Richtlinien für mobile Geräte zentral zu erstellen und durchzusetzen. Nehmen wir an, ein Unternehmen möchte sicherstellen, dass alle mobilen Geräte Verschlüsselung aktiviert haben und nur bestimmte, genehmigte Apps installiert sind. Mit professionellen MDM-Lösungen können IT-Administratoren solche Richtlinien konfigurieren und automatisch auf alle verwalteten Geräte anwenden. Wenn ein Smartphone oder Tablet gegen diese Richtlinien verstößt, erhält der Administrator eine Benachrichtigung und kann sofort Maßnahmen ergreifen, wie das Sperren des Geräts oder das Erzwingen der Richtlinieneinhaltung. Diese Features minimieren Sicherheitsrisiken und stellen sicher, dass alle Geräte jederzeit den Unternehmensanforderungen entsprechen und keine unnötigen Einstiegsmöglichkeiten für Angreifer entstehen.

**it security:** *In welchem Zusammenhang stehen MDM und BYOD (Bring Your Own Device)?*

**André Schindler:** BYOD ist inzwischen weit verbreitet und aus Unternehmens- sowie Mitarbeitersicht eine großartige Sache: Kostenreduzierung, Produktivitätssteigerung, maximale Flexibilität, optimale Work-Life-Balance – auf den ersten Blick spricht vieles für diesen Ansatz. Allerdings bringt die Nutzung der eigenen Devices für berufliche Zwecke auch besondere Herausforderungen mit sich. Denn es ist durchaus nachvollziehbar, dass Mitarbeiter nicht sämtliche privaten Informationen mit der IT-Abteilung ihres Arbeitgebers teilen wollen. Wichtig ist daher vor allem eine klare Trennung zwischen persönlichen und geschäftlichen Daten auf denselben Devices. IT-Administratoren müssen heutzutage dazu in der Lage sein, berufliche Anwendungen und Daten sicher zu verwalten und gleichzeitig die Privatsphäre der Mitarbeiter zu respektieren. Mit dem richtigen Tool können sie beispielsweise Unternehmens-Apps remote installieren oder entfernen und sicherstellen, dass geschäftliche Daten verschlüsselt sind, ohne auf persönliche Informationen zuzugreifen.

**it security:** *Wie bewerten Sie Mobile Device Management aus der Business-Perspektive?*

**André Schindler:** Der geschäftliche Nutzen von MDM ist erheblich. Die professionelle Verwaltung sämtlicher mobiler Devices sorgt für Konsistenz und Effizienz durch standardisierte Praktiken und Prozesse. Die einfache Bereitstellung und Verwaltung von Apps, die Erstellung und Durchsetzung von Richtlinien und die verbesserte Sicherheitslage sind in letzter Konsequenz wettbewerbskritische Aspekte. Denn sie führen zu einer größeren Produktivität und Zufriedenheit der Endnutzer: Probleme werden schneller gelöst und die Geräte optimal konfiguriert. MDM bildet das Fundament für kontinuierliche Business-Erfolge.

**it security:** *Dazu muss allerdings die Integration in bestehende IT-Umgebungen und -Prozesse optimal gelingen, richtig?*

**André Schindler:** Das stimmt. Die richtige MDM-Lösung muss sich nahtlos in bestehende IT-Umgebungen und -Prozesse integrieren lassen, um die Komplexität zu reduzieren und nicht stattdessen zusätzlichen Aufwand zu produzieren. Außerdem unterstützen professionelle Tools eine breite Palette von Geräten und Betriebssystemen, einschließlich Windows, macOS, Linux, Android und iOS. IT-Administratoren können die gewählte MDM-Lösung idealerweise unkompliziert in ihre be-

stehende Infrastruktur integrieren und ihre vorhandenen Tools und Prozesse weiter nutzen. APIs und Integrationen mit gängigen IT-Management-Tools sorgen für eine reibungslose Implementierung und Nutzung.

**it security:** *Welche Rolle spielt Automatisierung in Zusammenhang mit MDM und wie profitieren Unternehmen davon?*

**André Schindler:** Automatisierung ist ein zentraler Bestandteil zahlreicher IT-Bereiche und kann auch im MDM-Umfeld deutliche Vorteile bringen: Sie ermöglicht es IT-Teams, wiederkehrende Aufgaben zu minimieren und sich auf strategischere Initiativen zu konzentrieren. Beispielsweise können Administratoren automatische Updates und Patches für alle verwalteten Geräte planen und durchführen, ohne manuell eingreifen zu müssen. Dies stellt sicher, dass alle Geräte stets auf dem neuesten Stand und vor bekannten Sicherheitslücken geschützt sind. Außerdem können Verantwortliche automatisierte Workflows erstellen, um neue Geräte automatisch zu registrieren, zu konfigurieren und betriebsbereit zu machen. Diese Automatisierung verbessert die Effizienz, reduziert die Wahrscheinlichkeit menschlicher Fehler und entlastet die ohnehin stark gefragten IT-Teams. Das Ergebnis: mehr Sicherheit, steigende Produktivität und zufriedene Mitarbeiter.

**it security:** *Wie kann MDM mit den besonderen Herausforderungen in stark regulierten Branchen umgehen?*

**André Schindler:** In stark regulierten Branchen wie dem Gesundheitswesen oder dem Finanzsektor sind die Anforderungen an die Datensicherheit und Compliance besonders hoch. Wichtig ist hier die Auswahl eines MDM-Tools, das umfangreiche Funktionen zur Einhaltung regulatorischer Anforderungen bietet. Dazu gehören die Möglichkeit, detaillierte Sicherheitsrichtlinien zu erstellen, die Einhaltung dieser Richtlinien zu überwachen und bei Bedarf Maßnahmen zu ergreifen. Außerdem brauchen solche Organisationen häufig Audits und Berichte, die nachweisen, dass alle Geräte und Prozesse den regulatorischen Vorgaben entsprechen. Auch diese können professionelle Lösungen relativ einfach bereitstellen. Durch die Kombination von fortschrittlichen Sicherheitsfunktionen und umfassenden Compliance-Tools können Unternehmen in stark regulierten Branchen ihre mobilen Geräte effektiv und sicher verwalten.

**it security:** *Zum Abschluss noch ein Blick in die Glaskugel: Welche Trends sehen Sie in der Zukunft des Mobile Device Managements?*

**André Schindler:** Wir beobachten einen klaren Trend zur Konsolidierung der Technologiestacks. IT-Organisationen streben danach, Komplexität zu reduzieren und effizienter zu arbeiten, indem sie weniger Tools verwenden, aber mehr Funktionen abdecken. Zudem wird die Rolle der mobilen Sicherheit immer wichtiger, da mobile Geräte zunehmend im Fokus von Cyberangriffen stehen. Mit zentralen Plattformlösungen sind Unternehmen besser gerüstet, um diese Herausforderungen zu meistern und gleichzeitig die Produktivität und Zufriedenheit ihrer Mitarbeiter zu steigern.

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


# PRAXISHANDBUCH KI-VO

## KÜNSTLICHE INTELLIGENZ RECHTSKONFORM IM PRIVATEN UND ÖFFENTLICHEN BEREICH EINSETZEN

Von Expertinnen für Praktiker – mit diesem Handbuch erhalten Sie einen fundierten Überblick über die europäische KI-Verordnung und ihre Auswirkungen auf die verschiedenen Anwendungsbereiche künstlicher Intelligenz im privaten und öffentlichen Sektor.

Beginnend mit einer kurzen Einführung in die Geschichte und Technik von KI, beleuchtet das zweite Kapitel detailliert den Inhalt der KI-Verordnung anhand der verschiedenen Risikoklassen. Daran anschließend werden mit dem Einsatz von KI eng verbundene Rechtsgebiete, insbesondere Datenschutz-, IP- und IT-Recht, eingehend behandelt.

Darüber hinaus behandeln die Autorinnen auch die Auswirkungen der KI-Verordnung auf verschiedene Industrien wie etwa Mobilität, Arbeit, kritische Infrastruktur, Medizin etc. anhand von Fallbeispielen bzw. die Wechselwirkung mit den für diese Bereiche relevanten Rechtsgebieten.



**Praxishandbuch KI-VO**
Künstliche Intelligenz rechtskonform im privaten und öffentlichen Bereich einsetzen;
Natascha Windholz;
Carl Hanser Verlag GmbH & Co.KG; 11-2024

Ein Praxisüberblick über das Thema AI Governance Risk Compliance in Unternehmen, Tipps zur Anwendung von Richtlinien und Governance-Rahmenwerken, Umsetzungsideen für eine vertrauenswürdige KI sowie Standards, Normen und Zertifizierungen runden das Werk ab.

Nutzen Sie dieses Handbuch, um sich umfassend zu informieren und aktiv mit den Herausforderungen und Chancen der europäischen KI-Verordnung auseinanderzusetzen.

Das Autorinnenteam besteht aus Juristinnen, die auf IT- und Datenschutzrecht und den Einsatz von KI spezialisiert sind. Es besteht u.a. aus der Vertreterin Österreichs bei den KI-Gesetzesverhandlungen auf EU-Ratsebene und der Gründerin der österreichischen Sektion von Women in AI.

# DriveLock Hypersecure Platform

## GANZHEITLICHE IT-SICHERHEIT FÜR UNTERNEHMEN

In unserer dynamischen, digitalen Welt wird IT-Sicherheit zunehmend komplexer. Unternehmen müssen mit begrenzten finanziellen und personellen Ressourcen den steigenden Sicherheitsanforderungen gerecht werden. Fragmentierte und isolierte Technologieumgebungen stellen dabei häufig erhebliche Hindernisse dar.

**Die Komplexität der IT-Sicherheit bewältigen**

Cyberkriminelle nutzen zunehmend raffinierte Methoden - von Ransomware über gezielte Phishing-Angriffe, Sicherheitslücken bis hin zu staatlich unterstützten Cyberangriffen. Diese Bedrohungen werden durch den Einsatz von Künstlicher Intelligenz (KI) verstärkt, was die Angriffe noch gefährlicher und schwerer erkennbar macht.

Um sich vor der Vielfalt an Bedrohungen zu schützen, kommt häufig auch eine Vielzahl an Sicherheitslösungen zum Einsatz. Der Einsatz dieser Lösungen ist aber oft fragmentiert und nicht optimal aufeinander abgestimmt, was zu ineffizienten Prozessen und Sicherheitsrisiken führt.

**Der Nutzen einer Plattformlösung**

Moderne Endpoint-Security-Lösungen erfordern mehrere, integrierte Technologien, um die Wirksamkeit des Bedrohungsschutzes zu verbessern. Angesichts dieser An- und Herausforderungen macht es Sinn, auf eine Plattformlösung zu setzen, die darauf abzielt, die IT-Sicherheit von Unternehmen ganzheitlich zu verbessern und deren Bedienung und Verwaltung zu vereinfachen. Eine Plattform integriert mehrere Module, die reibungslos zusammenarbeiten und umfassende Endgeräte-Sicherheit gewährleisten. Dies erhöht nicht nur den Schutz vor Attacken, sondern erleichtert IT-Administratoren auch die Verwaltung der Security-Lösungen.

**Eine Plattformlösung bietet folgende Vorteile:**

**#1 Integration und Synergie:**
Eine konsolidierte Plattform, wie die DriveLock Hypersecure Platform, integriert verschiedene Sicherheitsmodule. Dies minimiert die Notwendigkeit, mehrere, isolierte Lösungen zu verwalten, die oft nicht optimal aufeinander abgestimmt sind. Die Synergien zwischen den verschiedenen Komponenten sorgen für eine ganzheitliche Sicherheitsstrategie.

**#2 Einfache Verwaltung:**
Durch eine zentrale Verwaltungskonsole können IT-Admins alle Sicherheitsmodule effizient und übersichtlich steuern. Dies spart Zeit und reduziert die Komplexität, die oft mit der Verwaltung isolierter Lösungen einhergeht.

**#3 Cloud-Betrieb und Outsourcing:**
Die Nutzung einer Cloud-basierten Plattform ermöglicht eine schnelle Bereitstellung und Aktualisierung der Sicherheitslösungen ohne hohe Investitionskosten. Zudem besteht die Möglichkeit, das Management der Sicherheitslösungen an einen externen Dienstleister auszulagern, was die internen Ressourcen entsprechend entlastet.

**#4 Kompatibilität und Zertifizierungen:**
Sicherheitslösungen, die nach anerkannten internationalen Standards zertifiziert sind, bieten ein hohes Maß an Vertrauen. DriveLock beispielsweise stellt sicher, dass seine Lösungen frei von Backdoors sind und den höchsten Sicherheitsstandards entsprechen.

**Best-of-Breed Lösungen aus Deutschland und Europa**

Besonders attraktiv sind Plattformlösungen, die aus Deutschland oder Europa stammen, um die digitale Souveränität und die Einhaltung lokaler Sicherheitsstandards sicherzustellen.

DriveLock verfolgt die Vision, deutsche und europäische Best-of-Breed-Hersteller zu integrieren, um eine gemeinsame europäische Cybersicherheitslösung zu

schaffen. Diese Plattform und ihre Komponenten sollen höchsten Sicherheitsanforderungen entsprechen und die Souveränität des europäischen IT-Marktes stärken.

Ein Beispiel für die Integration von europäischen Best-of-Breed-Lösungen in die DriveLock Hypersecure Platform ist das neue Modul „Human Risk & Awareness". Dieses Modul analysiert das Sicherheitsbewusstsein der Mitarbeitenden, identifiziert gefährdete Geschäftsbereiche, Rollen oder Teams und stärkt diese mit Hilfe gezielter, individueller Schulungsprogramme.

Die Grundvoraussetzungen für Partnerunternehmen und -technologien, um in die Hypersecure Platform aufgenommen zu werden, sind streng. DriveLock arbeitet nur mit Partnern zusammen, deren Lösungen in Deutschland oder Europa qualitätsgeprüft sind und die entsprechenden regulatorischen Anforderungen erfüllen.

**Einfache Verwaltung und schnelle Verfügbarkeit**

Ein zentraler Vorteil ist die einfache und transparente Verwaltung über eine zentrale Konsole, mit der Kunden ein umfassendes Portfolio an leistungsstarken Sicherheitsösungen effizient managen können. Die Cloud-basierte Plattform ermöglicht die schnelle Verfügbarkeit der Komponenten ohne hohe Investitions- oder Betriebskosten.

**Made in Germany: Zertifizierungen und Auszeichnungen**

DriveLock-Lösungen werden in Deutschland entwickelt und zeichnen sich durch hohe Qualitäts- und Sicherheitsstandards aus. Diesen Qualitätsanspruch unterstreicht die Zertifizierung von Entwicklung, Support und Betrieb der On-Premises- sowie der Cloud-basierten Plattform nach ISO/IEC27001:2022. Darüber hinaus sind die DriveLock-Lösungen Application Control und Device Control nach Common Criteria EAL3+ zertifiziert.

DRIVELOCK VERFOLGT DIE VISION, DEUTSCHE UND EUROPÄISCHE BEST-OF-BREED-HERSTELLER ZU INTEGRIEREN, UM EINE GEMEINSAME EUROPÄISCHE CYBER-SICHERHEITSLÖSUNG ZU SCHAFFEN.

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

Bereits zum 5. Mal in Folge wurde das Unternehmen in der Marktuntersuchung ISG Provider Lens ™ „Cyber Security – Solutions & Services Germany 2024" als ein Leader im Segment „Data Leakage/Loss Prevention" ausgezeichnet.

**Welche Elemente sind Bestandteil der Hypersecure Platform?**

Viele Security-Lösungen zielen darauf ab, kriminelle Machenschaften innerhalb von IT-Systemen zu bekämpfen und einzudämmen. Ziel der Hypersecure Platform ist es, diese Angriffe gar nicht erst so weit eindringen zu lassen, sondern sie aktiv zu verhindern. Der präventive Ansatz bildet das Herzstück der Plattform und bestimmt ihre Inhalte und Zusammenstellung aus den Elementen:

- **Endpoint Protection:** Schutz der Endgeräte vor Malware, Ransomware und anderen Bedrohungen. Dies beinhaltet Device Control und Application Control, die nach Common Criteria EAL3+ zertifiziert sind.
- **Data Protection:** Verschlüsselung von Daten, um sicherzustellen, dass sensible Informationen auch bei unberechtigtem Zugriff geschützt bleiben.
- **Detection & Response:** Frühzeitige Erkennung und effektive Reaktion auf Sicherheitsvorfälle durch fortschrittliche Analysetools und automatische Maßnahmen.
- **Security Awareness:** Schulungsprogramme, die Mitarbeitende für Sicherheitsrisiken sensibilisieren und sicherstellen, dass sie im Umgang mit potenziellen Bedrohungen richtig reagieren.
- **Cloud-Management:** Zentrale Verwaltung und schnelle Bereitstellung der Sicherheitslösungen über die Cloud, was IT-Admins erhebliche Flexibilität und Effizienz bietet.
- **Zentrales Policy Framework:** Hilft dabei, die Heterogenität aller Endpoints zu homogenisieren und eine einheitliche Sicherheitsstrategie umzusetzen.
- **Zentrales Alerting:** Ermöglicht die schnelle Erkennung von Auffälligkeiten und Anomalien, sodass Bedrohungen sofort adressiert werden können.
- **Flexible Dashboards & Reports:** Bieten Einblicke über den Status der Endgeräte nahezu in Echtzeit. Dies unterstützt das Reporting und den Nachweis im Kontext der Anforderungen verschiedener Sicherheitsrichtlinien.

***Andreas Fuchs***

# Absicherung komplexer E-Mail-Infrastrukturen

## INDIVIDUELLES ROUTING, CONTENT-ANALYSE UND WORKFLOW-AUTOMATISIERUNG

Je mehr Kontrolle Unternehmen über ihren E-Mail-Verkehr haben, desto besser können sie ihre Arbeitsabläufe automatisieren und die Sicherheit ihrer E-Mail-Infrastruktur gewährleisten. Und je früher Regelwerke greifen, desto höher ihre Wirkung. Hierbei unterstützen flexible Cloud-Lösungen. Sie analysieren eingehende E-Mails bereits vor der Zustellung und verarbeiten sie individuell und automatisiert weiter.

Unternehmen mit komplexen E-Mail-Infrastrukturen stehen häufig vor der Herausforderung, große Mengen an Nachrichten effizient verwalten und absichern zu müssen. Denn E-Mails sind nicht nur ein zentraler Bestandteil jedes Arbeitsplatzes, sondern auch vieler geschäftskritischer Prozesse. Um den eingehenden E-Mail-Verkehr im Unternehmen effizient und gemäß eigener Policies zu managen, bieten moderne Cloud-Lösungen klare Vorteile: Sie sind flexibel, skalierbar, wartungsfrei und kostengünstig.

**Automatisierung und intelligentes Routing**

Spezielle Infrastruktur-Services aus der Cloud analysieren, optimieren und leiten E-Mails nach individuellen Regeln weiter, noch bevor sie die Unternehmensinfrastruktur oder den genutzten Cloud-E-Mail-Dienst überhaupt erreichen. Idealerweise geht ein solcher Service über den Funktionsumfang lokaler Regelwerke oder Policy Engines hinaus. So verarbeitet etwa die Predelivery Logic von Retarus E-Mails inhalts-, Adress- und sprachabhängig und routet sie beispielsweise an das richtige Funktionspostfach, den Server der zuständige Landesgesellschaft oder an die richtige Applikation. Darüber hinaus ermöglichen die Regelwerke, E-Mails nach ihrer länderspezifischen Herkunft („Geo IP") zu identifizieren und entsprechende Maßnahmen automatisch einzuleiten. Dies kann etwa sinnvoll sein, wenn Unternehmen vorsorglich alle Nachrichten aus bestimmten Regionen oder Ländern isolieren möchte. Je nach Konfiguration können entsprechende Nachrichten in die Benutzerquarantäne geleitet oder vollständig blockiert werden.

MIT EINER PREDELIVERY LOGIC LASSEN SICH ANHAND INDIVIDUELLER REGELWERKE EINGEHENDE E-MAILS ANALYSIEREN UND WORKFLOWS AUTOMATISIEREN.

**Sören Schulte,**
**Senior Product Marketing Manager Email,**
**Retarus GmbH, www.retarus.de**

**Einheitliche Kommunikation nach Außen**

Auch für den Outbound-Kanal können individuelle Richtlinien festgelegt werden. Bei Ereignissen wie Ausgründungen von Tochtergesellschaften, Fusionen oder Rebrandings können Adressen automatisch auf eine einheitliche Domain umgeschrieben werden – ohne Änderungen an den jeweiligen, eigenständigen Infrastrukturen. Mitarbeiter treten somit nach außen hin ab einem bestimmten Datum nahtlos unter einem einheitlichen Namen auf. In Kombination mit Outbound Security Features lässt sich auch die Reputation und Sicherheit einer einheitlichen Domain in komplexen und heterogenen Infrastrukturen sicherstellen.

**Transparenz, Support und sichere Datenverarbeitung**

Idealerweise stellt der Anbieter den Service über ein webbasiertes Self-Service-Tool bereit, über das sich alle Regeln transparent anlegen, verändern und priorisieren lassen. Es empfiehlt sich auf einen Dienstleister zurückzugreifen, der alle Daten in selbst betriebenen, auditierbaren Rechenzentren innerhalb Europas verarbeitet und branchenspezifische Standards sowie individuelle Compliance-Vorgaben erfüllt. Darüber hinaus sollte den Kunden bei der Umsetzung individueller Regeln für ein effizientes E-Mail Management ein 24/7-Support in der jeweiligen Landessprache jederzeit beratend zur Seite stehen.

***Sören Schulte***

# E-Mail-Sicherheit

## GEMEINSAM STARK ODER EINSEITIG SICHER?

Wie muss man eigentlich seine E-Mails verschlüsseln, damit die Inhalte sicher sind? Dazu gibt es verschiedene Verschlüsselungstechnologien. Die Spontanverschlüsselung beispielsweise ermöglicht es, Nachrichten und Daten ohne vorherige Vereinbarungen oder Schlüsselaustausch verlässlich zu verschlüsseln. Nutzer können so spontan und ohne Absprache geschützt kommunizieren. Spontanverschlüsselung funktioniert dabei einseitig: Ein Teilnehmer kann die Daten verschlüsseln, ohne dass der Empfänger zuvor Maßnahmen ergreifen muss.

Demgegenüber stehen bewährte asymmetrische Verschlüsselungstechnologien wie S/MIME und OpenPGP. Diese Verfahren nutzen ein Schlüsselpaar aus einem öffentlichen und einem privaten Schlüssel, um die Vertraulichkeit und Integrität der Nachrichten zu gewährleisten. Bei S/MIME werden Nachrichten mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und können nur mit dessen privatem Schlüssel entschlüsselt werden. OpenPGP ist ein weiterer Standard für sichere E-Mail-Kommunikation. Es bietet ebenfalls asymmetrische Verschlüsselung, mit einem besonderen Fokus auf Flexibilität und breite Unterstützung durch verschiedene E-Mail-Programme.

Beide Technologien erfordern eine beidseitige Implementierung: Sowohl Sender als auch Empfänger müssen entsprechende Schlüssel generieren und austauschen, um die Verschlüsselung zu nutzen. Die Kombination von Spontanverschlüsselung und etablierten asymmetrischen Verfahren bietet eine robuste Lösung für die Sicherung moderner Kommunikationssysteme. Spontanverschlüsselung ermöglicht schnelle Sicherheitsmaßnahmen, während S/MIME und OpenPGP für langfristige und bewährte Verschlüsselung sorgen.

DIE KOMBINATION VON SPONTANVERSCHLÜSSELUNG UND ETABLIERTEN ASYMMETRISCHEN VERFAHREN BIETET EINE ROBUSTE LÖSUNG FÜR DIE SICHERUNG MODERNER KOMMUNIKATIONSSYSTEME.

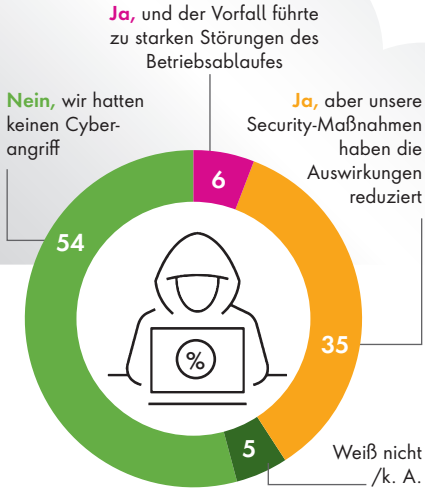
**Günter Esch, Geschäftsführer, SEPPMail AG, www.seppmail.com**

***Günter Esch***

---

# Die Cloud als Schutzschild?

## CYBERANGRIFFE WERDEN MEIST ABGEWEHRT




Basis: Unternehmen, die Cloud-Computing nutzen (n=487)
Quelle: Bitkom Research 2024

Phishing-Mails, DDoS-Angriffe oder Ransomware-Attacken – das ist Alltag für viele Unternehmen. Cloud-Dienste bieten dabei Schutz gegen viele dieser Cyberangriffe.

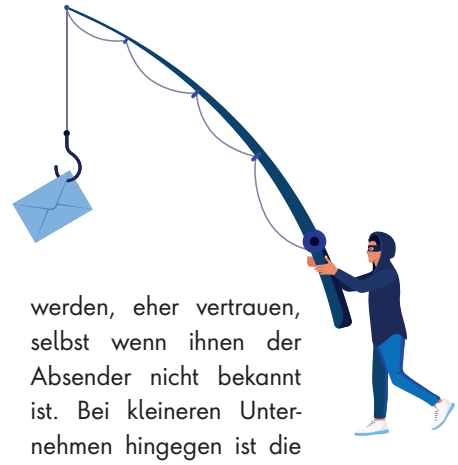
Von jenen 81 Prozent der Unternehmen, die aktuell Cloud Computing nutzen, geben mehr als die Hälfte (54 Prozent) an, dass bei ihnen in den vergangenen zwölf Monaten keine Cyberangriffe auf die Cloud-Umgebung stattgefunden haben. Bei weiteren 35 Prozent hat es zwar Angriffe gegeben, die Security-Maßnahmen haben aber gegriffen und die Auswirkungen reduziert. Nur bei 6 Prozent kam es zu starken Störungen des Betriebsablaufs durch die Angriffe. Das sind Ergebnisse einer repräsentativen Befragung von 603 Unternehmen ab 20 Beschäftigten aus allen Wirtschaftsbereichen in Deutschland im Auftrag des Digitalverbands Bitkom. „Cloud-Anbieter beschäftigen hochspezialisierte Experten, um ihre Dienste zu schützen und immer auf dem neuesten Stand der technologischen Entwicklung zu halten.

Das können viele IT-Abteilungen vor allem in kleineren und mittelständischen Unternehmen nicht leisten“, sagt Lukas Klingholz, Cloud-Experte beim Bitkom. „Die Cloud bietet jedem Unternehmen die Chance, seine IT-Sicherheit auf Top-Niveau zu bringen.“

***www.bitkom.org***

# Laterales Phishing

## BELIEBTE METHODE FÜR E-MAIL-ANGRIFFE AUF GRÖSSERE UNTERNEHMEN



Unternehmen ab mehreren tausend Mitarbeitern sind immer häufiger von lateralem Phishing betroffen, einer Cyber-Angriffsmethode, bei der die Angriffe von einem bereits kompromittierten, internem E-Mail-Konto aus auf weitere E-Mail-Postfächer innerhalb des Unternehmens erfolgen. Wie ein aktuelles Threat Spotlight von Barracuda Networks zeigt, macht laterales Phishing fast die Hälfte (42 Prozent) der gezielten E-Mail-Bedrohungen aus, die auf Unternehmen mit 2.000 oder mehr Mitarbeitende abzielen.

**Externe Phishing-Angriffe gegen die „Kleinen“**

Die Ergebnisse des Threat Spotlights basieren auf einer Analyse der gezielten E-Mail-Angriffe auf Unternehmen zwischen Anfang Juni 2023 und Ende Mai 2024 und zeigen zudem, dass kleinere Unternehmen am ehesten von externen Phishing-Angriffen betroffen sind. In den vergangenen zwölf Monaten betrafen 71 Prozent der gezielten E-Mail-Angriffe Unternehmen dieser Größe, im Vergleich zu 41 Prozent bei den größeren Unternehmen.

Kleinere Unternehmen sind zudem dreimal so häufig von Erpressungsversuchen betroffen als ihre größeren Pendants. Diese machten bei den kleineren Unternehmen sieben Prozent der auf sie abzielenden Angriffe aus, im Vergleich zu nur zwei Prozent bei Unternehmen mit 2.000 oder mehr Mitarbeitern. Die Unternehmensgröße hatte hingegen keine Auswirkung auf die Häufigkeit der Angriffsmethoden Business E-Mail Compromise (BEC) und Conversation Hijacking.

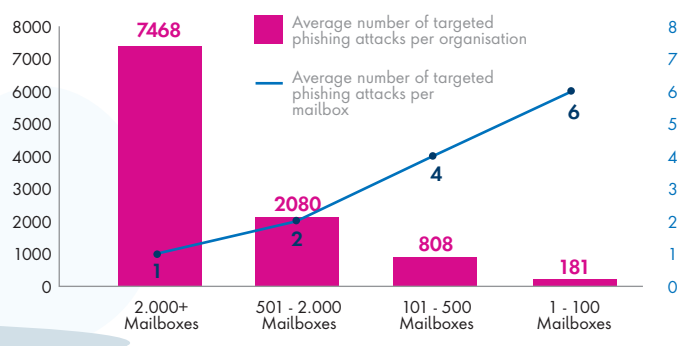
**Jedes Unternehmen gefährdet**

„Alle Unternehmen, unabhängig von ihrer Größe, sind durch E-Mail-basierte Angriffe gefährdet, allerdings auf unterschiedliche Art und Weise“, sagt Olesia Klevchuk, Director Product Marketing bei Barracuda. „Größere Unternehmen mit vielen E-Mail-Postfächern und Mitarbeitenden bieten Angreifern mehr potenzielle Angriffspunkte und Kommunikationskanäle, um schädliche E-Mails im Unternehmen zu verbreiten. Gleichzeitig werden Mitarbeiter E-Mails, die von innerhalb ihres Unternehmens gesendet werden, eher vertrauen, selbst wenn ihnen der Absender nicht bekannt ist. Bei kleineren Unternehmen hingegen ist die Wahrscheinlichkeit geringer, dass sie über mehrschichtige Sicherheitsstrategien verfügen. Zudem ist es wahrscheinlicher, dass kleinere Unternehmen aufgrund von mangelnder interner Expertise und mangelnden Ressourcen falsch konfigurierte E-Mail-Filter einsetzen.“

Barracuda empfiehlt regelmäßige Security Awareness Trainings für Mitarbeitende durchzuführen, die auch laterales Phishing umfassen, damit diese in der Lage sind, entsprechend verdächtige E-Mails zu erkennen. Eine mehrschichtige, KI-gestützte Abwehrstrategie ist der Schlüssel zur Erkennung und Behebung von komplexen Cyberangriffen, um die Folgen dieser Art von Angriffen einzudämmen und zu minimieren. Für kleinere Unternehmen kann es zudem sinnvoll sein, einen Managed Service Provider an Bord zu holen, um zusätzliche Expertise und Unterstützung für die Verbesserung ihrer Cyberabwehr gegen verschiedene Arten von Bedrohungen zur Verfügung zu haben.

***www.barracuda.com***

**VOLUME OF TARGETED PHISHING THREATS AFFECTING ORGANISATIONS** (June 2023 - May 2024)



# it-sa SPEZIAL

**Die it-sa in Nürnberg ist Deutschlands Epizentrum für IT-Sicherheit und steht vor ihrer vielleicht wichtigsten Ausgabe. Nicht nur, weil sich vom 22. - 24. Oktober 2024 hier die Elite der Cybersicherheit trifft, sondern weil regulatorische Umwälzungen wie NIS2 die Branche wachrütteln. In unserem it-sa Spezial diskutieren Experten, wie man die neuen Anforderungen am besten umsetzt. Gleichzeitig präsentieren Aussteller clevere Handkniffe und ihre neuesten technischen Lösungen.**

it sa EXPO CONGRESS

HOME OF IT SECURITY

# KI-basiertes Security Operations Center

## SCHLÜSSEL ZUM SCHUTZ VOR DIGITALEN BEDROHUNGEN


Seit Jahrzenten ist Alexander Sowinski im Bereich Forensik, IT-Security und IT-Beratung unterwegs, seit 2014 ist er Gründer und CEO der ASOFTNET GmbH & Co. KG. Viele Innovationen sind auch an ihm nicht vorbeigegangen, eine von denen beschäftigt ihn gerade sehr: KI. Wie gehen wir in der IT-Security mit dieser neuen Bedrohungslage um, wo sind unsere Chancen? Was ist eigentlich ein KI-Abwehrzentrum? Darüber sprach er mit Carina Mitzschke, Redakteurin it-security.

**Carina Mitzschke:** *Guten Tag Herr Sowinski, vielen Dank, dass Sie sich die Zeit für dieses Interview nehmen. Künstliche Intelligenz hat in den letzten Jahren enorm an Bedeutung gewonnen. Können Sie uns einen Überblick über das Potenzial und die Risiken von KI geben?*

**Alexander Sowinski:** Guten Tag und vielen Dank für die Einladung. Künstliche Intelligenz hat tatsächlich das Potenzial, unsere Welt grundlegend zu verändern. Anwendungen wie ChatGPT zur Textgenerierung oder Dall-E und Midjourney zur Bilderstellung zeigen, wie vielseitig KI eingesetzt werden kann. Doch diese Technologie birgt auch enormes Risikopotenzial. Deepfakes, fraudGPT und die Generierung von Schadcode sind nur einige Beispiele, wie KI missbraucht werden kann. Ähnlich wie Feuer nützlich aber auch gefährlich sein kann, verhält es sich auch mit Künstlicher Intelligenz. Sie ermöglicht es Menschen, ohne tiefgehende Kenntnisse in bestimmten Bereichen wie Poesie, Kunst oder Programmierung tätig zu sein – leider auch im Bereich der Cyberkriminalität.

**Carina Mitzschke:** *Das klingt besorgniserregend. Können Sie uns konkrete Beispiele nennen, wie KI für böswillige Zwecke eingesetzt werden kann oder bereits wird?*

**Alexander Sowinski:** Absolut. Ein klassisches Beispiel sind Phishing-E-Mails. Früher konnte man diese oft an Rechtschreibfehlern erkennen. Mit KI-gestützter Textgenerierung könnten solche E-Mails jedoch nahezu perfekt werden, sodass sie kaum noch von echten E-Mails zu unterscheiden sind. Auch Deepfakes stellen eine erhebliche Gefahr dar. Es reicht schon eine kurze Audioaufnahme, um eine täuschend echte Stimme zu erzeugen. Stellen Sie sich vor, Sie erhalten eine Sprachnachricht von Ihrem Vorgesetzten, die Sie auffordert, umgehend Geld zu überweisen. Diese Nachricht könnte komplett gefälscht sein.

**Carina Mitzschke:** *Wie sieht es mit der Erkennung und Abwehr solcher Angriffe aus? Gibt es effektive Maßnahmen?*

**Alexander Sowinski:** Die Bedrohung durch KI ist tatsächlich enorm und wird weiter zunehmen. Traditionelle Sicherheitsmaßnahmen sind oft nicht ausreichend, um solche fortschrittlichen Angriffe abzuwehren. Deshalb setzen wir auf unser KI-Abwehrzentrum. Wir entwickeln ein Security Operation Center (SOC), das mithilfe von KI sowohl Angriffe erkennt als auch autonom Gegenmaßnahmen einleitet. Unsere KI-Systeme können Angriffsmuster in Echtzeit analysieren und darauf reagieren, schneller und effizienter als es Menschen möglich wäre.

DIE ZUKUNFT DER IT-SICHERHEIT WIRD STARK VON KI GEPRÄGT SEIN.

Alexander Sowinski, Gründer und CEO der ASOFTNET GmbH & Co. KG, https://asoftnet.de/

**Carina Mitzschke:** *Das klingt vielversprechend. Können Sie genauer erläutern, wie Ihr KI-Abwehrzentrum funktioniert und welche Vorteile es bietet?*

**Alexander Sowinski:** Natürlich. Unser KI-Abwehrzentrum nutzt maschinelles Lernen und andere KI-Technologien, um Angriffsmuster zu identifizieren und entsprechende Gegenmaßnahmen zu ergreifen. Wenn ein Vorfall erkannt wird, alarmiert das System unser Incident Response Team, das dann für forensische Analysen oder im schlimmsten Fall für Krisenmanagement bereitsteht. Die KI lernt kontinuierlich dazu, indem sie mit bekannten Angriffsmustern gefüttert wird. So können wir uns auf neue Bedrohungen besser vorbereiten und schneller reagieren. Unser SOC kann somit mehr Angriffe abwehren, als es einem menschlichen Team möglich wäre.

**Carina Mitzschke:** *Das klingt nach einer sehr zukunftsweisenden Lösung. Wie sehen Sie die Zukunft der IT-Sicherheit in Bezug auf KI?*

**Alexander Sowinski:** Die Zukunft der IT-Sicherheit wird stark von KI geprägt sein. Wir müssen uns darauf einstellen, dass KI sowohl als Angriffs- als auch als Verteidigungsmittel eingesetzt wird. Unser Ziel ist es, die positiven Aspekte der KI zu nutzen, um die negativen abzuwehren. Mit dem KI-Abwehrzentrum setzen wir einen wichtigen Schritt in diese Richtung. Unternehmen müssen bereit sein, in solche Technologien zu investieren, um sich gegen die zunehmenden Bedrohungen zu schützen und gleichzeitig die Chancen zu nutzen, die KI bietet.

**Carina Mitzschke:** *Vielen Dank, Herr Sowinski, für diese aufschlussreichen Einblicke. Wir wünschen Ihnen und Ihrem Team viel Erfolg bei Ihrer wichtigen Arbeit.*

# KI UND RECHT

## DER LEITFADEN FÜR RECHTLICHE HERAUSFORDERUNGEN BEIM EINSATZ VON KI-ANWENDUNGEN

Die Nutzung von KI-Anwendungen im beruflichen Alltag bringt zahlreiche Herausforderungen mit, mit denen sich Unternehmen wie Behörden frühzeitig beschäftigen sollten. Das Urheberrecht, das Datenschutzrecht oder auch allgemeine Persönlichkeitsrechte sind betroffen.

In diesem Buch werden die komplexen rechtlichen Fragen, die mit dem Einsatz von künstlicher Intelligenz (KI) einhergehen, umfassend betrachtet. Wem gehört ein KI-Werk? Erlangt ein KI-Werk Schutz nach dem Urheberrecht, wenn es von einem Menschen bearbeitet wird? Verliert das Werk eines Menschen das Urheberrecht, wenn es von der KI bearbeitet wird? Müssen von einer KI generierte Inhalte gekennzeichnet werden? Darf ein Mensch sich als „Urheber" eines KI-Werks ausgeben? Darf eine KI ohne Weiteres frei verfügbare Online-Daten zu Trainingszwecken verwenden? Auf diese und weitere Fragen erhalten Sie Antworten und lernen, wie Sie KI-Tools bei der täglichen Arbeit verantwortlich einsetzen.

**Aus dem Inhalt:**

- Was ist KI und welche rechtlichen Problemfelder gibt es
- KI und Urheberrecht
- KI-Trainingsdaten
- KI und Datenschutzrecht
- KI und allgemeines Persönlichkeitsrecht
- KI-Guidelines
- KI-Regulierung


**KI und Recht:**
Der Leitfaden für rechtliche Herausforderungen beim Einsatz von KI-Anwendungen; Michael Rohrlich; Carl Hanser Verlag GmbH & Co.KG; 11-2024

# Cyber-Verteidigung auf Hochtouren

## VERWERTBARE SICHERHEITSINFORMATIONEN UND ZIELFÜHRENDE ALERTS BESCHLEUNIGEN UND VERBESSERN DIE CYBERABWEHR

Die MITRE Engenuity ATT&CK-Evaluation 2024 bestätigt den MDR-Diensten von Bitdefender gutes Erkennen von Bedrohungen sowie korrelierte und kontextualisierte Informationen zur Cybersicherheit.

Die Qualität der Arbeit von Sicherheitsexperten basiert auf zeitnahen, aussagekräftigen, verwertbaren und relevanten Informationen zu aktuellen Gefahren für das Unternehmensnetz in einer Branche und in einer Region. Die Experten von MITRE Engenuity bewerteten deswegen Managed-Detection-and-Response (MDR)-Dienste verschiedener Hersteller nach Kriterien wie Umsetzbarkeit und Relevanz der Sicherheitsinformationen.

**MITRE-Test**

Für die unabhängige Evaluation nutzten die Tester eine Closed-Book-Emulation mit Taktiken, Techniken und Verfahren (TTPs), die BlackCat/ALPHV - eine aktive Ransomware-as-a-Service (RaaS)-Gruppe - sowie menuPass verwenden. Hinter menuPass stehen auf Spionage fokussierte Cyberkriminelle, die Unternehmen in Gesundheitswesen, Industrie und Produktion sowie Behörden angreifen. In der Simulation konzentrierten sich die Testangreifer auf Netze vermeintlicher Tochtergesellschaften und versuchten, die Abwehr zu umgehen, vertrauenswürdige IT-Konnektivitäten oder Tools auszunutzen, Daten zu verschlüsseln und das Wiederherstellen von Systemen in Windows- und Linux-Umgebungen zu verhindern.

MITRE Engenuity evaluierte auch Bitdefender MDR, einen Managed Security Service, der die IT einer Organisation rund um die Uhr überwacht und auf Gefahren reagiert. Bitdefender MDR bietet Threat Hunting sowie das Knowhow und die Expertise von Sicherheitsexperten in einem globalen Netzwerk miteinander verbundener, voll ausgestatteter Security Operations Center (SOC). Kunden mit begrenzten Ressourcen profitieren von den Forschungen und der Beobachtung der Cybergefahrenlage sowie forensischen und anderen Analysemethoden, die eine hohe Kompetenz und die notwendige Zeit der Experten benötigen.

**Besonders hervorzuheben sind folgende MITRE-Testergebnisse:**

- Höchste Aktionsfähigkeit (Actionability) – Die Actionability bewertet, ob ein Security-Operation-Center (SOC)-Analyst hinreichende Informationen über das Was, Wo, Wann, Wer und Warum des Angriffs erhält, um sofort einschlägige Maßnahmen zu ergreifen. Bitdefender MDR meldete mehr als 95 Prozent der bösartigen Aktivitäten für BlackCat und menuPass. Hinsichtlich der Aktionsfähigkeit bewertete MITRE die Warnungen von Bitdefender MDR 32 Prozent besser als die aller anderen Teilnehmer im Durchschnitt.

- Beste Alarmgenauigkeit (Alert Fidelity) – Bitdefender MDR erzeugte ein geringes Gesamtaufkommen an Nachrichten, welches sich aus der Summe der Alarme in der Konsole und der während der Evaluation generierten E-Mails ergibt. Sowohl für BlackCat als auch für menuPass erzeugte Bitdefender 82 Alerts und E-Mails – deutlich weniger als die Wettbewerber, die sich im Schnitt über 500 Mal an die Nutzer wendeten - einige Anbieter sogar über 1.000 Mal.

- Niedrige Mean Time to Detect (MTTD) – Im Schnitt warnte der Bitdefender-Dienst bereits 24 Minuten nach Einleitung des Angriffs. Die MTTD für alle Teilnehmer lag bei 42 Minuten.

- Wirksamer nativer Technologie-Stack – Ein natives Bündel an Tools ist Eckpfeiler für die gesamte IT-Abwehr eines Unternehmens. Unternehmen integrieren dadurch nahtlos Bedrohungsprävention, Endpoint Detection and Response (EDR) und Extended Detection and Response (XDR) in Managed-Detection-and-Response (MDR)-Dienste, ohne dass kostspielige Add-Ons nötig sind.

***www.bitdefender.de***


# Industrie 4.0-Sicherheit

## SCHLÜSSELBEREICHE MODERNER IT-SCHUTZKONZEPTE

Die diesjährige it-sa fokussiert auf vier Schwerpunkte: Cloud- und Mobile-Security, Daten- und Netzwerksicherheit, Absicherung kritischer Infrastrukturen und Industrie 4.0-Sicherheit. Über die Herausforderungen und Anforderungen von Industrie 4.0 spricht Malte Marquardt, Leiter der Cybersecurity-Strategie EMEA bei Belden.

**it security:** *Was bietet Belden´s macmon NAC für das Thema Daten – und Netzwerksicherheit?*

**Malte Marquardt:** macmon Network Access Control (NAC) von Belden bietet eine umfassende Lösung für Daten- und Netzwerksicherheit und ermöglicht einen sofortigen Netzwerküberblick mit grafischen Berichten und Topologie. IT- und OT-Abteilungen erhalten klare Einblicke in ihr Netzwerk. Durch moderne Authentifizierungsmethoden wird ein Höchstmaß an Sicherheit erreicht. Unbekannte oder unautorisierte Endgeräte werden erkannt und reguliert. Alle Netzwerke lassen sich leicht segmentieren, Bedrohungen isolieren und Sicherheitszonen einrichten.

Unsere Lösung kann in jedem heterogenen Netzwerk installiert werden und bietet Integrationen mit verschiedenen IT- und OT-Sicherheitslösungen. Die Implementierung ist intuitiv und kann innerhalb eines Tages erfolgen. Belden schützt heterogene Netzwerke vor unberechtigtem Zugriff und bietet damit eine solide Grundlage für die Netzwerksicherheit.

**it security:** *Wie sichert Belden´s macmon NAC kritische Infrastrukturen? Auf was muss man achten?*

**Malte Marquardt:** Die Sicherheit von kritischen Infrastrukturen ist mit mehreren Herausforderungen verbunden. Die steigende Komplexität von Sicherheitslösungen stellt eine große Herausforderung dar. Die Auswahl von Insel-Lösungen kann die Verwaltung erschweren und die Effizienz verringern. Daher ist es wichtig, auf die Kompatibilität der ausgewählten Lösungen zu achten. Unternehmen erhalten Transparenz, sichere Authentifizierung und granulare Zugriffskontrolle in kritischen Netzwerken. Die Software bietet umfassende Sicherheit für kritische Infrastrukturen wie Gesundheitswesen, Stadien, Energie, Verkehrs- und Transportwesen, Konsumgüter, Fördertechnik und Automobilfertigung. Sie verhindert Systemausfälle und Produktionsstopps.

**it security:** *Bietet das Unternehmen branchenspezifische Lösungen?*

**Malte Marquardt:** Der große Vorteil liegt darin, dass jede Art von Netzwerk unterstützt wird und die Lösung bestens geeignet ist für alle erdenklichen Branchen und Industrien. Circa ein Drittel unserer Kunden stammen aus dem industriellen Umfeld. Die Lösung hilft, branchenspezifische Regularien im Bereich der Netzwerksicherheit zu erfüllen. Wir bieten eine Lösung, um diese Herausforderungen zu bewältigen. Die Security-Lösung schützt das Netzwerk vor dem Eindringen unerwünschter Geräte, ermöglicht eine genaue Übersicht über alle Geräte im Netzwerk und bietet ein aktuelles IT-Bestandsmanagement. Die zentrale Administration ermöglicht die Verwaltung aller Unternehmensswitche über SNMP, SSH/Telnet und via API. Dadurch können switchportgenaue Regeln erstellt werden, um den Zugang zu gewähren oder zu verweigern. Bei Maschinenverlagerungen oder -umbauten hilft macmon NAC, Endgeräte physisch zu lokalisieren. Dies ist besonders wichtig, wenn Entwickler von Speicherprogrammierbaren Steuerungen (SPS) nach be-

**it-sa Expo&Congress**

Wir freuen uns über Besucher an unserem Stand.
**Halle 9 – 135**

stimmten Geräten fragen, die nicht kommunizieren können.

**it security:** *Wie haben sich die Anforderungen an das Thema Sicherheit für die Industrie 4.0 verändert?*

**Malte Marquardt:** Liegt der Fokus häufig noch auf dem physischen Zutrittsschutz von Fabrikhallen, so wird der Schutz vor Cyberkriminellen bedeutsamer, da bisher getrennte Welten immer stärker zusammenwachsen. Beispiele für solche Berührungspunkte sind Router, Remote Devices und IIoT-Hardware wie Sensoren oder Aktoren.

Zu den besonderen Herausforderungen der OT-Sicherheit gehören die Trennung von maschineninternen Netzwerken und dem IT-Netzwerk, der Fernzugriff und die Verwendung anderer Protokolle als in der klassischen IT. macmon NAC bietet die umfassende Übersicht aller Geräte der Produktion im Netzwerk, Live-Bestandsmanagement, sofortige Alarmierung bei unbekannten Geräten und Einleitung automatischer Gegenmaßnahmen. Mit dem Modul Advanced Security findet die Erfassung des Endgeräte-Betriebssystems und der Domäne und des Namens zur eindeutigeren Identifizierung statt. In Verbindung mit der Netzwerkzugangskontrolle werden diese Informationen zur Erkennung, Abwehr und Lokalisierung von Angriffen genutzt.

Unsere Lösung erlaubt das Definieren einer maßgeschneiderten NAC-Strategie für alle Teile des Netzwerks. So können beispielsweise in Büroumgebungen andere Durchsetzungsstrategien als in Produktionsnetzwerken umgesetzt werden, ohne dass dies erheblichen Mehraufwand bei der Verwaltung mit sich bringt.

**it security:** *Wie können Unternehmen ihre Cybersicherheit kontinuierlich verbessern?*

**Malte Marquardt:** Unternehmen stehen vor der Herausforderung, ihre Sicherheitsmaßnahmen kontinuierlich anzupassen. Neue Technologien bringen viele Vorteile mit sich, erhöhen jedoch das Risiko von Sicherheitsverletzungen. Daher ist es wichtig, eine ganzheitliche Herangehensweise zu wählen, die sowohl technische als auch organisatorische Aspekte berücksichtigt.

Bevor Unternehmen ihre Sicherheitsmaßnahmen anpassen, sollten sie spezifische Risiken identifizieren, die mit den neuen Technologien verbunden sind. Dazu gehören Aspekte wie Datenintegrität, Datenschutz, Zugriffskontrolle und Netzwerksicherheit. Regelmäßige Schulungen für Mitarbeiter sind unerlässlich. Dabei sollten sie für potenzielle Bedrohungen sensibilisiert werden und Best Practices im Umgang mit Technologien vermittelt bekommen. Sicherheitsbewusstsein muss ein integraler Bestandteil der Unternehmenskultur sein.

Unternehmen sollten klare Sicherheitsrichtlinien erstellen, die auf die neuen Technologien zugeschnitten sind. Diese sollten Aspekte wie Passwortverwaltung, Geräteauthentifizierung und sichere Datenübertragung abdecken. Die Einhaltung dieser Richtlinien ist regelmäßig zu überwachen. Sicherheitsaudits sind wichtig, um Schwachstellen zu identifizieren und zu beheben. Unternehmen sollten die Konfiguration von Netzwerken, Firewalls und Zugriffsrechten überprüfen. Die Ergebnisse von Audits sollten in die kontinuierliche Verbesserung der Sicherheitsmaßnahmen einfließen.

Automatisierte Sicherheitslösungen können Bedrohungen in Echtzeit erkennen und darauf reagieren. Unternehmen sollten kontinuierlich Netzwerke, Endpunkte und Anwendungen überwachen. Automatisierung kann die Effizienz erhöhen und menschliche Fehler minimieren.

Die Zusammenarbeit mit Sicherheitsexperten, Beratern und Technologieanbietern ist entscheidend. Externe Expertise kann wertvolle Einblicke bieten und sicherstellen, dass keine blinden Flecken vorhanden sind. Die Anpassung der Sicherheitsmaßnahmen erfordert eine proaktive und vorausschauende Herangehensweise. Indem Unternehmen diese Schritte befolgen, können sie ihre Sicherheit verbessern und gleichzeitig die Vorteile neuer Technologien nutzen.

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

NEUE TECHNOLOGIEN BRINGEN VIELE VORTEILE MIT SICH, ERHÖHEN JEDOCH DAS RISIKO VON SICHERHEITSVERLETZUNGEN.

**Malte Marquardt, Leiter Cybersecurity-Strategie EMEA, Belden, https://de.belden.com/**

THANK YOU

# Hackerangriffe auf Anwendungen und APIs nehmen zu

## „STATE OF THE INTERNET"-BERICHT (SOTI)

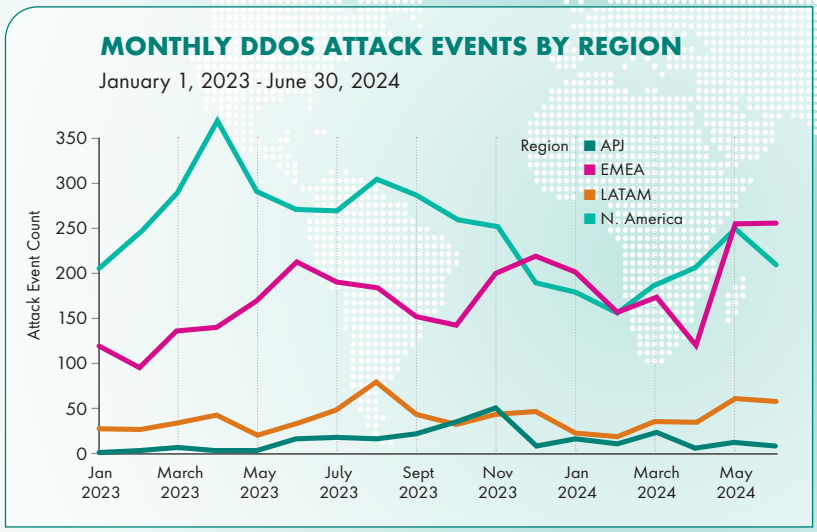
Akamai, Anbieter für Web-, Cloud- und Sicherheitslösungen, beobachtet zwischen dem ersten Quartal 2023 und dem ersten Quartal 2024 einen Anstieg der Webangriffe um 21 Prozent.

Das ist die Erkenntnis aus dem „State of the Internet"-Bericht (SOTI). Aus dem Report „Digitale Festungen unter Beschuss: Bedrohungen für moderne Anwendungsarchitekturen" geht hervor, dass die Zahl der monatlichen Angriffe auf Webanwendungen und APIs in Europa, dem Nahen Osten und Afrika (EMEA) in den ersten sechs Monaten des Jahres 2024 weiterhin erhöht war.

Der Bericht zeigt, dass im Monat durchschnittlich 40 Prozent dieser Webangriffe auf APIs abzielen. Dies ist angesichts der hohen Verbreitung von APIs in EMEA – zum Teil durch gesetzliche Vorgaben bedingt – nicht überraschend.

Zentrale Erkenntnisse aus „Digitale Festungen unter Beschuss: Bedrohungen für moderne Anwendungsarchitekturen" sind Folgende:

- Zwischen dem ersten Quartal 2023 und dem ersten Quartal 2024 war insgesamt ein Anstieg der Webangriffe um 21 Prozent zu beobachten.
- Die drei von Angriffen auf Webanwendungen und APIs am stärksten betroffenen Länder waren das Vereinigte Königreich (20,5 Mrd.), die Niederlande (15,6 Mrd.) und Spanien (12,7 Mrd.).
- Der Handel war die von Webangriffen am häufigsten betroffene Branche in EMEA. Das zeigte sich in einem hohen Prozentsatz von API-Angriffen. Der Handel war außerdem die Branche, in der die meisten DDoS-Angriffe auf Layer 7 stattfanden.
- Die Zahl der Layer-7-DDoS-Angriffe auf APIs blieb relativ stabil und machte 25 Prozent dieser Angriffe aus.
- Innerhalb von EMEA waren Deutschland (461 Mrd.) und das Vereinigte Königreich (366 Mrd.) die Staaten mit der höchsten Anzahl von DDoS-Angriffen auf Layer 7, gefolgt von Schweden (167 Mrd.).




**Geopolitischer Hacktivismus**

Die Anzahl der DDoS-Angriffe auf Layer 3 und 4 stieg in EMEA ebenfalls stetig an und war in fünf der letzten sieben Monate höher als die Anzahl in Nordamerika. Die meisten Attacken (1.523 Ereignisse) richteten sich gegen Ziele im Finanzdienstleistungssektor. Russische Hacktivistengruppen erklärten ihre Absicht, DDoS-Angriffe auf das europäische Bankensystem zu starten. Akamai geht davon aus, dass dieser geopolitische Hacktivismus der Hauptgrund für die Zunahme von DDoS-Angriffen in dieser Branche ist. Am zweithäufigsten angegriffen ist der Sektor Manufacturing mit 890 Angriffen.

„Europa erlebt eine Flut von API-Angriffen. Anwendungen bieten großartige Kommunikationsmöglichkeiten. Sie können aber auch die Achillesferse eines Unternehmens sein, wenn sie nicht effektiv abgeschirmt werden", so Richard Meeus, Director of Security Technology and Strategy, EMEA, bei Akamai. „Die Zunahme von Angriffen auf Webanwendungen und APIs in EMEA unterstreicht, wie wichtig es ist, Netzwerke effektiv zu schützen. Das stellt sicher, dass die erhöhte Angriffsfläche nicht von Cyberkriminellen ausgenutzt werden kann. Angriffe gefährden nicht nur die Umsätze und den Ruf von Unternehmen. Der wirksame Schutz ist auch eine Frage der Einhaltung wichtiger EU-Richtlinien wie NIS2 und DORA."

***www.akamai.com***

# Mehrschichtige Sicherheit

## NETZWERK-, ENDGERÄTE- UND IDENTITÄTSSICHERHEIT IM EINKLANG

Angesichts fortschrittlicher Angriffsszenarien gewährleistet nur ein ganzheitliches IT-Security-Konzept, bei dem Abwehrmechanismen auf verschiedenen Ebenen konsequent zusammenwirken, optimalen Schutz.

Diesen Ansatz verfolgt WatchGuard auf Basis der WatchGuard Cloud. Durch das Zusammenwirken verschiedenster, vielschichtiger Lösungsbausteine kann sich ein Unternehmen gegenüber einer Vielzahl von Bedrohungen wappnen und die von einer einzelnen Schwachstelle ausgehende Gefahr auf ein Minimum reduzieren. Über die Implementierung stichhaltiger Sicherheitsmaßnahmen auf verschiedenen Ebenen lassen sich Netzwerk, Endgeräte, Benutzer und Daten eines Unternehmens effektiv vor Cyberbedrohungen schützen.

**Warum ein mehrschichtiges IT-Sicherheitskonzept?**

Eine einzelne Sicherheitsebene reicht heute mittlerweile schlicht und ergreifend nicht mehr aus, um ein System zu schützen. Hingegen lassen sich mit einer Kombination von mehreren Abwehrmechanismen und Technologien die Abwehrstärke, Zuverlässigkeit und Sicherheitslage der Unternehmenssphäre entscheidend verbessern. Cyberkriminellen wird das Eindringen ins System dadurch deutlich erschwert. Anstatt auf Angriffe am Endpunkt zu warten, geht es um eine ganzheitliche Betrachtung der Cyberabwehr. Dabei werden viele


Kanäle berücksichtigt, über die moderne Malware übertragen wird und die für die Netzwerk-, Endpunkt- und Identitätssicherheit bedeutend sind.

Ziel muss es sein, die Hauptangriffspunkte einer Organisation nachhaltig abzusichern – vom einzelnen Peripheriegerät bis hin zum Unternehmenslogin des Praktikanten. Ob Phishing-Angriffe, Ransomware, Datenschutzverletzungen oder Insider-Bedrohungen: Jede Art von Cyberangriff erfordert eine maßgeschneiderte Abwehrstrategie. Mit vielfältigen und idealerweise ineinandergreifenden Sicherheitsmechanismen können Unternehmen die spezifischen Bedrohungen effizient bekämpfen. Die Vorteile eines mehrschichtigen Ansatzes sind somit schnell auf den Punkt gebracht:

**#1 Ganzheitliche Abwehr:** Ein mehrschichtiger Ansatz bietet eine vollständige Abdeckung durch unterschiedliche Abwehrmechanismen, um jeder Art von Angriff zu begegnen.

**#2 Schutz gegen fortschrittliche Bedrohungen:** Wenn eine Ebene durchbrochen wird, bieten andere Schichten weiterhin Schutz, sodass Zeit bleibt, um den Angriff zu identifizieren, zu isolieren und darauf zu reagieren.

**#3 Anpassungsfähigkeit an zukünftige Bedrohungen:** Eine mehrschichtige Strategie ermöglicht hohe Flexibilität, um neue Sicherheitskontrollen zu integrieren und sich gegen künftige Gefahren und Malware-Technologien zu rüsten.

**Mehr Schutz ohne Mehraufwand**

Durch die Implementierung von Sicherheitsmaßnahmen auf mehreren Ebenen können Unternehmen einen übergreifenden Schutzwall schaffen. Besonderen Mehrwert bei der Umsetzung verspricht dabei der Einsatz einer End-to-End-Sicherheitsplattform, die die umfangreichen IT-Security-Funktionalitäten für Netzwerk-, Endgeräte und Identitätssicherheit in sich vereint. Genau dies bietet WatchGuard Cloud: Durch das passgenaue Zusammenspiel der unterschiedlichen Sicherheitsmechanismen lassen sich gezielt zwei Fliegen mit einer Klappe schlagen: Der Etablierung einer mehrschichtigen Security-Strategie stehen alle Türen offen. Gleichzeitig wird der damit einhergehende Aufwand auf ein Minimum reduziert.

***www.watchguard.de***

**it-sa Expo&Congress**
Besuchen Sie uns in **Halle 7-129**
WatchGuard

# Datenrisiken beim Einsatz von GenAI

## SO LASSEN SIE SICH VERMEIDEN

Viele Mitarbeiter nutzen generative KI im Arbeitsalltag. Damit steigt für Unternehmen das Risiko, dass vertrauliche Daten abfließen oder personenbezogene Daten bei externen Diensten landen. Wie können sie das verhindern, ohne ihre Mitarbeiter zu sehr einzuschränken?

ChatGPT hat auf fast alle Fragen eine Antwort. Kein Wunder, dass viele Mitarbeiter inzwischen oft den Chatbot statt einer Suchmaschine ansteuern, wenn sie Informationsbedarf haben. Sie sparen sich das Durchforsten langer Ergebnislisten und können leicht Anschlussfragen stellen. Außerdem fasst ChatGPT bei Bedarf auch Dokumente zusammen oder übersetzt sie, hilft beim Erstellen von Präsentationen und optimiert Quellcodes.

Neben ChatGPT gibt es noch unzählige weitere GenAI-Dienste, die Bilder und Videos generieren, Texte und Code verbessern oder Websites und Apps erstellen. Microsoft Copilot fungiert gar als persönlicher Assistent, der bei der Vorbereitung auf Besprechungen hilft und diese anschließend zusammenfasst. Darüber hinaus formuliert Copilot auch Antwortvorschläge für E-Mails, zieht die wichtigsten Erkenntnisse aus komplexen Excel-Tabellen, bereitet lange Word-Dokumente übersichtlich auf und liefert gut strukturierte, bereits mit den wesentlichen Informationen gefüllte PowerPoint-Präsentationen.

Allen GenAI-Diensten gemein ist, dass sie Mitarbeitern im Arbeitsalltag viele zeitraubende Tätigkeiten abnehmen und sie produktiver machen. Entsprechend gerne werden sie genutzt, wobei sich die Mitarbeiter häufig kaum Gedanken machen, welche Informationen sie gegenüber den Diensten preisgeben und was mit diesen Informationen geschieht. Geben Mitarbeiter personenbezogene Daten ein, damit die KI ein persönliches Anschreiben verfassen kann, verstößt das gegen Datenschutzgesetze, wenn der Dienst beispielsweise die Daten außerhalb der EU speichert und verarbeitet. Bei den meisten GenAI-Diensten ist das der Fall, da deren Anbieter ihren Sitz in Nordamerika oder Asien haben. Bereits das simple Zusammenfassen oder Übersetzen unbekannter Dokumente ist dann riskant, wenn sie personenbezogene Daten enthalten.

IM GRUNDE VERLIEREN UNTERNEHMEN DIE KONTROLLE ÜBER IHRE SENSIBLEN DATEN, SOBALD DIESE EINMAL BEI KI-DIENSTEN EINGEGEBEN WURDEN.

**Frank Limberger, Data & Insider Threat Security Specialist, Forcepoint**
**www.forcepoint.com**

### Kontrolle über Firmendaten geht verloren

Zudem nutzen die Anbieter der Dienste die Nutzereingaben teilweise, um ihre KI-Modelle zu verfeinern. Enthalten die Eingaben sensible Daten, ist das für Unternehmen ein unkalkulierbares Risiko, denn im Prinzip füttern ihre Mitarbeiter die Algorithmen mit neuem Wissen, das in der einen oder anderen Form in den Ausgaben für die Mitarbeiter anderer Unternehmen auftauchen kann. Wer selbst geschriebenen Quellcode analysieren lässt, muss daher damit rechnen, dass besonders innovative oder effiziente Code-Fragmente anderen Entwicklern als Optimierungsmöglichkeit vorgeschlagen werden. Und wer PDFs mit technischen Konzepten, Präsentationen zu einer anstehenden Firmenübernahme oder vertrauliche Finanzdaten hochlädt, damit KI diese übersetzen oder besser strukturieren kann, darf sich nicht wundern, wenn die Informationen an die Öffentlichkeit gelangen.

Im Grunde verlieren Unternehmen die Kontrolle über ihre sensiblen Daten, sobald diese einmal bei KI-Diensten eingegeben wurden. Selbst wenn die Anbieter die Daten nicht zum Training ihrer KI-Modelle verwenden, könnten sie im Falle eines Cyberangriffs gele-

akt oder für einen Erpressungsversuch missbraucht werden.

**Blocken ist keine Lösung**

Die vermeintlich einfachste Lösung, Datenrisiken im Zusammenhang mit generativer KI zu vermeiden, ist das Sperren der KI-Dienste mit URL- oder DNS-Filtern. Allerdings funktionieren diese Sperren nur innerhalb des Unternehmensnetzwerks, sodass Mitarbeiter sie leicht umgehen können, indem sie aus dem Homeoffice auf die Dienste zugreifen. Zudem ist es angesichts der riesigen und stetig wachsenden Anzahl von Angeboten ein nahezu aussichtsloses Unterfangen, wirklich alle Dienste zu sperren.

Abgesehen davon ist generative KI ein mächtiges Werkzeug. Sie zu blockieren, würde bedeuten, auf eine gesteigerte Produktivität zu verzichten und den Mitarbeitern liebgewonnene Tools wegzunehmen, was für Frust und sinkende Motivation sorgen kann. Besser ist es daher, den Zugang zu den Diensten ähnlich wie den Zugang zu Cloud-Services zu reglementieren, um die enormen Möglichkeiten von GenAI auszuschöpfen, ohne Compliance-Vorgaben zu unterlaufen und die Datensicherheit zu gefährden.

Unternehmen sollten verschiedene KI-Dienste evaluieren, um diejenigen zu ermitteln, die ihnen und ihren Mitarbeitern den größten Nutzen bringen und deren Preis- und Lizenzmodelle am besten zu den eigenen Budgets und Anforderungen passen. Anschließend können sie Richtlinien definieren, welche Dienste zugelassen sind und welche Mitarbeiter auf sie zugreifen dürfen. Sie müssen diese Richtlinien aber auch durchsetzen und dafür sorgen, dass keine sensiblen Daten mit den Diensten geteilt werden.

**DSPM hilft beim Schutz sensibler Daten**

Mit Sicherheitslösungen wie Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA) und Secure Web Gateway (SWG) stellen Unternehmen sicher, dass nur geprüfte und freigegebene KI-Dienste nur von autorisierten Mitarbeitern genutzt werden. Diese können unabhängig davon, ob sie sich im Unternehmensnetzwerk, im Homeoffice oder an anderen Standorten befinden, mit beliebigen Geräten sicher auf die Dienste zugreifen. Lösungen für Data Security wachen dann über die Eingaben und Uploads und verhindern, dass sensible und personenbezogene Daten das Unternehmen verlassen. Bei weniger kritischen Daten genügt auch ein einfacher Warnhinweis, während bei kritischen Daten die Übertragung direkt unterbunden wird.

Die Herausforderung dabei ist, einen Überblick über die eigenen Daten zu erhalten, um schützenswerte Informationen zu identifizieren. Schließlich wachsen die Datenbestände kontinuierlich und sind über eigene Server, das Web, die Cloud und die Endgeräte der teilweise remote arbeitenden Mitarbeiter verteilt. Ein Data Security Posture Management (DSPM) hilft, Daten über alle Speicherorte hinweg aufzuspüren, zu klassifizieren, nach Risiken zu priorisieren und kontinuierlich zu schützen und zu überwachen.

Moderne Lösungen nutzen dafür auch KI: Anhand von Beispielen besonders sensibler Daten, etwa Verträge, Kundenlisten, oder Daten aus Forschung und Entwicklung, die Fachabteilungen bereitstellen, spüren sie automatisiert vergleichbare Daten innerhalb der gesamten Systemlandschaft auf. Sobald diese Daten ganz oder in Teilen über KI-Dienste abzufließen drohen, sorgen die Lösungen dafür, dass die Sicherheitsrichtlinien durchgesetzt werden. Und das selbst dann, wenn die zu schützenden Inhalte sich in einem Screenshot verstecken.

Auf diese Weise ermöglichen Unternehmen nicht nur die sichere Nutzung von generativer KI, sondern legen auch den Grundstein für Zertifizierungen und Testate wie ISO 27001:2022, TISAX, NIS2 und C5, deren hohe Anforderungen an Datensicherheit und Datenschutz sich mit einem DSPM leichter erfüllen lassen.

***Frank Limberger***

# EUROPAS SORGE UM ONLINE-IDENTITÄT

## DIGITALE IDENTITÄT UNTER BESCHUSS

9 von 10 Europäern befürchten digitalen Identitätsdiebstahl und zeigen sich besorgt darüber, wie KI die Sicherheit im Internet verschlechtern kann. Das zeigen die aktuellen Ergebnisse der European Customer Identity Survey 2024 von Okta.

Die Erhebung befragte über 4.000 Verbraucher in Deutschland, Frankreich, Großbritannien und den Niederlanden. Sie ergab, dass 93 Prozent der Befragten besorgt über digitalen Identitätsdiebstahl sind: Während sich in Deutschland immerhin 81 Prozent Sorgen machen, sind es 92 Prozent in Großbritannien, 93 Prozent in den Niederlanden und in Frankreich sogar 95 Prozent.

Mit 54 Prozent hat mehr als die Hälfte der Verbraucher im vergangenen Jahr ihre Aufmerksamkeit auf ihren digitalen Fußabdruck erhöht, wobei zunehmende Cyberangriffe (39 Prozent) und der Aufstieg der KI (28 Prozent) als die häufigsten Gründe hierfür genannt wurden. Darüber hinaus sind die meisten Verbraucher der Meinung, dass KI das Internet unsicherer gemacht hat (56 Prozent) und die Wahrscheinlichkeit von Angriffen auf digitale Identitäten erhöht (59 Prozent).

**Weitere wichtige Ergebnisse**

### #1 Viele betreiben grundlegende Passworthygiene

Jeder zweite Deutsche (50 Prozent) kennt jemanden, dessen persönliche Daten gehackt wurden. Dies könnte das gestiegene Bewusstsein für eine grundlegende Passworthygiene erklären: Die Hälfte der befragten Deutschen (49 Prozent) gab an, für jedes Online-Konto unterschiedliche Passwörter zu verwenden, während nur 11 Prozent dasselbe Passwort für alles nutzen.

### #2 Online-Banking ist Hauptziel

Deutsche Verbraucher betrachten Online-Banking als das Hauptziel für Cyberkriminelle (60 Prozent). Deutlich weniger Sorgen bereiten Identitätsangriffe auf Social Media Accounts und Arbeitsplatzkonten. Nur 7 Prozent der europäischen Verbraucher glauben, dass ihre Social Media-Accounts primäre Ziele für Cyberkriminelle sind, obwohl sie eine Quelle persönlicher Daten sind, und 2 Prozent denken dasselbe über ihre Arbeitsplatzkonten.

### #3 Sicheres Einloggen bleibt für viele ein Problem

Fast drei Viertel (71 Prozent) der Verbraucher wollen ihre Vorgehensweise verbessern, um ihre Online-Identität abzusichern, immerhin 45 Prozent betrachten den Schutz ihrer Online-Identität als persönliche Verantwortung. Mit 26 Prozent ist über ein Viertel der Überzeugung, dass Privatpersonen, die Regierung und Unternehmen gemeinsam für den Schutz der Online-Identität verantwortlich sind.

Europäische Verbraucher stehen jedoch vor einigen gemeinsamen Hindernissen. 72 Prozent berichten über Frustration beim Einloggen in ihre Online-Konten - obwohl die Hälfte (49 Prozent) der Befragten wahrscheinlich mehr Geld ausgeben würde, wenn der Login-Prozess einfach, sicher und reibungslos wäre. 54 Prozent der Deutschen sagen, dass KI die Online-Umgebung unsicherer gemacht hat, ganze 60 Prozent sind sogar der Meinung, dass KI die Wahrscheinlichkeit von Angriffen auf digitale Identitäten erhöht. Gleichzeitig ist jeder zweite Deutsche damit einverstanden, wenn Unternehmen mithilfe von KI das Einloggen schneller, einfacher und sicherer machen.

***www.okta.com***

# Schluss mit dem Versteckspiel

## SICHER DANK DIGITALER E-MAIL-SIGNATUR

Nur weil eine E-Mail von einer bekannten Adresse stammt, heißt das nicht, dass sie nicht manipuliert wurde. Eine digitale E-Mail-Signatur kann das anzeigen und dadurch warnen!

Phishing-Mails sind weit verbreitet. Täglich erreichen E-Mails den Posteingang, die Kontosperrungen androhen oder Anmeldedaten anfragen. Manche dieser Nachrichten lassen sich leicht als Spam erkennen: Andere E-Mails hingegen wirken professioneller und erlangen oft Zugang zu sensiblen Daten. Doch es gibt eine einfache Möglichkeit, sich zu schützen. Hier kommt SEPPmail ins Spiel. Das Unternehmen bietet E-Mail-Verschlüsselung mit digitaler Signatur an. Die Einrichtung ist unkompliziert und erfordert keinerlei Nutzeraufwand

**Authentizität dank digitaler Signatur**

E-Mails müssen nicht gleich verschlüsselt werden, sondern können durch eine einfache Maßnahme sicher gestaltet werden. Ein bewährtes Verfahren ist die digitale Signatur. Dank SEPPmail werden E-Mails digital signiert und dem Empfänger ungebrochen angezeigt, wenn die Nachrichten nicht manipuliert wurden und wirklich von der angegebenen Absenderorganisation stammen. So wird die Authentizität, als auch die Integrität der E-Mails angezeigt.

Für die digitale Signatur kommt ein validiertes Zertifikat zur Verwendung, das von einer akkreditierten Zertifizierungsstelle ausgestellt wird. Die SEPPmail-Appliance automatisiert diesen Prozess. Mit dem Versand der ersten E-Mail starten die erforderlichen Schritte automatisch und alle ausgehenden E-Mails werden fortan signiert.

Schützen Sie Ihre Kunden und Kommunikationspartner vor Phishing und Schadsoftware – mit der digitalen Signatur von SEPPmail! Sagen Sie es weiter!

***www.seppmail.com***

**it-sa Expo&Congress**

Besuchen Sie uns in **Halle 7-131**

SEPPMAIL

# Management digitaler Identitäten

## DIGITALE SOUVERÄNITÄT ALS KÖNIGSDISZIPLIN

Daten sind nicht das neue Öl. Digitale Identitäten sind es. Klügere Gauner haben schon immer Missbrauch mit Identitäten getrieben. Man denke nur an Frank Abagnale aus „Catch Me If You Can" oder – Ältere mögen sich erinnern – den Hauptmann von Köpenick. Analog dazu haben heutige Cyberkriminelle es auf digitale Identitäten abgesehen. Ein unerlaubter Zugriff auf Unternehmenssysteme nimmt seinen Anfang fast immer mit dem Kapern einer digitalen Identität in Folge eines erfolgreichen Cyberangriffs. Einen entsprechend hohen Stellenwert sollten Verwaltung und Sicherung digitaler Identitäten für IT-Verantwortliche in Unternehmen und Behörden einnehmen.

**Effizientes Management**

Um Management und Sicherung digitaler Identitäten diesen hohen Stellenwert einzuräumen, ist ein modernes System zu ihrer Verwaltung notwendig, das eine Reihe Anforderungen erfüllen sollte. Zunächst sollte es eine flexible Nutzerverwaltung gewährleisten, die sowohl die Integration lokaler Verzeichnisse als auch die Anbindung externer Systeme über standardisierte Schnittstellen ermöglicht. Essenziell ist dabei eine zentrale Verwaltungsoberfläche, die einen Gesamtüberblick über alle Nutzer und deren Attribute bietet. Darüber hinaus spielt ein effizientes Berechtigungsmanagement eine entscheidende Rolle. Das System sollte die granulare Steuerung von Zugriffsrechten auf Ressourcen und Anwendungen erlauben und die Möglichkeit bieten, Administratorenrollen zu definieren und Berechtigungen zu delegieren. Nur so lässt sich das Prinzip der minimalst möglichen Berechtigung umsetzen: Jeder Mitarbeiter sollte nur genau die Berechtigungen erhalten, die er oder sie zur Erfüllung von Aufgaben benötigt. Die Automatisierung von wiederkehrenden Aufgaben, wie zum Beispiel Onboarding- und Offboarding-Prozessen, trägt zusätzlich zur Effizienzsteigerung bei.

Besonders wichtig sind umfassende Sicherheitsfunktionen. Dazu gehören die Möglichkeit, individuelle Sicherheitsrichtlinien zu definieren und durchzusetzen, sowie die Unterstützung starker Authentifizierungsmechanismen wie Multi-Faktor-Authentifizierung (MFA). Die revisionssichere Protokollierung aller Aktionen im Zusammenhang mit der Verwaltung von Identitäten und Berechtigungen ist ebenfalls unverzichtbar. Darüber hinaus sollte das System zum Management digitaler Identitäten skalierbar und performant sein, um auch bei einer wachsenden Anzahl von Nutzern, Anwendungen und Daten eine reibungslose Funktion zu gewährleisten. Die Unterstützung offener Standards und Schnittstellen ist entscheidend für die Integration in bestehende IT-Landschaften. Nicht zuletzt spielt die Benutzerfreundlichkeit eine wichtige Rolle, sowohl für Administratoren, die das System verwalten, als auch für Endnutzer.

EIN UNERLAUBTER ZUGRIFF AUF UNTERNEHMENSSYSTEME NIMMT SEINEN ANFANG FAST IMMER MIT DEM KAPERN EINER DIGITALEN IDENTITÄT IN FOLGE EINES ERFOLGREICHEN CYBERANGRIFFS.

**Elmar Eperiesi-Beck, Management – Vertrieb & Strategie, Bare.ID, www.bare.id/de/**

**Die richtige Authentifizierung: Passwort-Manager?**

Ein weiteres wichtige Element zur Verwaltung und Sicherung digitaler Identitäten ist die Identitätskontrolle, sprich Authentifizierung. Dieses Thema ist zu wichtig, als dass man sich dabei auf jeden einzelnen Mitarbeiter verlassen könnte. Nur allzu gerne verwenden diese ihr Geburtsdatum oder eine Zahlenfolge wie „123456" als Passwort. Die Einführung eines Passwort-Managers für die gesamte Belegschaft kann die Sicherheit deutlich erhöhen. Ein Nutzer muss lediglich ein Masterpasswort für die Passwort-Lösung festlegen und kann alle anderen Kennwörter für die verschiedenen Konten und Anwendungen seines beruflichen Alltags sicher generieren lassen. Anschließend kann er sich mit den unterschiedlichen gespeicherten Passwörtern bei all seinen Anwendungen anmelden, ohne sich jedes davon merken zu müssen. So wird eine höhere Passwortsicherheit gewährleistet und der Nutzer profitiert von einem Bequemlichkeitsgewinn.

Trotz eines grundsätzlich steigenden Sicherheitsniveaus durch einzigartige und sichere Passwörter anstelle von unsicheren und geteilten, ist ein einfacher Login über Benutzername und Passwort allerdings nicht für kritische Systeme zu empfehlen. Passwörter, die nicht durch weitere Faktoren im Rahmen einer Multi-Faktor-Authentifizierung (MFA) verstärkt werden, bleiben eine riskante Schwachstelle. Zusätzliche MFA für jeden Login an einer Anwendung führt die Benutzerfreundlichkeit jedoch ad absurdum, die durch Einführung des Pass-

wort-Managers erzielt wurde. Zudem bietet ein einfacher Passwort-Manager dem Unternehmen nicht die nötige Transparenz. Es fehlt die Möglichkeit, das Verhalten der Mitarbeitenden und sicherheitsrelevante Aktivitäten zu überwachen. Zudem bleibt Phishing eine Bedrohung: Verwalten Mitarbeitende ihre Passwörter individuell über den Passwort-Manager, besteht auch weiterhin eine große Gefahr, dass sie auf Phishing-Angriffe hereinfallen.

**Single Sign-On**

SSO-Lösungen bieten gegenüber Passwort-Managern deutliche Vorteile, sind sie doch auf maximale Benutzerfreundlichkeit und Sicherheit ausgelegt. Über eine zentrale Authentisierung erhalten Nutzerinnen und Nutzer Zugriff auf alle Anwendungen, die sie benötigen, ohne sich jeweils einzeln anmelden zu müssen. Weil die Nutzenden nur eine zentral gesteuerte Anmeldung verwenden müssen, um auf mehrere Anwendungen zuzugreifen, können sie eine hochsichere Authentisierung nach vorgegeben Sicherheitskriterien wählen; oder diese sogar gestuft nach Anwendungen, Zeiten, Anwendungsfunktionalitäten etc. nutzen. Mit einer SSO-Lösung können Unternehmen alle Anmeldungen von Mitarbeitenden zentral verwalten und überwachen. Sie können alle nötigen Zugriffsberechtigungen an einer Stelle einrichten, erfassen und ändern. Außerdem übernimmt die IT-Abteilung die Verantwortung für die Zugriffsverwaltung – Mitarbeitende werden entlastet und sind weniger anfällig für Phishing-Versuche, die Passwortänderungen oder ähnliches vortäuschen.

**Ohne MFA keine Sicherheit**

Um größtmögliche Sicherheit zu gewährleisten, gilt es, ein SSO-System mit MFA zu kombinieren. Weil der zweite Faktor bei einem SSO-System lediglich einmal zur Anwendung kommen muss, beeinträchtigt er das Nutzererlebnis nur minimal. Moderne SSO-Lösungen bieten Unternehmen die Auswahl aus einer Vielzahl integrierter Authentifizierungsverfahren, von Einmalpasswörtern (OTP: One-Time Password) bis zu Hardware-Token nach WebAuthN-Standard, innovativen passwortlosen Authentifizierungen sowie modernen Verfahren wie Passkeys. Letztendlich können nur Authentifizierungsverfahren, die den Nutzern Bequemlichkeit und den IT-Verantwortlichen einfaches Management und Kontrolle bieten, mittel- bis langfristig sicher bleiben.

**Digitale Souveränität – Die Königsdisziplin**

Selbst bei Nutzung einer SSO- mit integrierter MFA-Lösung können Unternehmen und Behörden in eine Sackgasse geraten, wenn sie ihre digitale Souveränität verlieren. Der Verlust digitaler Souveränität droht vor allem durch drei Faktoren: Nichteinhaltung gesetzlicher Vorschriften, Anbieterabhängigkeit („Vendor Lock-in") und Ausfallzeiten. Letztere sind besonders bei einem zentralen System wie einer SSO-Lösung nicht akzeptabel.

Nichteinhaltung gesetzlicher Vorschriften droht zum Beispiel bei Speicherung und Verarbeitung sensibler Daten außerhalb der EU. Sie lässt sich am besten vermeiden, indem ein Unternehmen auf Technologie „Made in Europe" setzt und einen Anbieter wählt, der ausschließlich Rechenzentren in Europa nutzt, um seine Dienste zur Verfügung zu stellen. Der Anbieter darf auch nicht aus Ländern stammen, die ein problematisches Datenschutzniveau bieten. So können immer noch in einigen Ländern staatliche Stellen ohne richterlichen Beschluss Zugriff auf Kundendaten fordern und gesetzlich vorschreiben, Hintertüren in die Software einzubauen, die Zugriff auf Kundendaten ermöglichen.

Problematisch dabei: Kundendaten sind die Zugriffsrechte auf sensible Unternehmensanwendungen und diese Zwangs-Hintertüren werden auch von Angreifern genutzt. Dies zeigen die vielen erfolgreichen Angriffe der jüngsten Vergangenheit. Um die Abhängigkeit von einem Anbieter zu vermeiden, sind Open-Source basierte Lösungen die beste Wahl. Open-Source-Lösungen sind zudem durch das „Viele-Augen-Prinzip" inhärent sicherer. Insbesondere hat im Falle von Open-Source nicht ein einzelner Anbieter zum Beispiel Interesse daran, eine entdeckte Sicherheitslücke zu verschweigen, statt sie zu stopfen. Zu guter Letzt sollten Organisationen einen SSO-Anbieter wählen, der Hochverfügbarkeit garantieren kann. Der Anbieter sollte nicht nur seine Dienste im Multi-Nodes-Betrieb mit Georedundanz-Architektur betreiben, sondern auch die gesamte Systemarchitektur auf maximale Systemverfügbarkeit ausgelegt haben.

***Elmar Eperiesi-Beck***

# iShield Key Pro

## FÜR DEN SCHUTZ DIGITALER IDENTITÄTEN


Im schnelllebigen Geschäftsumfeld ist der Schutz digitaler Identitäten und die Implementierung sicherer Arbeitsabläufe entscheidend. Die iShield Key Pro-Serie von Swissbit meistert diese Herausforderungen und bietet stärkste hardwarebasierte Authentifizierung – einfach, sicher und flexibel!

- **Einfach:** Mühelos lässt sich der iShield Key Pro in Ihren Workflow integrieren. Kompatibel mit FIDO2-zertifizierten Websites und Diensten wie Google, Microsoft und vielen mehr, bietet der Token intuitive Anmeldemöglichkeiten per USB und NFC.
- **Sicher:** Der iShield Key Pro schützt effektiv vor Online-Angriffen wie Phishing, Social Engineering und Kontoübernahmen und kann zudem für das Signieren und Verschlüsseln digitaler Dokumente eingesetzt werden.
- **Flexibel:** Der iShield Key Pro bietet flexible Einsatzmöglichkeiten für die passwortlose Zwei-Faktor- (2FA) oder Multi-Faktor-Authentifizierung (MFA). Darüber hinaus lässt er sich für die physische Zugangskontrolle einsetzen und macht ihn so zu einem der vielseitigsten Security Keys auf dem Markt.

**Unvergleichliche Funktionalität**

Der iShield Key Pro geht weit über einen normalen FIDO-Token hinaus. Er bietet dank Personal Identity Verification (PIV) Funktionen zum Signieren und Verschlüsseln von Dokumenten und ist zudem mit älteren Systemen und Technologien kompatibel, einschließlich HOTP (HMAC-basiertes Einmal-Passwort) für Offline-Anwendungen und TOTP (zeitbasiertes Einmal-Passwort). Des Weiteren eignet er sich zur Umsetzung von Sicherheitsrichtlinien wie NIS2, die eine Multi-Faktor-Authentifizierung im Zusammenhang mit IT-Systemen für die Zugangskontrolle vorschreibt.

***www.swissbit.com***

**it-sa Expo&Congress**
Besuchen Sie uns
in **Halle 6-336**
(Unteraussteller bei Allnet)

# Kein Platz für Ermüdungserscheinungen

## GETEILTES WISSEN UND CLEVERE LÖSUNGEN FÜR SECURITY IN KMUS

Mittelständischen und kleineren Unternehmen ist mit ständigen Mahnungen kaum geholfen. Sie benötigen ein smartes Security-Ökosystem, das sich an den Bedürfnissen orientiert.

Den Angaben der Weltbank zufolge tragen mittelständische Unternehmen 90 Prozent des globalen Business mit 50 Prozent der Mitarbeitenden weltweit. Den Cyberschutz dieser Unternehmen zu sichern und sie mit der Fähigkeit auszustatten, den heutigen Risikofaktoren der Cyberwelt zu widerstehen, ist das Gebot der Stunde.

Marktforschungen, darunter beispielsweise der aktuelle Sophos Threat Report: Cybercrime on Main Street unterstreichen diese Notwendigkeit – demnach galten etwa im Jahr 2023 fast 50 Prozent aller von Sophos analysierten Schadsoftware-Fälle diesem Marktsegment.

**Sensibilisierung für reale Bedrohungen**

Unternehmen werden täglich von Nachrichten und Informationen über Cyberrisiken oder aktuelle Fälle überschwemmt – teils mit ausgeprägter technischer Tiefe, was beispielsweise dem Management nur wenig hilft, das benötigte Schutzpotenzial für das eigene Unternehmen einzuschätzen. Im Gegenteil, die permanenten Schreckensszenarien können zu Überforderung und Resignation führen. Bringt doch eh nichts, mag ein Gedanke sein, und wie als KMU standhalten, wenn es doch auch die großen, gut ausgestatteten Unternehmen regelmäßig trifft?!

Die Realität zeigt, dass Cyberkriminalität für Organisationen jeder Größenordnung eine Herausforderung darstellt. Häufig unter dem Radar der Öffentlichkeit trifft sie kleine und mittelgroße Unternehmen jedoch besonders hart. Die Gründe dafür sind erstaunlich trivial: Der Mangel an erfahrenem Sicherheitspersonal, unzureichende Strategien für die Cybersicherheit, geringes Gefahrenbewusstsein und begrenzte Budgets tragen zu dieser Verwundbarkeit bei.

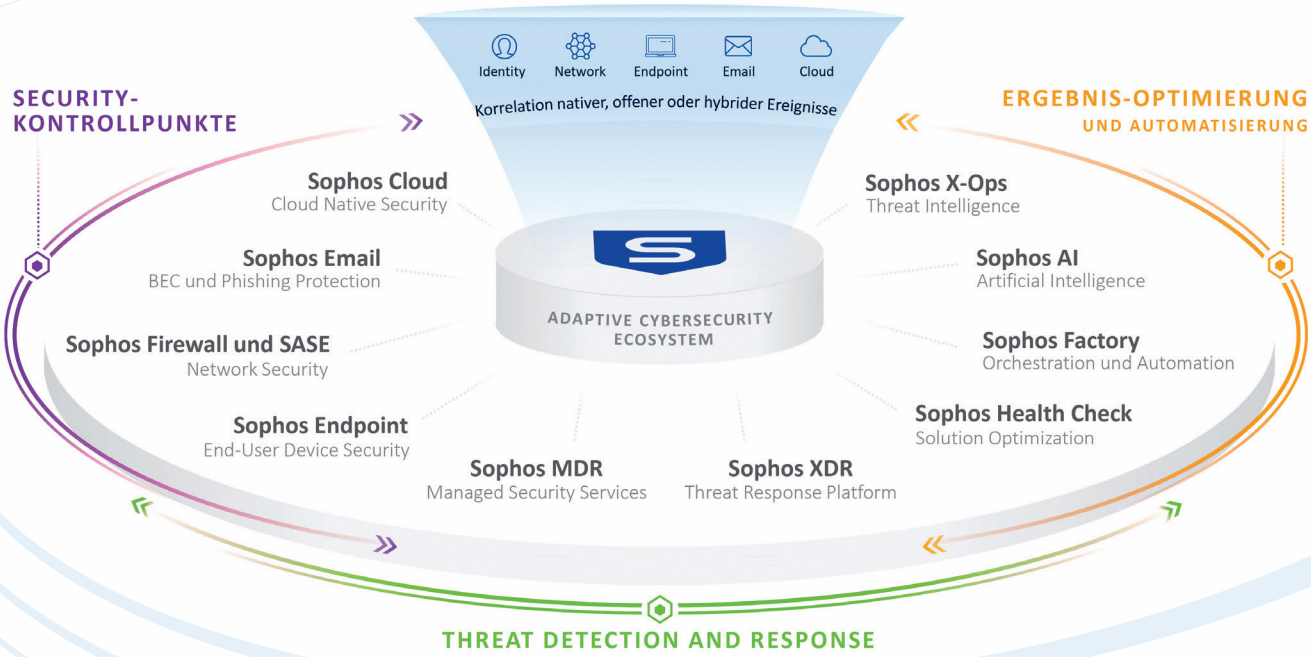
**Information statt Resignation**

Anstatt permanent den mahnenden Zeigefinger zu heben, hilft es kleinen und mittelständischen Unternehmen (KMUs) viel mehr, wenn sie exakte Informationen über die Angriffsvektoren erhalten. Denn nur wer weiß, wer oder was die Bedrohung ist und welche Strategie sich dahinter verbirgt, ist in der Lage, einen wirksamen Schutzschild aufzubauen. In diesem Zusammenhang ist es wichtig zu erwähnen, dass Cyberkriminelle nicht immer den direkten Weg ins Unternehmen suchen, sondern auch vom einem zum anderen Unternehmen schleichen, indem sie die digitalen Geschäftsbeziehungen, sprich die Supply-Chain, ausnutzen.

Für die Cyberkriminellen geht es fast ausschließlich um die Daten. Denn der monetäre Wert von Daten ist unter Cyberkriminellen exponentiell gewachsen. 90 Prozent aller von Sophos im Jahr 2023 untersuchten Cyberangriffe waren Daten- oder Identitätsdiebstähle. Bei fast der Hälfte aller Angriffe auf KMUs kommen Keylogger, Spionagesoftware und sogenannte Stealers, also Schadsoftware zum Stehlen von Daten und Zugangsdaten, zum Einsatz. Der Sophos-Report identifiziert zudem sogenannte IABs (Initial Access Brokers) als hohes Gefahrenpotenzial für KMUs. Hierbei handelt es sich nicht um eine Angriffstechnologie, sondern um Cyberkriminelle, die sich darauf spezialisiert haben, in Computer-Netzwerke einzubrechen. Sie bieten im Dark Web ihre kriminellen Dienstleistungen gezielt für KMU-Netzwerkangriffe an. Sie sind es auch, die die gestohlenen Zugänge an die meistbietende Kundschaft verkaufen.

**Pragmatische Security**

Wer die potenzielle Herausforderung kennt, muss in die Lage versetzt werden, das Problem gezielt anzugehen. In der Security kann das Lösen dieser Aufgabe schnell kompliziert, teuer und ineffektiv werden. Die maßgeblichen Gründe dafür sind die Vielzahl an Anbietern unterschiedlicher Sicherheitslösungen, der Mangel an Fachpersonal sowie Budgetlimits. Dabei müsste im Grunde auch ein KMU dieselbe Security-Infrastruktur wie ein Großunternehmen aufstellen, um sicher zu sein. Sogenannte SOCs (Security Operation Center), wie es




große Konzerne haben, sind jedoch enorm kostspielig und ressourcenintensiv. Warum also nicht einen anderen Weg gehen?

Die Rede ist von einer integrierten Security-Plattform inklusive Security-Dienstleistungen und Services, die das gesamte Spektrum der Abwehr und Forensik abdecken und den Betrieb externen Spezialisten überlassen, die das Business der Cybersicherheit zu ihrer Passion gemacht haben. Die Rede ist von einem Sicherheits-Ökosystem, das alle Facetten der Security, von Endpoints, Server, Mobilgeräte über Public Cloud, Firewall, E-Mails, Wireless, WAF bis hin zu Zero Trust Network Access mit Künstlicher Intelligenz sowie der stetigen Einbeziehung von menschlichen Experten und Expertinnen für das schnelle Handeln unter einem Schutzschirm subsummiert. Es geht auch darum, nicht einzelne Security-Lösungen mühsam zu betreiben und aufeinander abzustimmen, sondern auf eine intelligente Vernetzung mit automatischer Reaktion zu setzen. Ein derartiges Ökosystem ist vergleichsweise einfach von den IT- und Security-Spezialisten im Unternehmen steuerbar, kann aber auch komplett als Service von einem spezialisierten externen Partner betrieben werden.

**Wissen und die Erfahrungen anderer clever nutzen**

Bei der Cybersecurity für KMUs geht es um maximalen Schutz mit möglichst geringem Aufwand. Unternehmen, die beispielsweise das integrierte Sicherheitsökosystem von Sophos im Einsatz haben – die Mehrzahl sind KMUs – bestätigen nach der Transformation ihrer Security, dass der Aufwand für den Betrieb und die Verwaltung der IT-Sicherheit um mindestens 50 Prozent reduziert wurde. Mehr noch, diese Kunden berichten von 85 Prozent weniger Sicherheitsvorfällen und 90 Prozent weniger Zeitaufwand für das Erkennen von Sicherheitsproblemen.

Erreicht haben die Unternehmen dieses Sicherheitsniveau durch das adaptive Cybersecurity Ökosystem, das alle Aspekte der Sicherheit unter einem Dach vereint und sogar offen für die Einbindung von Sicherheitskomponenten Dritter und deren Telemetriedaten ist. Der Vorteil: Die Analyse und der Schutz baut auf einem enorm großen Wissenspool auf. Security-Administratoren können sich dabei nicht nur auf das hohe Schutzniveau und eine zentrale Konsole für die gesamte Sicherheitsinfrastruktur verlassen, sondern auch auf die automatisch inkludierten Schutzmechanismen der speziell entwickelten Künstlichen Intelligenz. Ein weiteres Plus: Sophos stellt nicht nur die Schutztechnologie zur Verfügung, sondern innerhalb seiner Services (Managed Detection und Response – MDR) auch Experten, die anormales Verhalten im Unternehmensnetzwerk, das durch die rein technische Security bis heute meist unentdeckt bleibt, aufspüren und unterbinden.

Das Ziel einer cleveren Security-Strategie muss es sein, Unternehmen wirksam vor den Cyberattacken zu verteidigen, die täglich auf Netzwerke einprasseln. Eine smarte Sicherheitsstrategie und ein integriertes Ökosystem verwehren Cyberkriminellen dabei möglichst von vornherein die Chance, sich überhaupt in eine Organisation einzuschleichen. Schäden wie Datendiebstahl, Verschlüsselung oder Erpressung sollten damit nur noch in die Welt der Schreckens-Schlagzeilen gehören.

***Michael Veit | www.sophos.de***

# CYBER-BEDROHUNGSLAGE ERREICHT NEUEN HÖHEPUNKT

## SO GEHEN DACH-UNTERNEHMEN MIT DER SITUATION UM

Mehr als jede zweite Organisation (52 Prozent) im DACH-Raum war bereits von Cyberangriffen betroffen. 77 Prozent der Sicherheitsexpertinnen und -experten in Deutschland, Österreich und der Schweiz sind der Meinung, dass die Bedrohungslandschaft am kritischsten Punkt der letzten fünf Jahre ist. Das geht aus der SoSafe Studie „Human Risk Review 2024" hervor.

Der Bericht basiert auf den Antworten von mehr als 1.250 Sicherheitsverantwortlichen in Westeuropa sowie auf 3,2 Millionen Datenpunkten der SoSafe-Plattform für Security Awareness und Human Risk Management.

54 Prozent der Befragten schätzen das Risiko, dass Cyberangriffe erhebliche negative Auswirkungen auf ihr Unternehmen haben, als hoch ein. Nur 44 Prozent sind der Auffassung, dass die Cyberangriffe auf den Faktor Mensch zurückzuführen sind, während Forrester prognostiziert, dass 2024 bei 90 Prozent aller Datenschutzverstöße der menschliche Faktor beteiligt sein wird. Außerdem geben 3 von 4 Befragten (75 Prozent) an, dass die Zufriedenheit ihrer Mitarbeitenden eine zentrale Rolle für die Cybersicherheit des Unternehmens spielt.

**Ganzheitliche Ansätze nötig**

„Organisationen sind mit einer herausfordernden Cyber-Bedrohungslage konfrontiert. Cyberkriminelle entwickeln laufend neue Angriffsmethoden, die in den meisten Fällen auf unsere menschlichen Emotionen abzielen. Die aktuelle geopolitische Instabilität schafft neue Angriffsmotive für Kriminelle und staatliche Akteure und resultiert in einer komplexen Lage. Besondere Vorsicht ist durch den Einsatz ausgefeilter, KI-gestützter Tools geboten, Angriffe treten vermehrt in unerwarteter Form auf. Wir dürfen die Größe und das Ausmaß dieser Bedrohungen nicht unterschätzen und müssen die Menschen befähigen, ihnen zu begegnen. Das schaffen wir, indem Organisationen Mitarbeitende als stärkste und vielseitigste Komponente ihrer Sicherheitsstrategien verstehen - und wir ihnen helfen, sie durch ganzheitliche, verhaltensbasierte Ansätze zu aktivieren", so Dr. Niklas Hellemann, Psychologe und CEO von SoSafe.

**DACH-Unternehmen deprioritisieren Cybersicherheit**

Starke technische Sicherheitsmaßnahmen sind zwar unerlässlich, aber sie allein schützen nicht vor den Taktiken moderner Cyberkrimineller. Bereits 87 Prozent der Sicherheitsbeauftragten sehen den Aufbau einer ganzheitlichen Sicherheitskultur im Unternehmen als klare Priorität.

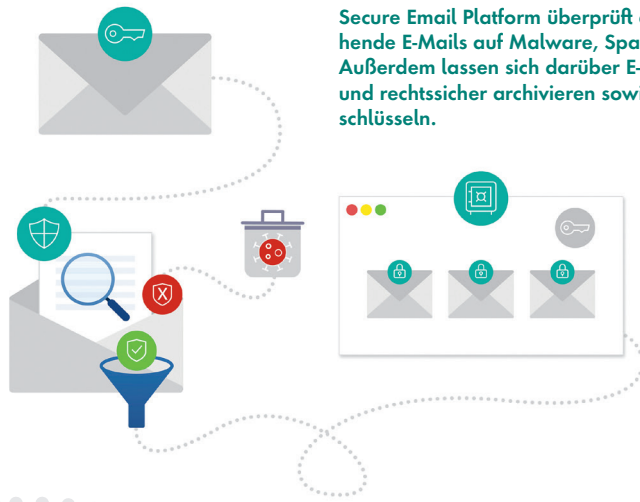
Nahezu alle Unternehmen (99 Prozent der Befragten) gaben an, dass leitende Angestellte und der Vorstand an der Verwaltung und Entscheidungsfindung im Bereich der Cybersicherheit beteiligt sind. Gleichzeitig gaben weniger als die Hälfte der Befragten (43 Prozent) an, dass der Fokus auf Cybersicherheit aufseiten der Geschäftsleitung ansteigt. Zum Vergleich: In Großbritannien sind es 73 Prozent und in Spanien 66 Prozent. Ein Fünftel im DACH-Raum sagte, dass der Fokus nachlässt; bei 10 Prozent der Befragten ist Cybersecurity noch gar keine Unternehmenspriorität.

***www.sosafe-awareness.com***

# Archivierung & Verschlüsselung

## BUSINESS-E-MAILS BESTMÖGLICH ABSICHERN

Laut IT-Branchenverband BITKOM gehen in deutschen Unternehmen täglich durchschnittlich 40 E-Mails pro Postfach ein. Dabei tauschen Mitarbeiter auch häufig sensible Informationen aus. Um vertrauliche Daten vor unbefugtem Zugriff zu schützen, müssen Unternehmen ihre E-Mail-Kommunikation bestmöglich absichern. Hierfür erhalten Unternehmen mit der cloudbasierten Retarus Secure E-Mail Platform alles Notwendige aus einer Hand.



**Alles aus einer Hand: Die cloudbasierte Retarus Secure Email Platform überprüft ein- und ausgehende E-Mails auf Malware, Spam und Phishing. Außerdem lassen sich darüber E-Mails revisions- und rechtssicher archivieren sowie ver- und entschlüsseln.** (Bild: retarus)

**Langzeitaufbewahrung für die Business-Kommunikation**

Geschäftliche E-Mails müssen revisions- und rechtssicher archiviert werden. Gesetzliche Vorgaben wie Aufbewahrungspflichten sind dabei herausfordernd für Unternehmen. Hier kommt das Retarus Email Archive in Spiel. Es speichert automatisch, zuverlässig und rechtskonform den ein- und ausgehenden sowie auf Wunsch auch den internen E-Mail-Verkehr im Original-Raw-Format inklusive SMTP-Informationen. Dabei erfüllt Retarus Email Archive zuverlässig alle internationalen Datenschutzrichtlinien wie die DSGVO, individuelle Branchenstandards sowie Compliance-Richtlinien. Die E-Mails werden in auditierbaren, hochverfügbaren und redundanten Retarus-Rechenzentren in Europa unveränderbar gespeichert und dabei durch eine hybride Verschlüsselung geschützt.

**Sichere Ent- und Verschlüsselung von vertraulicher Kommunikation**

Retarus Email Encryption schützt personenbezogene Daten ebenso wie wertvolles Firmen-Know-how. Die Lösung entschlüsselt eingehende Nachrichten zentral über die Cloud-Plattform, bevor sie im Originalformat im wiederum verschlüsselten Archiv abgelegt werden. Im Gegensatz zu einer Entschlüsselung auf dem Client des Nutzers ist dadurch sichergestellt, dass die Nachrichten auch dann lesbar sind, wenn die jeweiligen privaten Schlüssel zum Zeitpunkt des Zugriffs nicht mehr existieren.

Zusätzlich reduziert die User Synchronization for Encryption (USE) von Retarus den Aufwand für Administratoren deutlich. Mit dieser Funktion lassen sich einzelne Nutzer, Gruppen, Schlüssel/Zertifikate sowie Richtlinien automatisiert verwalten. Der IT-Security-Admin definiert, welche Mitarbeiter oder Gruppen welche Schlüssel und Zertifikate benötigen und wie das individuelle Regelwerk aussehen soll. Anhand dieser kundenspezifischen Regelwerke werden vertrauliche Nachrichten inklusive aller Dateianhänge automatisch verschlüsselt. Dies gelingt bei ausgehenden Mails mit nur einem Klick direkt im E-Mail-Client. Falls der Empfänger keine Verschlüsselung nutzt, kann die E-Mail über ein sicheres Webmail-Postfach zur Abholung bereitgestellt werden.

**E-Mail Rundumschutz aus einer Hand**

Das Retarus Email Archive sowie Retarus Email Encryption sind Teil der cloudbasierten Retarus Email Security Services. Ihre umfassenden Sicherheitsmechanismen überprüfen ein- und ausgehende E-Mails auf Malware, Spam und Phishing. Darüber hinaus umfasst die ganzheitliche Abwehrstrategie die Erkennung und Isolierung unbekannter Bedrohungen durch KI-gestützte Mechanismen und Sandboxing. Zum Funktionsumfang zählt außerdem die patentierte Retarus Patient Zero Detection, die bereits zugestellte Schad-E-Mails anhand eines digitalen Fingerabdrucks identifiziert.

***Sören Schulte | www.retarus.de***

# Das moderne SOC

## WIE EINE KOMBINATION AUS KI UND ERFAHRENEN SICHERHEITSEXPERTEN FÜR BESTMÖGLICHEN SCHUTZ SORGEN

Unternehmen investieren zunehmend in Cyberabwehr und sensibilisieren ihre Mitarbeiterinnen und Mitarbeiter für Cyberbedrohungen – trotzdem kann es immer wieder zu sicherheitsrelevanten Vorfällen kommen. In einem solchen Fall ist es gut, Zugriff auf ein modernes Security Operations Center zu haben, das automatisierte, KI-basierte Bedrohungserkennung mit menschlicher Expertise verbindet.

Die Aufgabe eines SOC besteht darin, Sicherheitsvorfälle rund um die Uhr in Echtzeit zu erkennen, zu analysieren und darauf zu reagieren, um einen proaktiven Schutz gegen Cyberbedrohungen zu gewährleisten. Dafür besteht ein SOC in der Regel aus mehreren erfahrenen Sicherheitsexperten, mit Unterstützung durch eine Reihe an spezialisierten Tools und Prozessen.

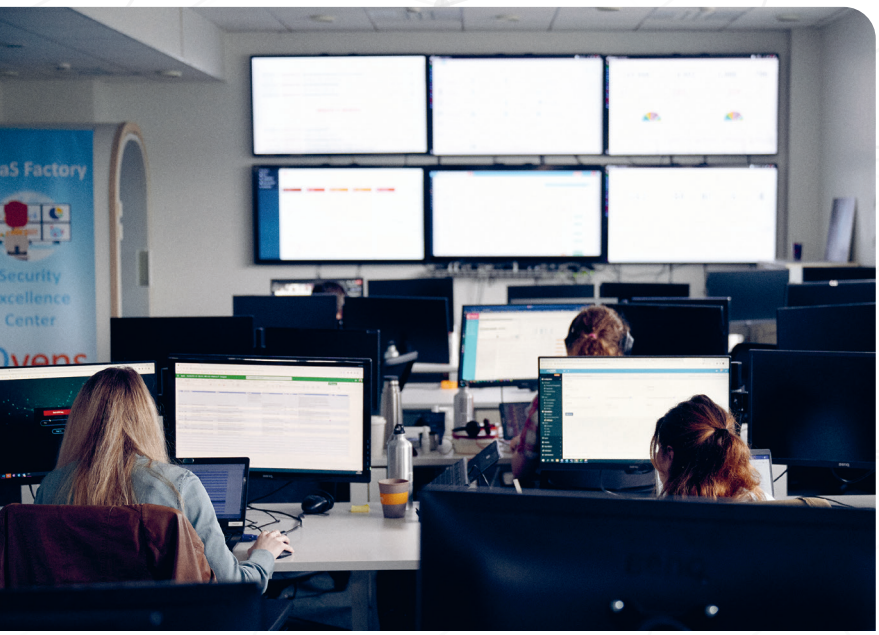
**Die Datenflut im SOC meistern**

Im SOC laufen Informationen aus allen diesen Tools, die Cloud-, Anwendungs- und vernetzte Industrieumgebungen überwachen, im Rahmen eines Big-Data-Prozesses zusammen. Die Summe dieser Rohdaten wird als Security Data Lake (SDL) bezeichnet. Wichtig ist in diesem Zusammenhang, dass der SDL nicht hinsichtlich der Art der Daten, die er aufnehmen kann, beschränkt ist, wie es bei SOCs der älteren Generation, die lediglich auf SIEM (Security Information and Event Management) basieren, der Fall ist. Nur so schafft das SOC ein möglichst vollständiges Bild der Sicherheitslage.

Das Volumen der Daten, die bei modernen SOC-Ansätzen in den SDL fließen, steigt jedoch kontinuierlich, bedingt durch die konstante Weiterentwicklung der Angriffsvektoren. Die Auswertung der Datenmengen, die nachfolgende Priorisierung und die Reaktion auf Vorfälle wird daher für SOC-Teams zu einer immer aufwändigeren und komplexeren Aufgabe. So kann es sein, dass ein SOC-Team pro Woche eine bis zu sechsstellige Anzahl an Alarmen prüft. In vielen Fällen handelt es sich dabei zudem um false-positive Alarme – gerade ältere, SIEM-basierte SOC-Konzepte erzeugen eine große Anzahl dieser.

In der Vergangenheit wurde die Prüfung der Alarme üblicherweise manuell durchgeführt. Dafür stehen im typischen SOC-Modell Level-1-, Level-2-, und Level-3-Analysten zur Verfügung. Jeder dieser Level spielt eine wichtige Rolle bei der Gewährleistung umfassender Cybersicherheit, von der ersten Erfassung von und Reaktion auf Alarme bis hin zu einer eingehenden Analyse und Gestaltung der Cybersicherheitsstrategie.

Die Erfassung von Alarmen wird von Level-1-Analysten durchgeführt, die alle false-positive Alarme aussortieren und nur die tatsächlich sicherheitsrelevanten Ereignisse an die Level-2- und -3-Analysten weiterleiten. Angesichts der bereits erwähnten Masse an Alarmen braucht es dafür jedoch eine große Anzahl an Level-1-Analysten – diese bereitzustel-



**Als zentraler Knotenpunkt überwacht das Security Operations Center (SOC) die gesamte IT-Infrastruktur eines Unternehmens und koordiniert die Reaktion auf potenzielle Sicherheitsvorfälle.**

len ist in Zeiten des Fachkräftemangels oft nicht oder nur mit großem finanziellem Aufwand möglich – und zudem keine effiziente Nutzung der ohnehin schon knappen Ressource des Sicherheitsexperten. Die Lösung liegt hier in der Nutzung von künstlicher Intelligenz (KI) und Machine-Learning-Algorithmen an der richtigen Stelle.

**Automatisierung und Künstliche Intelligenz als „Level-0-Analyst"**

Durch entsprechend trainierte Algorithmen, klassische Metrik und auf Erfahrungswerten aufbauende Automatisierung ist KI in der Lage, selbst die riesigen Datenvolumen, die ein modernes SOC generiert, zu bewältigen. Bestimmte false-positive Alarme kann die KI bereits automatisiert aussortieren. Auf diese Weise müssen die Level-1-Analysten nur die Ereignisse prüfen, die als potenziell sicherheitsrelevant eingestuft wurden – eine signifikante Entlastung und ein Modell, das fast beliebig skalierbar und damit zukunftssicher ist.

Und auch die nachfolgenden Analyseprozesse kann KI unterstützen, beispielsweise indem sie den Analysten Empfehlungen für verschiedene Schritte und Maßnahmen anzeigt, die mithilfe von spezialisierten Large-Language-Modellen generiert werden. Diese werden auf Basis interner Wissensdatenbanken trainiert und kontextuell angereichert.

Konkret bedeutet dies: In der Vergangenheit waren SOCs wie Pyramiden aufgebaut – eine breite Basis an Level-1-Analysten mit wenigen Level-2- und -3-Analysten. Ein moderner, KI-basierter SOC-Ansatz stellt diese Pyramide auf den Kopf – es werden dank KI und Machine Learning weniger Level-1-Analysten benötigt, die dafür in den Level 2 und 3 eingesetzt werden können.

DURCH ENTSPRECHEND TRAINIERTE ALGORITHMEN, KLASSISCHE METRIK UND AUF ERFAHRUNGSWERTEN AUFBAUENDE AUTOMATISIERUNG IST KI IN DER LAGE, SELBST DIE RIESIGEN DATENVOLUMEN, DIE EIN MODERNES SOC GENERIERT, ZU BEWÄLTIGEN.

**Julien Reisdorffer, VP Managed Detection & Response (DACH), aDvens, www.advens.com**

**Die menschliche Note: Was ein gutes SOC-Team ausmacht**

KI stellt im modernen SOC daher nach wie vor nur ein unterstützendes Werkzeug dar. Die Erfahrung der menschlichen Analysten fällt im modernen SOC nicht weg. Sie wird weiterhin gebraucht und lediglich an anderer Stelle effektiver genutzt. Worin besteht aber die entsprechende Expertise und welche Eigenschaften muss ein SOC-Team mitbringen?

Das Offensichtliche zuerst: Ein gutes SOC-Team verfügt über die notwendigen Kompetenzen im Bereich Cybersicherheit. Das heißt, das Team muss einen sicherheitsrelevanten Vorfall erkennen können und wissen, welche Maßnahmen getroffen werden müssen, um die Folgen eines Vorfalls einzudämmen oder zu beheben. Dies erfordert auch entsprechende technische Expertise. Das Team muss in der Lage sein, die im SOC vorhandenen Sicherheitslösungen und -tools korrekt zu konfigurieren, zu verwalten und zu nutzen. Jedes moderne SOC-Team sollte zudem einen oder mehrere Penetration-Tester und Red Teamer zum Purple Teaming umfassen, um Cyberangriffe zu simulieren und so zusätzlich die Effektivität der Methodik und Techniken zur Angriffserkennung zu validieren.

Und nicht zuletzt geht es auch bei SOC-Teams immer öfter um ‚Soft Skills': Die Sicherheitsexperten im SOC werden für Entscheidungsträger im Unternehmen immer öfter zum Berater in allen sicherheitsrelevanten Aspekten.

**Das SOC von morgen: Ein Managed Service**

Letztlich ist für ein modernes SOC das Zusammenspiel von Technologie, Prozessen und Menschen entscheidend. Diese Komponenten bereitzustellen und zu koordinieren ist jedoch eine komplexe Aufgabe, die viele Unternehmen nicht oder nur mit großem finanziellem und personellem Aufwand leisten können.

Im Idealfall sollten also Unternehmen, die die Vorteile eines SOCs nutzen möchten, auf dedizierte SOC-Anbieter setzen. Nicht nur sparen sich Unternehmen auf diese Weise die oftmals hohen, initialen Investitionskosten, die der Aufbau eines SOCs üblicherweise mit sich bringt. Die interne IT-Abteilung kann sich mit einem SOC-as-a-Service-Ansatz zudem wieder vermehrt auf für das Tagesgeschäft relevante Aufgaben konzentrieren – ein echter Wettbewerbsvorteil in Zeiten des IT-Fachkräftemangels.

***Julien Reisdorffer***

# Cyberkriminelle überall

## da tut Hilfe not


Mehr Infos dazu im Printmagazin

itsecurity

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

# Die Balance halten

## ZWISCHEN REGULIERUNG UND LEISTUNGSERWARTUNG


Die Sicherstellung der Cyberresilienz wird zunehmend zu einer anspruchsvollen Gratwanderung zwischen betriebswirtschaftlichen Erwartungen und regulatorischen Anforderungen. In Anbetracht einer immer komplexeren Sicherheitslage ist Cyberresilienz eine unerlässliche Voraussetzung für die Betriebskontinuität sowohl im privaten als auch im öffentlichen Sektor. Diese Herausforderung wird auch vom Gesetzgeber zunehmend in den Fokus gerückt. Mit Regelungen wie DORA, NIS2, dem Cyber Resilience Act und dem EU AI Act stehen europäische Organisationen vor einer Vielzahl neuer Vorschriften im Bereich Cyber- und Datensicherheit. Zusätzlich wird dem Prinzip der digitalen Souveränität Europas, insbesondere seit der CrowdStrike-Panne, auf höchster Ebene verstärkte Aufmerksamkeit geschenkt.

In Ländern wie Deutschland und Frankreich werden die Robustheit und die Konformität von Cybersicherheitslösungen an europäischen Anforderungen durch historische Institutionen zertifiziert, nämlich die ANSSI und das BSI. Beide Ämter bestätigten im Mai dieses Jahres erneut die gegenseitige Anerkennung von Zertifizierungen und Qualifizierungen. Stormshield, ein renommierter europäischer Hersteller von Cybersicherheitslösungen, begrüßt die Erneuerung dieser Zusammenarbeit als einen möglichen Schritt in Richtung einer europäischen Harmonisierung. Die Zuverlässigkeit und die Vertrauenswürdigkeit des Stormshield-Portfolios sind der Dreh- und Angelpunkt der Entwicklungsarbeit des in Frankreich ansässigen Unternehmens.

Stormshields Lösungen sind ein integraler Bestandteil eines freiwilligen, kontinuierlichen Qualifikations- und Zertifizierungsprozesses der ANSSI. Sie prüft den gesamten Quellcode der Lösungen, um sicherzustellen, dass keine Hintertüren vorhanden sind, und um die Robustheit des Codes gegen Angriffe zu zertifizieren. Stormshields Lösungen wurden vielfach für ihre Vertrauenswürdigkeit und Leistungsfähigkeit anerkannt, etwa mit Zertifikaten wie Common Criteria EAL3+ und EAL4+, Zertifizierungen der ersten Sicherheitsebene (CSPN) sowie ANSSI-Standardqualifikationen. Auch die Siegel Diffusion Restreinte (DR), NATO Restricted und EU Restricted Classification sowie das Label „Cybersecurity – Made in Europe" bestätigen diese Aspekte.

Auf der ITSA 2024 wird Stormshield seine in die XDR-Plattform nahtlos integrierten Lösungen präsentieren, darunter Stormshield Endpoint Security (SES) und Stormshield Network Security (SNS) sowie die jüngst angekündigten Firewalls der Serien SN-L und SN-XL. Der XDR-Ansatz von Stormshield ermöglicht es CISOs, von nahtlos orchestrierten Sicherheitspolicies und einer höheren Reaktionsfähigkeit bei Vorfällen zu profitieren. Konsolidierte Berichte bieten eine sofortige Sichtbarkeit über Anomalien oder Sicherheitslücken und erhöhen so die Effizienz der Sicherheitsmaßnahmen. Die Absicherung kritischer Infrastrukturen (KRITIS) ist ein besonderer Schwerpunkt des Herstellers: Die Lösungen schützen umfassend und in Echtzeit vor den immer ausgeklügelteren digitalen Bedrohungen für IT- und OT-Umgebungen und eignen sich ideal für Betreiber wesentlicher Dienste in Europa.

Stormshield lädt alle Interessierten herzlich zu den Partnerständen bei Allnet und Sysob auf der ITSA ein. Dort wird der Hersteller Einblicke in die neuesten Entwicklungen der IT-Sicherheit teilen.

***www.stormshield.com***

# NIS2 ist da

## FAHRPLAN ZUR UMSETZUNG DES NEUEN BETRIEBLICHEN CYBERSECURITY MANAGEMENTS

Mit NIS2 kommt gerade für viele neu durch die EU-Cybersicherheitsrichtlinie betroffene Unternehmen die Unsicherheit, wie sie die Anforderungen zeitnah umsetzen können und welche Maßnahmen auch bei zahlenmäßig begrenzten Budgets realisierbar sind. Während Berater allenthalben schon vor den ganz erheblichen Bußgeldern bei Non-Compliance und den fehlenden Umsetzungsfristen warnen, will dieser Beitrag einen Ausblick auf das Risikomanagement nach NIS2 geben – und warum dieses letztlich weniger dramatisch ist, als es so oft dargestellt wird.

**NIS2 macht Cybersicherheit zum digitalen Wirtschaftsschutz**

Als die Europäische Union im Jahr 2016 die erste Netz- und Informationssicherheitsrichtlinie (NIS1) ins Leben rief, war Cybersicherheit als rechtliche Anforderung verstanden vor allem eine Aufgabe der Kritischen Infrastrukturen. Seither jedoch hat sich in Sachen Vernetzung, aber auch Bedrohungslage viel getan. Nicht umsonst wird deshalb der Anwendungsbereich von NIS2 erheblich ausgedehnt – einerseits qualitativ mit Blick auf betroffene Sektoren und Branchen, andererseits quantitativ bezogen auf die Größe der Unternehmen.

Neben neu betroffenen mittelständischen Unternehmen ist dabei ein besonderer Blick auch auf Konzerninfrastrukturen wie Holdings zu werfen, denn bei der Bestimmung der zahlenmäßigen Schwellenwerte werden Konzernverbünde berücksichtigt, die auch verbundene Unternehmen und Partnerunternehmen enthalten können. Besonderheit beim Risikomanagement jedoch: Innerhalb einer solchen Konzerninfrastruktur ist nur diejenige juristische Person zum Cybersecurity-Risikomanagement nach NIS2 verpflichtet, die Tätigkeiten erbringt oder Dienstleistungen anbietet, die qualitativ in den Anwendungsbereich der EU-Richtlinie fallen. Das wiederum bedeutet, dass ein in einer Holding angesiedeltes Unternehmen isoliert betrachtet an sich nicht nach NIS2 verpflichtet wäre, weil es die zahlenmäßigen Schwellenwerte alleine nicht erreicht, jedoch aufgrund der zahlenmäßigen Gesamtbetrachtung der Konzerninfrastruktur vom neuen Cybersecurity Compliance Rahmen betroffen sein kann und deshalb entsprechende Maßnahmen umsetzen muss.

> WEDER EIN BSI NOCH EIN BMI SIND GEGENWÄRTIG IN DER LAGE, EINE ALLGEMEINGÜLTIGE INTERPRETATION DARÜBER ABZUGEBEN, WAS DER NACH NIS 2 GESETZLICH GEFORDERTE STAND DER TECHNIK FÜR DIE VERSCHIEDENEN BRANCHEN UND UNTERNEHMENSGRÖSSEN BEDEUTEN SOLL.
>
> **Prof. Dr. Dennis-Kenji Kipker, cyberintelligence.institute, www.cyberintelligence.institute**

Doch auch über die gesetzlichen Anforderungen hinaus können Unternehmen betroffen sein – wichtigster Anwendungsfall ist die digitale Lieferkette zwischen NIS2-Unternehmen und Dienstleistern, die vertraglich abzusichern ist. Ein praktisches Beispiel ist der Fall, wenn sich verschiedene Gesellschaften IT-Systeme teilen und in diesen Informationsverbund ein Unternehmen einbezogen ist, das NIS2 erfüllen muss. In einem solchen Fall sollten vertragliche Regelungen zur Cybersicherheit als Bestandteil des NIS2-Risikomanagements vorgesehen werden.

**Keine NIS2 Compliance „von der Stange"**

Die allgemeine Unsicherheit, die wir bei der Umsetzung von NIS2 zurzeit erleben, ist ganz normal – und insbesondere auch kein speziell deutsches Phänomen. Und selbst wenn man aktuell bei den für die NIS2-Umsetzung zuständigen Behörden einmal nachfragt und um Konkretisierung bittet, ist die Antwort recht eindeutig: Weder ein BSI noch ein BMI sind gegenwärtig in der Lage, eine allgemeingültige Interpretation darüber abzugeben, was der nach NIS2 gesetzlich geforderte Stand der Technik für die verschiedenen Branchen und Unternehmensgrößen bedeuten soll. Dass eine solche Unsicherheit aber nicht unbedingt schlecht sein muss, wird bei einem Blick in besagte Vorgängerregelung NIS1 deutlich: So wird in Artikel. 14 NIS1 bestimmt, dass von den betroffenen Betreibern geeignete und verhältnismäßige technische und orga-

nisatorische Maßnahmen zu ergreifen sind, um die Risiken für die Sicherheit der Netz- und Informationssysteme zu bewältigen, die sie für ihre Tätigkeiten nutzen. Diese vorgenannten Maßnahmen müssen schlussendlich unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau gewährleisten, das dem bestehenden Risiko angemessen ist. Dieser sogenannte „risikobasierte Ansatz" findet sich ebenfalls in NIS2 wieder.

Hier ist die zentrale Vorschrift der Artikel. 21, der festlegt, dass die durch die Richtlinie betroffenen Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen haben, um die Risiken für die Sicherheit der für den Betrieb bzw. die Diensteerbringung genutzten IT-Systeme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Diensteempfänger oder andere Dienste zu verhindern oder möglichst gering zu halten. Und aus diesen offenen rechtlichen Formulierungen folgt eben auch, dass es keine Schablone für NIS2 Compliance gibt, die man 1:1 über jedes Unternehmen legen könnte. Aus dieser Unschärfe ergeben sich aber gewisse Vorteile, da Unternehmen damit auch selbst darüber entscheiden können, ob und in welcher Tiefe sie bestimmte technisch-organisatorische Maßnahmen zur Cybersicherheit umsetzen wollen.

**Individuelle Risikoanalyse als zentraler Ausgangspunkt**

Auch mit NIS2 wird keine hundertprozentige Cybersicherheit geschuldet, sondern vielmehr das Bemühen um ein angemessenes betriebliches Cybersicherheitsniveau. Das wiederum bedeutet, dass auch Verhältnismäßigkeits- und Wirtschaftlichkeitsgesichtspunkte einer Umsetzung der EU-Richtlinie zugrunde gelegt werden können. Die Angemessenheit der betrieblich zu ergreifenden Maßnahmen muss sich am bestehenden Risiko orientieren und ebenjenes Risiko macht sich an möglichen vergangenen Vorfällen, am status quo der IT-Landschaft des Unternehmens, aber auch an zukünftigen betrieblichen Entwicklungen fest. Relevante Fragen, die sich die Geschäftsleitung stellen sollte, können in diesem Zusammenhang sein:

- Welche Kritikalität besitzt ein Unternehmen? Ist es in der Öffentlichkeit besonders exponiert?
- Inwieweit ist das Unternehmen in seiner Funktion von vernetzten IT-Systemen abhängig?
- Gibt es Risiken aus der digitalen Lieferkette, die zu berücksichtigen sind? Inwieweit ist das Unternehmen abhängig von digitalen Lieferketten, die sich aus Outsourcing und Cloud-Nutzung ergeben können?
- Welche Cybersicherheitsvorfälle hat es in der Vergangenheit gegeben oder ist anzunehmen, dass sich Cyberangriffe in Zukunft häufen werden?
- Was könnten potenzielle Cyberangreifer infolge einer erfolgreichen Kompromittierung des Unternehmens erlangen?

Eine mit der Beantwortung dieser Fragen verbundene Risikoanalyse lässt sich nicht generalisieren oder gar im Sinne eines abstrakten Katalogs an Maßnahmen abschließend beurteilen, sondern ist in ihren Ergebnissen immer von ihrem zugrunde zu legenden Einzelfall abhängig.

**Digitale Resilienz als Konzept**

Auch wenn die Maßstäbe zur Umsetzung von NIS2 nicht als One-Stop-Shop durchführbar sind, so kann man gleich-

wohl einige Grundregeln definieren, die für die Umsetzung nach Durchführung einer Risikoanalyse wichtig sind. Der EU-Rechtsakt zur Cybersicherheit beschreibt in seinem Artikel. 21 nämlich, dass die zu treffenden Maßnahmen auf einem „gefahrenübergreifenden Ansatz" beruhen müssen, der die digitale und physische Sicherheit von IT-Systemen adressiert. Aufgezählt wird in diesem Zusammenhang ein ganzer Katalog an Mindestmaßnahmen, der in seiner Abstraktheit zunächst einmal massiv klingt, aber in seiner Umsetzung eben unter jenes Primat der individuellen Risikoanalyse zu stellen ist. Das wiederum hat zur Folge, dass es in der Praxis durchaus sehr graduelle Abstufungen davon geben kann, was Backup-Management, Krisen- und Notfallpläne, Lieferkettensicherheit, Schwachstellenmanagement, Cyberhygiene, Awareness, Verschlüsselung, Zugriffsmanagement und die Verwendung Authentifizierungstechnologien im Einzelfall bedeutet.

Unter Umständen gar könnten bestimmte der durch den NIS2-Mindestkatalog vorgeschlagenen Maßnahmen zur Cybersicherheit für manche Betriebe nicht einschlägig bzw. infolge betrieblicher Besonderheiten nicht realisierbar sein. Eines aber steht in jedem Falle fest: Zumindest beim Abschluss von Cyberversicherungen sollte man vorsichtig sein und sich im Vorfeld genau überlegen, ob eine solche Police für das konkrete Unternehmen auch Sinn macht, denn allein mit einer Cyberversicherung kommt man der NIS2-Umsetzung keinen Schritt näher, da der Gesetzgeber das Management der technischen Folgen und nicht der bloß mittelbaren wirtschaftlichen Folgen verlangt.

**Nicht verrückt machen lassen**

Feststellen kann man also, dass NIS2 zwar viele Unsicherheiten schafft, aber diese eigentlich vorteilhaft sind, weil sie den betroffenen Unternehmen individuellen Spielraum bei der Umsetzung belassen. Keinesfalls verrückt machen lassen sollte man sich deshalb von Prophezeiungen, dass man zum Start von NIS2UmsuCG in Deutschland von einem Tag auf den anderen „compliant" sein muss und ansonsten mit BSI-Sanktionen zu rechnen hat – dieses Szenario wird nicht sofort eintreten. Zu empfehlen ist aber, schon jetzt das allgemeine betriebliche Risikomanagement auch auf die Cybersicherheit auszudehnen und kompetente Verantwortlichkeiten in der Geschäftsleitung zu schaffen, um die Umsetzung von NIS2 anzustoßen, denn zwangsläufig werden nicht wenige Unternehmen über die digitale Lieferkette „mitverpflichtet" werden. Hilfreich kann es überdies sein, sich ebenso schon jetzt mit den jeweiligen Branchenverbänden in Verbindung zu setzen, soweit vorhanden, um gemeinsam mit weiteren betroffenen Unternehmen individuelle Best Practices zur NIS2-Umsetzung zu entwickeln und zu gestalten sowie Erfahrungen auszutauschen.

***Prof. Dr. Dennis-Kenji Kipker***




**GUT ZU WISSEN**

Prof. Dr. Kipker nimmt an einer **Talkrunde zum Thema NIS2** live auf der it-sa am 23.10. von 12:45 bis 13:00 Uhr teil.

# Gut gewappnet für NIS2

## INDIVIDUELL UNTERSTÜTZT

Ab Herbst wird IT-Sicherheit für das Topmanagement zur Pflicht. Dariush Ansari ist Geschäftsführer des IT-Sicherheitsspezialisten und Managed Security Service Provider Anqa IT-Security in Köln. Er erklärt, was hinter NIS2 steckt und wie Anqa IT-Security Systemhäusern und IT-Verantwortlichen bei der Umsetzung hilft.

**Was ist NIS2?**

NIS2 ist die Überarbeitung der EU-Sicherheitsrichtlinie. Sie soll sicherstellen, dass Unternehmen mit der neuen Generation an Cyberkriminalität Stand halten. Die bisherigen Anforderungen werden deutlich verschärft und auf wesentlich mehr Branchen und Sektoren ausgeweitet.

**Was bedeutet das konkret?**

NIS2 nimmt sowohl IT-Verantwortliche als auch die Chefetagen stark in die Pflicht, besonders in puncto Risikoanalyse und Schutz der Informationssysteme wie Krisen- und Notfallmanagement. Hinzu kommen verschärfte Meldepflichten von IT-Sicherheitsfällen innerhalb von 24 Stunden. Bei Nichteinhaltung können Bußgelder von bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Vorjahresumsatzes drohen.

**Wie kann Anqa IT-Security helfen?**

Um den neuen Anforderungen gerecht zu werden, bieten wir eine fundierte Ist-Analyse an, anhand derer wir Ihren individuellen Bedarf ermitteln. Gibt es Schwachstellen? Wie können wir diese kostengünstig und mit wenig Aufwand schließen? Wir schützen als externer Partner die IT von über 500 Systemhauspartnern und bieten IT-Sicherheitsberatungen, UTM-Firewalls, Security Awareness Trainings und 360°-Betreuungen als 24/7 Managed Service an. Inklusive aller Anforderungen von NIS2 – ohne dass unseren Partnern Aufwand entsteht.

***https://anqa-itsecurity.de/***

**it-sa Expo&Congress**

Besuchen Sie uns in **Halle 7-439**

Anqa IT-Security

# Ist meine Firma von NIS2 betroffen?

## NIS2-CHECK FÜR UNTERNEHMEN

Die Europäische Union hat die Einführung der neuen IT-Sicherheitsrichtlinie NIS2 beschlossen, um die Cyberresilienz wesentlicher und wichtiger Unternehmen in den Mitgliedsstaaten zu stärken. Die neue EU-Richtlinie trat am 16. Januar 2023 in Kraft. Spätestens bis zum 17. Oktober 2024 ist sie ohne Übergangsfristen von den Mitgliedsstaaten in nationales Recht zu überführen. Dann müssen deutlich mehr Unternehmen die Vorgaben erfüllen, als die der Vorgängerrichtlinie NIS1 aus dem Jahr 2016.

Die Herausforderung besteht darin, dass Unternehmen selbst feststellen müssen, ob sie in den Geltungsbereich der NIS2 fallen. TÜvVIT, ein Tochterunternehmen der TÜV NORD GROUP, bietet ab sofort einen Betroffenheitscheck an, der Unternehmen dabei unterstützt, festzustellen, ob sie von den Anforderungen dieser neuen EU-Richtlinie betroffen sind.

NIS2 gilt für Firmen ab 50 Mitarbeitenden und 10 Millionen Euro Umsatz in 18 festgelegten Sektoren. Entscheidend dafür, ob ein Unternehmen von der Richtlinie betroffen ist, sind die beiden Kriterien Unternehmensgröße und Unternehmenssektor.

**Hier den Check machen!**

Darüber hinaus gibt es einige Sonderfälle.

Mit dem Betroffenheits-Check von TÜV IT können Unternehmen prüfen, ob die Anforderungen der NIS2-Richtlinie für sie in Zukunft verpflichtend sind. Der Check enthält Angaben dazu, welche Anforderungen wie und von wem umzusetzen sind.

***www.tuev-nord-group.com***

# Attributdaten haben oder nicht haben

## EIN KOMMENTAR ZUM AKTUELLEN MEDIENHYPE UM DIE WALLET

UM DIE ATTRIBUTDATEN EINER ORGANISATION EFFEKTIV IM RAHMEN EINER DIGITAL IDENTITY-WALLET ZUM EINSATZ BRINGEN ZU KÖNNEN, MUSS DAS DATENMANAGEMENT GUT AUFGESETZT SEIN.

**David Baier,**
**Senior Sales Engineer, Ping Identity**
**www.pingidentity.com**

In diesem Frühjahr wurde die EU-Verordnung eIDAS 2.0 verabschiedet. Eines ihrer Kernziele: die Entwicklung einer verifizierbaren digitalen Identität samt qualifizierter elektronischer Signatur für jeden Bürger Europas – dezentral eingelagert in einem sicheren Wallet-Objekt auf dem Smartphone ihres jeweiligen Besitzers. Bis 2026 haben die europäischen Staaten nun Zeit, je eine nationale Wallet-Lösung zu entwickeln und mit einer derzeit im Entstehen begriffenen European Digital Identity Wallet (EUDIW) kompatibel zu machen. In ganz Europa sollen die digitalen Identitäten dann Gültigkeit haben, sollen Bürger rechtssicher Online-Dienstleistungen von staatlichen Institutionen und privatwirtschaftlichen Unternehmen in Anspruch nehmen können.

Schon lange wird in den Medien intensiv über die vielfältigen Einsatzmöglichkeiten verifizierbarer Attributdaten, rechtssicher aufbewahrt in digitalen Wallets, berichtet – als Ausweis, als Reisepass, oder auch als Bankkarte. Viele weitere Anwendungsfälle sind denkbar. So könnte etwa ein Unternehmen für seine Angestellten Attributdaten bereitstellen, um die Arbeitsstelle zu betreten oder um an Ordnern oder Dateien zu arbeiten.

Das Problem: derzeit dreht sich die diesbezügliche Medienberichterstattung – drehen sich die Fachdiskussionen – im Wesentlichen nur um eines: um die Fortschritte bei der Entwicklung der Wallet-Technologie. Doch auch die vielversprechendste Wallet-Technologie wird nur dann erfolgreich sein, wenn ihre Anwender ihr die entsprechenden Attributdaten ohne größere Probleme zur Verfügung stellen können.

Um die Attributdaten effektiv zum Einsatz bringen zu können, muss das Datenmanagement gut aufgesetzt sein – und zwei Dinge gewährleisten können:

**ERSTENS** Die Struktur des Lagerorts der Attributdaten muss einen einfachen, nahtlosen, Zugriff ermöglichen und

**ZWEITENS** Die Attributdaten müssen so eingepflegt werden, dass sie Nutzern in einer homogenen Qualität zur Verfügung stehen.

Das Problem: In vielen Unternehmen und Behörden wurden und werden Attributdaten immer noch entweder zentral, aber ungepflegt in Datentöpfen oder aber, gepflegt aber dezentral in Datensilos gespeichert. Dies führt dann zwangsläufig zu einem Issuer-Attribut-Problem.

Ein Lösungsansatz: Die Attributdaten müssen umgelagert und aufbereitet werden – in einem Data Pool, einem Data Warehouse oder einem Data Hub. Letztere müssen dann mit Schnittstellen ausgestattet werden, die es externen Identitäts- und Access-Management-Systemen ermöglichen, anzudocken. So können dann Attributdaten von Mitarbeitern aus den unterschiedlichsten Abteilungen, zum Beispiel der HR-Abteilung, der IT-Abteilung oder dem Werkschutz, in den Gesamtprozess einfließen, ohne dass es zu einer Zerstückelung, zur Bildung ‚abteilungsinterner' statt unternehmensinterner Attributdaten und Credentials kommt.

***David Baier***


CONNECT YOUR WALLET

# Krieg der KIs

## CHANCEN MAXIMIEREN, RISIKEN MINIMIEREN

In unserer vernetzten Welt, die immer häufiger Ziel von Hackern wird, sind moderne Technologien der Schlüssel, um Netzwerke und Daten zu schützen. Künstliche Intelligenz (KI) ist nicht nur ein Hype, sondern eine transformative Technologie, die viele Bereiche unseres Lebens durchdringt. Wir hatten die Erfindung der Elektrizität, die Erfindung des Internets und die Ankunft der KI. Eines der Gebiete, in denen KI besonders stark zum Einsatz kommt, ist die Cybersicherheit. Diese Beziehung zwischen KI und Cybersicherheit kann jedoch als zweischneidiges Schwert beschrieben werden. Einerseits bietet KI mächtige Werkzeuge zur Bekämpfung von Cyber Bedrohungen, andererseits kann sie von Cyberkriminellen für bösartige Zwecke missbraucht werden.

TRADITIONELLE ANTI-VIREN-SOFTWARE BASIEREN AUF SIGNATUREN, DIE AKTUALISIERT WERDEN MÜSSEN, UM NEUE MALWARE-VARIANTEN ZU ERKENNEN. KI-GESTÜTZTE SYSTEME HINGEGEN KÖNNEN DURCH VERHALTENS-ANALYSE UND MUSTER-ERKENNUNG AUCH UNBEKANNTE MALWARE IDENTIFIZIEREN.

**Stefan Henke, RVP Cloudflare GmbH**
**www.cloudflare.com**

**KI, eine wertvolle Ressource für Hacker**

Für Hacker ist KI eine Goldmine und sie waren schnell darin die Ressourcen von KI zu Cyberattacken anzuwenden wie bei Automatisierung der Angriffe, die Erkennung und Ausnutzung von Schwachstellen, Täuschung und Manipulation und die Umgehung der Sicherheitsmassnahmen.

**Automatisierte Angriffe**

Angreifer können KI nutzen, um automatisierte Angriffe zu steuern und oft komplexe und koordinierte Angriffe in großem Maßstab durchzuführen. Beispielsweise können KI-gesteuerte Bots Netzwerkschwachstellen schneller und effizienter ausnutzen als menschliche Hacker.

**Erkennung und Ausnutzung von Schwachstellen**

Hacker verwenden KI, um Schwachstellen in Netzwerken und Software zu scannen und zu identifizieren. Ein Angreifer könnte eine KI trainieren, um Sicherheitslücken in Echtzeit zu erkennen und auszunutzen. Dies stellt eine erhebliche Bedrohung dar, da es die Geschwindigkeit und Präzision von Cyberangriffen erhöht.

**Täuschung und Manipulation**

Deepfake auf KI-basierten Technologien können verwendet werden, um täuschend echte E -Mails, Audios und Videos zu erstellen. Damit können Angriffe geführt werden, bei denen vertrauliche Informationen durch Social Engineering und Manipulation von Personen gewonnen werden. Beispielsweise könnten gefälschte Anrufe von Führungskräften erstellt werden, um Mitarbeiter zur Freigabe sensibler Daten zu bewegen, oder noch schlimmer, um Finanztransaktionen anzuordnen.

**Umgehung von Sicherheitsmaßnahmen**

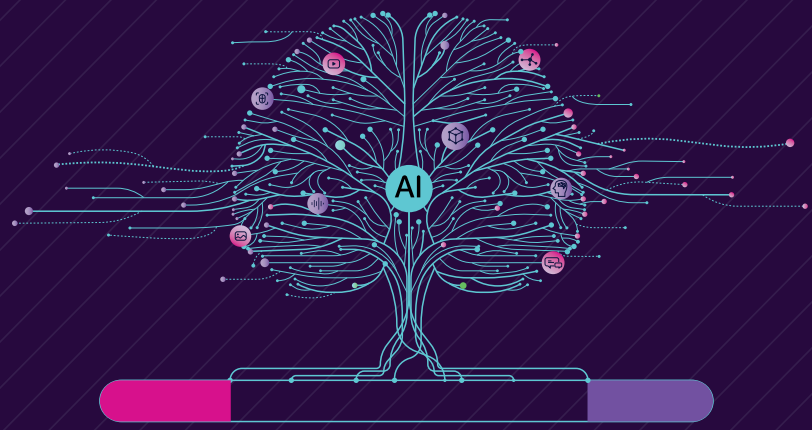
Um bestehende Sicherheitsmaßnahmen zu umgehen, können Angreifer KI-Algorithmen entwickeln, die speziell darauf ausgelegt sind, von Sicherheitssystemen nicht erkannt zu werden. Dies stellt eine ernsthafte Herausforderung für die Verteidiger dar, da sie ständig, fast in Echtzeit, ihre Systeme aktualisieren und anpassen müssen.

**Eine tugendhafte KI gegen Hacker KI**

Im Cyber-Sicherheitsbereich können starke KI-Tools und Anwendungen implementiert werden. Dazu gehören Automatisierung und Effizienzsteigerung, Bedrohungsanalyse und Vorhersage, Identifizierung von Malware und Nutzer Verhaltensanalyse.

**Automatisierung und Effizienzsteigerung**

KI kann große Mengen an Daten in Echtzeit analysieren und Muster erkennen, die für das menschliche Auge unsichtbar bleiben. Dies ermöglicht eine proaktive Identifizierung und Reaktion auf Bedrohungen. Beispielsweise können bei Cloudflare KI-gesteuerte Systeme Anomalien im Netzwerkverkehr erkennen und automatisch Maßnahmen ergreifen, um mögliche Angriffe abzuwehren, bevor sie Schaden anrichten. Dies verbessert nicht nur die Sicherheit, sondern reduziert auch die Arbeitsbelastung für Analysten.




**Bedrohungsanalyse und Vorhersage**

Durch den Einsatz von Machine Learning (ML) und Deep Learning (DL) kann KI historische Daten analysieren und Vorhersagen über zukünftige Bedrohungen treffen. Diese Vorhersage Fähigkeiten sind besonders wertvoll, da sie es Sicherheitsteams ermöglichen, sich auf potenzielle Angriffe vorzubereiten und Schwachstellen im Vorfeld zu beheben. Bei Cloudflare werden eine große Menge an Daten über Bedrohungen in der ganzen Welt extrahiert und KI dazu genutzt, um Zero-Day-Schwachstellen vorherzusagen. In diesem Fall funktioniert die KI wirklich gut. Im letzten Quartal hat Cloudflare einen Durchnitt von 150 Milliarden Cyberangriffe pro Tag abgewehrt

**Identifizierung von Malware**

Traditionelle Antiviren-Software basieren auf Signaturen, die aktualisiert werden müssen, um neue Malware-Varianten zu erkennen. KI-gestützte Systeme hingegen können durch Verhaltensanalyse und Mustererkennung auch unbekannte Malware identifizieren. Dies erhöht die Erfolgsquote bei der Erkennung neuer und mutierter Bedrohungen erheblich. Mit seinem globalen Netzwerk in 330 Städten und über 120 Ländern, und seiner KI-gestützten Connectivity Cloud kann Cloudflare bösartige Domains und Malware schnell erkennen und abwehren.

**Nutzer Verhaltensanalyse**

KI kann das Verhalten von Nutzern überwachen und Abweichungen vom normalen Verhalten identifizieren. Dies ist besonders nützlich, um Insider-Bedrohungen zu erkennen, bei denen legitime Benutzerkonten kompromittiert werden. Durch die Analyse von Login-Zeiten, -Orten und -Verhalten kann KI potenziell schädliche Aktivitäten frühzeitig erkennen. Das Cloudflare Threat Intelligence Tool Cloudforce One kombiniert den Einblick von Cloudflare in den Echtzeit-Zugriff Traffic mit einem erstklassigen Team für Bedrohungsforschung, um unübertroffene operative Bedrohungsinformationen zu bieten.

**Den KI Krieg gewinnen**

Angesichts dieser dualen Natur der KI in der Cybersicherheit stellt sich die Frage, wie man die Chancen maximieren und die Risiken minimieren kann. Das Wichtigste bleibt vorbereitet zu sein. In einer aktuellen Cloudflare-Studie die mit mehr als 4.000 Führungskräften aus Wirtschaft und Technologie in ganz Europa und 430 in Deutschland durchgeführt wurde, ergab es sich, dass fast die Hälfte (42 Prozent) der deutschen Unternehmen in den letzten 12 Monaten mindestens einen Vorfall im Bereich der Cybersicherheit erlebt haben. Die Mehrheit (69 Prozent) der deutschen Unternehmen erwartet in den nächsten 12 Monaten einen Cyberangriff, aber nur 23 Prozent der Organisationen fühlen sich gut darauf vorbereitet. Die beste Strategie besteht darin, auf kontinuierliche Forschung und Entwicklung zu setzen, um den Verteidigungs-Vorsprung aufrechtzuerhalten.

**Innovation, Zusammenarbeit und Silos aufbrechen**

Konvergenz zwischen Netz-Teams, Sicherheitsteams und IT-Teams ist der neue Arbeits-Trend. Es handelt sich um eine relativ neue Entwicklung, insbesondere mit dem Aufkommen von Zero Trust, bei dem die Cybersicherheit eine zentrale Rolle spielt. Plötzlich verschwimmen in vielen Unternehmen die Grenzen, die früher ganz klar waren. Daher ist es wichtig, dass interne organisatorische Abläufe es ermöglichen, die richtigen Entscheidungen zu treffen, um das Unternehmen zu modernisieren.

Darüber hinaus ist eine enge Zusammenarbeit zwischen Industrie, Regierung und akademischen Institutionen erforderlich, um ein umfassendes Verständnis der Bedrohungslandschaft zu entwickeln und effektive Gegenmaßnahmen zu erarbeiten.

Innovation spielt hier eine kritische Rolle und daher ist es umso wichtiger darüber nachzudenken, wie man KI in seine eigenen Produkte und Dienstleistungen integrieren kann.

Trotz Herausforderungen bleibt die Zukunft von KI im Allgemeinen und im Besonderen in der Cybersicherheit vielversprechend. Cloudflare investiert weiterhin in Forschung und Entwicklung, um seine KI-Fähigkeiten in seiner Connectivity Cloud zu erweitern und seinen Kunden noch effektivere Sicherheitslösungen bereitzustellen.

***Stefan Henke***

# Managed Security Service

## EINFACHER GEHT'S NICHT

IT-Schutz, Security Awareness, Schwachstellenmanagement. Viele IT-Verantwortliche und Systemhäuser sind mit dem Bereich IT-Sicherheit überfordert. Es mangelt an Zeit, Personal und Fachwissen. Eine günstige und ohne Aufwand umzusetzende Lösung bietet beispielsweise Anqa IT-Security, indem die IT-Sicherheit als externer Partner vollumfänglich übernommen wird.

Cybercrime ist ein Rund-um-die-Uhr-Geschäft. Angreifergruppen kennen keinen Feierabend und attackieren Unternehmen auch an Wochenenden und im Homeoffice. Daher ist 24/7-Schutz schon lange Pflicht. Zudem ist eine sofortige Reaktion im Falle eines erfolgreichen Angriffs entscheidend. Security Operations Center (SOC) spielen hierbei eine wichtige Rolle. Sie schulen Mitarbeitende in Unternehmen im richtigen Umgang mit E-Mails und Daten, führen Dark Web Monitorings und Blacklist Scans durch und bieten IT-Sicherheitsberatungen inklusive Pentests an.

**100 Prozent IT-Security ohne Aufwand**

Den IT-Verantwortlichen und Systemhäusern entsteht dabei null Aufwand. Sie müssen weder Personal bereitstellen, noch selbst Zeit aufbringen für die Einrichtung, Umsetzung oder Kundenkorrespondenz. Das gilt nicht nur für den Schutz der IT-Systeme, auch den Bereich Security Awareness übernehmen erfahrene SOCs vollumfänglich als Managed Service – vom Onboarding über die Durchführung bis hin zum Reporting. Dabei entscheidet das Systemhaus oder die IT-Verantwortlichen, inwieweit sie Teil der Prozesse sein möchten oder ob sie den Bereich IT-Sicherheit komplett in die Hände des Anbieters geben und sich mit gutem Gefühl ihrem Kerngeschäft widmen.

***https://anqa-itsecurity.de/***

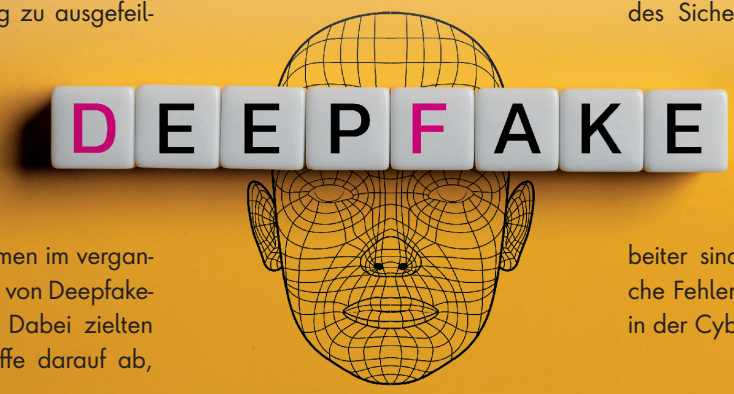
---

# Deepfakes auf dem Vormarsch

## UNTERNEHMEN WAPPNEN SICH GEGEN RAFFINIERTE KI-ANGRIFFE

Eine kürzlich veröffentlichte Studie von Deep Instinct offenbart, dass 97 Prozent der Unternehmen befürchten, Opfer eines Sicherheitsvorfalls durch bösartige KI zu werden. Mit dem Aufkommen neuer, auf großen Sprachmodellen (LLM) basierender KI-Plattformen haben Cyberkriminelle nun Zugang zu ausgefeilten Technologien, die es ihnen ermöglichen, überzeugende Deepfakes zu erstellen.

Die Studie zeigt, dass 61 Prozent der Unternehmen im vergangenen Jahr eine Zunahme von Deepfake-Vorfällen verzeichneten. Dabei zielten 75 Prozent dieser Angriffe darauf ab, sich als CEO oder andere Mitglieder der Führungsetage auszugeben. Deepfakes werden von den Unternehmen als größte Sorge identifiziert, wobei 34 Prozent diese Art von Angriffen als erhebliche oder kritische Bedrohung einstufen.




Infolgedessen haben 73 Prozent der Unternehmen begonnen, KI-Angriffe als Anlass zu nehmen, um ihre Cybersicherheitsstrategien von einer reaktiven auf eine präventive Ausrichtung umzustellen. Die wichtigste Methode, die hierbei zur Anwendung kommt, ist die Schulung des Sicherheitsbewusstseins der Mitarbeiter (47 Prozent der Unternehmen), gefolgt von prädiktiven Präventionsplattformen sowie der Endpunkt-Erkennung und -Reaktion. Schulungen für Mitarbeiter sind entscheidend, da menschliche Fehler oft die größte Schwachstelle in der Cybersicherheit darstellen.

***www.knowbe4.com***


# Samsung Knox Native

## EINGEBAUTE SICHERHEIT FÜR VERSCHLUSSSACHEN

Mobiles Arbeiten verlangt umfassende Sicherheit, vor allem in Geschäftsbereichen mit hohen Sicherheitsanforderungen durch vertrauliche Daten. Mit Knox Native bietet Samsung erstmals eine Hardware-basierte und vom BSI (Bundesamt für Sicherheit in der Informationstechnik) evaluierte Sicherheitslösung, die die hohen Standards für die Verarbeitung von Verschlusssachen des Geheimhaltungsgrades „VS – Nur für den Dienstgebrauch" (VS-NfD) erfüllt.

**Eingebauter Hardware-Anker**

Sichere mobile Lösungen für die Speicherung von Daten gibt es schon länger – auch für die Bearbeitung von Verschlusssachen. Doch bisher waren dafür externe SD-Karten, zusätzliche Software und verschiedene PINs notwendig. Samsung geht nun einen neuen Weg: Als Herzstück wird in ausgewählten mobilen Endgeräten erstmals ein zertifizierter Hardware-Anker – das Samsung embedded Secure Element (eSE) – verbaut. Dieses Element ist nach dem Common Criteria Evaluation Assurance Level (CC EAL) 6+ zertifiziert und schafft einen sicheren, isolierten Bereich auf dem Gerät. Gemeinsam mit dem BSI Java Card Applet (Mobile Security Anchor) ermöglicht es die verschlüsselte Speicherung personenspezifischer und klassifizierter Daten nach den Vorgaben des BSI. Damit wurde die Lösung nun auch offiziell für die Verarbeitung von Informationen des Geheimhaltungsgrades „VS – Nur für den Dienstgebrauch" (VS-NfD) zugelassen.

**Hohe Sicherheit für Standard-Applikationen**

Mit der Freigabe für das VS-NfD-Umfeld kommt Samsung den wachsenden Sicherheitsanforderungen im Umfeld von Bundesbehörden entgegen. Native Funktionen wie E-Mail, Kalender oder Kontakte lassen sich auf den entsprechenden Endgeräten nun auch für die Verarbeitung von Verschlusssachen nutzen. Aber nicht nur der öffentliche Bereich kann von den hohen Sicherheitsstandards beim mobilen Arbeiten profitieren. Auch für private Unternehmen wie Energieversorger, Banken oder andere Organisationen mit strengen Anforderungen an die Sicherheit ihrer vertraulichen Daten, ist der Einsatz von Knox Native problemlos möglich.

**Vereinfachte Sicherheitsfeatures**

Ein Vorteil von Knox Native ist die einfache Handhabung: Eine einzige PIN reicht zur Aktivierung aller Bereiche aus. Zudem müssen Anwender trotz des hohen Sicherheitsstandards keine Einschränkungen bei der Nutzererfahrung hinnehmen: Mit Knox Native können sie die vorinstallierten Apps in der gewohnten Android-Umgebung nutzen. Durch die Trennung der beiden Bereiche lassen sich die Geräte zudem geschäftlich und privat einsetzen.

Darüber hinaus gibt es die Möglichkeit, über spezifische Schnittstellen unternehmenseigene Apps ohne aufwändige Evaluation zu integrieren. So können auch größere Geräteflotten auf hohem Sicherheitsniveau wirtschaftlich betrieben werden.

**Verwaltung über Knox Suite**

Zur Verwaltung der Samsung Geräte steht die Knox Suite bereit. Das Tool-Set bündelt alle Knox-Produkte wie Enrollment, Manage, E-FOTA, Asset Intelligence oder Remote Support für die IT-Administration. Damit lassen sich unterschiedliche Prozesse im Unternehmensumfeld – von der automatischen Ersteinrichtung über die Durchsetzung geltender Sicherheitsrichtlinien bis hin zum Update-Management – effektiv und über den gesamten Lebenszyklus der mobilen Geräte hinweg abdecken.

GUT ZU WISSEN
IT-Sicherheit für Unternehmen


# Multi-Faktor-Authentifizierung

## WARUM ES OHNE NICHT MEHR GEHT

Anfang Juni wurde die CDU das Opfer eines schwerwiegenden Cyberangriffs. Die Täter konnten sich rund 14 Tage unerkannt im Netzwerk bewegen und hatten Zugriff auf kritische Daten. Die Sicherheitslücke befand sich innerhalb einer VPN-Software, wie das BSI in einer Sicherheitswarnung vom 3. Juni bestätigte. Darin stellte das Bundesamt zudem klar, dass nur Nutzer gefährdet waren, bei denen der VPN-Zugang ausschließlich über lokale Benutzernamen-/Passwort-Kombinationen erfolgte. Dieser prominente Sicherheitsvorfall zeigt in aller Deutlichkeit, dass ein Passwort zur Authentisierung keinen ausreichenden Schutz bietet – es braucht mindestens einen weiteren Faktor. Nicht ohne Grund empfahl sowohl das BSI als auch der betroffene VPN-Anbieter die Verwendung „zusätzlicher Authentisierungsmechanismen". Auch die kommende EU-Richtlinie NIS2 schreibt für entsprechende Unternehmen die Umsetzung einer Multi-Faktor-Authentifizierung (MFA) für digitale Zugänge zwingend vor.

Es zeigt sich einmal mehr: MFA ist von essenzieller Bedeutung. Die Auswahl der passenden Lösung bleibt den Nutzern überlassen. Gerade Unternehmen und Organisationen mit vielen Mitarbeitenden bieten Token auf Basis des etablierten FIDO2-Standards eine kostengünstige und leicht umsetzbare MFA-Methode, die zudem bestmögliche Sicherheit garantiert.

Noch wichtiger als die Auswahl einer MFA-Technologie ist allerdings, jetzt zu handeln. Im Wettlauf mit Hackern ist Abwarten keine Option mehr. Cybersicherheit muss endlich mit der nötigen Entschlossenheit angegangen werden.

***Claus Gründel | www.swissbit.com***

# KRITIS im Visier

## SCHÄDLICHER DATENVERKEHR STEIGT MASSIV AN

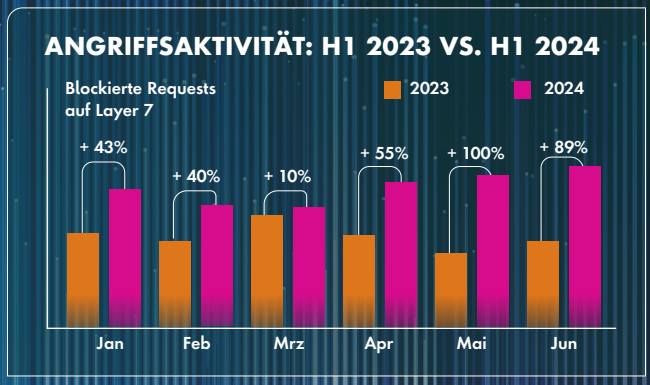
Der schädliche Datenverkehr im Internet steigt immer weiter an. Das zeigt der neue Report des europäischen Cybersicherheitsanbieters Myra Security.

Die im Report angegebenen Daten aus dem Security Operations Center (SOC) von Myra zeigen, dass die Anzahl schädlicher Anfragen auf Webseiten, Online-Portalen und Web-Schnittstellen (APIs) im ersten Quartal 2024 um 29,8 Prozent im Vergleich zu 2023 angestiegen ist. Im zweiten Quartal fällt der Zuwachs mit 80 Prozent noch deutlicher aus. Über das gesamte erste Halbjahr 2024 hinweg beträgt der Anstieg schädlicher Anfragen 53,2 Prozent gegenüber dem Vorjahreszeitraum.

**Kritische Infrastrukturen unter Dauerfeuer**

Laut dem aktuellen BKA-Lagebericht verzeichnete jede sechste KRITIS-Organisation im ersten Quartal 2024 einen Cybervorfall. Insbesondere die Sektoren Energie, Finanz- und Versicherungswesen, Transport und Verkehr sowie das Gesundheitswesen stehen im Visier von Cyberkriminellen. Diese Erkenntnisse decken sich mit den Beobachtungen des Myra SOC. Auch Einrichtungen der öffentlichen Verwaltung sind verstärkt betroffen. Behörden sehen sich zunehmend mit Angriffskampagnen politisch motivierter Gruppierungen konfrontiert.

***www.myrasecurity.com***



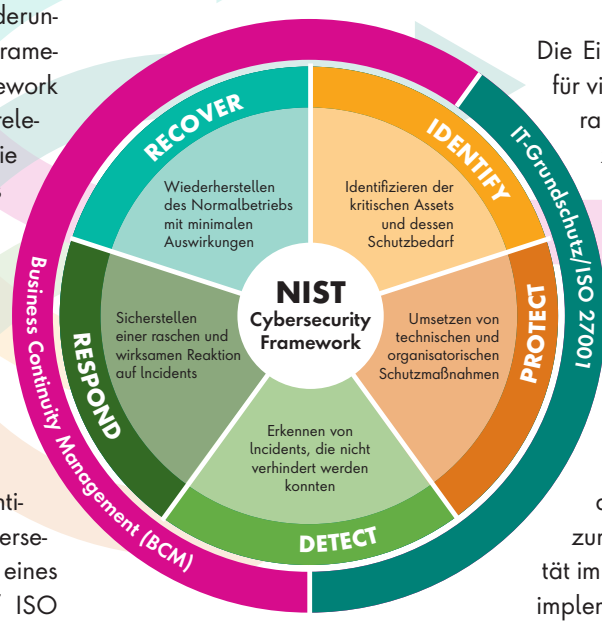
# Effektive Umsetzung der NIS2-Richtlinie

## MIT DER RICHTIGEN SOFTWARE DEN ÜBERBLICK BEHALTEN

Die europäische NIS2-Richtlinie markiert eine bedeutende Weiterentwicklung in der Cybersicherheitspolitik der Europäischen Union und betrifft ca. 30.000 Unternehmen in Deutschland. Im Vergleich zur ursprünglichen NIS-Richtlinie legt NIS2 einen stärkeren Fokus auf Cybersicherheit und Cyberhygiene, um den wachsenden Bedrohungen in diesem Bereich effektiv zu begegnen. Die NIS2-Richtlinie legt zwar keinen spezifischen Compliance-Rahmen fest, allerdings lassen sich ihre Anforderungen in den NIST Cybersecurity Framework abbilden. Dieses Framework deckt die NIS2-Ziele ab und ist relevant für IT- und OT-Netzwerke. Die fünf zentralen Funktionen des NIST Cybersecurity Framework können durch die Managementsysteme IT-Grundschutz, ISO 27001 und BCM in HiScout abgedeckt werden.

**BCM: Sicherstellung der Geschäftskontinuität**

Neben Anforderungen zu präventiven Schutzmaßnahmen zur Cybersecurity, die durch die Anwendung eines aktiven ISMS (IT-Grundschutz / ISO 27001) abgedeckt werden, ist ein zentraler Aspekt der NIS2-Richtlinie das Risikomanagement – und somit auch Business Continuity Management (BCM). Mit der HiScout GRC Suite steht Unternehmen eine zentrale Management-Suite für Informationssicherheit, Datenschutz und Business Continuity Management zur Verfügung. Das BCM-Modul bietet die Möglichkeit, zentralisiert detaillierte Business Continuity-Pläne zu erstellen und regelmäßig zu testen. Die Software unterstützt bei der Identifikation kritischer Geschäftsprozesse, der Priorisierung von Maßnahmen und der Bildung von Krisenstäben. Durch regelmäßige Übungen und Tests können Unternehmen und Organisationen sicherstellen, dass sie auf Notfälle vorbereitet sind und ihre betrieblichen Abläufe schnell wiederherstellen können. So trägt HiScout maßgeblich zur Resilienz und Sicherheit von Unternehmen bei.




Doch was ist BCM eigentlich? BCM stellt sicher, dass ein Unternehmen auch in Krisensituationen geschäftsfähig bleibt. Unvorhergesehene Ereignisse wie Cyberangriffe, Naturkatastrophen oder technische Ausfälle können den Geschäftsbetrieb massiv beeinträchtigen. Ohne ein effektives BCM können solche Vorfälle zu erheblichen finanziellen Verlusten, Rufschädigung und sogar zur Geschäftsaufgabe führen. Ein gut durchdachtes und getestetes BCM gewährleistet, dass kritische Geschäftsprozesse schnell wiederhergestellt werden können, die Auswirkungen auf Kunden und Partner minimiert werden und die Unternehmensführung in der Lage ist, fundierte Entscheidungen zu treffen.

Die HiScout GRC Suite deckt einen Großteil der NIS2-Anforderungen ab, einschließlich:

- Risikoanalyse;
- Business Impact-Analyse;
- Notfallumgebung in Cyber-Krisen-Übungen;
- Sicherheit und Continuity Awareness;
- GAP-Analyse und Bedrohungssimulationen; Business Continuity-Pläne und Krisenmanagement.

Die Einhaltung der NIS2-Richtlinien ist für viele Unternehmen eine große Herausforderung, insbesondere in Bezug auf die Sicherheit und Integrität ihrer digitalen Infrastrukturen. Um diesen Anforderungen gerecht zu werden, spielen BCM-Lösungen wie die HiScout GRC Suite eine zentrale Rolle. Sie bietet Unternehmen nicht nur die Möglichkeit, potenzielle Risiken zu identifizieren und zu bewerten, sondern auch robuste Mechanismen zur Wiederherstellung und Kontinuität im Falle von Sicherheitsvorfällen zu implementieren.

Setzen Sie auf die HiScout GRC Suite, um die Anforderungen der NIS2-Richtlinie zu erfüllen und eine sicherere digitale Umgebung zu schaffen.

***Silke Menzel | www.hiscout.com***

# UNSICHERE ANDROID-KERNELS

## VERSÄUMNISSE DER SMARTPHONE-ANBIETER?

In einer Analyse von Smartphones von zehn Herstellern haben Forschende der TU Graz festgestellt, dass die genutzten Android-Kernels trotz vorhandener Schutzmechanismen anfällig für bekannte Angriffe - sogenannte One-Day Exploits - sind.

Je nach Hersteller und Modell konnten bei den untersuchten 994 Smartphones nur zwischen 29 und 55 Prozent der vom Forschungsteam getesteten Angriffe verhindert werden. Im Gegensatz dazu konnte das von Google bereitgestellte Generic Kernel Image (GKI) der Version 6.1 rund 85 Prozent der Angriffe verhindern. Im Vergleich zum GKI schnitten die Hersteller-Kernels bei der Angriffsabwehr bis zu 4,6-mal schlechter ab.

Untersucht hat das Forschungsteam um Lukas Maar, Florian Draschbacher, Lukas Lamster und Stefan Mangard vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz, zwischen 2018 und 2023 auf den Markt gekommene Geräte dieser Hersteller (Auflistung vom sichersten zum unsichersten): Google, Realme, OnePlus, Xiaomi, Vivo, Samsung, Motorola, Huawei, Oppo und Fairphone. Die auf diesen Smartphones verwendeten Android-Versionen reichten von Version 9 bis 14, die Kernels deckten den Bereich von Version 3.10 bis 6.1 ab, wobei Hersteller, die auf niedrigere Kernel-Versionen setzen, auch weniger Sicherheit bieten.

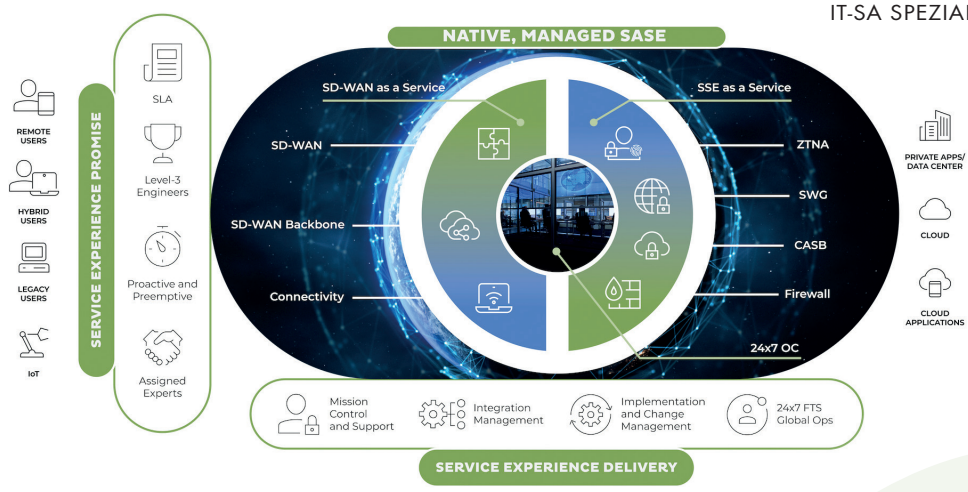
**Effektive Abwehrmechanismen selten aktiviert**

Ein weiterer Kernpunkt der Analyse: Es gäbe bereits effektive Abwehrmaßnahmen für eine Reihe der bekannten Angriffsmethoden, in den Kernels der Hersteller sind sie aber selten aktiviert beziehungsweise sind die Kernels falsch konfiguriert. Das führt dazu, dass sogar die Kernel-Version 3.1 aus dem Jahr 2014 mit allen aktivierten Sicherheitsmaßnahmen besser vor bekannten Angriffen schützen könnte als rund 38 Prozent der von den Herstellern selbst konfigurierten Kernels.

Zusätzlich stellten die Forschenden fest, dass Low-End-Modelle der Hersteller um rund 24 Prozent stärker gefährdet waren als High-End-Modelle. Ein wichtiger Grund dafür liegt im Leistungsverlust, den zusätzliche Sicherheitsmaßnahmen bedeuten, weswegen sie in Low-End-Modellen zur Ressourcenschonung oft deaktiviert bleiben.

„Wir hoffen, dass unsere Ergebnisse dazu beitragen, dass in Zukunft effektivere Sicherheitsmaßnahmen in den Kernels der Hersteller zu finden sind und Android damit sicherer wird", sagt Lukas Maar. „Wir haben unsere Analyse auch mit den untersuchten Herstellern geteilt und Google, Fairphone, Motorola, Huawei und Samsung haben diese zur Kenntnis genommen – einige haben sogar Patches veröffentlicht. Wir haben Google auch vorgeschlagen, das Android Compatibility Definition Document (CDD) zu aktualisieren, in dem der Rahmen für die Anforderungen festgelegt wird, damit Geräte mit Android kompatibel sind. Google selbst hat betont, sich des Problems bewusst zu sein und möchte die Integration von Kernel-Sicherheitsmaßnahmen Schritt für Schritt verstärken."

***www.tugraz.at***




# SD-WAN

## DIE GRUNDLAGE FÜR EINE ERFOLGREICHE SASE JOURNEY

Secure Access Service Edge (SASE) wurde zwar erst 2019 eingeführt, gilt aber nach wie vor als bahnbrechendes Konzept für Netzwerke und Sicherheit. Viele Unternehmen beginnen ihre SASE-Reise mit der Einführung eines Software-definierten Wide Area Network (SD-WAN), das auf einer agilen, zuverlässigen und Cloud-fähigen Netzwerkarchitektur aufbaut. Ein SD-WAN zu implementieren ist jedoch nicht so einfach, wie die Installation eines isolierten Netzwerk-Tools, wie etwa das Monitoring des Netzwerkverkehrs. Die Migration auf ein SD-WAN ist aufwändig, da erhebliche Veränderungen nötig sind: von der physischen Konnektivität über das Routing bis zum Betrieb und der Verwaltung des Netzwerks. Diese Umstellung kann mit erheblichen Kosten und begrenztem Nutzen verbunden sein, wenn sie nicht richtig durchgeführt wird. Daher ist es wichtig, den SD-WAN-Anbieter mit Bedacht auszuwählen, um eine erfolgreiche SD-WAN-Implementierung und den Übergang zu SASE sicherzustellen.

Zunächst ist es wichtig, sich auf die Netzwerkleistung zu konzentrieren. Ein SD-WAN-Anbieter sollte verschiedene Konnektivitätsoptionen (MPLS, Internet, 4G/5G) und einen zuverlässigen Cloud-Backbone mit globaler Abdeckung und End-to-End-SLAs anbieten. Dies gewährleistet Kosteneinsparungen, Flexibilität und eine verbesserte Benutzererfahrung für die Mitarbeiter, egal wo auf der Welt sie sich befinden. Ein weiterer wichtiger Aspekt bei der SD-WAN-Implementierung und beim Übergang zu SASE ist die Sicherheit. Die SASE-Lösung sollte ein Sicherheitsportfolio umfassen, das den größten Teil der Cyber-Kill-Chain abdeckt und mit dem SD-WAN-Stack eine Einheit bildet, um Komplexität und Kosten zu reduzieren. Fragmentierte Lösungen, denen es an einer umfassenden Abdeckung mangelt, sind oft komplex zu verwalten, intransparent und führen zu Sicherheitslücken.

**Kriterien bei der Auswahl von SD-WAN-Anbietern**

Auch das Technologiemanagement und der Betrieb sind entscheidend. Ein SD-WAN-Anbieter sollte die Plattform proaktiv überwachen und aktualisieren, um sicherzustellen, dass der Datenverkehr optimiert und sicher bleibt. Im Idealfall kann der SD-WAN-Anbieter das Netzwerkdesign und die Richtlinien auf die individuellen Anforderungen und Bedürfnisse des jeweiligen Unternehmens abstimmen, eine effiziente Bereitstellung und einen zuverlässigen 24x7-Support mit direktem Zugang zu Fachexperten bietet, um einen reibungslosen täglichen Betrieb zu gewährleisten. Und schließlich sind das Fachwissen und die Agilität des Anbieters für den langfristigen Erfolg entscheidend. Der SD-WAN-Anbieter sollte ein Partner sein, der nicht nur die Technologie liefert, sondern auch strategische Beratung und einen Fahrplan bietet, der auf die Geschäftsziele des jeweiligen Unternehmens abgestimmt ist. Durch die Priorisierung dieser Faktoren kann eine solide Grundlage für eine sichere, flexible und zukunftsfähige SD-WAN- und SASE-Implementierung geschaffen werden.

Als Teil seiner SASE Experience bietet Open Systems mit Hauptsitz in der Schweiz eine umfassende, einheitliche und benutzerfreundliche Plattform zusammen mit einem erstklassigen Support. Das Unternehmen ist ein zentraler Ansprechpartner für alle, die einen erstklassigen Managed Service für SD-WAN und SSE suchen. Ihr privates WAN Backbone, mit mehr als 500 PoPs weltweit, bietet eine unübertroffene Dichte und Reichweite an Netzwerk-Zugangspunkten. Somit ist eine hohe Verbindungs- und Datentransfer-Qualität sichergestellt, welche in Kombination mit ihrem Last-Mile Connectivity Service sogar durch End-to-End-SLAs zwischen den Standorten garantiert werden kann.

***www.open-systems.com/de***

# Excel war gestern

## KRISENSICHER DANK ZENTRALEM BUSINESS CONTINUITY MANAGEMENT

DIE UMSTELLUNG VON EXCEL-BASIERTEN PROZESSEN AUF SPEZIALISIERTE BCM-SOFTWARE ERMÖGLICHT ES UNTERNEHMEN IHRE WIDERSTANDSFÄHIGKEIT GEGENÜBER KRISEN NACHHALTIG ZU VERBESSERN.

**Silke Menzel, Productmanagement, HiScout GmbH, www.hiscout.com**

Kennen Sie die Risiken, denen Ihr Unternehmen ausgesetzt ist? Cyberattacken, technische Betriebsunterbrechungen oder Naturkatastrophen sind nur ein Bruchteil der Gefahren. Natürlich muss davon nichts passieren, aber was, wenn doch? Es reicht nicht aus, nur darauf zu reagieren. Hier kommt Business Continuity Management (BCM) ins Spiel.

**Die Hauptaufgaben des Business Continuity Management**

Als strategischer, ganzheitlicher Managementansatz hilft BCM Unternehmen dabei, ihre Widerstandsfähigkeit gegen Krisen zu stärken und den Geschäftsbetrieb auch in Krisensituationen aufrechtzuerhalten. Durch die Identifikation kritischer Geschäftsbereiche und potenzieller Bedrohungen ermöglicht es BCM, präventive Maßnahmen zu entwickeln und Krisensituationen effizient zu bewältigen. In vielen Branchen ist BCM gesetzlich vorgeschrieben, insbesondere für Unternehmen, die Regularien wie KRITIS, NIS2 oder DORA unterliegen.

Zu den Hauptaufgaben eines BCM gehören:

#1 Erkennen und Bewerten von Schadensszenarien: Identifikation potenzieller Bedrohungen und Risiken sowie deren Auswirkungen;

#2 Business Impact-Analyse: Identifikation kritischer Geschäftsprozesse sowie Analyse der Auswirkungen von Störungen auf diese, um Prioritäten für die Wiederherstellung festzulegen;

#3 Entwicklung von Business Continuity-Plänen: Erstellung von Plänen und Maßnahmen zur Bewältigung von Störungen, zur Aufrechterhaltung der Geschäftskontinuität und Wiederherstellung des Normalbetriebes;

#4 Testen und Üben: Regelmäßige Überprüfung, Aktualisierung und Durchführung von Tests und Übungen, um die Wirksamkeit der Pläne sicherzustellen und Erfahrungen zu dokumentieren.

**Erfolgsfaktoren für ein robustes BCM**

Der Erfolg eines BCM hängt stark von der Unterstützung der Unternehmensführung ab und erfordert ein Bewusstsein bei den Mitarbeitern für die täglichen Risiken und Bedrohungen. Die Zusammenarbeit aller Abteilungen ist entscheidend, um das Unternehmen nicht nur proaktiv zu schützen, sondern auch nach Vorfällen schnell wieder auf Kurs zu bringen.

Viele Unternehmen verlassen sich jedoch noch immer auf Word und Excel zur Verwaltung ihres BCM. Wie sieht der Prozess mit diesen Tools beispielsweise aus, wenn ein Mitarbeiter das Unternehmen verlässt, der in Krisensituationen eine wichtige Rolle einnehmen sollte? Jede Veränderung im Unternehmen erfordert eine Anpassung des BCM. Sich hier durch unzählige Word- und Excel-Dokumente zu kämpfen und händisch Änderungen vorzunehmen, Verknüpfungen und Abhängigkeiten zu berücksichtigen, birgt eine hohe Fehleranfälligkeit und kostet viel Zeit.

**Von Excel zur zentralen Softwarelösung**

Im Gegensatz zu Word und Excel dienen softwarebasierte BCM-Tools als zentrale Lösung für ein strukturiertes und effizienteres Arbeiten, ohne Gefahr zu laufen, die Übersicht zu verlieren. Diese Tools automatisieren nicht nur Prozesse wie Business Impact-Analysen und die Erstellung von Notfallplänen, sondern reduzieren auch den Verwaltungsaufwand. Sie bieten eine bessere Skalierbarkeit und Compliance-Überwachung, was gerade in komplexen Unternehmensstrukturen und für die Einhaltung gesetzlicher Standards von entscheidender Bedeutung ist.

Die Umstellung von Excel-basierten Prozessen auf spezialisierte BCM-Software ermöglicht es Unternehmen, nicht nur ihre Effizienz zu steigern, sondern auch ihre Widerstandsfähigkeit gegenüber Krisen nachhaltig zu verbessern. Indem sie sich von manuellen, fehleranfälligen Prozessen verabschieden, lässt sich sicherstellen, dass das Unternehmen auch in herausfordernden Zeiten geschäftsfähig bleibt.

***Silke Menzel***

# Automatisierte Zertifikatsverwaltung

ENTRUST AUF DER IT-SA 2024

Entrust, weltweit führender Anbieter für Identitäts-, Zahlungs- und Datensicherheit, wird auf der it-sa neue Lösungen aus seinem umfangreichen Portfolio vorstellen. Ein besonderer Schwerpunkt liegt dabei auf dem Thema Datensicherheit, PKI und Zertifikats-Management.

**Komplexität der digitalen Zertifikate nimmt zu**

Die Verwendung digitaler Zertifikate wird stetig komplexer. Traditionelle PKI-Anwendungsfälle wie Benutzerauthentifizierung und VPN-Sicherheit koexistieren mit Anwendungen im Bereich Internet der Dinge (IoT), Software-Containerisierung und DevOps-Systemen. Die Anzahl der digitalen Zertifikate erhöht sich dadurch stetig, gleichzeitig werden die zugrundeliegenden Infrastrukturen immer komplexer.

Viele Unternehmen haben Schwierigkeiten, ihre Zertifikate nachzuverfolgen und proaktiv zu verwalten. Ihre Umgebungen sind zu komplex und verteilt, um Hunderte oder Tausende von Zertifikaten in Tabellenkalkulationen zu verwalten. Dies eröffnet Schwachstellen, die Angreifer ausnutzen.

**Certificate Hub: Automatisierte Zertifikatsverwaltung**

Mit dem Certificate Hub hat Entrust ein Tool für das Lebenszyklus-Management von Zertifikaten geschaffen, welches die Erkennung, Verwaltung und Automatisierung von Zertifikaten standardisiert, vereinfacht und rationalisiert. Durch Automatisierung und moderne Orchestrierungstechnologie hilft der Certificate Hub über eine einfach zu bedienende und intuitive Schnittstelle Unternehmen dabei, die Komplexität ihrer Infrastruktur zu beherrschen – einschließlich Netzwerkerkennung, Zertifikatsausstellung und vollautomatischem Reporting.

***www.entrust.com***

**it-sa Expo&Congress**
Besuchen Sie uns in **Halle 7-410**

# Branchen uneins in Sachen Verschlüsselung

## HERAUSFORDERUNGEN IM UMGANG MIT DEM SCHUTZ SENSIBLER DATEN

Der Handel in Deutschland muss sich beim Thema Datenschutz mit einer Kluft zwischen Wunsch und Wirklichkeit auseinandersetzen. Das hat eine im zweiten Quartal 2024 in Deutschland durchgeführte Umfrage von eperi ergeben. Über alle Branchen und Organisationsgrößen hinweg verschlüsseln 67,5 Prozent der befragten Unternehmen ihre sensiblen Daten.

Anders der Handel: Hier geben lediglich 30 Prozent der Handelsunternehmen an, ihre sensiblen Daten zu verschlüsseln, um sie vor Missbrauch zu schützen. Gleichzeitig spielt für die Retail-Branche Rechtssicherheit für das Management mit 62,5 Prozent eine überdurchschnittlich große Rolle – der Durchschnittswert aller Branchen liegt bei 43 Prozent.

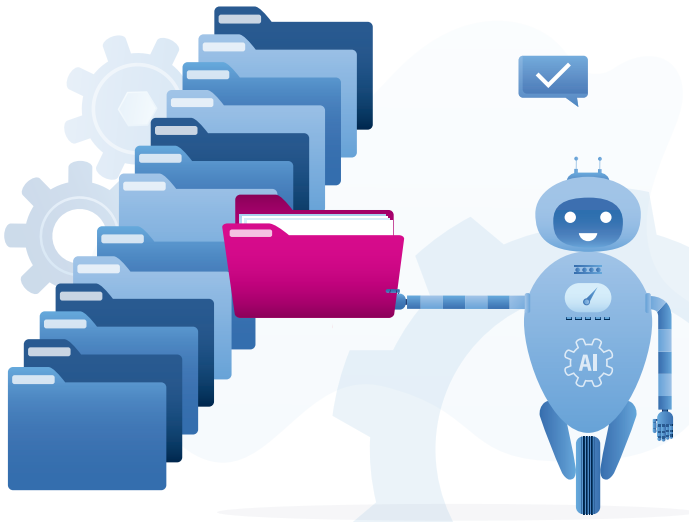
Demnach scheinen gesetzliche Vorgaben wie beispielsweise NIS2 für den Handel wichtiger zu sein als für andere Branchen. Folgerichtig legen 75 Prozent der deutschen Handelsunternehmen zudem großen Wert darauf, dass ausschließlich das eigene Unternehmen – nicht aber der Cloudprovider – Zugriff auf den Schlüssel hat, mit dem die Unternehmensdaten verschlüsselt werden.

**Gesetzlicher Mindeststandard ausreichend?**

Laut eperi-Umfrage nutzen 86,5 Prozent aller Unternehmen Clouddienste – das stark regulierte Banken- und Versicherungswesen sogar zu knapp 95 Prozent. Von einer Verschlüsselung ihrer sensiblen Daten versprechen sich die Unternehmen daher in erster Linie Schutz vor Cyberkriminalität (56 Prozent) und die Einhaltung des DSGVO (51 Prozent). Mit durchschnittlich 27 Prozent weit abgeschlagen ist das Ziel, die unternehmensinternen Sicherheitsstandards durch Verschlüsselung zu erreichen. Dies könnte darauf hinweisen, dass der gesetzliche Mindeststandard als ausreichend angesehen wird.

Bei der Betrachtung der einzelnen Branchen erhoffen sich 68 Prozent der Banken und Assekuranzen durch die Datenverschlüsselung einen zuverlässigen Schutz vor Spionage und für 47 Prozent spielt die Verschlüsselung hinsichtlich der Einhaltung allgemeiner Sicherheitszertifikate eine wichtige Rolle. Ähnliches gilt für die Industrie, die sich durch den Einsatz von Verschlüsselungstechnologie zu je 57,4 Prozent vor staatlicher und industrieller Spionage schützen und die DSGVO einhalten möchte. Auffällig im Durchschnittswert und auch bei Betrachtung der Unternehmensgrößen und Branchen ist das niedrige Interesse daran, mit der Verschlüsselung die digitale Souveränität – beispielsweise in der Cloud – zu realisieren. Insgesamt nur 36,5 Prozent verfolgen dieses Ziel.

***www.eperi.com***




# Guter Bot, böser Bot

## BALANCEAKT ZWISCHEN SCHUTZ UND BENUTZERFREUNDLICHKEIT

Bot-Management spielt eine zentrale Rolle bei der Sicherung von Netzwerken und Anwendungen. Bots - automatisierte Programme, die eine Vielzahl von Aufgaben im Internet ausführen - sind sowohl nützlich als auch potenziell schädlich. Die Herausforderung besteht darin, nützliche Bot-Aktivitäten zu ermöglichen und gleichzeitig bösartige Bots abzuwehren.

Aktuelle Studien zeigen, dass fast die Hälfte des gesamten Internet-Traffics auf Bots zurückzuführen ist. Viele von ihnen erfüllen wichtige Funktionen, die das Internet nutzbar machen. Operations- und Sicherheitsteams können also nicht wahllos den gesamten Bot-Traffic blockieren, denn dies würde verhindern, dass gutartige Bots ihren Job erledigen können. Auch das kann negative Auswirkungen haben, denn gutartiger Bot-Traffic kann unter anderem das organische SEO-Ranking verbessern.

Leider sind bösartige, Bot-generierte Webanfragen, die es auf die Webanwendungen und APIs von Unternehmen abgesehen haben und sich Zugang zu Netzwerken verschaffen, inzwischen ebenfalls Normalität. Ein effektives Bot-Management kann hier nicht nur unerwünschte Aktivitäten blockieren, sondern auch legitime Bots erkennen und menschliche Nutzer schützen. Zwei wichtige Komponenten sind dabei maschinelles Lernen und Verhaltensanalyse.

Um legitime von schädlichen Bots zu unterscheiden, werden beispielsweise Muster und Anomalien im Datenverkehr analysiert. Regelmäßiges und vorhersehbares Verhalten deutet auf nützliche Bots wie Suchmaschinen-Crawler hin, während unregelmäßiges und erratisches Verhalten auf bösartige Bots schließen lässt. Durch die Festlegung von Schwellenwerten für normales Verhalten können verdächtige Aktivitäten identifiziert und Maßnahmen wie das Blockieren oder Beschränken des Zugriffs ergriffen werden. Dabei sollten Faktoren wie die Zeit zum Ausfüllen von Formularen, die Bildschirmauflösung, Mausbewegungen und die Verwendung von VPNs oder Proxies berücksichtigt werden.

**Positive Auswirkungen auf die Nutzererfahrung**

Durch das Herausfiltern bösartiger Bots wird die Last auf den Servern verringert, was zu schnelleren Ladezeiten führt. Auch die Sicherheit wird erhöht: Der Schutz vor automatisierten Angriffen wie Brute-Force-Login-Versuchen und Credential Stuffing sorgt dafür, dass Nutzer sicher mit der Anwendung interagieren können. Ein effektives Bot-Management optimiert die Ressourcenzuweisung, senkt die Bandbreitenkosten und schützt die Benutzerkonten vor illegalen Zugriffen.

**Die Zukunft des Bot-Managements**

Intelligente Bot-Management-Lösungen müssen die Auswirkungen auf legitime Nutzer minimieren und ein nahtloses Nutzererlebnis gewährleisten. So werden zunehmend adaptive und benutzerfreundlichere Überprüfungsmethoden zum Einsatz kommen, um zwischen Menschen und Bots zu unterscheiden, ohne die Benutzerinteraktionen zu unterbrechen. Diese bieten Sicherheitsmaßnahmen, die im Hintergrund ablaufen und so Reibungsverluste und Frustrationen verringern.

Nicht zuletzt werden Bot-Management-Lösungen von der Integration fortschrittlicher Threat-Intelligence-Plattformen profitieren. Diese ermöglichen Echtzeit-Überwachung, haben Zugriff auf umfassende Daten unterschiedlicher, gesicherter Quellen, bieten AI-unterstützte Analysen und können damit die Sichtbarkeit und die Erkennungsmöglichkeiten durch kollaborative Threat-Intelligence erheblich verbessern.

***www.fastly.com***


# Passwortlose Authentifizierung

## WAS BEDEUTET SIE FÜR DAS PRIVILEGED ACCESS MANAGEMENT?

Das Privileged Access Management (PAM) zielt darauf ab, die risikoreichsten Zugriffe in einem Unternehmen zu sichern, einschließlich der Verwendung von privilegierter Zugangsdaten wie Passwörtern oder SSH-Schlüsseln. Wie können sich nun PAM- und Identity-Security-Teams auf eine Zukunft ohne Passwörter vorbereiten?

Das Konzept der passwortlosen Authentifizierung ist zwar nicht neu, doch hat sich die Methode erst in den letzten Jahren durchgesetzt. Verschiedene Formen sind dabei zu unterscheiden, von physischen Authentifizierungsfaktoren wie USB-Schlüsseln bis hin zu digitalen Faktoren wie Passkeys. Jede Methode kann dazu beitragen, den Zugang eines Nutzers effizient zu validieren.

Doch trotz der Vorteile dieser Authentifizierungsformate kann die passwortlose Authentifizierung nicht die erforderliche Sicherung risikoreicher Zugriffe ersetzen. Sie verringert zwar das Risiko – aber sie können immer noch kompromittiert werden. Beispiele dafür sind Biohacking-Angriffe auf die biometrische Authentifizierung und der physische Diebstahl von Yubikeys. Phishing-resistente Passkeys sind zwar schwieriger zu entwenden als Passwörter, allerdings können Angreifer dennoch auf den Passkey-Speicher eines Geräts zugreifen und gültige Passkeys nutzen.

Unternehmen müssen folglich einen Defense-in-Depth-Ansatz verfolgen. Bewährte PAM-Konzepte wie Least Privilege, Session-Isolierung, Privileged Session Audit und Identity Threat Detection and Response (ITDR) bleiben Verteidigungsmaßnahmen, die das Risiko einer Identitätskompromittierung und einer Seitwärtsbewegung von Angreifern reduzieren.

**Ohne Passwörter geht es noch nicht**

Ohnehin verhindern derzeit mehrere betriebliche Erwägungen die vollständige Einführung der passwortlosen Authentifizierung. So sind für viele Systeme eines Unternehmens standardmäßig Passwörter erforderlich. Beispielsweise verfügt jedes Notebook, jeder Server und jedes vernetzte Gerät über ein integriertes lokales Administrator-Passwort. Diese Anmeldeinformationen sind die Hauptziele von Ransomware-Angriffen. PAM-Lösungen zielen darauf ab, diese Anmeldeinformationen zu entfernen und sie sicher in einem Tresor zu verwalten.

Auch die Nutzung von Shared-Accounts verhindert die flächendeckende Einführung einer passwortlosen Authentifizierung. Um ihre Angriffsfläche zu verringern oder Audit-Anforderungen zu erfüllen, versuchen viele Unternehmen, die Anzahl der Accounts mit Zugriff auf ihre kritischen Ressourcen zu reduzieren. Eine gängige Strategie ist dabei die Konsolidierung auf eine kleine Anzahl hoch-privilegierter Konten, die von mehreren IT- und Cloud-Operations-Nutzern gemeinsam verwendet werden. Diese Konten beruhen in der Regel auf gemeinsamem Wissen und erfordern deshalb wissensbasierte Authentifizierungsfaktoren wie Credentials. PAM-Lösungen können hier dann mehrere Layer von Kontrollen anwenden.

Darüber hinaus benötigt jedes Unternehmen in Cloud-Umgebungen ein gewisses Maß an Shared-Privileged-Access, da die Root- und Registrierungskonten, die zur Einrichtung einer Cloud-Umgebung erforderlich sind, niemals außer Betrieb genommen werden können. Diese Root-Account-Credentials werden immer vorhanden sein und müssen mit intelligenten Berechtigungskontrollen gesichert werden.

Selbst aus Compliance-Gründen kann eine Umstellung auf einen passwortlosen Prozess schwierig sein. Auditoren achten häufig auf eine umfassende Identitätssicherheit. Einige Vorschriften verlangen die Verwendung von Passwörtern und eine sorgfältige Kontrolle dieser, etwa durch die Implemen-

LOGICALIS
Architects of Change

itsa EXPO CONGRESS
HOME OF IT SECURITY
Stand 7A-402

# Security hat viele Gesichter

## Wir haben die Experten

- **Multi Vendor Security**
- **End to End Protection**
- **Managed Services**

www.logicalis.de

tierung von Least Privilege, Multi-Faktor-Authentifizierung (MFA) oder richtlinienbasierter Rotation von Anmeldedaten. Eine vollständige Eliminierung von Passwörtern kann folglich Audit-Prozesse erschweren und verzögern. Nicht zuletzt dienen Passwörter in Notfallsituationen als verlässliche Fallback-Authentifizierungsmethode, wenn passwortlose Optionen versagen.

**Wichtige Berechtigungskontrollen für eine passwortlose Welt**

Selbst wenn es irgendwann gelingen sollte, den passwortbasierten Zugang überflüssig zu machen, sind für privilegierte Zugriffe mit hohem Risiko weiterhin verstärkte Kontrollen erforderlich. Dazu zählt zunächst die Umsetzung des Least-Privilege-Prinzips. Durch die Einschränkung von Berechtigungen für Identitäten, die sich ohne Passwörter authentifizieren, können Unternehmen die Gefahr von Seitwärtsbewegungen der Angreifer reduzieren. Least Privilege ist ein wesentliches Element einer Zero-Trust-Strategie in der Identitätssicherheit. Auch eine Session-Isolierung ist erforderlich. Schließlich ist eine Welt ohne Passwörter immer noch von Ransomware und anderen Malware-Formen bedroht. Der Einsatz von Proxy-Servern zur Isolierung hoch-privilegierter Sitzungen verhindert, dass durch Malware kompromittierte Geräte auf Unternehmensressourcen zugreifen können. Darüber hinaus sind ein Session-Audit und Screen-Recording empfehlenswert. Prinzipiell sollten Unternehmen hoch-riskante Benutzeraktivitäten immer überprüfen und potenzielle Sicherheitsvorfälle untersuchen. Um die Effizienz von Audits zu optimieren, benötigen sie dabei eine zentrale Sicht auf Endnutzer-Sessions über Systeme, Cloud-Workloads und -Services sowie Webanwendungen hinweg.

Zwei weitere essenzielle Kontrollmaßnahmen betreffen die Themen ITDR und Zero-Standing-Privileges (ZSP). Auch in einer passwortlosen Umgebung müssen Sicherheitsteams immer noch bösartige oder anomale Verhaltensweisen erkennen, die auf laufende Angriffe hindeuten könnten. ITDR-Funktionen von führenden Anbietern für Identitätssicherheit können mithilfe von KI und Maschinellem Lernen bekannte Indikatoren für böswillige Zugriffe erkennen und Vorfälle an ein Security Operations Center (SOC) zur automatischen Reaktion weiterleiten. Nicht zuletzt sollten Unternehmen die Sicherheitsrisiken nach einer erfolgten passwortlosen Authentifizierung berücksichtigen. Dabei geht es darum, den Aktionsradius möglicher Angreifer zu verkleinern. Hier bietet sich eine ZSP-Strategie an, auf deren Basis Berechtigungen spontan erstellt und zugewiesen sowie nach der Verwendung wieder entfernt werden, wobei die entscheidenden Einstellungen wie Zeit und Dauer, Entitlements und Genehmigungen genau kontrolliert werden.

SELBST WENN ES IRGENDWANN GELINGEN SOLLTE, DEN PASSWORTBASIERTEN ZUGANG ÜBERFLÜSSIG ZU MACHEN, SIND FÜR PRIVILEGIERTE ZUGRIFFE MIT HOHEM RISIKO WEITERHIN VERSTÄRKTE KONTROLLEN ERFORDERLICH.

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

Es steht außer Frage, dass Passwörter für jedes Unternehmen ein hohes Sicherheitsrisiko darstellen. Folglich liegt die passwortlose Authentifizierung derzeit im Trend. Dabei darf aber nicht außer Acht gelassen werden, dass auch die passwortlose Authentifizierung mit Risiken verbunden ist. Letztlich gewährleistet aber nur eine vollständig integrierte Identity-Security- und Zero-Trust-Strategie eine zuverlässige Gefahrenabwehr – selbst in der passwortlosen Welt.

***Sam Flaster***


# Mit infodas wertvolle Daten in Kritischen Infrastrukturen schützen

## SDOT INDUSTRY GATEWAY: DAS FLEXIBLE CYBERSICHERHEITS-TOOL

Die heutige vernetzte Welt entwickelt sich zunehmend als Zielscheibe für Cyberkriminelle und die Auswirkungen der Angriffe gewinnen immer mehr an Tragweite. Besonders für Kritische Infrastrukturen und gefährdete industrielle Sektoren nimmt die Bedrohungslage zu.

Basierend auf der SDoT Produktfamilie von infodas, die seit vielen Jahren erfolgreich im Verteidigungssektor eingesetzt wird, wurde das SDoT Industry Gateway für die spezifischen Anforderungen im Bereich Kritische Infrastrukturen entwickelt. Das Hochleistungsprodukt bietet dem privaten Sektor einen umfassenden Cybersecurity-Schutz mit variablen Einsatzmöglichkeiten und höchsten Zertifizierungslevels.

infodas vereint langjähriges Know-how in der Cybersecurity-Branche mit einem umfassenden und zertifizierten Produkt- und Beratungsportfolio zum effektiven Schutz Ihrer sensiblen, digitalen Strukturen. Die 50-jährige Expertise aus der Absicherung komplexer Kommunikations- und Datenströme im Bereich der Bundeswehr und Verteidigungsindustrie haben wir komplett auf die spezifischen Anforderungen von Kritischen Infrastrukturen angewandt. Wir stehen Ihnen als zertifizierter und vertrauenswürdiger Partner zur Seite und unterstützen Sie dabei, branchenspezifische regulatorische Anforderungen gemäß IEC 62443, NIST oder Common Criteria sowie vielen weiteren Standards zu erfüllen.

***www.infodas.com***

**it-sa Expo&Congress**
Besuchen Sie uns
in **Halle 7-131**
infodas

---

# Mit Kunst gegen Cyberkriminalität

## KOMPLEXE SACHVERHALTE LEBENDIG MACHEN

WithSecure (ehemals F-Secure Business) will die abstrakte Welt der Cyber-Sicherheit mit der geplanten Eröffnung des „Museum of Malware Art" in eine zugängliche und faszinierende Erfahrung verwandeln. Diese neue Initiative zielt darauf ab, die Kluft zwischen komplexen technischen Themen und der allgemeinen Bevölkerung durch fesselnde und lehrreiche Kunstinstallationen zu überbrücken. Das Museum soll im November 2024 im neuen Hauptsitz von WithSecure in Wood City, Helsinki, eröffnet werden.

**Cyber-Sicherheit greifbar machen**

Das „Museum of Malware Art" will Kunstwerke zeigen, die von realen Cyber-Bedrohungen inspiriert sind und technische Daten in nachdenklich stimmende Exponate verwandeln. Kuratiert von Mikko Hyppönen, Branchenveteran und Chief Research Officer von WithSecure, sowie einem Team von Cyber-Sicherheitsforschern, Threat Intelligence Experten und Kreativen, präsentiert das Museum prominente Malware in künstlerischer Form. WithSecure lädt die Öffentlichkeit ein, zu einem der Exponate beizutragen: Einer Skulptur, die aus gespendeten Computermäusen besteht.

„Cyber-Sicherheit ist eine kollektive Verantwortung. Unser Ziel ist es, sie zu entmystifizieren und für jeden greifbar zu machen", sagt Mikko Hyppönen. „Indem wir Cyber-Bedrohungen in Kunst verwandeln, hoffen wir, ein tieferes Verständnis und Bewusstsein zu fördern. Wir glauben, dass wir mit unserem Museum Cyber-Bedrohungen sichtbarer und zugänglicher machen können, um so viele Menschen zu Aktionen und zur Zusammenarbeit im Kampf gegen Cyberkriminalität zu inspirieren."

***www.withsecure.com***

**Sauber definierte Schnittstellen in komponentenbasierten Softwarearchitekturen dienen der Sicherheit und Robustheit. Sie sind Teil des Security-by-Design-Ansatzes, den genua für seine IT-Security-Produkte seit jeher verfolgt.**

Foto: genua GmbH

# Cyber Resilience Act

## DARAUF MÜSSEN HERSTELLER UND ZULIEFERER ACHTEN

Die EU erhöht den Druck auf Hersteller digitaler Produkte: Der Cyber Resilience Act (CRA) verlangt unter anderem dokumentierte Software-Stücklisten, längere Update-Zeiträume und erweitert den Haftungsrahmen. Das hat nicht zuletzt beim allgegenwärtigen Einsatz von Open-Source Konsequenzen.

Der Cyber Resilience Act (CRA) der Europäischen Union war bereits für Anfang 2024 geplant und wird voraussichtlich noch diesen Sommer in Kraft treten. Als Verordnung wird er unmittelbar mit dem Beschluss wirksam werden.

Mit seinen Forderungen nach mehr Software-Sicherheit, Mindest-Support-Lebenszyklen, mehr Transparenz für digitale Produkte und erweiterter Haftung für die Hersteller stößt er kaum auf Widerstand, bei dem die Stoßrichtung des CRA grundlegend abgelehnt würde. Trotzdem gibt es bis zu seiner endgültigen Fassung noch Diskussionsbedarf – etwa darüber, wer Hersteller ist, welche Pflichten für wen gelten und wer am Ende haftet. Vor allem die Open-Source-Community hatte in den vergangenen Monaten noch Nachbesserungen gefordert.

### Die Lieferkette unter Kontrolle bringen

Eine der zentralen Forderungen ist, dass Hersteller von Produkten, die direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden sind, prüfen und dokumentieren müssen, welche Fremdkomponenten in ihren Erzeugnissen zum Einsatz kommen. Dazu dienen sogenannte „Software Bill of Materials" (SBOM). Wie die Dokumentation praktisch erfolgen soll, hat das BSI für deutsche Hersteller in der Richtlinie TR-03183-2 beschrieben.

Der Nutzen liegt auf der Hand: Mit nur einem Blick können Hersteller, Anwender und auch zentrale Stellen erkennen, welche Produkte von neu entdeckten Schwachstellen betroffen sind; eine wichtige Voraussetzung, um eigene Lieferketten besser kontrollieren zu können. Verbunden mit den Pflichten, Sicherheits-Updates zur Verfügung zu stellen, ist auch klar, welcher Hersteller in der Pflicht ist, entsprechend nachzubessern.

Was in der Theorie gut und sinnvoll klingt, kann in der Praxis zu Problemen führen. Softwareabhängigkeiten etwa haben eine große Tragweite. Fremdkomponenten verwenden ihrerseits wieder andere Komponenten und so fort. Das Netz der Abhängigkeiten gewinnt schnell an Tiefe und Breite und die Wahrscheinlichkeit ist hoch, dass irgendwo außerhalb des Sichtbereichs Komponenten in das eigene Produkt Einzug gehalten haben, die weder dokumentiert noch geprüft wurden.

Um die Sicherheit seiner Software gewährleisten zu können, darf man sich nicht nur auf Zusagen seiner Zulieferer und Quellen verlassen. Ein Hersteller

muss in der Lage sein, selbst die Lieferkette zu durchleuchten und in der Tiefe bestimmen zu können, welche Komponenten tatsächlich aus welcher Quelle kommen, welche Sub-Sub-Sub-Komponenten gegebenenfalls nicht mehr supportet werden und welche Sicherheitsrisiken damit verbunden sein könnten.

**Konsequentes Security by Design ist gefragt**

Darüber hinaus muss ein Hersteller auch in der Lage sein, auf Probleme zu reagieren. Das eigene Produkt sollte so designed sein, dass Programmkomponenten isoliert sind, dass geschirmte Bereiche existieren und Komponenten nur über definierte Schnittstellen kommunizieren können. Dadurch lassen sich Übergänge und Kontrollmöglichkeiten klar definieren und einzelne Komponenten zum Beispiel über Sandboxen zusätzlich isolieren. Im Kontext von CRA und Security by Design dient ein solcher Aufbau der Sicherheit und Robustheit.

Auf der proaktiven Seite schafft der CRA verbesserte Möglichkeiten, um Abhängigkeiten und damit die Risiken von Fremdkomponenten zu bewerten und im Vorfeld Risiken zu minimieren. Aber sowohl das Design der Software als auch die Prozesse, die Auswahl und Einbinden von Fremdkomponenten leiten, lassen sich nicht mit vertretbarem Aufwand nachträglich implementieren, um CRA-Compliance zu erreichen. Es müssen Prinzipien sein, die sich in der DNA des Herstellers und in der DNA des Produkts wiederfinden lassen.

Hinzu kommt, dass die Selbstverpflichtung für das benötigte CE-Kennzeichen bei kritischen Infrastrukturen und sicherheitsrelevanten Komponenten nicht mehr ausreichen wird. Bei besonders kritischen Systemen ist dann zwingend eine dritte Partei für die Zertifizierung erforderlich.

Spätestens dann müssen Hersteller nachweisen können, wie sie die Sicherheit ihrer Produkte tatsächlich umsetzen. Security by Design, Maintainability, Availability und Monitoring schon im Produktdesign und im Entwicklungsprozess zu verankern ist letztlich nicht nur ein Sales-Argument für sicherheitsbewusste Käufer, sondern essenziell, um den Marktzugang nicht zu verlieren.

**Der Umgang mit Open Source**

Die Option eines Unternehmens, auf Open-Source in seinen Produkten zu verzichten, ist kaum realisierbar. Selbst wenn dies im eigenen Unternehmen gelingt, wird es schwer sein, Auftragnehmer zu finden, die ihrerseits sich dazu verpflichten wollen. Laut verschiedenen Studien beinhalten zwischen 80 und 90 Prozent aller digitalen Lösungen Open-Source-Komponenten.

Mit Blick auf Lieferketten und CRA wirft Open-Source zwei Probleme auf: Erstens sind nicht-gewinnorientierte Akteure von der Haftung ausgenommen und zweitens gibt es einige Open-Source-Komponenten, die weit verbreitet sind.

Sicherheitslücken in Komponenten wie Log4j oder jüngst OpenSSH und XZ für Linux verdeutlichen die Gefahr, die so auch für proprietäre Software besteht: Mehr als ein Jahr nach Schließung der Log4j-Schwachstelle waren fast 40 Prozent aller Systeme immer noch betroffen. Ein Grund dafür ist sicherlich die bislang mangelnde Haftung für solche Sicherheitslücken. Systeme werden teils wider besseres Wissen aus Kostengründen nicht gepatcht. Der CRA könnte sich hier positiv auswirken. Ein zweiter Grund ist, dass das Vorhandensein dieser kompromittierten Libraries dem Inverkehrbringer – in der Regel also dem Softwarelieferanten – gar nicht bekannt ist. Die Wahrscheinlichkeit, dass irgendwo in der Lieferkette Komponenten wie Log4j eingebunden sind, ist hoch, die Wahrscheinlichkeit, dass dies bislang dokumentiert wurde, jedoch gering.

Nun gibt es aber gegenüber Open-Source-Akteuren weder Haftungsansprüche noch Nachbesserungspflichten. Es wäre auch nur schwer verständlich, wenn ein Programmierer in seiner Freizeit frei verfügbaren, nicht kommerziellen Code veröffentlicht und im Anschluss dafür haften muss, wenn ein Unternehmen damit Profit erzielen möchte. Die Python Software Foundation hatte damit gedroht, sich komplett aus dem europäischen Markt zurückzuziehen, wenn der CRA bei den Ausnahmeregelungen für Open Source nicht nachgebessert würde.

Dies bedeutet im Umkehrschluss wiederum mehr Verantwortung für die Hersteller. Denn sie müssen ihre Lieferkette in der Tiefe durchleuchten können, um eben auch die vermeintlich unkritischen, millionenfach verwendeten und mit einem Click eingebundenen Libraries im Auge zu behalten und sie müssen im Zweifel auch die eigene Kompetenz besitzen, Schwachstellen in Open-Source-Komponenten zu beheben.

***Vanitas Berrymore***

FÜR HERSTELLER BEDEUTET DER CRA HÖHERE ANFORDERUNGEN AN DIE SICHERHEIT IHRER PRODUKTE. FÜR KUNDEN WENIGER RISIKEN BEI DER DIGITALISIERUNG.

**Steffen Ullrich, IT-Sicherheitsforscher, genua GmbH, www.genua.de**

# IT-Sicherheitsteams unter Cyberstress

## VERBESSERTE CYBERSICHERHEIT DURCH PLATTFORMLÖSUNGEN UND EXTERNE HILFE


Die Verantwortlichen für Cybersicherheit stehen unter Druck und das hat Folgen: 76,6 Prozent der deutschen IT-Sicherheitsexperten planen laut Bitdefender Cyber Security Assessment Report 2024 in den kommenden zwölf Monaten einen Jobwechsel – ein Anstieg um mehr als das Doppelte im Vergleich zu 30,9 Prozent in 2023. Alarm-Müdigkeit, operativer Mehraufwand, Überstunden, Wochenendarbeit, interner Druck sowie die hohe Frequenz komplexer Angriffe erhöhen den Stress für jeden Einzelnen. Konsolidierende Plattformtechnologien und externe Expertise können helfen.

Die Überlastung hat viele Gründe. Diese reichen von ineffizienten Prozessen bis hin zu einer komplexen, dynamisch wachsenden Angriffsfläche. Zugleich verursachen verschiedene Tools mit einer großen Menge an Informationen – und auch vielen False Positives – schnell Bearbeitungsstau und ein Gefühl der Machtlosigkeit. Das Arbeitsaufkommen erfordert ein hohes Maß an Überstunden. Laut dem Bitdefender-Report leisteten 77,1 Prozent der deutschen Befragten im vergangenen Jahr Wochenendarbeit.

DIE ZUNEHMENDE BELASTUNG IM CYBERSICHERHEITSBEREICH VERDEUTLICHT DEN DRINGENDEN BEDARF AN BESSEREN TOOLS UND STRATEGIEN.

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

Angreifer werden immer raffinierter und selbst wenig versierte Kriminelle können heute mit generativer KI anspruchsvolle Attacken ausführen. Hinzu kommt der steigende interne Druck auf die IT-Sicherheit. Da ein gezielter Angriff Kundendaten kompromittieren oder verschlüsseln sowie Geschäftsprozesse zum Erliegen bringen kann, stehen Cybersicherheitsteams besonders im Fokus der Chefetage. CEOs fürchten im Fall eines Sicherheitsvorfalles, für diesen verantwortlich gemacht zu werden und suchen ihrerseits nach Verantwortlichen.

**Verstärkung an Bord holen**

Plattformtechnologien zum Überwachen und Verwalten der IT-Sicherheit sind in der Lage, die Gefahrenlage ganzheitlich zu erkennen, Aufgaben zu automatisieren, Arbeitsabläufe zu rationalisieren und Probleme schneller zu beheben. Sie machen es möglich, Cyberresilienz effizient und sicher abzubilden. Zusammen mit Managed Security Service Providern (MSSPs) können diese Technologien die IT deutlich entlasten und gleichzeitig die Unternehmenssicherheit verbessern.

Extended-Detection-and-Response (XDR)-Plattformen überwachen die gesamte IT-Infrastruktur und konsolidieren die Informationen verschiedener Monitoring Tools in komplexen IT-Landschaften in einem einzigen Dashboard. Mithilfe von KI analysieren diese Tools Threat Intelligence Feeds, bieten visualisierte Einblicke zu den Vorfällen und geben Sicherheitsteams nachvollziehbare Hinweise für die nächsten Schritte. So erkennen die Anwender Gefahren rasch und können sie frühzeitig beseitigen.

Darüber hinaus können MSSPs angesichts des Fachkräftemangels und beschränkter Unternehmensressourcen mit ihren Experten, deren Fachwissen und ihrer Routine im Umgang mit den aktuellen, anspruchsvollen Attacken interne Sicherheitsteams erheblich unterstützen. Vor allem stehen sie rund um die Uhr und auch an Wochenenden bereit und verfügen nicht zuletzt über die nötigen und stets aktuellen Tools.

Die zunehmende Belastung im Cybersicherheitsbereich verdeutlicht den dringenden Bedarf an besseren Tools und Strategien. Die Integration fortschrittlicher Technologien und eine Zusammenarbeit mit erfahrenen MSSPs können einen Großteil des Arbeitsstresses von Sicherheitsteams reduzieren. Diese Lösungen rationalisieren nicht nur die Prozesse und optimieren das Erkennen und die Abwehr, sondern fördern damit auch ein gesünderes Arbeitsumfeld.

***Jörg von der Heydt***


# KRITIS-Konferenz protekt

## DIE EINZIGE IHRER ART

Die protekt ist DIE Plattform für Cyber- und Informationssicherheit sowie physischen Schutz von kritischen Infrastrukturen in Deutschland. Vom 6. bis 7. November finden sich mehr als 450 Experten, KRITIS-Betreiber aus allen Sektoren, die Sicherheitsindustrie und Vertreter aus Bund, Ländern und Kommunen zusammen, um gemeinsam zu diskutieren.

Das Konferenzprogramm der protekt wird noch vielfältiger. So wird es in Ergänzung zu den bewährten Themen Cyber- und Informationssicherheit, physischer Schutz, Workshops, Praxisberichte aus dem UP KRITIS und KRITIS und Kommunen drei zusätzliche Programmblöcke geben: In Zusammenarbeit mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe wird es erstmals einen neuen Vortragsstrang „KRITIS und Zivile Verteidigung" geben.

Um das KRITIS Dachgesetz und die NIS2–Umsetzung geht es im Vortragsstrang „Onboarding neue gesetzliche Grundlagen bei KRITIS". Am zweiten Konferenztag werden im Themenblock „Young Professionals" wissenschaftliche Arbeiten aus dem KRITIS-Bereich vorgestellt. Das hochkarätige Plenum überzeugt mit Prof. Thomas Popp, von der Sächsischen Staatskanzlei, Dr. Jessica Däbritz vom Bundesministerium des Innern und für Heimat, Claudia Plattner, Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik, Ralph Tiesler, Präsident des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe und Sabine Lackner, Präsidentin der Bundesanstalt Technisches Hilfswerk.

***www.protekt.de***

**Tickets für die protekt** in der zentral gelegenen KONGRESSHALLE am Zoo Leipzig sind ab sofort online erhältlich.

**protekt**
**6.–7.11.2024**
leipzig

konferenz für den schutz kritischer infrastrukturen

# ANONYM & SICHER IM INTERNET MIT LINUX

## DER PRAXISEINSTIEG FÜR MEHR SICHERHEIT UND DATENSCHUTZ


**Anonym & sicher im Internet mit Linux:** Der Praxiseinstieg für mehr Sicherheit und Datenschutz; Robert Gödl; mitp Verlags GmbH & Co.KG; 09-2024

In diesem Buch lernen Sie alle Grundlagen, die Sie brauchen, um anonym im Internet zu surfen sowie Ihre Privatsphäre und Ihre Daten zu schützen. Da Linux als Betriebssystem ein hohes Maß an Kontrolle und Sicherheit bietet, erhalten Sie eine umfassende Einführung in die Installation, Konfiguration und tägliche Nutzung von Linux Mint. Auch die Verwendung des Terminals wird leicht verständlich erläutert.

Egal ob beim Surfen, Versenden von E-Mails oder Übertragen von Dateien – überall sind Unternehmen und böswillige Hacker auf Ihre Daten aus. Anhand leicht verständlicher Schritt-für-Schritt-Anleitungen lernen Sie, wie Sie Ihr System mit einer Firewall und zusätzlichen Tools absichern, Ihre Daten und E-Mails verschlüsseln, privat surfen, eine sichere VPN-Verbindung herstellen, eine eigene private Cloud betreiben und vieles mehr.

Ein Mindestmaß an Sicherheit ist bereits mit geringem Aufwand und wenigen Tools zu erreichen. Für alle, die höhere Anforderungen an die Sicherheit haben, bietet dieses Buch außerdem fortgeschrittene Techniken wie die Verwendung von Proxy-Servern, um den eigenen Standort zu verschleiern sowie die Nutzung sog. virtueller Maschinen und des Tor-Netzwerks.

# KRITIS-Unternehmen müssen jetzt handeln

## SYSTEME ZUR ANGRIFFSERKENNUNG

KRITIS-Unternehmen (Betreiber kritischer Infrastrukturen) sind besonders betroffen von Auswirkungen durch Cyberangriffe – denn sie sind für das Gemeinwohl einer Gesellschaft verantwortlich. Bereits seit über einem Jahr sind KRITIS-Unternehmen deshalb dazu verpflichtet, den Einsatz von Systemen zur Angriffserkennung (SzA) gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachzuweisen. Trotz dieser Vorgaben zeigt eine aktuelle Statistik des BSI, dass viele Unternehmen die Anforderungen noch nicht erfüllen können, somit nicht angemessen auf Cyberangriffe vorbereitet sind. Dabei gibt es bereits einfach umzusetzende Lösungen, die alle regulatorischen Anforderungen erfüllen – eine Einordnung.

190 Störungen wurden dem BSI im zweiten Quartal 2024 von KRITIS-Unternehmen gemeldet. Dazu zählen die Branchen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Siedlungsabfallentsorgung. Durch ihre Bedeutung für das Gemeinwesen sind diese Unternehmen besonders schützenswert. Deshalb sind Betreiber kritischer Infrastrukturen gesetzlich verpflichtet, gegenüber dem BSI oder der Bundesnetzagentur nachzuweisen, dass ihre IT- und OT-Sicherheit dem aktuellen Stand der Technik entspricht.

Dazu zählt ein funktionierendes Informationssicherheitsmanagementsystem (ISMS) sowie ein Business Continuity Management System (BCMS). Seit dem 1. Mai 2023 müssen betroffene Unternehmen gemäß IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) zudem den Einsatz von Systemen zur Angriffserkennung gegenüber dem BSI nachweisen. In der Praxis wird dies allerdings laut BSI-Statistik von Mai 2024 noch nicht umgesetzt. Die Mehrzahl der betroffenen Unternehmen ist derzeit erst dabei, ein Konzept zur Umsetzung der Anforderungen aufzusetzen. Dabei müssen KRITIS-Betreiber gemäß BSI Orientierungshilfe mindestens Umsetzungsgrad 3 oder 4 erreichen – doch was hat es eigentlich mit den Umsetzungsgradmodellen auf sich?

GERADE BEI MITTELSTÄNDISCHEN KRITIS-BETREIBERN SIND SYSTEME NÖTIG, DIE EINE EINFACHE INSTALLATION, KONFIGURATION UND HANDHABE ERMÖGLICHEN.

**Steffen Heyde,**
**Leiter Marktsegmente, Division Industry,**
**secunet Security Networks AG**
**www.secunet.com**

**Exkurs: Umsetzungsgradmodelle und ihre Bedeutung**

Um zu beurteilen, wie weit die organisatorischen und technischen Maßnahmen in der geprüften kritischen Infrastruktur fortgeschritten sind, nutzen Auditoren und Prüfer ein vom BSI definiertes Umsetzungsgradmodell. Das Ziel dieses Modells ist es, die Umsetzung der Systeme zur Angriffserkennung zu messen und einen definierten Mindeststandard bei KRITIS-Betreibern zu erreichen. Die BSI-Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung definiert für die notwendigen Nachweise gemäß § 8a Absatz 3 BSIG und § 11 Absatz 1e EnWG fünf Umsetzungsgrade:

- **Umsetzungsgrad 0:** Es sind bisher keine Maßnahmen zur Erfüllung der Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Maßnahmen.
- **Umsetzungsgrad 1:** Es bestehen Planungen zur Umsetzung von Maßnahmen zur Erfüllung der Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen.
- **Umsetzungsgrad 2:** In allen Bereichen wurde mit der Umsetzung von Maßnahmen zur Erfüllung der Anforderungen begonnen. Es sind noch nicht alle MUSS-Anforderungen erfüllt worden.
- **Umsetzungsgrad 3:** Alle MUSS-Anforderungen wurden für alle Be-

reiche erfüllt. Idealerweise wurden SOLLTE-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert oder ist in Planung.

- **Umsetzungsgrad 4:** Alle MUSS-Anforderungen wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen wurden erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
- **Umsetzungsgrad 5:** Alle MUSS-Anforderungen wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen und KANN-Anforderungen wurden für alle Bereiche erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse/Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

Während eines Audits wird auf Basis dieser Definitionen eine Bewertung der Umsetzung bei dem jeweiligen Betreiber geprüft.

**Angriffserkennung mit System: secunet monitor KRITIS**

Gerade bei mittelständischen KRITIS-Betreibern sind Systeme nötig, die eine einfache Installation, Konfiguration und Handhabe ermöglichen – und das ohne tiefgehendes Know-how zu Bit und Bytes, geschweige denn Forensik-Kenntnissen bei einem Cyberangriff.

secunet hat genau zu diesem Zweck secunet monitor KRITIS entwickelt. Das Monitoring-System setzt die regulatorischen Anforderungen an die Angriffserkennung auf Netz- und Systemebene um und lässt sich einfach bedienen. Es nutzt eine signaturbasierte Angriffserkennung, um den Schutz von IT- und OT-Infrastrukturen zu gewährleisten. Dabei erfüllt secunet monitor KRITIS die technisch umsetzbaren MUSS- und SOLLTE-Anforderungen, die das BSI in seiner Orientierungshilfe zum IT-SiG 2.0 festlegt und unterstützt Unternehmen dabei, mehr Transparenz im IT- und OT-Netzwerk zu schaffen – und das mit dem Umsetzungsgrad 4.

**KRITIS sind erst der Anfang: Cybersicherheit braucht jedes Unternehmen**

Systeme zur Angriffserkennung kombinieren fortschrittliche technische Funktionen mit organisatorischen Maßnahmen, um einen umfassenden Schutz vor Cyberangriffen zu gewährleisten – und den sollten nicht nur KRITIS-Unternehmen haben. Denn Angreifer machen auch vor anderen Wirtschaftszweigen keinen Halt. Ein zuverlässiges SzA erhöht die allgemeine Sicherheit und trägt dazu bei, die Wertschöpfung zu schützen. Mit Systemen zur Angriffserkennung wie secunet monitor KRITIS lassen sich Cyberangriffe frühzeitig erkennen und Schäden minimieren. Denn sie können beispielsweise verhaltensbasierte Anomalien und verdächtige Aktivitäten im Netzwerk identifizieren, bevor diese zu größeren Sicherheitsvorfällen führen. Es gilt, Maßnahmen zu ergreifen und die notwendigen Systeme zur Angriffserkennung zu implementieren. Nur so können Unternehme ihr Business sichern und ihre Resilienz gegenüber Cyberangriffen steigern.

***Steffen Heyde***

# Der SD-WAN-Transformationsguide

## WIE DIE MIGRATION REIBUNGSLOS VERLÄUFT

BEVOR UNTERNEHMEN MIT DER MIGRATION IHRER NETZWERKE AUF SD-WAN BEGINNEN, SOLLTEN SIE ZUNÄCHST EINE INVENTUR DER BESTEHENDEN INFRASTRUKTUR VORNEHMEN.

**Marcel Stadler, Product Manager SD-WAN, Open Systems**
**www-open-systems.com/de/**

Software-definierte Wide Area Networks sind genau das richtige Fundament für KI und IoT (Internet of Things)-Umgebungen. Doch auch wenn Unternehmen gerne einfach den sprichwörtlichen Schalter umlegen würden, bedarf es guter Planung und Kommunikation sowie fundiertem Verständnis der internen Anforderungen für eine erfolgreiche Netzwerktransformation.

SD-WANs versprechen vereinfachtes und günstigeres Netzwerkmanagement, optimierten Cloud-Zugang, mehr Sicherheit und eine bessere Nutzererfahrung. Um eine reibungslose Umsetzung zu gewährleisten, ist jedoch sorgfältige Planung erforderlich. Bevor Unternehmen mit der Migration ihrer Netzwerke auf SD-WAN beginnen, sollten sie zunächst eine Inventur der bestehenden Infrastruktur vornehmen. Neben einer Analyse der Netzwerk- und Sicherheitsanforderungen gehört dazu auch eine Evaluierung der aktuellen Systeme und Dienste. Ziel ist es, notwendige Änderungen zu identifizieren, die Vorteile für die Umsetzung von strategischen IT-Projekten bringen. Wichtige Aspekte der IT-Infrastruktur wie kritische Anwendungen, Standortklassifizierungen oder Legacy-Systeme gehören dabei ebenfalls auf den Prüfstand.

Um keinen Flickenteppich an Regeln und Richtlinien nach der Einführung einer SD-WAN-Infrastruktur aufarbeiten zu müssen, sollten Unternehmen zudem bereits vor der praktischen Migration einheitliche Standards für alle Standorte festlegen. Sie müssen die Muster der Kommunikation über das Netzwerk, Bandbreite und mögliche Einschränkungen berücksichtigen, die für jeden Standort gelten.

**Planung, Praxis, Prüfung**

Da selten alles auf einmal funktioniert, ist es wichtig, nach der Inventur und der Definition von Standards eine strukturierte und realistische Roadmap aufzustellen. Sie ist die Grundlage dafür, die Umstellung auf SD-WAN nicht nur möglichst schnell, sondern auch effizient durchzuführen. Dabei sollten Unternehmen insbesondere die Vorlaufzeiten der Internetprovider für das Provisionieren von Internetanschlüssen und andere zeitliche Einschränkungen berücksichtigen. Auch wichtig ist, die Implementierung neuer Netzwerkkomponenten schrittweise durchzuführen. So können Administratoren einen reibungslosen Übergang sicherstellen und Ausfallzeiten minimieren.

Nach der intensiven Planungsphase folgt logischerweise die praktische Umsetzung: Es ist an der Zeit, die neue SD-WAN-Infrastruktur zu implementieren und die Umschaltung von der alten Lösung vorzunehmen. Diese Schritte erfordern eine gute Koordination zwischen den zentralen und lokalen IT-Teams sowie dem SD-WAN-Anbieter, um Downtimes und Netzwerkausfälle zu minimieren sowie eine nahtlose Integration zu gewährleisten. Das Testen der neuen Umgebung vor, während und nach der Migration stellt sicher, dass alle Systeme reibungslos funktionieren. Doch auch bei noch so sorgfältiger Planung und gewissenhaftem Testings kann es während des Transformationsprozesses zu Herausforderungen kommen. Das an sich ist tolerierbar, sofern Unternehmen sie frühzeitig identifizieren und die notwendigen Anpassungen vornehmen.

Zu guter Letzt ist es wichtig, dass die Projektleitung eine offene Kommunikation mit allen Beteiligten und Stakeholdern etabliert. Nur so wird keiner übergangen und nichts übersehen. Zudem ist Flexibilität entscheidend, um die Migration zu SD-WAN erfolgreich umzusetzen. Sind all diese Dinge erfüllt und berücksichtigt steht einem zukunftssicheren Netzwerkbetrieb nichts mehr im Wege.

***Marcel Stadler***

# Precision AI

## CYBERSICHERHEIT IN ECHTZEIT

Künstliche Intelligenz (KI) treibt schon seit über einem Jahrzehnt die Produktivität in Unternehmen voran – häufig im Hintergrund. Durch die Einführung von generativer KI ist sie den meisten Mitarbeitern ein Begriff und auch in deutschen Firmen gewinnt KI an Bedeutung: Laut einer Erhebung des Statistischen Bundesamtes nutzte Ende 2023 jedes achte Unternehmen künstliche Intelligenz.

Die schnelle Verbreitung von KI in Unternehmen birgt aber auch viele Sicherheitsrisiken, darunter Datenlecks, die Preisgabe von vertraulichen Informationen oder Reputationsrisiken.

KI revolutioniert nicht nur die Geschäftswelt, sondern auch Angriffe, die sich gegen uns richten. Cyberkriminelle kennen und nutzen die Vorteile von KI, um Unternehmen in kürzerer Zeit mit authentischeren Angriffen zu attackieren. Durch immer neue Methoden gewinnt die Cyberlandschaft an Komplexität.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) zeigt in seinem Bericht zur Lage der IT-Sicherheit in Deutschland auf, dass täglich eine Viertelmillion neue Schadsoftware-Varianten und 21.000 infizierte Systeme verzeichnet werden. Dazu kommen mehr als 2.000 Schwachstellen in Softwareprodukten pro Monat.

Die aktuellen Abwehrmechanismen reichen nicht mehr aus, um Unternehmen ausreichend zu schützen. Damit sie mit Angreifern mithalten können, sind KI-gestützte Technologien unabdingbar. Precision AI von Palo Alto Networks ist die nächste Generation der künstlichen Intelligenz, die speziell für die Cybersicherheit entwickelt wurde.

### Abwehr von Cyberangriffen durch Precision AI

Das proprietäre KI-System kombiniert die Vorhersagegenauigkeit von maschinellem Lernen (ML) und Deep Learning, und automatisierte Abwehrmaßnahmen mit der Zugänglichkeit von generativer KI. Precision AI wurde in alle bestehenden und neuen Funktionalitäten integriert, um Unternehmen bei der Bekämpfung neuartiger Bedrohungen zu unterstützen. Copilots für die Plattformen Strata (Netzwerk), Prisma (Cloud) und Cortex (Security Operations) ermöglichen einen besseren Einblick in die Sicherheitsdaten des Unternehmens und dadurch einen besseren Schutz. Precision AI vereinfacht Abläufe, ohne sich negativ auf die Cybersecurity auszuwirken.

Der Schlüssel für gute KI-Ergebnisse sind qualitativ hochwertige Daten, die zur Abwehr von Angriffen genutzt werden. Precision AI basiert auf dem weltweit größten Sicherheitsdatensatz unter den führenden Anbietern von Cybersicherheit: Palo Alto Networks analysiert täglich 4,6 Milliarden neue Vorfälle, entdeckt täglich 2,3 Millionen neue und bisher nicht vorkommende Angriffe und blockiert täglich 11,3 Milliarden Attacken. Dadurch besitzt Palo Alto Networks große Datenschätze, die für effektive KI ausschlaggebend sind. Precision AI zentralisiert diese Daten und analysiert sie mit sicherheitsspezifischen Modellen, um die Erkennung, Prävention und Reaktion auf Cyberangriffe zu automatisieren. Das KI-System ermöglicht präzise und vertrauenswürdige Sicherheitsergebnisse in Echtzeit und reduziert so das Risiko von Angriffen.

### Fazit

Sicherheit hat sich zu einem Datenproblem entwickelt. Durch die Analyse von Terabytes an Daten kann Precision AI die Cyberabwehr verändern, um rechtzeitig auch auf bisher unbekannte Sicherheitsbedrohungen in Echtzeit reagieren zu können. Gleichzeitig erhalten Sicherheitsteams umfassende Einblicke und die genauesten Sicherheitsergebnisse in der Branche. In Kombination mit dem Plattform-Ansatz von Palo Alto Networks ist Precision AI der Eckpfeiler zur Transformation der Cybersicherheit.

***Martin Zeitler***

UM KI WIRKLICH SINNVOLL IM SECURITY-KONTEXT EINSETZEN ZU KÖNNEN, BENÖTIGT MAN EIN ÖKOSYSTEM, EINE ZENTRALE STELLE, DIE ALGORITHMEN TRAINIERT UND ZUR VERFÜGUNG STELLT, UND EINEN GROSSEN DATENPOOL MIT HOHER DIVERSITÄT UND VIELEN ATTRIBUTEN.

**Martin Zeitler, Senior Director Systems Engineering für Zentraleuropa, Palo Alto Networks, www.paloaltonetworks.com**

# Gekaperte Router entfesseln DDoS-Tsunami

## WENN CORE-ROUTER GEFÄHRLICH WERDEN

**– TEIL 1 VON 2 –**

Seit Anfang 2023 lässt sich ein starker Anstieg von DDoS-Angriffen beobachten. Ein neuer Trend besteht darin, Angriffe mit hoher Paketrate zu versenden. Dieser Artikel stellt die Ergebnisse des OVHcloud-Teams vor, um über neue Erkenntnisse zu dieser Bedrohung zu informieren.

Interessanterweise fällt die jüngste Ankündigung, dass das 911 S5 Botnet zwischen dem 25. und dem 30. Mai 2024 zerschlagen wurde, mit einem deutlichen Rückgang der DDoS-Angriffe zusammen, der Mitte Mai einsetzte. Wir können jedoch nicht mit Sicherheit bestätigen, dass diese Ereignisse miteinander verbunden sind. Während sich die Häufigkeit der Angriffe scheinbar wieder normalisiert hat, beobachten wir immer noch eine große Anzahl von DDoS-Angriffen mit Paketraten von mehr als 100 Mpps (Millionen Pakete pro Sekunde).

**Angriffe mit hoher Paketrate**

Normalerweise beruhen die meisten DDoS-Angriffe auf dem Senden einer großen Menge von Datenmüll, um die Bandbreite zu sättigen (Angriffe auf der Netzwerkschicht), oder auf dem Senden einer großen Menge von Anwendungsanforderungen, um eine übermäßige CPU- oder Speichernutzung zu verursachen (Angriffe auf der Anwendungsschicht). Natürlich gibt es auch andere Methoden: Dazu gehören Angriffe, die auf der Paketrate oder auf Paketen pro Sekunde basieren.

Ziel von Angriffen auf die Paketrate ist es, die Paketverarbeitungsengines von Netzwerkgeräten in der Nähe des Ziels zu überlasten, anstatt die verfügbare Bandbreite auszuhungern. Die allgemeine Idee besteht darin, die Infrastrukturen vor dem anvisierten Dienst (etwa Load-Balancer, Anti-DDoS-Systeme, …) lahmzulegen und so möglicherweise eine große Infrastruktur als Kollateralschaden zu beeinträchtigen. Einfach ausgedrückt: Anstatt zu versuchen, Lücken in Anti-DDoS-Systemen zu finden, werden sie einfach ausgeschaltet.

Angriffe auf die Paketrate sind recht effektiv, da es in der Regel schwieriger ist, mit vielen kleinen Paketen umzugehen als mit größeren, aber weniger zahlreichen Paketen. Dies liegt daran, dass die Rechenkosten im Allgemeinen höher sind. Wird etwa Software zur Verarbeitung von Paketen verwendet, bedeutet jedes Paket mindestens einen Speicherzugriff (abgesehen von möglichen Kopien oder Zugriffen auf gespeicherte Daten wie Verbindungstabellen), anstatt einfach über mehr Bytes zu iterieren. Wird Hardware verwendet, wird die Leistung der Paketverarbeitung zwar nicht unbedingt von der Paketrate beeinflusst, aber die Prozesspipeline hängt wahrscheinlich von anderen Komponenten ab, wie zum Beispiel dem Speicher (wieder!), der durch hohe Paketraten stark belastet werden könnte. Unter diesen Bedingungen kann man aufgrund der sehr hohen Rate an Grenzen stoßen oder einfach nur, weil man nicht genügend Puffer hat, um alles zu speichern, was wahrscheinlich zu Latenzzeiten oder Leistungseinbußen führt. Wir können dieses Problem in einem einzigen Satz zusammenfassen: Wenn Ihre Aufgabe darin besteht, hauptsächlich mit Nutzlasten umzugehen, kann die Bandbreite die harte

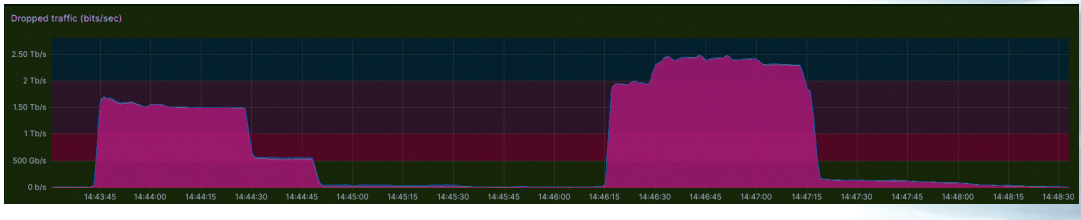
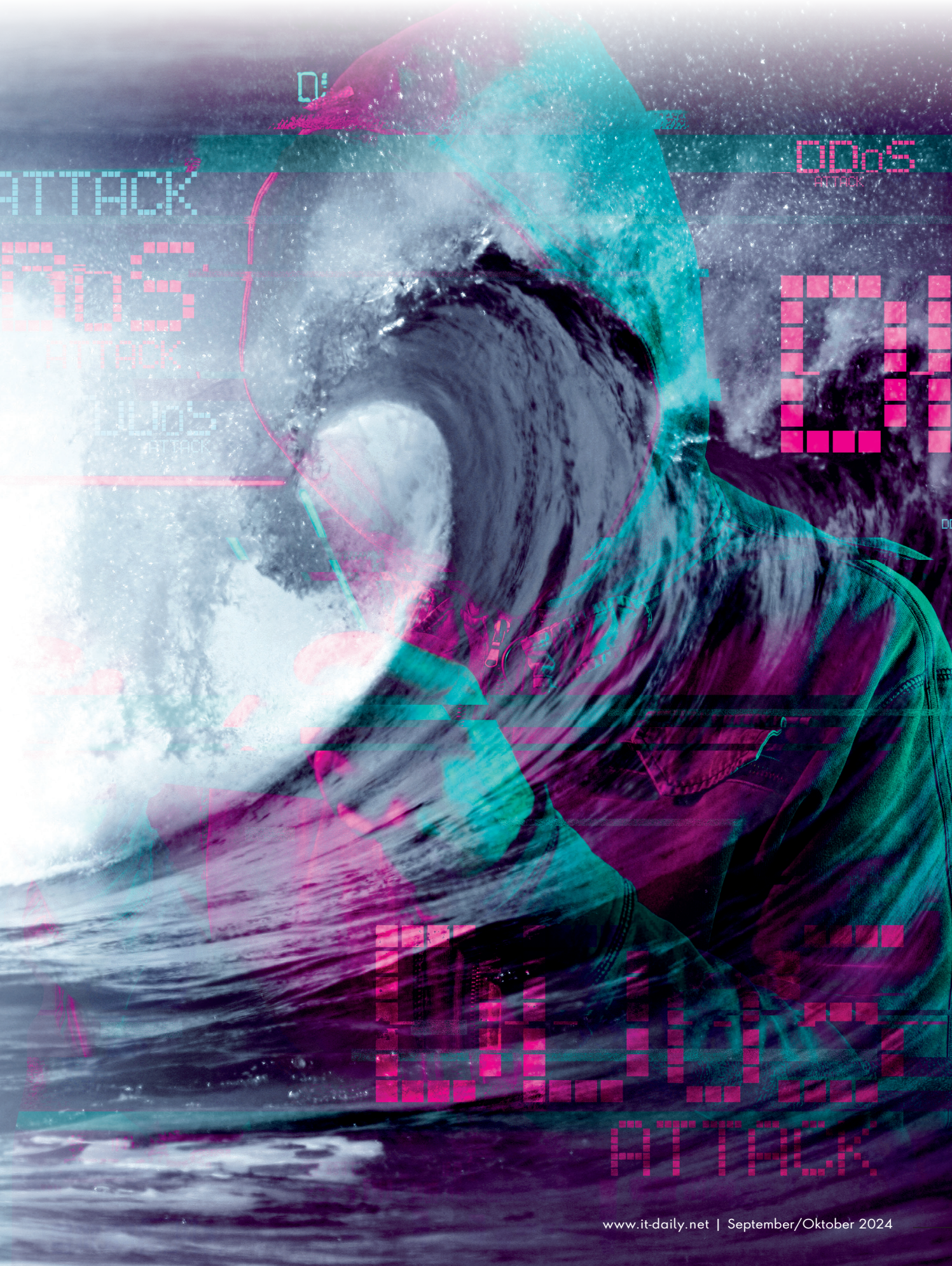



**Bild 1: Am 25. Mai. 2024 erfolgte ein Angriff mit 1,5 Tbps, direkt gefolgt von der größten jemals bei OVHcloud aufgezeichneten Bitrate mit 2,5 Tbps in der Spitze.**


ATTACK
DDoS
ATTACK

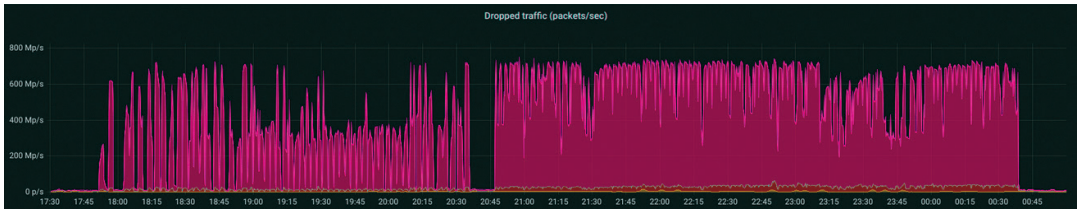



**Bild 2: Dieser spezielle Angriff machte seinerzeit deutlich, dass Botnets zunehmend in der Lage sind, enorme Paketraten zu erzeugen und diese über einen langen Zeitraum aufrechtzuerhalten.**

Grenze sein. Wenn Ihre Aufgabe aber darin besteht, hauptsächlich mit Paketköpfen umzugehen, ist die Paketrate die harte Grenze.

Aus diesem Grund ist es unter den meisten Bedingungen schwieriger, mit kleinen Paketen umzugehen als mit großen Paketen. Kurz gesagt, ein 10-Gbit/s-DDoS-Angriff mit großen Paketen (1480 Byte) ergibt circa 0,85 Mpps: im Vergleich dazu ergeben 10 Gbit/s mit den kleinsten Paketen (84 Byte auf der Leitung für Ethernet) massive circa 14,88 Mpps.

Im Zusammenhang mit der Standard-MTU des Internets (1500) können 17-mal mehr Pakete auf der Leitung untergebracht werden, wenn nur die kleinstmöglichen Pakete erzeugt werden, im Vergleich zu großen Paketen. Um eine Vorstellung von den Rechenkapazitäten zu vermitteln, die im Zusammenhang mit der DDoS-Abwehr erforderlich sind, kann eine 100-Gbit/s-Verbindung eine Leitungsrate von 149 Mpps bewältigen: Dies ermöglicht bis zu sechs Nanosekunden Verarbeitungszeit pro Paket oder 18 Zyklen für eine einzelne Rechenpipeline, die mit einer Taktfrequenz von 3 GHz läuft. Anders ausgedrückt: Selbst mit Dutzenden von parallelen Pipelines stehen nicht viele Zyklen zur Verfügung, vor allem, wenn man auf Speicher zugreifen muss.

Nebenbei bemerkt ist dies einer der Gründe, warum OVHcloud seine eigenen Netzwerk-Appliances für DDoS-Infrastrukturen entwickelt. Wir verwenden eine Kombination aus FPGA und Userland-Software (DPDK), um Appliances mit handelsüblicher Hardware zu bauen. Jede Netzwerk-Appliance, die zur Abschwächung von DDoS-Angriffen eingesetzt wird, wird intern entworfen, implementiert und gewartet (wie übrigens auch der Rest unserer Anti-DDoS-Systeme). Dank dieses schlanken Ansatzes können wir die Leistungserwartungen und -beschränkungen genau abstimmen und sicherstellen, dass unsere Appliances den Anforderungen entsprechen.

**Der Anstieg der (großen) Paketraten-Angriffe**

DDoS-Angriffe, die sich auf hohe Paketraten stützen, sind nicht neu, und Netzbetreiber auf der ganzen Welt waren mindestens einmal mit solchen Angriffen konfrontiert. Der höchste öffentlich bekannte Angriff mit hoher Paketrate wurde beispielsweise von Akamai im Jahr 2020 gemeldet und erreichte 809 Mpps. Trotz dieser hohen Zahl liegt die überwiegende Mehrheit der Angriffe auf die Paketrate jedoch weit unter 100 Mpps. Dies liegt wahrscheinlich daran, dass die Erzeugung vieler kleiner Pakete schwieriger ist als die Erzeugung großer Pakete (man braucht viel mehr Rechenleistung, ähnlich wie bei der Verarbeitung) und dass es schwieriger ist, sie vor Netzwerküberwachungs- und Missbrauchsschutzsystemen zu verbergen.

Angriffe auf die Paketrate haben bei uns vor zwei Jahren begonnen, ernsthaft Aufmerksamkeit zu erregen, nachdem wir mehr als sechs Stunden lang von einer gigantischen UDP-Flut betroffen waren, die im Durchschnitt circa 700 Mpps für ungefähr vier Stunden erreichte, aber erfolgreich eingedämmt wurde.

In den letzten 18 Monaten und insbesondere in den letzten sechs Monaten, haben wir einen starken Anstieg von DDoS-Angriffen mit Paketraten von über 100 Mpps festgestellt. Wir konnten nicht mehr nur wenige Angriffe pro Woche abwehren, sondern Dutzende oder sogar Hunderte pro Woche. Anfang 2024 mussten unsere Infrastrukturen mehrere Angriffe mit über 500 Mpps abwehren, darunter einen mit 620 Mpps in der Spitze. Im April 2024 entschärften wir sogar einen rekordverdächtigen DDoS-Angriff, der circa 840 Mpps erreichte und damit knapp über dem bisherigen Rekord von Akamai lag.

Dieser Angriff bestand zu 99 Prozent aus TCP ACK, die von etwa 5.000 Quell-IPs stammten. Interessanterweise war das restliche Prozent ein DNS-Reflection-Angriff, bei dem circa 15.000 DNS-Server zur Verstärkung des Datenverkehrs genutzt wurden, was bei Angriffen mit hoher Paketrate nicht wirklich effizient ist.

Obwohl der Angriff weltweit verteilt war, kamen zwei Drittel der Gesamtpakete von nur vier PoPs, die sich alle in den USA befanden, wobei drei davon an der Westküste lagen. Dies verdeutlicht die Fähigkeit der Täter, eine

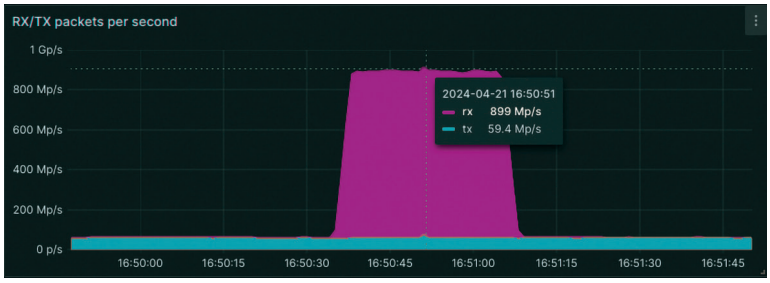



**Bild 3: Ein rekordverdächtiger DDoS-Angriff mit 840 Mpps wurde von OVHcloud entschärft.**

hohe Paketrate über nur wenige Peerings zu senden, was sich als sehr problematisch erweisen kann. Im Allgemeinen gehen Anti-DDoS-Reaktionsteams – nicht nur bei OVHcloud – davon aus, dass es wirklich schwierig ist, massive DDoS-Angriffe von nur wenigen geografischen Standorten aus zu versenden. Ausgehend von dieser Annahme sind unsere Infrastrukturen horizontal skaliert und weltweit verteilt, so dass sie die Last leichter aufnehmen können. Die Verteilung des Datenverkehrs bei dem Angriff mit 840 Mpps hat diese Annahme jedoch stark in Frage gestellt. Wir verfügen zwar über die lokalen Kapazitäten, um diesen Angriff zu entschärfen, aber wir werden das allgemeine Skalierungs- und Verteilungsmodell unserer Anti-DDoS-Infrastrukturen anpassen, um sicherzustellen, dass wir künftige (und wahrscheinlich größere) Angriffe so bewältigen können, wie wir es heute tun.

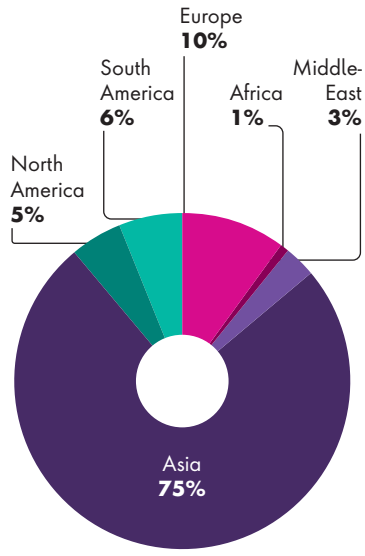



**Bild 4: Verteilung der 70 IPs mit den höchsten Paketraten nach Standorten des AS**

Der signifikante Anstieg von Angriffen mit hoher Paketrate hat uns schließlich dazu veranlasst, uns intensiv mit dem Thema zu beschäftigen. Als weltweiter Cloudanbieter prüft OVHcloud täglich viele DDoS-Angriffe, was uns einen besonderen Blickwinkel auf dieses Thema ermöglicht. Wir wollten verstehen, wie diese Angriffe generiert werden, woher sie kommen und möglicherweise herausfinden, was wir tun können, um unsere Infrastrukturen und Kunden besser gegen diese Art von Angriffen zu schützen.

**Böse Core-Router entlarven**

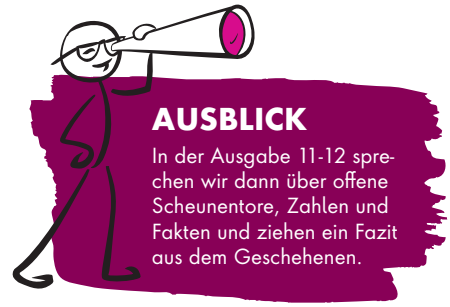
Während unserer Analysekampagne, bei der wir fast hundert Angriffe mit einer Paketrate von 100 bis 500 Mpps manuell untersuchten, stellten wir fest, dass viele Angriffe von nicht allzu vielen Quellen ausgingen, die einen großen Teil des gesamten Datenverkehrs verursachten. Wir erstellten eine Liste bekannter angreifender IPs, die jeweils mindestens 1 Mpps erzeugen können, und beschlossen, weiter zu graben.

Wir analysierten die 70 IPs mit den höchsten Paketraten von bis zu 14,8 Mpps pro IP. Diese IPs gehören hauptsächlich zu Autonomen Systemen (AS) in Asien, aber auch Europa, der Nahe Osten, Nordamerika und Südamerika sind vertreten. Die ermittelten AS scheinen überwiegend zu Unternehmens-ISPs oder Cloud-Konnektivitätsanbietern zu gehören.

Um zu verstehen, welche Art von Geräten an diesen DDoS-Attacken beteiligt waren, haben wir Onyphe verwendet, um festzustellen, ob diese IPs bekannt waren. In der Tat ist ein großer Teil dieser IPs als MikroTik-Router bekannt und stellt im Internet – zumindest – die Konfigurationswebseite zur Verfügung.

Zum jetzigen Zeitpunkt ist es möglich, dass dieser Datenverkehr entweder von Servern erzeugt wird, die sich hinter einem mit NAT konfigurierten Router befinden, eine gefälschte IP verwenden oder eine seltsame TCP-Reflexion ausnutzen. Wir haben diese Hypothesen jedoch schnell verworfen, da es unwahrscheinlich ist, auf eine so große Anzahl identifizierter MikroTik-Router zu stoßen, zumal MikroTik keinen großen Marktanteil hat. Darüber hinaus zeugt die Offenlegung einer Administrationsschnittstelle von schlechten Management-Praktiken. Sie vergrößert die Angriffsfläche des Geräts und kann die Kompromittierung durch einen Angreifer erleichtern. Darüber hinaus wurde RouterOS – das Betriebssystem von MikroTik – in den letzten Jahren von mehreren kritischen CVE-Lücken heimgesucht. Selbst wenn ein Patch veröffentlicht wurde, sind diese Geräte möglicherweise noch nicht gepatcht worden.

***Sebastien Meriot und Christophe Bacara***
***www.ovhcloud.com***



## 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:***
Christophe Bacara, David Baier, Lars Becker, Elmar Eperiesi-Beck, Vanitas Berrymore, Sam Flaster, Andreas Fuchs, Günter Esch, Claus Gründel, Stefan Henke, Steffen Heyde, Jörg von der Heydt, Raphael Kelbert, Prof. Dr. Dennis-Kenji Kipker, Frank Limberger, Silke Menzel, Sebastien Meriot, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Julien Reisdorffer, Sören Schulte, Marcel Stadler ,Michael Veit, Martin Zeitler

***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, +49 152-3634 1255, mann@it-verlag.de

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

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

***Erscheinungsweise:*** 6 x pro Jahr

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

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

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

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

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




## INSERENTENVERZEICHNIS

***it security***


| | |
|---|---|
| DriveLock SE (Teaser) | U1, 14 |
| ASOFTNET GmbH & Co.KG (Teaser) | U1, 20 |
| macmon secure GmbH (Teaser) | U1, 24 |
| NürnbergMesse GmbH | U2 |
| Bitdefender GmbH (Advertorial) | 23 |
| WatchGuard Technologies GmbH (Advertorial) | 27 |
| SEPPmail Deutschland GmbH (Advertorial) | 31 |
| it Verlag GmbH | 31, 35, 42, 59, U3 |
| Swissbit AG (Advertorial) | 35 |
| retarus GmbH (Advertorial) | 39 |
| Stormshield (Advertorial) | 43 |
| Anqa IT-Security GmbH (Advertorial) | 47 |
| Ping Identity | 49 |
| Samsung Electronics GmbH (Advertorial) | 53 |
| Hiscout GmbH (Advertorial) | 55 |
| Open Systems (Advertorial) | 57 |
| Entrust (Advertorial) | 59 |
| Fastly (Advertorial) | 61 |
| Logicalis GmbH | 63 |
| INFODAS GmbH (Advertorial) | 65 |
| Leipziger Messe GmbH (Advertorial) | 69 |
| Palo Alto Networks (Advertorial) | 73 |
| Aagon GmbH | U4 |

SAVE THE DATE

it security Digitalevent

# WE SECURE IT

## 13. und 14. November 2024

#WesecureIT2024

it-daily.net

Eine Veranstaltung von itsecurity & it-daily.net

# WIR SIND DABEI!

Aagon

itsa 365

**22. bis 24. Oktober**
**in Nürnberg**

**Halle 7**
**Stand 7-436**

## Vortrag

„NIS-2: Handlungsanweisungen und
der entscheidende Beitrag von UEM“
23.10.2024 von 11:15 bis 11:30 Uhr, Forum 7-C

Mehr erfahren und
Gratis-Dauerkarte sichern:
www.aagon.com/it-sa2024

PUR 2024
Professional User Rating

ACMP ist 5fach Champion

Aagon