



# it management

Der Motor für Innovation  
März/April 2024

INKLUSIVE 48 SEITEN

it  
security



ENERGIEEFFIZIENZGESETZ FÜR RECHENZENTREN

## Digitalisierung nicht ausbremsen

Anna Kluft, Rittal

### GENERATIVE KI

Neue Horizonte eröffnen

### WISSENSMANAGEMENT

Effizienzsteigerung Servicedesk



KONICA MINOLTA

Managed Services  
ab Seite 34



# Der Ratgeber für Ihre SAP S/4 HANA Transformation

**Sie haben eine IT-Transformation vor der Brust oder stecken bereits mittendrin? Dann hilft Ihnen sicher unser kostenloses Transformation Roadbook. Darin haben wir Tipps, Tricks und Erfahrungswerte aus über 1.000 Transformationen.**

Das Transformation Roadbook führt Sie in 10 Schritten durch eine erfolgreiche IT-Transformation (z. B. Migration auf SAP S/4HANA). Angefangen bei der Vorbereitung, über das Projektmanagement, die Berücksichtigung vieler Compliance Aspekte, bis hin zur Qualitätsprüfung. Auf über 60 Seiten finden Sie Unterstützung zu allen Bereichen einer erfolgreichen Modernisierung Ihrer IT-Systeme. Nutzen Sie die reichhaltige Erfahrung internationaler Transformationsexperten!



Jetzt downloaden!





## ANALOG? DIGITAL? HYBRID?

”

LIEBE LESERINNEN UND LESER,

Wer dachte, die IT macht alles einfacher, der irrt. Ständig steigt die Geschwindigkeit, mit der sich alles um uns herum verändert. Egal ob Metaverse, Kryptowährungen, Quantencomputing, Cyberbedrohungen, stets müssen wir bei Innovationen auch die Risiken im Blick haben.

Rund 15 Jahre ist es her, dass wir uns beim Smartphone an die Touchfunktion gewöhnt haben, doch bei Desktop und Notebook? Fehlanzeige! Nun endlich folgt der nächste Quantensprung.

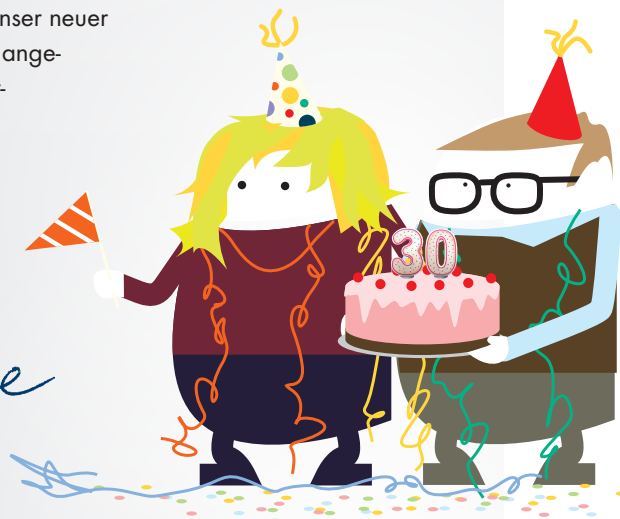
AMERIA hat jetzt ein Weltneuheit angekündigt. Ein neues Device, dass die Art und Weise revolutionieren wird, wie wir mit Computern, Tablets und anderen digitalen Geräten umgehen: MAVERICK AI, das weltweit erste AI-Device, die virtuelle Welt ohne VR-Brille, berührungslose Interaktion mit Bildschirmen und Künstliche Intelligenz zusammenbringt – und das alles auf der kleinen Fläche eines Notebooks. Vielleicht gehören Maus und Tastatur bald der Vergangenheit an? Das Video dazu finden Sie auf [it-daily.net](http://it-daily.net).

Und bei uns? Wir feiern mit dieser Ausgabe 30 Jahre it management, ruhen uns darauf aber sicher nicht aus. Wir haben neue Tools für unser Onlineportal [www.it-daily.net](http://www.it-daily.net) eingeführt, die unsere Sichtbarkeit und die Performance erhöhen. Unser neuer täglicher Newsletter wird hervorragend angenommen und eine neue Suchfunktion verbessert die User Experience unserer Homepage.

Es bleibt spannend!

*Ulrich Parthier*

Ulrich Parthier  
Publisher it management & it security





# INHALT

## COVERSTORY

- 12 Energieeffizienzgesetz für Rechenzentren**  
Aufholen, nicht bremsen
- 14 Wenn der Standard die beste Lösung ist**  
Neubau eines Rechenzentrums

## 30 JAHRE IT MANAGEMENT

- 18 Happy Birthday!**  
30 Jahre it management
- 20 Innovatives Customer Onboarding**  
Kundenbindung par excellence
- 22 30 Jahre it management**  
Was wir schon immer mal fragen wollten

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

- 25 eIDAS Summit 2024**  
Business & Prozesse sicher und einfach digitalisieren
- 26 E-Rechnungspflicht**  
Wie sich Unternehmen effektiv vorbereiten
- 28 Archivdaten und die digitale Transformation**  
Altdaten: Mehr eine rechtliche als technische Herausforderung
- 29 Wi-Fi oder DECT?**  
Entscheidend ist der Einsatzzweck
- 30 USU means Service**  
Cloud Cost Management
- 33 Effizienz-Boost gegen Fachkräftemangel**  
Produktivitätsstellschraube ERP

## IT MANAGEMENT

- 34 Managed Services**  
Wir sind flexible "IT-Hausmeister"
- 36 Lizenzmanagement**  
Gelassen in den Audit
- 39 Raus aus der Kostenspirale**  
Lizenzmanagement für die Microsoft Cloud
- 40 Wissensmanagement im Servicedesk**  
Effizienzsteigerung durch den KCS-Ansatz





36



46

- 42 SAP S/4HANA-Transition**  
Security & Compliance als unverzichtbarer Bestandteil
- 44 Effiziente Projektabwicklung**  
Mehr Eigenständigkeit und immer auf dem neuesten Stand
- 46 Testdatenmanagement (Teil 2 von 5)**  
Automatisierte Ausführung von Testdaten-Jobs
- 49 Hannover Messe 2024**  
Lösungen für eine klimaneutrale Industrie
- 50 Der moderne Sisyphos**  
Die Herausforderungen der Daten-zusammenführung
- 52 Keine Angst vor komplexen Datenbeständen**  
So setzen Sie eine erfolgreiche Data-Lakehouse-Strategie um
- 56 Wo Wettbewerbsvorteile winken**  
Gartner-Analyse zu Partnerprogrammen
- 60 KI in der Industrie 4.0**  
Zwischen Hype und Wertschöpfung
- 62 Generative KI im Servicegeschäft**  
Neue Horizonte für innovative Lösungen
- 65 Ein Hub für alle KI-Chatbots**  
Was ist Poe AI und wie funktioniert es?



Inklusive 48 Seiten  
it security



**GUT ZU  
WISSEN**

Achten Sie auf dieses Icon  
und lesen sie mehr  
zum Thema im Internet auf  
[www.it-daily.net](http://www.it-daily.net)



# STORAGE

## INNOVATIONEN NONSTOP

Gartner hat 2023 einen neuen Magic Quadranten für Primärspeicher veröffentlicht. Anwender von Primärspeicherlösungen setzen demnach auf verbrauchsbasierte Infrastruktur-Services für hybride, multidomäne und unternehmenskritische Anwendungen sowie auf die Anpassung der Kosten an Geschäftsanforderungen. I&O-Führungskräfte sollten die Zeit nutzen, um Abläufe zu automatisieren, Komplexität und Abwanderung zu reduzieren und den IT-Betrieb zu transformieren.

Der Hauptzweck eines Primärspeicherprodukts ist die Unterstützung von Workloads mit strukturierten Daten, die auf Antwortzeiten und IO/s angewiesen sind. Darüber hinaus wird die Primärspeicherfunktionalität mit einer zentralisierten Steuerungsebene für automatisiertes Infrastrukturmanagement, Datendienste und Datenbewegungen sowie für Storage-as-a-Service-Angebote für hybride Infrastrukturplattformen integriert und unterstützt deren unabhängige Nutzung.

### Aus dem Inhalt:

- Composable Storage
- Sekundärdaten – ein Informationsdesaster
- Hybrid Storage
- Rein in den Container?
- Anforderungen moderner Data Warehouses
- Enterprise-SSDs
- 22-TByte-HDDs



Das **eBook** umfasst 44 Seiten und steht zum kostenlosen Download bereit





snom



M55



M58



M500

# Profitieren Sie vom drahtlosen VoIP!

Dynamische Unternehmen benötigen eine flexible Arbeitsumgebung. Die neue DECT-Basisstation mit Dualzellen-System M500 und die Endgeräten M55 und M58 sorgen dafür.

# IT-SICHERHEIT = CHEFSACHE?

## NIS2 ERHÖHT DEN DRUCK

Sollte IT-Sicherheit Chefsache sein? Definitiv! Durch die zunehmende Digitalisierung von Arbeits- und Produktionsprozessen in Unternehmen ist Cybersecurity längst kein Nebenschauplatz mehr und sollte höchste Priorität bei der Firmenleitung haben. Cyberattacken sind sehr teuer und nehmen schnell existenzbedrohende Züge an. Laut der repräsentativen Studie „Cybersicherheit in Zahlen“ von G DATA, Statista und brand eins überträgt die Geschäftsführung die Verantwortung für Sicherheitsvorkehrungen gegen Cyberangriffe aber am häufigsten auf die IT-Abteilung. Nur bei einem Viertel der deutschen Firmen sieht die Unternehmensführung die Notwendigkeit, die Implementierung und Aufrechterhaltung von

Schutzmaßnahmen selbst zu verantworten. Spätestens mit NIS2 erhöht sich der Druck auf viele Vorstände und sie werden gesetzlich in die Pflicht genommen, das Thema IT-Sicherheit ernst zu nehmen. Bei Nichteinhaltung können sie auch persönlich haftbar gemacht werden.

### IT-Sicherheit hat Priorität

Je größer ein Unternehmen ist, desto seltener liegt die Verantwortung bei der obersten Firmenleitung. Nur bei einem von zehn Unternehmen mit 1.000 oder mehr Mitarbeitenden ist die Geschäftsleitung für die IT-Sicherheit verantwortlich. Das ist in Hinblick auf NIS2 fatal. Und die Zeit drängt. Überraschend ist aber: Bei 40 Prozent der kleinen Unternehmen

mit unter 50 Mitarbeitenden liegt die Verantwortung für IT-Sicherheit bereits bei der Geschäftsführung oder dem Vorstand. Trotzdem besteht auch bei kleinen Unternehmen akuter Nachholbedarf, denn bei drei von fünf kleinen Firmen ist IT-Sicherheit noch keine Chefsache. Es ist dringend erforderlich, dies nachzuholen, denn die Chefetage spielt eine Schlüsselrolle bei der Etablierung einer Sicherheitskultur im Unternehmen.

[www.gdata.de](http://www.gdata.de)

**MEHR  
WERT**

Cybersicherheit in Zahlen



## WER IST IN IHREM UNTERNEHMEN FÜR IT-SICHERHEIT VERANTWORTLICH? (Insgesamt)







### WELCHEN MEHRWERT HABEN DIGITALE TECHNOLOGIEN FÜR IHR UNTERNEHMEN?

✓ **51%**

Zeitersparnis und Steigerung der Effizienz

✓ **38%**

Verkauf von mehr Produkten und Dienstleistungen

✓ **37%**

Kosteneinsparungen

✓ **16%**

Zugang zu Finanzierungen

# Elektronische Rechnungsstellung

DEUTSCHE KMU BESSER ALS IHR RUF

Deutsche KMU haben den Mehrwert digitaler Technologien für ihr Unternehmen erkannt und sehen sich auf einem guten Weg. Gerade in wirtschaftlich schwierigen Zeiten mit starkem Druck auf Gewinnmargen und notwendiger Steigerung der Effizienz messen sie der Digitalisierung einen hohen Stellenwert bei. Das ist ein Ergebnis der Studie „Empowering SMEs in The Digital Decade: the 600 billion EUR opportunity“ im Auftrag von Sage. 72 Prozent der befragten deutschen KMU bezeichnen den Stellenwert digitaler Technologien für die Gründung ihres Unternehmens als „wichtig“. 85 Prozent messen digitalen Technologien einen hohen Stellenwert für den Erfolg ihres Unternehmens bei und 89 Prozent für das Unternehmenswachstum. Sogar 90 Prozent schreiben ihnen eine wichtige Rolle für die Resilienz ihres Unternehmens zu.

#### Der Mittelstand holt auf

„Nicht selten wird gerade deutschen KMU vorgehalten, ihnen fehle das Verständnis für die Bedeutung digitaler Technologien, verbunden mit dem Vorwurf, deshalb hinken sie bei der Digitalisierung im internationalen Vergleich hinterher“, kommentiert

Christoph Stoica, Managing Director CEU von Sage. „Unsere Studie belegt das Gegenteil. Wir sehen das übrigens auch an der Nachfrage nach unseren Produkten: Der deutsche Mittelstand holt bei der Digitalisierung mächtig auf. Auch darum ist es wünschenswert, dass von staatlicher Seite mehr Unterstützung für KMU kommt, damit diese ihre Digitalisierungsziele auch erreichen können. Zu den erforderlichen Maßnahmen zählen finanzielle Anreize, umfassende Schulungen und passende digitale Werkzeuge, die KMU in die Lage versetzen, ihre digitale Transformation erfolgreich zu bewältigen.“

#### Ein Buch mit sieben Siegeln

Deutsche KMU verorten den Mehrwert digitaler Technologien für ihr Unterneh-

men in verschiedenen Bereichen, zum Beispiel bei Zeitersparnissen oder Kosteneinsparungen. Der Beitrag digitaler Technologien für den Zugang zu Finanzierungen landet hingegen mit 16 Prozent abgeschlagen auf dem letzten Platz.

Letzterer Befund spiegelt sich auch in der Einstellung der KMU zur elektronischen Rechnungsstellung wider. Für 16 Prozent ist das Konzept der elektronischen Rechnungsstellung ein Buch mit sieben Siegeln und 37 Prozent verfügen über einige Kenntnisse von E-Invoicing, sehen hier aber weiteren Informationsbedarf. Nur 28 Prozent der KMU fühlen sich vollständig auf die verpflichtete elektronische Rechnungsstellung vorbereitet. Dieser Befund dürfte darin begründet sein, dass viele KMU die Vorteile des E-Invoicing unterschätzen. Nur 16 Prozent erwarten, dass die elektronische Rechnungsstellung die Anzahl der Betrugsfälle in ihrer Branche signifikant reduzieren kann. Lediglich 29 Prozent gehen davon aus, dass E-Invoicing ihren Cashflow signifikant verbessern kann.

[www.sage.com](http://www.sage.com)



## REFURBISHED-IT

**15 %** haben  
wiederaufbereitete Geräte  
im Einsatz

**75 %** sehen  
darin einen wichtigen Beitrag zum  
Klima- und Umweltschutz

**15 %** würden  
Refurbished-IT künftig  
benutzen

## REFURBISHED-IT

## DIE NACHFRAGE STEIGT

Ob Smartphones, Monitore oder Laptops – für eine zunehmende Zahl an Unternehmen in Deutschland muss es bei elektronischen und digitalen Geräten nicht immer Neuware sein.

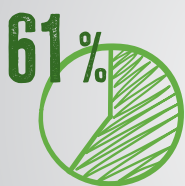
Schon 15 Prozent haben gebrauchte, aber professionell wiederaufbereitete IT im Einsatz: 5 Prozent bereits in vielen Bereichen des Unternehmens, 10 Prozent in Einzelfällen. Weitere 15 Prozent der Unternehmen ziehen den Einsatz von Refurbished-IT in Erwägung (2022: 13 Prozent). Das ist das Ergebnis einer repräsentativen Befragung unter mehr als 500

Unternehmen in Deutschland ab 20 Beschäftigten, die im Auftrag des Bitkom durchgeführt wurde.

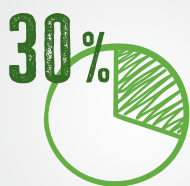
2022 hatten gerade einmal vier Prozent der Unternehmen angegeben, lediglich in Einzelfällen Refurbished-IT zu nutzen. „Wir müssen in Deutschland und Europa weniger Elektroschrott erzeugen. Dabei hilft, IT-Geräte länger zu nutzen. Mit Refurbished-IT können Unternehmen ihre Umweltbilanz verbessern und sparen dabei gleichzeitig Geld“, sagt Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder.

Für Unternehmen, die bislang noch keine Refurbished-IT nutzen, bedarf es in den meisten Fällen größerer Anreize: 61 Prozent würden entsprechende Geräte nutzen, wenn es mehr steuerliche oder finanzielle Vorteile hätte. 30 Prozent würden die dadurch erzielten CO<sub>2</sub>-Einsparungen gern in ihren Nachhaltigkeitsberichten ausweisen können. Für eine Mehrheit von 75 Prozent wäre aber eine lange Gewährleistung beziehungsweise Garantie Voraussetzung für die Nutzung von Refurbished-IT, bei 61 Prozent eine ausreichend lange Versorgung mit Updates. „Seit Einführung der Updatepflicht im Jahr 2022 werden viele digitale Produkte und Dienste länger als zuvor und regelmäßig mit Updates versorgt“, stellt Rohleder klar. „Und einige Händler für Refurbished-IT gehen mit ihren Garantie- und Gewährleistungszusagen sogar über die gesetzlichen Fristen von Neuprodukten hinaus.“

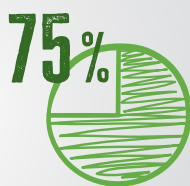
## WANN WÜRDEN SIE REFURBISHED-IT NUTZEN?



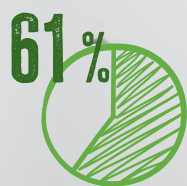
wenn es mehr  
steuerrechtliche  
Vorteile hätte



wenn die CO<sub>2</sub>-  
Einsparungen im  
Nachhaltigkeitsbe-  
richt ausgewiesen  
werden könnten



lange Garantie  
oder Gewähr-  
leistung als  
Voraussetzung

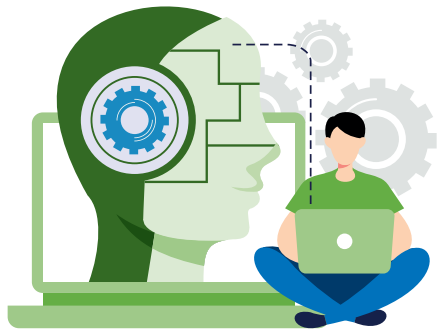


ausreichend  
lange Versorgung  
mit Updates

Insgesamt stimmen 75 Prozent aller Unternehmen der Aussage zu, die Nutzung von Refurbished-IT leiste einen wichtigen Beitrag, um Ressourcen und Rohstoffe zu sparen. 61 Prozent meinen, es sollten möglichst viele Unternehmen den Einsatz solcher Geräte zumindest prüfen. 56 Prozent halten die Nutzung von Refurbished-IT für ein wichtiges Zukunftsthema.

[www.bitkom.org](http://www.bitkom.org)





# Künstliche Intelligenz

## ENERGIEBEDARF WÄCHST RASANT

Künstliche Intelligenz kann in Bereichen wie der Klimaforschung einen positiven Beitrag leisten, jedoch hinterlässt die Technologie selbst einen erheblichen CO<sub>2</sub>-Abdruck, so Patrick Gilroy, Referent Künstliche Intelligenz und Bildung beim TÜV-Verband.

Insbesondere das Training von KI-Modellen mit großen Datenmengen sowie die fortlaufende Nutzung verbraucht beträchtliche Mengen an Energieressourcen. Wissenschaftler schätzen, dass der Energieverbrauch von Künstlicher Intelligenz bis zum Jahr 2027 auf 85 bis 134 Terawattstunden (TWh) ansteigen könnte, was etwa dem heutigen Stromverbrauch der Niederlande entsprechen würde.

Allerdings sind diese Berechnungen unsicher, da bis dato insbesondere die Entwickler großer Sprachmodelle („Large Language Models“) wie Open AI / Microsoft mit ChatGPT oder Google mit Bard

keine Angaben zum Energieverbrauch ihrer KI-Systeme veröffentlichen. „Für die zukünftige Ermittlung des Energieverbrauchs einer KI nach einheitlichen Standards müssen Messmethoden entwickelt werden“, sagt Gilroy. „Darüber hinaus sollten die Anbieter der großen Basismodelle verpflichtet werden, den Energie-

verbrauch ihrer KI-Systeme transparent zu machen.“

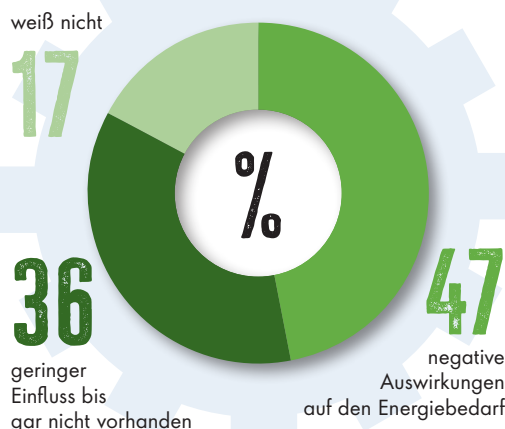
### Rechtliche Vorgaben notwendig

Entsprechende rechtliche Vorgaben sind im kürzlich verabschiedeten europäischen AI Act teilweise verankert. So sollen im Rahmen der laufenden Normungsarbeiten auch KI-spezifische Standards für den Ressourcenverbrauch entwickelt werden. Wirksam werden die Regelungen mit Inkrafttreten der Verordnung aber erst im Jahr 2026. „Der AI Act setzt nicht nur bei der Sicherheit, sondern auch beim Thema Nachhaltigkeit Maßstäbe“, sagt Gilroy. Jetzt komme es darauf an, wie die Ressourceneffizienz von KI in der Praxis gemessen wird und auf dieser Basis verbessert werden kann. Forschungseinrichtungen sowie Prüf- und Normungseinrichtungen könnten hier wichtige Beiträge leisten.

[www.tuev-verband.de](http://www.tuev-verband.de)

(Quelle: Grundlage der Angaben ist eine repräsentative bundesweite Befragung des Marktforschungsunternehmens Ipsos GmbH im Auftrag des TÜV-Verbands.02.2024)

### WELCHE AUSWIRKUNGEN WIRD KÜNSTLICHE INTELLIGENZ (KI) AUF DEN ENERGIEBEDARF HABEN?



**EXKLUSIV. ERP FÜR LOSGRÖSSE 1+**

**ams ERP**

YOU CAN COUNT ON US THE PART OF MEETING EXPECTATIONS

[www.ams-erp.com/webinare](http://www.ams-erp.com/webinare)

# Energieeffizienzgesetz für Rechenzentren

## AUFHOLEN, NICHT BREMSEN

Anna Kluft, Vice President Solution Sales IT bei Rittal und Vorsitzende der German Datacenter Association, im Interview über Entwicklungen bei der IT-Infrastruktur, die Hürden des Energieeffizienzgesetzes und Standardisierung als Tempomacher.

**it management:** Nachdem lange vor allem von Cloud und ihren Anwendungen die Rede war, rückt jetzt auch die physische Infrastruktur wieder mehr in die Aufmerksamkeit. Wo sehen Sie die Gründe?

**Anna Kluft:** In der Sache war die Relevanz nie klein. Denn jede Cloud und das gesamte Internet „wohnt“ irgendwo auf der Welt in einem Rechenzentrum – auch wenn die Nutzer gar nicht darüber nachdenken. Es gibt aber gute Gründe, warum die Rechenzentren jetzt noch stärker ins allgemeine Interesse rücken – einerseits als hochrelevante Infrastruktur und andererseits, weil der dafür nötige Stromverbrauch gemanagt werden muss.

Klar ist: Sie müssen dringend weiter ausgebaut werden, denn Rechenzentren sind das Rückgrat der digitalen Transformation. Ob Energiewende mit Smart Grids oder sämtliche Kritische Infrastruktur für das öffentliche Leben und fast alle Prozesse in den Unternehmen – das alles wird erst durch leistungsfähige IT-Infrastruktur möglich. Durch neue Anwendungen wie generative künstliche Intelligenz (GenAI) steigt der Bedarf an Rechenleistung und Strom jetzt geradezu dramatisch.

**it management:** Was heißt das für die Rechenzentrums-Betreiber?

Anna Kluft: Wir müssen die Infrastruktur schnellstens skalieren. Die Analysten von Omdia gehen davon aus, dass sich der Bedarf in den nächsten fünf Jahren verzehnfacht. Sie prognostizieren CAPEX-Ausgaben von 30 Milliarden Dollar allein für GenAI. Mit der immensen Rechenleistung und ihrem Strombedarf erhält auch Energieeffizienz eine Bedeutung auf ganz anderen Level – und zwar für alle, nicht nur für Hyperscaler. Auch Colocators und klassische Enterprise-Rechenzentren rüsten auf. In Deutschland könnte genau hier ein erheblicher Stolperstein liegen. Das neue Energieeffizienz-Gesetz enthält ungeschickt gewählte Vorgaben für Rechenzentren, die nicht zur Digitalisierungs-Bremse werden dürfen.

**it management:** Können Sie das Energieeffizienz-Gesetz für unsere Leser einordnen?

**Anna Kluft:** Rechenzentren sind elektrische Großverbraucher. Daher ist völlig klar, dass ihre Energieeffizienz mit hoher Priorität bis an die Grenze des physikalisch und wirtschaftlich Möglichen optimiert werden muss. Das machen die meisten Rechenzentrumsbetreiber schon längst, nicht nur aus Kostengründen. Verständlich, dass die Politik diesen Prozess beschleunigen möchte. Aber es hätte geholfen, wenn das gut Gemeinte auch gut gemacht worden wäre – mit differenzierten und realistischen Vorgaben. Die Praktiker der Rechenzentrums-Branche hätten

”

RECHENZENTREN MÜSSEN DRINGEND WEITER AUSGEBAUT WERDEN, DENN SIE SIND DAS RÜCKGRAT DER DIGITALEN TRANSFORMATION.

Anna Kluft, Vice President Solution Sales IT, Rittal, Vorsitzende der German Datacenter Association, [www.rittal.com](http://www.rittal.com)



sicher einen konstruktiven Beitrag geleistet, wenn man sie denn einbezogen hätte. Als Vorsitzende der German Datacenter Association (GDA) habe ich mich schon während des laufenden Gesetzgebungsprozesses dafür stark gemacht, dass die erstrebenswerte Energieeffizienz nicht den Ausbau der dringend benötigten Digitalinfrastruktur bremsen darf. Deutschland ist bei der Digitalisierung die Nummer 27 in der Welt. Wir müssten aufholen, nicht bremsen.

**it management:** Wo liegen die größten Stolpersteine der neuen Vorgaben?

**Anna Kluft:** Das Gesetz sieht für Rechenzentren, die ab Juli 2026 den Betrieb aufnehmen, eine Power Usage Effectiveness (PUE) von 1,2 vor. Dieser Wert zur Energieeffizienz ist ein sehr ambitioniertes Ziel, das die meisten Rechenzentrumsbetreiber trotzdem schon anstreben. Dennoch bleiben bei der Vorgabe drei entscheidende Aspekte unberücksichtigt:

**#1** Ein derart niedriger Wert muss von Anfang an eingeplant werden – die Rechenzentren, die 2026 ihren Betrieb aufnehmen, sind heute bereits geplant oder genehmigt. Wenn das Gesetz den Bau verzögert, bremst es den Ausbau dringend benötigter Infrastruktur, auch für die Energiewende.

**#2** Um diesen Wert zu erreichen, benötigen die IT-Systeme eine definierte Auslastung. Colocation-Anbieter haben darauf aber gar keinen Einfluss. Sie stellen als Betreiber lediglich die Infrastruktur zur Verfügung. Bis 2025 soll dieses Betreiber-Modell 50 Prozent des deutschen Marktes ausmachen.

**#3** Der technische und wirtschaftliche Aufwand hängt stark von den lokalen Gegebenheiten ab. Im norwegischen Lefdal betreibt Rittal beispielsweise eines der grünen Rechenzentren Europas und erreicht eine PUE unter 1,15. Durch die idealen Bedingungen in einer Mine ist das sogar mit Garantie möglich.

In Frankfurter Stadtlage dagegen wäre es – wenn überhaupt – nur mit immens höherem Aufwand umsetzbar.

Noch deutlicher wird der Mangel an Differenzierung beim Thema Wärmerückgewinnung. Mit einer pauschalen Verpflichtung ist keine Garantie von Effizienzsteigerung verbunden. Stattdessen kommt diese Vorgabe vielerorts defacto einem Verbot für neue Rechenzentren gleich. Die Nutzung von Abwärme ist immer dann sinnvoll, wenn es einen klaren Abnehmer gibt.

Immerhin sind die Vorgaben seit dem Bundestagsbeschluss klar. Jetzt können wir in der Branche gemeinsam die Challenge angehen. Es liegt nun bei Betreibern, Planern und Anbietern wie Rittal, Lösungen für die manchmal unrealistisch scheinenden Vorgaben zu finden.

**it management:** Wie sehen Sie die Situation der Rechenzentrumsbetreiber?

**Anna Kluft:** Auch ohne neues Gesetz mussten die Betreiber schon eine dynamische Situation managen. Welche Rechenleistung wird in fünf Jahren benötigt? Und mit welcher Latenz, welcher Verfügbarkeit und welcher physischen Sicherheit? Jetzt kommt in Deutschland noch die drängende Frage hinzu: Erreichen meine Bestands-Rechenzentren die vorgeschriebenen Effizienzwerte der Stufen ab 2027 und 2030? Nehme ich das Gesetz zum Anlass für Optimierung als Retrofit oder doch für ein neues RZ, zum Beispiel als schlüsselfertiger Container? Oder verlagere ich mehr Richtung Colocation und Cloud?

**it management:** Wie unterstützt Rittal dabei?

**Anna Kluft:** Eine wesentliche Frage unserer Kunden lautet: Mit welcher Strategie erreiche ich die nötige Kapazität, Verfügbarkeit und Energieeffizienz technologisch und wirtschaftlich am besten? Für die Antworten müssen Digitalisierungs-, IT- und OT-Strategie mit ganzheitlicher Betrachtung ineinandergreifen. Ebenso

sollte das Rechenzentrum selbst als Gesamtsystem aufgefasst werden, um zum Beispiel Optimierungseffekte für die Energieeffizienz besser vorhersehen zu können. Für Flexibilität, Skalierbarkeit und Tempo sorgen hohe Standardisierung und Module. Rittal berät ganzheitlich bei der Strategie und setzt sie für die IT-Infrastruktur mit hohem Tempo um. Wir haben dafür die Plattform RiMatrix mit den modularen Säulen Rack, Cooling, Power, Monitoring und Security entwickelt. Je nach Umfeld kommen Raum-im-Raum-Konzepte, schlüsselfertige Container mit Blue e+ Kühlung, kleinere Microdatacenter oder weitere Konzepte in Frage. Zudem unterstützen wir bei ROI-Berechnungen, PoC und Analysen mit Computational Fluid Dynamics (CFD).

**it management:** Wo sehen Sie den größten technologischen Umbruch?

**Anna Kluft:** Ganz klar bei der Kühlung. Anwendungen für generative AI erfordern Hochleistungs-Prozessoren (GPU). Diese erzeugen so viel Wärme, dass die Hersteller sie gleich für Flüssigkeitskühlung auslegen. Wasser wird dabei wieder eine größere Rolle spielen, vor allem für einphasige direkte Flüssigkeitskühlung. Rittal ist Hauptlieferant für Racks bei mehreren großen Hyperscalern. Mit ihnen sind wir im intensiven Austausch bei der Entwicklung der passenden modularen Kühllösungen. Das nützt dann auch Rechenzentren in Deutschland, weil diese Form der Kühlung bessere Voraussetzungen bietet, um die gesetzlichen Vorgaben zur Wärmerückgewinnung umzusetzen.

**it management:** Frau Kluft, wir danken für das Gespräch.





# Wenn der Standard die beste Lösung ist

## NEUBAU EINES RECHENZENTRUMS: SICHERHEIT OHNE BÖSE ÜBERRASCHUNGEN

Bauen und planen Unternehmen ihre Rechenzentren neu, stehen sie vor der Wahl: freie Planung oder standardisierte Lösung? Die Elbe Kliniken Stade-Buxtehude GmbH haben sich aus gutem Grund für Letzteres entschieden und dabei immens Zeit und Kosten eingespart. Never change a running system – diese alte Weisheit gilt noch immer unter IT-Verantwortlichen. Muss ein Rechenzentrum doch neu aufgebaut werden, wird oft echtes Neuland betreten. Denn Projekte solcher Größenordnung und Relevanz gehören eben nicht zum Tagesgeschäft von IT-Leitern. Ist erstmal die Entscheidung für einen Neubau getroffen, geht es um die Antwort auf die Grund-satzfrage: frei planen oder eine standardisierte Lösung? Nach der Erfahrung von Dr. Armin Ortlam, Leiter IT-Strategie KHZG Controlling (Krankenhaus-zukunftsgesetz) an den Elbekliniken, wer-

den immer wieder Gründe gegen eine freie Planung angeführt.

### Aufwand und Komplexität reduziert

Für ihn sind es unter anderem die Unwägbarkeiten durch die große Zahl der beteiligten Personen, wie Architekten, Fach- und Rechenzentrumsexperten, die vieles teurer als unbedingt nötig und damit schlechter kalkulierbar machen. „Vor diesem Hintergrund haben wir nach einer geeigneten Option ‚von der Stange‘ gesucht und sie schließlich mit einer Raum-in-Raum-Lösung gefunden. Ich habe mir gewünscht, dass wir uns nicht um Dinge wie Wasser- und Stromanschluss oder Kühlung kümmern müssen“, berichtet Dr. Ortlam über die Anfänge der Zusammenarbeit mit dem Rechenzentrumsspezialisten Rittal. „Heute muss ein Rechenzentrumsbau wirklich nicht mehr so kompliziert sein wie früher: Es müssen keine



siebenstelligen Beträge mehr ausgegeben, keine Überraschungen einkalkuliert werden – wie, dass aus dem angesetzten Projektbudget von einer Million Euro plötzlich drei werden.“

Wer sich für ein standardisiertes Rechenzentrum entscheidet, bekommt vielmehr alles aus einer Hand, so Dr. Ortlam. „Ein Krankenhaus muss lediglich Daten, Wasser, Strom und eventuell Kälte einbringen, und es kommt nur ein einzelner Rittal Fachplaner, mit dem wir alles abwickeln.“ Mit diesem Konzept werden standardisierte Data Center insbesondere für KMU immer interessanter. „Bei uns in Stade funktionierte alles reibungslos – angefangen bei der Logistik über die Planung und Projektierung bis zum Einbau und schlussendlich zur Inbetriebnahme.“

Auch die bereits sprichwörtliche Verlässlichkeit und Verbindlichkeit des Rittal Projektteams hat wesentlich zur Entspannung beigetragen, sodass der Leiter IT-Strategie nicht Tag und Nacht von seinem Data-Center-Redundanzprojekt verfolgt wurde, sondern vor allem auch seinen eigentlichen Hauptaktivitäten nachgehen konnte. Dr. Ortlam: „Ich wusste, wir können alle Projektbeteiligten von Rittal jederzeit anrufen, angefangen beim Vertrieb bis



EINE RITTAL RAUM-IN-RAUM-STANDARDLÖSUNG  
ENTSPRICHT DAGEGEN VON  
ANFANG AN KOMPLETT  
DEN GESETZLICHEN  
KRITERIEN UND VORGABEN.

Dr. Armin Ortlam, Leiter IT-Strategie  
KHZG Controlling

hin zum Projektleiter, und wir haben auch stets eine solide und verlässliche Rückmeldung erhalten.“

### Modular und zertifiziert

Kernkompetenz der modularen Raum-in-Raum-Standardlösung von Rittal ist es, für das zukünftige Rechenzentrum in einem bereits bestehenden Gebäude einen zertifizierten Raum zu errichten, der alle vom Gesetzgeber und von den Verbänden geforderten Sicherheitskriterien erfüllt. Auf diese Weise wird ein multifunktionaler Schutzschirm gegen die meisten physischen Risiken im Bereich der Data Center-Anwendungen aufgespannt. „Unser Grundschutzraum in Stade ist 34 Quadratmeter groß und vorläufig mit acht VX IT Racks und der Flüssigkeitskühlung Liquid Cooling Package, LCP, ausgestattet. Dazu kommt noch ein spezieller, elf Quadratmeter großer Technikraum, unter anderem für die USV-Anlage, der selbst kein Bestandteil des Grundschutzraumes ist. Die Raum-in-Raum-Standardlösungen sind einfach nur genial zu nennen, vor allem für Bestandsgebäude mit genügend lichtem Raum. Zum Glück haben wir nach langer Suche in den unteren Ebenen des Krankenhauses den Platz dafür gefunden und von der Geschäftsführung das ‚Go‘ erhalten, diese als neues, noch redundantes, aber zukünftig primäres Firmenrechenzentrum zu verwenden“, so Dr. Ortlam.

### FÜNF VORTEILE DES RITTAL SICHERHEITSRAUMS

- #1** Systemgeprüftes Sicherheitskonzept auf Basis europäischer Normen
- #2** Ideal für den Einsatz in Bestandsgebäuden
- #3** Drei Ausführungsvarianten (GSR, GSR+, HVR)
- #4** Schnelle Umsetzung
- #5** Hoher Schutz gegen physikalische Risiken wie Feuer oder Wasser



Warum muss ein Rechenzentrum überhaupt in einen speziell dafür ausgestatteten Grundschutzraum einziehen, wenn doch im Kellerraum Platz ist? „Das Problem ist, dass die bauliche Substanz eines normalen Gebäudes mit seinem spezifischen Mauerwerk bereits in der Statik den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bei Weitem nicht genügt“, erklärt Dr. Ortlam. Andernfalls müsste entsprechend individuell nachgerüstet werden. Dr. Ortlam: „Eine Rittal Raum-in-Raum-Standardlösung entspricht dagegen von Anfang an komplett den gesetzlichen Kriterien und Vorgaben – und mit dem gesamten Rest, angefangen bei der Statik und Lüftung bis hin zum kompletten IT-Grundschutz, hat man als Betreiber dann nicht mehr viel zu tun.“

### Eine effektive Lösung

Ein weiteres dickes Plus sind auch die Kosten: „Mit der Raum-in-Raum-Lösung konnten wir unser Redundanz-Projekt Stade zu

einem Bruchteil der Summe einer freien Planung realisieren und sind dazu noch um einiges schneller“, zeigt sich Dr. Ortlam überzeugt, von Anfang an auf das richtige Pferd gesetzt zu haben. „Unser Projekt hat bislang in etwa eine Viertelmillion Euro verschlungen. Das klingt nach viel. Eine freie Planung im gleichen Umfang ist am Markt aber nicht unter einer Million zu haben.“ Welche Kosten genau eingespart werden können, ist von Projekt zu Projekt verschieden – je nachdem, welches Kühlmodul verwendet wird, wie hoch die Redundanz angesetzt wird, welche Server und andere IT-Geräte zum Zuge kommen und so weiter. Als Faustformel gilt den am Projekt beteiligten Experten: „Ein Krankenhaus mittlerer Größe kann mit einer Standardlösung 60 bis 70 Prozent einsparen – und für andere Dinge ausgeben“, so Dr. Ortlam.

**Harald Lutz | [www.rittal.de](http://www.rittal.de)**





# FALLSTRICKE IM LIZENZMANAGEMENT

## SCHWACHSTELLEN REDUZIEREN

Virtuelle Umgebungen stellen im Lizenzmanagement eine Herausforderung dar. Microsoft Produkte sind im gesamten Rechenzentrum präsent, erfordern korrekte Lizenzierung von Server-Betriebssystemen bis zu On-Premises-Produkten wie SQL und Exchange. Henrik van der Linde, Senior Consultant bei Aagon, beleuchtet in diesem Webinar die Fallstricke des Lizenzmanagements.

Besondere Aufmerksamkeit gilt der Lizenzfassung und -mobilität. Oft übersehene Lizenzformen, wie Client Access Lizenzen (CALs), führen zu Nachlizenzierungen in Beratungen oder Audits. Terminal Server mit Office Installation sind lizenztechnisch oft problematisch. Microsoft 365 kann Abhilfe schaffen, doch es gibt Schwachstellen in Verwaltung und Beschaffung, die wir beleuchten werden (die Fitness-Studio-Falle).

### Henrik van der Linde erklärt in diesem Webinar:

- Warum ist die korrekte Lizenzierung in virtuellen Umgebungen, insbesondere bei Microsoft-Produkten im Rechenzentrum, eine entscheidende Herausforderung
- Welche oft übersehenen Lizenzformen, wie Client Access Lizenzen (CALs), können in Beratungen oder Audits zu Nachlizenzierungsproblemen führen
- Inwiefern können Schwachstellen in der Verwaltung und Beschaffung von Microsoft 365, einschließlich der „Fitness-Studio-Falle“, zu Problemen führen



**SPRECHER:**  
**HENRIK VAN DER LINDE**

Henrik van der Linde ist seit über 20 Jahren bei der Aagon GmbH beschäftigt. Er ist als Senior Consultant mit Aufgaben in den Bereichen Beratung, Vertrieb und Durchführung von Client-Management Projekten betraut. Darüber hinaus betreut er interne und externe Trainings.

**Das Webinar** findet live am Donnerstag, 21.03.2024, von 10:00 bis 11:00 Uhr statt. Die Teilnahme ist gebührenfrei.



**JETZT KOSTENFREI  
ANMELDEN**





# INNOVATIV INS JUBILÄUM UND IN DIE ZUKUNFT

In den letzten drei Dekaden haben wir nicht nur die sich ständig verändernde Welt der Informationstechnologie dokumentiert, sondern auch dazu beigetragen, sie besser zu verstehen, anzuwenden und weiterzuentwickeln.

Über die Jahre haben wir viele Trends kommen und gehen sehen – wir haben sie vorgestellt, hinterfragt, die Weiterentwicklung beobachtet und uns auch von vielen wieder verabschiedet.

Auch der it verlag unterliegt einer kontinuierlichen Veränderung. Seit Jahren wird der Zeitschriftenbranche nachgesagt, eine aussterbende Art zu sein. Nach 30 Jahren ist it management immer noch da – sowohl als Fachzeitschrift als auch als Onlineplattform it-daily.net.

Grund genug, uns zu feiern und unseren Lesern und Kunden einmal Danke zu sagen.

# Happy birthday!

## 30 JAHRE IT MANAGEMENT

Aktuell feiern wir 30 Jahre it management. Als wir zur CeBIT 1993 auf den Markt kamen, wurden wir noch belächelt. Nach unserem Magazin DATENBANK FOKUS, war das unser zweites Magazin. Und: Es war das erste, dass das Akronym IT als Abkürzung für Informationstechnologie im Titel führte und in der Folge den Begriff EDV ablöste. Der Begriff setzte sich schnell durch. Viele Trittbrettfahrer sprangen auf den Zug auf und nutzten diesen Terminus. Doch so schnell sie kamen, so schnell gingen sie auch wieder. Was blieb war die it management. Darauf sind wir stolz.

### Fragt man mich was sich verändert hat, so kann ich nur sagen: ALLES!

Die Einführung des PCs war für die Anwender sicherlich ein Segen, für die IT an sich, die aus monolithischen, geschlossenen und sichereren Systemen bestand war es ein Desaster. Alle Probleme von heute haben ihren Ursprung in dieser Zeit. Und das Versprechen, das die IT durch Innovationen immer besser, schneller, einfacher werde, das war nichts anderes als heiße Luft.

### Grüße aus Absurdistan

Und so kamen mit immer leistungsfähigeren Systemen auch neue Software. Sie brachten uns mit: Bugs. Was in anderen Industrien völlig undenkbar wurde, wurde mit Microsoft zur Normalität erhoben. Von der Floppy Disk zur CD, Harddisk, Flash-Speicher und so weiter.

Der nächste Schub kam mit der breiten Einführung des Internets. Als Erfindungsdatum gilt noch immer das des Vorläufers „Arpanet“, nämlich der 29. Oktober 1969. An diesem Tag gelang die erste Datenübertragung, leider direkt gefolgt



von einem System-Crash. Dann war lange Jahre Sendepause. Was fehlte war ein „Sprache“. Erst 1989 kam Tim Berners-Lee die zündende Idee - es entstand das World Wide Web.

Natürlich folgten darauf viele Innovationen, aber der letzte große Move, wenn man das so sagen kann, erfolgte durch die Smartphones. Auch hier war es eine schwierige Geburt. Martin Cooper gilt als der Erfinder. Als er am 3. April 1973 das erste Mal in New York ein schnurloses Telefon nutzte, hielten ihn viele für verrückt. Bis dahin war das kabelgebundene Telefonieren noch völlig unbekannt.

Richtig los in Sachen Mobiltelefon ging es dann mit dem Motorola DynaTAC 8000X, das am 21.9.1983 auf den Markt kam. Allerdings: Erster heißt nicht gleich Bester und schon gar nicht Marktführer.

Das wurde ziemlich schnell Nokia. Doch wie vielen anderen Marktführern auch erliefte das Unternehmen der Schlaf der Gerechten und niemand anderes als Apple, sorgte für DIE Revolution in Sachen Smartphone und Benutzerfreundlichkeit.

Wer erinnert sich nicht an den legendären Satz von Steve Jobs bei den Produkt-einführungen: „But there’s one more thing...“. Am 9. Januar 2007 wurde von Steve Jobs das erste iPhone vorgestellt. Der Rest ist Geschichte.

### Und nun?

Die große Frage ist, was erwartet uns in den nächsten Jahren in der IT. Nun, ich denke, dass das Thema KI ein großes werden wird. Aber einen fast noch größeren Einfluss erwarte ich von der Einführung der Quantencomputer. Denn obwohl wir heute schon zum Großteil in der Cloud sind, Performance und Security wird durch das Quantencomputing grundlegend verändert werden.

Apropos KI: Für viele ist es ja so etwas wie die Lösung aller Probleme. Nun, das ist sie ganz sicher nicht. Wenn man zum Beispiel ChatGPT fragt, was es zu den Veränderungen in der IT seit 1991 sagt, dann bekommt man folgenden Output:

„Seit 1991 hat sich in der Informationstechnologie (IT) eine enorme Entwicklung vollzogen. Hier sind einige der wichtigsten Veränderungen und Trends:

**#1** Internet und Webtechnologien: 1991 war das Internet noch in seinen Anfängen. Die Einführung des World Wide Web durch Tim Berners-Lee im selben Jahr revolutionierte die Art und Weise, wie Informationen geteilt und abgerufen werden. Seitdem hat das Internet eine



exponentielle Expansion erlebt, mit Milliarden von Nutzern weltweit und einem unermesslichen Einfluss auf Wirtschaft, Bildung und soziale Interaktionen.

**#2** Mobiltechnologie: Die Entwicklung von Smartphones und Tablets hat die Art und Weise, wie Menschen kommunizieren und auf Informationen zugreifen, grundlegend verändert. Diese Geräte sind leistungsstark genug, um viele Funktionen eines Computers zu übernehmen, und ihre ständige Vernetzung hat zu neuen Formen der Interaktion und des Geschäfts geführt.

**#3** Cloud Computing: Die Einführung von Cloud-Diensten, bei denen Daten und Anwendungen auf entfernten Servern gespeichert und über das Internet zugänglich gemacht werden, hat die IT-Infrastruktur verändert. Unternehmen und Einzelpersonen können nun auf leistungsstarke Rechenressourcen und Datenspeicherung zugreifen, ohne eigene Hardware und Software warten zu müssen.

**#4** Soziale Medien: Plattformen wie Facebook, Twitter, Instagram und LinkedIn, die seit den frühen 2000ern entstanden sind, haben die Art und Weise, wie Menschen kommunizieren und Informationen teilen, revolutioniert. Sie haben auch neue Herausforderungen in Bezug auf Datenschutz und Informationsverbreitung mit sich gebracht.

**#5** Big Data und KI: Die exponentiell wachsenden Datenmengen und die Fortschritte in der künstlichen Intelligenz (KI) haben zu neuen Möglichkeiten in der Datenanalyse und Automatisierung geführt. KI-Technologien wie maschinelles Lernen und Deep Learning ermöglichen es, Muster in großen Datenmengen zu erkennen und intelligente Systeme für eine Vielzahl von Anwendungen zu entwickeln.

**#6** Cybersicherheit: Mit der Zunahme der Vernetzung und Digitalisierung ist auch die Bedeutung der Cybersicherheit gestiegen. Die Bedrohung durch Cyberangriffe und Datenlecks erfordert fortlaufend verbesserte Sicherheitsmaßnahmen und -technologien.

**#7** Open Source und Kollaboration: Die Verbreitung von Open-Source-Software und -Technologien hat die Art und Weise verändert, wie Software entwickelt und genutzt wird. Es ermöglicht eine breitere Kollaboration und Innovation, da Softwarequellcode für jeden zugänglich ist.

**#8** Virtuelle und erweiterte Realität (VR/AR): Obwohl noch in den Kinderschuhen, entwickeln sich VR und AR schnell und finden Anwendungen in Bereichen wie Bildung, Unterhaltung, Medizin und Industrie.

Diese Entwicklungen sind nur einige Beispiele dafür, wie sich die IT-Landschaft seit 1991 verändert hat. Sie zeigen, dass die IT-Branche einer der dynamischsten und sich schnell verändernden Sektoren ist, mit weitreichenden Auswirkungen auf fast alle Aspekte des modernen Lebens.“

#### Fazit

Doch es geht nicht ohne Human Intelligence. Zwar spielt Social Media im Consumer-Bereich eine große Rolle. Im B2B-Bereich aber ist es völlig überbewertet. KI-Plattformen hingegen sind für Google eine echte Gefahr - das universelle Wissen betreffend. Und das Metaverse? Gestern noch hochgelobt, zweifeln mittlerweile immer mehr daran. Was fehlt, ist die Idee der breiten Nutzung und des User Interfaces. Eben genau das, was für das iPhone bahnbrechend war. Da heißt es weiter: Warten auf Visionäre!

Ulrich Parthier





# Innovatives Customer Onboarding

## KUNDENBINDUNG PAR EXCELLENCE

Die Phase zwischen Vertragsunterzeichnung und Implementierungsbeginn markiert traditionell eine Zeit des Wartens für neue Kunden, in der die eigentliche Umsetzung in weiter Ferne scheint. Dabei sind gerade jetzt stilles Warten und Einreihen nicht das, was sich Kunden wünschen. „ASAP“ ist die Devise. Denn die Euphorie ist hoch - Chancen wurden erkannt und Lösungen für akute Probleme sind in Sicht.

Bei TOPdesk haben wir die Phase des „Abwartens“ daher umgebaut. Ein Team von Experten rund um die Standard-Implementierung, steht unseren Kunden unmittelbar nach Vertragsunterschrift zur Seite und begleitet aktiv die Phase vor Implementierungsbeginn.

### Unser Ansatz hierbei:

#### #1 Langfristige Kundenbeziehung:

Wir betrachten die „Post-Purchase-Phase“ als entscheidenden Faktor für eine erfolgreiche und langfristige Kundenbeziehung. Der erste Eindruck zählt, und dieser beeinflusst maßgeblich die spätere Umsetzung.

#### #2 Individuelle Fokussierung:

Wir verstehen, dass Menschen das gleiche Produkt aus unterschiedlichen Gründen kaufen. Die individuelle Ausgangssituation sowie Anforderungen unserer Kunden stehen daher im Fokus.

#### #3 Automatisierung von Planungs- und Verwaltungsaufgaben:

Durch die Automatisierung verschiedener Aufgaben wie der Terminierung, legen wir den Grundstein für eine personalisierte Betreuung, die sich auf die spezifischen

Anforderungen und Wünsche unserer Kunden konzentriert.

#### #4 Vermeidung des Wartens auf den Berater:

Wir brechen mit der Tradition des passiven Wartens auf den Berater und ermöglichen einen schnellen Start mit vorbereitenden Maßnahmen, ohne die Beratung abwarten zu müssen.

#### #5 Übertreffen von Kundenerwartungen:

Wir setzen darauf, die Erwartungen unserer Kunden bereits früh in der Customer Journey zu übertreffen, um einen bleibenden Eindruck zu hinterlassen.

### Umsetzung des Ansatzes

Das Onboarding eines neuen Kunden gilt erst als abgeschlossen, wenn ein Kunde TOPdesk produktiv einsetzt. Doch unser Fokus innerhalb des Customer Onboarding Teams liegt besonders auf Neukunden in der Phase zwischen Angebotsunterzeichnung und erstem Beratungstag. Hierbei sind uns folgende Aspekte wichtig:

➔ **Schneller Start:** Wir ermöglichen einen raschen Einstieg durch passgenaue Vorbereitungen, ohne dass Kunden auf einen Berater warten müssen. Rückfragen hierzu können aus erster Hand beantwortet werden.

➔ **Frühzeitige Beantwortung von Fragen:** Wir beantworten Fragen, die normalerweise erst beim ersten Treffen mit einem Berater besprochen würden.

➔ **Fehlerreduktion bei der Implementierung:** Durch unser tiefgehendes Wissen über TOPdesk, die Standardimplementierung und bewährte Beratungspraktiken

minimieren wir häufige Fehler während der Implementierung.

➔ **High Touch-Ansatz:** Wir betreuen Neukunden individuell und setzen dabei auf direkten Kundenkontakt. Ein Termin mit einem Mitglied des Onboarding Teams ist in der Regel bis zum nächsten Werktag möglich.

➔ **Individuelle Planung der Umsetzung:** Wir unterteilen das gesamte Projekt in sinnvolle Phasen und bringen es in eine geordnete Reihenfolge. Dabei setzen wir auf automatisierte Terminfindung durch unser 3S-System (Self Service Scheduling).

Innovation in der Kundenbindung beginnt für uns nicht erst bei der Implementierung, sondern bereits in der Phase zwischen Vertragsabschluss und Umsetzungsstart. Unser Ziel ist es, Kunden nicht nur als Käufer, sondern als langfristige Partner zu gewinnen, indem wir ihre individuellen Bedürfnisse von Anfang an ernst nehmen und erfüllen.



UNSER INNOVATIVER ANSATZ IM CUSTOMER ONBOARDING BIETET NICHT NUR EINEN SCHNELLEN START FÜR NEUE KUNDEN, SONDERN AUCH EINE LANGFRISTIGE KUNDENBINDUNG DURCH INDIVIDUELLE BETREUUNG UND FRÜHZEITIGE ERFÜLLUNG VON KUNDENERWARTUNGEN.

Christoph Hemm, Team Lead Customer Onboarding, Consultancy, TOPdesk Deutschland GmbH, [www.topdesk.de](http://www.topdesk.de)

Christoph Hemm

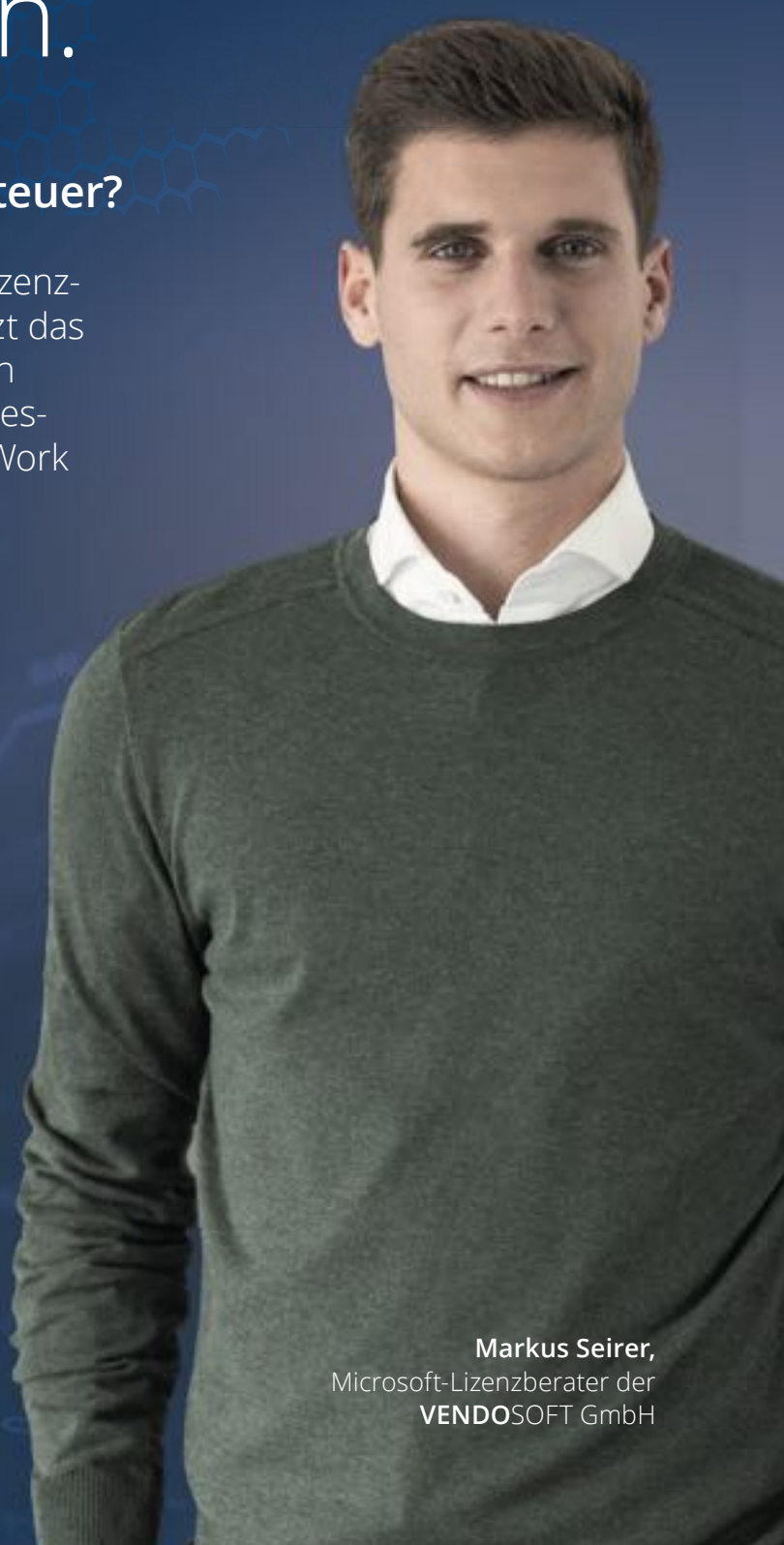
# Die **Kostenspirale** der Microsoft Cloud durchbrechen.

**M365 wird Ihnen langsam zu teuer?**

Ein modernes und kostenbewusstes Lizenzmanagement ist heute hybrid und nutzt das Beste von beidem: die fix kalkulierbaren Einmalkosten (gebrauchter!) on-premises-Software und die Vorteile für Remote-Work und Agilität aus der Cloud.

Kostenlos beraten lassen

[www.vendosoftware.de](http://www.vendosoftware.de)





# 30 JAHRE IT MANAGEMENT

WAS WIR SCHON IMMER MAL  
FRAGEN WOLLTEN

Es ist bereits fünf Jahre her, seit wir ein Spezial zum 25jährigen Jubiläum unseres Magazins *it management* veröffentlicht haben – doch es fühlt sich so an, als wäre es erst gestern gewesen.

Damals begaben wir uns auf eine kleine Zeitreise durch die technologischen Entwicklungen der letzten Jahre und versuchten einen Ausblick auf die kommenden.

Als IT-Fachmagazin ist es unsere Aufgabe aktuell zu sein und Unternehmen hinsichtlich ihrer Strategien und Lösungen zu befragen, manchmal auch zu hinterfragen.

Diese Interviews führt hauptsächlich unser Chef Ulrich Parthier. Für unser Jubiläum werden ausnahmsweise mal die Seiten getauscht und wir, das Team von *it management* und *it daily*, stellen Fragen an Silvia und Ulrich Parthier.

**EVA NEFF,**  
Buchhaltung,  
im Team seit 1994

? Gab es in den 30 Jahren irgendwann mal die Überlegung das Magazin einzustellen?

**Silvia:** Aus rein finanzieller Sicht hätten wir *it management* gleich in den ersten Jahren einstellen müssen. Wir waren aber von dem Konzept überzeugt, dass sich nicht nur reine Techies über IT informieren müssen, sondern auch die Menschen auf der Management-Ebene.

Heute im Zeichen der Digitalisierung war die Entscheidung für unsere Online-Plattform [www.it-daily.net](http://www.it-daily.net) eine goldrichtige Entscheidung. Wir haben stets wegweisende und richtige Entscheidungen getroffen. Bei *it-daily* geht es jetzt aber erst richtig los. In Kombination mit Print und einem cross-medialen Konzept sind wir bestens positioniert.

? Wie hat sich die Qualität der eingereichten Texte von den Anfängen bis heute entwickelt, besonders im Zusammenhang mit der wachsenden Onlinepräsenz von Unternehmen und PR-Agenturen?

**Ulrich:** Früher haben Technik-Begeisterte für unsere Magazine geschrieben. Das hat man in jedem Satz gespürt. Und alle Fachbeiträge waren technisch sehr tiefgehend. Heute müssen wir gezielt nach diesen Deep-Dive-Artikeln suchen. Viele eingereichte Beiträge sind zu dürrig oder nicht-exklusiv. Wir arbeiten mit Fachautoren und PR-Agenturen daran, das zu ändern. Vielleicht bringen alle die neuen KI-Themen auch wieder etwa Enthusiasmus in die Texte.



**KAREN REETZ,**  
Media Consultant, im  
Team seit 2008







**CARINA MITZSCHKE,**  
Redakteurin,  
im Team seit 2007

? *Ihr habt beide Fächer außerhalb der IT studiert. Wie kommt man auf die Idee dann ein IT Magazin zu gründen?*

**Ulrich:** Eigentlich hatte ich einen Platz in der Sportfördergruppe der Bundeswehr erhalten, konnte aber durch eine glückliche Fügung abspringen. So lief das Leben in eine andere Richtung, geografisch wie berufsmäßig. Studium für das Gymnasiallehramt in den Fächern Deutsch, Gemeinschaftskunde, Geschichte und Sport mit Abschluss, danach in Paderborn zur Nixdorf Computer AG und dann folgte wieder die Entscheidung, zurück in die Heimatstadt oder nach München als Redakteur einer neugegründeten Computer Wochenzeitung. Ich arbeitete als freier und fester freier Redakteur, bevor ich zusammen mit meiner Frau den Verlag gründete – der Traum eines jeden Journalisten. Unser erstes Team, das waren wir allein in einem Kellerbüro, quasi das Pendant zum US-Garagen Start-up.

**Silvia:** Eigentlich wollte ich ja Informatik studieren. Es wurde mir aber von allen ausgeredet. „Nur IBM stellt ein paar Informatiker ein.“ „Das ist doch nichts für Frauen“, so die Berufsberatung. Daraufhin habe ich in Regensburg Volkswirtschaftslehre mit Schwerpunkt auf Statistik, Ökonometrie und Wirtschaftsinformatik studiert. Das war eigentlich noch viel besser als pure Informatik. Während des Hauptstudiums habe ich als Apple Promoter gejobbt und mit meinem damaligen Freund das Buch „UCSD-Pascal“ geschrieben. Als erste Frau an der Uni Regensburg habe ich einen Pascal-Programmierungskurs geleitet. Da sind viele Kommilitonen nur hingegangen, um sich die „Pascal-sprechende“ Frau anzuschauen und auf Fehler zu lauern. Insofern musste man immer perfekt vorbereitet sein.

? *Wie sah Eure Vision vor 30 Jahren aus? Wie hat sie sich im Laufe der Zeit entwickelt und inwiefern ist sie heute zur Realität geworden?*

**Ulrich:** 1991 gab es in den USA drei Datenbankmagazine. In Deutschland wollte kein Verlag etwas davon wissen. Die dachten alle, dass es dBASE III ewig geben wird. Ein Irrtum und die Geburtsstunde von DATENBANK FOKUS, 1994 folgte it management einfach aus dem Grund, nicht nur auf einem Standbein zu stehen und 2002 schließlich it-daily.net als logische Entwicklung des Internet-Booms.



**VICKY MIRIDAKIS,**  
Head of Marketing,  
im Team seit 2016,  
Geschäftsführung  
seit 2024

? *Was war die größte Krise, die Ihr in 30 Jahren überwinden musstet und welche Tipps würdet Ihr insbesondere jungen Unternehmern rückblickend geben?*

**Ulrich:** Die Internet-Blase und die Finanzkrise. Da mussten wir innerhalb einer Woche entscheiden, ob die Umsatzeinbrüche von rund 50 Prozent in einem Monat systemrelevant waren oder nur ein Ausrutscher und sofort Kosten einsparen.

Mein Tip für junge Unternehmer: Start small, think big! Das wird sich bei it-daily in den nächsten Wochen auch zeigen.



**VALERIE PARTHIER,**  
Online-Redakteurin,  
im Team seit 2010

? *Ihr habt den Verlag vor 30 Jahren gemeinsam gegründet. Was ist das Geheimnis Eurer harmonischen und erfolgreichen Zusammenarbeit?*

**Silvia:** Gute Frage. Ich konzentriere mich auf redaktionelle Themen und das Online-Kampagnenmanagement, Ulrich auf die Themen Business Development, Sales-Unterstützung, Innovationen und Qualitätsmanagement.



**PAULINE DORNIG,**  
Online-Redakteurin,  
im Team seit 2020



**KERSTIN FRAENZKE,**  
Head of Media  
Consulting,  
im Team seit 2015

**?** Nachdem Ihr in den letzten 30 Jahren - von ISDN bis KI - unglaublich viele unterschiedliche Themen mitbekommen habt, würde es mich interessieren, welches Themenfeld Ihr persönlich am faszinierendsten fandet?

**Silvia:** Jedes Thema hatte seine Zeit. Der Aufstieg der relationalen Datenbanksysteme in den Neunzigern, die 2000er Jahre mit dem Aufstieg des Internets, die Jahre ab 2010 mit dem Beginn der IT-Sicherheitsproblematik und schließlich die 20er mit Themen wie Metaverse, NFT, Blockchain und KI/ML.



**ROXANA GRABENHOFER,**  
Online Marketing  
Manager, im Team  
seit 2021

**?** Was waren Eure größten Erfolge? Auf was seid Ihr besonders stolz?

**Ulrich & Silvia:** Unser jetziges Team. Als alle zu Beginn der Pandemie auf die Bremse getreten haben, haben wir entschieden genau das Gegenteil zu tun. Alles richtig gemacht!

**?** Neben der Arbeit, den ständigen Terminen und vorausschauenden Planungen braucht es auch mal Pausen. Welche Orte oder Länder stehen auf Eurer Reise-to-Do-Liste ganz oben?

**Ulrich & Silvia:** Das entscheiden wir von Jahr zu Jahr. Fixpunkt ist im Sommer Griechenland, dieses Jahr im März Skifahren in Sun Peaks/Kanada und dann gibt es immer noch mal eine Städtetour in Europa. Wenn dann noch Zeit bleibt, nehmen wir gern eine Woche Wanderurlaub zur Regeneration im Herbst.



**DANIELA SEEBER,**  
Online-Redakteurin,  
im Team seit 2020



**JENNIFER KALISCH,  
BRIGITTE SCHÖN,**  
Grafikerinnen,  
im Team seit 2019

**?** Wenn es mit der KI-Entwicklung so weiter geht wie bisher, sind wir Gestalter in den kommenden Jahren ja bald überflüssig. Denkt Ihr, dass das Layout unserer Magazine durch den Einsatz von KI noch genauso kreativ, lustig und auf die individuellen Kundenwünsche zugeschnitten werden kann, wie mit uns?



**LARS BECKER,**  
Redakteur,  
im Team seit 2021

**?** Was war für Euch die disruptivste technische Innovation oder Entwicklung in den letzten 30 Jahren?

**Silvia:** KI, Mobilfunk und Internet, alles sind disruptive Innovationen. 1993 haben mir zwei Kollegen gezeigt, wie man mit Studenten in Kalifornien über ein weltweites Netzwerk hin- und herschreibt. Das war mein erster „Chat“! Ich fand das total cool. Das iPhone fasziniert mich seit ich es im Dezember 2007 zum ersten Mal in der Hand hielt. Heute spiele ich mit diversen KI-Tools und bin begeistert. Am faszinierendsten ist auf jeden Fall das Internet. Ohne das Web gäbe es weder das Smartphone noch die KI.

**Silvia:** Auf Euch Kreative möchte ich niemals verzichten! Eure Ideen sind super. KI kann Grafiker/innen unterstützen, die eigenen Ideen schneller und vielleicht sogar noch besser umzusetzen, es kann als Sparringspartner dienen. Egal ob Grafik, Redaktion, Sales oder Kampagnenmanagement Human Intelligence bleibt immer die Nummer 1!



DANKE UND  
WEITERHIN  
VIEL ERFOLG



# eIDAS Summit 2024

BUSINESS & PROZESSE SICHER  
UND EINFACH DIGITALISIEREN

Digitale Prozesse lassen sich nicht mehr aus unserem Leben wegdenken und sind der Schlüssel für effiziente Unternehmen und eine funktionierende Verwaltung. Deswegen ist es essenziell, dass sie nicht nur schnell und einfach, sondern auch sicher und vertraulich eingesetzt werden können. Um dabei auch vom europäischen Binnenmarkt zu profitieren, müssen Unternehmen und Arbeitnehmende ortsunabhängig und über Ländergrenzen hinweg agieren können. Genau das regelt die eIDAS-Verordnung: Unternehmen

können mit elektronischen Identifizierungsmitteln und Vertrauensdiensten digitale Dokumente wie Angebote, Bestellungen und Verträge rechtssicher, effizient und transparent innerhalb der EU austauschen und so Geschäfte abwickeln. Für Wirtschaft und öffentliche Verwaltung bieten sich große Chancen und neue Entwicklungsmöglichkeiten.

Wie die Digitalisierung von papierbasierten Transaktionen, betrieblichen Abläufen und Geschäftsprozessen erfolgreich

umgesetzt werden kann, besprechen wir auf dem eIDAS Summit des Bitkom. Deutschlands führende Konferenz rund um Digital Trust & Identity bringt am 16. April 2024 Fachleute aus Politik, Wirtschaft und Technologie zu einem digitalen, branchenübergreifenden und interaktiven Austausch zusammen.

Auf dem #eidas24 erleben Sie ein vielfältiges Programm aus interaktiven Workshops, aufschlussreichen politischen Keynotes, Best-Practice-Beispielen und konkreten Handlungsempfehlungen aus der ganzen EU. Entdecken Sie Technologietrends, diskutieren Sie über die eIDAS-Verordnung und erweitern Sie Ihr Netzwerk. Jetzt Tickets sichern und dabei sein!



bitkom  
events

eIDAS

# USU Means Service

**Software und Services – USU verknüpft beides.**

Und veredelt dies mit der Beratungs-Kompetenz aus 45 Jahren Erfahrung. **Wir sind Service-Meister** und liefern Lösungen für IT & Kundenservice-Organisationen – überall dort, wo Menschen und Systeme zusammentreffen.

Erfahren Sie mehr unter [www.usu.com](http://www.usu.com)

**USU**



# E-RECHNUNGSPFLICHT

## WIE SICH UNTERNEHMEN EFFEKTIV VORBEREITEN

Ab Januar 2025 wird die Papierrechnung im deutschen Geschäftsverkehr voraussichtlich durch die strukturierte E-Rechnung ersetzt. Deutschland steuert auf eine E-Rechnungspflicht im B2B-Bereich zu.

E-Rechnungen müssen, um als solche zu gelten, in einem strukturierten elektronischen Format (entsprechend der CEN-Norm EN 16931 aus Richtlinie 2014/55/EU) ausgestellt, übermittelt und empfangen werden. Sie müssen sich elektronisch verarbeiten lassen, die erforderlichen Angaben müssen vollständig und richtig extrahiert werden können. Technisch erfüllen dieses E-Rechnungserfordernis die Formate XRechnung sowie ZUGFeRD 2.x. Von einer E-Rechnung spricht man auch dann, wenn der strukturierte Teil um einen visuellen ergänzt wird, in der Regel ein PDF (hybrid).

Zur Annahme und Verarbeitung von digitalen Eingangsrechnungen benötigt man eine entsprechende Softwarelösung, wie sie die xSuite Group anbietet. Spezielle E-Invoicing-Dienstleister übernehmen die Übermittlung und sorgen dafür, dass die Empfänger Rechnungen immer im gewünschten Format zugestellt bekommen. Die Auswahl der passenden Technologien und Partner sollte man gründlich vorbereiten, idealerweise durch Bildung eines abteilungsübergreifenden Projektteams „E-Invoicing“.

In diesem Gremium wird zunächst geklärt, welche rechtlichen Voraussetzungen für das eigene Unternehmen überhaupt gelten. Es findet außerdem eine Analyse der bisherigen Struktur der Rechnungseingangs- und -ausgangsprozesse statt: Wie sind die Durchlaufzeiten, welche Kosten entstehen hier? Dem schließt



**JEDES UNTERNEHMEN  
SOLLTE SICH IDEALERWEISE  
DAHER DARAUF VORBEREITEN,  
AB 1.1.2025 E-RECHNUNGEN  
ANNEHMEN,  
VERARBEITEN UND ARCHIVIEREN  
ZU KÖNNEN.**

Dina Haack, Head of Marketing,  
xSuite Group GmbH, [www.xsuite.com](http://www.xsuite.com)

sich eine Bewertungsphase an, innerhalb derer untersucht wird, inwieweit sich die Prozesse optimieren lassen und welche Einsparungen durch die Verlagerung von Input- und Output-Anwendungen in die Cloud möglich sind. Auch ist im Rahmen einer Kreditoren- und Debitorenanalyse zu klären, welche Geschäftspartner überhaupt in der Lage sind, E-Rechnungen zu senden und zu empfangen.

Wichtig ist, alle Stakeholder, die mit Rechnungen zu tun haben, von Anbeginn an mitzunehmen und dafür zu sorgen, dass sie ein richtiges Verständnis für das Thema entwickeln. Zeitziele aufgrund rechtlicher Fristen sowie qualitative Ziele zur Prozessoptimierung müssen rechtzeitig kommuniziert werden. Aus den genannten Analysen und Zielvorgaben entsteht schließlich ein Anforderungskatalog, auf Basis dessen die Auswahl von

Softwareanbieter und Dienstleister stattfinden kann.

### Fristen

Die Regelungen zur E-Rechnungspflicht finden sich im November 2023 vom Bundestag beschlossenen Wachstumschancengesetz. Mittlerweile liegt dieses im Vermittlungsausschuss. Der früheste Zeitpunkt im Falle einer Einigung zwischen Bundestag und Bundesrat unter „Moderation“ des Vermittlungsausschusses zur Verabschiedung des Gesetzes ist die Bundestagssitzung am 22.03.2024.

Bei der Umstellung räumt der Gesetzgeber Übergangsfristen ein. Bis zum 31.12.2026 darf man weiterhin Papierrechnungen verschicken, ebenso wie andere elektronische Formate (nur, wenn der Empfänger einwilligt). Die Papierrechnung hat dann keinen Vorrang mehr. Wer bereits ab 1.1.2025 vollständige elektronische Rechnungen verschicken möchte, kann dies tun – der Empfänger hätte dann die Verpflichtung zur Annahme.

Jedes Unternehmen sollte sich idealerweise daher darauf vorbereiten, ab 1.1.2025 E-Rechnungen annehmen, verarbeiten und archivieren zu können. Gleiches gilt für den Versand von steuerbaren und steuerpflichtigen B2B-Rechnungen im Inland, der ab dann elektronisch in einem strukturierten Format erfolgen muss. Ausgenommen sind Kleinbetragsrechnungen bis 250,- € netto und Fahrausweise.

Es gilt also, sich rechtzeitig zu informieren und frühzeitig „seinen“ Anbieter für Annahme und Versand von E-Rechnungen auszuwählen, um eine Umstellung fristgerecht vornehmen zu können.

**Dina Haack**



Dein ERP. Deine KI. Dein Flow. Dein APplus.

# MEHR POWER. WENIGER BLABLA.

APplus 8.  
Effizienz auf den Punkt gebracht.

[applus-erp.com](https://applus-erp.com)

**asreco**  
SOLUTIONS

# Archivdaten und die digitale Transformation

## ALTDATEN: MEHR EINE RECHTLICHE ALS TECHNISCHE HERAUSFORDERUNG

Im Schnitt verdoppelt sich die Menge der Geschäftsdaten alle zwei Jahre. Gleichzeitig müssen Systeme durch moderne ersetzt und transformiert werden. Spätestens dann stellt sich die Frage, welche Daten auf die neue Lösung übernommen werden und was mit den Altdaten geschieht. Nicht selten stößt man hier auf Fragen des Rechts und der Compliance.

Unternehmen entscheiden sich beispielsweise für SAP S/4HANA, weil sie sich von den neuen Funktionen einen Vorsprung versprechen oder weil sie es wegen der Support-Abkündigung der Altsysteme müssen. In diesen Fällen steht immer das Management der Bestands- und Altdaten auf der Aufgabenliste. Wird man alle Daten auf das neue System transformieren oder besser per selektiver Data-Transition die alten von den aktuellen Daten trennen? Welche Altdaten dürfen oder müssen gelöscht werden und welche unterliegen Aufbewahrungsfristen oder gar Compliance-Vorschriften?

### Umgang mit Archivdaten

Beim Transformationsmanagement von Daten gibt es einiges zu beachten, dar-

unter die gesetzlichen Aufbewahrungs- und Löschfristen. Für steuerrechtliche Unterlagen gilt in der Regel eine Aufbewahrungsfrist von sechs oder zehn Jahren. Verträge, Urkunden oder Patientenunterlagen müssen oft mehrere Jahrzehnte vorgehalten werden. Aber auch datenschutzrechtliche Bestimmungen und die Pflicht, personenbezogene Daten zu löschen, sobald der Zweck ihrer Erhebung entfällt, bestimmt das Vorgehen beim Datenmanagement einer Transformation.

### Altsystem behalten oder stilllegen

Der positive Aspekt: Gesetzliche Vorschriften verpflichten Unternehmen zur Aufbewahrung bestimmter Daten, nicht aber zum Weiterbetrieb alter Systeme. Das heißt, dass für die Archivierung und fristgerechte Löschung von Altdaten geeignete Archivierungslösungen beziehungsweise Data-Retention-Management-Systeme in Frage kommen. Diese sind im Vergleich zum weiteren Betrieb alter Operativsysteme eine kostengünstige Alternative. Wichtigste Kriterien bei der Wahl eines solchen Systems sind die Revisionssicherheit, die Einhaltung der DSGVO und dass die Archivierung nur für



ELEMENTAR BEI DER TRANSFORMATION IST DAS REGELKONFORME UND ZUGLEICH WIRTSCHAFTLICHE MANAGEMENT VON ALT- UND ARCHIVDATEN.

Philipp von der Brüggen,  
CMO, Natuvion, [www.natuvion.de](http://www.natuvion.de)

Berechtigte zugänglich und dokumentierbar sowie die Einhaltung der jeweiligen Aufbewahrungsfristen gewährleistet ist.

### Automatisiertes Einhalten von Fristen und Regeln

Ein elementarer Schritt bei der Datenarchivierung ist das Festlegen, was in Zukunft wann mit welchen Daten passieren soll. Hierbei können moderne Lösungen helfen, die künftige Archivierung zu automatisieren. Der Natuvion Intelligent Data Store (IDS) wurde als ein DSGVO-konformes „Lager“ für Altdaten, egal, aus welchem Quellsystem, entwickelt. Einmal die Archivdatenkategorisierung festgelegt und die Automatisierung durchlaufen, hält die Lösung gesetzliche Aufbewahrungsfristen und die Datenschutzkonformität ein. Beispielsweise erfolgt die Löschung periodisch oder nach vorab festgelegten Fristen. Ein weiterer Vorteil: Die kostspieligen Altsysteme werden stillgelegt und die Daten (Read Only) stehen weiterhin zur Verfügung – ein Muss für die Steuer- und Wirtschaftsprüfung oder für die Fachrecherche. Sicherheitsrisiken wie etwa der Weiterbetrieb von alten und unsicheren Systemen sind ebenso passé, wie hohe Betriebs- und Lizenzkosten für Altsysteme.

Philipp von der Brüggen





# Wi-Fi oder DECT?

ENTSCHEIDEND IST DER  
EINSATZZWECK

Die wachsende Notwendigkeit von Mobilität beziehungsweise die in Zeiten von geteilten Arbeitsplätzen nicht vorhandene Netzwerkverkabelung führen in der Telekommunikationsbranche immer häufiger zu Diskussionen darüber, welcher Technologie der Vorzug zu geben ist.

## Das Funksignal

DECT und WLAN sind drahtlose Technologien, die ein Signal von einem Punkt zum anderen via Funkwellen übertragen. Normalerweise übertragen niedrigere Frequenzen zwar weniger Informationen, legen jedoch längere Strecken zurück, bevor das Signal abnimmt. Umgekehrt bieten hohe Frequenzen meist eine sehr gute Qualität, haben aber eine deutlich eingeschränkte Reichweite.

## DECT versus Wi-Fi

DECT ist ein auf die Sprachübertragung spezialisiertes Protokoll. Im Gegensatz zu WLAN (oder Wi-Fi) wird die Sprachübertragung bei DECT kaum von externen Faktoren gestört. Da das WLAN ursprünglich zur Datenübertragung konzipiert wurde, ist es etwas störanfälliger im Bereich der Kommunikationsübertragung. Beide ermöglichen aber, sich im Gespräch innerhalb eines geografisch begrenzten Bereichs zu bewegen – je nach Abdeckung durch Accesspoints oder Zellen.

## Die Vorteile der DECT-Technologie

Allein aufgrund der Frequenz (zwischen 1.880 und 1.900 MHz) bietet DECT eine größere Signalabdeckung als WLAN (zwischen 2.400 und 6.000 MHz) mit ungefähr 300 m im Freien gegenüber den 100 m von Wi-Fi. Dadurch werden viel weniger Antennen benötigt. Die Akkulaufzeit von DECT-Geräten ist im Allgemeinen wesentlich länger, während Wi-Fi die Akkus der Endgeräte stark beansprucht. Da es sich um ein dediziertes Netzwerk handelt, weist DECT zudem eine bessere Qualität und keine Bandbreitenprobleme auf. Und: Die Endgeräteauswahl ist bei DECT breiter aufgestellt und funktionaler (zum Beispiel Staub- und Wasserschutz, Stoßfestigkeit, AlarmpFunktionen).

## Die Vorteile der Wi-Fi-Technologie

Der Einsatz von Wi-Fi-Telefonen ist normalerweise anfänglich kostengünstiger. Mittlerweile verfügen alle Unternehmen über WLAN-Accesspoints, womit Endgeräte verbunden werden könnten. Aber Wi-Fi-kompatible schnurlose Telefone sind häufig in der Anschaffung viel teurer als DECT-Modelle.

Wi-Fi ist immer dann von Vorteil, wenn ein unverhältnismäßig großer Unterschied zwischen Antennen und eingesetzten Endgeräten besteht. Benötigen etwa in einem fünfstöckigen Hotel lediglich zwei Personen schnurlose Telefone, ist die Verwendung eines Wi-Fi-Schnurlostelefon ratsam, da die Kosten für die Abdeckung der gesamten Struktur mit DECT-Zellen im Verhältnis zu nur zwei Benutzern viel zu hoch wären.

Auch die auf Smartphones installierten Apps ermöglichen es, von den VoIP-Vorteilen über Wi-Fi-Netzwerke zu profitieren. Diese Lösung ist allerdings meistens nicht für Umgebungen wie Produktionsstätten oder Lagerhallen geeignet, da die baulichen Gegebenheiten wie Stahlbeton oder Stahltüren das WLAN-Signal stören.

## Schlussfolgerungen

Wie so oft kommt es bei der Wahl von DECT oder WLAN vor allem auf die Art des Einsatzes an. In einem Unternehmensumfeld wie Büros, Produktion oder Lager ist der Einsatz eines DECT-Antennennetzwerks zu empfehlen, da es dediziert, stabiler und eindeutig flexibler ist. Darüber hinaus ermöglicht es die Einbindung von Automations-, Alarmierungs- oder Live-Tracking-Komponenten, deren Betriebskontinuität durch keine weiteren Aktivitäten der Organisation beeinträchtigt wird. Soll die Option jedoch nur sporadisch und für wenige Mitarbeiter zur Verfügung stehen, ist sicher ein Einsatz über WLAN absolut ausreichend.

[www.snom.com](http://www.snom.com)

Adobe Stock | 717164773



# USU MEANS SERVICE

„WIR SIND EIN TEIL  
VON JENER KRAFT, DIE STETS  
DAS GUTE WILL UND  
DESHALB SOFTWARE  
SCHAFFT...“

Inspiziert durch Goethe möchten wir als USU mit unseren Kunden gemeinsam Technologien schaffen, die Menschen mitreißen und begeistern - weit über binäre Codes hinaus. Denn echte Power entsteht erst in der praktischen Anwendung.

Das war und ist unsere Devise von Anfang an. Denn wer Software entwickelt, hat es mit Menschen zu tun. Mit ihren Ideen, Fähigkeiten, ihrem Wissen, ihren Defiziten - mit ihrer Persönlichkeit. Als Softwarehaus ist es Teil unserer DNA, dass wir uns ständig weiterentwickeln. Denn IT-Wissen hat nur noch eine Halbwertszeit von zwei Jahren. Insofern mussten wir uns schon einige Male neu erfinden. Was 1977 als Udo-Strehl-Unternehmensberatung begann, ist heute ein mittelständisches IT-Unternehmen mit über 800 Mitarbeitenden. Das erste Büro in Möglingen bei Ludwigsburg ist längst durch viele Geschäftsstellen und Niederlassungen rund um den Globus ergänzt worden. Doch die internationalen Kommunikationswege lau-

fen nach wie vor in der Möglinger Zentrale zusammen.

## Service. Wow!

Software und Services - wir verknüpfen heute beides. Und veredeln dies mit der Beratungs-Kompetenz aus 45 Jahren Erfahrung. Wir liefern Service für Service - vor allem dort, wo Menschen und Systeme zusammenkommen. Intelligente USU-Lösungen ermöglichen es Unternehmen, sich mit hochwertigen Dienstleistungen vom Wettbewerb abzuheben. Das betrifft vielfältige Service-Themen in Organisationen, aber auch im Alltag als Endkunde oder Bürger. Bei Volkswagen beispielsweise profitiert die Qualitätssicherung, der weltweite technische Kundendienst und alle Automobilisten bei einer Panne, bei der Wüstenrot & Würt-

tembergischen, Robert Bosch oder der Bundeswehr profitiert die IT, bei der einheitlichen Bürgerhotline 115 über 30 Millionen Bürgerinnen und Bürger. Immer geht es darum, Wissen in die Geschäftsprozesse zu integrieren.

## Anwendungs-Innovator für KI, Cloud & Co.

Als Softwarehaus leben wir von neuen Ideen und neuen Technologien. Daher sind wir ganz vorne dabei, wenn es um Innovationen geht. Im Mittelpunkt der Forschung stehen Zukunftsthemen wie Cloud-Lösungen oder Künstliche Intelligenz. Entscheidend ist, dass aus diesen abstrakten Technologien beim Einsatz in realen Use Cases konkrete Unternehmenswerte gewonnen werden. Ein gutes Beispiel ist der Einsatz von intelligenten Chatbots im Customer Service. Das Technologiekonzept von miteinander vernetzten Chatbots - eines „USU Bot Universe“, ist nach Ansicht von US-Markt-Analysten einzigartig. Damit lassen sich mit geringem Aufwand sehr leistungsfähige Dialogsysteme aufbauen und aufgrund der Multibot-Architektur auch generative KI-Sprachmodelle wie ChatGPT integrieren - zum Beispiel für das automatische Erstellen von FAQ-Dokumenten.

Mit der dynamisch steigenden Nutzung von Cloud-Ressourcen wird auch die Fähigkeit, diese Kosten-optimiert zu nutzen, zur großen Herausforderung. Mit unserer Expertise im Bereich IT Service, IT Monitoring und Software Asset Management haben wir uns dem Thema „Cloud Cost Management“ verschrieben. Mit Erfolg. Unsere Managed Services liefern die Datengrundlage zur Cloud-Kostenoptimierung. Und erfahrungsgemäß liegt der ROI bei nur wenigen Monaten.

**Dr. Thomas Gerick | [www.usu.com](http://www.usu.com)**

## AUF EINEN BLICK

- > 800 Mitarbeitende
- ~ 132 Mio. € Umsatz
- > 1.200 Kunden weltweit
- > 2,2 Millionen Nutzer in 185 Ländern

## Kompetenzfelder:

IT Service & Enterprise Management, Knowledge Management, Software Asset Management, IT Monitoring, Digital Consulting







# Intelligente Automatisierung für E-Invoicing und P2P-Prozesse

## Wir schließen für Sie jede Lücke

- Digitale, KI-gestützte Rechnungsverarbeitung
- Annahme und Verarbeitung von E-Rechnungen
- Einbindung von E-Rechnungsportalen inkl. Peppol
- Durchgängige Bestell- und Rechnungsprozesse (P2P)



Webinare zum Thema



# DIGITALE TECHNOLOGIE IM GLOBALEN WANDEL

## CHANCEN EINER SICH SCHNELL VERÄNDERNDEN WELT NUTZEN

Unsere Welt durchlebt eine dramatische Phase des Wandels. Wir alle stehen vor erheblichen Herausforderungen in Bezug auf Umwelt und Gesellschaft. Vom Klimawandel über den Verlust biologischer Vielfalt bis hin zu Ressourcenknappheit – die natürliche Umwelt und die von uns geschaffene Welt sind durch unseren Lebensstil und die Art und Weise bedroht, wie die Menschheit expandiert und sich weiterentwickelt. Deshalb müssen wir Veränderungen herbeiführen.

In diesem eBook greifen wir einige der wichtigsten Herausforderungen auf, vor denen die Weltbevölkerung steht. Welche Rolle spielen Unternehmen in diesem Zusammenhang? Wie kann der intelligente Einsatz von Technologie uns alle auf dem Weg in eine positivere Zukunft unterstützen?

## INHALT:

1. Die zunehmende Bedrohung durch Cyberangriffe und -kriege
2. Neue Technologien und Softwaresysteme
3. Der Einzug der Generation Z in den Arbeitsmarkt
4. Die Klimakrise
5. Zunehmende Globalisierung
6. Digitale Verantwortung und die Einbeziehung von Mitarbeitern



**38 %**  
mehr **Cyberangriffe**  
im Jahr 2022 als im  
Jahr 2021



Das eBook umfasst 33 Seiten und steht zum kostenlosen Download bereit.  
[www.it-daily.net/download](http://www.it-daily.net/download)

# EFFIZIENZ-BOOST GEGEN FACHKRÄFTEMANGEL

## PRODUKTIVITÄTSSTELLSCHRAUBE ERP



Die Annonce ist geschaltet, doch Bewerbungen bleiben aus – der Fachkräftemangel hat die Unternehmen fest im Griff. Um weiterhin erfolgreich zu sein, brauchen sie effizientere IT-Lösungen, die ihnen deutliche Produktivitätsgewinne verschaffen. Dies gilt insbesondere für das ERP-System, den Motor ihrer Geschäftsprozesse.

Gut 1,3 Millionen offene Stellen gab es 2022 in Deutschland, knapp die Hälfte davon (0,63 Millionen) konnte bereits rein rechnerisch nicht besetzt werden – so die Zahlen des Kompetenzzentrums für Fachkräftesicherung (KOFA) im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Ein Trend, der

sich in den kommenden Jahren noch weiter verschärfen wird, denn mehr und mehr Babyboomer erreichen das Rentenalter und dringend benötigte Nachwuchstalente bleiben aus.

Wenn bestehende Teams vielfach bereits heute am Anschlag arbeiten, bleibt Unternehmen oft nur die verwendete Technologie als Stellschraube für mehr Effizienz. Als zentrales IT-System der meisten Unternehmen birgt dabei vor allem das ERP-System ein hohes Effizienzpotenzial. Nicht zuletzt, da entsprechende Lösungen bislang in der Regel einem datenzentrierten Ansatz folgen: Sie stellen Anwendern eine Fülle an Informationen, Schaltflächen und Masken bereit, aus denen die Nutzer die benötigten Daten selbst auswählen und erforderliche Arbeitsschritte in der richtigen Reihenfolge bearbeiten müssen – ungewünschte Verzögerungen inklusive.

### Komplexität reduzieren, Geschwindigkeit verdoppeln

Verbessern lässt sich die Effizienz dieser Arbeitsschritte beispielsweise durch die Einführung einer benutzerfreundlichen Prozessschicht. Durch sie wird es möglich, zentrale ERP-Aufgaben in übersichtlichen, geführten Einzelschritten zu bearbeiten, die passgenau den individuellen Erfordernissen des jeweiligen Unternehmens entsprechen. Die Komplexität sinkt, die Qualität der Prozessbearbeitung steigt: Dadurch, dass die Benutzer einer klaren Prozessstruktur folgen können und stets nur angezeigt bekommen, was für sie aktuell relevant und erforderlich ist, sind auch Fehlerquellen deutlich reduziert.

In der Folge wird es Anwendern möglich, ihre täglichen Aufgaben deutlich schneller als bislang zu erledigen: Verschiedene Tests in der Praxis haben gezeigt, dass ERP-Nutzer ihre Abläufe mithilfe einer klar strukturierten Prozessebene je nach konkreter Aufgabe doppelt bis zweieinhalbmal so schnell erledigen können wie in der klassischen, datenzentrierten Welt.

### Wettbewerbsfähigkeit erhalten und stärken

Ein weiterer Vorteil einer geführten Prozessebene besteht darin, dass auch fachfremde Kollegen deutlich schneller eingelernt und produktiv arbeiten können. Schließlich gibt die Prozesssicht den jeweils nächsten erforderlichen Schritt vor und fragt alle dazu benötigten Daten aktiv vom User ab. Dies wiederum verschafft Unternehmen die Möglichkeit, personelle Engpässe flexibler auszugleichen und zu kompensieren.

Kurz- bis mittelfristig ist mit einer Besserung der angespannten Fachkräftesituation in Deutschland nicht zu rechnen. Genau wie Unternehmen und ihre Mitarbeiter gilt es daher auch für IT-Systeme, sich der heutigen Arbeitsrealität anzupassen und Möglichkeiten zu bieten, den Herausforderungen des modernen Arbeitsmarkts gerecht zu werden. Eine prozessorientierte Nutzungsweise kann hier ein entscheidender Schritt zu mehr Effizienz sein, die Unternehmen die dringend benötigte Entlastung verschafft und ihre Wettbewerbsfähigkeit auch mit einer dünneren Personaldecke bestmöglich erhalten und stärken hilft.

**Ralf Bachthaler**



EIN VORTEIL EINER GEFÜHRTEN PROZESSEBENE BESTEHT DARIN, DASS AUCH FACHFREMDE KOLLEGEN DEUTLICH SCHNELLER EINGELERNT UND PRODUKTIV ARBEITEN KÖNNEN.

Ralf Bachthaler, Vorstand,  
Asseco Solutions AG,  
[www.applus-erp.com](http://www.applus-erp.com)



# Managed Services

WIR SIND FLEXIBLE „IT-HAUSMEISTER“ MIT GROSSER VERANTWORTUNG

Der IT-Fachkräftemangel hat den Mittelstand fest im Griff: Erfahrenes Personal fehlt in allen Branchen und in Betrieben jeder Größe. Administratoren haben alle Hände voll mit einem steigenden Aufkommen an Aufgaben zu tun. Für wichtige Projekte sind kaum noch Kapazitäten frei im Kopf. Zwar lässt sich manches automatisieren – ein großer Teil der Aufgaben verlangt jedoch menschliche Aufmerksamkeit und einen erfahrenen Blick. Der

Befreiungsschlag kann durch Managed Services gelingen: Michael Süß und Christian Kaspar von Konica Minolta erklären, wie es funktioniert und worauf es ankommt.

**it management:** *Herr Kaspar, Sie beraten Unternehmen zu Cloud-Strategien und Managed Services. Aus welchen Gründen kommen Sie mit den Kunden ins Gespräch?*

**Christian Kaspar:** Das ist ganz unterschiedlich. Manche haben sich beispielsweise kürzlich entschieden, bestimmte Cloud Services zu nutzen und wollen sie mit Managed Services zum Komplett-Paket ergänzen. Andere haben noch gar nichts darüber gehört und werden hellhörig, wenn wir über Managed Services reden. Was alle gemeinsam haben: Sie sind sehr daran interessiert, zeitraubende `IT-Hausmeister`-Tätigkeiten aus der Hand zu geben, um sich mehr um strategische Themen und Projekte zu kümmern.

**it management:** *Herr Süß, ihr Team setzt die Managed Services für die Kunden um. Wie sehen Sie ihre Rolle?*

**Michael Süß:** Die Aufgaben, die wir übernehmen, sind unverzichtbar und binden deshalb oft einen Großteil der bestehenden IT-Ressourcen in Unternehmen. Sie sind in der Regel stark standardisiert, befolgen klare Regeln und bestimmte Zeitpläne. Insofern stimmt es schon, dass wir `IT-Hausmeister` sind. Und zwar im positiven Sinne, denn wir sind flexibel, zuverlässig, finden immer eine Lösung und übernehmen ein hohes Maß an Verantwortung.

**it management:** *Um was für eine Art von Verantwortung geht es?*

**Michael Süß:** Nehmen wir das Monitoring, einen unserer gefragtesten Managed Services. Wir überwachen aus der Ferne ganze IT-Infrastrukturen in der Cloud oder im Netzwerk des betreuten Unternehmens. Da kommt es unter anderem darauf an, dass bestimmte Server rund um die Uhr ohne Unterbrechung laufen, damit die Geschäftsprozesse funktionieren. Es reicht also nicht, erst zu reagieren, wenn ein Problem eine kritische Auswirkung zeigt – wir agieren proaktiv und verhindern so eine nachhaltige



## WHITEPAPER DOWNLOAD

Im Whitepaper „Entlastung bei IT-Aufgaben durch Outsourcing“ zeigt Konica Minolta anhand von Praxisbeispielen, bei welchen Aufgaben ein Managed Service Provider Sie unterstützen und Ihrem Unternehmen einen Mehrwert bieten kann.





Störung, die den Betrieb beeinträchtigen könnte.

**it management:** Wie funktioniert das ganz konkret?

**Michael Süß:** Wir können mit spezieller Software einzelne Geräte bis auf die Komponenten-Ebene überwachen. Wenn zum Beispiel ein Lüfter in einem Server nicht ordnungsgemäß funktioniert, bekommt mein Team sofort eine Warnmeldung. Zunächst überprüfen wir, ob es wirklich ein Hardware-Problem ist oder der Sensor einen falschen Wert geliefert hat. Dafür stehen wir im direkten Kontakt mit Partnern vor Ort. Wenn sich der Verdacht bestätigt, bestellen wir sofort ein Ersatzteil, das unsere Partner schnellstmöglich einbauen. Da bei wichtigen Servern die Komponenten redundant sind, können wir den Austausch einer Komponente veranlassen, während die zweite parallel weiterläuft. Es läuft alles einfach ohne Störung weiter – der einzig sichtbare Effekt ist die Erwähnung in unserem Reporting.

**Christian Kaspar:** Das ist in etwa so, als würden wir auf der Autobahn bei voller Fahrt einen Reifen wechseln, ohne dass jemand etwas mitbekommt.

**it management:** Was Unternehmen sehr wohl mitbekommen, sind Cyber-Bedrohungen. Wie können Sie hier helfen?

**Michael Süß:** Managed Security ist im Moment ein sehr gefragter Service. Was genau das beinhaltet, kommt ganz auf das Unternehmen an. Wir können unter anderem IT-Infrastrukturen gegen Zugriffe von außen absichern, Zugriffsversuche protokollieren, Firewalls und Virens Scanner monitoren und vieles mehr. Den Grad der Überwachung legen wir individuell fest. Außerdem arbeiten wir mit unseren hauseigenen IT-Security-Consultants zusammen, um gründliche Sicherheitschecks oder Workshops durchzuführen.

**Christian Kaspar:** Übrigens trägt nicht nur Managed Security, sondern auch ein

Umstieg auf Cloud-Lösungen zu einer verbesserten Sicherheit bei. Bei den großen Cloud-Anbietern oder auch in unserem Rechenzentrum sind viel schärfere Sicherheitsmaßnahmen möglich als im eigenen Unternehmen. Allein der physikalische Zugriff auf die Hardware wird sehr streng kontrolliert, das ist in vielen Betrieben nicht der Fall.

**it management:** Was raten Sie Unternehmen, die Ihre eigenen Anwendungen gegenüber Cloud-Software bevorzugen?

**Christian Kaspar:** Es gibt nicht nur schlüsselfertige Anwendungen, sogenannte „Software-as-a-Service“, als Cloud-Dienst. Wir bieten zum Beispiel „Infrastructure-as-a-Service“ an, das heißt: Unsere Kunden nutzen Kapazitäten in unserem Rechenzentrum und können darauf zugreifen, als wären es ihre eigenen Server. Sie können jede beliebige Anwendung aufspielen. Der einzige Unterschied: Wir sorgen dafür, dass alles funktioniert und sicher ist. Die Kunden kümmern sich derweil nicht um Technik, sondern um ihre Prozesse und ums Geschäft. Das Prinzip ist also daselbe wie bei Managed Services.

**it management:** Welche weiteren Services haben Sie im Portfolio?

**Michael Süß:** Neben Monitoring und Security ist Patch Management eine sehr hilfreiche Leistung. Hierbei kümmern wir uns darum, dass die Software beim Kunden aktuell ist, führen regelmäßig alle wichtigen Updates und Installationen aus und erstellen ein Reporting. Damit eliminieren wir einen der größten Zeitfresser in IT-Abteilungen. Zudem bieten wir Backups als Service an – eine extrem wichtige Aufgabe, die aber in vielen Unternehmen hintenüberkippt. Sehr beliebt ist auch unsere Unterstützung des IT-Helpdesks oder User Service Desks: Wir nehmen stellvertretend für die IT-Abteilung im Unternehmen Anfragen der Mitarbeitenden an, erstellen Tickets und können einfache Fragen so-

fort klären, ohne das IT-Personal zu be-  
helligen.

**it management:** Welche Cloud-Dienste und Managed Services brauchen typische mittelständische Unternehmen?

**Christian Kaspar:** Wir haben keine pauschale Lösung, die wir allen Unternehmen verkaufen wollen. Wir sehen uns in erster Linie als transparente Berater. Mir persönlich ist es ein Anliegen, offen in ein Beratungsgespräch zu gehen. Optimal ist es, wenn die Gegenseite dieselbe Offenheit mitbringt. So können wir gemeinsam herausfinden, wo der Bedarf ist und welche Lösungen dazu passen. Aufklärung ist ebenso wichtig: Ich muss meinem Gegenüber klar verständlich machen, welche Vor- und Nachteile eine Lösung hat. Denn die müssen ihre Mitarbeitenden mitnehmen, welche am Ende die IT-Umgebung nutzen.

**it management:** Zu guter Letzt: Was sollten Unternehmen unbedingt vermeiden?

**Michael Süß:** Vorschnell den erstbesten Services buchen und hinterher feststellen: Ich brauch eigentlich etwas ganz Anderes oder könnte eine wesentlich günstigere Lösung haben. Ich kann nur dazu raten, mit Bedacht vorzugehen und alle Optionen abzuwägen, damit die eingesetzten Cloud- und Managed Services auch wirklich zu einer Erleichterung im Arbeitsalltag führen.

**it management:** Herr Süß, Herr Kaspar, wir danken Ihnen für das Gespräch.

”  
THANK  
YOU

[www.konicaminolta.de](http://www.konicaminolta.de)

# Lizenzmanagement

GELASSEN IN DEN AUDIT

Von der goldenen Mitte, also dem idealen Ausgleich zweier Extreme als erstrebenswertes Ziel eines ausgeglichenen Verhaltens, wusste schon Aristoteles zu berichten. Auf das Thema Softwarenutzung bezogen bedeutet dies: Unterlizenzierung ist schlecht, weil womöglich Personen im Unternehmen nicht arbeitsfähig sind, Überlizenzierung wiederum ist gleich zum Fenster herausgeworfenes Geld. Hinzu kommen Probleme mit der Compliance. Eine UEM-Lösung wie die ACMP Suite mit ihrem Modul für Lizenzmanagement hilft dabei, beim Softwareeinsatz immer die richtige Mitte zu finden.

Systeme für Unified Endpoint Management, kurz UEM (oder auch Client Management) übernehmen die zentrale Verwaltung und Steuerung von Arbeitsplatzrechnern und Servern in einem Unternehmensnetzwerk.

Administrationsabteilungen regeln damit die erforderlichen administrativen Aufgaben auf den Clients zentral und im Idealfall komplett automatisiert. Die Automatisierung reduziert den Zeitaufwand und erhöht sowohl Zuverlässigkeit, Sicherheit als auch Produktivität von Usern und Administrationsabteilung gleichermaßen.

Klassische Bereiche des UEM sind Inventarisierung, Softwareverteilung, Patch Management und eben das Lizenzma-

agement. Hier geht es darum, eine Balance zu finden zwischen Senkung der Softwarekosten und Minimierung von Compliance-Risiken. Voraussetzung dafür ist ein stets aktueller Überblick über Verfügbarkeit und Nutzung von Lizenzen. Natürlich lässt sich das Management von Lizenzen auch manuell erledigen. Ab einer Unternehmensgröße von rund 100 Clients allerdings wird der Aufwand, den Lizenzbestand permanent zu erfassen und aktuell zu halten, unverhältnismäßig groß. Wer diese Aufgaben an ein automatisiertes Lizenzmanagement auslagert, spart viel Zeit, die sich für andere wichtige Projekte nutzen lässt.

Kostensenkung ist auf der einen Seite möglich durch Lizenzkonsolidierung. Das umfasst zunächst eine Analyse, wie im Einzelnen die Software genutzt wird: ganz, gar nicht oder nur bestimmte Elemente?

Zu Beginn steht deshalb immer eine Bestandsaufnahme: Welche Lizenzen gibt es, wo fehlen welche, wie sind sie verknüpft? Resultat ist eine transparente Abbildung der im Unternehmen installierten Programme und ihrer genauen Verwendung. Überflüssige oder doppelte Lizenzen kostenpflichtiger Programme werden identifiziert und anschließend eliminiert. Zugleich lassen sich zusätzliche Investitionen in Lizenzen – unter Anbetracht erforderlicher Ressourcen – besser planen und realisieren.

**Vorhandene Lizenzen optimal nutzen**  
Lizenzmanagement verschafft zudem eine gute Übersicht der intern verwendeten Lizenzmodelle, von denen es im Unternehmen häufig mehrere nebeneinander gibt. Es erlaubt, den monetären Aufwand durch kostenpflichtige Programme gleicher Art gegenüberzustellen. Auf diese Weise er-



**LIZENZMANAGEMENT VERSCHAFFT EINE GUTE ÜBERSICHT DER INTERN VERWENDETEN LIZENZMODELLE, VON DENEN ES IM UNTERNEHMEN HÄUFIG MEHRERE NEBENEINANDER GIBT.**

Sebastian Weber,  
Head of Product Management,  
Aagon GmbH, [www.aagon.com](http://www.aagon.com)

wächst ein Bewusstsein dafür, welcher Faktor ausschlaggebend für die jeweilige Softwarelizenzierung ist und wie sich die vorhandenen Lizenzen optimal nutzen lassen. Das wiederum schafft die Basis für bessere Verhandlungen mit den Softwareanbietern. Mit einem gut organisierten Lizenzmanagement können Unternehmen günstigere Vertragsbedingungen aushandeln, erhalten günstigere Preise, Rabatte oder flexiblere Lizenzmodelle.

## **Unterlizenzierung bedeutet Vertragsverstoß**

Compliance ist ein weiteres im Zusammenhang mit dem Lizenzmanagement verbundenes Thema. Auf Basis der mit einer UEM-Lösung geschaffenen Transparenz lassen sich unternehmensinterne Richtlinien entwerfen, die nicht nur zu Kosteneinsparungen, sondern auch zu einer unternehmensinternen Compliance führen. Denn Differenzen zwischen Lizenzvolumen und tatsächlich höherer Nutzung der Software – sprich eine Unterlizenzierung – stellen immer einen Vertragsverstoß dar und damit die latente Gefahr, rechtliche Konsequenzen und Rechtskosten zu verursachen. Durch das Vermeiden von Unterlizenzierung senken Organisationen also zugleich auch ihr Compliance-Risiko. Zudem lässt sich



schnell erkennen, dass Software genutzt wird, die dem Sicherheitskonzept der internen Unternehmens-IT widerspricht.

Hauptmodul zum Verwalten von Lizenzen bei der ACMP Suite ist das Lizenzmanagement. Es bildet die verwendete Software transparent ab und hilft dadurch, Kosten für deren Pflege und Investitionen in sie zu optimieren. Das Modul lässt sich intuitiv bedienen und dient auch der Erfassung von (Wartungs-)Verträgen und aller zugehöriger Lizenzen. Die IT-Abteilung hat damit eine umfangreiche Kontrolle über alle Aspekte des Lizenzmanagements: Verkettung, Zuordnung, Faktorberechnung, Down- und Upgrades sowie Zweitnutzungsrechte. Die Windows-Server-Standards CAL und RDS CAL werden erfüllt.

#### **Identifizierung lizenzpflichtiger Software**

Das ACMP Lizenzmanagement verknüpft inventarisierte Software zu Produkten mit einem weiteren Modul, dem ACMP

DNA. Dabei handelt es sich um eine Fingerprint-Datenbank zur Identifizierung lizenzpflichtiger Software. Sie erkennt neue und alte Versionen installierter Software automatisch und bietet umfangreiche Möglichkeiten zur Kategorisierung. So lässt sich zum Beispiel eine Kategorie für Software einrichten, die im Unternehmen allgemein nicht erwünscht ist. Die Datenbank umfasst über 14.000 Hersteller und wird täglich aktualisiert. Über sie lässt sich nicht nur kostenpflichtige Software identifizieren, sondern auch Bundles werden automatisch erkannt und bestehenden Lizenzen zugeordnet.

Ein weiteres Nebenmodul ist das ACMP AUT (Application Usage Tracking). Über dieses lässt sich detailliert die Softwarenutzung im Unternehmen ermitteln. IT-Abteilungen haben damit einen guten Überblick über ungenutzte Programme und können Einsparpotenziale identifizieren. Das Modul arbeitet konform zu allen nationalen und europäischen Normen aus Betriebsrecht und DSGVO. Die Daten

werden ausschließlich anonymisiert erhoben und erlauben keinerlei Rückschlüsse auf das individuelle Verhalten einzelner Beschäftigter. Gespeichert wird nur, ob eine Software an einem bestimmten Tag genutzt wurde – nicht wie oft und wie lange. Die Untersuchung bezieht sich zudem ausschließlich auf ausgewählte Clients und explizit festgelegte Anwendungen. Dies stellt sicher, dass in sensiblen Umgebungen keine AUT-Daten protokolliert werden. Auf Daten und Auswertungen des Moduls können nur autorisierte Fachkräfte der IT-Abteilung zugreifen.

Somit bietet Aagon ein ausdifferenziertes Produktportfolio rund um das Lizenzmanagement. Im Vorfeld eines angekündigten Audits lassen sich damit auf Knopfdruck unternehmensweite Übersichten der installierten Softwarelizenzen erstellen. „Diese haben wir Microsoft übermittelt, seitdem haben wir Ruhe“, wie der IT-Administrator eines Aagon-Kunden zufrieden berichtet.

**Sebastian Weber**





# KÜNSTLICHE INTELLIGENZ

## WISSENSVERARBEITUNG – NEURONALE NETZE

Die künstliche Intelligenz hat unseren Alltag erreicht: Wir nutzen Chatbots, reden mit Sprachassistenten, KI digitalisiert die Dokumentenverarbeitung, die Muster-, Bild- oder Objekt-Erkennung. Sie ermöglicht neue, intelligentere Lösungen in vielen Bereichen, von der Medizin bis zum autonomen Fahren.

Das Buch gibt eine Einführung in die KI. Es wird gezeigt, wie symbolverarbeitende KI in Form von Wissensnetzen oder Geschäftsregeln heute angewendet und

wie künstliche neuronale Netze in der Mustererkennung oder auch im Data Mining eingesetzt werden können.

Wissensrepräsentation und -verarbeitung auf Basis der Logik wird unter Nutzung der logischen Programmiersprache PROLOG eingeführt. Logische Schlussfolgerungen lassen sich in PROLOG wesentlich leichter als in Python oder Java implementieren. Die Konzepte neuronaler Netze werden mit dem System JavaNNS und mittels Python praktisch vertieft.

Fragen und Aufgaben am Ende eines Abschnittes fordern zum aktiven Lesen und Lernen auf. Die Webseiten zum Buch enthalten Demo-Programme, die diskutierte Vorgehensweisen veranschaulichen und das Verständnis fördern.

### Aus dem Inhalt:

- Überblick zur künstlichen Intelligenz
- Darstellung und Verarbeitung von Wissen
- Problemlösung mittels Suche
- Wissensverarbeitung mit PROLOG
- Künstliche neuronale Netze
- Vorwärtsgerichtet neuronale Netze
- Autoassoziative Netze

## PLUS

Abschnitte zu den Themen ChatGPT sowie Decision Model und Notation



### Künstliche Intelligenz: Wissensverarbeitung – Neuronale Netze

Uwe Lämmel, Jürgen Clevel;  
Carl Hanser Verlag GmbH &  
Co.KG; 10-2023



# Raus aus der Kostenspirale

## MIT DEM RICHTIGEN LIZENZMANAGEMENT FÜR DIE MICROSOFT CLOUD

Immer im Februar finden die Vertragsverlängerungen der Cloud-Dienste mit Microsoft statt. Und alle Jahre wieder stauen CIOs über eine Verschlechterung ihrer Konditionen. Angekündigt wurden Preiserhöhungen für nahezu alle 365-Pläne lang im Voraus. Besonders betroffen sind Monats-Abos. Auch TEAMS ist nicht mehr überall enthalten und kostet bei Neulizenzierung ordentlich extra (Bestandskunden bekommen Aufschub, dann aber trifft es auch sie). Klingt, als gäbe es kein Entrinnen aus der Kostenspirale der Cloud. Doch in nahezu jeder M365-Lizenzierung stecken Sparpotenziale, sagt Björn Orth, Geschäftsführer des Microsoft Partners VENDOSOFT.

### Das Optimum

„Wer sich bei der Microsoft-Lizenzierung über Jahre stabile Kosten wünscht, der kann nicht auf ‚Cloud-only‘ setzen“, sagt der Microsoft-Experte. Das ist seiner Ansicht nach auch nicht nötig. „Ein modernes und kostenbewusstes Lizenzmanagement ist heute hybrid und nutzt das Beste von beidem: die fix kalkulierbaren Einmalkosten von on-premises-Software und die Vorteile für Remote-Work und Agilität aus der Cloud.“ Orths Mitarbeitende sind zertifizierte Microsoft Licensing Professionals. Sie helfen Unternehmen dabei, die IT-Infrastrukturen optimal und am Bedarf orientiert auszurichten. Hunderte Umstellungen von on-prem auf hybrid – und auch von Cloud-only auf hybrid – haben sie im letzten Jahr erfolgreich vorgenommen. „Erfolgreich“ – das heißt: maxi-

mal effizient und kostensparend für den Kunden. VENDOSOFT setzt dafür unter anderem gebrauchte Kaufsoftware ein. Denn die ist selbst in der neuesten Version bedeutend günstiger als im Neukauf oder Cloud-Abo.

### Die Einsparungen

An konkreten Beispielen, die zeigen, wie sich hybride Lizenzierungen rechnen (ohne Einbußen in Performance und Zweckmäßigkeit), mangelt es Björn Orth nicht. Ein internationales Logistikunternehmen hatte sämtliche Arbeitsplätze mit M365-Plänen ausgestattet, darunter auch 25 PCs im Lager. An diesen arbeiten im Wechsel 60 Lageristen. Das kostete Jahr für Jahr 10.320 Euro, weil in der Cloud jeder Anwender angebunden sein muss. „Wir haben dem CIO vorgerechnet, was er spart, wenn er stattdessen die Geräte lizenziert, was in diesem Fall Sinn machte, aber nur noch on-prem möglich ist.“ Unter dem Strich stand ein Einmalposten von 5.250 Euro für gebrauchte Office 2021 Standard Device Programme versus der jährlichen Cloud-Kosten von 10.320 Euro. Für 25 Computer. Man rechne sich das hoch!

### Von Cloud auf hybrid in wenigen Stunden

Wenn Unternehmen auf die 365-Dienste migrieren und dann erleben, wie ihnen die Gebühren explodieren, scheint alles zu spät. Björn Orth kann jedoch beruhigen: „Es gibt da keinen Point-of-no-Return. Eine Rückkehr aus der Cloud ist jederzeit möglich!“ Das bestätigen ihm andere IT-Dienstleister – wie das Münchener Systemhaus TakeData, das für seine Geschäftskunden gebrauchte Microsoft Server, CAL, Betriebssysteme und Office-Pakete bei VENDOSOFT bezieht. Technical Consultant Andreas Ramelow:



„WER SICH BEI DER MICROSOFT-LIZENZIERUNG ÜBER JAHRE STABILE KOSTEN WÜNSCHT, DER KANN NICHT AUF ‚CLOUD-ONLY‘ SETZEN.“

Björn Orth, Geschäftsführer,  
Vendosoft GmbH, [www.vendosoft.de](http://www.vendosoft.de)

„Wir wickeln den Rückzug aus der Cloud bereits für Kunden ab und bieten die Dienste über eigene Rechenzentren an. Das ist dann sicher und günstig.“ Office-Applikationen von O365- auf Kaufsoftware umzustellen, ist eine Sache von ein paar Minuten. E-Mail-Konten der Exchange Server dauern etwas länger. „Bei einem Seniorenheim mit 100 PC-Arbeitsplätzen war das kürzlich pro Standort innerhalb eines Tages durchgeführt.“ Die Kosten für den Wechsel, sagt Andreas Ramelow, seien im Verhältnis zur Einsparung quasi sofort amortisiert.

Die richtige Lizenzierung kann erheblich zur Entlastung von IT-Budgets beitragen. Die Cloud hingegen schnell zur Belastung werden. Deshalb sollte sie immer hinterfragt – und im Zweifelsfall rückabgewickelt werden. Das ist auch in Teilen möglich. VENDOSOFT identifiziert Bereiche, in denen das sinnvoll ist, und bietet Unterstützung auf dem Weg.

Angelika Mühleck | IT-Fachjournalistin





# Wissensmanagement im Servicedesk

## EFFIZIENZSTEIGERUNG DURCH DEN KCS-ANSATZ

Ein effektives Wissensmanagement ist entscheidend, insbesondere wenn ein Servicedesk häufig mit wiederkehrenden Anfragen konfrontiert ist. Der Knowledge

Centered Service (KCS)-Ansatz bietet eine innovative Lösung, um die Effizienz zu steigern, sich mit mehr Zeit den komplexeren Aufgaben zu widmen und den Servicedesk optimal zu gestalten.

nicht nur einmalig für eine Anfrage genutzt werden, sondern auch für zukünftige ähnliche Probleme.

### Die KCS-Elemente: Lösen und Verbessern

Die KCS-Methodik besteht aus zwei zentralen Elementen: dem „Lösen“ und dem „Verbessern“. Beim „Lösen“ geht es darum, Wissen durch die Bearbeitung eingehender Anfragen aufzuzeichnen und zu erweitern. Wenn eine Anfrage auftritt, wird geprüft, ob sie bereits in der Wissensdatenbank vorhanden ist. Falls nicht, wird die Lösung aufgezeichnet und die Anfrage bearbeitet. Beim „Verbessern“ analysiert man die Wissensdatenbank, um die Effektivität zu steigern und herauszufinden, wie man wiederkehrende Anfragen vermeiden kann.

### Warum in Wissensmanagement investieren?

Zeitersparnis bei wiederkehrenden Anfragen: Durch ein gut strukturiertes Wissensmanagement kann die Zeit zur Bearbeitung wiederkehrender Anfragen um durchschnittlich 20 Prozent reduziert werden.

### Die Herausforderung

Im Arbeitsalltag stoßen Servicedesk-Mitarbeiter oft auf ähnliche Probleme, die bereits vielfach gelöst wurden. Dennoch kann die Suche nach den entsprechenden Lösungen zeitaufwendig sein, insbesondere wenn das Wissen nicht strukturiert und dokumentiert ist. Dies führt nicht nur zu unnötigen Verzögerungen, sondern auch dazu, dass der 2nd-Level-Support überlastet wird.

### Wissensmanagement und KCS

Wissensmanagement geht über bloße Anleitungen und Dokumentationen hinaus. Es umfasst auch die Erfahrungen und Lösungen, die in den Köpfen der Mitarbeiter existieren. Der KCS-Ansatz ermöglicht es, den Fokus von der reinen Bearbeitung von Anfragen auf das Aufzeichnen und Teilen von Wissen zu verlagern. So wird sichergestellt, dass Lösungen



**„DIE EINFÜHRUNG VON WISSENSMANAGEMENT UND DEM KCS-ANSATZ IST EIN ENTSCHEIDENDER SCHRITT ZUR OPTIMIERUNG DES SERVICEDESKS.“**

Felix Hagemann  
Service Management Consultant,  
Talent Coach Customer Services,  
[www.topdesk.de](http://www.topdesk.de)



➤ **Steigerung der Melderzufriedenheit:** Eine vollständige Wissensdatenbank ermöglicht es dem 1st-Level-Support, mehr Anfragen zu bearbeiten und gewährleistet zuverlässige Lösungen. Dies führt zu einer höheren Zufriedenheit der Melder.

➤ **Schnellere Einarbeitung neuer Mitarbeiter:** Neue Teammitglieder können durch den Zugriff auf eine umfassende Wissensdatenbank schneller einsatzbereit werden.

➤ **Mehr Freude an der Arbeit:** Der KCS-Ansatz macht die Arbeit am Servicedesk interessanter, da Mitarbeiter aktiv an der Lösung komplexer Probleme beteiligt sind mehr Zeit haben sich den komplexeren Problemen in Ruhe zu widmen.

**Wie Sie Ihre Zeitersparnis berechnen**  
Die Einführung von Wissensmanagement

führt in den ersten zwei bis vier Monaten zu einer durchschnittlichen Zeitersparnis von 20 Prozent. Die Netto-Zeitersparnis beträgt dabei etwa 10 Prozent.

**Beispielrechnung für einen Servicedesk mit 4 Mitarbeitern:**

- **Stunden pro Woche für Anfragen: 224**
- **Anteil schneller abgeschlossener Anfragen: 75 Prozent**
- **Netto-Zeitersparnis: 10 Prozent**

Ergebnis: 224 Stunden pro Woche x 0,75 der Anfragen x 0,10 Netto-Zeitersparnis = 16,8 pro Woche eingesparte Stunden.

#### Fazit

Die Einführung von Wissensmanagement und dem KCS-Ansatz ist ein entscheidender Schritt zur Optimierung des Servicedesks. Durch die systematische

Aufzeichnung und Weiterentwicklung von Wissen wird nicht nur die Effizienz gesteigert, sondern auch die Zufriedenheit der Mitarbeiter und Melder erhöht. Investieren Sie in Wissensmanagement, um einen serviceorientierten, effizienten Servicedesk zu schaffen.

*Felix Hagemann*



# HPE GREENLAKE FOR BLOCK STORAGE

## MEHR GEHT IMMER

Die digitale Transformation macht Unternehmen agiler und innovativer – so die Theorie. In der Praxis verläuft der Wandel oft schleppend. Zu den Bremsklötzen gehört meist die eigene Storage-Landschaft. Ideal wäre eine schnelle und leistungsstarke, auf Ihre Anforderungen abgestimmte Storage-as-a-Service-Lösung mit lokaler Datenspeicherung.

Aufgrund knapper Budgets entscheiden sich viele mittelständische Unternehmen beim Kauf einer neuen Storage-Lösung häufig für einen Kompromiss zwischen Preis und Leistung. Wer das Pendel zugunsten des Preises ausschlagen lässt, bekommt meist eine Lösung die im Betrieb viel Personal bindet und kaum ausbaufähig ist. Wer sich für Leistung entscheidet, nimmt teure Überkapazitäten in Kauf und bindet damit benötigtes Kapital. Ein Dilemma!

#### INHALT DIESES EBOOKS:

1. Die Storage-Lösung für Ihre Anforderungen
2. Flexibel durch disaggregierte Skalierbarkeit
3. Mehr geht immer: start small, scale big!
4. Weniger IT-, mehr Service-Betrieb
5. Die Wirtschaftlichkeit eröffnet Spielräume



Das eBook umfasst 20 Seiten und steht **kostenlos** zum Download bereit.

# SAP S/4HANA-Transition

## SECURITY & COMPLIANCE ALS UNVERZICHTBARER BESTANDTEIL

Für die Österreichischen Sozialversicherungsträger lag der Fokus bei der S/4HANA-Einführung auf der Vereinfachung durch Standardisierung und Harmonisierung, insbesondere hinsichtlich neuer Rollenmodelle. Im Unterschied zu vielen anderen haben sie dabei jedoch weder das Thema Security auf die lange Bank geschoben noch die Compliance vernachlässigt. Bei dem auf vier Jahre angelegten Umstellungsprojekt und der schrittweisen Migration bis 2024 ist der Anspruch der Projektleitung, von den Erfahrungen vorausgegangener Einführungsprojekte zu profitieren. Eine Erfolgsgeschichte.

### Die Ausgangssituation

Im Rahmen einer Sozialversicherungsreform im Jahr 2019 wurde die im Vergleich zu Deutschland ohnehin schon geringe

Anzahl der Sozialversicherungsträger von 21 auf fünf reduziert. Dieser gesetzliche Auftrag des Zusammenführens und Konsolidierens war auch der Auslöser, dass die beschlussführenden Gremien dem SAP Competence Center der Sozialversicherungsträger grünes Licht gaben, die bereits geplante Migration auf S/4HANA zu starten. „Schon zuvor“, berichtet Walter Schinnerer, Leiter des SAP Competence Centers, „hatten wir entschieden, die S/4HANA-Migration nach dem Greenfield-Prinzip anzugehen, also nicht 20 Jahre lang gewachsene Systeme mit all ihren Problemen zu migrieren, sondern SAP neu aufzusetzen.“

Maßgabe dabei war, die Prozesse und Technologien so einheitlich und standardisiert wie möglich umzusetzen. Begonnen

wurde im Frühjahr 2020 damit, einen Baseline-Mandanten als Master-Mandanten zu erzeugen. Dann wurde ein Template beim ersten Sozialversicherungsträger, der BVAEB eingesetzt – aufgrund des Greenfield-Ansatzes mit einer langen Laufzeit von 18 Monaten, sodass Anfang 2022 das Go-live stattfand.

### Externe Unterstützung

Die Sozialversicherungsträger-Community beauftragte ihr Competence Center zudem, ein einheitliches, standardisiertes Security-Werkzeug auszuwählen. Im Laufe des Jahres 2021 entschied man sich für den Einsatz der Pathlock Suite und deren technische Umsetzung durch akquinet, den in Österreich ansässigen Partner von Pathlock. Mit den Pathlock-Komponenten wurde im Rahmen des Einführungsprojek-



Quelle: AdobeStock

tes mit dem Sozialversicherer BVAEB die Grundlage für die weiteren Migrationen gelegt.

Es gelang, Standards zu setzen sowie Templates zu entwickeln, die flächendeckend bei allen anderen Rollouts eingesetzt wurden. Das heißt, auch für den zweiten Sozialversicherungsträger, die Österreichische Gesundheitskasse, gab es ein Vorprojekt über sechs Monate, um anschließend innerhalb von 18 Monaten die Pathlock Suite zu implementieren. Dazu Walter Schinnerer: „Ende 2024 sind dann alle Sozialversicherungsträger auf S/4HANA umgestellt und im Rahmen der Migration auch im Security- und Compliance-Umfeld mit neuen Standards unterwegs.“

#### Template-Ansatz des Rollenmodells

akquinet Österreich fungiert als Implementierungsberater für die IT des Projektes und steuert die technische Umsetzung. Christopher Kobald, Teamleiter SAP Security bei akquinet Österreich, betont, dabei werde sich der Pathlock Suite in hohem Maße bedient. Um einen schnellen Start von Berechtigungstests zu ermöglichen, wählte man beim Rollenmodell einen Template-Ansatz, basierend auf einem Vorlagenkatalog aus insgesamt mehr als 1000 Einzelrollen für alle gängigen SAP-Standardmodule. „Dieser Template-Katalog bildet das Grundgerüst, aus dem man gemäß Baukastenprinzip das finale Rollenmodell erstellen kann“, erklärt Christopher Kobald. „Die Vorteile sind klar: inhaltlich genau dokumentierte und in sich geschlossene Rollen, die frei von Funktionstrennungskonflikten sind. Bedeutet, die Kritikalität jeder Rolle ist vorbewertet. Und dies erleichtert, die Template-Rollen schlussendlich in Sammelrollen zu überführen und einzusetzen.“ Das Sammelrollen-Modell bildet die unterschiedlichen Arbeitsplätze ab und wurde gewählt, um den Fiori-First-Ansatz stringenter verfolgen sowie den Joiner-Mover-Leaver-Prozess vereinfachen zu können.

#### Die GRC-Lösung

Das Template-Rollenmodell ist in der Governance-Risk-and-Compliance-Lösung von Pathlock nahtlos integriert. Die Funktionen des Automated Roll Designs reduzieren den Arbeitsaufwand bei der Verwaltung des Rollenmodells deutlich. Um die Transparenz im Berechtigungswesen zu straffen und bei der Berücksichtigung von Kundenanforderungen über das Template-Modell hinaus auf der sicheren Seite zu sein, bietet Pathlock mit Access Analysis schon bei der Rollenerstellung Verweise auf einzelne kritische Berechtigungen und Funktionstrennungskonflikte. Christopher Kobald betont: „Der von den Projektleitern am meisten geschätzte Faktor war das Testen mit Sicherheitsnetz, das Safe Go-live Management.“ Fehlen einem Benutzer während des Testens benötigte Berechtigungen, kann er eine Fall-back-Funktion aktivieren und ihm werden unverzüglich weitläufigere Berechtigungen zur Verfügung gestellt. Der Vorteil: Die Testphase läuft ungestörter, effizienter und schneller.

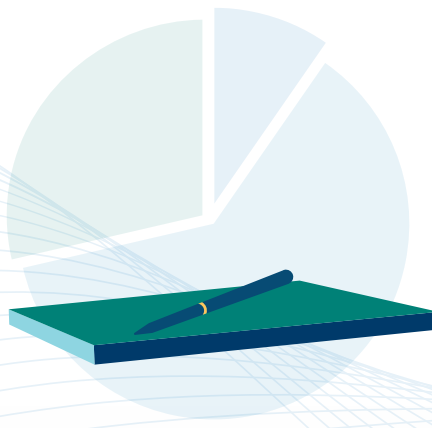
„Dieses Vorgehen ermöglicht uns, das Projekt ressourcenschonend und kostengünstig abzuschließen, während die schon live gegangenen Sozialversicherungsträger bereits weitere Pathlock-Funktionen verwenden“, so Kobald. „Dazu zählen das Compliant Provisioning für den Joiner-Mover-Leaver-Prozess und das Vulnerability Management für die systemische Sicherheit. Damit aber nicht genug: Wir führen über 2024 hinaus bereits Gespräche, wie mittels Pathlock Threat Detection und Data Loss Prevention kritische Events in Echtzeit überwacht und geloggt werden können. Und nicht zuletzt profitieren Führungskräfte von einem passgenauen Security Management Dashboard.“

#### Lessons Learned

Gefragt nach den im Rahmen des Projekts gewonnenen Erkenntnissen hebt Walter Schinnerer hervor: „Was ich Verantwortlichen mit auf den Weg geben kann: Wenn es bis dato schwierig war, Security-Budget intern zu beantragen, hat es uns geholfen, die gesamte Pathlock Suite direkt in das Budget zur S/4HANA-Migration zu integrieren. So ist das Thema Security von Beginn an ein integrativer Bestandteil der Gesamtstrategie.“ Die wesentliche Entscheidungsgrundlage für die Auswahl der Pathlock Suite seien aber die Template-Rollen gewesen. „Uns überzeugte, dass wir hier eine Komponente haben, die wir auf unsere S/4HANA-Plattform mit integrieren konnten und keine zusätzlichen Services brauchten.“ Natürlich habe man auch darauf geachtet, Ressourcen so optimal wie möglich einzusetzen und alles so weit wie möglich zu automatisieren, Herausforderungen nur einmal anzugehen und aus ihnen zu lernen. „Wir haben uns unterschiedliche Tools angeschaut, die Pathlock Suite war am erfolgversprechendsten. Und jetzt, am Ende des Projektes können wir sagen, es war die richtige Entscheidung.“

Ralf Kempf, CTO von Pathlock Deutschland, hebt angesichts des erfolgreichen gemeinsamen Projektes hervor, er beobachte viele Unternehmen, die bei der S/4HANA-Migration die Themen SAP-Sicherheit und Berechtigungswesen auf die lange Bank schieben – ein hohes Risiko für das gesamte Vorhaben. „Ganz wichtig ist deshalb ein ganzheitliches IT-Risikomanagement, da es ein großes Wertschöpfungs- und Einsparungspotenzial birgt. Was andere Unternehmen häufig machen, sind viele kleinteilige, nicht abgestimmte Projekte. Letztlich ist es sogar einfacher, wie das Beispiel der Österreichischen Versicherungsträger zeigt, den großen Schritt zu wagen und das ganze Projekt wirklich integrativ anzugehen.“

[www.pathlock.de](http://www.pathlock.de)





# Effiziente Projektabwicklung

MEHR EIGENSTÄNDIGKEIT  
UND IMMER AUF DEM NEUESTEN STAND

Auch für kleinere Fertigungsbetriebe sind ERP-Systeme unverzichtbar für eine effiziente Projektabwicklung. Damit sie den größtmöglichen Nutzen aus der Software ziehen können, sollte der zeitliche und finanzielle Aufwand für die Administration und die Modernisierung überschaubar bleiben. Auf Basis dieser Überlegungen entschieden sich die Verantwortlichen der Otto Gruber Maschinenbau GmbH für den Einsatz der Multiprojektmanagement-Software ams.erp, mit der sie seit 2022 sukzessive einen unternehmensweiten Datenfluss etablieren.

Die Otto Gruber GmbH ist bekannt für hochwertige Heuladewagen, Dungstreuer und Aufbauadewagen, die speziell für den Einsatz in alpinen Hang- und Steillagen entwickelt wurden.

Um ihre Wettbewerbsposition langfristig zu stärken, legen die Geschäftsführer Heidi Lainer und Andreas Schweiger großen Wert auf eine effiziente Auftragsabwicklung. Das bisherige ERP-System, das seit 2010 im Einsatz war, erschwerte diese Bemühungen zunehmend, insbesondere da

die zehn Jahre alte Version vom Anbieter nicht mehr unterstützt wurde. Andreas Schweiger zeigt sich selbstkritisch, da Aktualisierungen vernachlässigt wurden. Der Hauptgrund dafür war der hohe Aufwand aufgrund zahlreicher Anpassungen, der schließlich den Systemwechsel so teuer wie eine Neueinführung gemacht hätte.

Diesen Umstand nahm der Geschäftsführer zum Anlass, den Markt nach einem passenderen System zu sondieren, das alle benötigten Funktionalitäten direkt im Standard mitbrachte. Es sollte zudem die Möglichkeit bieten, die Definition von Workflows oder geringfügige Änderungen in Eigenregie durchführen zu können. Fündig wurden die Verantwortlichen bei der ams.erp Solution GmbH, der österreichischen Tochter von ams.Solution.

## Anwenderfreundlichkeit als Kriterium

Vor allem das zeitgemäße Erscheinungsbild des Systems weckte ihr Interesse. Im Rahmen von Referenzbesuchen bestätigte sich der anfängliche Eindruck. „Auch im Praxisbetrieb zeigte ams.erp im Ver-

gleich zu anderen Programmen sofort mehr Modernität. Die Darstellung in Tabellenform hebt sich deutlich von der klassischen ERP-Formularlogik ab. Auch die umfassenden Such- und Filterfunktionen gefielen uns auf Anhieb“, erinnert sich der ERP-Projektleiter Franz Gensbichler. Für Geschäftsführer Andreas Schweiger spielt die Anwenderfreundlichkeit vor allem mit Blick auf die Nutzerakzeptanz eine entscheidende Rolle. Über die unterschiedlichen Darstellungsoptionen, die individuelle Anpassbarkeit der Arbeitsbereiche und die Möglichkeit, schnell zwischen Ansichten wechseln zu können, seien die Mitarbeitenden später in der Tat schnell mit dem System vertraut gewesen.

Das Ziel, die gesamte Prozesslandschaft vollständig im Standard und ohne jedwede Zusatzprogrammierung abzubilden, konnte umgesetzt werden. Dadurch steht kontinuierlichen Release- und Versionswechseln nichts mehr im Wege, die Anwender profitieren umgehend von allen neuen Funktionalitäten. Zudem werden die Insellösungen und Parallelsysteme, die sich infolge der ehemals zu eingeschränkten ERP-Prozesse etabliert hatten, sukzessive eliminiert.

Dass die neue Software so gut passt, liegt an ihrem Zuschnitt auf die Einzel-, Auftrags- und Variantenfertigung. Denn alle Maschinen der Saalfelder sind individuell. Ähnlich wie bei PKW bestehen vielfältige Konfigurationsoptionen, etwa hinsichtlich der Fahrzeugmaße, des Fassungsvermögens oder der Anzahl der Achsen. Obwohl es das Bestreben ist,

Seit 75 Jahren werden bei dem Familienunternehmen qualitativ hochwertige Heuladewagen, Dungstreuer und Aufbauadewagen gebaut.

möglichst viele Bauteile zu standardisieren, gibt es fast immer einen Anteil an Sonderkomponenten, die ERP-seitig Flexibilität hinsichtlich der Modifizierbarkeit der Stücklisten im laufenden Fertigungsprozess erfordern. Diese Flexibilität bringt ams.erp dank der Funktionalität der wachsenden Stückliste und der Möglichkeit des Arbeitens mit und ohne Artikelnummern mit. Was den großen Anteil der Standardkomponenten anbelangt, soll der ebenfalls in ams.erp verfügbare Produktkonfigurator die Konfiguration künftig so weit wie möglich automatisieren. Das Tool hatte die beiden Entscheidungsträger mit seiner Funktionsweise und der im Vergleich nutzerfreundlichen Bedienbarkeit überzeugt.

#### Der Standard als Maßstab

Eine Grundanforderung an das neue System waren umfangreiche integrierte Kalkulationsmöglichkeiten. Andreas Schweiger benötigte eine Software, „die sämtliche Produktions- sowie alle Material- und Personalkosten bis zum letzten Artikel und zur letzten Baugruppe berücksichtigt und zudem die Baugruppen aufsplittet“. Auch bei der Verfolgung der gesamten laufenden Kosten hinterließ ams.erp den besten Eindruck.

Auf dem Weg zu der angestrebten übergreifenden Datendurchgängigkeit kommt das Finanzmodul ams.finance zum Einsatz, das die Buchhaltung mit seinen im

Hintergrund laufenden Automatismen bereits an vielen Punkten entlastet. Nachdem die Abläufe rund um die Kontierung einwandfrei laufen, ist geplant, künftig auch weiterführende Analysen zu erstellen, wofür die tiefe Integration von ERP- und Fibu-Software laut dem Firmenchef eine Menge Potenzial bietet. Ebenso fest eingeplant ist die Anbindung der CAD-Software SolidWorks.

Für solche und ähnliche Überlegungen lassen sich der Geschäftsführer und der ERP-Projektleiter ausreichend Zeit. „Wir schätzen es, sukzessive vorgehen zu können, angefangen mit dem Lager- und dem Auftragsmanagement. Sobald diese reibungslos funktionieren, gehen wir die nächsten Schritte motiviert an, weil wir wissen, dass die Gesamtabwicklung mit jedem integrierten Teilbereich besser läuft“, sagt Franz Gensbichler.

Besser laufen heißt für Geschäftsführer Andreas Schweiger, dass sich der interne Prüfaufwand dank der automatisierten Abläufe insgesamt reduziert, wenn manuelle Überträge und aufwendige Doppelinträge obsolet werden. Dadurch werden vor allem zusätzliche Personalressourcen frei. Die Mitarbeitenden registrieren die positiven Effekte in ihrer täglichen Arbeit und sind zumeist in der Lage, die Software nach entsprechender Unterweisung durch die Projektverantwortlichen zu bedienen – aufwendige Anbieterschu-

lungen sind nicht notwendig. Die Bedienungsfreundlichkeit kommt auch Franz Gensbichler zugute, der sich in den Umgang mit dem SQL-Server eingearbeitet hat und weiß, wo er in der Datenbank für die Erstellung von Reports und Dashboards fündig wird.

#### Releasewechsel als Chance

Besser geworden ist das Unternehmen definitiv hinsichtlich der Kapazitätsplanung, die zuvor provisorisch über eine ERP-externe Software erfolgte. Alle Projektbeteiligten sind nun jederzeit darüber informiert, zu welchem Termin einzelne Maschinen eingeplant sind. Sollten fehlende Teile oder die Urlaubssituation die Fertigung absehbar beeinträchtigen, können Projekte verschoben werden. Speziell der Vertrieb, der bis zur Maschinenübergabe den Kontakt zu den Kunden hält, profitiert von den exakten Zeitangaben, die über visualisierte Dashboards bereitgestellt werden.

Durch die eigenständige Erstellung von Reports und Dashboards gelang es, viele Aufgaben direkt im System zu erledigen. Zudem haben die Release-Wechsel ihren Schrecken verloren. Früher entschied sich Andreas Schweiger oft gegen eine Aktualisierung, da er mehrtägige Ausfälle fürchtete. Heute verläuft die Situation ganz anders. „Die letzten Updates waren meist innerhalb eines Tag abgeschlossen, und die Nutzer haben kaum etwas davon mitbekommen. Sie konnten einfach weiterarbeiten und profitierten von zusätzlicher Funktionalität“, stellt der Geschäftsführer fest.

**Guido Piech**



# Testdatenmanagement

## AUTOMATISIERTE AUSFÜHRUNG VON TESTDATEN-JOBS INNERHALB EINER GITLAB CI/CD-PIPELINE

– TEIL 2 VON 5 –

Diese Artikelserie widmet sich dem Thema des Testdatenmanagements (TDM). In einer sich rasch entwickelnden IT-Landschaft ist die Qualitätssicherung von Softwareprodukten von entscheidender Bedeutung, wobei das korrekte Handling von Testdaten eine Schlüsselrolle spielt. Insbesondere wird die Rolle realistischer Testdaten in der Qualitätssicherung sowie die effiziente Durchführung von Performance-Tests hervorgehoben. Diese Aspekte tragen nicht nur zur Effektivität von Softwaretests bei, sondern auch zur Entwicklung robuster und zuverlässiger IT-Lösungen.

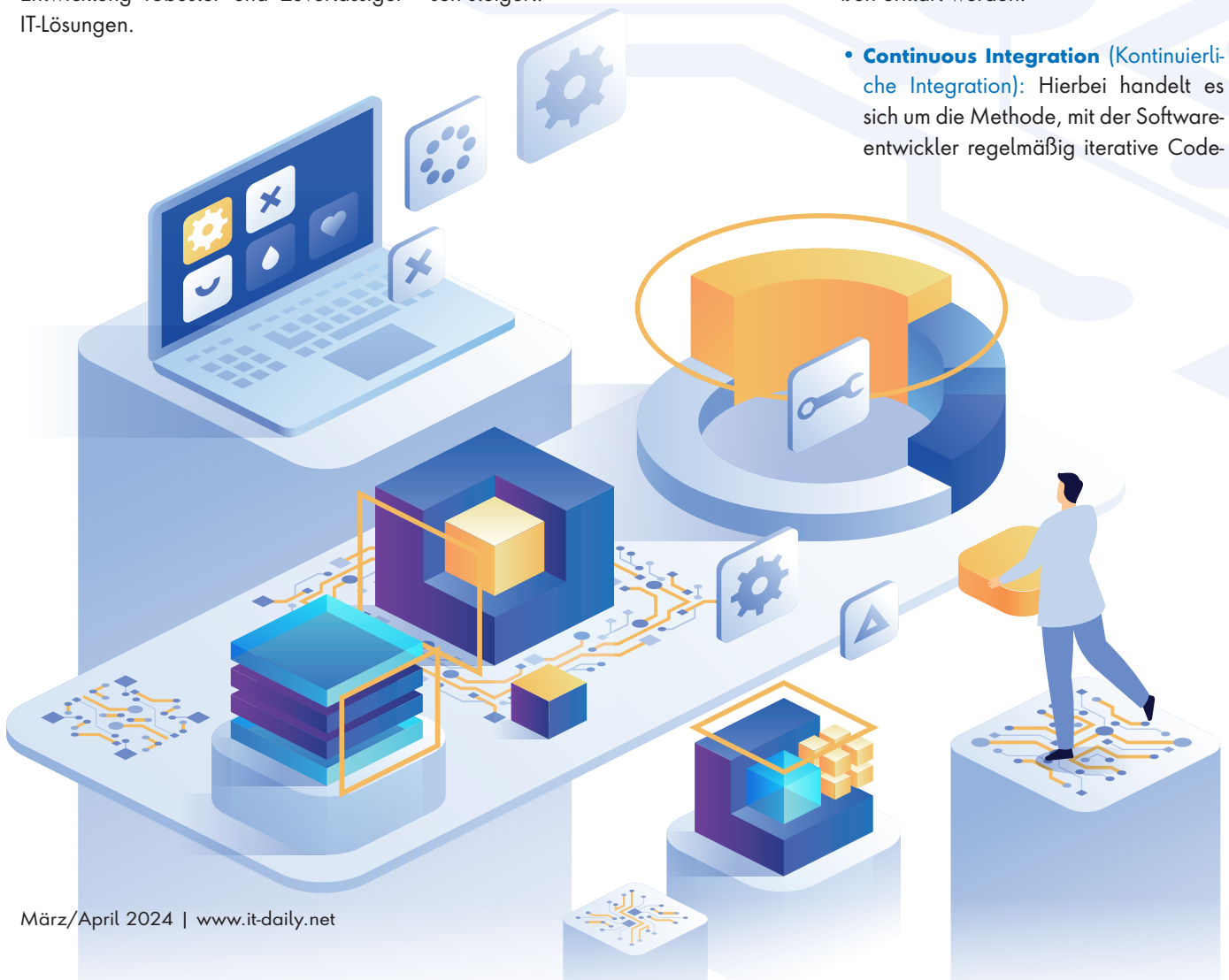
Das TDM bezieht sich auf den Prozess der Verwaltung und Bereitstellung von Daten, die in Softwaretests verwendet werden. Es umfasst die Bereitstellung von Testdaten, Anonymisierung und Maskierung sensibler Daten, Bildung von Teilmengen, Sicherstellung von Datenkonsistenz sowie die Integration in CI/CD-Pipelines. Effektives TDM trägt zur Verbesserung der Softwarequalität bei, indem es Tests unter realistischen Bedingungen ermöglicht, potenzielle Probleme frühzeitig erkennt und die Effizienz von Testprozessen steigert.

Die Serie hebt die TDM-Funktionen von IRI Voracity in verschiedenen Kontexten hervor. IRI Voracity, als End-to-End Datenmanagementplattform, vereint Datenerkennung, -integration, -migration und -verwaltung in einem Metadaten-Framework.

### Generierung von Testdaten in einer CI/CD-Pipeline

In der Welt von DevOps steht CI/CD für Continuous Integration und Continuous Delivery/Continuous Deployment. Die Phasen von CI/CD können folgendermaßen erklärt werden:

- **Continuous Integration (Kontinuierliche Integration):** Hierbei handelt es sich um die Methode, mit der Softwareentwickler regelmäßig iterative Code-





Änderungen in ein Repository einspielen. Ein CI-Dienst wird dann automatisch die neuen Änderungen im Repository erstellen und Tests durchführen.

- **Continuous Delivery (Kontinuierliche Bereitstellung):** Dies beginnt nach der CI-Phase. Der Code wird in eine Test- oder Produktionsumgebung bereitgestellt. Automatisierte Tests können während dieser Phase durchgeführt werden. Wenn alle Tests bestehen, kann der Code manuell für ein Update in der Produktion freigegeben werden.
- **Continuous Deployment (Kontinuierliche Bereitstellung):** Dies unterscheidet sich von Continuous Delivery dadurch, dass die Bereitstellung in der Produktion ohne manuelle Freigabe erfolgt.

DevOps kombiniert Softwareentwicklung (Dev) und IT-Betrieb (Ops), um den Lebenszyklus der Systementwicklung zu beschleunigen und eine kontinuierliche Bereitstellung von qualitativ hochwertiger Software zu ermöglichen. DevOps-Prozesse sind ein wesentlicher Bestandteil des Produktlebenszyklus-Managements für große Unternehmen, die neue Versionen des Quellcodes veröffentlichen. Ein häufiges Beispiel für DevOps CI/CD in der realen Welt sind die häufigen, iterativen Bereitstellungen von APIs (Application Programming Interface).

#### Effizienz und Konsistenz

Ein zentrales Prinzip der DevOps-Automatisierung ist die konsequente Automatisierung, wann immer und wo immer dies möglich ist. Diese Grundhaltung spiegelt sich besonders in der Integration von IRI Voracity-Job-Skriptausführungen wider, welche darauf abzielen, Testdaten zu maskieren oder zu synthetisieren und dabei in der CI/CD-Pipeline zum Einsatz kommen. In diesem Kontext fungieren die automatisierten Prozesse als treibende Kraft hinter den Bestrebungen von DevOps, Effizienz und Konsistenz in der Softwareentwicklung zu maximieren.



**„DIE AUTOMATISIERUNG IN DEVOPS WIRD DURCH DEN WUNSCH NACH KONSISTENZ, GESCHWINDIGKEIT UND ZUVERLÄSSIGKEIT GETRIEBEN, UND JE MEHR AUTOMATISIERT WIRD, DESTO PRODUKTIVER WIRD DAS TESTEN!“**

Amadeus Thomas, Geschäftsführer,  
JET-Software, [www.jet-software.com](http://www.jet-software.com)

Durch die Integration in CI/CD-Pipelines bietet IRI Voracity automatisierte Funktionen für Datenentdeckung, Maskierung, Teilmengenbildung und synthetische Datengenerierung. Diese ermöglichen eine umfassende Anpassung von Testdaten. CI/CD und GitLab haben eine enge Verbindung, da GitLab eine integrierte Plattform für DevOps bietet, die sowohl Versionskontrolle als auch CI/CD-Funktionen bereitstellt:

**#1** Versionskontrolle (Git): GitLab ist in erster Linie eine Plattform für Versionskontrolle, die auf dem Git-System basiert. Git ermöglicht die effiziente Verwaltung von Quellcodeänderungen in Pro-

jekten. Entwickler können ihre Codebasis mit GitLab hosten, verwalten und kollaborativ arbeiten.

**#2** GitLab CI/CD-Pipelines: GitLab integriert umfassende CI/CD-Tools direkt in die Plattform. Die CI/CD-Pipelines in GitLab ermöglichen automatisierte Prozesse, die vom Testen bis zur Bereitstellung reichen. Entwickler können Konfigurationsdateien (.gitlab-ci.yml) erstellen, um den CI/CD-Workflow zu definieren.

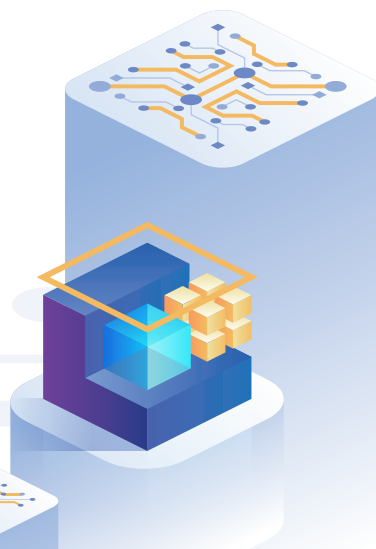
**#3** Automatische Builds und Tests: Bei jedem Push oder Merge-Request in das GitLab-Repository können CI/CD-Pipelines automatisch gestartet werden. Dies führt zu automatischen Builds und Tests des Codes, um die Integrität und Funktionalität sicherzustellen.

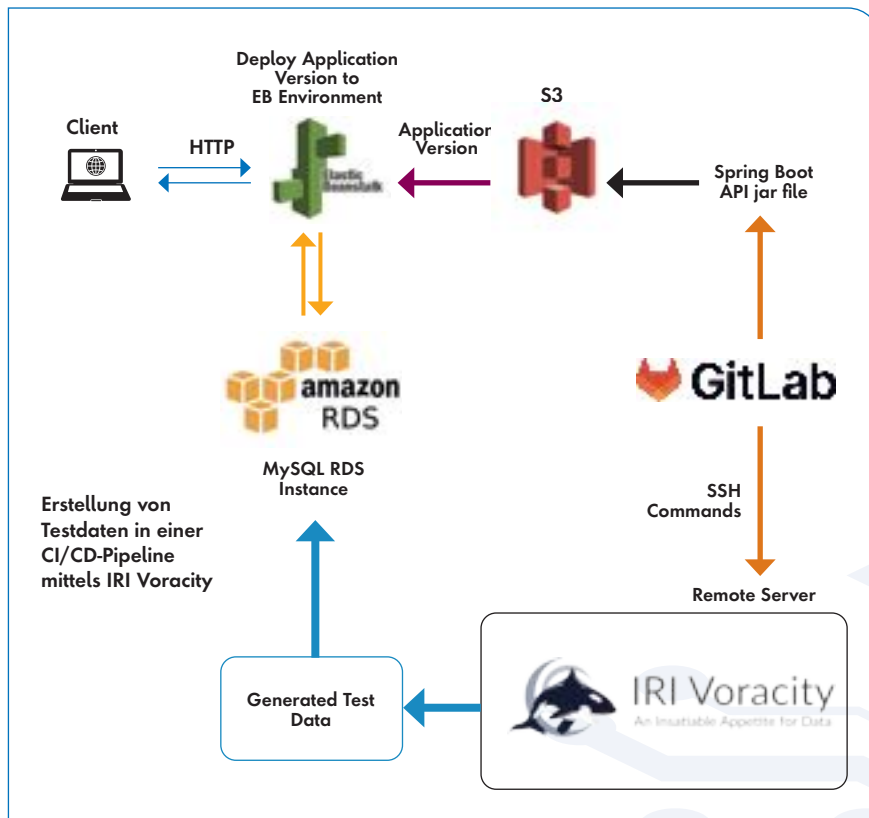
**#4** Integration von Drittanbietertools: GitLab CI/CD ermöglicht die Integration von Drittanbieter-Tools für spezifische Aufgaben im Entwicklungszyklus. Dies können Tools für statische Code-Analyse, Sicherheitsscans, Container-Bereitstellung und mehr sein.

**#5** Deployment-Strategien: Mit GitLab CI/CD können Entwickler verschiedene Deployment-Strategien implementieren, sei es Continuous Deployment (automatische Bereitstellung) oder Continuous Delivery (manuelle Freigabe nach erfolgreichen Tests). Dies bietet Flexibilität je nach den Anforderungen des Projekts.

**#6** Enge Integration mit GitLab-Repositories: CI/CD-Pipelines in GitLab sind eng in die GitLab-Repository-Infrastruktur integriert. Entwickler können ihre CI/CD-Konfiguration direkt im Repository verwalten und überwachen.

**#7** Umgebungsmanagement: GitLab bietet Funktionen zur Verwaltung von Umgebungen, die in CI/CD-Pipelines erstellt werden. Dies ermöglicht eine einfachere Handhabung von Entwicklungs-, Test- und Produktionsumgebungen.





zeile ausgeführt werden können, von der Pipeline aus gestartet werden.

### Datengenerierung

Es gibt zwei Ansätze für die Generierung von Testdaten: Synthetisierung von Daten unter Vermeidung von echten Daten aus unsicheren Umgebungen oder das Finden und Maskieren sensibler Daten auf Feldebene. Letzteres ermöglicht die sichere Verwendung von echten Daten aus Produktionsumgebungen in Testumgebungen. Die Maskierung kann auf einem Produktions-Snapshot basieren oder direkt (ETL-Stil) erfolgen, wenn Daten von der Produktion in die untere Umgebung kopiert werden.

Die automatisierten Job-Skripte liefern sichere Daten für Tests nach der Bereitstellung. In der bereitgestellten API werden dann später diese neu generierten Datenzeilen aus der Testdatenbank abgerufen, um sie als Teil des Testprozesses nach der Bereitstellung zu verwenden.

Zusammengefasst bietet GitLab eine durchgängige Plattform, die die Kollaboration im Entwicklungsprozess erleichtert, von der Versionskontrolle über automatisierte Builds und Tests bis hin zur Bereitstellung von Anwendungen. Dies trägt dazu bei, den DevOps-Ansatz zu unterstützen und die Effizienz von Softwareentwicklungsprozessen zu verbessern.

Continuous Testing im Kontext von DevOps CI/CD bedeutet das fortlaufende Testen und Evaluieren von Software in sämtlichen Phasen des Softwareentwicklungslebenszyklus, auch nach ihrer Bereitstellung in einer Umgebung. In einer GitLab CI/CD-Pipeline kann eine API inte-

griert werden, die erstellt, getestet und bereitgestellt wird. Durch die Einbindung von IRI Voracity-Jobs in diese Pipeline wird die automatisierte Bereitstellung von Testdaten in einer Testdatenbank ermöglicht. Die Testdaten-Jobs füllen automatisch die Pipeline mit intelligenten Daten, die für Tests nach der Bereitstellung verwendet werden können. Über SSH können alle Job-Skripte, die über die Befehls-

### Fazit

Es ist möglich mit IRI Voracity eine GitLab-Pipeline mit intelligenten Daten zu füllen, die für Tests nach der Bereitstellung verwendet werden können. Die Automatisierung in DevOps wird durch den Wunsch nach Konsistenz, Geschwindigkeit und Zuverlässigkeit getrieben, und je mehr automatisiert wird, desto produktiver wird das Testen!

**Amadeus Thomas**

## AUSBLICK

IRI Voracity wird als umfassende Lösung für die Automatisierung von Testprozessen und die Generierung von maßgeschneiderten Testdaten präsentiert, die verschiedene Datenquellen abdecken. Die nächsten drei Artikel dieser Serie zeigen Beispiele, wie Testdaten in Amazon CodePipeline, Azure DevOps und Jenkins integriert werden können.



# HANNOVER MESSE 2024

## LÖSUNGEN FÜR EINE KLIMANEUTRALE INDUSTRIE

Die eigene Wettbewerbsfähigkeit ausbauen, das Klima schützen, Wohlstand vorantreiben – das sind die großen Aufgaben, denen sich die Industrie heute widmet. Innovative Technologien sind der Schlüssel zur Bewältigung dieser Herausforderungen. Doch wie können Unternehmen Automation, künstliche Intelligenz, erneuerbare Energien und Wasserstoff effizient einsetzen? Die Hannover Messe 2024 gibt Antworten.

Innovative Technologien, wie wir sie im April auf der Hannover Messe erleben, ebnen den Weg zur klimaneutralen und zugleich leistungsfähigen Industrie. Unternehmen benötigen jedoch Orientierung in der Frage, wie sie Automation, künstliche Intelligenz, erneuerbare Energien oder Wasserstoff sinnvoll einsetzen. Gleichzeitig bremsen Bürokratie und der Fachkräftemangel das Wachstumspotenzial.

Unter dem Leitthema „Energizing a Sustainable Industry“ gibt die Messe Antworten auf diese Herausforderungen. Der Schlüssel liegt im Zusammenspiel der Technologien, branchenübergreifenden Kollaborationen, Technologieoffenheit und einem klaren politischen Rahmen. Gleichzeitig gilt es, die junge Generation für Hightech-Industriejobs zu begeistern.

### Treffpunkt für Industrie, Politik und Forschung

Die Hannover Messe ist die weltweit einzige Plattform, die den engen Austausch zwischen Politik, Industrie und Forschung vorantreibt, um gemeinsam Lösungen zu erarbeiten und den notwendigen Transformationsprozess zu gestalten.

Auf der weltweit wichtigsten Industriemesse stellen Unternehmen aus dem Maschinenbau, der Elektro- und Digitalindustrie sowie der Energiewirtschaft gemein-

sam Lösungen für eine gleichermaßen leistungsstarke und nachhaltige Industrie vor. Bis zu 4 000 Unternehmen agieren als industrielles Ökosystem und zeigen, wie Klimaneutralität durch Elektrifizierung, Digitalisierung und Automation erreicht werden kann. Insbesondere der Einsatz künstlicher Intelligenz führt in der Industrie zu mehr Effizienz und Produktqualität.

**Hannover Messe  
2024**

**22. – 26. April 2024**

Mehr als 300 Startups aus unterschiedlichen Technologiefeldern zeigen Innovationen mit disruptivem Potenzial. Die Messe bietet innovative Beteiligungsformen, um die Industrieunternehmen mit den Startups über das persönliche Kennenlernen zu vernetzen.

### Fokus auf nachhaltiger Energieversorgung

Die nachhaltige und emissionsfreie Energieversorgung rückt zunehmend in den Fokus. Dazu zählt der Einsatz erneuerbarer Energien sowie deren Speicherung, die Implementierung eines umfassenden Energiemanagementsystems und die Integration in ein intelligentes Stromnetz. Mit dem vermehrten Einsatz von volatilen Energiequellen hat grüner Wasserstoff an Bedeutung gewonnen. Auf der kommenden Hannover Messe präsentieren rund 500 Aussteller der Wasserstoff- und Brennstoffzellenbranche ihre Lösungen für ein emissionsfreies Wirtschaften.

### Your Future

Mit dem Nachwuchsprogramm YOUR FUTURE hat die Hannover Messe im Jahr 2023 ein Projekt gestartet, das jetzt deutlich ausgebaut wird. Das Programm hat das Ziel, noch mehr junge Menschen für die MINT-Fächer zu begeistern.

[www.hannovermesse.de](http://www.hannovermesse.de)

Quelle: Deutsche Messe AG





# Der moderne Sisyphos

## DIE HERAUSFORDERUNGEN DER DATENZUSAMMENFÜHRUNG

Vertrauen ist eine Währung, die sich nur schlecht in Euro und Cent aufwiegen lässt. Eines steht jedoch fest: Ist das Vertrauen erst einmal verspielt, lässt es sich nicht so einfach wieder herstellen. Das gilt nicht nur im Privatleben, sondern auch in Wirtschaft, Politik und Gesellschaft. Gerade in einer schnelllebigen Zeit, die durch Veränderungen und Unruhe geprägt ist, spielt der Faktor Vertrauen eine umso größere Rolle. Das hat Folgen für die Art und Weise, wie Unternehmen heutzutage geführt werden. Denn wer erfolgreich sein will, dem müssen die Kunden vertrauen. Das wiederum funktioniert nur, wenn ein Unternehmen zuverlässig ist und seine Produkte einwandfrei sind. Um das zu schaffen, muss die Unternehmensleitung jederzeit auf topaktuelle und korrekte Unternehmensdaten zugreifen können.

Was so trivial klingt, ist keineswegs selbstverständlich, denn in den allermeisten Firmen setzen sich die zentralen Unternehmensinformationen aus einer Vielzahl an Daten aus unterschiedlichsten Quellen zusammen. Der Dynamik des modernen Digitalzeitalters ist es geschuldet, dass das Zeitfenster für das Zusammenführen dieser Daten extrem klein ist. Ergo lässt sich das Problem nicht mehr mit Fleißarbeit lösen, sondern nur noch mit den richtigen Automatisierungskonzepten.

### Finanzdatenerstellung und Vertrauen

In einer aktuellen Studie, die das Censwide Marktforschungsinstitut im Auftrag von BlackLine kürzlich weltweit durchgeführt hat, zeigte sich, dass das Vertrauen in die Finanzzahlen nach wie vor zu wünschen übriglässt. 40 Prozent der in Deutschland befragten Führungskräfte und Finanzspezialisten geben an, ihren

eigenen Unternehmensdaten nicht vollständig zu vertrauen – weltweit waren es 37 Prozent. Ein interessanter Aspekt dabei: Je größer die Nähe der befragten Personen zur Erzeugung der Daten, umso geringer ist das Vertrauen in dieselben: 50 Prozent der internationalen und 33 Prozent der deutschen leitenden Finanz- und Buchhaltungsexperten verraten, dass sie den Finanzdaten, mit denen sie arbeiten, nicht vollumfänglich glauben.

Auch beim Cashflow führen die Studienergebnisse zu Handlungsbedarf: Das zweite Jahr in Folge bescheinigen erstaunliche 98 Prozent der international Befragten (97 Prozent in Deutschland), dass sie kein volles Vertrauen in die Transparenz des Cashflows ihres Unternehmens haben. Gleichzeitig gehen weltweit 37 Prozent der Fachleute (30 Prozent in Deutschland) davon aus, dass das Wissen über den Cashflow in Echtzeit für den Umgang mit unvorhersehbaren Marktver-

änderungen entscheidend ist. Ein Spannungsfeld, das größer kaum sein könnte.

### Gründe für das mangelnde Vertrauen

Grundsätzlich stellt sich die Frage, warum die Richtigkeit der Finanzinformationen überhaupt angezweifelt wird. Dazu hat die Studie drei zentrale Einflussfaktoren identifiziert: die Vielzahl der Datenquellen im F&A, die mangelnde Automation der Abrechnungsprozesse sowie das vermehrte Arbeiten im Homeoffice.

Weltweit gibt knapp ein Drittel der C-Suite sowie der Finanzspezialisten an, dass sie sich nicht sicher sind, ob in ihren Finanzdaten alles vollständig erfasst ist, da die Daten aus zu vielen verschiedenen Quellen kommen. Auffällig ist, dass dieser Aspekt in Deutschland im internationalen Vergleich weniger wichtig zu sein scheint. Hier geben nur 26 Prozent an, dass die Vielzahl der Datenquellen ein Problem ist. Auf den ersten Blick könnte vermutet werden, dass deutsche Unternehmen und Organisationen stark auf eine Datenkonsolidierung mit SAP, dem in Deutschland ansässigen ERP-Weltmarktführer, setzen. Das widerspricht aber der Tatsache, dass 34 Prozent der Finanzfachleute, also diejenigen, die mit den Systemen arbeiten, die Datenquellenvielfalt für problematisch halten, wogegen das nur 16 Prozent der C-Suite in Deutschland tun.

Interessanterweise werden die verschiedenen Datenquellen insbesondere in denjenigen Ländern als Gründe für mangelndes Vertrauen in die Finanzzahlen genannt, in denen die Digitalisierung bereits weit vorangeschritten ist. Was auf den ersten Blick irritierend erscheint, macht auf den zweiten Blick klar, dass die Digitalisierung keinem durchgängigen Kon-



**WER ERFOLGREICH SEIN WILL, DEM MÜSSEN DIE KUNDEN VERTRAUEN.**

Ralph Weiss,  
Geo VP DACH, BlackLine,  
[www.blackline.com](http://www.blackline.com)





zept folgt. Denn als Digitalisierung kann man sowohl das Digitalisieren einzelner Systeme als auch der gesamten Prozesse bezeichnen. Das kann dazu führen, dass zwar eine hoch automatisierte IT-Systemlandschaft entsteht, diese jedoch durch viele Silos zu einer Heterogenität führt, die die Datenzusammenführung problematisch macht. In der Studie beispielsweise geben die USA (36 Prozent) und Singapur (37 Prozent) an, dass sich die Datenquellenvielzahl negativ auf das Vertrauen in die Finanzdaten auswirkt.

#### **Lückenloser Datenaustausch**

Man darf zwar festhalten, dass sich durchaus einige Unternehmen einer zielgerichteten Automatisierung und Modernisierung in Finance & Accounting (F&A) gewidmet haben, dadurch aber noch lange keine Konsolidierung der Daten stattgefunden hat. Folglich ist eine übergeordnete Steuerung schwierig und die Wirkung der einzelnen Lösungen verpufft. Im F&A beispielsweise können nicht integrierte Automation-Tools leicht dazu führen, dass Unternehmen auf Basis un-

genauer oder sogar falscher Daten und Zahlen planen, weil trotz aller Automatisierung einzelner Aufgaben, kein durchgängiger Prozess etabliert wurde. Deshalb ist es ratsam eine Automation auf Basis von „End-to-end-Prozessen“ umzusetzen – idealerweise auf einer ganzheitlichen und integrativen Plattform. Andernfalls müht sich Sisyphos auch in Zukunft weiter ab.

Themen wie Continuous Accounting und Predictive Accounting, bei denen Buchungen im Finanz- und Rechnungswesen hochautomatisiert und zeitlich verteilt erfolgen, können helfen, diese Herausforderung zu meistern. Diese Trends, nicht zuletzt durch KI stark getrieben, stellen Zukunftsszenarien dar. Voraussetzung dafür: eine durchgehende Datenbasis, in der Daten aus den unterschiedlichen Quellen konsolidiert und damit zuverlässig und in hoher Qualität und Aktualität verarbeitbar werden.

Am Beispiel einer plattformübergreifenden Struktur im F&A lässt sich festma-

chen, wie wertvoll dieses Konzept ist, denn es eröffnet den Verantwortlichen – in diesem Fall den CFOs – genau die Betätigungsfelder, die Unternehmen für eine gesicherte Zukunft benötigen: Das Erstellen von belastbaren Analysen und Szenarien, um dem Management Entscheidungshilfen zu geben. Nicht nur durch den Zeit-, sondern vielmehr durch den Qualitätsgewinn einer übergreifenden, konsolidierten Automation und des dadurch realisierbaren Continuous Accountings werden dem CFO und den Finanzexperten die nötigen Werkzeuge für die Unternehmenssteuerung übertragen.

#### **Fazit**

Eine plattformbasierte Automation, beispielsweise mit BlackLine, ermöglicht ein modernes und kontinuierliches Accounting. Es hilft nicht nur einzelne Prozesse in der Finanzabteilung zu optimieren, sondern sorgt zudem für mehr Validität bei den Finanzzahlen, einer hohen operationalen Agilität und damit für mehr Vertrauen ins Unternehmen.

**Ralph Weiss**

# Keine Angst vor komplexen Datenbeständen

SO SETZEN SIE EINE ERFOLGREICHE DATA-LAKEHOUSE-STRATEGIE UM

Exponentiell wachsende Datenvolumina stellen nach wie vor eine große Herausforderung für Unternehmen dar. Data Lakehouses sind ein innovativer Lösungsansatz für dieses Dilemma.

Seit Jahrzehnten kämpfen Unternehmen damit, die ständig wachsenden Datenmengen, die sie tagtäglich generieren, zu speichern, zu verwalten und daraus wertvolle Informationen zu gewinnen. Das World Economic Forum schätzt, dass diese tägliche Datenflut 294 Milliarden E-Mails, 65 Milliarden WhatsApp-Nach-

richten und 5 Milliarden Suchanfragen umfasst. Dieses Datenvolumen ist so gewaltig geworden, dass die bisher gängigen Vergleiche, die diese Zahlen verständlich machen sollen, wie Bibliotheksbestände oder Papierstapel bis zum Mond, schon vor langer Zeit hinfällig geworden sind.

Unternehmen sind sich der Herausforderung bewusst, aus dieser Fülle von Daten nützliche Erkenntnisse zu gewinnen. Das Institut der deutschen Wirtschaft hat herausgefunden, dass rund die Hälfte der Großunternehmen (51 Prozent) glaubt, Daten effizient verwalten zu können. Das bedeutet, dass nahezu jedes zweite Unternehmen mangelnde Kompetenz in diesem Bereich einräumt. Wenn Daten „das neue Öl“ sind, wie einige Kommentatoren gerne behaupten, sollte es im Interesse dieser Unternehmen liegen, ihre Defizite im Bereich des Data-Managements zu beheben. Glücklicherweise gibt es neue technologische Lösungen, die diese Unternehmen dabei unterstützen.

für vordefinierte Schemata optimiert sind. Im Vergleich dazu speichert ein Data Lake große Mengen unverarbeiteter Rohdaten in ihrem ursprünglichen Format, ohne dass eine vorherige Datentransformation erforderlich ist. Ein Data Lakehouse kombiniert die besten Leistungsmerkmale beider Systeme und bietet eine einheitliche Plattform für die Speicherung, Verarbeitung und Analyse von Daten.

In einer frühen Phase der Einführung können Unternehmen, die Data Lakehouses implementieren, ihre Daten-Architekturen straffen und effizienter gestalten, Kosten senken und die Umsetzung von Self-Service-Analysen unterstützen. Es gibt bereits heute zahlreiche Anwendungsfälle wie Data-Mesh-Support (Data-Mesh: dezentralisierte Datenarchitektur, die die Zugänglichkeit, Interoperabilität und Nutzbarkeit von Daten fördert), die Bereitstellung einer einheitlichen Zugriffsebene für Analysen oder die Datenmodernisierung in Hybrid-Cloud-Umgebungen. Viele weitere Use Cases werden folgen.



”

EIN DATA LAKEHOUSE KOMBINIERT DIE BESTEN LEISTUNGSMERKMALE EINES DATA WAREHOUSES UND EINES DATA LAKES UND BIETET EINE EINHEITLICHE PLATTFORM FÜR DIE SPEICHERUNG, VERARBEITUNG UND ANALYSE VON DATEN.

Andreas Vogels,  
Head of Central Europe, Dremio,  
[www.dremio.com](http://www.dremio.com)

## Data Lakehouses können Abhilfe schaffen

Das Konzept eines Data Lakehouse, das Data-Warehouse-Funktionalitäten mit der Flexibilität eines Data Lakes kombiniert, gewinnt zunehmend an Bedeutung, wobei Unternehmen wie Netflix und Uber hier eine Vorreiterrolle spielen. Um diese Begriffe zu verdeutlichen: Data Warehouse speichert verarbeitete, organisierte und gefilterte Daten für Analysen und Reportings. Sie bieten einen zuverlässigen und konsistenten Überblick über die Daten, sind jedoch in Bezug auf Skalierbarkeit und Flexibilität eingeschränkt, da sie



**DATA LAKEHOUSE**



## DATENLEBENSZYKLUS BLEIBT KOMPLEX, SPRÖDE UND TEUER



Gängige Enterprise Data Warehouse Architektur

Die meisten Unternehmen wissen jedoch nicht, wo und wie sie beginnen sollen. Das Risiko, Zeit und Geld zu investieren und das Projekt möglicherweise scheitern zu sehen, hält viele davon ab, sich die Vorteile von Data Lakehouses zu Nutze zu machen. Der Aufbau und die Umsetzung einer Data-Lakehouse-Strategie lässt sich jedoch in vier einfache Schritte unterteilen.

### Was kann ein Data Lakehouse leisten?

Das Data Lakehouse kombiniert die Struktur und Leistung eines Data Warehouse mit der Flexibilität eines Data Lake. Dabei handelt es sich um eine Art Daten-Architektur, die Data-Warehouse-Befehle, häufig in SQL (Structured Query Language), verwendet, um Data-Lake-Objektspeicher mit hoher Geschwindigkeit abzufragen – On-Premises oder in der Cloud.

Das Data Lakehouse unterstützt sowohl Data-Science-Workloads als auch Business Intelligence (BI), da es Abfragen sowohl auf relationale Daten als auch auf multi-strukturierte Daten, die in Dateien gespeichert sind, ausführen kann. In nahezu allen Unternehmen besteht die

Notwendigkeit, die explodierende Nachfrage nach Analysen zu erfüllen und zu vereinfachen – und dies treibt die Einführung von Data Lakehouses voran.

Da schnelle Abfragen direkt im Objektspeicher des Data Lakes ausgeführt werden, müssen Unternehmen keine Daten kopieren oder verschieben, um den BI-Leistungsanforderungen gerecht zu werden. Damit kann auch der Bedarf an Datenextrakten und einem Data Warehouse sinken, was wiederum den Aufwand für die Verwaltung mehrerer Kopien minimiert und die Kosten reduziert. Da das Data Lakehouse sowohl BI als auch Data Science unterstützt, benötigen Unternehmen nur noch eine Plattform und können ihre Workloads konsolidieren. Die offene Architektur und die offenen Formate können beibehalten werden, sodass die Interoperabilität mit anderen Tools gewährleistet ist.

Bei der Evaluierung der Data-Lakehouse-Lösungen gibt es einige wichtige Faktoren zu berücksichtigen. Eine davon ist die Verfügbarkeit benutzerfreundlicher Self-Service-SQL-Analysen. Im Idealfall können auch technisch weniger versierte Be-



### OPEN DATA

nutzer Abfragen ohne die Unterstützung von Data Engineers durchführen. Der Wunsch nach Open-Source-Standards ist ein weiterer wichtiger Aspekt, da Unternehmen damit Zugang zu den besten Processing-Engines haben und sich nicht an einen bestimmten Anbieter binden müssen (Vendor Lock-in).

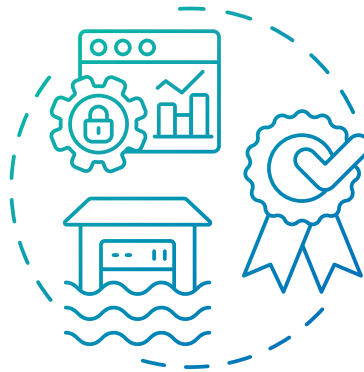
Einige Unternehmen bevorzugen flexible Bereitstellungsmodelle. Das Data Lakehouse muss sowohl in einer beliebigen Cloud-Umgebung als auch On-Premises betrieben werden können.

### Priorisieren Sie Ihre geschäftlichen Anwendungsfälle

Sobald Sie ein klares Verständnis dafür haben, welche Vorteile ein Data Lakehouse Ihrem Unternehmen bieten kann, ist es wichtig, die geschäftlichen Anwendungsfälle und Business-Szenarien mit der höchsten Priorität zu definieren. Nur dann können Sie die „Quick Wins“, die schnellen Erfolge, identifizieren und die Architektur-Charakteristika priorisieren, die zu deren Unterstützung erforderlich sind – etwa wie einheitlich, einfach, zugänglich, leistungsstark, wirtschaftlich, reguliert oder offen die Architektur sein soll.

Zu den gängigen Anwendungsfällen gehören regelmäßige Reportings, interaktive Berichte und Dashboards, Ad-hoc-Abfragen, 360-Grad-Sichten auf Kunden oder künstliche Intelligenz und maschinelles Lernen.

Ein Unternehmen aus der Konsumgüterindustrie könnte beispielsweise eine Lakehouse-Plattform auf Microsoft Azure Data



## DATA GOVERNANCE

Lake Storage implementieren, um mehrfach vorgehaltene Datensilos zu beseitigen, die Datenqualität zu verbessern und die Analysen der Lieferkette zu optimieren. Anstatt Daten aus dem Data Lake in Satellite-Data Warehouses oder BI-Extrakte zu replizieren, könnte das Unternehmen das Lakehouse nutzen, um die

Abfragen im Data Lake selbst zu beschleunigen. Eine derartige Konsolidierung der Umgebung ermöglicht es den Data-Teams, doppelte Datenhaltung zu vermeiden und die Zahl der Kopien zu reduzieren, die Effizienz zu verbessern und die Compliance zu unterstützen.

### Nehmen Sie Ihr erstes Projekt in Angriff

Nachdem Sie die vorrangigen Anwendungsfälle identifiziert und festgelegt haben, können Sie das erste Projekt mit der höchsten Priorität planen und durchführen. Mit den richtigen Stakeholdern – darunter ein Projekt-Verantwortlicher, ein Data Analyst oder Data Scientist, ein Data Engineer, ein Data Architect und ein Governance Manager – können Sie eine Roadmap erstellen und umsetzen, um Ihre Umgebung schrittweise anzupassen und zu verändern.

Um beispielsweise 360-Grad-Kundenansichten zu unterstützen, könnte das Team semi-strukturierte Kundendaten von HDFS

## ZUR VEREINFACHUNG ZIEHEN UNTERNEHMEN IN EIN LAKEHOUSE



### ETL TO ELT

- Komplexe Transformations-Pipelines in Java/Scala/Python (z.B. Spark) reduzieren
- Wechsel zu SQL-basierten Transformationen
- Der gesamte Transformationslebenszyklus findet im Lake statt

### LAKEHOUSE ADVANTAGES

- Offene Daten- und Tabellenformate
- Getrennte Speicherung/Rechenleistung, elastische SQL-Engine
- keine Kopie der Architektur
- ständige ACID-Transaktionen, Zeitreisen, Schema-/Partitionierungsentwicklung
- überzeugende Wirtschaftlichkeit

(Hadoop Distributed File System, primäres Speichersystem für Hadoop-Anwendungen) in einen Cloud-Objektspeicher für das Ziel-Lakehouse migrieren. Das Team könnte beispielsweise auch abteilungsspezifische Data Lakehouses einrichten, um den Geschäftsbereichen Marketing, Handel, Supply Chain Management und E-Commerce unterschiedliche Ansichten von konsolidierten Datenbeständen bereitzustellen – ohne dabei die Datenbestände im Objektspeicher des Unternehmens zu replizieren oder zu migrieren. So könnten die verschiedenen Abteilungen ihre eigenen Erkenntnisse gewinnen und ihre eigenen Projekte unterstützen, während sie dieselbe Benutzeroberfläche für Abfragen und dieselbe semantische Schicht wie die anderen Teams nutzen.

#### Erweitern Sie Ihr Data Lakehouse

Sobald der geschäftliche Nutzen erwiesen ist, sollte dieser „Quick Win“ ein Budget, die Unterstützung der Geschäftsleitung und Architektur-Plattformen für die Erweiterung des Data Lakehouse eröffnen. Dies sollte dazu führen, ein weiteres Projekt zu planen und durchzuführen, das andere funktionelle Daten – beispielsweise Finanz- oder Lieferkettendaten – von HDFS in das Lakehouse migriert. Ein Unternehmen könnte auch die Entscheidung treffen, die einheitliche Zugriffsebene zu erweitern, um Legacy-Datenbanken On-Premises zu unterstützen. Dies könnte ein

Data-Mesh unterstützen, in dem Domänen-Teams (die Dateneigentümer, beispielsweise Fachverantwortliche) den Nutzern (Datenkonsumenten) im gesamten Unternehmen sogenannte „Datenprodukte“ im Self-Service-Modell zur Verfügung stellen.

Ziel ist es, eine Reihe von inkrementellen und machbaren Projekten zu schaffen, die jeweils den ROI des Lakehouses aufzeigen. Dann sollten Sie das ganze Verfahren für jeden Geschäftsbereich solange wiederholen, bis jede Abteilung des Unternehmens von dem Lakehouse profitiert.

**Andreas Vogels**



#### TRANSACTIONAL SUPPORT



#### SCHEMA MANAGEMENT

## GLOSSAR

### DATA WAREHOUSE:

Eine relationale Datenbank zur Speicherung und Integration großer Datenmengen in vordefinierten Schemata, vor allem für Business Intelligence und zur Entscheidungsfindung.

### DATE LAKE:

Eine groß angelegte Storage-Lösung, die die Speicherung großer Mengen von Rohdaten sowie von unstrukturierten und semistrukturierten Daten in ihrem ursprünglichen Format ermöglicht.

### DATA LAKEHOUSE:

Eine skalierbare Architektur, die kostengünstigen Cloud-Objektspeicher für strukturierte, unstrukturierte und semistrukturierte Daten verwendet. Das Lakehouse integriert Metadaten-Ebenen über diesem Speicher, um Datenstrukturen sowie Funktionen für das Daten-Management bereitzustellen.



# Wo Wettbewerbsvorteile winken

## GARTNER-ANALYSE ZU PARTNERPROGRAMMEN

Cloud Computing ist für Unternehmen heute nicht mehr wegzudenken. Dies spiegelt sich deutlich in den Marktzahlen wider. Laut einer aktuellen Prognose von Gartner werden Unternehmen weltweit ihre Ausgaben für Public Cloud Services im Jahr 2024 um 20,4 Prozent auf insgesamt 678,8 Milliarden US-Dollar steigern. 2023 waren es noch 563,6 Milliarden Dollar.

Auch die Einführung von generativer künstlicher Intelligenz (GenAI) wird das Wachstum von Cloud-Plattformen vorantreiben. Diese Entwicklung stellt eine große Chance für IT-Services Anbieter dar, sich als Partner für eine verantwortungsvolle und maßgeschneiderte Einführung von GenAI zu positionieren. Aber wie gut sind sie darauf vorbereitet? Haben sie sich bereits die nötigen Qualifikationen als Partner der Hyperscaler angeeignet?



UM DIE VORTEILE DER PUBLIC CLOUD VOLL AUSZUSCHÖPFEN, BRAUCHEN UNTERNEHMEN PARTNER, DIE DIE ENTSPRECHENDEN KOMPETENZEN FÜR DIESE THEMEN MITBRINGEN.

René Büst, Senior Director Analyst, Gartner, [www.gartner.de](http://www.gartner.de)

Es gibt Daten, die Rückschlüsse auf diese und andere Entscheidungen der Anbieter zulassen: Die großen Cloud-Anbieter wie Amazon Web Services, Microsoft und Google verfügen heute über ein riesiges Partner-Ökosystem. Eine Analyse der Daten aus den Online-Verzeichnissen der einzelnen Partnerprogramme gibt eine Orientierung für strategische Investitionsentscheidungen von IT-/Cloud-Dienstleistern, auch im Hinblick auf die großen Trendthemen. Gartner hat sich die Zahlen für Europa genauer angeschaut und daraus Empfehlungen für Verantwortliche von IT-Anbietern abgeleitet.

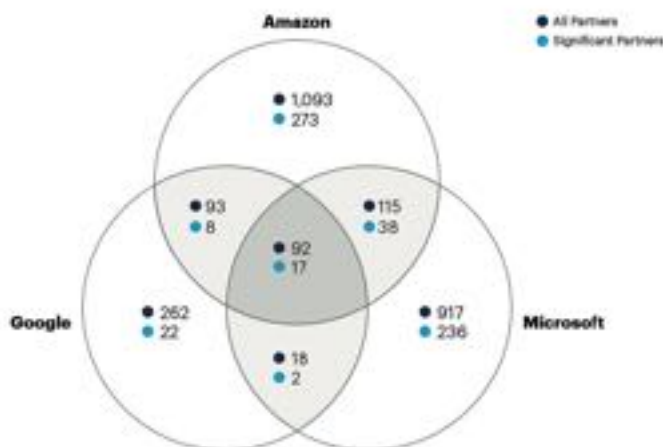
### Partner bleiben oft bei einem Hyperscaler

Betrachtet man die Verteilung der Cloud-Partner (Bild 1) hinsichtlich der Tiefe ihres Engagements, ergibt sich ein divergierendes Bild: Amazon hat das größte Partner-Ökosystem in Europa, gefolgt von Microsoft und Google. Von den 2.590 Partnern in Europa zeigen nur 596 (23 Prozent) ein signifikantes Engagement mit mindestens einer Spezialisierung (z.B. MS Azure) oder mindestens einer Mitgliedschaft in einem speziellen Programm (z.B. AWS Partner Network). Diese Unternehmen werden im Folgenden als „signifikante“ Partner bezeichnet.

Multi-Cloud ist ein Trend, der Unternehmen seit einiger Zeit beschäftigt. Die Verteilung zeigt jedoch, dass nur 318 (zwölf Prozent) aller Partner in mehr als einer Cloud aktiv sind. Bei den signifikanten Partnern liegt der Anteil der Multi-Cloud-Anbieter sogar nur bei elf Prozent. Die Partner sehen in den Partnerprogrammen also vor allem eine Möglichkeit, sich auf

### CSP PARTNER PROGRAM MEMBERSHIP MAP – EUROPE

Illustrative



n = 2,590 total partners; 596 significant partners

Source: Gartner  
791802\_C

Gartner



ihre primäre Wahl zu spezialisieren, aber nicht so sehr, sich als Multi-Cloud-Anbieter zu positionieren.

Bemerkenswert ist auch, dass Amazon über den größten Anteil an signifikanten Partnern verfügt. Nur knapp 11 Prozent der Google-Partner sind signifikant in der Partnerschaft engagiert, im Vergleich zu Amazon (24 Prozent) und Microsoft (26 Prozent).

**Empfehlung:** Cloud-Partner sollten erwägen, einen zweiten Hyperscaler ins Boot zu holen. Eine Multi-Cloud-Strategie ist zwar keine Erfolgsgarantie, kann aber für Differenzierung und Vertrauen bei europäischen Endkunden sorgen.

#### Wer bietet die größten Chancen

Bild 2 zeigt die Anzahl der Partner in verschiedenen europäischen Ländern im Vergleich zu den Marktanteilen von Amazon, Google und Microsoft im Bereich Infrastructure-as-a-Service. Hinsichtlich der Chancen ergibt sich ein uneinheitliches Bild. Die größten Chancen scheinen der deutsche und der französische Markt zu bieten: Zum einen bieten sie Raum für das Wachstum des Partner-Ökosystems, zum anderen sind hier die Ausgaben für die drei Hyperscaler hoch.

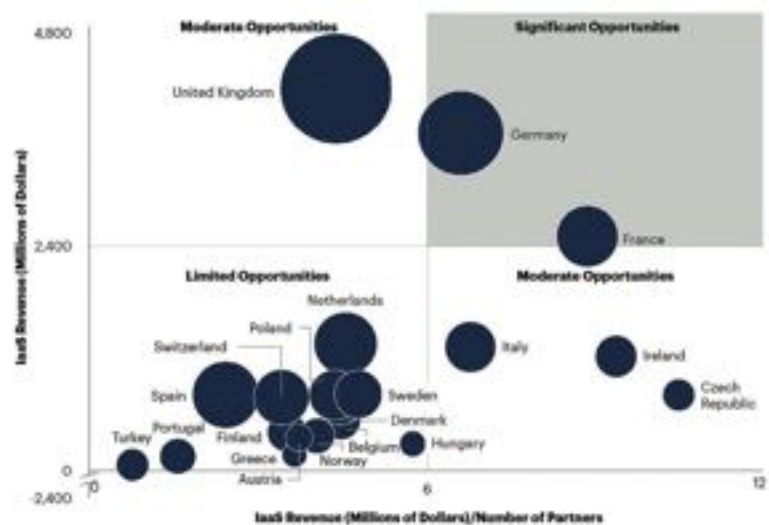
**Empfehlung:** CSPs sollten die Größe des Partner-Ökosystems und die Ausgaben für Public Clouds für jedes Land bewerten, um unterversorgte Märkte und damit Wachstumschancen zu identifizieren. Es lohnt sich auch, sich regelmäßig darüber zu informieren, in welchen Regionen die Hyper-

scaler neue Rechenzentren planen, da sich hier neue Möglichkeiten ergeben.

#### KI-Qualifikation steht noch nicht im Fokus

Bild 3 zeigt, in welche „Kompetenzen“, „Spezialisierungen“ und „Initiativen“ die

### PARTNER POPULATION IN EUROPE PER COUNTRY



Source: Gartner  
Note: Revenue is for Amazon, Google and Microsoft infrastructure as a service (IaaS).  
7/2022, IC

Gartner



## VERIFIED CREDENTIAL BREAKDOWN IN EUROPE ACROSS NINE TECHNOLOGY DOMAINS

Percentage of the Total Number of Credentials Issued



Gartner

Partner auf der Grundlage der Partnerzertifizierungen in verschiedenen Technologiebereichen investieren. Die Investitionsbereitschaft in diese Kompetenzen zeigt, dass sie sich von der Beherrschung dieser Technologien eine Stärkung ihrer Wettbewerbsposition versprechen. Dabei handelt es sich im Wesentlichen um neun Technologiebereiche, für die von allen drei Hyperscalern verifizierte Kompetenznachweise vorliegen.

Es zeigt sich, dass fast die Hälfte aller untersuchten Zertifizierungen auf die Anwendungsentwicklung (meist Microsoft) und ein weiteres Viertel auf die Datenanalyse entfallen. Die restlichen 31 Prozent verteilen sich auf sieben weitere Bereiche.

Dass der Anteil für SAP Services relativ gering ist, liegt daran, dass es sich um ein Nischenthema handelt. Erstaunlich ist hingegen, dass die Themen Container und Kubernetes sowie Künstliche Intelligenz und Maschinelles Lernen (KI und ML)

unterrepräsentiert sind. Und auch das Thema Cloud Managed Services ist überraschenderweise eher klein. Investitionen in diesen Bereich können sich lohnen, um ein Differenzierungsmerkmal zu schaffen.

Der geringe Anteil an Referenzen im Zusammenhang mit Containern und Kubernetes lässt vermuten, dass die Partner sowohl bei der Softwareentwicklung als auch bei den Migrationsdienstleistungen Investitionen in den Aufbau von Spezialkompetenzen in Containerumgebungen nicht für unbedingt notwendig halten. Bei KI und ML ist die niedrigere Zahl wahrscheinlich auf die Schwierigkeit zurückzuführen, diese Kompetenzen zu zertifizieren. Dies kann mit der Neuheit des Themas zusammenhängen, aber auch mit der Schwierigkeit, Fachkräfte in diesem Bereich zu finden, zum Beispiel qualifizierte Datenwissenschaftler. Diese sind jedoch unerlässlich, um die nachzuweisenden Fähigkeiten demonstrieren zu können.

**Empfehlung:** IT-Service-Anbieter sollten beginnen, in die Bereiche KI und ML sowie Container und Kubernetes zu investie-

ren. Derzeit haben nur wenige Wettbewerber nachweisbare Referenzen in diesen Bereichen. Für Kunden werden sie jedoch immer wichtiger, da sie diese für die Entwicklung neuer digitaler Produkte und Dienstleistungen benötigen.

Zudem sollten IT-Service-Anbieter geprüfte Cloud-Managed-Services-Zertifikate in ihr Portfolio aufnehmen, um den Kreislauf aus Anwendungsentwicklung, Datenanalyse und Sicherheit zu schließen. Denn Kunden suchen End-to-End-Lösungen von Anbietern, die Gartner als Cloud-IT-Services bezeichnet. Dabei handelt es sich um Partner, die eine Kombination aus Managed Services und Professional Services für die Cloud anbieten.

### Fazit

Die Cloud ist in Unternehmen heute gesetzt, um die Digitalisierung und die Entwicklung innovativer Themen wie Künstliche Intelligenz (KI) voranzutreiben. Dabei wird die Public Cloud eine immer größere Rolle spielen, da sie den Unternehmen mehr Flexibilität, Skalierbarkeit und Kosteneffizienz bietet als die Private Cloud oder die traditionelle IT.

Um die Vorteile der Public Cloud voll auszuschöpfen, brauchen die Unternehmen jedoch Partner, die die entsprechenden Kompetenzen, also nachgewiesene Qualifikationen, für diese Themen bei Amazon, Microsoft oder Google mitbringen. Noch gibt es wenige Partner, die diese Anforderungen erfüllen können. Das ist eine Chance für die Dienstleister, sich mit ihrer Cloud-Qualifikation von anderen abzuheben und einen Wettbewerbsvorteil zu erlangen.

René Büst



**ZIEL**



# IT ROADMAP<sup>3.0</sup>

15. Mai 2024

Digitalevent

PROZESSE



Mehr erfahren



STRATEGIE



START

#Roadmap2024

# KI in der Industrie 4.0

## ZWISCHEN HYPE UND WERTSCHÖPFUNG

Künstliche Intelligenz (KI) erlebte 2023 dank leicht zugänglicher Plattformen wie ChatGPT einen Hype im öffentlichen Bewusstsein. Daraus resultiert nicht nur die Frage, wie Menschen KI im Alltag nutzen können, sondern auch wie Unternehmen mit KI-Anwendungen ihre Prozesse wertschöpfender gestalten können.

So auch in der Industrie: Nie war es so vielschichtig und anspruchsvoll wie heute, eine effiziente Produktionsanlage zu betreiben. Unternehmen müssen ihre Anlagen und Prozesse optimieren sowie nachhaltiger gestalten, die Produktion maximieren, ungeplante Ausfallzeiten reduzieren und einen zuverlässigen Betrieb gewährleisten. Zwischen der schwankenden Nachfrage, gestörten Lieferketten sowie erhöhten Sicherheitsanforderungen im Werk braucht es technologische Stellschrauben, die die Leistung steigern können. Viele Betriebe haben bereits Dateninfrastrukturen und Analysesysteme implementiert, doch bei diesen komplexen Anforderungen bedarf es technologischer Mittel, die diesen ebenbürtig sind.

Ein Weg ist, vorhandene Datenbestände um weiterführende, KI-gestützte Analytik sowie Modelle zu ergänzen. Jede industrielle Anlage befindet sich an einem individuellen Punkt auf ihrer datenzentrierten Digitalisierungsreise. Während einige ihre historischen Betriebsinformationen in verschiedenen Datenbanken erfassen und simple Analysen durchführen, nutzen andere bereits Echtzeit-Datenströme und fortgeschrittene Analysemodelle. Um alle Werke auf den gleichen Stand zu bringen, können Unternehmen einzelne Standorte also um die neuen KI-gestützten Systeme ergänzen.



**KÜNSTLICHE INTELLIGENZ STELT FÜR EFFIZIENTE ABLÄUFE UND LANGFRISTIGEN ERFOLG EINE ZENTRALE TECHNOLOGISCHE KOMPONENTE DAR.**

Awraam Zapounidis, Vice President  
Central & Eastern Europe,  
AVEVA GmbH, [www.aveva.com](http://www.aveva.com)

KI findet unter anderem in Form von Prozesssimulationen, aber auch prädiktiver Analytik Anwendung in der Industrie. Die Prozesssimulation der nächsten Generation berechnet wichtige Leistungsindikatoren, die über die direkt in der Anlage messbaren Werte hinausgehen. Die prädiktive Analytik erkennt wiederum Anomalien und kann vorhersagen, wann Anlagen ausfallen oder eine Wartung erforderlich ist, um dies zu verhindern. Zusammengefasst können die Teams vor Ort potenzielle Risiken analysieren und Maßnahmen entwickeln, um maximal effizient und rentabel zu arbeiten.

### Prozesssimulation auf Basis des Digitalen Zwillings

Bevor Betriebe ergänzende KI-Anwendungen einsetzen, benötigen sie eine verlässliche digitale Datengrundlage. Der digitale Zwilling ist ein virtuelles Abbild und spiegelt einzelne Maschinen oder gesam-

te Anlagen wider. Er führt Informationen beispielsweise zu geometrischen und physikalischen Eigenschaften oder Umgebungseinflüssen aus verschiedenen Datenquellen zusammen. Entwickler und Ingenieure eines Unternehmens können dann von überall auf dieses virtuelle Abbild zugreifen, dessen Zustand analysieren und bei Bedarf Anpassungen vornehmen.

Mit der Prozesssimulation und prädiktiven Analytik stehen inzwischen bewährte Ansätze zur Verfügung, die in den letzten Jahren kontinuierlich verbessert wurden. Jetzt können Echtzeitdaten in Kombination mit First-Principal-Prozessmodellen verwendet werden, um einen angereicherten digitalen Zwilling eines Betriebs zu erhalten. KI-Algorithmen erweitern das Potenzial des digitalen Zwillings, damit Betreiber die optimalen Bedingungen für ihr Werk ermitteln und es mit Weitsicht steuern können. Dank ansonsten nicht-messbarer Prozessvariablen können sie ihren Energieverbrauch senken oder auch die Zuverlässigkeit ihrer rotierenden und stationären Anlagen erhöhen.

### Optimierte Wartungsprozesse

Unternehmen auf der ganzen Welt entscheiden sich dafür, KI und Machine Learning (ML)-Modelle als Deep-Learning-Tools zu nutzen, um die Restnutzungsdauer einer Anlage zu prognostizieren. So können die Teams das Kosten-Risiko-Verhältnis analysieren sowie Pläne erstellen, die die Effizienz und Rentabilität maximieren.

Herkömmliche Programme zur Anlagenüberwachung stützen sich auf Daten, die während des gesamten Prozesses erhoben werden, um Entscheidungen über

Wartungsintervalle zu treffen. So können Temperatur- und Schwingungsdaten eine Vielzahl von möglichen Ausfällen einer Kreislaspumpe vorhersagen.

Durch die Verwendung historischer Daten können Zuverlässigkeitsingenieure einen Basiswert für jede Messung bestimmen und Warnmeldungen konfigurieren, wenn die Werte außerhalb dieses Bereichs liegen. Diese zustandsabhängige Überwachung ist eine einfache Möglichkeit, Messdaten zur Verbesserung der Prozesszuverlässigkeit zu nutzen. Benutzer definieren dabei Frühindikatoren auf der Grundlage von Sensor- und anderen Betriebsdaten, um selbst subtile Veränderungen der Anlagenleistung zu erkennen. Indem der KI-basierte Algorithmus Vorhersagen trifft, können sie den Wartungsbedarf auf der Grundlage von Dringlichkeit, Zeitplänen, verfügbaren Teams, Ressourcen und Ersatzteilverfügbarkeit priorisieren.

#### Ein Blick in die industrielle Glaskugel

Während die zustandsorientierte Überwachung für Anlagen mit relativ stabilem

Betrieb nützlich ist, kann die Berücksichtigung unterschiedlicher Betriebsfenster oder Prozessmodi schnell zu einer Herausforderung werden. Ingenieure müssen möglicherweise häufig Betriebsfenster anpassen oder sich mit störenden Alarmen auseinandersetzen, was die Effizienz und Effektivität eines vorausschauenden Wartungsprogramms schnell zunichte machen kann. Anstelle der zustandsbasierten Überwachung setzen viele Unternehmen heute auf prädiktive Analytik als Teil eines robusten Asset Performance Management-Programms.

So konnte das thailändische Petrochemie-Unternehmen SCG Chemicals mithilfe von Big Data, KI-basierter prädiktiver Analytics sowie maschinellem Lernen die Zuverlässigkeit ihrer Anlagen von 98 Prozent auf 100 Prozent steigern. SCG Chemicals erhöhte dabei den Return on Invest um das Neunfache und sparte Energie. In einem weiteren Schritt können Betriebe die Remaining Use of Life Estimation (RULE) ihrer Anlagen sowie derer Kompo-

nenten berechnen, um die Vorhersagegenauigkeit der KI zu erhöhen. Das ermöglicht auch einen rechtzeitigen Austausch von Komponenten in energieeffiziente, moderne Alternativen.

#### KI als i-Tüpfelchen

Dieser Einsatz einer leistungsstarken Kombination aus Echtzeitdaten, prädiktiver Analyse und First-Principle-Simulationen lässt Industriebetriebe KI-Anwendungen zielgerichtet und effizient in ihre bestehenden Prozesse integrieren. Indem sie fortschrittliche KI auf die bestehende Dateninfrastruktur aufsetzen, können Industrieunternehmen die Vorteile sowohl von aktuellen Echtzeit-Daten als auch von historischen Betriebsdaten nutzen. Die damit verfügbaren tiefergehenden Erkenntnisse erleichtern die Entscheidungsfindung, damit Industrieanlagen künftig leistungsstark, sicher, rentabel und nachhaltig arbeiten können.

Künstliche Intelligenz stellt für effiziente Abläufe und langfristigen Erfolg eine zentrale technologische Komponente dar. Im KI-Hype steckt daher für viele Betriebe der Schlüssel zu ihrer Zukunft.

**Awraam Zapounidis**



Quelle: Aveva GmbH



# Generative KI im Servicegeschäft

NEUE HORIZONTE FÜR INNOVATIVE LÖSUNGEN  
UND EFFIZIENZSTEIGERUNGEN

Generative KI bietet, durch die Fähigkeit zur eigenständigen Erstellung von Inhalten, im Service-Bereich zahlreiche Vorteile: Von personalisierter Kundenkommunikation, automatisierten Prozessen bis hin zu schnellen Problembehebungen. Dabei sind der Microsoft Copilot und der Azure OpenAI Service zweifellos interes-

sante Technologien. Nahezu jedes Unternehmen, das es mit Digitalisierung ernst meint, beschäftigt sich derzeit mit diesen Tools.

Im Kontext des Wissensmanagements ist Microsoft Copilot eine Art KI-Assistent, der darauf abzielt, das Sammeln, Orga-

nisieren und Nutzen von Wissen innerhalb einer Organisation zu erleichtern und zu verbessern. Obwohl der Copilot ursprünglich für die Softwareentwicklung konzipiert wurde, lässt sich seine zugrunde liegende Technologie auch auf Wissensmanagement-Aufgaben anwenden.



Nebst dem Copilot finden auch die OpenAI Services von Microsoft Azure in mehr und mehr Unternehmen Anwendung. Die Azure OpenAI Services sind eine Sammlung von KI-Diensten und -Funktionen, die von Microsoft Azure in Partnerschaft mit OpenAI bereitgestellt werden. Mit Hilfe der bereitgestellten Sprachmodelle wie GPT-4 wird die Beantwortung von Fragen, die Übersetzung von Sprachen und die Automatisierung von Kundenservice-Anfragen auch im Unternehmenskontext möglich.

### Verwendung im Servicekontext

Indem Microsoft Copilot als Schnittstelle für das interne Wissensmanagement eingesetzt wird, kann es die Art und Weise, wie Informationen im Unternehmen gefunden und genutzt werden, grundlegend verändern und die Produktivität steigern.

Copilot- oder auch OpenAI-Service-basierte Anwendungen können komplexe Anfragen in natürlicher Sprache verarbeiten und verstehen.

Benutzer können Fragen so stellen, wie sie es in einem normalen Gespräch tun würden. Dies erleichtert den Zugang zu Informationen, da keine spezifischen Schlagwörter oder Suchphrasen mehr benötigt werden.

Der übergeordnete Begriff des Wissensmanagements ist, insbesondere im Service, für mehrere einzelne Use Cases zu gebrauchen. Diese Use Cases unterscheiden sich in ihren Komplexitätsstufen:

### STUFE#1: Wissensdatenbank für Servicemitarbeitende und/oder Servicetechnik

Das gesamte dokumentierte Wissen aus Arbeitsanweisungen, Produkthandbüchern, Gebrauchsanleitungen etc. wird über ein Chat-Interface abrufbar. Für Servicemitarbeitende fallen bisherige Re-

chercheaufwände weitestgehend weg. Das verspricht kompetente, kundenfreundliche Beratung und bietet gleichzeitig viel Automatisierungspotenzial.

### STUFE#2: Generative Ticket-Antwort-Erstellung

Der entwickelte IT-Service erkennt das Problem des eingereichten Support-Tickets und sucht innerhalb der bereits gelösten Tickets sowie anderer Wissensquellen nach einer passenden Lösung und generiert daraus automatisch ein Antwortvorschlag. Besonders im First-Level-Support werden die Mitarbeitenden von wiederkehrenden Anfragen entlastet - die Kundenzufriedenheit steigt. An solchen Funktionen arbeiten derzeit alle großen Anbieter von Service-Ticketssystemen - vereinzelt existieren schon Prototypen auf dem Markt. Viele Unternehmen haben eigenentwickelte Ticketsysteme - die Verantwortung für Innovation liegt ganz bei ihnen selbst!

### STUFE#3: Ausweitung von Mail- auf telefonischen Eingangskanal

Die generative Answererstellung ist nicht nur bei schriftlichen Eingangskanälen möglich, sondern auch in Rahmen des telefonischen Kundensupports. Ein exemplarischer Servicefall könnte zukünftig wie folgt ablaufen: Der Kunde ruft an und wird automatisch dazu aufgefordert, sein Problem in wenigen Sätzen zu beschreiben. Diese Problembeschreibung wird automatisch an den IT-Service übermittelt (Speech-2-Text). Darauf basierend erhält der Servicemitarbeitende alle zur Beantwortung des Kundenproblems relevanten Informationen schon vorab auf seinen Bildschirm - noch bevor der Kunde überhaupt zu ihm durchgestellt wird.

Auch wenn existierende Services als „out-of-the-box“ Lösungen für viele Anwendungsfälle angepriesen werden, sollte klar sein, dass dies für keine der drei Stufen der Fall ist.



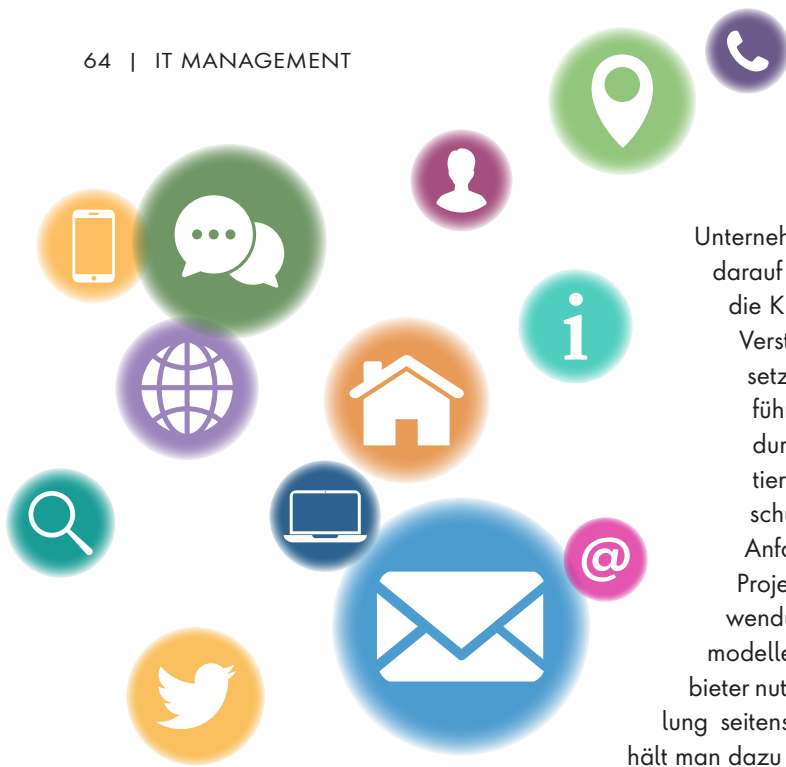
### Die Probleme

Die vier Gründe, weshalb kein „out of the box“-Service ein kundenindividuelles Projekt ersetzen kann, sind folgende:

### #1 Integration in bestehende Prozesse

Der Copilot entfaltet seine Vorteile vor allem in der Microsoft365 Welt. M365 Produkte, wie beispielsweise SharePoint, lassen sich gut in den Copilot integrieren. Jedoch arbeiten die meisten Unternehmen mit einer ganzen Bandbreite an verschiedenen Datenquellsystemen, wie vergangene Tickets, Arbeitsanweisungen und Handbücher, die herangezogen werden müssen. Davon sind nicht alle im Microsoft-Umfeld daheim. „Out of the box“-Lösungen sind zudem in ihrer Anpassungsfähigkeit begrenzt. Die Integration von Copilot in bestehende Systeme und Arbeitsabläufe kann herausfordernd sein und erfordert oft signifikante Änderungen oder Anpassungen an der aktuellen IT-Infrastruktur, beispielsweise bei existierenden Kundensupport-Ticketssystemen. Das Wissen darin sollte unverzichtbar sein, doch leider gelingt es nicht, dieses Wissen sinnvoll an den Copilot zu übergeben.

Das interne Wissensmanagement erfordert oft hochgradig angepasste Lösungen, um den spezifischen Anforderungen und Strukturen eines Unternehmens gerecht zu werden. „One size fits all“ passt hier selten.



## #2 Sicherheits- und Datenschutzbedenken

Die Verwendung von Services erfordert deren Anreicherung mit sensiblen Unternehmensdaten in das System. Dies kann zu Bedenken hinsichtlich des Datenschutzes und der Datensicherheit führen. Und zwar in unterschiedlichen Hinsichten:

### ► Verschiedene Datentöpfe sind die Grundvoraussetzung

Wer hat Zugriff auf die Daten? Diese Frage sollte bei jedem Anwendungsfall ausgiebig hinterfragt werden. Mitarbeitende im Lager sollten keine Antwort auf die Frage nach der Gehaltsstruktur bekommen, die im SharePoint der HR-Abteilung zu finden sind. Es muss gewährleistet werden, dass Informationen nie ihren Geltungsbereich verlassen. Das lässt sich jedoch nicht „out of the box“ umsetzen.

### ► Was passiert mit meinen Daten

Wo und wie werden die Daten gespeichert? Erfüllt die Verwendung von Azure OpenAI die Datenschutzstandards, wie etwa die DSGVO?

MS Copilot und der Azure OpenAI Service bieten möglicherweise nicht das erforderliche Maß an Kontrolle und Sicherheit, insbesondere wenn es um sensible Unternehmensdaten geht.

Unternehmen müssen sich darauf fokussieren, dass die KI-Nutzung nicht zu Verstößen gegen gesetzliche Vorschriften führt. Das gelingt nur durch die Implementierung von Datenschutzprinzipien von Anfang an in jedem Projekt oder jeder Anwendung, die Sprachmodelle etablierter Anbieter nutzen. Eine Hilfestellung seitens der Anbieter erhält man dazu leider nicht.

## #3 Qualität

Nicht selten sind Unternehmen von der Auslesequalität der „out of the box“-Dienste enttäuscht. Als Beispiel gelten oft Tabellen, deren komplexe Spalten- und Zeilenstrukturen inhaltlich nicht korrekt interpretiert werden können. Das ist ein möglicher Grund, weshalb keine Antwort auf Fragen ausgegeben wird, obwohl diese eigentlich in dem Dokument steht, das als Datenquelle dient. Tabellen sind oft vielschichtig und enthalten eine Fülle an Informationen, die in einem spezifischen Format angeordnet sind. Sie enthalten vor allem auch Informationen, die durch die Struktur der Tabelle selbst gegeben sind.

Diese Infos bleiben beim einfachen Parsen des Textinhalts auf der Strecke. Bei der Beantwortung der Frage, wie mit solchen Herausforderungen umzugehen ist, kommt die Fragestellung „fit your System“ versus „fits your System“ zum Tragen. Ersteres wäre die Einführung von Standardformaten für beispielsweise Tabellen oder Dokumentationen, um der KI die Analyse zu erleichtern. Zweiteres wäre eine Lösung, die sich Ihren Prozessen anpasst und nicht andersherum. Daher ist es erforderlich, spezielle Tools und Preprocessing-Schritte zu entwickeln, die auch mit spezifischen Dokumentstrukturen zurechtkommen und überhaupt zunächst dafür sorgen, dass das Wissen aus Ihren Datenquellen verfügbar ist.

## Fazit

Als Proof of Concept eignet sich der Azure OpenAI Service hervorragend. Hingegen ist der Microsoft Copilot eine produktive Lösung, die bei Unternehmen zu empfehlen ist, die sich hauptsächlich im Microsoft 365 Umfeld bewegen. Dennoch erfordern beispielsweise Anbindung weiterer Datenquellen oder Einbindungen in Produktiv-Systeme ein individuelles Customizing.

Obwohl Azure OpenAI und auch der Copilot mächtige Technologien sind, stoßen sie insbesondere beim Verständnis komplexer Dokumente an ihre Grenzen. Dies kann zu Herausforderungen führen, wenn Nutzer auf der Suche nach Antworten aus ebensolchen Dokumenten sind.

Nichtsdestotrotz sollte jedes Unternehmen erste Gehversuche mit diesen Technologien wagen. Wohlwissend, dass der produktive Betrieb einer solchen Lösung einiges an Customizing Aufwand mit sich bringt – egal, ob bezüglich Benutzer- und Rollenkonzept, Prozessintegration oder Datenschutz.

**Daniel Blümlein**



ES GIBT VIER GRÜNDE, WESHALB KEIN „OUT OF THE BOX“-SERVICE EIN KUNDENINDIVIDUELLES PROJEKT ERSETZEN KANN.

Daniel Blümlein, Technology Consultant,  
Artificial Intelligence & Data Analytics,  
Lufthansa Industry Solutions,  
[www.lufthansa-industry-solutions.com](http://www.lufthansa-industry-solutions.com)



# Ein Hub für alle KI-Chatbots

## WAS IST POE AI UND WIE FUNKTIONIERT ES?

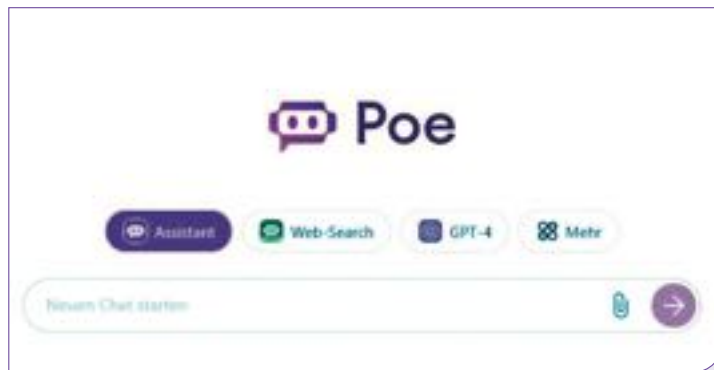
Mit der wachsenden Zahl an verfügbaren KI-Chatbots stellt sich die Frage: Wie wählt man den richtigen aus? Eine Antwort darauf will Poe AI bieten, ein Aggregator für KI-Chatbots, der den Zugang zu einer breiten Palette dieser Technologien in einem einzigen Hub ermöglicht.

### Was ist Poe AI?

Poe AI steht für „Platform for Open Exploration“ und ist eine Plattform der Frage-und-Antwort-Seite Quora, die es Nutzern ermöglicht, verschiedene KI-Chatbots über eine einzige Schnittstelle zu nutzen. Die Plattform wurde 2022 gelauncht und bietet nicht nur Zugang zu einer Vielzahl von bestehenden Chatbots, sondern ermöglicht es den Usern auch, eigene Chatbots zu erstellen und zu verwalten.

### Wie funktioniert es?

Die Plattform aggregiert verschiedene KI-Chatbots, sodass Nutzer nicht mehrere Apps oder Websites durchsuchen müssen, um die gewünschten KI-Dienste zu finden. Stattdessen können sie auf Poe AI zugreifen und aus einer Reihe von Chatbots auswählen, die für unterschiedliche Zwecke und Anforderungen entwickelt wurden. Dies soll den Zugang zu KI-Technologien erheblich vereinfachen und eine effizientere Nutzung ermöglichen. Ursprünglich unterstützte die Webanwendung mehrere allgemeine Chatbots: Sage und Dragonfly von OpenAI und Claude von Anthropic. Anfang 2023 hat die Plattform eine Abonnementfunktion eingeführt, die den Zugang zu größeren Bots ermöglicht, insbesondere zu GPT-4 von OpenAI und Claude+ von Anthropic.



Das User-Interface von Poe AI ist klar und übersichtlich strukturiert. Auf der Startseite können Anwender direkt loslegen und einen neuen Chat beginnen.

Quelle:  
Screenshot / Poe AI

### Die Features im Überblick

**Vielfältige KI-Modelle:** Poe enthält mehrere textgenerierende KI-Modelle, darunter ChatGPT, Sage, Claude-instant, claude-instant-100k und Claude+. Diese Modelle erweitern die Fähigkeiten der App und bieten den Nutzern eine Vielzahl von Chatbot-Persönlichkeiten, aus denen sie wählen können.

**Vereinfachter Zugang:** Quora entwickelt eine API, die es KI-Entwicklern ermöglicht, ihre Modelle in Poe zu integrieren, wodurch sie ein breiteres Publikum erreichen können. Diese Integration reduziert den Aufwand für die Interaktion mit Nutzern und erweitert die Verfügbarkeit von KI-gestützten Anwendungen.

**Bot-Aggregator-Konzept:** Poe fungiert als Bot-Aggregator, der es den Nutzern ermöglicht, innerhalb einer einzigen App mit verschiedenen Chatbots zu interagieren, die für unterschiedliche Aufgaben optimiert sind. Diese zentralisierte Plattform verbessert den Komfort und die Zugänglichkeit für Nutzer.

die Nutzung der Plattform variieren können, bietet sie ein Geschäftsmodell, bei dem Entwickler ihre eigenen KI-basierten Lösungen erstellen und auf dem Markt anbieten können. Dies öffnet die Tür für innovative Anwendungen und Dienstleistungen, die auf spezifische Bedürfnisse zugeschnitten sind.

Die Entwickler von Poe haben eine Funktion implementiert, die es ermöglicht, persönliche Chatbots auf der Grundlage von großen Bots mit Prompts zu erstellen. Damit können Nutzer die Werkzeuge entwickeln, die sie für hochspezialisierte Aufgaben benötigen. Derzeit können Nutzer ihren eigenen Bot auf der Grundlage von Claude Instant und ChatGPT erstellen. Jeder persönlich erstellte Bot hat seine eigene URL, die diesen direkt in Poe öffnet.

### Ist Poe AI kostenlos?

Ja, Poe AI bietet eine kostenlose Basisversion an, allerdings mit Einschränkungen bei den Funktionen und täglichen Nachrichten. Der Entwickler bietet zwei Abonnementpläne an, die jeweils ihre eigenen Vorteile und Einschränkungen haben.

Lars Becker | [www.it-daily.net](http://www.it-daily.net)



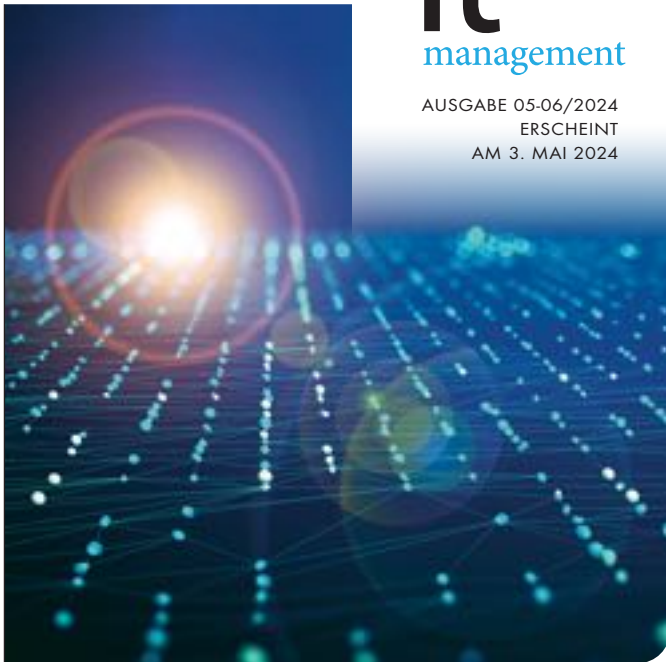
### Monetarisierung

Ein weiterer Aspekt von Poe AI ist die Möglichkeit für Nutzer, durch die Erstellung eigener Chatbots Geld zu verdienen. Während die genauen Kosten für



# it management

AUSGABE 05-06/2024  
ERSCHEINT  
AM 3. MAI 2024



## UNSERE THEMEN

Cloud Computing  
IT Service Management  
SAP-Partnerlösungen



# it security

AUSGABE 05-06/2024  
ERSCHEINT  
AM 3. MAI 2024



## UNSERE THEMEN

Zero Trust  
Cloud & Mobile Security  
KI Security



WIR  
WOLLEN  
IHR **FEED  
BACK**

Mit Ihrer Hilfe wollen wir dieses Magazin weiter entwickeln. Was fehlt, was ist überflüssig? Schreiben sie an [u.parthier@it-verlag.de](mailto:u.parthier@it-verlag.de)

## INSERENTENVERZEICHNIS

### it management

Konica Minolta Business Solutions Deutschland GmbH (Teaser)	U1
Natuvion GmbH	U2
snom technology AG	7
ams.Solution AG	11
VENDOSOFT GmbH	21
USU Software AG	25
Asseco Solutions GmbH	27
xSuite Group GmbH	31
it verlag GmbH	59
E3/B4B Media	U3
TOPdesk Deutschland GmbH	U4

### it security

Aagon GmbH	U2
Konica Minolta Business Solutions Deutschland GmbH (Advertorial)	11
Stormshield SAS	13
WatchGuard Technologies GmbH (Advertorial)	17
Bitdefender GmbH	19
tenfold GmbH (Advertorial)	21
it verlag GmbH	39, U3
DriveLock SE	U4

## IMPRESSUM

**Herausgeber:** Ulrich Parthier (08104-6494-14)

**Geschäftsführer:** Ulrich Parthier, Vasiliki Miridakis

**Chefredaktion:** Silvia Parthier (-26)

**Redaktion:** Carina Mitzschke (nur per Mail erreichbar)

**Redaktionsassistentin und Sonderdrucke:** Eva Neff (-15)

**Autoren:** Ralf Bachthaler, Lars Becker, Daniel Blümlein, Philipp von der Brüggen, René Büst, Dr. Thomas Gerick, Dina Haack, Felix Hagemann, Christoph Hemm, Harald Lutz, Carina Mitzschke, Angelika Mühle, Silvia Parthier, Ulrich Parthier, Guido Piech, Amadeus Thomas, Andreas Vogels, Sebastian Weber, Ralph Weiss, Awraam Zapounidis

### 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](mailto:info@it-verlag.de)  
Homepage: [www.it-daily.net](http://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 Programnteilen 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](http://www.kalischdesign.de)  
mit Unterstützung durch [www.schoengraphic.de](http://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,  
E-Mail: [fraenzke@it-verlag.de](mailto:fraenzke@it-verlag.de)  
Karen Reetz-Resch, Home Office: 08121-9775-94,  
E-Mail: [reetz@it-verlag.de](mailto:reetz@it-verlag.de)

### Online Campaign Manager:

Roxana Grabenhofer, 08104-6494-21, [grabenhofer@it-verlag.de](mailto:grabenhofer@it-verlag.de)

### Head of Marketing:

Vicky Miridakis, 08104-6494-15, [miridakis@it-verlag.de](mailto:miridakis@it-verlag.de)

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

**Erscheinungsweise:** 6 x pro Jahr

**Verkaufspreis:** Einzelheft 20 Euro  
Jahresabpreis 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](mailto: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.



# SUMMIT DER SAP-COMMUNITY

# COMPETENCE CENTER

Salzburg,  
5. und 6. Juni 2024

## Conversion, ALM, BTP, Lizenzen, Monitoring und Automatisierung,

die SAP-Basis-Funktionen und damit das CCC, Customer Competence Center, und CCoE, Customer Center of Expertise, sind sowohl für die Private (On-prem) als auch für die Public Cloud die Garantie für nachhaltigen Erfolg. Wir greifen die Tradition des erfolgreichen CCC-Forums auf und präsentieren den Competence Center Summit 2024.

Auf dem Weg nach Hana und S/4 entstehen viele Fragen hinsichtlich Betriebsmodell, Architektur, Lizenzen und natürlich Basissupport. Viele dieser Fragen werden am 5. und 6. Juni in Salzburg auf dem Summit 2024 beantwortet.

Der Summit liefert die On-prem- und Cloud-Antworten zu SolMan und ALM sowie Maintenance, Monitoring, System-Updates, Applikationsbetreuung, Programmdokumentation, DevOps und API, Change Management, ITSM und 1<sup>st</sup>/2<sup>nd</sup> Support, Sourcing-Strategien, Automatisierung und Modifikationen, DB-Management und Berechtigungsmanagement etc.

Jetzt anmelden: Die Teilnahmegebühr zum Summit exkl. USt. beträgt 590,- Euro.

Alle Infos unter [e3mag.com/de/cc-summit](https://e3mag.com/de/cc-summit)

E3-Summit **COMPETENCE CENTER** wird gesponsert von:

**HONICO** **itesys**

[e3mag.com/de/cc-summit](https://e3mag.com/de/cc-summit)





# Vereinheitlichen Sie Ihre IT-Prozesse

Gleichbleibend gute Services zu bieten, sollte einfach sein – auch wenn Sie viel zu tun haben. Aus diesem Grund haben wir TOPdesk entwickelt. Eine Software, die das Leben im IT-Servicedesk vereinfacht, damit Sie mehr Zeit für die wichtigen Aufgaben haben.

- ✓ Schnelle Implementierung mit Vorlagen und Best Practices
- ✓ Einfach anzupassen für kontinuierliche Serviceverbesserungen
- ✓ Unsere deutschsprachigen Experten unterstützen Sie bei jedem Schritt

TOPdesk Deutschland GmbH  
Carl-Euler-Straße 8 | 67663 Kaiserslautern  
info@topdesk.de | +49 631 624 000



[www.topdesk.de](http://www.topdesk.de)





# it security

Detect. Protect. Respond.

März/April 2024

GANZHEITLICHE DATENSICHERHEIT

## Blindspots waren gestern

Fabian Glöser, Forcepoint

**DIGITALE  
IDENTITÄTEN**

Wo stehen wir heute  
wirklich?

**DIMENSIONEN  
DER CYBERSECURITY**

Sicherheit beginnt  
beim User

**NEXT  
GENERATION EPP**

Bedrohungen erkennen  
und beheben



AUF DER

**secIT** by heise

HANNOVER 2024

**06. – 07. MÄRZ**

# Secure Unified Endpoint Management!

Eilenriedehalle Stand-Nr.: 69

**Live**

## Deep Dive

Wie Unified Endpoint Management Systeme die IT-Administration automatisieren.

06.03.2024 um 10:00 - 11:00 Uhr

Workshopraum 18

**Live**

## Vortrag

Unified Endpoint Management beginnt mit Wissen!

06.03.2024 um 15:35 - 15:55 Uhr

Bühne 2 in der Eilenriedehalle

Mehr Infos: [www.aagon.com/secit2024](http://www.aagon.com/secit2024)

**ACMP** ist 5fach Champion







COVERSTORY

04



14

# Inhalt

## COVERSTORY

### 4 **Ganzheitliche Datensicherheit**

Blindspots waren gestern

### 6 **Generative KI? Aber sicher!**

Sicherheitsrisiken minimieren, Technologie nicht blockieren

## IT SECURITY

### 8 **Die menschliche Dimension der Cybersecurity**

Sicherheit beginnt beim User

### 12 **Neue Rahmenbedingungen für Service**

Managed Services im Zeichen von KI und Nachhaltigkeit

### 14 **Cybergefahr im Netzwerk?**

Network Detection and Response (NDR) als Game Changer

### 22 **Revolution im Zugriffsmanagement**

Künstliche Intelligenz sinnvoll einsetzen

### 24 **Sieben IAM-Prognosen für die Zukunft**

Voraussagen zur Weiterentwicklung der Identitäts- und Zugriffsverwaltung

### 26 **Industrial Security Circus**

Energizing a sustainable Industry

### 27 **Insellösungen adé**

Die Cyberresilienz nicht unterminieren

### 29 **Cyberresilienz**

Auch ein SOC braucht Hilfe

### 30 **Digitale Identitäten in Deutschland und Europa**

Wo stehen wir heute wirklich?

### 34 **Digitale Identitäten im Wandel (Teil 1 von 2)**

Sicherheit und Autonomie in der vernetzten Welt

### 36 **SOAR**

Eine kleine Revolution stellt sich vor

### 40 **Next Generation EPP**

Besserer Schutz vor Cyber-Bedrohungen

### 44 **VPN & die Cloud**

Moderner Remote Access optimiert jedes IT-Security-Konzept



EINE GANZHEITLICHE DATENSICHERHEIT  
ERFORDERT IN MEINEN AUGEN FÜNF  
Kernaufgaben: Daten Erkennen,  
Klassifizieren, Priorisieren, Schützen  
und Monitoren.

Fabian Glöser, Team Leader Sales Engineering,  
Forcepoint, [www.forcepoint.com](http://www.forcepoint.com)

Security-Systemen in Angriff genommen haben, sehen sich meist mit einem hohen Komplexitätsgrad konfrontiert.

**it security:** Können Sie das etwas genauer erläutern?

**Fabian Glöser:** Unternehmen haben in der Regel viele separate, nicht integrierte Insellösungen im Einsatz. Diese machen IT-Sicherheit komplizierter, als sie eigentlich sein müsste. Als erstes bleibt die Effizienz auf der Strecke, weil diese verschiedenen Lösungen alle ihre eigenen Managementoberflächen mit individueller Logik mitbringen. Sicherheitsteams müssen deshalb mit viel Administrationsaufwand für jede Lösung ein komplett eigenes Policy Management betreiben.

Außerdem können die Teams dabei meist keine identischen Sicherheitsrichtlinien etablieren und durchsetzen. Dadurch ist ein ganzheitlicher Schutz gefährdet. Beim Zusammenspiel von Insellösungen können gefährliche Blind Spots und zusätzliche Angriffsvektoren entstehen. Je komplexer die Datenlandschaft ist, desto wichtiger ist eine möglichst einfache und ganzheitliche Datensicherheitsstrategie.

**it security:** Wie kann Datensicherheit vereinfacht werden?

**Fabian Glöser:** Unternehmen müssen zunächst einmal weg von den vielen Insellösungen und ihren unterschiedlichen Herstellern. Idealerweise setzen

# Ganzheitliche Datensicherheit

## BLINDSPOTS WAREN GESTERN

Fabian Glöser ist Team Leader Sales Engineering bei Forcepoint in München. Im Interview erläutert er, warum IT-Sicherheit oft unnötig kompliziert ist, Unternehmen eine umfassende Datensicherheitsstrategie brauchen, und was eine solche Strategie auszeichnet.

**it security:** Herr Glöser, was ist Ihrer Ansicht nach für Unternehmen aktuell die größte Herausforderung in der IT-Sicherheit?

**Fabian Glöser:** Die äußerst komplexe Datenlandschaft. Die Zeiten, in denen

sich Daten ausschließlich innerhalb des Unternehmensnetzwerks befanden, sind vorbei. Heute sind sie buchstäblich überall und bewegen sich durch Kanäle wie das Internet, Cloud- und Unternehmensanwendungen, E-Mails und seit neuestem auch verstärkt in Richtung generativer KI-Tools.

Durch diese Datenbewegungen entstehen zahlreiche neue potenzielle Risiken und Angriffsvektoren. Mit der herkömmlichen IT-Security ist es aber schwer, seine Daten überall zu schützen. Unternehmen, die das mit ihren vorhandenen

sie stattdessen eine All-in-One-Lösung ein, mit der sie die komplette Datensicherheit im gesamten Unternehmen abdecken können. Dadurch haben sie die Möglichkeit, Sicherheitsvorgaben mit einem einzigen Satz an Sicherheitsrichtlinien in einer einzigen Managementkonsole zentral zu verwalten und über die komplette Datenlandschaft hinweg durchzusetzen: von gemanagten und privaten Endgeräten bis hin zu Websites, Cloud-Diensten, Netzwerken, E-Mail-Systemen, On-Premises-Anwendungen und generativen KI-Tools.

Die Voraussetzung dafür ist, dass Datensicherheit nicht nachgelagert behandelt wird, sondern im Mittelpunkt steht. Doch viele Unternehmen sind schon hier mit einer großen Herausforderung konfrontiert, da sie nicht wissen, welche Daten schützenswert sind, wo diese liegen, wie und über welche Kanäle mit ihnen interagiert wird und wer darauf Zugriff hat.

**it security:** *Wie genau realisieren Unternehmen eine ganzheitliche Datensicherheit? Können Sie ihnen Best Practices an die Hand geben?*

**Fabian Glöser:** Eine ganzheitliche Datensicherheit erfordert in meinen Augen fünf Kernaufgaben: Daten erkennen, klassifizieren, priorisieren, schützen und monitoren. Diese Aufgaben stehen auch bei einem modernen Data Security Posture Management im Fokus – wenn Unternehmen sie angehen, können sie gewährleisten, dass ihre Datensicherheitsstrategie alle essentiellen Aspekte abdeckt.

Die Datenklassifizierung war in der Vergangenheit oft ein großer Knackpunkt. Sie musste manuell durchgeführt werden und stellte eine echte Sisyphusarbeit dar. Deshalb waren die meisten Datensicherheitsinitiativen auch schon wieder vorbei, bevor sie richtig begonnen hatten. Darum ist es keine Übererra-

schung, dass wir momentan im Bereich der automatisierten Datenklassifizierung die größte Nachfrage am Markt erleben. Heute gibt es KI-Tools, die in der Lage sind, die Inhalte von Dokumenten zuverlässig zu verstehen und sie entsprechend zu klassifizieren. Security-Teams haben dadurch keinen nennenswerten Zusatzaufwand und werden nicht in ihrer Produktivität eingeschränkt.

**it security:** *Mit welchen Einführungszeiten müssen Unternehmen rechnen? Wie lange dauert es, bis sie eine Datensicherheitslösung einsetzen können?*

**Fabian Glöser:** Eine gute Lösung kann beispielsweise schützenswerte Daten aus dem eigenen Unternehmen mit KI und Machine Learning analysieren und ähnliche Daten weitgehend automatisch aufspüren – und zwar unabhängig davon, ob sie auf firmeneigenen Servern, in Clouds oder auf den PCs der Mitarbeiter liegen. Zudem bringt sie einen umfangreichen Satz an vordefinierten Richtlinien für den Umgang mit schützenswerten Daten mit und ist darüber hinaus in der Lage, bereits bestehende Datenklassifizierungen zu übernehmen.

Mit diesen Features ermöglicht sie einen schnellen Grundschutz, der sich immer weiter verfeinern lässt. Unternehmen mit etwa 1.000 Mitarbeitern haben erfahrungsgemäß schon nach rund zwei Wochen die Data Discovery und Datenklassifizierung abgeschlossen, können nachvollziehen, was mit den Daten geschieht und sind in der Lage, zehn bis 15 firmenspezifische Richtlinien durchzusetzen.

**it security:** *Bisher haben wir das Thema Datensicherheit aus Sicht der Security Teams betrachtet. Was bedeutet es für die Mitarbeiter? Was ändert sich für sie, wenn ein Unternehmen eine ganzheitliche Strategie umsetzt?*

**Fabian Glöser:** Wenn sie richtig umgesetzt wird, ändert sich für die Mitarbeiter nichts. Statische Data Loss Prevention, die jedem die gleichen Regeln und Limitierungen aufbürdet, gehört der Vergangenheit an. An ihre Stelle ist inzwischen ein Risiko-adaptiver Ansatz getreten, der dem Zero-Trust-Gedanken folgt.

Moderne Lösungen geben jedem Mitarbeiter Zugang zu den Daten, die ihnen anvertraut sind, analysieren riskantes Verhalten und reagieren darauf mit Maßnahmen, die dem konkreten Kontext angemessen sind. Damit helfen sie den Mitarbeitern beim Umgang mit Daten bessere Entscheidungen zu treffen und bewahren sie vor folgenschweren Fehlern. Das tun sie beispielsweise durch das Aufpoppen einer Warnmeldung, wenn jemand im Begriff ist, kritische Daten zu versenden, in eine Public Cloud hochzuladen oder auszudrucken. So verhindern sie den ungewollten Abfluss von Daten, ohne die Produktivität der Mitarbeiter unnötig einzuschränken.

Als Data-Security-Experte mit zwei Jahrzehnten Erfahrung freuen wir uns bei Forcepoint, dass die User Experience heutzutage nicht mehr mit der eines klassischen DLP zu vergleichen ist und am Markt eine neue Bewegung in Richtung ganzheitlicher Datensicherheit zu erkennen ist.

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





# Generative KI? Aber sicher!

## SICHERHEITSRISIKEN MINIMIEREN, OHNE DIE TECHNOLOGIE ZU BLOCKIEREN

ChatGPT war nur der Anfang – seit dem enormen Erfolg des Chatbots sind KI-Tools wie Pilze aus dem Boden geschossen und generative Funktionen zum festen Bestandteil vieler Anwendungen geworden. Die KI beantwortet Fragen, fasst Besprechungen und lange Dokumente zusammen, erstellt Mails und Marketingtexte, optimiert Präsentationen und sogar Quellcode – und das alles binnen Sekunden in oft überraschend hoher Qualität. Damit nimmt sie Mitarbeitern einiges an Arbeit ab und befreit sie von vielen langweiligen Auf-

smartem Helfer möglichst schnell auf breiter Front einzusetzen, doch die allzu sorglose Nutzung ist riskant. Wer beispielsweise Antworten auf Kundenanfragen von generativer KI verfassen lässt, läuft leicht Gefahr, persönliche Daten des Kunden gegenüber den Anbietern der Tools preiszugeben und gegen Datenschutzgesetze zu verstoßen. Das gilt auch für die Auswertung von Lebensläufen oder das Zusammenfassen von unbekannten Dokumenten, die ebenfalls personenbezogene Informationen enthalten können.

muss damit rechnen, dass dieses Wissen in künftigen Ausgaben auftaucht. Wer selbst geschriebenen Quellcode analysieren lässt, zeigt der KI womöglich Optimierungsmöglichkeiten auf, sodass Code-Fragmente in den Verbesserungsvorschlägen für andere Entwickler landen können.

Damit stehen Unternehmen vor einem Dilemma: Sie verlieren die Kontrolle über ihre Daten, können die KI-Tools aber auch nicht kurzerhand sperren. Zu große Dienste leisten diese bereits jetzt im Arbeitsalltag, und das, obwohl ihre Entwicklung noch ganz am Anfang steht. Dauerhaft auf sie zu verzichten, wäre – insbesondere angesichts des anhaltenden Fachkräftemangels – ein eklatanter Wettbewerbsnachteil. Zumal bestehende Security-Tools wie URL- oder DNS-Filter den Zugang zwar sperren, aber nicht steuern können, welche Informationen mit den KI-Tools geteilt werden. Deshalb müssen Unternehmen andere Wege finden, die Nutzung generativer KI zu reglementieren.

**Schon einfache Maßnahmen helfen**  
Zunächst sollten Unternehmen verschiedene KI-Tools evaluieren, um diejenigen zu ermitteln, die tatsächlich einen handfesten Nutzen bringen. Anschließend können sie Richtlinien aufstellen, welche Tools von welchen Nutzergruppen eingesetzt werden dürfen – sie müssen die Mitarbeiter aber in Schulungen auch über die Risiken generativer KI aufklären und für die Einhaltung der Richtlinien sensibilisieren. Wichtige Vorgaben könnten sein, dass keine sensiblen Informationen mit den Tools geteilt und dass



**GENERATIVE KI MACHT MITARBEITER PRODUKTIVER, BIRGT ABER DAS RISIKO, DASS SENSIBLE DATEN AUS DEM UNTERNEHMEN ABFLIEßEN.**

Fabian Glöser, Team Leader Sales Engineering, Forcepoint,  
[www.forcepoint.com](http://www.forcepoint.com)

gaben. Das Beratungsunternehmen McKinsey rechnet mit einem jährlichen Produktivitätszuwachs von 2,6 bis 4,4 Billionen US-Dollar für die Weltwirtschaft durch generative KI, vor allem in wissens- und personalintensiven Bereichen wie Kundenservice, Marketing und Vertrieb, Software-Entwicklung sowie Forschung und Entwicklung. Zum Vergleich: Das Bruttoinlandsprodukt von Deutschland lag 2022 bei umgerechnet knapp 4,1 Billionen US-Dollar.

Letztlich haben die Fähigkeiten, die ChatGPT, Bard, Jasper, Copilot und andere Tools in den vergangenen Monaten bewiesen haben, eine riesige Erwartungshaltung geweckt. Unternehmen wie Mitarbeiter brennen darauf, die

### KI-Tools verursachen Datenrisiken

Überhaupt sollten Mitarbeiter den KI-Tools keinerlei sensible Daten für Analysen oder Überarbeitungen anvertrauen, denn die Anfragen werden auf den Systemen der Anbieter gespeichert. Von dort können die Informationen bei einem Cyberangriff an die Öffentlichkeit gelangen oder in die Antworten für andere Nutzer einfließen. Schließlich trainieren die Anbieter ihre KI-Modelle nicht nur mit eigenen Datenbeständen und frei im Internet verfügbaren Informationen, sondern zum Teil auch mit den Eingaben der Nutzer. Das heißt: Wer vertrauliche Finanzdaten oder eine Präsentation für eine anstehende Firmenübernahme hochlädt, füttert die Algorithmen mit neuem Wissen und

nur vom Unternehmen bereitgestellte Accounts verwendet werden. Analog zu den inzwischen üblichen Verpflichtungserklärungen zum Datenschutz müssten Mitarbeiter eine Vereinbarung zur KI-Nutzung unterschreiben und damit die Kenntnis der Regeln bestätigen.

Trotz umfassender Aufklärung kann es allerdings passieren, dass Mitarbeiter im hektischen Arbeitsalltag sensible Informationen eingeben oder Dateien mit vertraulichen Daten hochladen. Aus diesem Grund sollten Unternehmen sicherstellen, dass sie ihre KI-Richtlinien auch technisch durchsetzen können. Am besten dafür geeignet ist ein Zero-Trust-Ansatz, der auf Sicherheitskomponenten wie Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) und Data Security aufbaut. Mittels SWG und CASB wird der Zugriff auf KI-Tools beschränkt, die von IT-Abteilung, Security-Team und Rechtsabteilung geprüft und freigegeben wurden. Nur autorisierte Mitarbeiter dürfen auf die Tools zugreifen – das aber unabhängig vom Standort oder genutzten Endgerät. Data-Security-Lösungen wiederum wachen über die Eingaben. Wer-

den sensible Informationen entdeckt, können sie – je nachdem, wie sensibel die Daten sind – einen Warnhinweis einblenden oder die Übertragung blockieren.

### **Zentralisierte Ansätze sind sinnvoll**

Um den administrativen Aufwand gering zu halten, sollten Unternehmen zu Sicherheitslösungen greifen, die gut zusammenspielen und einen zentralen Richtlinienatz nutzen. Das verhindert auch inkonsistente Richtlinien, die bei der Pflege von separaten Regelwerken in den einzelnen Lösungen unweigerlich entstehen und zu Verletzungen der Datensicherheit führen können.

Sinnvoll ist es zudem, nicht gleich den ganz großen Wurf zu versuchen und sämtliche Daten im Unternehmen zu klassifizieren, um deren Nutzung über Richtlinien zu regeln. Zum Start reicht es erfahrungsgemäß, sich auf die besonders kritischen Daten zu konzentrieren. Welche das sind, wissen die einzelnen Fachbereiche normalerweise sehr genau und können beispielsweise Vertragsdokumente, Kundenlisten, CAD-Modelle, Quellcode oder Tabellen und

Präsentationen mit finanziellen Informationen zur Verfügung stellen. Data-Security-Lösungen analysieren diese und erkennen sie wieder, wenn sie ganz oder in Teilen aus dem Unternehmen abzufließen drohen – nicht nur über KI-Tools, sondern auch via Mail, Chat oder Datei-Upload zu cloudbasierten Anwendungen. Selbst wenn sich die vertraulichen Inhalte in einem Screenshot verstecken, funktioniert das dank fortschrittlicher Texterkennung (OCR) extrem zuverlässig.

### **Ideen von außen einholen**

Darüber hinaus ist es empfehlenswert, ein Governance-Framework für KI im Unternehmen aufzusetzen. Damit werden die Prozesse und Verantwortlichkeiten für die Evaluierung neuer KI-Tools, das Onboarding neuer Mitarbeiter und die Verwaltung von Berechtigungen sowie die Klassifizierung neuer Daten standardisiert und dokumentiert. Und schließlich kann die Mitarbeit in Allianzen, Verbänden und Konsortien dabei helfen, sich innerhalb der KI-Community zu vernetzen und Best Practices für eigene Initiativen und Frameworks zu erhalten.

**Fabian Glöser**

**Unternehmen dürfen den Einsatz generative KI nicht überstürzen, sonst drohen Datenschutz- und Datensicherheitsverletzungen**

(Quelle: Sergei Tokmakov - Pixabay)





# Die menschliche Dimension der Cybersecurity

SICHERHEIT BEGINNT BEIM USER

Die schnelle Falle eines Klicks: Es ist ein normaler Tag im Büro, als ein Mitarbeiter einen Link klickt, der ihn zu einem Dokument führen soll. Seine Kollegin, vermeintlicher Absender der Nachricht, bittet ihn um schnelle Korrektur des Dokuments. Doch was nach eilig und einfach zu erfüllender Aufgabe aussieht, entwickelt sich schnell zu einem digitalen Alptraum. Die professionell aufgesetzte E-Mail erweist sich als eine Phishing-Nachricht. Ransomware infiltriert das Netzwerk. Weite Teile des Unternehmens sind für die kommenden Tage und Wochen nicht arbeitsfähig. So oder so ähnlich legen Cyberkriminelle fast täglich Unternehmen und Organisationen lahm.

In der öffentlichen Wahrnehmung erscheinen Cyberattacken oft als das

Werk gesichtsloser Hacker, die sich durch trickreiche Angriffswellen Zugang zu Systemen verschaffen. In Wirklichkeit nutzen kriminelle Organisationen aber gezielt die menschliche Schwachstelle in der IT-Sicherheitsarchitektur. Der entscheidende Auslöser ist – wie im obigen Beispiel – oft ein simpler Klick. Aus diesem Grund gilt der Mensch gleichzeitig als das wichtigste und schwächste Glied eines ganzheitlichen Sicherheitskonzepts.

Eindringlich zeigt dieses Beispiel, wie ein einziger, unbedachter Klick das Tor für verheerende digitale Angriffe öffnen kann. Es verdeutlicht, dass die Sensibilisierung der Mitarbeitenden für Cybergefahren von grundlegender Bedeutung ist, um solche Katastrophen zu verhindern. Während IT-Netzwerke ge-

gen externe Angriffe in der Regel gut geschützt sind, setzen Cyberkriminelle häufig auf Methoden, die menschliches Verhalten ins Visier nehmen.

Social Engineering zielt darauf ab, den Zugriff auf Systeme über die Manipulation von Anwendern innerhalb einer Organisation zu erhalten. Zwei entscheidende Faktoren, die über Erfolg und Misserfolg einer Cyberattacke entscheiden können, sind Kreativität und kritisches Denken. Sie spielen sowohl auf Seite der Angreifenden wie auch auf Seite der Verteidigenden eine kritische Rolle. Auf Seite der Angreifenden geht es darum, welche Gestaltung und Inhalte mit größter Wahrscheinlichkeit zum gewünschten Klick führen. Auf Seite der Verteidigenden gilt es, einen kritischen Blick für Absender, URLs und



auch für die sprachliche Gestaltung oder die Wahl der Tonalität in einer E-Mail zu entwickeln.

Der Ansatz der „User Centric Security“ betont diese Fähigkeiten und damit die entscheidende Rolle des Menschen in der Cybersicherheit. Eine erfolgreiche Sicherheitsstrategie integriert menschliche Begabung und nutzt diese ergänzend zu Technologien und Tools. Sie schafft eine dauerhafte und effektive Kultur der Cybersicherheit, die die Mitarbeitenden auf emotionaler und intellektueller Ebene anspricht. Konkrete Maßnahmen hierfür umfassen gezielte und kontinuierliche Schulungen zum Sicherheitsbewusstsein sowie benutzerfreundliche Sicherheitsrichtlinien und -lösungen.

### Mensch und Maschine

Das Beispiel oben verdeutlicht: In vielen Fällen entscheiden Menschen darüber, ob sich ein Tor für Cyberkriminelle öffnet oder nicht. Öffnet sich eines dieser Tore versehentlich oder aus Unwissenheit so können Security-Tools wie eine Applikationskontrolle Schlimmeres verhindern. Aber: Wäre es nicht viel besser, wenn sich diese Tore gar nicht erst öffneten?

Trotz intensiver Bemühungen können Security-Tools und künstliche Intelligenz eines bisher nicht: Die Intuition und Kreativität des Menschen vollständig reproduzieren. Ein feines Gespür für Nuancen, das Erkennen ungewöhnlicher Betreffzeilen und Absender in Phishing-Mails sowie die Fähigkeit, Veränderungen im Sprachgebrauch zu erfassen, sind essenziell für die Verteidigung. Die kreativen und kritischen Fähigkeiten des Menschen spielen eine unersetzliche Rolle im Wettkampf gegen die Methoden von Cyberkriminellen.

Die Einzigartigkeit menschlicher Fähigkeiten macht den Menschen unersetzlich in der Verteidigung. „Menschlichkeit“ ist bisher nicht durch künstliche In-

telligenz replizierbar. Daher setzen die besten IT-Sicherheitsmodelle auf die Fähigkeit zu kritischem Denken und Kreativität, unterstützt von modernen Cybersecurity-Technologien.

### Für Sicherheitsrisiken sensibilisieren

Diese Fähigkeiten nun in die Praxis zu übertragen ist das Ziel von „User Centric Security“. Denn trotz theoretischen Wissens über sicheres Verhalten im Netz zeigen viele Anwender und Anwenderinnen unsichere Praktiken. Konkret heißt das: Sie sind sich über die Gefahren „dort draußen“ durchaus bewusst, verhalten sich aber nicht entsprechend. Aus diesem Grund ist es wichtig, nicht nur das Bewusstsein für potenzielle Risiken zu schaffen, sondern gleichzeitig auch nachhaltige Verhaltensänderungen und eine Kultur der Cybersicherheit zu etablieren.

Herkömmliche Schulungen erzielen hier oft nicht die gewünschten Ergebnisse. Regulierungen wie ISO 27001 schreiben Security Awareness als Teil eines Sicherheitsprogramms vor und so werden Schulungen oft lediglich als Pflicht – oder anders formuliert: für den Haken

auf dem Audit-Bogen – erfüllt. Ihr Ziel ist es nicht, nachhaltig zu wirken.

Effektiver sind kontinuierliche Sensibilisierungsmaßnahmen, die Herz und Verstand der Lernenden erreichen. Erfolgreiche Initiativen sprechen sowohl emotional als auch intellektuell an, nutzen moderne Lernmethoden und kurze, prägnante Inhalte. Situationsbedingte Sicherheitstrainings, die zu relevanten Zeitpunkten stattfinden, bringen mehr als umfassende Schulungen.

### Wenn Sicherheitsmaßnahmen im Weg stehen

Was ist der größte Fehler, den Verantwortliche bei der Implementierung von Sicherheitsrichtlinien oder -tools begehen können? Sie können noch so wirkungsvolle Lösungen einführen. Sobald diese aber die Produktivität der Mitarbeitenden gefährden passiert Folgendes: Die Kollegen und Kolleginnen setzen auf ihre einzigartigen menschlichen Fähigkeiten – sie werden kreativ.

Die Erfahrung zeigt, dass Teile der Belegschaft Sicherheitsrichtlinien aktiv umgehen, wenn sie das Gefühl haben, anders nicht produktiv genug zu sein. Die Einführung neuer Maßnahmen scheitert oft nicht am Unverständnis der Risiken, sondern an umständlichen Prozessen oder Technologien, die dazu führen, dass Anwendende nach Wegen suchen, Beschränkungen zu umgehen. Das Ergebnis ist häufig eine Schatten-IT.

Die Herausforderung moderner Sicherheitsstrategien ist es, User und Systeme zusammenzubringen. Ein gelungenes Zusammenspiel von modernen Technologien und menschlichen Fähigkeiten schützt Unternehmen und Organisationen effektiv vor Cyberbedrohungen. Sicherheitslösungen sollten Security-Teams in ihren Aufgaben unterstützen, ohne die menschlichen Aspekte zu vernachlässigen.

**Andreas Fuchs**



**DIE HERAUSFORDERUNG  
MODERNER SICHERHEITSSTRATEGIEN IST ES,  
USER UND SYSTEME  
ZUSAMMENZUBRINGEN.**

Andreas Fuchs,  
Director Product Management,  
DriveLock SE, [www.drivelock.com](http://www.drivelock.com)



# IT ACADEMY MASTERCLASS

## RANSOMWARE PROTECTION

Ransomware-Angriffe gehören zu den größten Bedrohungen für die IT-Sicherheit von Unternehmen und Organisationen weltweit. Doch sie verlieren ihren Schrecken, wenn man gut vorgesorgt hat. Schadensbegrenzung für den Ernstfall lautet die Devise!

Wie können Sie als IT-Professional Ihre Organisation effektiv vor diesen Cyberbedrohungen schützen?

Indem Sie Ihr Fachwissen mit dem neuen praxisorientierten Online-Kurs: Masterclass „Ransomware Protection“ vertiefen.

### Sie erfahren:

- wie Sie die Kronjuwelen Ihres Unternehmens vor Cyberkriminellen schützen,
- wie sich eine Ransomware-Attacke allmählich „anbahnt“,
- welcher Schutzmaßnahmen es bedarf,
- wie ein Ransomware-Notfallplan aussieht.
- Und das alles veranschaulicht mit Beispielen aus der Praxis.

### 20. März Masterclass Inhalt:

- #1** Einführung & Strategie
- #2** Training, Training
- #3** Sicherheitskonzept
- #4** Verschlüsselung & Backups
- #5** Proaktiver Schutz
- #6** Ransomware-Notfallplan
- #7** Cyberstorage

**JETZT TICKETS SICHERN:**  
[www.it-daily.net/academy](http://www.it-daily.net/academy)

Tag 1: Masterclass 20.03.2024

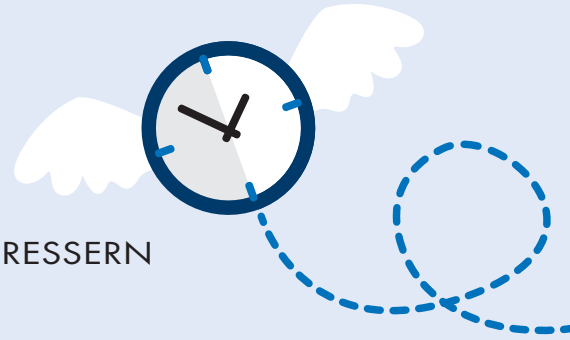
Tag 2: Creative Hub 22.03.2024



**ONLINE  
VIA ZOOM**

# Managed Services

## SO BEFREIEN SIE SICH VON 5 GROSSEN IT-ZEITFRESSERN



Überlastung, Überstunden und überfällige Projekte: So sieht der Alltag in vielen IT-Abteilungen aus. Laut einer Studie des Instituts der deutschen Wirtschaft bleibt der IT-Fachkräftemangel eine große Herausforderung. Um Zeit und Freiraum zu gewinnen, bieten sich Managed Services für wiederkehrende Standard-Tätigkeiten an: „Unternehmen sind sehr daran interessiert, IT-Hausmeisterarbeiten aus der Hand zu geben, um sich mehr um strategische Themen und wertschöpfende Projekte zu kümmern“, weiß Michael Süß. Der Leiter des Consulting-Teams IT Service Delivery benennt fünf Zeitfresser, die häufig mehr als die Hälfte der vorhandenen IT-Ressourcen in Anspruch nehmen – und von denen sich KMUs zu weiten Teilen befreien können.

### #1 Zeitfresser Nr. 1: Patches installieren

Einen PC up to date halten, kann aufwändig sein – Patches für eine ganze Rechnerflotte, Workstations, Server und Drucker zu installieren, umso mehr. „Patch Management ist einer unsere gefragtesten Managed Services“, berichtet Michael Süß von Konica Minolta.

Sein Team managed und überwacht automatisierte Updates ganz einfach aus der Ferne – eine sichere und effiziente Variante.

### #2 Zeitfresser Nr. 2: Tickets bearbeiten

Es gibt Tage, an denen Admins fast ausschließlich mit Usern telefonieren oder Mails beantworten. Zum Glück können Managed Services bei Service Desk oder User Helpdesk-Aufgaben entlasten. Michael Süß: „Wir nehmen stellvertretend für die IT-Abteilung Anfragen der Mitarbeitenden an, erstellen Tickets und können einfache Fragen sofort klären.“ Die interne IT-Mannschaft kümmert sich nur noch um die wirklich wichtigen Sachverhalte.

### #3 Zeitfresser Nr. 3: Server überwachen

Server sollen 24/7 laufen und müssen permanent überwacht werden, denn schon ein kleiner Defekt kann zu einem teuren Ausfall führen. Mit Managed Monitoring sparen sich Admins manuelle Kontrollen. „Wir können einzelne Geräte bis auf die Komponenten-Ebene überwachen. Läuft ein Lüfter ungleich-

mäßig, finden wir aus der Ferne das Problem und bestellen sofort ein Ersatzteil. Unsere Partner vor Ort bauen es ein, während der Server störungsfrei weiterläuft“, erklärt Süß. Von all diesen Schritten nimmt die IT-Abteilung erst im Reporting Notiz.

### #4 Zeitfresser Nr. 4: Firewalls checken

Die Cyber-Kriminalität hat in den letzten Jahren stark zugenommen – und damit der Aufwand, den IT-Abteilungen für die Cyber-Abwehr betreiben müssen. Doch häufig fehlt schon die Zeit, um den Status der Firewall zu checken. Managed Security ist eine wichtige Unterstützung: „Wir sichern IT-Infrastrukturen gegen Zugriffe von außen ab, protokollieren Angriffe, monitoren Firewalls und Virens Scanner und vieles mehr“, so Michael Süß. Auch gründliche Sicherheitschecks sind möglich.

### #5 Zeitfresser Nr. 5: Backups verwalten

Viele Fälle von Datenverlust kommen erst dadurch zustande, dass lückenlose Backup-Lösungen fehlen – oder Backups unbemerkt abgebrochen wurden. Nach der einmaligen Einrichtung werden Backup-Prozesse aus Zeitgründen selten überwacht. „Wer Backups als Managed Service bucht, kann sich zu 100 Prozent darauf verlassen“, meint IT-Consultant Michael Süß. „Außerdem erstellen wir übersichtliche Reports für optimale Kontrolle.“

[www.konicaminolta.de](http://www.konicaminolta.de)

#### MANAGED SERVICES VON KONICA MINOLTA

##### Das Team an Ihrer Seite

Mit über 20 Jahren Erfahrung gehört Konica Minolta zu den wichtigsten Technologie- und Managed Service Providern in Deutschland.



Hunderte KMUs und Konzerne vertrauen bereits auf die Expertise der professionellen Consultants.

Mehr Informationen zu den Managed Services finden Sie in unserem Whitepaper.



KONICA MINOLTA



# Neue Rahmenbedingungen für Service Provider

## MANAGED SERVICES IM ZEICHEN VON KI UND NACHHALTIGKEIT

Die Anforderungen an Managed Services in der IT nehmen zu. Neben Compliance, Skalierbarkeit, Flexibilität und der Integration hybrider und Multi-Cloud-Umgebungen sorgen Machine Learning (ML) und Künstliche Intelligenz (KI) für neue Rahmenbedingungen. Aber auch das Thema Nachhaltigkeit prägt das Management-Services-Geschäft der Zukunft: Managed Service Provider (MSP) müssen detailliert dokumentieren können, wie nachhaltig sie ihre Dienstleistungen und Lösungen anbieten können und welche Hardware zum Einsatz kommt.

Die Integration von KI in Managed Services, beispielsweise im Bereich IT-Sicherheit, birgt neue Herausforderungen für Service Provider und erfordert zusätzliches Fachwissen, vor allem hinsichtlich des Datenschutzes: Der Zugriff auf umfangreiche Mengen sensibler Informationen – eine Grundvoraussetzung für die effektive Nutzung von KI – setzt etwa voraus, dass Datenschutzaspekte rigoros eingehalten werden. Konkret stehen MSP in der Pflicht, Daten, die von der KI verarbeitet werden sollen, entweder zu anonymisieren oder dafür zu sorgen, dass sie nur für einen abgeschotteten Bereich der MSP-Dienstleistungen zugänglich sind. Neben der sorgfältigen Datenverwaltung durch qualifizierte Experten, die im Übrigen sowohl über KI- als auch Managed-Services-Kenntnisse verfügen müssen, sollte aus Datenschutzgründen zudem zwingend der Standort Deutschland Berücksichtigung finden. Nicht zuletzt wirft der Einsatz von KI in Mana-



**„DIE INTEGRATION VON KI IN MANAGED SERVICES, BEISPIELSWEISE IM BEREICH IT-SICHERHEIT, BIRGT NEUE HERAUSFORDERUNGEN FÜR SERVICE PROVIDER UND ERFORDERT ZUSÄTZLICHES FACHWISSEN.“**

Patrick Wunder, Team Lead Security Operations Center, Governance & Standards, noris network AG, [www.noris.de](http://www.noris.de)

ged Services Fragen zur ethischen Verantwortung auf, insbesondere im Hinblick auf Entscheidungen, die von Algorithmen getroffen werden. Auch hier sollte geschultes Personal zum Einsatz kommen, das wichtige KI-Entscheidungen freigeben oder bei Bedarf unterbinden kann.

### **Nachhaltigkeit verändert Spielregeln bei MSP**

Doch auch der anhaltende Trend zu mehr Nachhaltigkeit hat bedeutende Auswirkungen auf die Arbeit von MSP. Sie stehen mehr denn je vor der Herausforderung, ihre Dienstleistungen und Be-

triebsabläufe unter Berücksichtigung des Umweltschutzes zu gestalten, um Kunden gerecht zu werden. Ein Hauptaspekt in diesem Zusammenhang betrifft grünes Computing und Energieeffizienz. MSPs und Rechenzentrumsdienstleister stehen in der Verantwortung, ihre Data-center und Infrastrukturen zu optimieren, den Energieverbrauch zu minimieren und den ökologischen Fußabdruck zu reduzieren. Dazu gehören nicht mehr nur energieeffiziente Hardwarekomponenten, sondern mehr und mehr auch die Nutzung erneuerbarer Energien und effiziente Kühlungsmaßnahmen.

### **Recycling im großen Stil**

Mehr noch: Anbieter müssen sich Gedanken darüber machen, wie sich IT-Hardware, Batterien, Kälteaggregate, Schaltanlagen und sogar Gebäudeteile recyceln lassen. Aber auch die Zweitnutzung von Energie wird für MSP und RZ-Betreiber eine größere Rolle spielen als bisher. So könnte die Abwärme aus Rechenzentren für andere Projekte verwendet werden. Als Nachweis für nachhaltiges Computing steht die Spezifikation ISO-50001. Die internationale Norm unterstützt Unternehmen beim Aufbau eines systematischen Energiemanagements und dient zum Nachweis durch eine Zertifizierung. Ähnliches gilt für die Norm ISO-14001, mit der sich kontinuierliche Verbesserungen in Bezug auf die Umweltleistung erreichen lassen. Schließlich stehen MSP vor der Aufgabe, dieses Engagement für Nachhaltigkeit transparent in ihrer Berichterstattung unter Beweis zu stellen.

**Patrick Wunder**

# Stormshield

# XDR

Steigern Sie die  
operative Cyber-Effizienz  
Ihrer Infrastruktur

- ✓ **Kontrolle** aller XDR-Komponenten
- ✓ **Zentrale Verwaltung** von Sicherheitsvorfällen
- ✓ **Erhöhung** des Cybersicherheitsniveaus



Weiterführende  
Informationen über  
Stormshield XDR

[www.stormshield.com](http://www.stormshield.com)

**Stormshield XDR** ist die ideale Kombination aus Stormshield Network Security (SNS) und Stormshield Endpoint Security Evolution (SES), um Netzwerke zu sichern und Endgeräte zu schützen. Das Fachwissen von Stormshield im Bereich Cyber Threat Intelligence (CTI) ermöglicht es Ihnen, Bedrohungen zu antizipieren. Die Lösung wird vom Stormshield Log Supervisor (SLS) orchestriert, um Sie in Echtzeit zu warnen und eine schnelle und nachhaltige Reaktion im Netzwerk und auf den Endgeräten zu ermöglichen.

**STORMSHIELD**

# Cybergefahr im Netzwerk?

## NETWORK DETECTION AND RESPONSE (NDR) ALS GAME CHANGER

Fakt ist, dass Cyberkriminelle und interne Bedrohungen nicht nur über den klassischen Endpoint, sprich einen Computer, ein Mobiltelefon, ein Tablet oder einen Server ins Netzwerk gelangen. Es existieren unzählige weitere Schlupflöcher und es werden täglich mehr. Hybride Arbeitswelten, smarte, alte vergessene und ungepatchte Geräte oder Komponenten, die bisher bei der Cybersecurity nicht auf der Gefahrenliste standen, werden immer öfter zur Gefahr einer Netzwerkinfrastruktur in Unternehmen.

Für eine wirkungsvolle Security im Netzwerk ist es elementar, die klassischen und die neuen Gefahrenpotenziale zu erkennen. Die Schwierigkeit dabei ist, dass nur wenige Unternehmen einen aktuellen und vollständigen Überblick darüber haben, welche Komponenten in das Netzwerk eingebunden werden und eine potenzielle Gefahr darstellen. Zwar existieren wirksame Tools, um neue Geräte im Netzwerk zu entdecken, aber ob diese von einem Angreifer als Einfallstor genutzt werden, können sie nicht feststellen. Bedrohungsak-

teure, die über solch ungesicherte Wege ins Netzwerk gelangen, haben gute Chancen ihr kriminelles Vorhaben zu Ende zu bringen.

Die Lösung liegt in der Kombination aus klassischer Cybersecurity und der neuen Generation an Network Detection and Response (NDR)-Lösungen. Diese sind in der Lage, nicht nur Angreifer und deren Anomalien im Netzwerk zu erkennen. Sie erfüllen vor allem auch den Aspekt der „Response“, also der gezielten Reaktion auf Attacken. Die NDR-Technologie analysiert den Netzwerkverkehr und identifiziert verdächtige und potenziell bösartige Aktivitäten. Erst mit diesen Erkenntnissen können Sicherheitsteams aktiv Maßnahmen ergreifen, um Cyberangriffe zu bekämpfen.

### Was genau macht eine wirksame NDR-Lösung aus?

NDR-Lösungen der nächsten Generation überwachen in Zusammenarbeit mit den verwalteten Endpoints und Firewalls alle Netzwerkaktivitäten – also auch die Aktivitäten, die nicht vom Endpoint-Schutz

oder der Firewall geprüft und als bösartig erkannt werden. Möglich ist dies durch Künstliche Intelligenz, Machine Learning (ML) und Deep Learning (DL).

Während klassische NDR-Tools kontinuierlich den Rohdatenverkehr und/oder Datenflussaufzeichnungen scannen, geht NDR mit Deep-Learning-Technologie einen Schritt weiter. Sie ermöglicht die Erkennung von Mustern über mehrere Attribute hinweg und somit eine Identifizierung ohne IOC-basierte Bedrohungsdaten. Damit ist sogar die Erkennung von Bedrohungen im verschlüsselten Datenverkehr möglich.

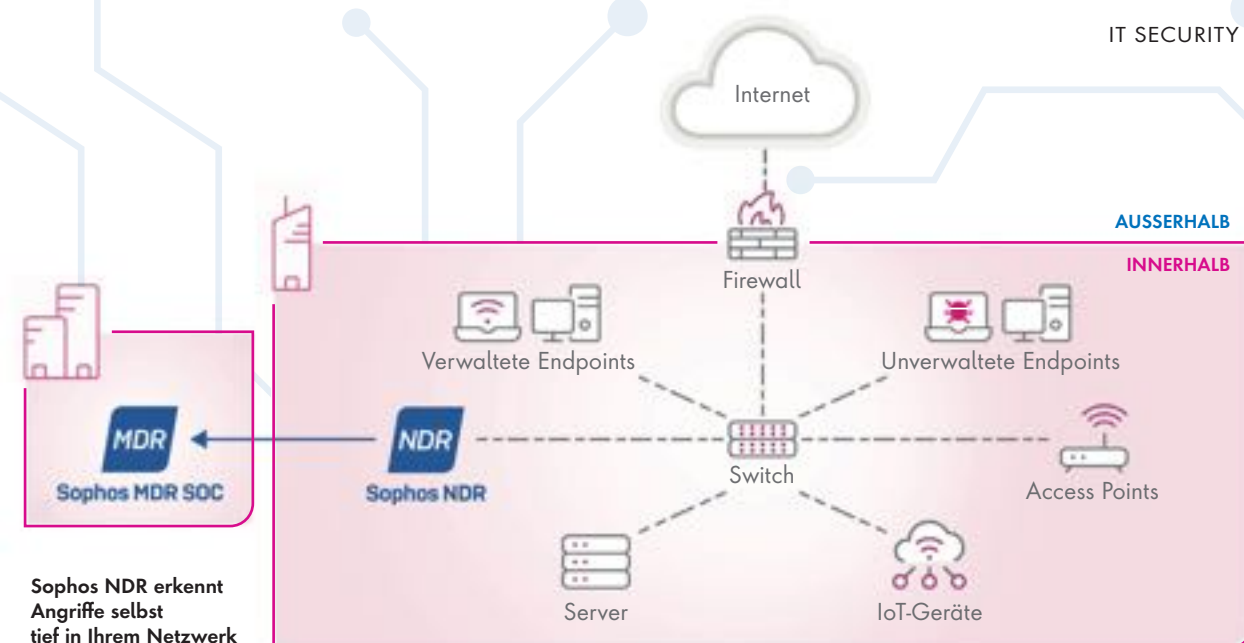
Durch die zusätzliche Verwendung von Live-Malware-Samples können schädliche Aktivitäten wie die Kommunikation von Angreifern mit infizierten Systemen in Echtzeit identifiziert werden, einschließlich Zero-Day- oder unbekannter Malware-Varianten. Dies ist elementar, wenn auf den Endgeräten kein herkömmliches Endpoint-Schutzprodukt ausgeführt werden kann und wenn die Netzwerkkommunikation aufgrund von Anforderungen zum Schutz von PII (Personal Identifying Information) nicht entschlüsselt werden sollte.

### Erkennung von ungeschützten oder unbekannten Geräten

Große, als auch mittelständische und kleinere Firmen sind über viele Jahre gewachsen oder legten bei der Gründung keinen gesteigerten Wert auf die Cybersecurity. Bei genauerer Suche findet man meist einen alten PC oder andere gefährliche IT-Komponenten ohne nötige Sicherheitsvorkehrungen. Mangels Updates oder wirksamen Schutzmechanismen sind diese Geräte ein offenes







Sophos NDR erkennt  
Angriffe selbst  
tief in Ihrem Netzwerk

Tor für Cyberkriminelle. Mit NDR der nächsten Generation haben Unternehmen die Möglichkeit, derartige Geräte zu finden und so schnell wie möglich zu patchen oder falls dies nicht möglich ist, vom Netz zu nehmen. Damit sind Unternehmen in der Lage, den internen Netzwerkverkehr detailliert auf Anomalien und Cyberaktivitäten zu prüfen.

### Angriffen auf IoT- und OT-Geräte identifizieren

Digitale Komponenten oder Gadgets sind zunehmend auch im Unternehmensumfeld zu finden. Hinzu kommen Systeme, die historisch nicht zwingend der IT-Abteilung zugeordnet waren. Es passiert schnell, dass beispielsweise ein IoT-Device, etwa eine IP-Telefonanlage, Überwachungskameras oder eine Gebäude-Automations- und Regelungstechnik ins Firmennetz eingebunden werden, ohne dass die Sicherheitsverantwortlichen der IT davon Notiz nehmen. Viele dieser Geräte und Lösungen wurden ohne Berücksichtigung der Sicherheit, sondern mit Fokus auf die Funktionalität entwickelt. Cyberkriminelle freuen sich über derartig offene Türen, zumal diese zunehmen. Denn der Zugang zum Firmennetz ist damit einfach, schnell und unauffällig. In diesen Fällen leistet NDR einen wichtigen Beitrag, um im ersten Schritt die Netzwerkaktivitäten dieser Geräte granular

zu überwachen und um bei Anomalien oder Angriffsmustern umgehend Alarm zu schlagen.

### Insider-Bedrohungen bekämpfen

Ein weiteres Gefahrenpotenzial für Netzwerke sind Insider, die ein Unternehmensnetzwerk sehr einfach infiltrieren und schädigen können – ganz gleich ob absichtlich oder durch Unachtsamkeit. Unzufriedene oder gekündigte Mitarbeiter, deren Zugänge nicht sofort und komplett gekappt werden, unzuverlässige Partner- und Service-Unternehmen oder Menschen, die gezielt von Cyberkriminellen als Industriespione oder für Sabotage angeheuert wurden, können niemals völlig ausgeschlossen werden. Tatsächlich gehen im State of Cybersecurity 2023 Report von Sophos 17 Prozent der weltweit befragten Unternehmen davon aus, dass interne Nutzer vorsätzlich ein Risiko darstellen. In Deutschland haben sogar 21 Prozent derartige Befürchtungen. Diese Bedrohungen, die keinen Einbruch ins Netzwerk benötigen, um dort Schaden anzurichten, können von Endpoint-Schutztechnologien oder Firewalls kaum gefunden werden. Denn was innerhalb des Netzwerks geschieht, wird in den meisten Sicherheitsstrategien traditionell als gutartig definiert. NDR ist in der Lage, diese Gefahren zu erkennen und

den Verantwortlichen schnell die entscheidenden Hinweise zu geben, um den Schaden abzuwehren und vor allem um die Übeltäter zu identifizieren.

### Die Response ist entscheidend bei NDR

Entscheidend ist nicht nur das Aufspüren, sondern viel mehr die Reaktion auf eine Anomalie oder ein Angriffsmuster im Netzwerk. Die Angreifer müssen aus dem Netzwerk schnell entfernt und die Schlupflöcher geschlossen werden. NDR der neuen Generation, eingebunden in ein umfassendes Sicherheitsökosystem, kann diese Anforderung, teils sogar automatisiert, abbilden. Im Zusammenspiel mit MDR (Managed Detection and Response Services) werden Administratoren, Threat Hunter und weitere Verantwortliche automatisch darüber informiert, dass sich potenziell ein Angreifer im Unternehmensnetzwerk befindet. Anschließend tritt das MDR Security Operations Center Team in Aktion und untersucht den Fall. Wenn ein Angriff festgestellt wird, neutralisiert es diesen umgehend. Gleichzeitig forschen die Analysten nach den Einfalls- und Verbreitungswegen des Angriffs, um weitere infizierte Systeme zu identifizieren und zu bereinigen oder Manipulationen und Rechteveränderungen im Netzwerk aufzudecken und zu korrigieren.

**Michael Veit | [www.sophos.de](http://www.sophos.de)**

# Die Zukunft der IT-Sicherheit



Immer wieder gibt es neue Bedrohungen für die IT- und Datensicherheit von Organisationen. Laut repräsentativer Umfragen gehen 90 Prozent der Verantwortlichen in Unternehmen davon aus, in Zukunft einer Cyberattacke ausgesetzt zu sein. Dabei kann das Identity & Access Management (IAM) eine Schlüsselrolle im Verhindern beziehungsweise Abmildern dieser Angriffe einnehmen.

[www.ogitix.de](http://www.ogitix.de)

## SCHLÜSSELROLLE IAM?

### WIE HILFT IAM BEI DER CYBERSICHERHEIT?

**94%**

der Organisationen waren in den vergangenen 12 Monaten von einem Sicherheitsvorfall betroffen – darunter Phishing-Angriffe, Insider-Bedrohungen und Ransomware-Angriffe: IAM-Systeme können dazu beitragen, diese Angriffe zu verhindern

**82%**

der Führungskräfte sind der Meinung, dass die Zahl der Cyberangriffe auf ihre Organisation zunehmen wird

### WIE HILFT IAM BEI COMPLIANCE UND DATENSCHUTZ?

#### Datenschutz-Grundverordnung (DSGVO)

IAM-Lösungen können dazu beitragen, die Einhaltung der DSGVO zu gewährleisten, indem sie sicherstellen, dass nur autorisierte Benutzer auf personenbezogene Daten zugreifen können und die Verarbeitung dieser Daten kontrolliert wird

#### NIS2 (Network and Information System Directive 2)

IAM-Lösungen können Organisationen dabei helfen, die Anforderungen der NIS2-Richtlinie zu erfüllen. Richtig umgesetzt stellt IAM sicher, dass Mitarbeiter Zugang zu allen benötigten Ressourcen erhalten, während sensible Daten gleichzeitig vor unerwünschten Zugriffen geschützt bleiben

#### ISO 27001

IAM spielt eine Schlüsselrolle bei mehreren ISO 27001-Kontrollen, und eine starke IAM-Lösung kann bei einer erfolgreichen ISO-Auditierung oder einer Auditierung in einem anderen Rahmen eine wichtige Rolle spielen

#### Payment Card Industry Data Security Standard (PCI DSS)

IAM-Lösungen können Organisationen dabei unterstützen, die PCI DSS-Compliance zu erfüllen, indem sie den Zugriff auf Kreditkarteninformationen und andere sensible Finanzdaten kontrollieren

#### Berichterstattung und Überwachung

IAM-Tools erstellen Berichte anhand der Aktionen, die auf einem System stattfinden. Dies hilft dabei, Compliance zu gewährleisten und eventuelle Sicherheitsrisiken zu bewerten



# WatchGuard Endpoint Risk Assessment

GEZIelt AUF SCHWACHSTELLENSUCHE

Cyberkriminelle werden niemals müde, nach neuen Wegen zu suchen, um Unternehmenssysteme zu kompromittieren. Mit viel Ehrgeiz versuchen sie, Lücken in der Abwehr einer Firmen-IT zu finden. Und diese sind manchmal schnell verortet, schließlich wird es für IT-Abteilungen immer schwieriger, die gesamte Angriffsfläche unter Kontrolle zu behalten. Oft fehlt es an Überblick über die Gesamtstruktur der IT-Landschaft. Zudem gibt es keine Visualisierungsmöglichkeiten, mit denen sich feststellen lässt, ob einzelne Geräte im Netzwerk Schwachstellen aufweisen, die dringend gepatcht werden müssen. Das Gleiche gilt für Devices, deren Sicherheitseinstellungen grundsätzlich schwach oder unzureichend sind. Auch der Hinweis auf unangemessenes oder anomales Verhalten innerhalb der Systeme als mögliches Anzeichen dafür, dass komplexe Angriffe im Gange sind, bleibt aus.

## Was sind die größten Stolperfallen im Hinblick auf die Absicherung von Endgeräten?

- Nachlässiger Umgang mit Patches
- Falsch konfigurierte Sicherheitslösungen
- Versehentlich nicht abgesicherte Endgeräte
- Mangelnde Sicht auf Angriffsindikatoren (Indicators of Attack – IoA)

## Risk Assessment als entscheidendes Puzzleteil, um Endpunktsicherheit zu gewährleisten

Wer böswillige Akteure davon abhalten will, ihre Pläne erfolgreich umzusetzen, benötigt Einblick, welche potenziellen Lücken von den jeweiligen Endgeräten selbst ausgehen – beispielsweise verursacht durch Fehlkonfigurationen oder fehlende, aber wichtige Patches.

Entsprechende Transparenz bieten die WatchGuard-Lösungen für Endpoint Security. Durch die integrierte Funktion des Risk-Monitorings werden Schwachstellen und Konfigurationsmängel identifiziert und automatisch nach Dringlichkeitsstufe kategorisiert. Die Überprüfung erfolgt in Echtzeit und spezifische Reportings geben jederzeit einen Überblick zum Risikostatus, so dass IT-Teams die gefährdeten Punkte sofort im Auge haben und die notwendigen Entschei-

dungen treffen können, bevor es zu spät ist. Infektionen in Folge schlechter Sicherheitskonfigurationen oder fehlender Patches kann so von Anfang an gezielt entgegengesteuert werden. Insofern gilt ein effektives Risk-Monitoring im Zuge vollständiger IT-Sicherheit heutzutage als unverzichtbar.

Wer mehr über WatchGuard Endpoint Security und das Risk-Monitoring erfahren möchte, sollte am besten gleich die kostenlose Demo-Version ausprobieren. Jeder kann hier am direkten Beispiel erleben, wie die WatchGuard-Lösung die aktiven und potenziellen Risiken ans Licht bringt und IT-Verantwortliche in die Lage versetzt, rechtzeitig adäquate Gegenmaßnahmen zu ergreifen.

[www.watchguard.de](http://www.watchguard.de)

**MEHR  
WERT**  
Demo-Version



## ENDPOINT RISK ASSESSMENT

Mit dem „Endpoint Risk Assessment“ bietet WatchGuard seit kurzem ein hilfreiches Werkzeug, mit dem Unternehmen die Sicherheitslage ihrer Endgeräte jederzeit auf Herz und Nieren prüfen können – selbst, wenn im individuellen Szenario die Lösung eines anderen Anbieters für Endpoint Security zum Tragen kommt. Der nach erfolgter Bestandsaufnahme erstellte Bericht liefert dabei nicht nur detaillierte und aussagekräftige Einblicke in das Risikoprofil, sondern umfasst ebenso Empfehlungen zur Verringerung der Angriffsfläche sowie Tipps zur Stärkung der IT-Sicherheit im Ganzen.





# DARKGATE-MALWARE

## DURCH DIE HINTERTÜR INS NETZWERK

HP Inc. hat seinen neuesten „HP Wolf Security Threat Insights Report“ veröffentlicht, der vierteljährlich erscheint und neue Entwicklungen im Bereich Cyber-Sicherheit aufzeigt. Der Bericht legt dar, dass Cyber-Kriminelle fortlaufend innovative Methoden entwickeln, um Endgeräte zu kompromittieren.

Eines der Hauptthemen des Berichts ist die DarkGate-Kampagne, die Werbe-Tools nutzt, um ihre Reichweite und Effektivität zu steigern. Durch den Einsatz von manipulierten PDF-Anhängen, die als OneDrive-Fehlermeldungen getarnt sind, werden Benutzer auf gesponserte Inhalte umgeleitet, die Malware verbreiten. Diese Strategie ermöglicht es

Angreifern, ihre Kampagnen präzise zu justieren, um eine maximale Infektionsrate zu erreichen. Zusätzlich erschweren CAPTCHA-Tools die automatisierte Erkennung der Malware.

Somit verschafft DarkGate Cyber-Kriminellen den Zugang durch die Hintertür zu Netzwerken. Dieser Zugriff setzt die Opfer Risiken wie Datendiebstahl und Ransomware aus.

### Zunahme von PDF-Malware

Ein weiterer Trend ist die steigende Verwendung von PDF-Dokumenten zur Verbreitung von Malware. Im vierten Quartal wurden elf Prozent der analysierten Malware zur Verbreitung von PDF-

## WAS SIND DIE WICHTIGSTEN BEDROHUNGSVEKTOREN

75 %  
E-Mails

12 %  
Hardware wie  
USB-Laufwerke

13 %  
Download  
von Browsern



### WEITERE ERGEBNISSE:

- Archive waren im siebten Quartal in Folge die beliebteste Malware-Übertragungsart. Sie wurde in 30 Prozent der analysierten Malware verwendet.
- Die drei wichtigsten bösartigen Archivformate: RAR, ZIP und GZ
- Mindestens 14 Prozent der von HP Sure Click identifizierten E-Mail-Bedrohungen umgingen einen oder mehrere E-Mail-Gateway-Scanner.

# MEHR WERT

HP Wolf Security Threat Insights Report



Dokumenten genutzt, verglichen mit nur vier Prozent im ersten und zweiten Quartal 2023. Ein Beispiel hierfür ist eine WikiLoader-Kampagne, die ein gefälschtes Paketlieferungs-PDF einsetzte, um Nutzer zur Installation von Ursnif-Malware zu verleiten.

Außerdem nutzen Cyber-Kriminelle legitime Datei- und Text-Sharing-Websites, um bösartige Dateien zu hosten. Unternehmen stufen die Websites häufig als vertrauenswürdig ein, dadurch wird die Erkennung durch Anti-Malware-Scanner umgangen und die Chancen der Angreifer, unentdeckt zu bleiben, steigen.

### **Verlagerung von Makros zu Office-Exploits**

Im vierten Quartal hatten mindestens 84 Prozent der Angriffe das Ziel, Schwachstellen in Tabellenkalkulationen auszunutzen, während 73 Prozent auf Word-Dokumente abzielten, um Schwachstellen in Office-Anwendungen auszunutzen. Dies setzt den Trend fort, sich von makroaktivierten Office-Angriffen zu entfernen. Trotzdem behalten makrobasierte Angriffe ihre Relevanz bei Cyberkriminellen, insbesondere bei Angriffen, die kostengünstige Malware wie Agent Tesla und XWorm einsetzen.

Alex Holland, Senior Malware Analyst im HP Wolf Security Threat Research Team, kommentiert, dass Cyberkriminelle zunehmend dazu neigen, sich in die Denkweise der Nutzer hineinzuversetzen, um deren Arbeitsweise zu verstehen. Sie verbessern beispielsweise das Design populärer Cloud-Dienste, sodass gefälschte Fehlermeldungen möglicherweise nicht sofort Verdacht erregen, selbst wenn der Benutzer zuvor noch nie damit konfrontiert wurde. Darüber hinaus kann GenAI mit geringem Aufwand überzeugende bösartige Inhalte generieren. Dies erschwert die Unterscheidung zwischen echten und gefälschten Inhalten zunehmend.

<https://hp.com/wolf>

# Bitdefender®

## Global Leader In Cybersecurity

Bitdefender ist ein führendes Unternehmen im Bereich der Cybersecurity, das weltweit erstklassige Lösungen zur Abwehr, Erkennung und Bekämpfung von Bedrohungen anbietet.



## Trusted. Always.

[bitdefender.de](https://bitdefender.de)



# HACKING

## DER UMFASSENDE PRAXIS-GUIDE

Dies ist ein praxisorientierter Leitfaden für angehende Hacker, Penetration Tester, IT-Systembeauftragte, Sicherheits-spezialisten und interessierte Power-user. Mithilfe vieler Workshops, Schritt-für-Schritt-Anleitungen sowie Tipps und Tricks lernen Sie unter anderem die Werkzeuge und Mittel der Hacker und Penetration Tester sowie die Vorgehensweise eines professionellen Hacking-Angriffs kennen. Der Fokus liegt auf der Perspektive des Angreifers und auf den Angriffstechniken, die jeder Penetration Tester kennen muss.

Dabei erläutern die Autoren für alle Angriffe auch effektive Gegenmaßnahmen. So gibt dieses Buch Ihnen zugleich auch schrittweise alle Mittel und Informationen an die Hand, um Ihre Systeme auf Herz und Nieren zu prüfen, Schwachstellen zu erkennen und sich vor Angriffen effektiv zu schützen.

Das Buch umfasst nahezu alle relevanten Hacking-Themen und besteht aus sechs Teilen zu den Themen: Arbeitsumgebung, Informationsbeschaffung, Systeme angreifen, Netzwerk- und sonstige Angriffe, Web Hacking sowie Angriffe auf WLAN und Next-Gen-Technologien.

Jedes Thema wird systematisch erläutert. Dabei werden sowohl die Hintergründe und die zugrundeliegenden Technologien als auch praktische Beispiele in konkreten Szenarien besprochen. So haben Sie die Möglichkeit, die Angriffstechniken selbst zu erleben und zu üben. Das Buch ist als Lehrbuch konzipiert, eignet sich aber auch als Nachschlagewerk.

Sowohl der Inhalt als auch die Methodik orientieren sich an der Zertifizierung zum Certified Ethical Hacker (CEHv11) des EC-Council. Testfragen

am Ende jedes Kapitels helfen dabei, das eigene Wissen zu überprüfen und für die CEH-Prüfung zu trainieren. Damit eignet sich das Buch hervorragend als ergänzendes Material zur Prüfungsvorbereitung.



### **Hacking: Der umfassende Praxis-Guide**

Eric Amberg, Daniel Schmid;  
mitp Verlags GmbH & Co.KG;  
04-2024



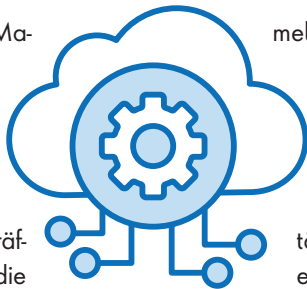
# Identity Access Management

WARUM ES JETZT NOCH EINFACHER, SICHERER UND EFFIZIENTER IST

Längst ist Identity Access Management (IAM) kein Geheimtipp mehr. Die korrekte Verwaltung von Benutzern und deren Berechtigungen ist unabdingbar, das ist IT-Fachkräften klar – nicht nur, um die Sicherheit und Effizienz in Unternehmen zu verbessern, sondern auch, um den hohen Anforderungen von Compliance-Richtlinien wie NIS2, ISO 27001 oder TISAX gerecht zu werden.

Allerdings setzen viele Organisationen weiterhin auf die manuelle Benutzerverwaltung, obwohl dies ab einer bestimmten Unternehmensgröße, sprich Benutzeranzahl, nicht mehr den Best Practices entspricht. Fehler schleichen sich ein, Berechtigungen werden nicht rechtzeitig entzogen und es fehlt generell an Überblick: Wer hat Zugriff auf welche Ordner? Wer hat die Berechtigungen erteilt? Bis wann sind sie gültig? Unternehmen, die auf diese Fragen ad hoc keine Antworten wissen, haben ein großes Sicherheitsproblem.

Mit einem geeigneten IAM-Tool hingegen kann sichergestellt werden, dass User nicht mehr Berechtigungen ansam-



eln, als sie für ihre Arbeit benötigen. Die Automatisierung von Prozessen wie Benutzeranlage und Rechtevergabe reduziert redundante alltägliche Aufgaben, und entlastet somit die IT.

## No-Code IAM für den Mittelstand

Viele Mittelstandsbetriebe schecken vor der Umsetzung einer solchen IAM-Lösung zurück, weil sie dies als „zu komplex, zu aufwendig“ abstempeln – nicht zuletzt auf Grund des Fachkräftemangels, mit dem die IT-Branche zu kämpfen hat. Es fehlt an Ressourcen, um eine aufwendige Lösung zu implementieren, die Monate bis Jahre an Programmierarbeit mit sich bringt.

Doch dank der innovativen No-Code IAM-Lösung von tenfold können auch mittelständische Unternehmen in den Genuss einer sicheren und effizienten Benutzerverwaltung kommen – ganz ohne aufwendiges Programmieren. Über vorgefertigte Plugins werden sämtliche gängigen Systeme wie Microsoft 365, Teams und OneDrive direkt angebunden, so dass man in nur wenigen Wochen startklar ist. Auf diese

Weise unterstützt tenfold seit Jahren Organisationen dabei, ihre User-Berechtigungen einfach und sicher zu verwalten.

## Ab März 2024 im neuen, modernen Design

tenfold Software arbeitet stets daran, auf dem neuesten Stand der Technik zu bleiben und Kunden gleichzeitig die bestmögliche User-Experience zu bieten. Ab März 2024 präsentiert sich tenfold daher im neuen Design.

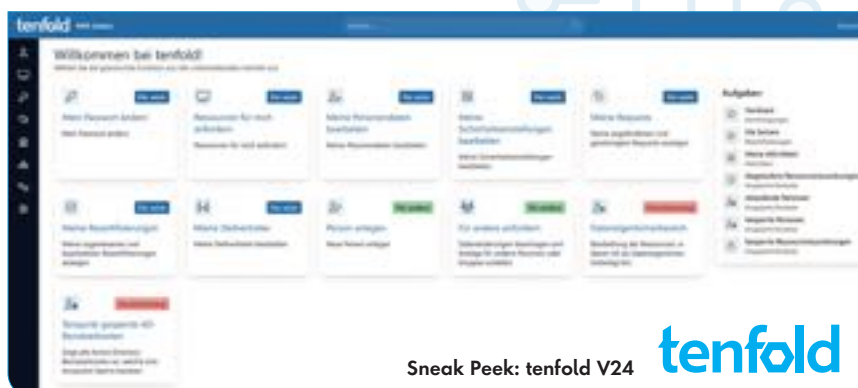
### Neue Features im Überblick:

**Modernes, benutzerfreundliches Design:** Der neue, moderne Look rückt die Benutzerfreundlichkeit noch weiter in den Fokus. Ein klares und übersichtliches Layout ermöglicht es Benutzern, sich schnell und intuitiv zurechtzufinden. Über 300 Anpassungen wurden an der Benutzeroberfläche vorgenommen.

**Noch schneller, noch effizienter:** Eine Reihe von Leistungsverbesserungen und Optimierungen im Backend sorgen für reibungslose Abläufe, die eine noch größere Zeitersparnis ermöglichen.

**Neuester Stand der Technik:** Im Zuge der Anpassungen wurden alle technischen Komponenten auf den neuesten Stand gebracht, um eine optimale Leistung und Zuverlässigkeit aller Dienste zu gewährleisten.

**Zusammenfassend:** Ein modernes Design, höchste Sicherheit, schnelle Leistung und eine intuitive Oberfläche machen tenfold zur idealen Lösung für Unternehmen, die ihre Identitäts- und Zugriffsverwaltung auf das nächste Level heben wollen.



Sneak Peek: tenfold V24

**tenfold**

[www.tenfold-security.com](https://www.tenfold-security.com)

# Revolution im Zugriffsmanagement

## KÜNSTLICHE INTELLIGENZ SINNVOLL EINSETZEN

Viele Unternehmen erwägen derzeit, künstliche Intelligenz (KI) für die Identitätsverwaltung zu verwenden. Mit der Technologie lassen sich nicht nur auffällige Verhaltensweisen von Nutzern effektiver und automatisiert überwachen, sondern auch Sicherheitssysteme verbessern. In der Studie „The State of Identity Governance 2024“ gaben fast 53 Prozent der 567 befragten IT-Experten und Führungskräfte an, dass etwa im Identitäts- und Zugriffsmanagement Funktionen zur Unterstützung von KI zu den fünf wichtigsten Prioritäten bei der Evaluierung einer solchen Lösung gehö-

ren. Immer mehr IT-Administratoren kommen zu dem Schluss, dass mit vielen hergebrachten IGA-Systemen (Identity Governance and Administration) ein zeitgemäßes Management von Zugriffsrechten nicht mehr machbar ist.

Die Analyse von Zugriffsversuchen und Nutzerverhalten wird dort nicht unterstützt, die regelmäßige manuelle Prüfung von Berechtigungen muss oft manuell erfolgen und ist für größere Unternehmen mit zahlreichen neuen SaaS-Anwendungen zu aufwändig. Selbst bei vielen modernen IGA-Lösungen ist die

„Zertifizierungsmüdigkeit“ ein häufig auftretendes Phänomen. KI-gesteuerte Lösungen, die auf maschinellem Lernen (ML) basieren, erleichtern die Überprüfung von Konten und Zugriffsrechten erheblich und erhöhen die Sicherheit.

### KI erweitert

#### Zugriffsmanagementfunktionen

Mit KI für IGA können Unternehmen sicherstellen, dass Benutzer nur Zugriff auf die Anwendungen und Systeme erhalten, die sie für ihre Arbeit benötigen - und zwar über den gesamten Identitätslebenszyklus hinweg: vom ersten Arbeitstag bis zum Ausscheiden aus dem Unternehmen. KI für IGA unterstützt Unternehmen dabei, das Zugriffsmanagement zu optimieren und sich an neue Bedrohungen anzupassen, indem fortschrittliche Analyse- und Automatisierungsfunktionen genutzt werden.

Hier einige Beispiele für Verbesserungen durch die Nutzung von KI:

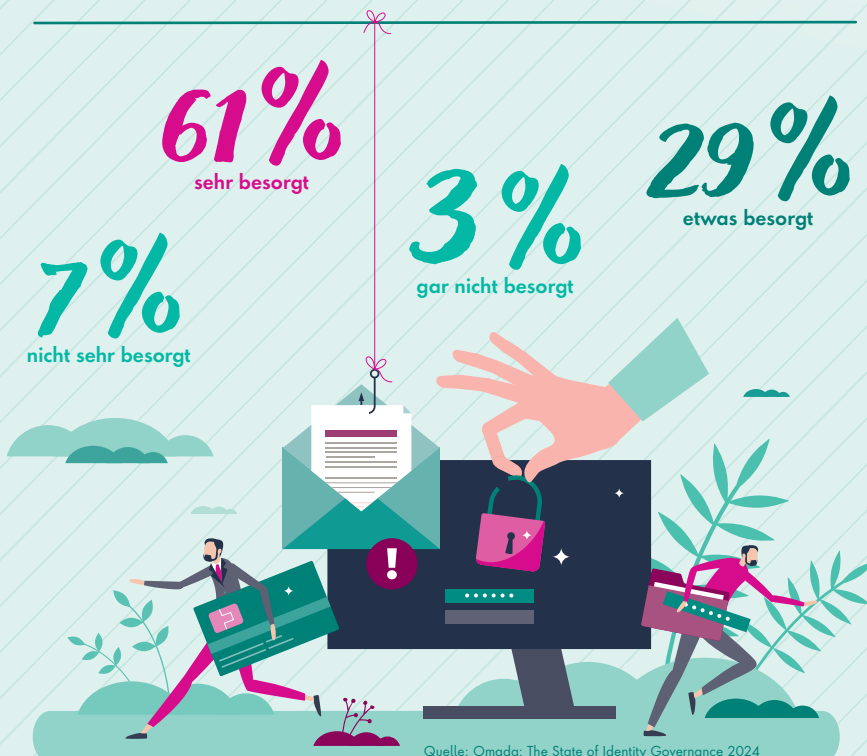
#### ➤ Verifizierung der Benutzeridentität:

KI-gestütztes Identitätsmanagement nutzt biometrische Daten (Gesichtserkennung, Stimm- sowie Fingerabdruckerkennung), um Benutzer zu identifizieren und sicherzustellen, dass Personen, die auf sensible Systeme und Anwendungen zugreifen, auch diejenigen sind, für die sie sich ausgeben. Die KI-gestützte Benutzerüberprüfung geht über andere Arten der Multi-Faktor-Authentifizierung (MFA) hinaus und bietet eine zusätzliche Ebene der Identitätssicherheit.

#### ➤ Verwaltung des Benutzerzugriffs:

KI-Lösungen erleichtern die rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC), indem sie die Aufgaben einer Person in der Organisation analysieren und ihr über vordefinierte Rollen die richtigen Zugriffsrechte zuweisen. Automatisierte KI-Algorithmen

### WIE BESORGT IST IHR UNTERNEHMEN ÜBER DIE RISIKEN IM ZUSAMMENHANG MIT IDENTITÄTSBEZOGENEN CYBERSECURITY-BEDROHUNGEN?



optimieren die Rechteverwaltung und verringern das Risiko eines unbefugten Zugriffs.

### ➤ **Analyse des Nutzerverhaltens:**

KI-Algorithmen optimieren die Erkennung von Anomalien. Greift ein Benutzer unerwartet auf Daten zu, die er für Erfüllung seiner Aufgaben nicht benötigt, identifiziert das System diese Aktivität als mögliches Sicherheitsrisiko.

### ➤ **Kontextualisierung von Zugriffsrichtlinien:**

KI-Algorithmen berücksichtigen Informationen wie Standort, Tageszeit, verwendetes Gerät, um bessere Entscheidungen über Zugriffsrechte zu treffen. Versucht ein Benutzer von einem unbekannten Ort aus auf sensible Daten zuzugreifen, kann das System eine zusätzliche Überprüfung anfordern.

### ➤ **Verwaltung des Lebenszyklus von Benutzeridentitäten:**

KI automatisiert die Zuweisung von Zugriffsrechten beim Onboarding und den Entzug des Zugriffs beim Offboarding.

### ➤ **Einhaltung der Sicherheitsrichtlinien:**

KI für das Identitätsmanagement erleichtert die konsistente Durchsetzung von Unternehmensrichtlinien für das Identitäts- und Zugriffsmanagement und stellt sicher, dass gesetzliche Anforderungen erfüllt sind.

### **Bedrohungen intelligent bekämpfen**

Die Einführung von KI für das Identitätsmanagement ist der erste Schritt zur Reduzierung der Identitätsbedrohungen, mit denen ein Unternehmen konfrontiert ist. Sobald automatisierte Prozesse eingerichtet sind, braucht es jedoch einen definierten Prozess, um die Daten, die die KI-gestützte Lösung liefert, in verwertbare Informationen umzuwandeln.

Hier sind drei Möglichkeiten, wie KI und ML-gestützte Analysen IGA unterstützen können:

**#1** Automatisierte Empfehlungen und Chat-basierte KI reduzieren die Lernkurve im Zusammenhang mit Zugriffsanfragen und -genehmigungen, erhöhen die Effizienz des Onboarding-Prozesses und ermöglichen IT-Administratoren und Benutzern Produktivität vom ersten Tag an.

**#2** Rollenerkennung, um festzustellen, welche Identitäten gemeinsame Zugriffsebenen haben, die Zuweisung zukünftiger Identitäten zu erleichtern, Zeit zu sparen und die richtige Zugriffsebene für die richtige Identität zu gewährleisten.

**#3** Verbesserte Berichte, mit denen Berechtigungen, Nutzerkonten im Zeitverlauf, organisatorische Kontexte oder Ressourcen analysiert werden können.

**Es wird klar:** Der Einsatz von KI im Identitätsmanagement bietet enorme Vorteile. Es gibt jedoch auch Risiken, die berücksichtigt werden müssen. Man muss daher sicherstellen, dass automatisierte Prozesse kein falsches Gefühl von Sicherheit vermitteln. Administratoren müssen sehr genau darauf achten, dass die KI-Algorithmen die gewünschten Ergebnisse liefern. KI-gestütztes Role Mining hilft Unternehmen beim Aufbau einer rollenbasierten, kontextbezogenen Rechteverwaltung als Basis für mehr Sicherheit und vereinfachte Governance.

Ein weiteres Thema ist der Schutz der Privatsphäre: KI-gestütztes Identitäts- und Zugriffsmanagement analysiert personenbezogene Daten, die vor Cyberangriffen geschützt werden müssen. Dabei ist zu berücksichtigen, dass sich die Datenschutzbestimmungen weiterentwickeln und dass Daten, die heute noch



**JEDE ORGANISATION SOLLTE EIN SYSTEM IMPLEMENTIEREN, DAS EINEN UMFASSENDE UND AUTOMATISIERTEN ANSATZ FÜR DAS IDENTITÄTS- UND ZUGRIFFSMANAGEMENT BIETET.**

Stephen Lowing,  
Vice President Marketing, Omada,  
[www.omadaidentity.com](http://www.omadaidentity.com)

nicht als sensibel betrachtet werden, morgen schon als sensibel gelten können.

### **Maßgeschneidertes Identitätsmanagement**

Jede Organisation sollte ein System implementieren, das einen umfassenden und automatisierten Ansatz für das IAM bietet und sicherstellt, dass die Anforderungen an Sicherheit, Compliance und Effizienz erfüllt werden. KI-gestützte Funktionen bringen die Möglichkeiten von IGA-Systemen auf ein neues Level, indem sie Identitätsprüfung, rollenbasierte Zugriffskontrolle und das Lebenszyklusmanagement automatisieren und die Nutzer unterstützen. KI-Algorithmen wandeln die gewonnenen Erkenntnisse dann in verwertbare Informationen um, die die Unternehmens-IT analysieren kann, um die Identitätssicherheitsstrategie zu optimieren. Zur Umsetzung einer modernen IGA-Strategie gehört schließlich noch ein Best-Practice-Verfahren, das sicherstellt, dass die Einführung eines IGA-Systems auch wirklich die Geschäfts- und Sicherheitsanforderungen des Unternehmens abbildet.

**Stephen Lowing**



# Sieben IAM-Prognosen für die Zukunft

## VORAUSSAGEN ZUR WEITERENTWICKLUNG DER IDENTITÄTS- UND ZUGRIFFSVERWALTUNG

Im Bereich der Identitäts- und Zugriffsverwaltung (IAM) sowie der IT-Sicherheit entwickeln sich kontinuierlich neue Trends und Prognosen, die die Art und Weise, wie Organisationen ihre Systeme schützen und verwalten, maßgeblich beeinflussen. Angesichts der ständig wachsenden Bedrohungen und der steigenden Anforderungen an Datenschutz und Compliance ist es unerlässlich, sich über die aktuellen Entwicklungen in diesen Bereichen auf dem Laufenden zu halten.

Daher werfen wir einen Blick auf die Trends und Prognosen, die die IAM-Landschaft in den kommenden Jahren prägen werden.

### #1 KI wird die Bedingungen für die Identitätsüberprüfung verändern und für Gesetzgebung sorgen

Das wachsende Potenzial und die zunehmende Bedeutung der KI waren im Jahr 2023 kaum zu übersehen. Schon jetzt macht sie kurzen Prozess mit der Datenanalyse, der Bilderzeugung und allen möglichen anderen Verarbeitungs- und kognitiven Aufgaben. Wenn man diese Fähigkeiten auf die Prüfung der Identitäten anwendet, entstehen neue Anwendungsfelder. Ein Beispiel für die disruptive Kraft der KI ist das Management der Passagierströme an Flughäfen. KI kann hier zur Identitätsüberprüfung bei elektronischen Gates eingesetzt werden. Die zunehmende Verbreitung von künstlicher Intelligenz in Verbindung mit einer Zukunft, in der sich



**DIE WACHSENDE VERBREITUNG VON KÜNSTLICHER INTELLIGENZ UND DIE ZUNEHMENDE DIGITALE IDENTIFIZIERUNG UND VERIFIZIERUNG DURCH MENSCHEN WERDEN VORAUSSICHTLICHE NEUE BEDROHUNGEN UND FÄLSCHUNGSTECHNIKEN HERVORBRINGEN.**

Danny de Vreeze,  
Vice President IAM, Thales,  
[www.thalesgroup.com](http://www.thalesgroup.com)

Menschen zunehmend digital identifizieren und verifizieren, wird wahrscheinlich neue Bedrohungen und Techniken zur Fälschung und Nachahmung hervorbringen. 2024 wird das Jahr sein, in dem KI eingesetzt wird, um Identitätstechnologien nach Belieben zu umgehen. Dies wird zu einer starken Zunahme von Tools führen, die KI und ihre Marker erkennen können, sowie zu Forderungen nach neuen Gesetzen, um dem Fälschungsrisiko zu begegnen.

### #2 Passkeys werden im Jahr 2024 das digitale Banking beherrschen

Im kommenden Jahr werden sich synchronisierte Passkeys branchenübergreifend durchsetzen. Dies wird den Finanzsektor, insbesondere die Banken, dazu veranlassen, entsprechend der Marktnachfrage mehr Passkeys einzuführen und gleichzeitig das Niveau der Compliance und der Sicherheit im digitalen Banking aufrechtzuerhalten. Die Herausforderung für Banken besteht darin, effizient und konform mit aufkommenden Standards wie PSD3 zu agieren, die eine Multi-Faktor-Authentifizierung erfordern und häufig auf Tools wie Hardware-Tokens angewiesen sind. Die Banken werden sich dieser Herausforderung stellen, indem sie in gerätegebundene Passkeys im Gegensatz zu synchronisierten Passkeys investieren, um ähnliche Vorteile wie Sicherheit und Benutzerfreundlichkeit zu gewährleisten.

### #3 Validierte ID- und Attribut-Provider werden das Zero-Knowledge-Protokoll und „vertrauenswürdige“ Nutzeridentitäten vorantreiben

Im Jahr 2024 werden die wichtigsten Anbieter von Identitäten und ihren Attributen auf den Plan treten und den ID-Markt mit Diensten, wie einem besseren Schutz der Privatsphäre, Personalisierung und einem differenzierten Zugang zu Ressourcen vorantreiben. Mit der Entwicklung der Ausweise werden sich Menschen im Alltag zunehmend auf „vertrauenswürdige Identitäten“ für die

grundlegende Überprüfung und den Zugang verlassen – nehmen wir zum Beispiel Identitäts-Wallets. Bis 2024 müssen alle EU-Mitgliedstaaten jedem Bürger einen digitalen Identitäts-Wallet zur Verfügung stellen, den er sowohl für Online- als auch für Offline-Dienste in der EU nutzen kann. Digitale ID-Geldbörsen werden dem Nutzer mehr Kontrolle über die Freigabe eines granularen und personalisierten Zugriffs auf Attribute für Dienstanbieter geben. Der Nachweis des Zero Trusts wird immer beliebter werden und die Türen für die Registrierung von Mandaten sowie für kommerzielle Geschäftsmöglichkeiten für Datenanbieter öffnen.

#### #4 Die Datenhoheit gewinnt an Bedeutung

Die DSGVO setzt weiterhin den Standard für die Speicherung und Verarbeitung von Daten auf regionaler Ebene, 2024 wird die Nachfrage nach dieser Kontrolle in den USA und Kanada steigen. Unternehmen werden diese Anforderungen auf Unternehmensebene erfüllen, indem sie starke Datenverschlüsselungsmethoden implementieren, einschließlich Bring-your-own-key- und Hold-your-own-key-Funktionen. Auf individueller Ebene werden die Nutzer von mehr Möglichkeiten profitieren, der Verwendung ihrer Daten zuzustimmen, sowie von einem Zero-Knowledge-Proof und mehr. Insbesondere in den USA ist mehr Bewegung in Sachen Datenschutz zu beobachten, dies wird sich auch auf die Datensouveränität in den Gesprächen mit den Gesetzgebern auswirken.

#### #5 Entwicklung bei digitalen Währungen

Sowohl die digitale Identität als auch die Technologien für Währungen und die damit verbundenen Vereinbarungen schreiten voran. In diesem Jahr hat Apple seine bestehende Partnerschaft mit der US-Großbank Goldman Sachs ausgeweitet und ein neues hochverzinsliches Sparkonto eingeführt, das über

die Apple-eigene Kreditkarte zugänglich ist und eine tiefgreifende Integration des digitalen Wallets bietet. Dies war nur eines von mehreren Finanzangeboten, die das Unternehmen in diesem Jahr angekündigt hat – ganz zu schweigen von Unternehmen wie Google, das bereits seit 2019 über eine EU-weite E-Geld-Lizenz verfügt. Die Europäische Zentralbank beschleunigt ihr digitales Euro-Projekt und die US-Regierung treibt ihre eigene Währung im Rahmen des „Project Cedar“ vor. Deshalb ist das Umfeld 2024 reif für einen großen Durchbruch dieser Art von Währung.

#### #6 Verschlüsselungs- und Signierschlüssel werden im Jahr 2024 ihre Bedeutung für die Identitäts- und Datensicherheit haben

Die Datensouveränität ist ein zunehmendes Problem für alle Arten von globalen Unternehmen – und hält sie davon ab, in die Public Cloud zu wechseln, insbesondere wenn sie außerhalb der USA ansässig sind. Gleichzeitig lässt sich ein enormes Wachstum bei der Verwendung von Signierschlüsseln sowohl für die passwortlose Identitätsüberprüfung als auch für die Verschlüsselung beobachten. Im Jahr 2024 werden mehr zentralisierte Schlüsselverwaltungssysteme auf den Markt kommen. Sie sind eng mit Public-Cloud-Anbietern verbunden und tragen dazu bei, die Barriere zu beseitigen, die derzeit für viele Unternehmen bei der vollständigen Umstellung auf die Public Cloud besteht. Indem sie Unternehmen eine größere Kontrolle über den gesamten Lebenszyklus ihrer Verschlüsselungsschlüssel geben, können Unternehmen ihren Kunden die notwendigen Garantien für die Souveränität ihrer Daten geben.

#### #7 Digitales Vertrauen in kollaborative Netzwerke wird entscheidend für Wachstum und Erfolg von Unternehmen sein

Kollaborative Netzwerke sind in Geschäftsmodellen für die moderne Ferti-

gung weit verbreitet, um die schnelllebigen Innovationen und komplexen Lieferketten von heute zu unterstützen. Die effiziente und sichere Verwaltung verschiedener Vertrauensstufen in kollaborativen Netzwerken ist entscheidend für die Produktentwicklung und die Markteinführung. Die Benutzererfahrung bei Verbraucheridentitäten und geschäftskritischen Identitätsnachweisen und -verifizierungen im Bankwesen ist Vorbild für ein sicheres B2B-Identitätsmanagement in allen Branchen. Ziel ist ein sicheres, rationalisiertes und passwortloses Onboarding und Authentifizierungen verschiedener Benutzer in den Collaborative Networks zu ermöglichen. Gleichzeitig sollen Risiken minimiert und die Geschäftskontinuität und deren Erfolg beschleunigt werden.

**Danny de Vreeze**







Quelle: Deutsche Messe AG

# Industrial Security Circus

## ENERGIZING A SUSTAINABLE INDUSTRY

Unter dem Leitthema „Energizing a Sustainable Industry“ gibt die Hannover Messe 2024 Antworten auf die Fragen unserer Zeit. Der Schlüssel liegt im Zusammenspiel der Technologien, branchenübergreifenden Kollaborationen, Technologieoffenheit und einem klaren politischen Rahmen.

Im Ausstellungsbereich Digital Ecosystems wird der gesamte digitale Wertschöpfungsbereich der produzierenden Industrie abgebildet. Es werden IT-Lösungen und Anwendungen gezeigt, die in jedem produzierenden Unternehmen die digitale Transformation voranbringen. Die zunehmende Vernetzung von industriellen Systemen und die Digitalisierung bringen auch neue Sicherheitsrisiken mit sich. Der Schutz von kritischen Infrastrukturen und industriellen Prozessen wird daher immer wichtiger. Dort setzt der Gemeinschaftsstand „Industrial Security Circus“ an. Präsentiert wird eine Mischung aus Technologien, Angeboten, Produkten und Dienstleistungen, unter anderem IT-Sicherheitstrainings und zielgerichtet-erklärendes Entertainment mit innovativen Wegen der Wis-

sensvermittlung im Kontext von IT/OT Security in der industriellen Fertigung.

### Industrial Security Circus

Auf der Industrial Security Circus Stage entsteht ein Erlebnisraum, der den Besuchern der Messe die Notwendigkeit von IT/OT Security verdeutlicht.

Auf der weltweit wichtigsten Industriemesse stellen Unternehmen aus dem Maschinenbau, der Elektro- und Digitalindustrie sowie der Energiewirtschaft gemeinsam Lösungen für eine gleichmaßen leistungsstarke und nachhaltige Industrie vor. Bis zu 4 000 Unternehmen agieren als industrielles Ökosystem und zeigen, wie Klimaneutralität durch Elektrifizierung, Digitalisierung und Automation erreicht werden kann. Insbesondere der Einsatz künstlicher Intelligenz führt in der Industrie zu mehr Effizienz und Produktqualität.

Mehr als 300 Startups aus unterschiedlichen Technologiefeldern zeigen Innovationen mit disruptivem Potenzial. Die Hannover Messe bietet innovative Beiteiligungsformen, um die Industrieunter-

nehmen mit den Startups über das persönliche Kennenlernen zu vernetzen.

Die nachhaltige und emissionsfreie Energieversorgung rückt zunehmend in den Fokus. Dazu zählt der Einsatz erneuerbarer Energien sowie deren Speicherung, die Implementierung eines umfassenden Energiemanagementsystems und die Integration in ein intelligentes Stromnetz. Mit dem vermehrten Einsatz von volatilen Energiequellen hat grüner Wasserstoff an Bedeutung gewonnen. Auf der kommenden Hannover Messe präsentieren rund 500 Aussteller der Wasserstoff- und Brennstoffzellenbranche ihre Lösungen für ein emissionsfreies Wirtschaften.

### Klima schützen, Wohlstand vorantreiben

Die eigene Wettbewerbsfähigkeit ausbauen, das Klima schützen, Wohlstand vorantreiben – das sind die großen Aufgaben, denen sich die Industrie heute widmet. Innovative Technologien sind der Schlüssel zur Bewältigung dieser Herausforderungen. Doch wie können Unternehmen Automation, künstliche Intelligenz, erneuerbare Energien und Wasserstoff effizient einsetzen? Die Hannover Messe 2024 gibt Antworten.

[www.hannovermesse.de](http://www.hannovermesse.de)

**Hannover Messe  
2024**

**22. – 26. April 2024**





# Insellösungen adé

## DIE CYBERRESILIENZ NICHT UNTERMINIEREN

Mit 2023 ging ein Jahr zu Ende, in dem kaum ein Sektor, von der privaten Wirtschaft bis hin zur öffentlichen Hand, von Angriffen unberührt blieb. Die Zeit ist reif für holistische Cybersicherheitsansätze.

Wie breit die Konsequenzen von Cyberangriffen ausfallen können, zeigte uns der Ende Oktober 2023 durchgeführte Ransomware-Angriff auf den kommunalen IT-Dienstleister Südwestfalen-IT. Von der dadurch bedingten Unterbrechung aller Verbindungen nach außen waren laut KonBriefing über 110 Gemeinden und Organisationen in Nordrhein-Westfalen sowie einige in Niedersachsen betroffen. Im neuen Jahr sieht es bereits düster aus, besonders im KRITIS-Umfeld. Cyberkriminelle Machenschaften finden kein Ende, doch begegnet man ihnen nach wie vor mit Ansätzen, die keine Sichtbarkeit auf das große Ganze gewähren: Insellösungen, die dem typischen Silos-Denken bei der Cybersicherheit entspringen, unterminieren die Cyberresilienz der Organisationen.

### Holistische Sicherheitskonzepte

Um kritische Infrastrukturen und industrielle Anlagen effektiv zu schützen und einen reibungslosen Betrieb zu gewährleisten, muss man zu Werkzeugen greifen, die eine solche Sichtbarkeit über alle in der Organisation eingesetzten Kommunikationskanäle und Prozesse hinweg liefern – ganz im Sinne holistischer Sicherheitskonzepte und -strategien. Stormshield, die auf Cybersicherheit spezialisierte Airbus-Tochter, bietet zum Beispiel mit ihrem XDR-Angebot eine hoch-

integrierte Plattform für die Erkennung und Reaktion auf Sicherheitsvorfälle. Sie besteht aus der idealen Kombination aus Stormshield Network Security (SNS) zum Schutz von Netzwerken und Stormshield Endpoint Security (SES) für die Endgerätesicherheit, unterstützt durch die Threat-Intelligence (CTI) von Stormshield zur Antizipation von Bedrohungen, und passt ihr Verhalten automatisch an das aktuelle Bedrohungsszenario an. Mit Stormshield XDR können Unternehmen über verschiedene Sicherheitsprodukte hinweg in Echtzeit auf Ereignisse reagieren, die sich aus der Analyse von Endgeräten, Netzwerken sowie Web- und E-Mail-Dateien ergeben. Der Stormshield Log Supervisor (SLS) orchestriert alle Lösungen, um eine schnelle Reaktion sowohl im Netzwerk als auch auf Endgeräten zu ermöglichen.

Doch nicht nur. Die Sicherheitslösungen von Stormshield bieten spezielle Funktionen, um Cyberangriffe auf OT-Infrastrukturen (Industrie, Gebäudeautomation und -management, Smart City) proaktiv zu bekämpfen. Die IPS-/UTM-Firewall-Modelle SNi40 & SNi20 sind nach dem ANSSI-Standard (französisches Pendant des hiesigen BSIs) zertifiziert und bieten einen robusten Schutz in solchen Umgebungen. Vom Hochver-



**STORMSHIELD BIETET MASSGESCHNEIDERTE PRODUKTE, UM DIE KONTINUIERLICHE FUNKTIONSFÄHIGKEIT UND DIE SICHERHEIT VON NETZEN ZU GEWÄHRLEISTEN.**

Uwe Gries, Country Manager DACH, Stormshield, [www.stormshield.com](http://www.stormshield.com)

fügarkeitsmodus bis hin zur Bandbreitenverwaltung sorgen diese Lösungen für eine zuverlässige Konnektivität und Betriebssicherheit. Nicht zuletzt ist auch der «Made in Europe»-Aspekt dieser Cybersicherheitslösungen ein Pluspunkt im Sinne der Entsprechung gesetzlicher Anforderungen: Die europäische Richtlinie für Cybersecurity NIS2 verlangt, dass sich Organisationen bis Ende 2024 nachweisbar und verpflichtend besser gegen IT-Angriffe schützen.

### Maßgeschneiderte Lösung

Angesichts der zunehmenden Komplexität und Leistungsfähigkeit moderner Architekturen, die das IP-Protokoll nutzen, sind kritische Kommunikationsnetzwerke zahlreichen Cyberbedrohungen ausgesetzt. Eine Unterbrechung des

Betriebs ist hier undenkbar. Stormshield bietet maßgeschneiderte Produkte, um die kontinuierliche Funktionsfähigkeit und die Sicherheit von Netzen zu gewährleisten, worauf Staat und Gesellschaft angewiesen sind.

Uwe Gries



# SMTP Smuggling

## IDENTITÄTSMISSBRAUCH IN E-MAILS BEKÄMPFEN

Cyberangriffe mit Hilfe von E-Mails sind weiterhin eine große Bedrohung für Unternehmen, Organisationen und Bürgerinnen und Bürger. Insbesondere Phishing-Mails, mit denen Zugangsdaten oder ganze Identitäten gestohlen werden sollen, sind ein weithin genutztes Angriffsmittel. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nun die Technische Richtlinie E-Mail-Authentifizierung (TR-03182) veröffentlicht, die E-Mail-Service-Providern eine Richtschnur im Vorgehen gegen Phishing und Spoofing, also das Fälschen des Absendernamens, zur Verfügung stellt. Die Maßnahmen müssen ausschließlich durch die jeweiligen Diensteanbieter umgesetzt werden, die ihre Kundinnen und Kunden damit aktiv schützen können.

Die TR-03182 formuliert Maßnahmen, mit denen Inhalt und Absender einer E-Mail authentifiziert werden können. So wird mit Hilfe des Standards SPF (Sender Policy Framework) die grundsätzliche Berechtigung zum Senden von E-Mails im Auftrag einer bestimmten Domain geprüft. Der ebenfalls in der Technischen Richtlinie geforderte Standard DKIM Domain Key Identified Mail (Domain Key Identified Mail) bindet jede gesendete E-Mail kryptographisch an die Domain. Damit wird die bereits etablierte TR-03108 (Si-

cherer E-Mail-Transport), die sich auf den sicheren E-Mail-Transport von Punkt zu Punkt bezieht, fachlich und technisch ergänzt. So können Mail-Anbieter ihre Kundinnen und Kunden vor Identitätsmissbrauch (Spoofing und Phishing) und unberechtigtem Mitlesen und Manipulation (Man-in-the-middle-Angriffen) schützen. Selbst neu entdeckte Angriffsmethoden wie das SMTP-Smuggling werden durch das Umsetzen der Maßnahmen erschwert.

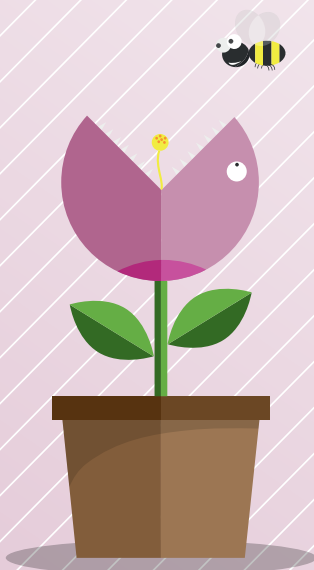
Große Mail-Anbieter haben bereits angekündigt, für das massenhafte Zustellen von E-Mails künftig Mechanismen zur E-Mail-Authentifizierung zu fordern. Die TR-03182 berücksichtigt diese geforderten Technologien bereits.

[www.bsi.bund.de](http://www.bsi.bund.de)

### SIMPLE MAIL TRANSFER PROTOCOL (SMTP) SMUGGLING

Beim SMTP Smuggling machen sich die Angreifenden zunutze, dass verschiedene SMTP-Implementierungen die Kennzeichnung des Endes einer E-Mail-Nachricht unterschiedlich interpretieren. Sie können so E-Mails versenden, die durch ein betroffenes E-Mail-System in mehrere E-Mails aufgespalten werden. Auf diesem Weg entstehen neue E-Mails, die gefälschte Absender nutzen (Spoofing), Authentifizierungsmechanismen, wie SPF, DKIM und DMARC umgehen oder Warnungen, wie zum Beispiel eine Spam-Markierung in der Betreffzeile, nicht mehr tragen.

Durch die Ausnutzung von Unterschieden in der Interpretation einer Sequenz zwischen ausgehenden und eingehenden SMTP-Servern können Angreifende gefälschte E-Mails im Namen vertrauenswürdiger Domänen versenden. Dies ermöglicht wiederum verschiedenste Social Engineering- oder Phishing-Angriffe.







# CYBERRESILIENZ

## AUCH EIN SOC BRAUCHT HILFE

Positiv ausgedrückt: Cyberresilienz ist eine vielseitige Aufgabe. Negativ ausgedrückt: eine sehr komplexe, für die kaum ein Unternehmen über die notwendigen Ressourcen verfügt. Selbst Unternehmen mit einem eigenen IT-Team oder einem internen Security Operation Center (SOC) sind dafür oft zu schwach aufgestellt. Für wirksame Sicherheit benötigen auch sie einerseits eine geeignete Plattformtechnologie. Andererseits bedarf es einer neuen Qualität der Zusammenarbeit in der Organisation. Und nicht zuletzt früher oder später der Hilfe von außen.

Ein wirksamer Schutz gegen die komplexer und professioneller werdenden Cyberangriffe benötigt eine umfassende Gefahrenerkennung basierend auf einer die gesamte IT-Infrastruktur umfassenden Visibilität. Entscheidend sind dabei ebenso die Flexibilität und das Wissen des verantwortlichen Teams, um Anwendungssicherheit, Netzwerkbetrieb und Infrastrukturarchitektur zu gewährleisten. Die neuen Kriterien für eine resiliente IT-Sicherheit definieren traditionelle IT-Rollen neu und erzwingen das Aufbre-

chen alter Silos: Das SOC braucht die Hilfe der operativen IT. Eine effektive Zusammenarbeit aller Beteiligten innerhalb des Unternehmens basiert auf den folgenden Elementen:

### Teamarbeit für die Risikoanalyse

Um die wertvollsten digitalen Assets des Unternehmens mit deren individueller Priorität effektiv zu schützen, muss man diese zunächst einmal kennen. Gleichzeitig muss man wissen, wie Mitarbeiter diese zur Erreichung der Unternehmensziele nutzen. Um Assets richtig zu priorisieren, benötigen IT-Sicherheitsbeauftragte zudem Informationen zu Anwendungen im Unternehmen und zur Netzwerkinfrastruktur. Nur durch regelmäßigen Austausch mit allen Beteiligten schaffen IT-Sicherheitsverantwortliche und IT-Teams die Informationsgrundlage, Abwehrmaßnahmen richtig zu priorisieren und Sicherheitsressourcen effizient und optimiert einzusetzen.

### Ressourcen optimal einsetzen und einholen

Um die vorhandenen Mittel richtig einzusetzen, kommt es auf die richtigen

Tools, effiziente Prozesse und den richtigen Mix an qualifizierten Mitarbeitern an. Die gegebenenfalls notwendigen zusätzlichen Fachkenntnisse – zum Beispiel für Cloud-Migration oder Cloud-Security – können über externe Spezialisten in der Regel problemlos auch temporär erworben werden. Nur wenige Unternehmen sind in der Lage, ausreichend große und dezidierte Security-Teams mit den nötigen Skills aufbauen und halten zu können. Auch sie können von externen SOC und deren Sicherheitsanalysten, die durch spezielle Kenntnis globaler, geographischer und branchenspezifischer Telemetriedaten zusätzliche Expertise und Kompetenz bereitstellen, profitieren. Ein Managed Detection and Response-Service (MDR) bietet zudem die Möglichkeit, ein unternehmenseigenes SOC zu ergänzen, wenn dort entsprechende Skills und oder Tools nicht bereitstehen.

So können Unternehmen jeder Art und Größe die optimalen Dienste nutzen.

Jörg von der Heydt  
[www.bitdefender.de](http://www.bitdefender.de)



# Digitale Identitäten in Deutschland und Europa

WO STEHEN WIR HEUTE WIRKLICH UND WIE SIEHT DIE NAHE ZUKUNFT AUS?

Identitätsnachweise sind im Alltag allgegenwärtig, vom Personalausweis über Mitarbeiter- bis hin zu Studentenausweisen. So unterschiedlich die einzelnen Ausweise gestaltet sind, sollen sie alle einen Zweck erfüllen: die Identität einer spezifischen Person in einem bestimmten Zusammenhang nachweisen. Doch in einer Welt, in der Interaktionen immer stärker digital stattfinden, wird das zunehmend zu einer Herausforderung – denn Nachweise sind heutzutage noch immer vorrangig physischer Natur.

Um die physischen Ausweise auch in digitalen Vorgängen zu nutzen, müssen diese zunächst „digitalisiert“ werden. Teilweise reicht bereits ein einfaches Foto oder Scan des Nachweises. Für die Eröffnung eines neuen Bankkontos hingegen ist ein Videoident-Verfahren notwendig. Für Nutzer und die prüfende Partei sind die Prozesse zumeist aufwändig und kostspielig. Gleichzeitig bergen sie diverse Sicherheitsrisiken, da viele Sicherheitsmerkmale der physischen Dokumente beim „Digitalisieren“ nur noch eingeschränkt funktionieren. Die Idee der digitalen Identitäten schließt diese Lücke.

## Vertrauensbeziehungen als Basis für digitale Identitäten

Nachweise werden direkt in digitaler Form in eine Wallet (zum Beispiel als Smartphone-App) ausgestellt, dort vom Nutzer eigenständig gehalten und verwaltet. Nutzer können aus der Wallet heraus die Nachweise einer prüfenden Partei (Verifier) vorzeigen. Die Anfrage für das Teilen dieses digitalen Nachweises kann beispielsweise über einen QR-Code vom Verifier kommen. Dieser wird direkt mit der Wallet gescannt, der Nutzer entscheidet dann eigenständig über die zu teilenden Daten.

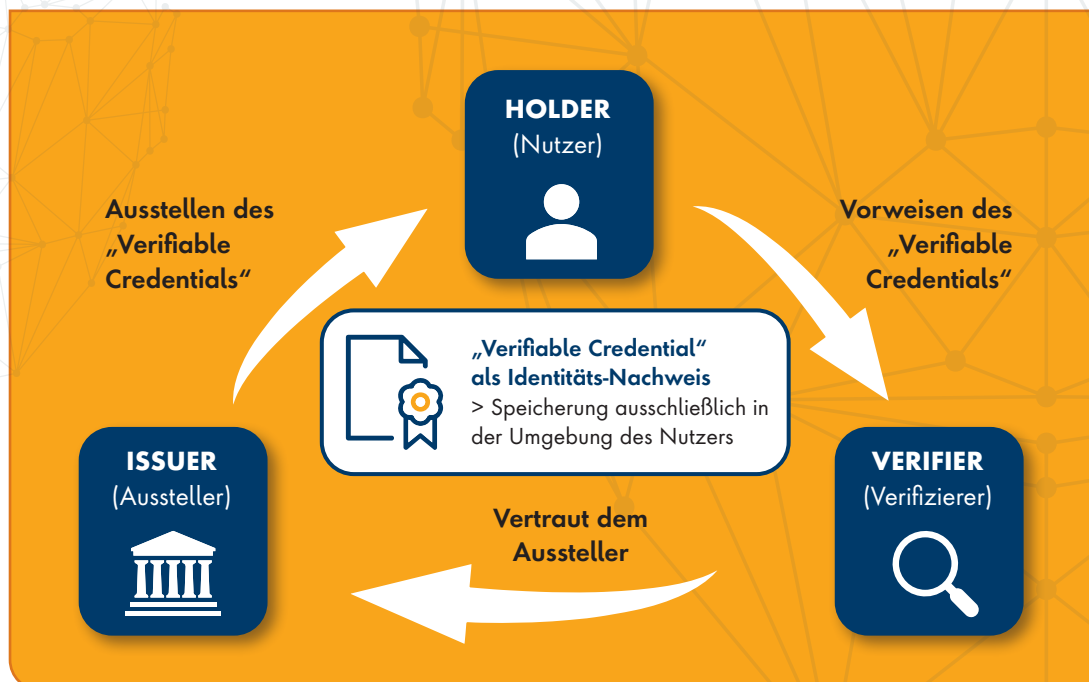


Bild 1: Rollen und Vertrauensverhältnisse für selbstbestimmte Identitäten



Digitale Identitätsnachweise sind nur als authentisch zu betrachten, wenn der Aussteller (Issuer) bekannt und vertrauenswürdig ist. Darüber hinaus möchten Nutzer auch wissen, mit wem sie ihre Identitätsdaten teilen, also wer genau der Verifier ist (Bild 1). Verifizierbare Vertrauensregister sollen hier helfen, Organisationen als seriöse Akteure in der Identitätsinfrastruktur auszuweisen. Ein Ansatz für die Umsetzung eines solchen Registers ist die Blockchain-Technologie als Basis. Dort werden Aussteller von Identitätsdaten in Issuer Registries und Empfänger von Identitätsdaten in Verifier Registries bekannt gemacht

(Bild 2). Sogenannte Widerrufsregister (Revocation Registries) dienen dazu, die Validität von einmal an den Nutzer ausgestellten Identitätsnachweisen zu widerrufen, auch wenn der Nachweis das Ablaufdatum noch nicht erreicht hat. Durch den dezentralen Ansatz können die Issuer und Verifier unmittelbar auf die dort abgelegten Informationen im Ökosystem zugreifen. Aufgrund der nachträglichen Unveränderlichkeit und der eindeutigen Zuordnung der dort abgelegten Daten eignet sich die Blockchain-Technologie für Registerimplementierungen besonders gut.

Die Dezentralisierung der Infrastruktur führt jedoch zu einer komplexen Governance: Die verschiedenen Teilnehmer



”  
IDENTITY WALLETS  
KÖNNEN DIE VERANT-  
WORTUNG FÜR UND  
KONTROLLE ÜBER DIE  
EIGENEN IDENTITÄTS-  
DATEN VON EXTERNEN  
ANBIETERN ZUM NUTZER  
SELBST VERLAGERN.

Alessandro Benke, IT-Architekt,  
Accenture GmbH,  
[www.accenture.com/de-de](http://www.accenture.com/de-de)

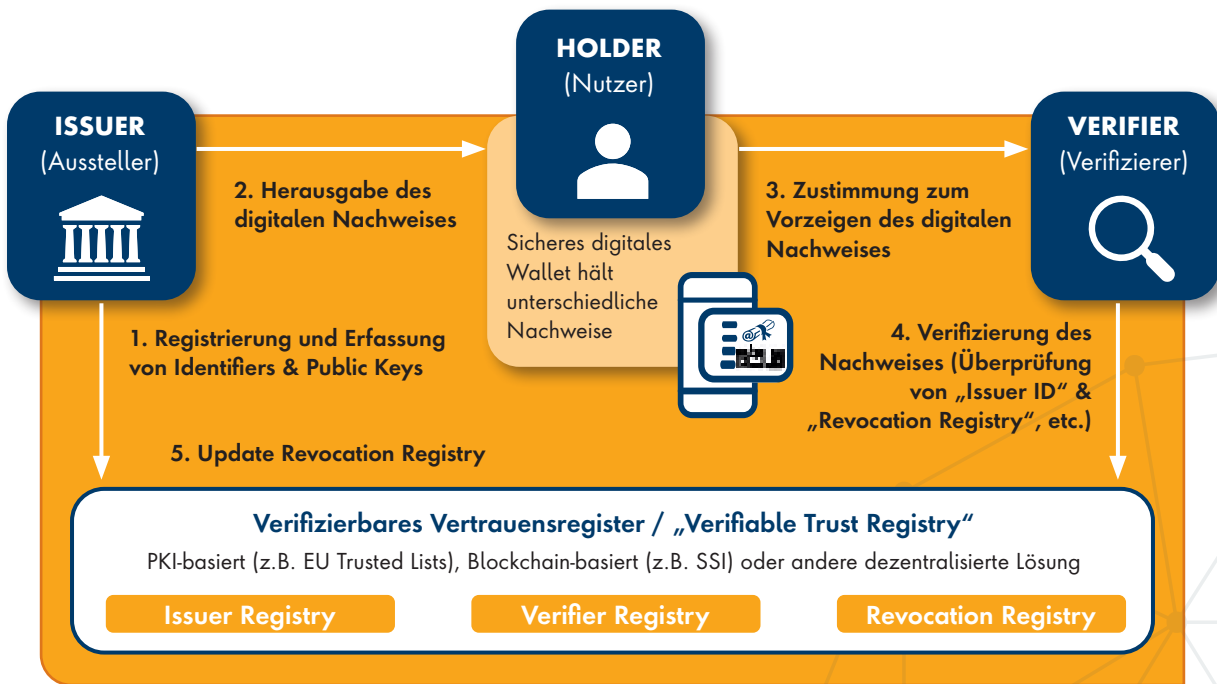


Bild 2: Ökosystem inklusive Vertrauensregister

nehmen unterschiedliche Rollen ein und verfügen über bestimmte Berechtigungen. Der Betrieb der Infrastruktur muss in einem Betreibermodell spezifiziert werden, das unter allen Beteiligten Zustimmung findet. Im Gegensatz zu Blockchain-basierten Ansätzen gestaltet sich die Governance-Problematik bei zentralisierten Lösungen oft einfacher. Grund dafür ist die von Beginn an klar geregelte Rollenverteilung sowie die zentral bereitgestellte und betriebene Infrastruktur. Weitere Akteure im Netzwerk treten zumeist als Nutzer, nicht jedoch als Betreiber der Vertrauensinfrastruktur selbst auf.

Zuletzt vereinfacht dieser Ansatz oftmals die Umsetzung regulatorischer Vorgaben und gewinnt darüber das benötigte Vertrauen. Instanzen wie beispielsweise die Europäische Kommission stellen in sogenannten Trusted Lists Berechtigungsinformationen zu Issuern und Verifiern bereit. Trusted Lists enthalten identifizierende Informationen zu

den agierenden Institutionen wie zum Beispiel Namen und kryptografische Schlüsselinformationen.

### Öffentliche Verwaltung und Privatwirtschaft

Die Europäische Kommission möchte digitale Identitäten nicht nur jedem EU-Bürger verbindlich zur Verfügung stellen, etwa für den digitalen „Gang“ zum Bürgeramt, sondern auch eine standardisierte und europaweit interoperable Infrastruktur schaffen. Konkret sollen deutsche Nachweise auch in allen anderen EU-Ländern funktionieren und umgekehrt. Hierzu befindet sich eine entsprechende Verordnung, die eIDAS-2.0, in der Finalisierung und Verabschiedung (Stand Dezember 2023). Die Version 1.0 regelt die eID ausführlich. Diese soll um digitale, meist Wallet-basierte, Identitäten im weitesten Sinne erweitert werden. Sobald die Verordnung in Kraft getreten ist, haben die Mitgliedsstaaten 24 Monate Zeit, ihren Bürgern einen verbindlich kostenfreien Zugang zu digitalen Identitäten wie etwa dem digitalen Personalausweis oder Führerschein zu verschaffen. Das wird voraussichtlich Ende 2026 der Fall sein.

Um die Umsetzung weiter zu unterstützen, stellt die EU technische Leitlinien zur Umsetzung im Architecture and Reference Framework bereit. Dies umfasst unter anderem Spezifikationen für Schnittstellen und Protokolle zum Datenaustausch, die oben beschriebenen Vertrauensregister und Sicherheitsstandards. Eine Referenzimplementierung, sprich eine Art „Beispiel-Wallet“ soll als Basis für die Entwicklung der nationalen Infrastruktur dienen. Zudem wurde Budget für vier Large Scale Pilot Konsortien (LSP) bereitgestellt. Ziel dieser ist die Entwicklung und Pilotierung mehrerer Anwendungsfälle in Zusammenarbeit zwischen der öffentlichen Verwaltung und Privatwirtschaft.

Die LSPs sind bereits Mitte 2023 gestartet und laufen über einen Zeitraum von zwei Jahren, mit dem Ziel bis Ende 2024 einen ersten Pilotbetrieb zu erreichen. Das größte der Konsortien, Potential, wird von der französischen ANTS und dem deutschen BMI geführt. Die Anwendungsfälle konzentrieren sich unter anderem auf den digitalen Führer-



schein (mDL) und den digitalen Personalausweis (PID) zur Identifizierung und Authentifizierung von Bürgern für Onlineverwaltungsdienstleistungen oder die Eröffnung von Bankkonten. Ebenfalls verprobt werden digitale Signaturen. Die weiteren Konsortien DC4EU, NOBID und EWC konzentrieren sich beispielsweise auf eine digitale Gesundheitskarte, digitale Bildungsnachweise, Identitätsnachweise für Organisationen und das Reisen sowie Wallet-basierte Zahlungen ohne Kreditkartennutzung.

### Wo stehen digitale Identitäten in Deutschland?

Vor fast vierzehn Jahren hat Deutschland den Personalausweis im Scheckkartenformat mit Onlineausweisfunktion eingeführt. Ein im Personalausweis eingebauter NFC-Chip speichert die hinterlegten Daten und ermöglicht über kryptografisches Schlüsselmateriel nicht nur eine sichere Verbindung zum „deutschen eID-System“, sondern verifiziert auch die Daten. Die Freigabe durch den Nutzer erfolgt mittels PIN-Code.

Ein erster Schritt in Richtung digitaler Identität, doch der große Erfolg der Online-Ausweisfunktion blieb aus. Die Gründe dafür sind vielfältig: Anfänglich gestaltete sich die Nutzbarkeit und Adaption schwierig, da ein separates Kartenlesegerät erforderlich war, während es gleichzeitig an einem flächendeckenden Angebot an Diensteanbietern, die die eID-Funktion als Authentifizierungsoption anbieten, fehlte. Mittlerweile können Bürger die Onlineausweisfunktion über die Ausweisapp Bund und die NFC-Schnittstelle des Smartphones nutzen, auch die Nutzerführung wurde verbessert und ließen die Nutzerzahlen steigen. In Summe liegen diese jedoch weiterhin hinter den Erwartungen zurück.



DIGITALE IDENTITÄTEN  
SIND DER SCHLÜSSEL  
ZU MEDIENBRUCHFREIEN  
DIGITALEN PROZESSEN  
IN DER VERWALTUNG  
UND PRIVATWIRTSCHAFT.

Nicklas Urban, Senior IT-Architekt,  
Accenture GmbH,  
[www.accenture.com/de-de](http://www.accenture.com/de-de)

Mit der Smart eID, die sich bereits seit mehreren Jahren in der Entwicklung befindet, will Deutschland eine digitale Version des Personalausweises schaffen. Ziel ist die Speicherung der Personalausweisdaten direkt auf dem Endgerät des Benutzers. Um jedoch weiterhin das Vertrauensniveau hoch zu halten, genügt eine software-technisch verschlüsselte Speicherung der Daten direkt auf dem Endgerät des Nutzers nicht. Vielmehr ist eine zusätzliche Absicherung auf Hardware-Basis erforderlich. Dies kann etwa über die eSIM oder ein embedded Secure Element (eSE) erfolgen – einer vom übrigen Speicher physisch eigenständige, gesicherte Speichereinheit. Die große Herausforderung ist jedoch die noch recht geringe Verbreitung dieser Optionen in den derzeit genutzten Smartphones auf dem deutschen Markt. Hinzu kommt die nötige Zusammenarbeit mit den Herstellern, um Zugriff auf diese Komponenten zu erhalten, insbesondere in Bezug auf das eSE. Mit Samsung gibt es bereits eine Kooperation für die Pilotphase. Der geplante Golive wurde im Dezember 2023 jedoch vorerst auf un-

bestimmte Zeit verschoben, der Pilotbetrieb eingestellt.

### Ausblick

Als Basis für die LSP-Teilnahme Deutschlands wird unter Leitung des BMI im nationalen „Wallet Projekt“ gegenwärtig eine Smartphone-Wallet für Bürger entwickelt, die schrittweise alle in Deutschland geplanten Anwendungsfälle abdecken soll. Auch wenn bereits 2024 mit ersten Tests gerechnet wird, werden Bürger die Wallet im App-Store erst voraussichtlich im Laufe des Jahres 2026 vorfinden – parallel zur Umsetzungsfrist aus der eIDAS 2.0 Verordnung.

Welche Funktionen diese Wallet dann genau unterstützen wird, ist gegenwärtig noch offen. Doch der Fokus liegt auf den Anwendungen, die das Potential Konsortium testet: PID, mDL und digitale Signatur. Die Integration der Anwendungsfälle der weiteren deutschen Beteiligungen in den anderen Konsortien ist derzeit im Gespräch. Interessierte Bürger können die Entwicklung öffentlich verfolgen. Das BMI hat dafür eine Seite auf OpenCode erstellt, auf der sie sowohl Updates zur technischen Umsetzung, den Anwendungsfällen als auch den potentiellen Geschäfts- und Betreibermodellen teilen.

Zusammenfassend gesagt, es ist sowohl in Deutschland als auch der EU derzeit viel in Bewegung, um digitale Identitäten zum Leben zu erwecken. Allerdings liegt noch ein langer Weg vor uns.

**Nicklas Urban, Alessandro Benke**



# Digitale Identitäten im Wandel

SICHERHEIT UND AUTONOMIE IN DER VERNETZTEN WELT

– TEIL 1 VON 2 –

Im digitalen Zeitalter sind Identitäten weit mehr als Benutzernamen und Passwörter. Sie fungieren als zentrale Schlüssel zu einer Vielzahl von Aktivitäten: von persönlichen und beruflichen Interaktionen bis hin zu finanziellen Transaktionen und dem Zugang zu diversen Online-Services. Für Nutzer ist es entscheidend, ihre Identität vor Missbrauch zu schützen, um finanzielle Verluste oder rechtliche Konsequenzen zu vermeiden. Ebenso ist es für Dienstanbieter essenziell, nur autorisierten Personen Zugriff zu gewähren, um keine rechtlichen Risiken einzugehen und die Integrität ihrer Services zu wahren. In diesem Kontext ist die Si-

cherheit digitaler Identitäten nicht nur eine technische Herausforderung, sondern auch ein zentraler Bestandteil des Vertrauens und der Zuverlässigkeit in die digitale Welt.

In traditionellen Systemen des Identitätsmanagements spielen Identity Provider (IDPs) eine essenzielle Rolle. Diese gewährleisten Sicherheit, hauptsächlich durch Authentifizierungsmethoden wie Benutzernamen und Passwörter, ergänzt durch Mehrfaktor-Authentifizierungen, wie SMS- oder E-Mail-TANs und zeitbasierte Einmalpasswörter (TOTP). Wenn Nutzer auf Dienste zugreifen möchten, erfolgt die Authentifizierung über einen vom Dienstleister ausgewählten oder anerkannten IDP mithilfe der genannten Methoden. Um Identitätsdaten sicher über verschiedene Domänen hinweg zu übertragen, kommen Standards wie Security Assertion Markup Language (SAML), OAuth und OpenID Connect (OIDC) zum Einsatz. Diese werden mittels HTTPS-Protokollen übermittelt, um einen hohen Grad an Datensicherheit zu gewährleisten und gegen Angriffe von außen zu schützen.

## Direkte Hostings vs. förderierte Systeme

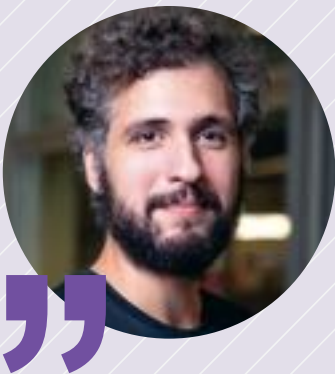
Das Vertrauensverhältnis zwischen Dienstleistern und IDPs ist ebenfalls von zentraler Bedeutung im Identitätsmanagement. Dieses Vertrauen kann entweder auf einer direkten Hosting-Beziehung basieren, wie es häufig bei Dienst Anbietern im Bereich des Online-Bankings der Fall ist, oder auf förderierten Systemen. Bei direkt gehosteten Systemen werden die Identitätsdaten und

Authentifizierungsprozesse in der Umgebung des Dienstanbieters verwaltet, was eine hohe Sicherheit und Kontrolle ermöglicht. Im Gegensatz dazu erlauben förderierte Systeme, wie die Login-Optionen über Facebook oder Google, den Nutzern den Zugriff auf verschiedene Dienste unter Verwendung ihrer digitalen Identitäten von einem oder mehreren IDPs. Solche förderierten Lösungen bieten den Vorteil der Benutzerfreundlichkeit und Komfort. Sie ermöglichen es, mehrere Dienste mit einer einzigen, vertrauenswürdigen Identität zu nutzen, während sie gleichzeitig die Sicherheit durch standardisierte Authentifizierungsprotokolle und Policy-Regeln der Föderation gewährleisten.

## Mehr Autonomie für Nutzer

Neue Ansätze des Identitätsmanagements, wie selbstbestimmte Identitäten, unterscheiden sich von traditionellen Ansätzen durch die Art und Weise, wie die Identitätsdaten verwaltet und genutzt werden. Bei selbstbestimmten Identitäten wird die Speicherung und Verwaltung der Identitätsdaten in die Umgebung des Endnutzers verlagert, oft in einer Wallet-App auf dem Smartphone. Der Nutzer authentifiziert sich und teilt die Identitätsdaten direkt mit der prüfenden Partei (Verifier), ohne dass ein zentraler IDP die Authentifizierung steuert oder infolgedessen die Identitätsdaten ermittelt.

Eine zentrale Komponente in diesem System ist die Rolle der ausstellenden Partei



IM DIGITALEN ZEITALTER SIND IDENTITÄTEN WEIT MEHR ALS BENUTZER-NAMEN UND PASSWÖRTER: SIE FUNGIEREN ALS ZENTRALE SCHLÜSSEL ZU EINER VIELZAHL VON AKTIVITÄTEN.

Hakan Yildiz,  
IT Architekt, Accenture GmbH,  
[www.accenture.com](http://www.accenture.com)



(Issuer). Im Gegensatz zu traditionellen IDPs, die umfangreiche Verantwortung für die Verwaltung und Sicherheit der Identitätsdaten tragen, ist die Hauptaufgabe des Issuers in selbstbestimmten Identitätssystemen auf die Ausstellung der Identitätsdaten beschränkt. Der Issuer stellt bestimmte Identitätsattribute als Verifiable Credentials (VCs) aus, ohne jedoch die vollständige Kontrolle über die Verwendung und Speicherung dieser Informationen zu haben. Dies verlagert die Verantwortung und Kontrolle hin zu den Nutzern, die ihre digitalen Identitäten und die damit verbundenen Daten eigenständig verwalten.

Aufgrund der Verwaltung und Speicherung der VCs in der Domäne des Endnutzers gibt es im Gegensatz zu traditionellen Ansätzen für den Issuer keine Möglichkeit, bereits ausgestellte VCs direkt zu editieren, um sie beispielsweise im Fall des Verlusts zu sperren. Um dem zu entgehen, können VCs einen Verweis enthalten, der auf ein vom Issuer editierbares Widerrufsregister (Englisch: Revocation Registry) zeigt. Sollte

die Notwendigkeit entstehen, ein VC zu widerrufen, kann der Aussteller dies im Register vermerken. Während des Verifizierungsprozesses kann der Verifier dieses Register überprüfen, um die aktuelle Gültigkeit unabhängig vom Ablaufdatum des VCs zu bestätigen.

Beim Ansatz von selbstbestimmten Identitäten interagieren die Nutzer direkt mit dem Verifier, der einen Dienst anbietet. Durch die direkte Speicherung und Verwaltung ihrer VCs auf dem eigenen Gerät können Nutzer entscheiden, welche Informationen sie für jeden spezifischen Kontext freigeben möchten. Diese Art des Identitätsmanagements ermöglicht somit eine personalisierte und direkte Interaktion zwischen Nutzern und Diensten.

### **Sicherheitsmechanismen**

Durch selbstbestimmte Identitäten ergeben sich zahlreiche sicherheitstechnische Fragen, die es zu adressieren gilt. Eine zentrale Frage ist, wie die vorgelegten VCs ihre Authentizität gegenüber dem Verifier glaubhaft darlegen

können. Ebenso wichtig ist es, digitale Angriffsvektoren wirksam zu mindern. Darüber hinaus stellt sich die Frage, wie Sicherheits-Best-Practices und -features physische Risiken abmildern können – wie den Verlust des Smartphones, auf dem die digitalen Identitäten gespeichert sind.

**Hakan Yildiz**

.....

## **VORSCHAU**

Der zweite Teil dieses Artikels wird sich intensiv mit den Sicherheitsaspekten selbstbestimmter Identitäten auseinandersetzen und beleuchten, wie diese Herausforderungen in der Praxis bewältigt werden können. Wie müssen Technologie, Prozesse und Richtlinien zusammenspielen, um ein robustes und vertrauenswürdiges Umfeld für die Verwaltung digitaler Identitäten zu schaffen und dabei gleichzeitig die Sicherheit und Autonomie der Nutzer zu wahren?





In der heutigen schnelllebigen und zunehmend digitalisierten Welt stehen Unternehmen vor einer beispiellosen Anzahl von Sicherheitsherausforderungen.

Cyberangriffe werden immer ausgefeilter, und die Notwendigkeit, auf Sicherheitsvorfälle schnell und effizient zu reagieren, war nie größer. Hier kommt SOAR (Security Orchestration, Automation and Response) ins Spiel, ein Ansatz, der darauf abzielt, die Reaktion auf Sicherheitsvorfälle zu optimieren, indem er Automatisierung, Orchestrierung und eine Vielzahl von Sicherheitstools in einer einzigen, kohärenten Lösung vereint.

#### Was ist SOAR?

SOAR bezeichnet eine Sammlung von Softwarelösungen und Tools, die zur Vereinfachung der Sicherheitsverwaltung und -reaktion entwickelt wurden. Diese Plattformen kombinieren drei Schlüsselemente: Sicherheitsorchestrierung, Automatisierung und Reaktion. Sie ermöglichen es Sicherheitsteams,

Alarme effizienter zu verwalten, Prozesse zu automatisieren und schneller auf Vorfälle zu reagieren.

Die wesentlichen Vorteile sind:

♦ **Effizienzsteigerung:** Durch Automatisierung wiederkehrender Aufgaben reduziert SOAR die Belastung für Sicherheitsteams.

♦ **Verbesserte Reaktionszeit:** SOAR ermöglicht eine schnellere Erkennung und Reaktion auf Sicherheitsvorfälle.

♦ **Bessere Entscheidungsfindung:** Mit umfassenden Informationen und Analysetools können Teams fundiertere Entscheidungen treffen.

♦ **Integration verschiedener Tools:** SOAR ermöglicht die Integration verschiedener Sicherheitstools und -plattformen, was zu einer umfassenderen Sicherheitsstrategie führt.

#### SOAR-Methoden

Die Methoden von SOAR umfassen folgende Aspekte:

♦ **Automatisierte Reaktion auf Vorfälle:** Eine effiziente SOAR-Lösung überwacht Sicherheitswarnungen und setzt automatisierte Werkzeuge ein, um diese abzuwehren.

♦ **Orchestrierung:** Die Tools arbeiten vernetzt und interagieren gemeinsam. Wichtig ist die Kompatibilität dieser Integrationen mit der bestehenden Umgebung.

♦ **Threat Intelligence:** Viele SOAR-Plattformen nutzen Threat Intelligence, um kontextbezogene Daten über potenzielle Bedrohungen zu sammeln, was Sicherheitsteams bei der Entscheidungsfindung unterstützt.

♦ **Zuverlässiges Incidentmanagement:** Vorfälle werden zentral dokumentiert, verwaltet und untersucht, um sowohl bekannte als auch unbekannte Bedro-



hungen zu erkennen und zu bewältigen.

♦ **Playbook-Automatisierung:** Bei der Auswahl einer SOAR-Lösung ist es wichtig, dass mehrere Playbooks erstellt und auf vorgefertigte sowie eigene Workflows zugegriffen werden kann.

♦ **Skalierbare, flexible Infrastruktur:** Wählen Sie eine Lösung, die sich an technologische Entwicklungen anpassen und bedarfsgerecht skalieren lässt.

### Wie funktioniert SOAR?

Diese Lösungen nutzen Daten aus verschiedenen Quellen, um Sicherheitsalarme zu identifizieren und zu priorisieren. Durch die Automatisierung bestimmter Aufgaben können die Systeme auf Vorfälle reagieren, ohne dass menschliches Eingreifen erforderlich ist. Weiterhin ermöglichen sie die Orchestrierung verschiedener Sicherheitstools und -prozesse, um eine effektive und koordinierte Reaktion zu gewährleisten.

### Anwendungsbeispiele

Die Frage, die sich nun stellt ist die, wo sich geeignete Anwendungsfelder finden. Dazu zählen unter anderem:



**SOAR- UND SIEM-SYSTEME ARBEITEN HAND IN HAND, ERGÄNZEN SICH ALSO, UM EIN UMFASSENDES SICHERHEITSMANAGEMENT ZU ERMÖGLICHEN.**

Ulrich Parthier, Publisher it security,  
[www.it-daily.net](http://www.it-daily.net)

♦ **Automatische Reaktion auf Phishing-Versuche:** Erkennen und isolieren von Phishing-Attacken, bevor sie Schaden anrichten können.

♦ **Streamlining Incident Response:** Vereinheitlichung und Koordination von Reaktionen auf Sicherheitsvorfälle.

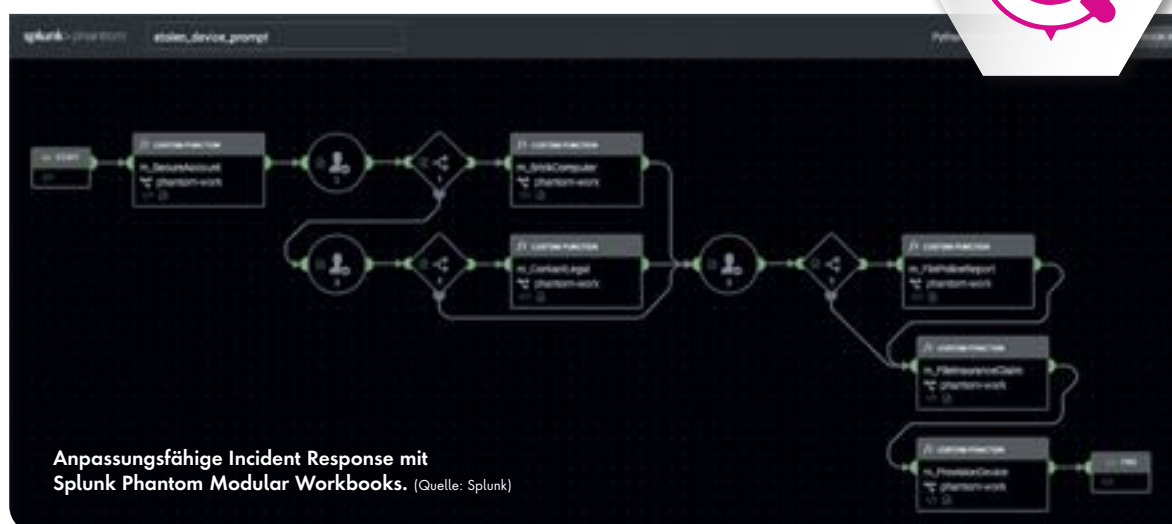
♦ **Bedrohungszintelligenz und Analyse:** Sammeln und Analysieren von Daten aus verschiedenen Quellen zur Erkennung komplexer Bedrohungen.

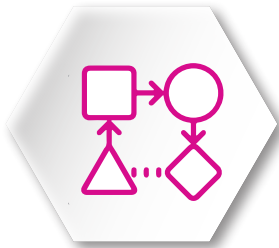
Zum Thema SOAR haben wir bereits mehrfach Artikel auf unserer Plattform [www.it-daily.net](http://www.it-daily.net) veröffentlicht. So etwa über ThreatQuotient. Dort wurde

ein datengesteuerter Ansatz für SOAR und XDR vorgestellt. Hierbei konzentriert sich die Automatisierung nicht nur auf Prozesse, sondern auf Daten. Die Automatisierung in drei Stufen – Initiate, Run, Learn – ermöglicht es, Aktionen basierend auf Datenrelevanz zu steuern. Der ThreatQ TDR Orchestrator von ThreatQuotient nutzt Smart Collections und datengesteuerte Playbooks für effizientere Automatisierungsprozesse. Anwendungsfälle beinhalten unter anderem Threat Hunting, Bereitstellen von Blockier- und Erkennungsinhalten sowie Anreicherung von Threat Intelligence. Dieser Ansatz soll die Effizienz erhöhen und Playbook-Läufe reduzieren.

### SIEM und SOAR: Entweder oder?

Oft stellt sich die Frage: wenn ich schon ein SIEM habe, wozu benötige ich dann SOAR? SIEM-Systeme sind primär darauf ausgerichtet, Daten aus verschiedenen Quellen zu sammeln und zu analysieren, um potenzielle Sicherheitsvorfälle zu erkennen. Sie dienen der Protokollierung, Überwachung und Analyse von Sicherheitsdaten.





SOAR-Systeme hingegen konzentrieren sich auf die Automatisierung der Reaktion auf Sicherheitsvorfälle, die von SIEM-Systemen und anderen Quellen erkannt wurden. Sie ermöglichen die Orchestrierung verschiedener Sicherheitstools, automatisieren wiederkehrende Prozesse und unterstützen Security Analysten bei der effizienten Verarbeitung und Reaktion auf Vorfälle.

SOAR- und SIEM-Systeme arbeiten Hand in Hand, ergänzen sich also, um ein umfassendes Sicherheitsmanagement zu ermöglichen. Während SIEM-Systeme für die Erkennung und Alarmierung zuständig sind, übernimmt SOAR die automatisierte Verarbeitung dieser Alarme und unterstützt bei der Durchführung von Schutzmaßnahmen und der Dokumentation von Sicherheitsvorfällen.

### Schlussfolgerung

SOAR repräsentiert eine signifikante Weiterentwicklung in der Welt der Cybersicherheit. Durch die Kombination von Automatisierung, Orchestrierung und fortschrittlichen Analysefunktionen bietet SOAR Unternehmen die Möglichkeit, ihre Sicherheitsposturen zu stärken und effizienter auf die ständig wechselnden Bedrohungslandschaften zu reagieren. Während SOAR nicht alle Sicherheitsherausforderungen lösen kann, stellt es einen wesentlichen Schritt in Richtung intelligenterer und reaktionsfähigerer Sicherheitsoperationen dar.

**Fazit:** SOAR stellt nicht nur eine technologische Innovation dar, sondern auch einen Paradigmenwechsel in der Art

## EINIGE DER BEKANNTESTEN SOAR-PRODUKTE SIND:

- **Splunk Phantom:** bietet fortschrittliche Automatisierungs- und Orchestrierungsfunktionen.
- **IBM Security Radar SOAR (früher Resilient):** ist eine SOAR-Lösung, die sich auf Incident Response und Fallmanagement konzentriert. Es bietet umfangreiche Möglichkeiten zur Anpassung und Integration in bestehende Sicherheitssysteme und unterstützt Unternehmen bei der schnellen und effektiven Reaktion auf Vorfälle.
- **Cisco SecureX:** ist eine Sicherheitsplattform, die SOAR-Funktionalitäten in Ciscos umfangreiches Produktportfolio integriert. Es bietet eine vereinheitlichte Sicht auf Sicherheitsdaten über verschiedene Produkte hinweg und unterstützt die Automatisierung von Sicherheitsprozessen.
- **Chronicle Security Operations (früher Siemplify):** bietet eine cloud-basierte SOAR-Lösung, die besonders für ihre benutzerfreundliche Oberfläche und die Fähigkeit zur effizienten Verwaltung von Sicherheitsvorfällen bekannt ist. Es ermöglicht die Integration einer Vielzahl von Sicherheitstools und bietet fortschrittliche Analysefunktionen.
- **Fortinet FortiSOAR (früher bekannt als CyberSponse):** ist ein Teil von Fortinets breiterem Cybersecurity-Portfolio. Es bietet umfassende Automatisierungs- und Orchestrierungsfunktionen, die es Organisationen ermöglichen, komplexe Sicherheitsworkflows zu vereinfachen und zu beschleunigen.
- **Rapid7 InsightConnect:** Diese Plattform konzentriert sich auf die Automatisierung von Sicherheitsaufgaben und die Integration von Sicherheitstools, um die Effizienz der Sicherheitsteams zu verbessern. InsightConnect ist bekannt für seine Anpassungsfähigkeit und Benutzerfreundlichkeit.
- **Palo Alto Networks Cortex XSOAR (früher Demisto):** Cortex XSOAR bietet eine umfassende SOAR-Lösung mit starken Funktionen zur Automatisierung, Orchestrierung und Reaktion. Es unterstützt auch die Erstellung und das Management von Playbooks, um die Reaktion auf Sicherheitsvorfälle zu standardisieren.

und Weise, wie Unternehmen ihre Sicherheitsstrategien angehen. In einer Zeit, in der Cyber-Bedrohungen immer raffinierter und schädlicher werden, bietet SOAR eine weitere Option im Arsenal der Cybersicherheit.

**Ulrich Parthier**





# Cyberkriminelle überall da tut Hilfe not



Mehr Infos dazu im Printmagazin

**itsecurity**

und online auf [www.it-daily.net](http://www.it-daily.net)

# Next-Generation EPP

## BESSERER SCHUTZ VOR CYBER-BEDROHUNGEN

In einer zunehmend vernetzten Geschäftswelt spielt das effektive Management von Endgeräten eine entscheidende Rolle für Unternehmen jeder Größe. Unified Endpoint Management (UEM) hat sich als eine Schlüsselstrategie etabliert, um die Herausforderungen der Verwaltung und Sicherheit von Endgeräten in einem zunehmend komplexen und vielfältigen Umfeld zu bewältigen.

Herkömmliche Antivirus-Lösungen reichen aber mittlerweile nicht mehr aus, um Endpoints zuverlässig vor Angriffen zu schützen. Um bisher unentdeckte Lücken bei der Endpoint-Sicherheit zu schließen, setzt ManageEngine auf einen ganzheitlichen Ansatz, der die Interoperabilität zwischen IT-Funktionen fördern soll. Die „Next-Generation Antivirus“-Technologie (NGAV) ist ein fortschrittlicher Malware-Erkennungs-Mechanismus, der Deep Learning, KI-gestützte Echtzeit-Verhaltenserkennung, forensische Untersuchungen von Vorfällen und die Abwehr von Angriffen nutzt, um bekannte und unbekannte Bedrohungen zu erkennen und zu verhindern.

Im Gegensatz zu herkömmlichen Lösungen überwacht das NGAV Bedrohungen kontinuierlich und reagiert proaktiv mit einem mehrschichtigen Malware-Schutz – unabhängig vom Online- oder Offline-Status eines Geräts – und führt zudem Monitoring-, Analyse- und Abhilfe-Workflows lokal auf dem überwachten Gerät aus (Tabelle).

TRADITIONELLES ANTIVIRUS VERSUS NEXT-GEN ANTIVIRUS		
Feature	Herkömmlicher Endpoint-Schutz	Next-Generation Antivirus
Änderung von Sicherheitseinstellungen	Begrenzte Flexibilität bei der Änderung wichtiger Sicherheitseinstellungen.	Bietet die Möglichkeit wichtige Endpunkt-Sicherheitseinstellungen nach Bedarf zu ändern; gibt Administratoren Flexibilität bei der Anpassung an sich verändernde Sicherheitsanforderungen.
Vorgehensweise beim Scannen	Die Durchführung von Scans kann sich verzögern und hauptsächlich auf bekannte Bedrohungen konzentrieren.	Identifiziert und behandelt bekannte, unbekannte und dateilose Malware sofort; reduziert die Erkennungs- und Reaktionszeit erheblich.
Malware Definitions-Updates	Updates können verzögert bereitgestellt werden und so das Zeitfenster für Anfälligkeiten vergrößern.	Keine Definitions-Updates erforderlich.
Umfang der Geräteprüfung	Begrenzter Untersuchungsumfang, potenzielle Schwachstellen können übersehen werden.	Untersucht jeden Aspekt des Geräts, einschließlich Dateien, und bietet so einen umfassenden Schutz vor verschiedenen Angriffsvektoren.
Überwachung von Bedrohungen und Abwehr	Reaktive Verteidigung mit periodischer Überwachung.	Ständige Überwachung und Abwehr von Bedrohungen, die für die Aktivitäten von Benutzern und Geräten relevant sind; proaktiver Schutz vor potenziellen Cyber-Bedrohungen.
Vorhersage und Vorbeugung	In erster Linie auf Basis historischer Daten für bekannte Bedrohungen.	Prognose und erfolgreiche Bekämpfung bekannter Malware-Varianten; dank KI-gestützter Technologie verbesserte Präventivmaßnahmen gegen sich verändernde und hochentwickelte Bedrohungen.
Wiederherstellung von Daten	Begrenzte oder keine Wiederherstellungsfähigkeiten.	Wiederherstellung von Daten in einen gesunden Zustand über einen sicheren Mechanismus; Minimierung der Auswirkungen erfolgreicher Angriffe.
Ansatz zum Endpoint-Schutz	Traditionelle Antivirus- oder Anti-Malware-Lösungen.	Nutzt KI und ML, um auf dem neuesten Stand hinsichtlich Bedrohungen und Cyberangriffen zu sein; übertrifft traditionellen Endpunkt-Schutz.



UNSER ZIEL IST ES, EINE KI-GESTÜTZTE, UMFASSENDE END-TO-END-PLATTFORM FÜR DIGITALE UNTERNEHMEN ANZUBIETEN, IN DEM CYBER-RESILIENZ VON GRÖßTER BEDEUTUNG IST.

Mathivanan Venkatachalam,  
Vice President, ManageEngine,  
[www.manageengine.com](http://www.manageengine.com)

Um sich effektiv gegen moderne Cyberbedrohungen zu schützen und an die sich ständig weiterentwickelnde IT-Landschaft anzupassen, muss eine Endpoint-Protection-Plattform (EPP) der nächsten Generation fortschrittliche Funktionen bieten.

#### Funktionen „NGAV“-Add-on:

##### Bedrohungserkennung (Threat Detection)

Der KI- und ML-gestützte Malware-Erkennungs-Mechanismus arbeitet in Echtzeit und erkennt sowohl bekannte als auch unbekannte Malware sowie dateilose Angriffe. Unabhängig vom Online- oder Offline-Status des Geräts wird eine kontinuierliche Überwachung gewährleistet.

##### Incident-Forensik

Verschaffen Sie sich einen detaillierten Überblick und reagieren Sie durch umfassende Berichte und MITRE-TTP-basierte Analysen schneller auf Cyber-Bedrohungen. Die präzise Darstellung von Angriffspfaden, -techniken und der Cyber-Kill-Chain hilft Ihnen, gezielt auf Vorfälle zu reagieren.

##### Bedrohungsminderung (Threat Mitigation)

Um Bedrohungen effektiv zu neutralisieren, kann der infizierte Endpoint mit einem einzigen Klick in den Zustand vor der Malware-Infektion zurückversetzt werden. Das ist entscheidend für die Abwehr von Bedrohungsakteuren, die

versuchen, Backups zu verschlüsseln oder zu löschen, um eine Wiederherstellung unmöglich zu machen. Mit der integrierten Netzwerkquarantäne-Funktion können Sie infizierte Geräte isolieren und die Malware umgehend unschädlich machen. So lässt sich der Angriff stoppen und Eindämmungsmaßnahmen verbessern.

Endpoint Central unterstützt IT-Abteilungen darüber hinaus bei bewährten Aufgaben wie dem Device Lifecycle Management, Remote Troubleshooting, User Experience Management sowie bei der Endpoint-Sicherheit. Für die Verwaltung der Endgeräte nutzt die Lösung einen kleinen Agent – eine Software, die auf den Client-Systemen installiert wird.

#### Vorteile der neuen Funktionen

##### Großer Spielraum für Abhilfemaßnahmen:

IT-Sicherheitsteams können Patches ausrollen, infizierte Geräte vom Internet und dem internen Netzwerk isolieren, das Zurücksetzen von Anmeldedaten

erzwingen, Geräte auf die von der IT genehmigten Basisversionen zurücksetzen und unsichere Anwendungen entfernen.

##### Untersuchung von Incidents:

Integrierte Funktionen zur Remote-Fehlerbehebung und -Systemverwaltung ermöglichen es, Incidents auf unter Quarantäne gestellten Geräten sofort und gründlich zu untersuchen.

##### Feedback-Schleifen zur Verbesserung der Sicherheitslage:

Die Sicherheitsrichtlinien können auf Grundlage der von der NGAV-Engine erkannten Bedrohungen laufend aktualisiert werden, wodurch sich die Cybersicherheitslage kontinuierlich verbessert.

Endpoints sind schon seit geraumer Zeit einer der am häufigsten genutzten Angriffsvektoren für Cyberkriminelle. In den

Die neuen Funktionen befinden sich derzeit in einer ‚Early-Access-Phase‘, in der interessierte Kunden von Endpoint Central diese nach Freischaltung durch den ManageEngine-Distributor MicroNova kostenfrei testen können.





Endpoint Central

HomeThreats & PatchesInventoryApp CtrlMobile Device MgmtEndpoint DLPNext Gen Antivirus

Next Gen Antivirus is currently in Early Access and a separate licensing will be introduced in the future. Learn more

All endpoints are secure, no threats detected currently.

100%

Incidents

Devices

Settings

Status: All

1

2

3

4

5

Total: 2

Name	Detection Source	Detected On	Severity	Alerts	Infected Devices	Incident Status	Action
LB3.exe	Ransomware Detection E...	Oct 17, 2023 04:34 PM	High	1	1	Resolved	True Positive
ConfLine	Ransomware Detection E...	Oct 30, 2023 05:12 AM	High	3	1	Resolved	False Positive

LB3.exe

Most Recent Detection: Oct 17, 2023 04:34 PM | Severity: High | Incident Status: Resolved | Marked as: True Positive

Summary

Alerts (1)

Devices (1)

Signer

Unsigned

SHA-256

0526f8d4c268b96a76007f620e682f1fadfb3d1cc56656b63205d4d031b7970

Organization Information

Company

Product

Description

Process Information

File Type

Original File Name

Internal File Name

Copyright

First Infected Device Information

Device Name

Time

LB3.exe

Most Recent Detection: Oct 17, 2023 04:34 PM | Severity: High | Incident Status: Resolved | Marked as: True Positive

Summary

Alerts (1)

Devices (1)

Detected

Oct 17, 2023 04:34 PM

Incident Summary

Expand

Wininit.exe.mui

Execution Details

Process

Process Start Time

Process End Time

Process ID

Command Line

File Details

d526f8d4c268b96a76007f620e682f1fadfb3d1cc56656b63205d4d031b7970

61

72

61 security vendors and 1 sandbox flagged this file as malicious

d526f8d4c268b96a76007f620e682f1fadfb3d1cc56656b63205d4d031b7970

LB3.exe

Size

Last Analysis Date

peexe

calls-wmi

self-delete

detect-debug-environment

Community Score

Join the YI Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.lockbit/blackmatter

Threat categories

trojan

ransomware

Family labels

lockbit

blackmatter

encoder

Security vendors' analysis

Acronis (Static ML)

Suspicious

AhnLab-V3

Ransomware.Win.LockBit.RS21581

Alibaba

Trojan.Win32.Lockbit.c72289dd

ALYac

Trojan.Ransom.LockBit

Antiy-AVL

Trojan.Ransom/Win32.LockBit.ha

Avastbit

Trojan.Generic.D4049D08

1

Wann hat der Angriff (Intrusion) stattgefunden?

Dieser Screenshot zeigt die Zeit des Angriffs, die Anzahl der generierten Alarme, die Anzahl der infizierten Geräte, den Fortschritt der Bedrohung sowie die Option, die Intrusion als Wahr- oder Falsch-Positiv zu kategorisieren.

2

Wie lässt sich der Alarm analysieren?

Durch einen Klick auf den entsprechenden Vorfall bietet die EPP-Lösung den Benutzern im Reiter „Zusammenfassung“ relevante Details zu diesem Ereignis an.

3

Erweitern Sie die Vorfalldatenzusammenfassung auf der Registerkarte Alerts

Die Vorfalldatenzusammenfassung lässt sich erweitern und bietet so detaillierte Einblicke, etwa in Prozessquelle, untergeordnete Prozesse und Befehlszeilentools. Per Klick auf einen untergeordneten Prozess werden detaillierte Informationen, einschließlich SHA-Wert, Bildpfad und Befehlszeilentails angezeigt.

4

Virus Total Verifizierung (unklar/keine Ergebnisse)


Eine Validierung durch VirusTotal kann den Hash als echten Positivbefund bestätigen und bietet einen eindeutigen Beweis für den Versuch der Infiltration durch Malware. VirusTotal führt eine umfassende Analyse mit verschiedenen Antiviren-Scan-Engines durch, um die Dateien auf potenzielle Bedrohungen zu untersuchen. User können so nach der Überprüfung proaktive Sicherheitsmaßnahmen ergreifen, indem sie das infizierte Gerät unter Quarantäne stellen.

letzten zehn Jahren hat ManageEngine kontinuierlich neue Endpoint-Security-Funktionen wie Vulnerability-Assessment und -Behebung, Browser-Sicherheit, Endpoint-Berechtigungsverwaltung, Data Leakage Prevention und Anti-Ransomware hinzugefügt, um Unternehmen bei der Minimierung ihrer Angriffsfläche zu

unterstützen. Die NGAV-Funktionen erweitern nun Endpoint Central um einen KI-basierten Malware-Schutz, der die Lösung als Enterprise-Protection-Plattform abrundet und Kunden so einen ganzheitlichen Ansatz bei der Cyber-Abwehr ermöglicht.


Mathivanan Venkatachalam

März/April 2024 | [www.it-daily.net](http://www.it-daily.net)



MEHR WERT

Endpoint Central Architecture



Next.Gen Antivirus

# DIGITALE IDENTITÄTEN IM SCHEINWERFERLICHT

## SCHLÜSSEL ZU WICHTIGEN DIENSLEISTUNGEN

Digitale Identifizierungs- und Identitätslösungen sind ein wichtiger Bestandteil des globalen technologischen Fortschritts. Neben vereinfachten und komfortableren Prozessen, beispielsweise bei Behördengängen oder auf Reisen, steht der Nachweis der eigenen Identität auch in direktem Zusammenhang mit grundlegenden Menschenrechten. Aus diesen Gründen kommt der Weiterentwicklung von Technologien und Lösungen eine entscheidende Rolle zu. Und Fortschritte gibt es reichlich.

**#1** Reisen werden digitaler und sicherer. Neue Technologien ebnen den Weg für ein neues Sicherheitsniveau bei elektronischen Reisepässen. So helfen Self-Check-in-Terminals und biometrische Daten auf Mikrochips etwa, das Boarding am Flughafen deutlich zu beschleunigen. Die nächste Stufe dieser Entwicklung: der physische Reisepass wird nicht mehr die einzige Möglichkeit sein, mit der Reisende ihre Identität verifizieren können – mit Digital Travel Credentials (DTC) lässt sich der zukünftige Reiseausweis auch vollständig digital abbilden, etwa bequem auf dem Handy oder der Smartwatch.

**#2** Der Reisepass wird nachhaltiger. Die Reise- und Tourismusbranche ist für geschätzte acht bis elf Prozent der weltweiten Emissionen verantwortlich. Um der Pflicht zur Reduzierung des eigenen Fußabdruckes nachzukommen, konzentriert sich die Forschung verstärkt auf recycelbare Materialien für Dokumente, die nachhaltigere Lieferketten

garantieren können. Die Tage der auf Virgin Plastic basierenden Pässe dürften damit schon bald gezählt sein. Die Digitalisierung dieser Dokumente kann dazu beitragen, den Bedarf an physischen Ausweisen zu reduzieren.

**#3** Self-Sovereign Identity (SSI) wird relevant. Mit der selbstbestimmten Identität erhält die individuelle Person die Kontrolle über ihre Daten zurück. Das revolutionäre Konzept ermöglicht die Wahlfreiheit, welche Informationen wann und an wen übermittelt werden sollen. Während die Vorlage eines Personalausweises etwa bei einer Mietwagenfirma sehr viele sensible Daten über eine Person verrät, ist mit einer SSI-Lösung das selektive Freischalten von benötigten Informationen realisierbar. Mit diesem Zero-Knowledge-Proof-Ansatz sind Bürger zukünftig in der Lage, sich effektiv gegen Data

Mining und den Missbrauch ihrer Daten zu schützen.

**#4** Die Identität wird digitaler. Menschen ohne rechtsgültigen Identitätsnachweis bleibt der Zugang zu zentralen Dienstleistungen und Menschenrechten verwehrt – etwa bei Wahlen, im Bildungssystem oder im Bankwesen. Ziel der Vereinten Nationen ist es daher, bis 2030 jedem Menschen die Möglichkeit zu geben, seine Identität zu registrieren. Universelle Lösungsansätze führender Anbieter konzentrieren sich dabei zunehmend auf digitale und phygitalle Technologien, also eine Mischung aus digital und physisch. Sie sind nicht nur sicherer und komfortabler als rein physische Ausweise, sondern öffnen auch die Türen zu elektronischen Diensten, sind einfacher zu verwalten und bieten ein höheres Maß an Sicherheit.

[www.veridos.com](http://www.veridos.com)



Quelle: Veridos

# VPN & die Cloud

MODERNER REMOTE ACCESS OPTIMIERT JEDES IT-SECURITY-KONZEPT

Cyber-Angriffe sind das Geschäftsrisiko, das von Firmen am meisten gefürchtet wird – das ergibt eine Befragung im Rahmen des Allianz Risk Barometer 2024. Unternehmen werden sich ihrer eigenen Verwundbarkeit also immer weiter bewusst, dennoch reißen die Fälle von erfolgreichen Cyberangriffen nicht ab. Auch aktuelle Cloud-IT-Strategien, die fortschrittlichen Schutz gegen Angreifer bieten sollen, können noch optimiert werden – und zwar durch die Kombination mit einer zeitgemäßen VPN-Lösung.

## Sicherheit durch Zero Trust neu gedacht ...

„Zero Trust“, „SD-WAN“, „SASE“, „SSE“ oder „SSO durch SAML“ – diese Begriffe sind sicherlich den meisten IT-Administratoren bekannt. Vor allem ein Ansatz davon gewann zuletzt zunehmend an Bedeutung: Zero Trust. Bei diesem Konzept wird der Fokus primär auf das „Least privilege“-Prinzip gelegt.

Den Nutzern und ihren Endgeräten wird kein blindes Vertrauen mehr ausgesprochen. Das System prüft, welcher Nutzer auf welche Daten Zugriff erhält. Ist der Anwender nicht für die entsprechende Netzwerkressource freigegeben, kann er nicht darauf zugreifen. So wird auch Kriminellen wenig Spielraum gelassen. Selbst wenn ein Angreifer ins Netzwerk gelangt, kann der IT-Administrator den kompromittierten Bereich gezielt abriegeln und weitere Maßnahmen ergreifen.

## ... und durch VPN optimiert!

Allerdings steht dieser IT-Philosophie die praktische Umsetzung im Weg. Schließlich ist Zero Trust kein fertiges Produkt, sondern nur ein theoretisches Konzept. Dieses muss von jedem Unternehmen für sich interpretiert und durch unterschiedliche Lösungen zum Leben erweckt werden. Jede Lösung bedient dabei einen oder mehrere Teilbereiche – etwa Datenübertragung, Endpoint

Security, Firewall-Konfiguration oder Multifaktor-Authentifizierung. Praktisch für Administratoren wird es dann, wenn ein Produkt direkt mehrere dieser Aspekte abdecken kann.

Das ist unter anderem bei fortschrittlichen, softwarebasierten VPN-Lösungen wie den Secure Enterprise Produkten von NCP der Fall. Diese funktionieren bereits seit Jahren nach dem Prinzip von Zero Trust. Per zentraler Management-Komponente definieren Administratoren alle Zugriffsrechte ihrer Nutzer mit wenig Zeitaufwand – und zwar nicht nur für Cloud-Applikationen, sondern IP-basiert für den kompletten Netzwerkbereich. Auf diese Weise kann sehr granular gesteuert werden, welcher Benutzer auf welche Dateien, Ordner und Anwendungen Zugriff erhält. Im Falle eines Phishing-Vorfalles sind betroffene Bereiche dadurch genau einzugrenzen und die IT-Administration kann entsprechend reagieren. Ergänzt wird die Lö-





sung durch Funktionen wie „Application based Tunneling“ oder „VPN-Bypass“, wodurch ganze Netzbereiche bei Bedarf am Tunnel vorbeigeleitet werden können. Auf diese Weise wird der Server entlastet, indem datenintensiver, nicht sicherheitsrelevanter Traffic nicht über das VPN übertragen wird.

### Kompatibilität mit Login-Verfahren

Unbefugte Zugriffe sollten nach Möglichkeit bereits im Vorfeld so weit wie möglich verhindert werden. Deshalb spielt auch der Login-Aspekt eine tragende Rolle. Hier ist es im Sinne eines jeden sicherheitsbewussten Unternehmens, dass veraltete Login-Mechanismen durch zeitgemäße Multifaktor-Authentifizierung (MFA) abgelöst werden. Schließlich ist MFA auch in einem Zero-Trust-Konzept essenziell und stellt nicht zuletzt eine der effizientesten Methoden dar, um die eigenen Zugänge effektiv vor Angreifern zu schützen. Gerade im Firmenkosmos erfreuen sich auch komplexere Protokolle wie SAML immer größerer Beliebtheit, mit denen die Verwendung von Anmeldeinformationen für mehrere Webseiten möglich wird. Nach dem Prinzip des Single Sign-On (SSO) muss sich der User dann ebenfalls nur ein Passwort merken, mit dem er sich einmal authentifiziert und anschließend auf alle benötigten Portale und Webseiten zugreifen kann.

Um diese Technologien in die eigene Cloud-Infrastruktur zu integrieren, bedarf es allerdings ebenfalls einer IT-Security-Komponente mit entsprechender Kompatibilität. Auch dies ist bei modernen Remote-Access-VPN-Lösungen gegeben. Der VPN-Client mit SAML ermöglicht den Datenaustausch zwischen einem internen Authentication-Provider und einem Online-Identity-Provider, der die Authentifizierung und Verwaltung der SAML-Benutzer zum Beispiel über Okta oder Microsoft Azure AD ermöglicht. Auf diese Weise können die Produkte nahtlos miteinander kommunizieren



„  
MODERNE VPN-LÖSUNGEN  
WERDEN EIN WERTVOLLER  
TEIL HOCHKOMPLEXER  
TECHNOLOGIEKONZEPTE  
UND LIEFERN BEDEUTENDE  
VORTEILE IN FORM VON  
ANWENDERFREUNDLICHER  
BEDIENUNG UND EINFACHER  
ADMINISTRATION.“

Dennis Christ, Content Marketing Manager,  
NCP engineering GmbH,  
[www.ncp-e.com](http://www.ncp-e.com)

ren und es kommt zu keinen Kompatibilitätsproblemen.

### Kompatibilität und Usability an die Spitze!

Dieses Prinzip gilt auch für Netzwerk-Technologien wie SD-WAN, SASE und SSE. Solche Netzwerkzusammenschlüsse setzen ein sehr hohes Sicherheitsniveau voraus, um das gesamte Netzwerk robust zu gestalten. Diese Absicherung können beispielsweise softwarebasierte VPN-Lösungen übernehmen, die entsprechende Kompatibilität aufweisen.

Bei aller Sicherheit darf jedoch auch ein wichtiger Faktor nicht vernachlässigt werden: die Nutzbarkeit der Lösung durch ihre Benutzer, denn die tägliche Arbeit sollte durch neue Technologien und IT-Anwendungen nicht eingeschränkt werden. Stattdessen muss moderner IT-Schutz immer mit einer hohen Usability vereint werden. Nur so können sowohl IT-Administratoren als auch Endanwender produktiv und damit sicher arbeiten. Aus der Sicht des Endanwenders muss die Lösung unkompliziert

im Hintergrund laufen. Im Idealfall muss der Mitarbeiter nach dem Start des Rechners nur seine Anmeldeinformationen im Client eingeben und auf „Verbinden“ klicken. Der Nutzer merkt von den sicherheitsrelevanten Prozessen im Hintergrund nichts und arbeitet von überall aus so, als würde er sich lokal in der Firma befinden – mit voller Geschwindigkeit und hochsicher.

Der betreuende IT-Administrator profitiert hingegen von der Möglichkeit eines zentralen Managements. Hier teilt er seine Nutzer mit wenigen Mausklicks in Gruppen ein, rollt global Updates aus und verteilt granulare Firewall- und Zugriffsrichtlinien – entweder an einzelne Nutzer, bestimmte Abteilungen oder die gesamte Organisation. Umständliches und zeitraubendes Management einzelner Accounts entfällt damit vollständig.

### Das Beste aus allen Welten vereint

Das Fazit: Zero Trust ist nicht mit „100 Prozent Cloud“ gleichzusetzen. Transparenter Netzwerkzugriff gehört auch 2024 für viele Unternehmen noch zum IT-Alltag und wird nicht von heute auf morgen verschwinden. Daher ist es für Unternehmen wichtig, dass ihre IT-Security-Lösung beide Welten bedienen kann. So bleibt beispielsweise auch eine im Firmennetz befindliche Telefonanlage mit VPN weiterhin nutzbar, während diese bei den meisten anderen Zero-Trust-fähigen Produkten in der Cloud stehen müsste. Moderne VPN-Lösungen werden somit ein wertvoller Teil hochkomplexer Technologiekonzepte wie SASE, SSE oder Zero Trust und liefern gleichzeitig bedeutende Vorteile in Form von anwenderfreundlicher Bedienung und einfacher Administration. Dazu kommt, dass sich Firmen mehrere Einzelanwendungen sparen, indem sie eine vielseitige VPN-Lösung als Ergänzung in ihr Sicherheitskonzept einbauen, die ihre individuellen Security-Bedürfnisse erfüllt.

Dennis Christ

## IMPRESSUM

**Herausgeber:** Ulrich Parthier (08104-6494-14)

**Geschäftsführer:** Ulrich Parthier, Vasiliki Miridakis

**Chefredaktion:** Silvia Parthier (-26)

**Redaktion:** Carina Mitzschke  
(nur per Mail erreichbar)

**Redaktionsassistent und Sonderdrucke:** Eva Neff (-15)

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

**Autoren:**  
Alessandro Benke, Dennis Christ, Andreas Fuchs, Fabian Glöser, Uwe Gries, Jörg von der Heydt, Stephen Lowing, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Nicklas Urban, Michael Veit, Mathivanan Venkatachalam, Danny de Vreeze, Patrick Wunder, Hakan Yildiz

**Anschrift von Verlag und Redaktion:**  
IT Verlag für Informationstechnik GmbH  
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing  
Tel: 08104-6494-0,  
Fax: 08104-6494-22

E-Mail für Leserbrief: 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,  
E-Mail: fraenzke@it-verlag.de  
Karen Reetz-Resch, Home Office: 08121-9775-94,  
E-Mail: reetz@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-Abbo 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 Gesellschafterskapitals hält Ulrich Parthier, Sauerlach.

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

Das Abonnement ist beim Verlag mit einer drei-  
monatigen Kündigungsfrist zum Ende des Bezugs-  
zeitraumes kündbar. Sollte die Zeitschrift aus  
Gründen, die nicht vom Verlag zu vertreten sind,  
nicht geliefert werden können, besteht kein An-  
spruch auf Nachlieferung oder  
Erstattung vorausbezahlter Beträge.

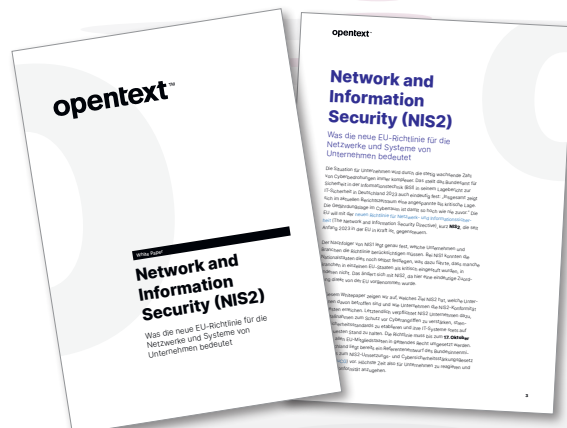


# NIS2

## WAS DIE NEUE EU-RICHTLINIE FÜR NETZWERKE UND SYSTEME BEDEUTET

Die Situation für Unternehmen wird durch die stetig wachsende Zahl von Cyberbedrohungen immer komplexer. Das stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Lagebericht zur IT-Sicherheit in Deutschland 2023 auch eindeutig fest: „Insgesamt zeigt sich im aktuellen Berichtszeitraum eine angespannte bis kritische Lage. Die Gefährdungslage im Cyberraum ist damit so hoch wie nie zuvor.“ Die EU will mit der neuen Richtlinie für Netzwerk- und Informationssicherheit (The Network and Information Security Directive), kurz NIS2, die seit Anfang 2023 in der EU in Kraft ist, gegensteuern.

In diesem Whitepaper zeigen wir auf, welches Ziel NIS2 hat, welche Unternehmen davon betroffen sind und wie Unternehmen die NIS2-Konformität am besten erreichen. Letztendlich verpflichtet NIS2 Unternehmen dazu, ihre Maßnahmen zum Schutz vor Cyberangriffen zu verstärken, strengere Sicherheitsstandards zu etablieren und ihre IT-Systeme stets auf dem neuesten Stand zu halten. Die Richtlinie muss bis zum 17. Oktober 2024 in allen EU-Mitgliedstaaten in geltendes Recht umgesetzt werden.



### WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 27 Seiten  
und steht kostenlos zum Download bereit.  
[www.it-daily.net/Download](http://www.it-daily.net/Download)





Fokustag  
IAM  
+

# WE SECURE IT

17. bis 19. April

Digitalevent

#WesecureIT2024



Mehr erfahren



# Herzlichen Glückwunsch

**30** Jahre  
it management



**Das sind mehr als 10.950 Tage voller Nullen und Einsen.**

Wir erinnern uns an die wilden Tage der Disketten, nervenaufreibende Upgrades auf Windows 95 und an Zeiten, in denen Passwörter so sicher waren wie Omas geheimes Apfelkuchenrezept.

In einer Welt, in der Cyberbedrohungen inzwischen schneller mutieren als Modetrends, seid Ihr die Informationsquelle für alle Wächter der Datensicherheit, Ritter der Firewalls und Architekten von digitalen Festungen.

**Dafür sagen wir von Herzen „DANKE!“**

**Euer DriveLock-Team**

