it management

Der Motor für Innovation
März/April 2023

INKLUSIVE 48 SEITEN
it security

DIGITALER WANDEL

# Die Säulen der modernen Arbeit

Christian Malzacher, Bechtle AG

THOUGHT LEADERSHIP

AB SEITE 20

PAESSLER
THE MONITORING EXPERTS

## CHATGPT

Revolution der Chatbot-Technologie?

## CENTER OF AUTOMATION

Zündet den Booster!

KONICA MINOLTA

Erfolgreich digitalisieren

ab Seite 16


o2business.de
Wir haben sehr gute Antennen dafür, was Firmen jetzt brauchen.
Andere Zeiten. Andere Lösungen.
Im sehr guten 5G Netz[1] von O2
zum sehr guten Preis[2].
O2 Business
can do
connect 1
SEHR GUT
MOBILFUNK UND 5G-NETZTEST
O2
Heft 1/2023
Eine Telefónica Marke
1 connect Mobilfunk- und 5G-Netztest, Heft 01/2023: „sehr gut“ (894 Punkte) für O2; insgesamt wurden vergeben: 2x „sehr gut“ (915 und 894 Punkte) und 1x „überragend“ (952 Punkte). 5G ist für geeignete Endgeräte an immer mehr Standorten verfügbar. Weitere Informationen unter: o2.de/netz. | 2 Mobilfunk-Studie 2022 durchgeführt vom Marktforschungsinstitut SWI Finance für Handelsblatt, Veröffentlichung Handelsblatt am 28.09.2022: „sehr gut“ (87,4 Punkte) für O2 Business; insgesamt wurden vergeben: 2x „sehr gut“ (87,4 und 85,3 Punkte) und 4x „gut“.

# REVOLUTION VORAUS?

LIEBE LESERINNEN UND LESER,

jetzt halten Sie bereits die zweite Ausgabe unseres Relaunches in den Händen – wir haben noch ein bisschen nachjustiert und hier und da etwas Feinschliff betrieben. Aber wie es bei allen Weiterentwicklungen und Prozessen so ist, zufrieden ist man nie wirklich und irgendetwas lässt sich immer verbessern - auch, wenn wir bisher durchweg positives Feedback erhalten haben. Das freut uns und soll natürlich auch so bleiben. An dieser Stelle auch ein Dankeschön an die Leser, die sich lobend geäußert haben (kritische Kommentare haben uns noch nicht erreicht).

Auch in dieser Ausgabe widmen wir uns wieder aktuellen Themen, so etwa dem gegenwärtigen Hype um ChatGPT. Ist das wirklich die lang ersehnte Revolution in der KI, der Zukunftstrend schlechthin oder ein weiteres Sicherheitsrisiko für Unternehmen und User? Lesen Sie dazu Einschätzungen im it management ab Seite 54 und im it security ab Seite 40.

Digitalisierung, New Work und Automatisierung: Das sind Themen, über die wir regelmäßig berichten. Dass die Digitalisierung mittlerweile ein modernes und flexibles Arbeitsmodell bedingt und eben dieses Arbeitsmodell ebenfalls kein Wettbewerbsvorteil mehr ist, wissen Sie wahrscheinlich längst. Aber dass das Thema New Work oder „Office 4.0", wie wir es nennen, zum zentralen Erfolgsfaktor geworden ist, wissen Sie auch? Lesen Sie mehr zu dieser These in der aktuellen Coverstory ab Seite 10.

Und was gibt es Neues im Bereich Unternehmenssicherheit? RBAC ist tot! Oder doch nicht? Warum Identity Access Management ein zentrales Element jeder Sicherheitsstrategie sein sollte und wie man MFA-Fatigue Angriffe vermeidet? Finden Sie es heraus, im Supplement it security.

Herzlichst

Carina Mitzschke | Redakteurin it management & it security



# INHALT

## COVERSTORY



## IT MANAGEMENT



Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

## THOUGHT LEADERSHIP



## IT MANAGEMENT

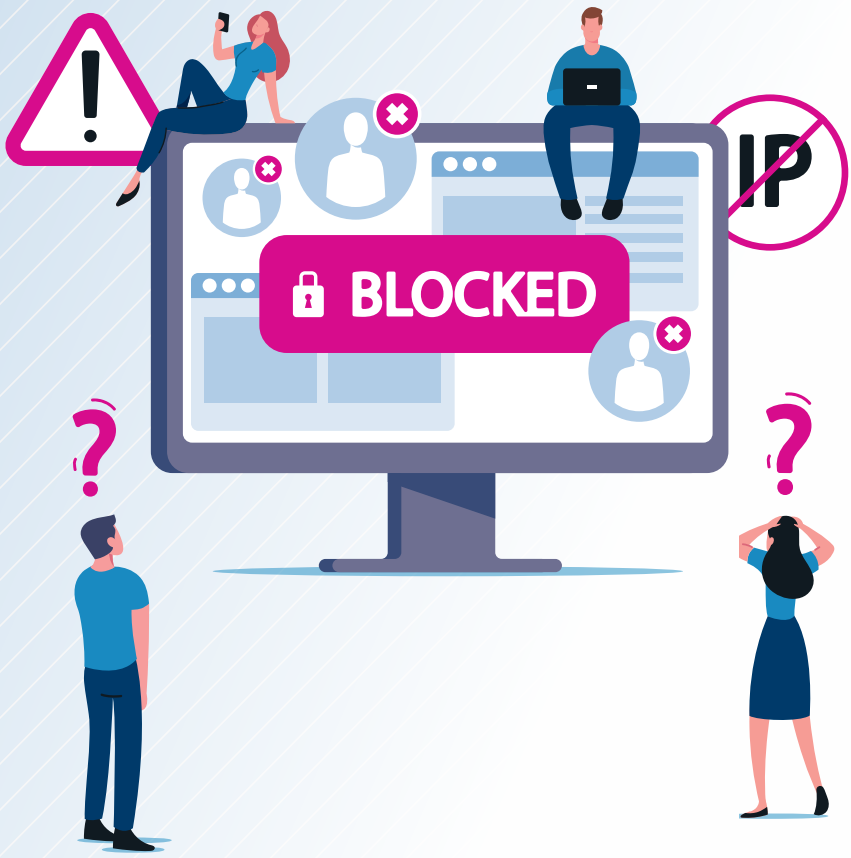





**Inklusive 48 Seiten it security**

**GUT ZU WISSEN**

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




# Ransomware oder Malware?

## WAS IST DER UNTERSCHIED?

Laut einer aktuellen Kaspersky-Umfrage bewertet die Führungsriege in Deutschland Cyberbedrohungen (47 Prozent) zwar als ein ebenso großes Risiko für ihr Unternehmen wie das sich derzeit verschlechternde wirtschaftliche Umfeld (47 Prozent), jedoch mangelt es gleichzeitig am Verständnis grundlegender Cybersicherheits-bezogener Begriffe. So sorgen beispielsweise gängige Begriffe wie Malware oder Ransomware für Verwirrung.

Ob Sky Deutschland oder T-Mobile – während sich Cyberangriffe in Deutschland gerade zu häufen scheinen, ist das Thema Cybersicherheit für nicht einmal die Hälfte (46 Prozent) der Führungsriege ein ständiger Tagesordnungspunkt in Vorstandmeetings. Die fehlende Integration des Themas in die Agenda lässt sich möglicherweise unter anderem darauf zurückführen, dass viele Führungskräfte die Begrifflichkeiten nicht voll verstehen.

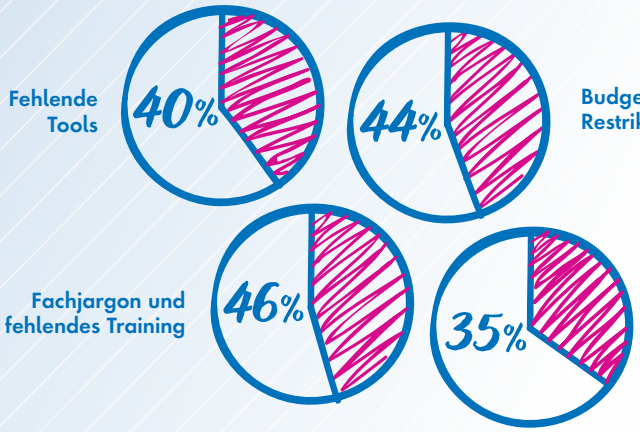
Denn für fast die Hälfte (46 Prozent) des C-Levels in Deutschland stellt der Fachjargon und Branchenbegriffe derzeit die größte Hürde für Cybersicherheit dar – noch vor Budget-Restriktionen (44 Prozent). Folgende Begrifflichkeiten sind demnach für die Führungsriege verwirrend:

- Malware (40 Prozent)
- Zero-Day-Exploit (40 Prozent)
- Phishing (39 Prozent)
- Ransomware (38 Prozent)
- APTs (36 Prozent)

Weniger überraschend ist deshalb, dass auch technischerer Fachjargon, wie IoC (Indicator of Compromise, 56 Prozent), YARA-Regeln (54 Prozent) oder TTPs (Tactics, Techniques, and Procedures – 54 Prozent) oft nicht verstanden wird.

***www.kaspersky.de***

## HINDERNISSE FÜR DIE CYBERSICHERHEIT VON UNTERNEHMEN




(Quelle: Kaspersky; Threat Intelligence)

**Die vollständige Studie**

„Sprechen Sie Cybersecurity? Threat Intelligence – Wissen Entscheider, mit welchen Cyberbedrohungen sie konfrontiert werden, und wie sie richtig reagieren?" ist verfügbar unter ***kas.pr/ti-report***

# METAVERSE

## WIRTSCHAFTSFAKTOR?

Auf 468 Milliarden Euro schätzen die Statista Advertising & Media Markets Insights den weltweiten Metaverse-Umsatz im Jahr 2030. Das ist eine vergleichsweise zurückhaltende Prognose. Andere Analystenunternehmen gehen von einem Marktvolumen zwischen 700 und 1.600 Milliarden US-Dollar aus. So unterschiedlich die Schätzungen sind, so unterschiedlich dürften auch die zugrundeliegenden Definitionen sein.

Bei Statista bezieht sich der Begriff Metaverse auf eine virtuelle Welt oder eine Sammlung virtueller Welten, die in einem gemeinsamen digitalen Raum existieren und auf die die Nutzer über das Internet zugreifen können. Es umfasst in der Regel virtuelle Realität, erweiterte Realität und andere immersive Technologien. Der Begriff Metaverse umfasst ein breites Spektrum an Möglichkeiten, aber einige der gängigsten Segmente sind der elektronische Handel und Spiele. Darüber hinaus könnte das Metaverse auch neue Möglichkeiten für Bildung, Unterhaltung, Gesundheit und Fitness und sogar Telearbeit bieten.

Während sich diese Definition noch relativ vorsichtig liest, zeigt das Rechenmodell, dass es genau diese Segmente sind, die den Markt treiben – vorausgesetzt unsere Analyst:innen behalten Recht. Allein der Metaverse-E-Commerce-Umsatz könnte bis 2030 auf fast 200 Milliarden Euro steigen. Dahinter folgt Gaming mit rund 156 Milliarden Euro vor Gesundheit & Fitness mit 52 Milliarden Euro.

***de.statista.com***

**Mehr Informationen und Daten** zum Thema liefert unser Metaverse Market Report:

**bit.ly/3jUnKsz**

# RESILIENZ STÄRKEN

## AGILE TECHNOLOGIEN NUTZEN

Bearing Point zeigt in einer aktuellen Studie: Führende Unternehmen verbessern ihre Widerstandsfähigkeit durch agile Technologien, die sie mithilfe von modernster Enterprise Architecture (EA) bereitstellen.

Im Rahmen der Studie analysierte BearingPoint mehr als 5.000 Projekte mit dem Ziel, die Resilienzmerkmale von 150 führenden Unternehmen zu bewerten. Anschließend entwickelte das Team ein Benchmarking-Tool, mit dem Unternehmen ihre eigene Resilienz untersuchen können.

Die Studie zeigt klar: Unternehmen, die in ihren Technologie-Bereichen agile Methoden nutzen, sind resilienter als ihre Wettbewerber. Gleichzeitig stellt sie aber fest, dass auch diese Unternehmen sich nicht einfach zurücklehnen können.

**Geschäftsmodelle und Technologie gehen Hand in Hand**

Resiliente Unternehmen legen großen Wert darauf, dass IT und Geschäftsbereiche eng zusammenarbeiten: So stellen sie einerseits sicher, dass aktuelle Technologien so effektiv wie möglich genutzt werden; andererseits erkennen sie frühzeitig, in welche neuen Technologien sie investieren sollten, um die Wertschöpfung zu steigern. Sie wissen: Erst nach der erfolgreichen agilen Transformation können sie das volle Potenzial ausschöpfen, das in ihrer Technologie steckt.

**Geschäftsaktivitäten stärken und Mehrwert schaffen**

Die Studie zeigt, dass führende Unternehmen mit fünf Maßnahmen echten Mehrwert schaffen, indem sie ihre Resilienz durch den Einsatz von Technologien steigern:

**#1** Sie nutzen Technologien, um zukünftige Geschäftsanforderungen frühzeitig zu erkennen

**#2** Sie tarieren ihre Wertschöpfungskette immer wieder aus

**#3** Sie entwickeln Kernkompetenzen in der Unternehmensarchitektur

**#4** Sie investieren in neue Technologien, Personal und den digitalen Arbeitsplatz

**#5** Sie arbeiten umfassend mit den Stakeholdern zusammen

***www.brearingpoint.com/de-de***

## AGILITÄT: WUNSCH & WIRKLICHKEIT

**Anteil der Befragten, die die folgenden Faktoren als Gründe ansehen, agile Methoden im Unternehmen einzusetzen**

# Corporate Digital Responsibility

## EIN THEMA FÜR ALLE BRANCHEN

Digitale Technologien wie künstliche Intelligenz, Blockchain, Smart City oder autonomes Fahren öffnen neue Geschäftsfelder für die Wirtschaft. Die Gesellschaft kann von solchen Zukunftstechnologien durch Effizienz, Automatisierung und Transparenz profitieren. Doch haben digitale Technologien Risiken und Nebenwirkungen – für die Mitarbeitenden in Unternehmen, für die Umwelt und für die Gesellschaft. Wie Unternehmen im digitalen Wandel systematisch Verantwortung übernehmen können, zeigt das Institut für ökologische Wirtschaftsforschung (IÖW) in einer Studie zur „Corporate Digital Responsibility" (CDR). Die Forschenden analysierten Nachhaltigkeitsberichte von über 60 deutschen Großunternehmen und schlussfolgern, dass die Unternehmen über die Branchen hinweg ihre Rolle als Nutzer digitaler Angebote stärker beachten müssen. Dabei geht es um Themen wie Datenschutz, ethische Fragen künstlicher Intelligenz oder die Auswirkungen digitaler Hardware und Infrastrukturen auf den Klimawandel.

**Im Einklang mit nachhaltiger Entwicklung**

In der Studie, die das IÖW mit Förderung des Bundesministeriums für Arbeit und Soziales (BMAS) erarbeitet hat, stellt das Institut ein wissenschaftlich fundiertes Konzept mit allen wesentlichen Handlungsfeldern zur digitalen Unternehmensverantwortung vor. Die Studie gibt Unternehmen ein Konzept an die Hand, wie sie ihre Digitalisierung im Einklang mit einer nachhaltigen Entwicklung gestalten können.

„Im digitalen Zeitalter ist es erforderlich, dass das Konzept der Corporate Social Responsibility zur gesellschaftlichen Verantwortung von Unternehmen ein Upgrade erfährt, indem es um die Corporate Digital Responsibility erweitert wird. Indem unser Konzept CDR in die etablierten Handlungsfelder der Unternehmensverantwortung integriert, können Firmen ihre Digitalverantwortung in bereits bestehende Strukturen einbetten.", so Vivian Frick, Wissenschaftlerin am IÖW und Mitverfasserin der Studie.

**Digitalverantwortung**

Die Studie ermöglicht Unternehmen, die sich mit ihrer Digitalverantwortung auseinandersetzen wollen, einen Blick über den eigenen Tellerrand: Sie zeigt systematisch auf, wie deutsche Großunternehmen zahlreicher Branchen in ihrer Nachhaltigkeitsberichterstattung CDR-Themen verstehen und angehen.

***www.ioew.de/cdr***

# Die Säulen der modernen Arbeit

## SO MEISTERN UNTERNEHMEN DEN DIGITALEN WANDEL

In einer volatilen und von Unsicherheit geprägten Zeit gilt es, die richtigen Weichen in die Zukunft zu stellen. Ulrich Parthier, Publisher it management sprach mit Christian Malzacher, Business Manager bei der Bechtle AG darüber, warum die Säulen der modernen Arbeit die Antworten auf die drängendsten Fragen der Unternehmen sind.

**Ulrich Parthier:** *Ein modernes und flexibles Arbeitsmodell ist kaum mehr ein Wettbewerbsvorteil, sondern zum zentralen Erfolgsfaktor geworden. Was ist die wichtigste Aufgabe, vor der Unternehmen derzeit stehen?*

> MODERNE TECHNOLOGIEN VERÄNDERN MIT IHREN MÖGLICHKEITEN DIE ART UND WEISE, WIE WIR ZUSAMMENARBEITEN, NACHHALTIG.
>
> **Christian Malzacher, Business Manager – Modern Workplace, Bechtle AG, www.bechtle.com**

**Christian Malzacher:** Die wichtigste Aufgabe muss es sein, eine gewinnbringende und schlüssige Strategie zu finden, um sich die Chancen der modernen Arbeitswelt zu erschließen.

Wir befinden uns mitten im digitalen Wandel. Kaum jemand kann heute noch anzweifeln, dass unternehmerischer Erfolg direkt mit dem Digitalisierungsgrad einer Organisation zusammenhängt. Egal, ob es nun die Krisen der Vergangenheit, der Fachkräftemangel, Nachhaltigkeitsthemen oder die Erwartung ist, dass Unternehmen Verantwortung für ihr Handeln übernehmen – all das führt über kurz oder lang dazu, dass modernes Handeln und modernes Arbeiten in den Firmen einziehen werden. Homeoffice, hybride Arbeitswelten und digitale Meetings bedeuten aber nicht nur Herausforderungen. Vielmehr bringen Sie Chancen und vor allen Dingen auch den angestrebten Erfolg. Dabei wird inzwischen immer deutlicher, dass ein digitales Büro mehr ist als nur ein neues Device für die Mitarbeitenden. Dies ist genau die richtige Zeit, sich den Möglichkeiten und Lösungen zu widmen, die moderne digitale Arbeitsplätze bieten. In zahlreichen Projekten hat sich unsere Herangehensweise an die Herausforderungen unserer Kunden bewährt. Sie stützt sich auf die sechs Säulen des modernen Arbeitens: Modern Deployment und Management, Modern Meetings, Modern Communication, Extended Reality, digitales Büro sowie User Adoption und Change Management.

**Ulrich Parthier:** *Was treibt den digitalen Wandel an und wie kann der Erfolg langfristig gesichert werden?*

**Christian Malzacher:** Der aktuelle Digitalisierungsschub im Fahrwasser der, unter anderem, Homeoffice-Pflichten der Vergangenheit oder auch der aktuellen Anforderungen, einen nachhaltigeren Umgang mit Ressourcen zu ermöglichen, fördert im Umfeld von Work-Life-Integration, Collaboration und Remote Work neue Arbeitsmodelle. Dabei kommt es im ersten Schritt nicht darauf an, welche technische Lösung eingesetzt wird. Wichtig ist, den langfristigen Erfolg zu sichern, indem alle notwendigen Maßnahmen ergriffen werden, die es Mitarbeitenden leicht machen, so produktiv wie möglich zu sein. Es geht also um Veränderungsbereitschaft und ein neues Mindset in allen Bereichen des Unternehmens. Nur wenn der Wille zur Veränderung vorgelebt wird, wird die Veränderung selbst auch von allen angenommen. So profitieren am Ende nicht nur die Angestellten von modernen, flexiblen Arbeitszeitmodellen, hochwertiger Ausstattung und agilen Arbeitsweisen. Für das ganze Unternehmen sind verbesserte Produktivität und gesteigerte Zufriedenheit der Mitarbeitenden ein Gewinn.

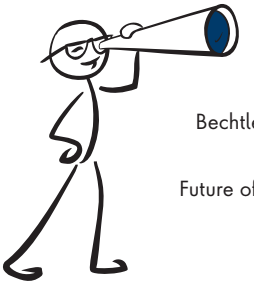
**Ulrich Parthier:** *Auf was sollten Unternehmen bei der Einführung moderner Arbeitsweisen besonders achten?*

**Christian Malzacher:** Immer wieder beobachten wir in unseren Kundenprojekten, dass sich viele noch gar nicht darüber im Klaren sind, welche technologische Entwicklung Ihnen einen echten Vorteil bringen kann. Ob es sich dann um eine Shared-Desk-Lösung handelt, Prozesse und Arbeitsabläufe digitalisiert werden oder Virtual- und Augmented Reality zum Einsatz kommt, hängt einzig von den individuellen Anforderungen der Unternehmen und Organisationen ab. Notwendig sind jedoch immer passgenaue Konzepte, ein zuverlässiger Partner in der Umsetzung und nicht zuletzt natürlich auch moderne Technologien. So stellen Sie Ihre Arbeitsumgebung zukunftssicher auf und schaffen die strukturellen Voraussetzungen für digitale Arbeitsplätze – und damit für eine zukunftsgerichtete, agile Arbeitswelt.

**Ulrich Parthier:** *Der moderne Arbeitsplatz sollte produktiv, flexibel und sicher sein. Wie sieht dafür die beste Strategie aus?*

**Christian Malzacher:** Es ist verständlich, dass Unternehmen zunehmend mehr in die Digitalisierung von Geschäftsprozessen und Lösungen investieren, welche die Zusammenarbeit erleichtern und auch verteilte Teams produktiver machen. Die steigende Nachfrage der Angestellten nach Möglichkeiten, hybrid oder gänzlich mobil arbeiten zu können, setzt Unternehmen dabei zusätzlich unter Druck. Produktiv, flexibel und sicher – dieser Dreiklang beschreibt die Anforderungen von Mitarbeitenden und Unternehmen an einen modernen digitalen Arbeitsplatz letztlich am besten. Bei der Umsetzung dieser von allen Seiten auf Unternehmen einwirkenden Anforderungen gilt es jedoch, geplant vorzugehen. „Den Wandel ganzheitlich sehen", beschreibt daher auch unser Vorgehen sehr gut. Erst auf Basis eines auf Ihre Bedürfnisse perfekt zugeschnittenen Zielbilds des modernen Arbeitsplatzes kann eine passgenaue IT-Roadmap erstellt werden, bei der nicht nur die benötigten Hard- und Software-Lösungen implementiert werden. Eine gute Strategie bezieht die Angestellten frühzeitig mit ein und begleitet so den Wandel des Mindsets weg von der klassischen Arbeitswelt hin zum zukunftsorientierten Denken erfolgreicher Unternehmen. Im besten Fall ist auch die Zeit nach dem Rollout in der Roadmap bedacht. Exklusive Supportleistungen und standardisierte Managed-Services-Angebote können so langfristig für eine hohe Akzeptanz seitens der Belegschaft und eine grundlegende Entlastung der IT sorgen.

**Ulrich Parthier:** *Modern Deployment, Hybrid Meeting - wie genau*



**PLUS**

Bechtle Modern Workplace:
**bit.ly/3Ya3BNv**

Future of Work – Services and Solutions:
**bit.ly/3HGEQDd**

*unterstützt Bechtle Unternehmen bei diesen Herausforderungen?*

**Christian Malzacher:** Unsere hervorragend vernetzte Community aus erfahrenen Expert:innen und zahlreichen Herstellerpartnern verfügt über das nötige Know-how, diesen Anforderungen die am besten geeigneten Lösungen gegenüberzustellen. Ein Leadership-Team treibt unsere Fokusthemen, die sechs Säulen des modernen Arbeitens, herstellerübergreifend voran und füllt unseren Anspruch mit Leben: der Technologiepartner zu sein, der auf alle Fachfragen zum kompletten IT-Lifecycle die richtige Antwort hat.

Modern Deployment und Management sorgt vor allen Dingen in den chronisch überlasteten IT-Abteilungen für die dringend notwendige Arbeitserleichterung. Unterschiedliche Plattformen zu verwalten und zu warten, wird so einfach wie die Einrichtung eines Smartphones. Eine perfekt abgestimmte Cloud-Strategie und Zero-Trust sorgen für den zuverlässigen und sicheren Betrieb der Endgeräte. Denn schon heute arbeitet der Großteil der Beschäftigten mobil. Immer mehr Besprechungen finden in hybriden Settings statt, bei denen ein Teil der Kolleg:innen vor Ort ist, während der andere im Homeoffice oder an verschiedenen Standorten arbeitet. Klar ist, dass auch in Zukunft kein Weg an diesen Modern Meetings vorbeiführt. Meeting-Räume und Arbeitsplätze müssen darauf vorbereitet sein, damit sie hybride Meetings schnell, zuverlässig und qualitativ hochwertig ermöglichen.

? **Ulrich Parthier:** *Die neue Arbeitswelt birgt auch Risiken, angefangen bei unsicheren Endgeräten. Doch ohne Kommunikation geht es nicht. Was raten Sie Unternehmen?*

**Christian Malzacher:** Unter dieser neuen, dezentralen Organisation der Angestellten kann im schlimmsten Fall tatsächlich die Kommunikation leiden. Unified-Communication-Plattformen bieten Unternehmen dann die Möglichkeit, unterschiedlichste Devices einfach zu kombinieren. Mit einer durchdachten Modern-Communication-Lösung kann die vorhandene Infrastruktur in moderne Kommunikations- und Teamwork-Tools integriert werden. So ist für eine verbesserte Kommunikation auch in verteilten Teams gesorgt. Effiziente, moderne Kommunikation ist mehr als nur ein neues Telefon oder ein schickes Smartphone. So kann auch eine gut integrierte Extended-Reality-Lösung Ihre Expert:innen dabei unterstützen, die Techniker:innen vor Ort durch notwendige Schritte während der Inbetriebnahme von Geräten zu führen, ohne selbst vor Ort sein zu müssen. Aber auch bei Schulungen, in der Produktentwicklung und bei neuartigen virtuellen Meetings bringen AR- und VR-Lösungen entscheidende Mehrwerte.

? **Ulrich Parthier:** *Die Digitalisierung schreitet nun ja schon eine Weile voran und das beispielsweise viel besprochene papierlose Büro hat sich nicht wirklich durchgesetzt. Was macht Ihrer Meinung nach die Zukunft der Arbeit wirklich aus?*

**Christian Malzacher:** Das papierlose digitale Büro kann mehr als lediglich Dokumente digital verwalten. Als Grundlage für modernes Arbeiten steht die Digitalisierung wichtiger Prozesse unter anderem für die HR- und Rechtsabteilung. Moderne Raumkonzepte, die auf hybrides Arbeiten ausgelegt sind und bequem von überall buchbare Shared-Desk-Lösungen unterstützen, sowie die digitale Signatur gehören schon heute zu den Anforderungen an den Arbeitsplatz der Zukunft. Moderne Technologien verändern mit ihren Möglichkeiten die Art und Weise, wie wir zusammenarbeiten, nachhaltig. All diese Tools und die damit verbundenen neuen Arbeitsweisen können aber nur dann zum Unternehmenserfolg beitragen, wenn sie von den Anwender:innen auch genutzt werden. Ein solides Konzept bei der User Adoption und beim Change Management begleitet die Mitarbeitenden in allen Bereichen eines Unternehmens beim digitalen Wandel und der Einführung neuer Tools und Arbeitsweisen.

? **Ulrich Parthier:** *Ein mit neuester Technologie ausgestatteter, moderner Arbeitsplatz hilft beim Recruiting, stärkt die Personalbindung, steigert die Produktivität und sichert das Geschäft. Doch wie setzen Sie das in Ihrem Unternehmen um?*

**Christian Malzacher:** Das ist eine berechtigte Frage, bei deren Beantwortung wir Unternehmen gerne unterstützen. Dafür haben wir uns bei Bechtle etwas ganz Besonderes überlegt: eine Umgebung, in der moderne Techniken bereits ganzheitlich im Einsatz sind – unsere Bechtle Digital Workplaces. An zehn Standorten zeigen wir verschiedenste, bereits in der Praxis erprobte und umgesetzte Lösungen. Vereinbaren Sie Ihren persönlichen Beratungstermin.

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


# Hybrid Working

## HYBRIDES ARBEITEN IST KEIN SELBSTLÄUFER

Zurück im Büro – und alles läuft einfach so weiter, wie vor wenigen Jahren? Diese Vorstellung greift zu kurz. Denn die Arbeitsweise in Unternehmen hat sich grundlegend gewandelt: Mitarbeiter:innen nutzen flexibel die Räumlichkeiten im Unternehmen und arbeiten mobil von zuhause.

Hybrides Arbeiten ist hier das Stichwort – das erleben wir bei Bechtle, sehen diese Entwicklung aber auch bei unseren Kunden. Die Herausforderung: Zwar steht Technik für das Arbeiten von überall bereit – doch damit ist es längst nicht getan. Gerade in hybriden Teams muss Kommunikation und Zusammenarbeit neu gedacht werden. Im Folgenden beleuchte ich drei Aspekte des Austauschs in hybriden, virtuellen Teams. Erfahren Sie mehr über mögliche Herausforderungen und wie Sie diese erfolgreich meistern.

### #1 Auf die Struktur kommt es an: individuelle Guiding Principles

Unternehmen, die hybrides Arbeiten leben und mit Change-Prozessen begleiten, sind, im Gegensatz zu anderen Firmen, die nur die Möglichkeit oder die passende technische Ausstattung bereitstellen, klar im Vorteil. Für mich ist der ganzheitliche Ansatz ein wichtiger Erfolgsfaktor, den viele Unternehmen bislang vernachlässigen. Zwar gibt es in den meisten Firmen Vorschriften, wie oft einzelne Mitarbeiter:innen das Homeoffice nutzen können. Darüber hinaus haben aber nur wenige die Zusammenarbeit in der hybriden Arbeitswelt weiter ausdefiniert. Wichtig finde ich, dass es Leitlinien für das ganze Unternehmen gibt. Dieses lockere Regelwerk muss einen ersten grundsätzlichen Rahmen vorgeben – gerade für Themen wie den Aufbau von Meetings oder die Nutzung von Kommunikationswegen und Technik.

Der Orientierungsrahmen sollte im ersten Schritt auf höchster Ebene ausgearbeitet und umgesetzt werden. Bei unseren Kunden sehe ich aber wie schwer es ist, allgemeine Regelungen für die ganze Firma aufzusetzen. Ein vorgegebenes, zentral erarbeitetes Regelwerk erfüllt oft nicht die Erfordernisse der verschiedenen Bereiche. So stellt die Marketingabteilung andere Anforderungen an Kommunikationswege wie beispielsweise die Produktion. Vielmehr sollten die Guiding Principles so etwas wie der „Stein des Anstoßes" sein, der die einzelnen Abteilungen und Teams dazu bewegt, sich individuell Gedanken zu ma-

chen. Jedes Team sollte die Regeln nach seiner Arbeitsweise adaptieren und nochmals optimieren – dieses Vorgehen holt meiner Erfahrung nach die Mitarbeiter:innen am besten ab und erleichtert die hybride Zusammenarbeit.

**Der Mensch zählt: Selbstfürsorge wird immer wichtiger.**

In der hybriden Arbeitsweise liegen viele Chancen: Mitarbeitende müssen weniger an andere Standorte oder zu Kunden reisen, können sich rund um den Globus besser vernetzen und sparen lange Anfahrtswege ins Büro – um nur einige zu nennen. Aber hier liegen auch Herausforderungen. Viele berichten beispielsweise, dass sie von einem Termin in den nächsten springen. Die Folge: ungesunder Dauerstress. Umso wichtiger ist es, den Faktor Mensch beim hybriden Arbeiten zu berücksichtigen. Mitarbeitende benötigen ausreichend Pausen, müssen sich genügend bewegen und auf die Arbeitszeit an sich achten.

Dabei muss jede einzelne Person die eigenen Bedürfnisse im Blick behalten. Im Homeoffice ist die Trennung zwischen Beruf und Freizeit zunehmend fließend. Auch der Arbeitsweg, eine Zeit, in der sich Mitarbeitende bewusst auf die Arbeit einstellen oder von ihr wieder Abstand nehmen, entfällt vermehrt. Das Thema Self-Awareness wird darum immer wichtiger. Für mich sind hier auch die Unternehmen in der Pflicht, den Mitarbeitenden die notwendigen Werkzeuge an die Hand zu geben. Sie müssen dafür sensibilisieren, auf die eigenen Bedürfnisse zu achten. Das kann in Form von Seminaren, Workshops oder Teamevents geschehen – aber auch Technologie kann unterstützen, ein Gefühl für die Arbeitszeit zu bekommen. Mittlerweile gibt es Tools wie Viva Insights oder Viva Suite von Microsoft zur individuellen und bewussten Selfreflektion. So können alle am Ende eines Arbeitstages für sich sehen, wie lange sie wirklich gearbeitet haben, wie viele E-Mails sie bekommen und ob sie genügend Pausen gemacht haben. Wichtig ist

> WIR UNTERSTÜTZEN UNSERE KUNDEN DABEI, WIEDER STRUKTUR IN IHRE KOMMUNIKATION UND TOOL-LANDSCHAFT ZU BEKOMMEN.
>
> Florian Vees, Consultant, Bechtle AG, www.bechtle.com

dabei, dass vorgesetzte Personen mit gutem Beispiel vorangehen und die Selbstfürsorge auch leben.

Darüber hinaus sollten Unternehmen die Mitarbeitenden rechtzeitig mit ins Boot holen. Denn am Ende ist es wichtig, dass die Anwender:innen die neuen Möglichkeiten auch nutzen. Größere Unternehmen setzen hier meist auf strukturierte User Adaption – kleinere Firmen haben oftmals nicht die notwendigen Ressourcen im Haus. Dann begleiten wir als IT-Partner diesen wichtigen Schritt und stellen so sicher, dass Mitarbeitende neue Arbeitsweisen und technologische Unterstützung verstehen – und auch wirklich gewinnbringend nutzen.

**Die Technik muss stimmen: reibungslose Zusammenarbeit.**

Natürlich ist am Ende die Technologie entscheidend, um reibungslose Zusammenarbeit und moderne Kommunikation zu ermöglichen. Egal, wo ich als Mitarbeitender sitze: Ohne geeignete Grundausstattung sind hybride Arbeitskonzepte nicht zu realisieren. Bei unseren Kunden sehen wir, dass mittlerweile so gut wie alle Unternehmen ihren Mitarbeitenden die passende Ausstattung für agiles Arbeiten zur Verfügung stellen. Doch durch hybride Arbeitsmethoden ergeben sich neue Herausforderungen – gerade was das Thema Meetings angeht. Eine rudimentäre Meetingraum-Ausstattung reicht heute beispielsweise nicht mehr für erfolgreiche hybride Meetings aus. Hier liegt dringender Handlungsbedarf. Es lohnt sich für Unternehmen schnell, auf moderne Meetingraum-Konzepte und die passende Ausstattung ihres Teams zu setzen.

Ein weiterer Punkt ist die Flut an unterschiedlichen Tools, die viele Unternehmen nutzen. In der Pandemie wurden oftmals neue Kommunikationswege wie Plattformen und Chats eingeführt. Was viele dabei vergessen haben: diese zu verknüpfen oder deren Nutzung strategisch zu definieren. Die Folge ist ein Tool-Chaos. Die meisten Teams werden ineffektiv, wenn sie über viele verschiedene Wege und ohne klare Regelungen miteinander kommunizieren. Wir unterstützen unsere Kunden dabei, wieder Struktur in ihre Kommunikation und Tool-Landschaft zu bekommen. Dafür betrachten wir im ersten Schritt den Status quo, die unterschiedlichen Kommunikationswege und erarbeiten gemeinsam die erwähnten Guiding Principles.

Zusammenfassend kommt es für mich darauf an, alle Aspekte miteinander zu vereinen, um hybride Zusammenarbeit erfolgreich gestalten zu können. Dazu gehören: die passende Technologie in Form von Soft- und Hardware sowie eine moderne Firmenphilosophie, die hybrides Arbeiten wirklich ermöglicht und unterstützende Guiding Principles bereitstellt. Und nicht zuletzt die Schulung und Begleitung von ganzen Teams und einzelnen Mitarbeitenden, um sie an veränderte Arbeitsweisen heranzuführen. Nur so können Unternehmen sicherstellen, dass die zwischenmenschliche Kommunikation auch in der hybriden Arbeitswelt funktioniert und Teams effizient zusammenarbeiten.

***Florian Vees | www.bechtle.com***

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

SCAN ME

https://www.it-daily.net/office/

SAVE THE DATE

#Office4.0

# Office 4.0

## 26. April 2023
## Digitalevent

# „Frei im Kopf“ heißt nicht „Hirn aus“!

## ERFOLGREICH DIGITALISIEREN

Schneller bessere Ergebnisse erzielen, passgenaue Angebote schaffen, Daten intelligent nutzen – durch die Digitalisierung versprechen sich Unternehmen nicht weniger als eine neue Art zu arbeiten. Die Idealvorstellung: Wenn Mitarbeitende weniger Zeit für Routinetätigkeiten aufwenden, haben sie den Kopf frei für Kreativität, Innovation und Projekt-Power. Was in der Realität machbar ist, wissen die Experten Mario Koch und Martin Schwaier vom Technologie- und Managed-Service-Provider Konica Minolta.

**it management:** *Herr Koch, Ihr Team unterstützt Unternehmen bei der Digitalisierung – etwa durch die Einführung von ECM-Systemen. Werden deren Mitarbeitende dann automatisch „frei im Kopf“?*

**Mario Koch:** Um wirklich anders zu arbeiten, reicht es nicht, sich auf IT-Lösungen zu verlassen. Es geht auch um das Zusammenspiel von Methoden, Organisation und Prozessen. Wir geben unseren Kundinnen und Kunden Werkzeuge an die Hand, mit denen sie ihre Mitarbeitenden von stupiden oder sich wiederholenden, administrativen Arbeiten befreien können. So wird etwa die Projektarbeit einfacher: Vor einem Meeting müssen die Teilnehmenden nicht alle nötigen Informationen zusammensuchen – die relevanten Dokumente sind kontextbezogen schon da.

**it management:** *Herr Schwaier, Sie sind seit einigen Jahren dafür verantwortlich, dass die Digitalisierung auch im Hause Konica Minolta weiter vorangeht. Wie sind Sie am Anfang vorgegangen?*

**Martin Schwaier:** Wir haben uns zunächst einzelne Bereiche oder Vorgänge angesehen und in verbesserte Prozesse überführt. Zum Beispiel die digitale Kunden- und Auftragsakte. Früher waren Informationen über ERP-, CRM- und andere Systeme verteilt und nicht miteinander verknüpft. Es fehlte eine Schicht, die alle Infos kontextbezogen zur Verfügung stellt – in einer leicht verständlichen Form. Heute können zum Beispiel unsere Vertriebs-Teams vom ersten Telefonat übers Angebot bis zur Rechnung alle Informationen auf einen Blick einsehen. Dadurch sind sie sofort aussagekräftig und müssen nicht erst die fehlenden Fakten zusammensuchen.

ES IST ENORM WICHTIG, MITARBEITENDE IN ENTSCHEIDUNGSPROZESSE EINZUBEZIEHEN UND IHNEN EIGENVERANTWORTUNG ZU ÜBERTRAGEN, UM IHR ENGAGEMENT UND IHRE MOTIVATION WEITERHIN ZU FÖRDERN.

**Martin Schwaier,**
**Manager Digital Business Process Innovation & Transformation,**
**Konica Minolta Deutschland,**
**www.konicaminolta.de**

**it management:** *Welcher Schritt der Digitalisierung war für Ihr eigenes Team der entscheidende?*

**Martin Schwaier:** Der vollständige Umstieg auf die Microsoft 365-Welt war ein Quantensprung. Und dass, obwohl wir als Tech-Abteilung ohnehin seit Jahren virtuell oder hybrid zusammenarbeiteten. Vorher hatte es nie reibungslos geklappt, verschiedene Anwendungen und Werkzeuge nahtlos miteinander zu verknüpfen; irgendein Baustein hat immer gefehlt. Heute sind über MS Teams meine Leute mit ihren Aufgaben und allen relevanten Infos immer und überall verbunden, können alles mobil aufrufen und nutzen. Diese Plattform für die digitale Zusammenarbeit ist jeden Cent wert, denn sie kann ein Game Changer sein.

**it management:** *Apropos: Welche aktuellen Trends haben großes Potenzial, die Arbeit in Unternehmen zu verändern?*

**Mario Koch:** Ein Trend geht im Moment zu 80/20-Best Practice-Ansätzen. Es ist nicht lange her, dass wir mit komplizierten Showcases in die Unternehmen gegangen sind, um möglichst EINE Lösung für ALLE Probleme zu bieten. Heute bekommen wir oft Anfragen für ganz konkrete Herausforderungen oder Prozesse, die schnell und einfach digitalisiert werden sollen. Wir bieten dann Tools an, die bereits 80 Prozent der Arbeit automatisch erledigen. Damit sich die Mit-

arbeitenden auf die restlichen 20 Prozent, die komplexen Fälle, voll konzentrieren können. Durch Low-Code-Lösungen können die Unternehmen dann sogar selbstständig ihre Prozesse in Vertrieb, Logistik, Recruiting, oder Personal weiterentwickeln.

**it management:** *Was bedeutet Low-Code?*

**Mario Koch:** Um die heutigen Tools perfekt auf die Prozesse in Unternehmen anzupassen, braucht es häufig keine großen Programmierkenntnisse. Die Hürde, selbst Prozesse zu digitalisieren, ist sehr niedrig – deswegen Low-Code. Oft sind auch gar keine Kenntnisse mehr nötig, dann reden wir von No-Code-Lösungen.

**Martin Schwaier:** Wir haben damit viele positive Erfahrungen gemacht. So steht nämlich nicht mehr die Technik im Fokus, sondern die Prozesse und die Arbeitserleichterung. Mein IT-Team setzt die Rahmenbedingungen, mit denen die Business-Teams selbst in kurzer Zeit professionelle Lösungen schaffen.

**it management:** *Ein weiterer großer Trend ist die künstliche Intelligenz (KI). Welche Potenziale stecken darin?*

**Martin Schwaier:** Wir bei Konica Minolta nutzen KI bereits seit Längerem. Etwa bei der Digitalisierung von Eingangsrechnungen, die automatisch Daten wie Positionen und Vorgangsnummern erfasst und den richtigen Abteilungen und Akten zuordnet.

**Mario Koch:** Privat-Nutzer kennen das vielleicht von ihrer Banking-App, wo sie nur noch die Rechnung fotografieren. Durch maschinelles Lernen werden die Ergebnisse immer besser. In der KI steckt auch viel Potenzial zur Unterstützung bei der Kommunikation mit Kundinnen und Kunden. Mit intelligenten Chatbots können Standard-Anfragen in Zukunft schnell und korrekt beantwortet werden. Aktuell heißester Trend in allen Bereichen ist ChatGPT, welcher Texte formulieren, argumentieren und sogar Programmcode schreiben kann.

WER ERFOLGREICH DIGITALISIEREN WILL, MUSS DIE MITARBEITENDEN VON ANFANG AN MITNEHMEN – ERST MIT KLEINEN SCHRITTEN UND DANN MIT RAUM FÜR KREATIVITÄT.

**Mario Koch, Head of ECM, Konica Minolta Deutschland, www.konicaminolta.de**

**it management:** *Kritische Stimmen befürchten, dass wir durch den Einsatz der KI langfristig das eingeständige Denken verlernen.*

**Mario Koch:** Bedenklich wird es nur dann, wenn wir die KI einfach laufen lassen. Das ist wie beim Navigationssystem, durch das wir nicht mehr wissen, welchen Weg wir genommen haben. Dabei ist in der Vergangenheit durchaus das ein oder andere schiefgelaufen. Daher müssen wir die Antworten und Thesen kritisch bewerten und als „Vorschlag" verwenden, das Denken aber nicht vergessen.

**Martin Schwaier:** Es wird auch zunehmend darum gehen, die KI richtig zu trainieren und zu überwachen. Wenn sich erstmal ein Fehler oder Bias einschleicht, und sei es nur eine falsch zugeordnete Nummer, wird die KI annehmen, richtig zu handeln – und schlimmstenfalls auf das falsche Konto überweisen. „Frei im Kopf" heißt eben nicht „Hirn aus"! Auch wenn Standard-Tätigkeiten automatisch ausgeführt werden, müssen die Mitarbeitenden sie weiterhin durchblicken.

**it management:** *Wie gelingt es, dass die Mitarbeitenden zugleich auch die Bereitschaft für Veränderungen behalten?*

**Mario Koch:** Wer erfolgreich digitalisieren will, muss die Mitarbeitenden von Anfang an mitnehmen – erst mit kleinen Schritten und dann mit Raum für Kreativität. Es geht los mit kleinen Prozessen und Tools, damit die Mitarbeitenden erkennen, was alles möglich ist. Wenn dann die Fachbereiche die richtigen Werkzeuge und Rahmenbedingungen erhalten, werden sie sich schnell selbst ausprobieren. Lassen Sie die Mitarbeitenden machen, der Appetit kommt beim Essen!

**Martin Schwaier:** Ich kann das von Mario Gesagte nur unterstreichen, es ist enorm wichtig, Mitarbeitende in Entscheidungsprozesse einzubeziehen und ihnen Eigenverantwortung zu übertragen, um ihr Engagement und ihre Motivation weiterhin zu fördern. Wenn es die Teams nicht längst mit Low-Code-Lösungen im Rahmen der Leitlinien umgesetzt haben.

**it management:** *Von der Digitalisierung mal abgesehen: Was macht wirklich frei im Kopf?*

**Martin Schwaier:** Simplizität, Entschleunigung – und ganz entspannt mit meinem Sohn spielen.

**Mario Koch:** Bei aller KI und Automatisierung: Digital Detox in der Freizeit ist auch wichtig.

**it management:** *Herr Schwaier, Herr Koch, danke für das Gespräch.*

# Office 4.0

## IN 4 SCHRITTEN ZU EINEM BENUTZERFREUNDLICHEREN SELF SERVICE

Die Digitalisierung hat gerade rasante Fortschritte gemacht und so das traditionelle Arbeitsleben auf den Kopf gestellt. Mobiles Arbeiten und keine festen Büroarbeitsplätze sind nur zwei Komponenten des Themas Office 4.0. Hierbei konzentrieren sich Unternehmen stärker auf mobile und flexible Arbeitsumgebungen, so dass Mitarbeiter rein theoretisch von überall aus arbeiten könnten. Dies wird durch die Verwendung von Cloud-Technologien, Self Service Portalen und mobilen Geräten, die Zugang zu Unternehmensressourcen bieten, ermöglicht. Gerade ein gut gepflegtes Self Service Portal ist dabei perfekt als Single-Point-of-Contact für Ihre Serviceabteilungen. Damit es aber von allen Mitarbeitern genutzt wird, gilt es ein paar Regeln zu befolgen. Wir haben vier Tipps, wie Ihr Self Service Portal Sie bei Office 4.0 unterstützen kann.

**1.Optimieren Sie das Nutzererlebnis Ihres Self Service Portals**

Serviceabteilungen sind für guten Service und nicht für Verwirrung zuständig. Ist Ihr Portal nicht benutzerfreundlich, stehen Sie direkt vor einem Problem. Das Marketing kümmert sich darum das Serviceerlebnis zu optimieren und genau darauf sollten Sie sich auch konzentrieren. Ihr Hauptziel während des Design-Prozesses sollte sein, das Nutzererlebnis Ihres Portals so reibungslos wie möglich zu gestalten. Letztendlich existiert das Portal für Ihre Mitarbeiter. Wenn diese vom Layout verwirrt werden, haben Sie das Ziel eines klaren, einfachen Self Service nicht erreicht. Daher empfiehlt es sich vor dem Portal-Start Mitarbeiter mit ins Boot zu nehmen und Anwendungsfälle durchzuspielen – so sehen Sie ganz schnell, wo noch Stolpersteine liegen.

**2.Denken Sie sowohl an „Klicker" als auch „Sucher"**

Wenn Sie sich Gedanken über das Nutzererlebnis machen, sollten Sie nicht vergessen, dass Menschen sich unterschiedlich verhalten. Manche Menschen sind „Klicker", die sich durch Seiten klicken und diese durchstöbern, bis sie die Antwort finden. Andere sind „Sucher", die schnell eine Antwort brauchen und diese am liebsten „googeln". Stellen Sie daher sicher, dass Ihr Portal über eine Suchfunktion verfügt. Denken Sie daran, Einträge untereinander zu verlinken, damit „Klicker" leicht durch das Portal navigieren können.

**3. Sprechen Sie die Sprache Ihrer Mitarbeiter**

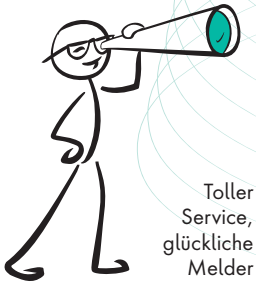
Das ist in Bezug auf das Nutzererlebnis ein sehr wichtiger Punkt. Ihre Mitarbeiter sprechen weder die Servicesprache, noch wissen sie genau, mit welcher Art Fehler sie sich gerade herumschlagen. Damit Sie die Nutzerfreundlichkeit Ihres Portals verbessern, sollten Sie immer versuchen, die Einträge so zu betiteln, dass auch Laien verstehen können, worum es geht. Statt „Anfrage für Arbeitsplatz-Materialien" sollten Sie zum Beispiel besser „Ich brauche neues Equipment " als Titel wählen. Auch hier empfiehlt es sich regelmäßig zu prüfen, welche Begriffe Ihre Mitarbeiter nutzen und diese im Portal anzupassen.

**4.Nutzen Sie ein Portal für mehrere Abteilungen**

Kommen wir auf den „Mitarbeiter nicht verwirren"-Punkt zurück. Ihre Mitarbeiter wissen nicht immer, an welche Abteilung sie sich wenden sollen. Ihr Service Portal sollte den Anwendern bei der Auswahl helfen. Wenn Sie Enterprise-Servicemanagement umsetzen möchten, also dass Abteilungen wie Facility, Personal oder IT zusammenarbeiten, sollten Sie auch ein gemeinsames Service Portal einrichten.

So haben Ihre Mitarbeiter einen Single-Point-of-Contact ohne nachdenken zu müssen an wen die Anfrage zu richten ist. Im Hintergrund laufen die Prozesse automatisiert über das Changemanagement ab.

***www.topdesk.de***



**PLUS**

Toller Service, glückliche Melder

# RECHENZENTREN IM WANDEL

THOUGHT LEADERSHIP

**Wie heißt es so schön: nichts ist beständiger als der Wandel. Wie wahr. Der Innovationsdrang der IT beflügelt das gesamte Wirtschaftsleben. Denken Sie nur an völlig neue Themen wie Blockchain, NFT, Metaverse. Aber auch in der „old economy" der IT tut sich viel. Lösungen erweitern sich, verschmelzen oftmals miteinander. Ein gutes Beispiel dafür ist die Frage, wie es mit DCIM-Lösungen (Data Center Infrastructure Management) weitergeht.**

**Auch sie sind vor Wandel nicht gefeit. Wir stellen heute die Frage: gibt es Alternativen?**

# DCIM oder Monitoring?

## „DER BETRIEB EINES RECHENZENTRUMS BRAUCHT EINE DCIM-LÖSUNG." IST DAS SO? ODER GEHT ES MANCHMAL AUCH EINFACHER, GÜNSTIGER UND VOR ALLEM EFFIZIENTER?

DCIM-Lösungen (Data Center Infrastructure Management) sind Systeme, die in Rechenzentren eingesetzt werden, um die Infrastruktur, sprich IT-Geräte, Gebäudetechnik, Stromversorgung, Temperatur und Platz zu überwachen, zu steuern und zu verwalten. Sie erstellen Berichte zu Verfügbarkeit, optimieren die Ressourcenauslastung und liefern die Datengrundlage für Kapazitätserweiterungen und Upgrades. Die Vielzahl der Funktionen macht DCIM-Systeme häufig komplex und damit schwer bedienbar und langsam (und teuer). Gerade die Überwachung eines Rechenzentrums erfordert aber schnelle Reaktionszeiten. SLA-Verletzungen können hohe Strafzahlungen nach sich ziehen und ein nicht zeitnah entdeckter Ausfall kann schwerwiegende Folgen haben.

DCIM BEDEUTET MEHR ALS NUR DAS ÜBERWACHEN VON VERFÜGBARKEIT DER RZ-KOMPONENTEN. PROFESSIONELLE DCIM-TOOLS LIEFERN AUSWERTUNGEN UND BERICHTE ZUM ZUSTAND DES RECHENZENTRUMS, AUTOMATISIEREN PROZESSE UND UNTERSTÜTZEN BEI DER KAPAZITÄTSPLANUNG.

**Thomas Timmermann, Senior Market Expert, Paessler AG, www.paessler.com**

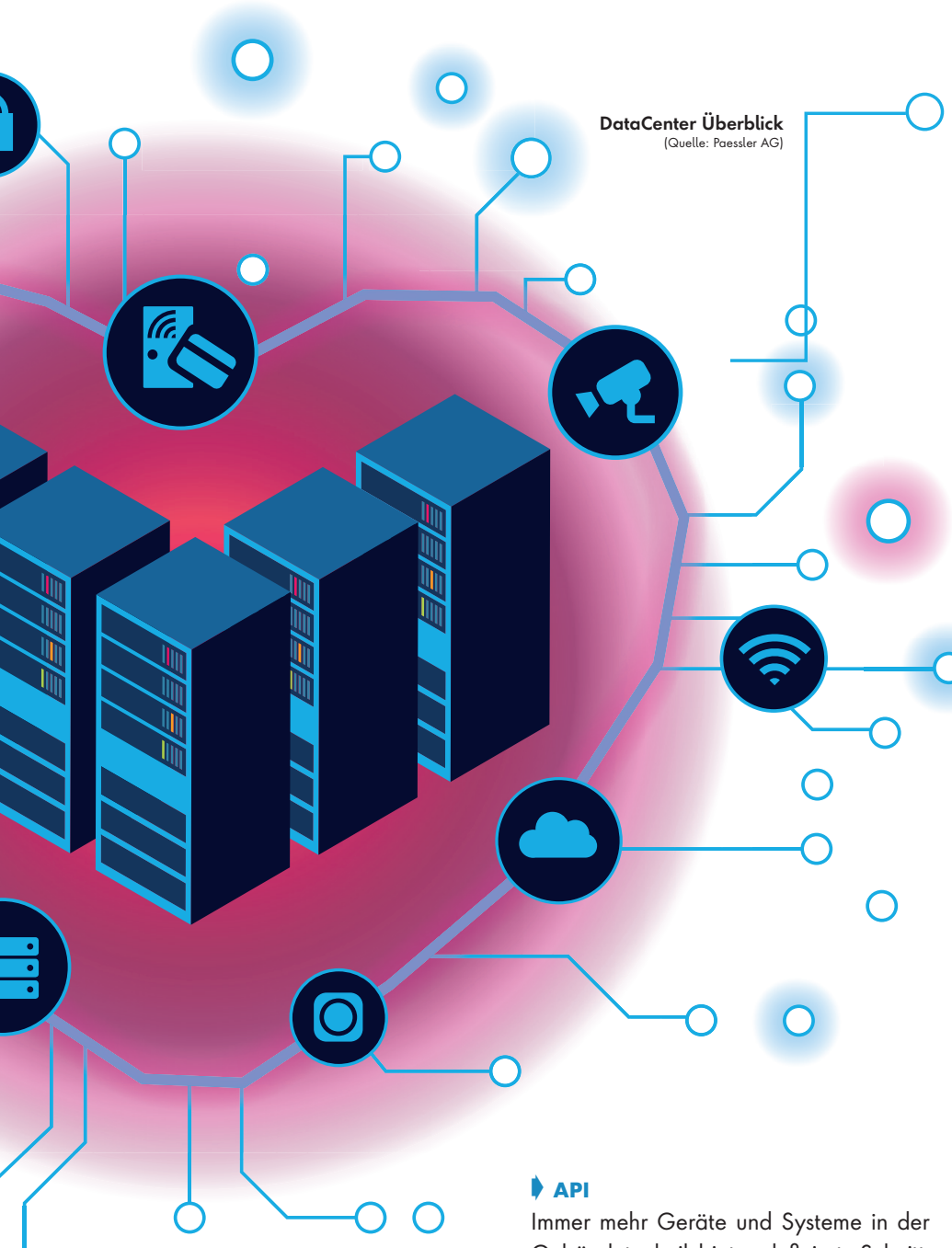
Hier kommen Monitoring-Tools ins Spiel. Klassische IT-Monitoring-Lösungen legen den Fokus auf Monitoring und auf Geschwindigkeit. Viele Monitoring-Lösungen können nahezu in Echtzeit reagieren und sind dank ihres klar umrissenen Aufgabenschwerpunkts noch relativ einfach und bedienbar und auch preislich günstig. Die ermittelten Monitoring-Daten lassen sich auch für Aufgaben einsetzen, die eigentlich in den Aufgabenbereich von DCIM-Lösungen fallen. Das können Berichte zur Ressourcenauslastung und zur Kapazitätsplanung sein oder die Automatisierung von Prozessen. Allerdings eignet sich nicht jede IT-Monitoring-Lösung auch für die Überwachung eines Rechenzentrums und für die Übernahme der erweiterten RZ-Management-Anforderungen.

### MONITORING IM RECHENZENTRUM

Nur ein Teil der RZ-Infrastruktur lässt sich mit klassischen IT-Mitteln wie SNMP, WMI oder Syslog hinreichend überwachen. Das funktioniert in der Regel für Hardware bei Storage-Systemen, Servern oder Netzwerkgeräten, manchmal auch noch bei Geräten zur Stromversorgung (USV) oder Umwelt-Sensorik (Temperatur, Luftfeuchtigkeit, Rauchmelder, Türschließanlagen...). Viele RZ-Komponenten sind allerdings nicht mit IT-Protokollen kompatibel, sondern können nur über spezielle Protokolle und Methoden abgefragt werden, die DCIM-Systeme in der Regel beherrschen. Im Wesentlichen sind das:

- **Modbus**

In der Gebäudetechnik ist Modbus im europäischen Raum wohl das verbreitets-



**DataCenter Überblick**
(Quelle: Paessler AG)

te Protokoll für die Kommunikation zwischen Überwachungssystemen und Gebäudekomponenten wie Klimaanlagen, Sicherheitskameras oder Zutrittskontrollsystemen.

### MQTT

Aus dem IoT-Umfeld kommend spielt MQTT in der Gebäudetechnik eine immer wichtigere Rolle, da es sich besonders gut für die Übertragung von Daten in Netzwerken mit begrenzter Bandbreite und/oder hoher Latenzzeit eignet.

### API

Immer mehr Geräte und Systeme in der Gebäudetechnik bieten definierte Schnittstellen (API) über die sie Daten und Informationen zu Zustand und Leistung bereitstellen.

Solange eine IT-Monitoring-Lösung also nur klassische IT-Methoden unterstützt, eignet sie sich nur bedingt für den Einsatz im Rechenzentrum. Allerdings gibt es IT-Monitoring-Lösungen, die über reines IT-Monitoring hinaus auch entsprechende Protokolle und Methoden unterstützen, um Industrieanlagen, medizinische Infrastrukturen, IoT-Umgebungen und eben auch Komponenten der Gebäudetechnik bzw. des Rechenzentrums in das zentrale Monitoring einzubeziehen. Damit kann eine IT-Monitoring-Lösung eine wertvolle Ergänzung zu einem DCIM-System darstellen, die eine Echtzeit-Überwachung und -Alarmierung zu den Management-Funktionen des DCIM beisteuert. Aufgrund des vergleichsweise günstigen Preises, des geringen Implementierungsaufwands und der einfachen Bedienbarkeit kann sich das durchaus lohnen. Was muss eine Monitoring-Lösung aber leisten können, um tatsächlich ein DCIM-System zu ersetzen?

## MONITORING STATT DCIM?

DCIM bedeutet mehr als nur das Überwachen von Verfügbarkeit der RZ-Komponenten. Professionelle DCIM-Tools liefern Auswertungen und Berichte zum Zustand des Rechenzentrums, automatisieren Prozesse und unterstützen bei der Kapazitätsplanung. Um eine gangbare Alternative zu einem DCIM-System zu bieten, muss eine Monitoring-Lösung also mehr können, als RZ-Infrastrukturen nur zu überwachen.

### #1 Auswertung und Publikation der Daten

Der Betrieb eines Rechenzentrums misst sich am Einhalten der SLA (Service Level Agreements), vertraglich definierter Verfügbarkeit im Verhältnis zu Ausfällen, deren Verletzung meist empfindliche Strafen nach sich zieht. Eine Monitoring-Lösung muss in der Lage sein, sogenannte

SLA-Reports zu liefern, die Einhaltung oder Verletzung der SLAs berechnen und darstellen. Darüber hinaus müssen die Monitoring-Daten in Dashboards so dargestellt werden, dass Service-Techniker sich für die Behebung von Störungen oder Ausfällen räumlich orientieren können, sprich wenn eine Sicherheitskamera ausfällt, sollte auf einem Gebäudegrundriss ersichtlich sein, wo diese Kamera platziert ist und nicht einfach nur eine Identifikationsnummer der Kamera geliefert werden, die dann erst über Inventory-Tools oder Lagepläne lokalisiert werden muss.

### #2 Prozessautomatisierung

Qualifizierte Fachleute sind heute rar gesät. Das hat zur Folge, dass die Belastung des Personals in Rechenzentren oft sehr hoch ist. Eine Möglichkeit dem entgegenzuwirken ist die Automatisierung von immer wiederkehrenden Prozessen. Damit können manche Probleme direkt ohne Eingreifen eines Experten behoben werden, andere können zumindest soweit vereinfacht werden, dass auch weniger qualifiziertes Personal die Aufgabe übernehmen und lösen kann. Voraussetzung ist, dass die eingesetzte Monitoring-Lösung die Möglichkeit bietet, statt einen Alarm zu verschicken ein vorbereitetes Skript auszulösen, das dann das Problem mittels Neustart oder auch durch komplexere Aktionen behebt. Von Vorteil ist auch, wenn die Lösung mehrere Komponenten in einem Prozess zusammenzufassen und damit die Ursache eines Problems identifizieren und beheben kann. Gleichzeitig könnte eine Nachricht an die zuständigen Techniker versendet werden, so dass diese informiert sind und beurteilen können, ob und wann ein weiteres Eingreifen nötig ist.

### #3 Kapazitätsplanung

Rechenzentrum sind aufwändig und teuer. Zu viele Ressourcen (sei es in der IT, bei der Gebäudetechnik oder auch ganz simpel bei der Gebäudegröße bzw. -nutzung) verursachen unnötige Kosten, zu knappe Ressourcen können in vielerlei Hinsicht Probleme verursachen. Um Erweiterungen bedarfsgerecht planen zu können, braucht es langfristige Datenerhebung und die Möglichkeit, diese Daten auch entsprechend auszuwerten – sei es innerhalb der Lösung oder über einen Datenexport.

Unterstützt eine IT-Monitoring-Lösung die benötigte Funktionalität, dann kann sie eine interessante Alternative zu einem DCIM-System darstellen:

- Viele IT-Monitoring-Tools sind schneller und einfacher als DCIM-Systeme. Schnellere Reaktionen, weniger Aufwand und damit auch Kostenersparnis sind Argumente, die für eine solche Alternative sprechen.
- IT-Monitoring-Lösungen können neben der RZ-Ausstattung auch die IT überwachen. Die Folge ist ein ganzheitlicher Überblick, der unter Umständen auch erweiterte Ursachenforschung ermöglicht und komplexe Zusammenhänge transparent machen kann, zum Beispiel zwischen IT-Applikationen und Raumtemperatur.
- Eine Lösung für IT und RZ verringert Kosten, Aufwand und Komplexität.

Vor allem für sehr große Rechenzentren können DCIM-Systeme aufgrund der komplexen Anforderungen manchmal unersetzbar sein. Aber auch in dem Fall kann ein einfaches und unkompliziertes Monitoring oft eine perfekte Ergänzung im täglichen Betrieb und bei der schnellen Fehlererkennung und Alarmierung sein.

***Thomas Timmermann***

# SAVE THE DATE

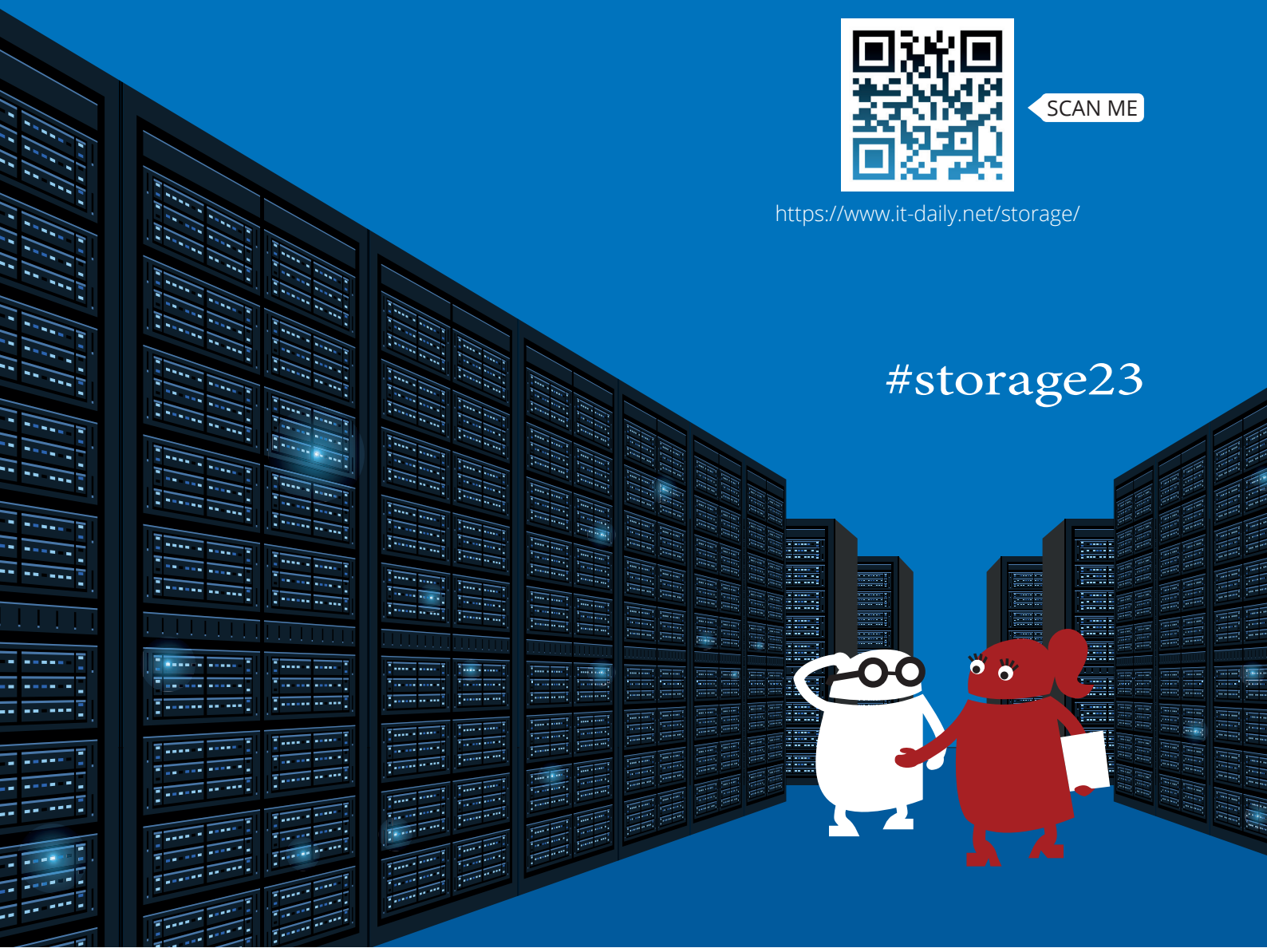
# Data Protection & Storage

*30. März 2023 | Digitalevent*

SCAN ME

https://www.it-daily.net/storage/

#storage23



Eine Veranstaltung von itmanagement & speicherguide.de Das Storage-Magazin powered by it-daily.net

# Work in Progress

## DSAG-TECHNOLOGIETAGE, 22. UND 23. MÄRZ IN MANNHEIM


„Work in Progress" lautet das Motto der Technologietage 2023 der Deutschsprachigen SAP-Anwendergruppe e. V. (DSAG). Das Motto bezieht sich auf Themen, die in den letzten Jahren angestoßen wurden. Sei es der einfache Umstieg und die Migration auf S/4HANA oder die IT-Security. Für S/4HANA gilt der Status „in Arbeit" seit mittlerweile über acht Jahren. Denn das „finale" Zielrelease soll erst in diesem Jahr auf den Markt kommen, was vielen Unternehmen den Umstieg erschwert hat oder sie immer noch zögern lässt.

„SAP muss unmissverständlich klarstellen, dass Innovationen und Weiterentwicklungen zeitnah auch den Private- Cloud- und On-Premises-Editionen von S/4HANA zugutekommen werden", erläutert DSAG-Technologievorstand Sebastian Westphal. Das wäre im Hinblick auf den Schutz der Investitionen vieler Unternehmen in kostenintensive S/4HANA-Projekte in den letzten Jahren eine wichtige Botschaft.

Unter „Work in Progress" fällt auch die Forderung der DSAG nach einem Security-Dashboard. Dabei ist das Ziel, eine Lösung einsetzen zu können, die automatisch auf sicherheitsrelevante Einstellungen und etwaige Sicherheitslücken der gesamten (hybriden) SAP-Architektur hinweist. In diesem Bereich haben wir nun zusammen mit SAP erste erfolgreiche Schritte begonnen", gibt Westphal den aktuellen Stand wieder Die zweite Phase wird sich mit den Programmierschnittstellen und den Berichtsfunktionen befassen. „Eine verbindliche Roadmap steht leider immer noch nicht, jetzt heißt es liefern", fasst Sebastian Westphal zusammen.

Die DSAG-Technologietage beleuchten den aktuellen Stand dieser und weiterer wichtiger Themen und zeigen Wege auf, um den Status von „in Arbeit" auf „erledigt" umzustellen.

***www.dsag.de/techtage***


# DIE SAP S/4HANA BUSINESS TRANSFORMATION

## MIT DIGITALISIERTEN END-TO-END- PROZESSEN DIE ZUKUNFT SICHERN

Es gibt viele Gründe für den Wechsel zu SAP S/4HANA. Dass Unternehmen heute immer größere Datenmengen bewältigen und ihre Geschäftsprozesse und -modelle flexibel an neue Rahmenbedingungen anpassen müssen, ist einer der wichtigsten. SAP S/4HANA ist die Antwort von SAP auf den digitalen Wandel und ein immer schnelllebigeres, global vernetztes Geschäftsumfeld.

SAP Kunden, die auf SAP S/4HANA umsteigen wollen, bleibt dafür allerdings nur noch wenig Zeit. 2027 soll der technische Support für ältere SAP ERP-Systeme auslaufen. Dieses Whitepaper beschreibt, welche Schritte dafür von der Planung bis zum erfolgreichen Abschluss notwendig sind, was es zu beachten und bedenken gilt und wie RISE with SAP bei der Transformation in die Cloud unterstützt.

**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 35 Seiten und steht kostenlos zum Download bereit. **www.it-daily.net/Download**

# MFA und Endpoint Security

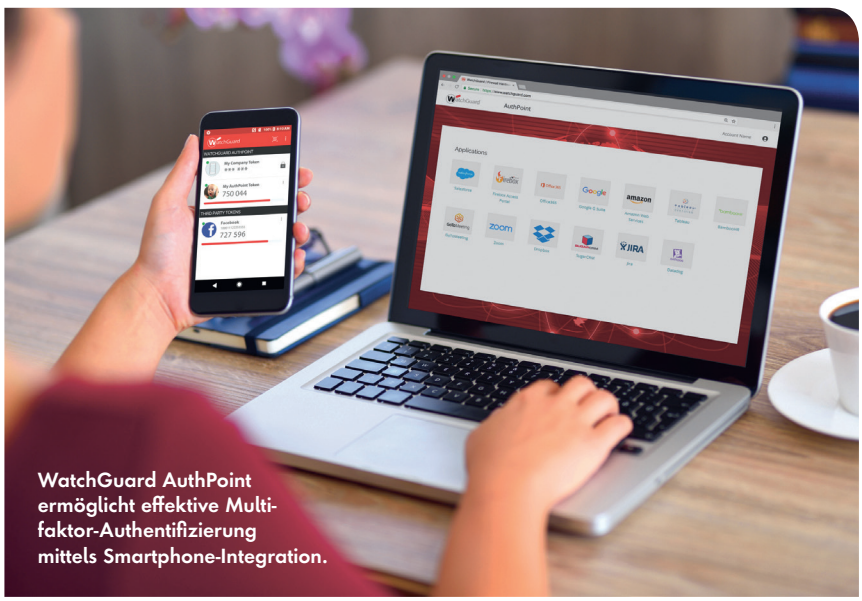
## MODERNER SECURITY-MIX

Die regelmäßige Auswertung der Gefahrenlandschaft durch die Analysten von WatchGuard bringt eindrucksvolle Ergebnisse ans Licht: Im Durchschnitt prasseln 170.000 Malware-Angriffe pro Tag auf Unternehmen weltweit ein, das entspricht über 7.000 Attacken pro Stunde. Gleichzeitig lässt auch die Betrachtung der Folgen eines erfolgreichen Übergriffs aufhorchen: Nach Angaben von IBM kostet eine Datenschutzverletzung ein Unternehmen im Durchschnitt 4,35 Millionen Dollar.

In dem Zusammenhang rücken immer wieder die gleichen Baustellen auf Unternehmensseite in den Fokus: ein nachlässiger Umgang mit Login-Daten sowie die enorm lange Zeit, die es braucht, eine Sicherheitsverletzung zu erkennen. Kein Wunder: Denn Hacker nehmen verstärkt Endpunkte ins Visier, um sich von diesen ausgehend per Seitwärtsbewegung ihrem eigentlichen Ziel zu nähern. Insofern kommt es mehr denn je auf die Einführung einer Multifaktor-Authentifizierung (MFA) in Kombination mit leistungsstarker Endpoint Security an.

**Schutzschild MFA**

Im Zuge der Gefahrenabwehr steht die Wirksamkeit der Multifaktor-Authentifizierung unter Experten außer Frage. Laut Aussage des Cybersecurity-Verantwortlichen der USA könnten mithilfe einer MFA-Implementierung 80 bis 90 Prozent der IT-Angriffe vermieden werden. Allerdings bieten nicht alle MFA-Optionen das gleiche Maß an Schutz. Cyberkriminelle wissen mittlerweile, wie sie mit ausgeklügelten Taktiken einige der am häufigsten verwendeten Methoden umgehen können. Bei der Auswahl entsprechender Lösungen sollten Unternehmen also genau auf die Details achten. Dass SMS- oder E-Mail-basierte Authentifizierungsmethoden Schwächen haben, hat die Praxis bereits mehrfach gezeigt. Dennoch sind diese bei der Mehrzahl von Unternehmen, die MFA nutzen, nach wie vor das Mittel der Wahl. Eine fortschrittliche Lösung wie WatchGuard AuthPoint, die auf Smartphone-Integration auf Basis der eindeutigen Geräte-DNA setzt, trumpft demgegenüber gleich mehrfach: sowohl im Hinblick auf die Sicherheit, als auch in Sachen Benutzerfreundlichkeit.



WatchGuard AuthPoint ermöglicht effektive Multifaktor-Authentifizierung mittels Smartphone-Integration.

Quelle: WatchGuard

**Angriffe am Endpunkt stoppen**

Gepaart mit der EPDR-Technologie von WatchGuard lässt sich die Angriffsfläche darüber hinaus massiv weiter reduzieren. Denn diese macht Cyberbösewichten, die darauf aus sind, Malware via Phishing, Social Engineering oder Ausnutzung von Lücken in Endgeräte-Anwendungen zu verteilen, von Anfang an einen zusätzlichen Strich durch die Rechnung. Per Zero Trust Application Service werden Endpunkte konsequent überwacht und unter Einsatz von künstlicher Intelligenz ausnahmslos alle Prozesse und Anwendungen klassifiziert. Nur nach der Einstufung als „vertrauenswürdig" ist eine Ausführung möglich. Mithilfe des Threat Hunting Services lassen sich zudem selbst Angriffsversuche, bei denen Hacker versuchen, Malware mit fortschrittlichen Taktiken und legitimen Tools unbemerkt einzuschleusen, stichhaltig aufdecken und abwehren.

**Mehrwert Unified Security**

Bei WatchGuard ist der besondere Pluspunkt: Die Unified Security Platform-Architektur ermöglicht ein umfassendes, einfaches, automatisiertes und intelligentes Management umfangreicher Security-Funktionalität – inklusive Multifaktor-Authentifizierung, Endpoint Security, Netzwerkschutz und WLAN. Das nahtlose Zusammenspiel der leistungsstarken Einzeltechnologien unter einer Oberfläche birgt entscheidende Vorteile: Denn auf diese Weise profitieren Unternehmen nicht nur von weitreichender Sicherheit, sondern gewinnen im Administrationsalltag auch spürbar an Zeit und Effizienz.

***www.watchguard.de***

# Automation

## AUF JEDEN FALL, ABER BITTE NICHT PUNKTUELL

Betrachtet man die Studien und Auswertungen der Wirtschaftsexperten, darunter das statistische Bundesamt, ist die Situation der Wirtschaft besser, als noch vor einigen Monaten prognostiziert. Trotz Lieferengpässen, Fachkräftemangel, weltweiten Instabilitäten oder Energieengpässen, hat es die Wirtschaft (wieder) einmal geschafft, entgegen düsterer Prognosen die Geschäfte so zu lenken und umzustrukturieren, dass auch der deutsche Handelsindex (ifo) im Dezember 2022 von gestiegen Werten berichtet. Die Agilität, die sich Unternehmen seit der Corona-Krise oder schon länger erarbeitetet haben und die Technologien, die dafür zum Einsatz kommen, haben einen nicht zu unterschätzenden Anteil daran. Unternehmen, die sich vor allem der Automatisierung und Modernisierung in Finance & Accounting gewidmet haben, können wesentlich dynamischer und vor allem zielgerichteter auf die schnellen Veränderungen der letzten Jahre reagieren. Mehr noch, Automation kann auch zu präziseren Prognosen und Planungen auf Basis von Szenarien führen, was ein präventives und aktives Agieren statt nur reagieren ermöglicht.

Allerdings kann die Automation sich wiederholender Aufgaben und Prozessen auch problematisch sein. Denn Automation mit Tools unterschiedlicher Anbieter bergen das Risiko eines Flickenteppichs, der nur schwer steuerbar ist und dessen Wirkung und Ergebnisse begrenzt sind. Im Finance & Accounting beispielsweise können nicht integrierte Automationstools leicht dazu führen, dass Unternehmen auf Basis ungenauer oder sogar falscher Daten und Zahlen planen. Daher ist es besser, die Automation von Prozessen mit einer Plattform „end-to-end" zu konsolidieren.

In der jährlich wiederkehrenden Studie „Im Auge des Sturms", die BlackLine gemeinsam mit dem unabhängigen Marktforschungsinstitut Censuswide durchführt, wurden in den USA, Kanada, Großbritannien, Deutschland, Frankreich, Singapur und Australien 1.483 C-Level-Führungskräfte sowie Finance & Accounting-Fachleute befragt. Im Vergleich zu den Studienergebnissen der Vorjahre nahmen in den Finanzabteilungen 2022 gleichzeitig das Engagement in die Automatisierung sowie das Vertrauen in die Finanzzahlen zu. Das könnte ein Hinweis darauf sein, dass die Automatisierung positive Wirkung zeigt.

Allzu optimistische Interpretationen sollten jedoch hinterfragt werden. Es stimmt zwar, dass die Unternehmen offen für mehr Automatisierung sind, aber in der Praxis zeigt sich, dass viele Organisationen ein Konglomerat unterschiedlicher Automatisierungs-Tools im Einsatz haben. Das trägt dazu bei, einzelne Prozesse zu verbessern oder zu beschleunigen. Sie sind jedoch in der Regel aufwändig in der Wartung und limitiert in der Skalierung, da der Gesamtzusammenhang in den einzeln automatisierten Finanzprozessen nicht hergestellt ist.

**Status Quo in Zahlen**

Dennoch, die BlackLine Studie, bestätigt, dass Unternehmen einen Nutzen in der Automation sehen. Mit 76 Prozent gab die deutliche Mehrzahl der Befragten an, dass die Finanzplanung, -analyse, -budgetierung und -prognose durch Automatisierung im Finance & Accounting verbessert wird. Das korrespondiert damit, dass 62 Prozent der Befragten der Meinung sind, dass Finanzdaten in Echtzeit in den nächsten zwölf Monaten sogar für das Überleben des Unternehmens unerlässlich sein können.

Fakt ist: In den letzten Jahren ging es Unternehmen darum, potenzielle Schwachstellen in F&A-Prozessen zu entlarven und manuelle Prozesse zugunsten höherer Transparenz, Genauigkeit und Agilität zu eliminieren. Das wird in Zukunft noch wichtiger werden. Allerdings sollte der Automation im F&A eine Gesamtstrategie zugrunde liegen, um die Vorteile der Technologie voll ausschöpfen zu können. Die maximale Wirksamkeit aus der Automation wird es nur in Zusammenhang mit einer integrierten Plattform geben, welche die Puzzlestücke der Einzelautomation in einem großen Ganzen zusammenführt.

**Automatisierung ja, aber bitte richtig**

Es wirkt wenig überraschend, dass die aktuelle Studie ein anhaltendes Interesse an moderner Technologie bestätigt wird: 28 Prozent der Führungskräfte und Finanzfachleute sagten, dass sie in ihre Datenanalysekapazitäten investieren. Sie gaben an, Automatisierungstechnologien zu implementieren oder diese zu skalieren, um akkuratere Finanzdaten zu erhalten. Während in der Vorgängerstudie von 2020 noch 80 Prozent der Unternehmen angaben, Automatisierungstechnologie umsetzen zu wollen, haben laut der aktuellen Studie dies bereits viele Unternehmen getan: 2022 gaben 76 Pro-

**PLUS**

**Im Auge des Sturms:**
Die Rolle von F&A bei der Reaktion auf Instabilität und Volatilität

Kostenloser Download unter:
**https://bit.ly/3JjNBnT**

zent der Befragten an, die Finanzplanung, -analyse, -budgetierung und -prognose durch Automatisierung verbessert zu haben. Das sind fast doppelt so viele wie vor zwei Jahren. Dreiviertel (75 Prozent) der Befragten berichteten zudem, dass sie auch die Finanzberichterstattung und -ablage automatisiert haben – mehr als doppelt so viele wie die Befragten, die 2020 angaben, dies tun zu wollen.

Nun könnte man dieses Ergebnis als einen Erfolg feiern. So einfach ist es aber nicht. Denn die Automatisierung inkludiert beispielsweise auch simple RPA-Lösungen, also Automatisierungs-Roboter, die an genau einer Stelle einen manuellen Prozess auf Basis von Regeln (im Idealfall sogar unter Einbindung von Künstlicher Intelligenz) ersetzen. Es werden einzelne Prozesse automatisiert, was ohne Frage eine Entlastung der Mitarbeiter im F&A erwirken kann. Allerdings führt das zu einem höheren Aufwand in der Datenkonsolidierung zu Lasten von Realtime-Ansichten und der Agilität.

Themen wie echtes Continuous Accounting, bei dem Buchungen im F&A hochautomatisiert und zeitlich verteilt anstatt am Ende der Berichtsperiode erfolgen oder gar Predictive Accounting, was Zukunftsszenarien und Trends aus der Gesamtheit der Finanzzahlen ableitet, können mit punktueller Automation nicht abgebildet werden. Dafür sind valide Daten und Prozessschritte über den gesamten Prozess hinweg nötig, die nur durch eine integrierte Automation der F&A-Kernprozesse erreicht werden kann.

**Die Zukunft ist geprägt durch die Leistung von F&A und dem CFO**

Die plattformorientierte Automation im F&A eröffnet CFOs und den Finanzexperten 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 Schlüsselrollen für die Unternehmenssteuerung eröffnet. Beispielsweise lassen sich mit Hilfe von Predictive Accounting verlässliche Trends für die Zukunft antizipieren, was dem Unternehmen einen zusätzlichen Wettbewerbsvorteil verschafft. Zusammengefasst: Eine plattformbasierte Automation ermöglicht ein modernes und kontinuierliches Accounting. Es hilft nicht nur einzelne Prozesse in der Finanzabteilung zu optimieren. Es sorgt durch eine ganzheitliche Sicht auf valide Finanzdaten in Echtzeit für die nötige Stabilität des Unternehmens.

***Ralph Weiss | www.blackLine.com***

## KORREKTHEIT DER FINANZDATEN

**43 %**

alle Befragten gaben an, dass sie derzeit kein volles Vertrauen in die Korrektheit der Finanzdaten ihres Unternehmens haben

### GRÜNDE DAFÜR:

1. UNSERE DATEN STAMMEN AUS ZU VIELEN QUELLEN, SODASS KAUM NACHVOLLZIEHBAR IST, OB ALLE DATEN KORREKT ERFASST WERDEN
2. ICH DENKE, DER PROZESS DER DATENERFASSUNG UND -VERARBEITUNG IST ZU KOMPLEX
3. ES GIBT NICHT GENÜGEND AUTOMATISCHE KONTROLLEN UND ÜBERPRÜFUNGEN FÜR DIE DATENMENGE

Quelle: BlackLine

# Agil & handlungsfähig

## INTELLIGENT AUTOMATION SORGT FÜR ENTLASTUNG & ZEIT

DER HOHE GRAD AN AUTOMATION SCHAFFT FREIE RESSOURCEN, UM DIE DIGITALE TRANSFORMATION VORANZUTREIBEN.

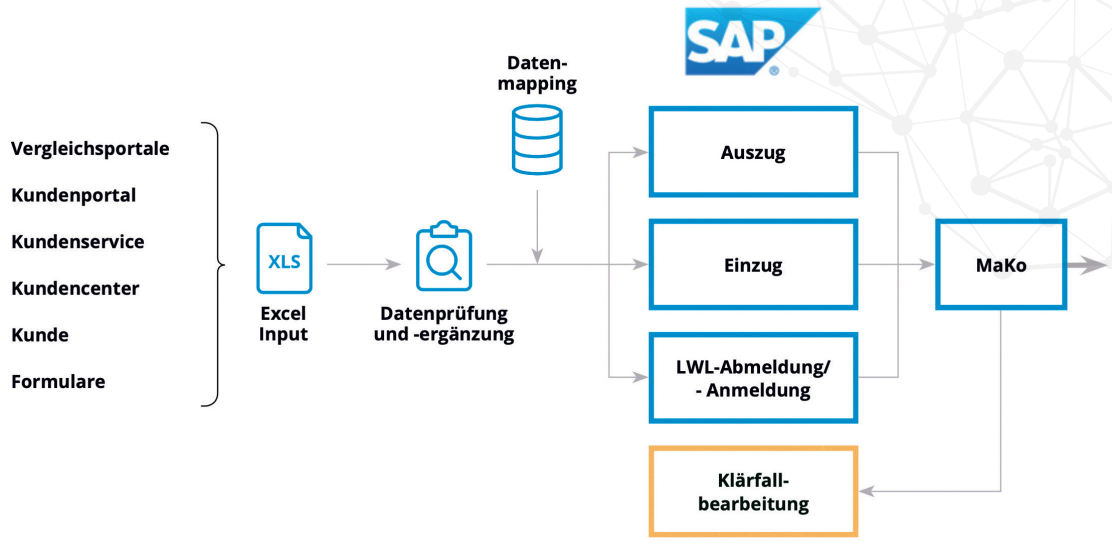
**Jesko Schultes**
**Geschäftsführer Natuvion Digital**
**www.natuvion.com/rpa**

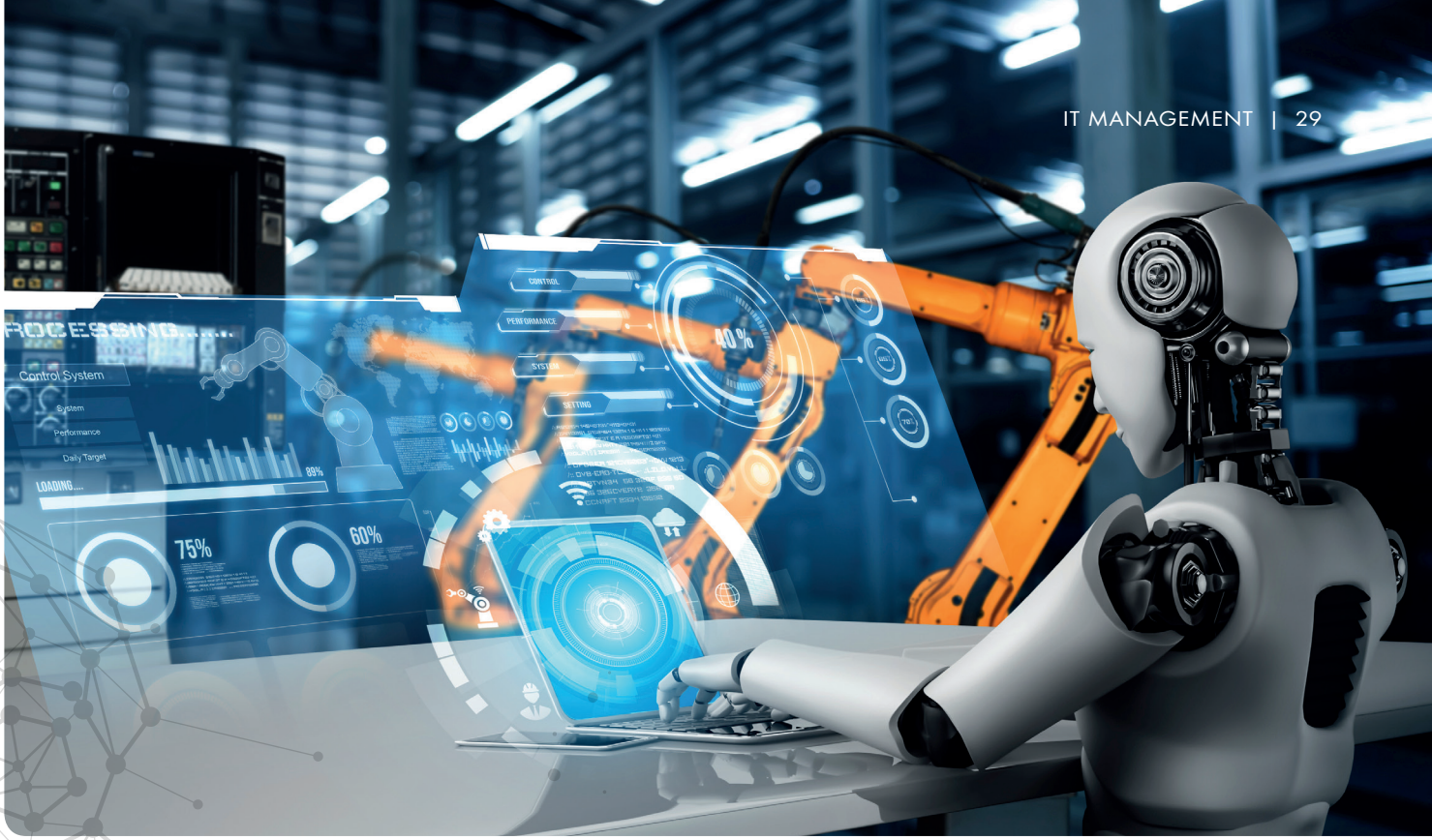
2022 war ein anspruchsvolles Jahr und auch das jetzige wird seine Herausforderungen an alle Wirtschaftszweige, öffentliche Einrichtungen und Organisationen oder an Betreiber von kritischen Infrastrukturen haben. Radikale Veränderungen und Unsicherheiten der letzten zwölf Monate betreffen jedoch insbesondere die Energieversorger, weshalb neben der Mammutaufgabe der digitalen Transformation auch die Automation seit geraumer Zeit viele IT-Abteilungen dieser Branche beschäftigt. Es geht darum, einzelne manuelle Prozesse zu automatisieren. Das schafft Entlastung und Zeit für die Mitarbeiter – insbesondere in Zeiten des Fachkräftemangels – und optimiert gleichzeitig die Qualität der Prozesse. Dieses Prinzip gilt gleichermaßen für große und mittelständische Unternehmen und es gibt eine Vielzahl an Optionen, die Automatisierung zu erreichen. Eine davon ist die sogenannte Intelligent Automation. Hierbei werden die Prozesse nicht nur einfach durch Automatisierungslösungen ersetzt, sondern durch intelligente Robotik optimiert.

**Intelligent Automation & Energieversorger**

Am Beispiel von typischen Prozessen eines Energieversorgers wird die Intelligent Automation erklärt. Das Prinzip lässt sich übrigens nahtlos auf nahezu alle anderen Branchen oder öffentliche Organisationen übertragen. Denn es gilt die Bedürfnisse der mittlerweile hoch digitalisierten Kundschaft zu befriedigen und die entsprechenden Applikationen bereitzustellen. Gleichzeitig herrscht bei Energieversorgern Stress wegen der Umstellung bisheriger Systeme, etwa auf SAP S/4HANA. Hinzu kommt, und das versetzt diesen Wirtschaftszweig in eine besonders exponierte Lage, dass der Gesetzgeber aufgrund der Energiekrise die

### AUF EINEN BLICK: DER PROZESSABLAUF DER AN- UND ABMELDUNG UND DES LIEFERANTENWECHSELS

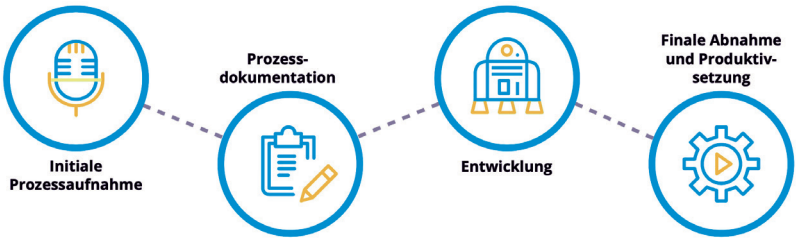





Rahmen- und Abrechnungsbedingungen immer wieder ändert. Als Beispiele seien die „Energiepauschale" oder der „Gaspreisdeckel" genannt. Diese Anpassungen greifen so tief in existierende Prozesse ein, dass sie nicht schnell über Nacht realisiert werden können. Dennoch müssen die Energieversorger diesen Anforderungen parallel zu allen anderen Herausforderungen Rechnung tragen.

Das höchste Ziel: Trotz aller Umwälzungen, veränderter Rahmenbedingungen und dem Debakel mit dem Einkauf oder der Bereitstellung von Energie für die Kunden, gilt es wirtschaftlich und konkurrenzfähig zu bleiben. Damit dies gelingt, konzentrieren sich viele Energieversorger darauf, die Prozesse möglichst effizient anzupassen und zu betreiben – durch Intelligent Automation mit Hilfe von Software-Roboter (RPA). Diese helfen, die wichtigen Aufgaben zu bewältigen und gleichzeitig die Ressourcen zu schaffen, um die großen Anpassungen und Transformationsprojekte zu stemmen. Zudem werden die Mitarbeiter von mühsamen und unattraktiven Arbeiten befreit und können sich um hochwertigere Aufgaben kümmern.

**RPA MODELLIERUNGSPROZESS**

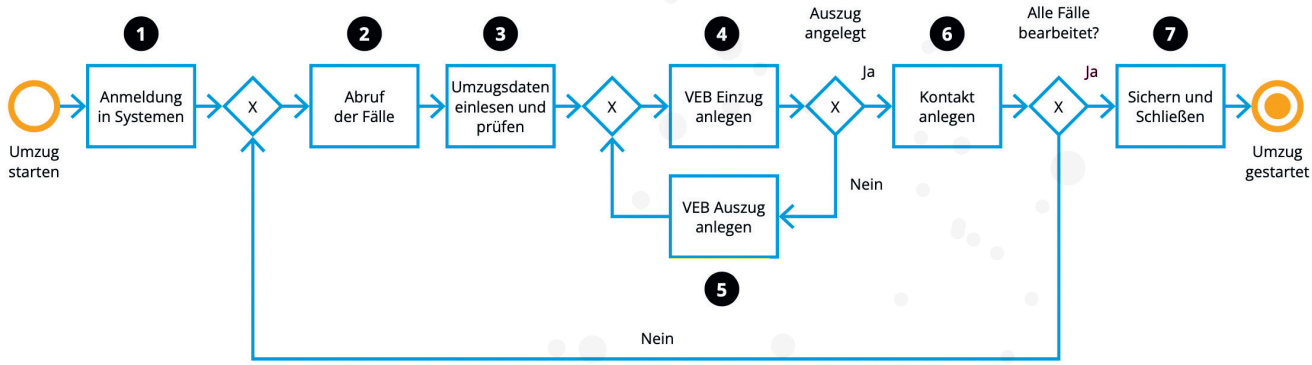



**Abhilfe durch Automation**

Speziell für Energieversorger hat Natuvion Digital mit Automation durch Software-Roboter (RPA) effiziente Lösungen im Portfolio, um die Agilität und Handlungsfähigkeit für die wichtigsten Systeme und Prozesse zu gewährleisten und verbessern. Mit Hilfe dieser digitalen Lösungen sind Unternehmen in der Lage, sehr viele Standardprozesse zu automatisieren und beschleunigen. RPA sorgt dafür, bisher manuelle Aufgaben, darunter die Durchführung eines Tarif- oder Lieferantenwechsels oder die Erhebung von Ableseergebnissen, in einen vollautomatisierten Prozess zu überführen. Damit wird in der Administration, aber auch bei den Systemverantwortlichen, viel Zeit freigesetzt. Mit den gewonnenen Ressourcen können dann wiederum andere dringende Aufgaben bewältigt werden. Als Nebeneffekt trägt die Automation auch dazu bei, die Situation des Fachkräftemangels zu entschärfen und das bei vergleichsweise niedrigen Investitionskosten.

Wichtig beim Einsatz von RPA ist, dass sich die Lösungen zur Automation nahtlos und unkompliziert in die existierenden Systeme der Energieversorger eingliedern lassen. Erreicht wird dies durch Cloudtechnologie - idealerweise auf Basis einer privaten Cloud-Infrastruktur. Neben der Software und der Infrastruktur sorgen zudem dezentrale Roboterlösungen und Services für die gewünschte Optimierung, auf die Energieunternehmen

## UMZUGSBEARBEITUNG INTELLIGENT GEDACHT




schnell und unkompliziert zugreifen können. Dabei sind sowohl standardisierte Roboter (Robot as a Service), aber auch kundenspezifische Designs möglich.

**Automation von Standardprozessen**

Da viele Energieversorger bei diversen Prozessen zusätzlich zum Kern-ERP-System auch auf manuelle Prozesse setzen (müssen), kommt nach wie vor trotz der fortschreitenden Digitalisierung beispielsweise eine Vielzahl an Tabellen und Formularen zum Einsatz. Händisch werden Vertragsdaten, Verbrauchswerte oder Forderungen mit dem ERP abgeglichen – mit allen Nachteilen wie hohen Zeitaufwand, verteilte Datensätze und Fehlerrisiko. Robotik hilft, dieses Problem und den damit verbundenen hohen Zeitaufwand zu lösen.

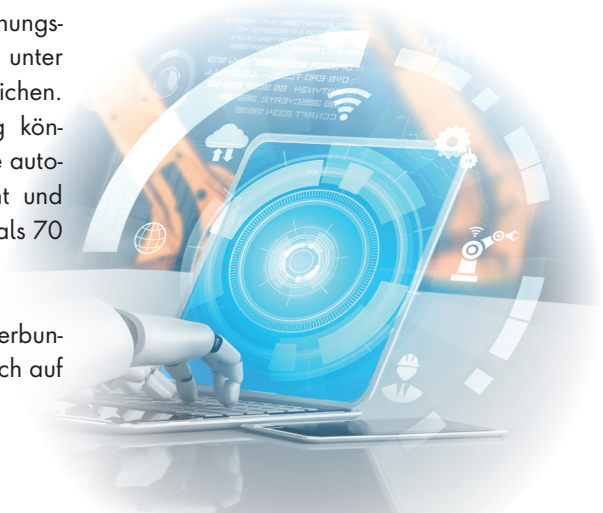
Ein Beispiel verdeutlicht die hohen positiven Effekte durch Automation: Die monatliche Abrechnung der Endkunden und die Verbuchung offener Posten und Forderungen sind die letzten, aber wichtigsten Schritte im Meter-to-Cash eines Energieversorgers. Tausende von Kundeneinzahlungen gehen zu den Abrechnungszeitpunkten auf den Bankkonten der Energieversorger ein und müssen gegen die zugehörigen Vertragskonten der Kunden gebucht werden. Hierfür stellen die Hausbanken Kontoauszüge zur Verfügung, die in das Abrechnungssystem importiert werden und daraus einzelne Zahlstapel zur Verbuchung erzeugen. Durch die automatische Systemverbuchung der Einzahlungen entsteht eine Vielzahl an Einzahlungen, bei denen nicht klar ist, von wem sie stammen. Bei vielen Energieversorgern wird jede einzelne Einzahlung manuell analysiert und anschließend eine Verbuchung oder Rückabwicklung initiiert.

Bei der Nutzung von RPA-Automationslösungen importieren die digitalen Helfer die Kontoauszüge der Hausbanken in das Abrechnungssystem. Bei der Erzeugung der Zahlstapel wird jede einzelne Einzahlung blitzschnell analysiert. RPA erkennt und bereinigt diese. Die bereinigten Zahlstapel werden anschließend durch das Abrechnungssystem verbucht. Die nicht eindeutig zuordenbaren Einzahlungen werden als sogenannte Klärfälle bereitgestellt. Die digitalen Helfer bearbeiten jeden einzelnen Klärfall und verbuchen diese offenen Posten durch Historienanalysen, Vergleiche von Rechnungs- und Vertragskontonummern oder unter Zuhilfenahme von Betragsabgleichen. Durch die Automatisierungslösung können bis zu 90 Prozent der Klärfälle automatisch bearbeitet sowie verbucht und damit eine Zeitersparnis von mehr als 70 Prozent erreicht werden.

Die RPA-Lösungen und das damit verbundene Automationspotenzial lässt sich auf viele unterschiedliche Bereiche der Energieversorger anwenden - mit sehr hohen Zeiteinsparpotenzialen, etwa bei der Erfassung oder der Plausibilisierung von Ableseergebnissen. Ebenso sind Ein- und Auszüge neuer und alter Kunden, Klärfälle aus der Marktkommunikation, die Rechnungseingangsverarbeitung, Auszahlung von Kundenguthaben, Lieferantenwechsel oder die Erfassung von SEPA-Mandaten typische Einsatzgebiete für Automation mit Hilfe von RPA. Damit hat die Automation nicht nur einen positiven Effekt auf Standardaufgaben im Hauptgeschäft der Energieversorger, sondern auch für Operations und die Bereitstellung der Systeme.

Der hohe Grad an Automation schafft freie Ressourcen, um die digitale Transformation voranzutreiben und vor allem auch, um die Systemumstellungen durch neue und veränderliche politische Vorgaben schnell zu ermöglichen.

***Jesko Schultes***



# Hannover Messe 2023

## DER WEG ZUR KLIMANEUTRALEN INDUSTRIE FÜHRT ÜBER HANNOVER

Die Liste der Herausforderungen für die Industrie ist lang: Klimawandel, Energieknappheit, unterbrochene Lieferketten, Fachkräftemangel. Die Lösung liegt im konsequenten Einsatz von Technologien. Gleichzeitig müssen die wirtschaftspolitischen Rahmenbedingungen richtig gesetzt werden. Die HANNOVER MESSE 2023 bietet Beides: Technologien für eine vernetzte und klimaneutrale Industrie sowie die Weltbühne für den Diskurs zwischen Industrie, Politik, Wissenschaft und Gesellschaft.

Auf der Weltleitmesse der Industrie zeigen rund 4 000 Unternehmen aus dem Maschinenbau, der Elektro- und Digitalindustrie sowie der Energiewirtschaft Lösungen für die Produktion und Energieversorgung der Zukunft.

Von der Digitalisierung und Automatisierung komplexer Produktionsprozesse über den Einsatz von Wasserstoff zur Energieversorgung von Fabriken bis hin zur Anwendung von Software zur Erfassung und Reduzierung des $CO_2$-Fußabdrucks bietet die HANNOVER MESSE ein ganzheitliches Bild.

Zu den ausstellenden Unternehmen gehören sowohl globale Tech-Konzerne wie Amazon Web Services, Microsoft, Google, SAP, Siemens, Bosch, NOKIA, ServiceNow oder Schneider Electric als auch mittelständisch geprägte Technologieführer wie Beckhoff, Festo, Harting, ifm, Pepperl+Fuchs, Phoenix Contact, Rittal oder SEW. Namhafte Forschungsinstitute wie Fraunhofer oder das KIT (Karlsruher Institut für Technologie) sowie mehr als 300 Startups versprechen Spitzentechnologien und völlig neue Geschäftsmodelle.

Die HANNOVER MESSE wird von Bundeskanzler Olaf Scholz und dem indonesischen Staatspräsidenten Joko Widodo eröffnet. Indonesien ist in diesem Jahr Partnerland der Industriemesse.

**Industrie 4.0 & Manufacturing X**

Damit das volle Potenzial von Industrie 4.0 erschlossen werden kann, braucht es Daten. Viele Daten, auf die alle am Wertschöpfungsprozess beteiligten Unternehmen zugreifen können. Ein neues zusammenhängendes Datenökosystem soll Abhilfe schaffen: Manufacturing X.


Vorangetrieben wird diese Vision einer souveränen und sicheren Datenplattform unter anderem von den Wirtschaftsverbänden BDI, VDMA und ZVEI. Im engen Schulterschluss mit dem Bundeswirtschafts- und Klimaministerium werden auf der HANNOVER MESSE die ersten Schritte zur Umsetzung von Manufacturing X vorgestellt.

**Künstliche Intelligenz**

Künstliche Intelligenz (KI) spielt in der Industrie eine immer größere Rolle. Neben der Optimierung von Prozessen setzt die produzierende Industrie zunehmend auf KI in der Simulation und in der Produktentwicklung.

Auch die sogenannte generative KI wird den Weg in die Industrie finden. Systeme wie ChatGPT oder DALL-E können heute schon beim Texten, Programmieren und Designen unterstützen. „In Zukunft ist durchaus denkbar, dass eine KI eine Maschine entwirft und der Mensch dann überprüft, welche Anpassungen für einen Realbetrieb notwendig sind. Das spart Zeit und bietet angesichts des vorherrschenden Fachkräftemangels erhebliches Potenzial", so Köckler.

**Energieströme und -verbrauch sichtbar machen**

Im Zusammenspiel von Software und Maschinen entstehen erhebliche Energieeinsparpotenziale. Smart Energy Monitoring-Lösungen der Aussteller helfen dabei, Energieverbräuche auf Maschinenebene zu ermitteln, zu optimieren und damit den $CO_2$-Fussabdruck zu reduzieren.

HANNOVER MESSE

**17. bis 21. April 2023**

Laden Sie sich jetzt Ihr kostenloses eTicket herunter.

***https://bit.ly/3DSwQg9***

# Strategische vs. punktuelle Prozessautomatisierung

## EIN CENTER OF AUTOMATION ZÜNDET DEN BOOSTER

Viele Unternehmen haben bereits damit begonnen, ihre Büro-Prozesse durch neue Technologien wie Robotic Process Automation (RPA), Low-Code in der Microsoft Power Platform oder in SAP zu automatisieren. Sie verbuchen damit positive Erfahrungen in einzelnen Abteilungen, jedoch gelingt es ihnen noch nicht, dass punktuell vorhandene Knowhow systematisch auf alle Bereiche zu übertragen, um so alle Potenziale zu heben und Synergieeffekte zu nutzen. Die organisatorische Lösung ist ein Center of Automation. Manchmal reicht es aus, wenn das Team aus zwei Mitgliedern besteht.

Automatisierung entlastet die Mitarbeitenden von aufwendigen Routinearbeiten. Ihre Umsetzung ist jedoch häufig davon abhängig, dass sich in einzelnen Abteilungen digital denkende Pioniere finden, die entsprechende Projekte initiieren und auch abschließen. Das Wissen verbleibt anschließend in dieser Abteilung und diffundiert nicht in andere mit geringerer Digital-Affinität. So bilden sich stark unterschiedliche Silos ohne Wissens- und Erfahrungstransfer, die im Gesamtbild schnell ein Automatisierungs-Chaos ergeben. Es fehlen zentral verantwortliche Treiber und eine unternehmensübergreifende Automatisierungsstrategie. Das Problem verschärft sich, wenn einzelne Kompetenzträger*innen das Unternehmen verlassen und mit ihnen das Wissen um den automatisierten Prozess und die Nachpflege der Automatisierung verloren geht.

Dem wirkt ein Center of Automation entgegen, das dafür verantwortlich ist, Automatisierungen abteilungsübergreifend zu erfassen, einzuführen, zu begleiten und weiterzuentwickeln. Ein solches zentrales Team verfügt über einen direkten Weg in die Fachabteilungen. Anstatt vieler einzelner Initiativen verfolgt das Center of Automation den Ende-zu-Ende-Gedanken: Die Verantwortlichen aus dem Center of Automation bilden nicht nur den Knotenpunkt zwischen IT- und Fachabteilung, sondern setzen Automatisierungen federführend ganzheitlich um.

### Die Nachteile punktueller Prozessautomatisierungen

Automatisierung ist ein kontinuierliches Projekt, da es im Laufe der Zeit stetige

Veränderungen im Prozess geben wird, die technische Anpassungen erfordern. Ebenfalls ist eine permanente Wartung von Nöten, die nur funktionieren kann, wenn eine entsprechende Verantwortlichkeit vorliegt. Werden also von Beginn an unzureichende Schnittstellen zwischen Fach- und IT-Abteilung geschaffen, entsteht das Problem der personenbezogenen Verantwortung. Fehl- oder Urlaubszeiten der Initiatoren haben Einfluss auf den Automatisierungsprozess, da bei etwaigen Fehlern ausschließlich sie einen Eingriff vornehmen können. Außerdem droht die Gefahr des abwandernden Prozesswissens und generell ein Abebben der Aktivitäten unter dem Druck der täglichen Aufgaben.

Eine weitere Schwierigkeit dieser Insellösungen ist die geringe Automatisierungseffizienz. Eine punktuelle Automatisierung hat zur Folge, dass unternehmensweite Automatisierungsvorhaben mangels institutionalisierter Gesamtverantwortlichkeiten im Sande verlaufen oder die einzelnen Teams ihre jeweiligen Projekte mit überhöhtem Zeitaufwand und verschiedenen Werkzeugen umsetzen. Der Erfolg von Automatisierungen beruht jedoch darauf, möglichst effizient und standardisiert Potenziale zu erkennen und Optimierungen vorzunehmen. Nur so lassen sich auch Aussagen über den Nutzen der einzelnen Automatisierungen in ihrem Zusammenspiel treffen.

**Der Faktor Mensch**

Neben dem technischen und organisatorischen Aspekt von Automatisierungen sollten Unternehmen die Überzeugungen und Ängste ihrer Mitarbeitenden berücksichtigen, die mit dem Thema verbunden sind. Dass der zunehmende Digitalisierungsdruck und die Überlastung von Mitarbeitenden aufgrund von Fachkräftemangel neue Lösungen fordern, ist bekannt und täglich erlebbar. Trotzdem liegen das Verständnis für die Entlastung durch Automatisierungen und die Angst vor Bedeutungs- und letztlich Arbeitsplatzverlust dicht beieinander. Ohne Akzeptanz in der Belegschaft werden Automatisierungsprojekte scheitern. Deshalb ist es wichtig, Mitarbeitende, denen ein „Roboter-Kollege" zur Seite gestellt werden soll, aber auch weitere Stakeholder, wie Betriebsräte, HR-Abteilungen und Vorgesetzte, von Anfang an einzubinden und das Projekt transparent zu erklären. In punktuellen Automatisierungen sind die fachlich Verantwortlichen mit dieser zusätzlichen Aufgabe nicht selten überfordert und benötigen Unterstützung der IT-Abteilung oder Unternehmenskommunikation.

Akzeptanz der Automatisierung ist ebenso bei den Führungskräften notwendig. Erkennen sie das Potenzial der Automatisierung nicht oder wird es nicht als strategisch und unternehmerisch wertvoll platziert, erhält das Thema nicht die Priorität, die es zu seiner vollen Entfaltung braucht. Mit der Befähigung durch ein Center of Automation setzt die Geschäftsführung hingegen ein klares Signal und wird die Führungskräfte motivieren, ihre Prozesse digital zu denken. Nur so ist End-to-End-Prozessautomatisierung zu erreichen.


*Geschäftsregeln*

*Automatisierung von Geschäftsprozessen*

**Ein Center of Automation leistet Abhilfe**

Damit im Unternehmen strategische statt punktueller Automatisierung stattfindet, Mitarbeitende schnell Entlastung spüren, die Kundenzufriedenheit dank besserer Prozesse steigt und eine mitwachsende Infrastruktur entsteht, sollte ein Center of Automation von Beginn an zentraler Treiber einer Automatisierungsstrategie sein. Das Team vereint Fachabteilungskenntnisse, Change Management, User Adoption Knowhow sowie IT-Expertise und ist von der Idee über die Umsetzung bis zur Evaluation verantwortlich für alle Automatisierungen im Unternehmen. Dazu gehören unter anderem die Identifikation technologisch sinnvoller Realisierungsmöglichkeiten sowie die Adaption erfolgreicher Projekte für weitere Unternehmensbereiche. Außerdem begleitet das Center of Automation den Prozess kulturell, um für eine breite Akzeptanz zu sorgen.

BEI DER IMPLEMENTIERUNG EINES CENTER OF AUTOMATION GEHT ES IN ERSTER LINIE DARUM, EFFIZIENTE STRUKTUREN ZU SCHAFFEN, DIE IM UNTERNEHMEN ERNST GENOMMEN WERDEN.

**Steffen Weiers, Automatisierungsexperte, BTC Business Technology Consulting AG, www.btc-ag.com/**

Bild: BTC Business Technology Consulting AG

**Implementierung eines Center of Automation**

Bei der Implementierung eines Center of Automation trifft internes Projektwissen auf IT-Expertise aus dem Unternehmen und Automationswissen von externen Expert*innen. In erster Linie geht es dabei darum, effiziente Strukturen zu schaffen, die im Unternehmen ernst genommen werden. Dies bedeutet jedoch nicht, dass ein Center of Automation aus einem größeren Pool an Mitarbeitenden bestehen muss. Bei kleineren Unternehmen kann es durchaus aus zwei Personen plus extern Beratenden zur Ergänzung beziehungsweise zum Ausbau des eigenen Knowhows bestehen. Wichtig ist, Automatisierung als übergreifende Funktion zu organisieren, sodass ausreichend Schnittstellen zwischen IT- und Fachabteilungen gegeben sind. Mangelt es an IT-Wissen und an der Sicherheit, mit eigenen Ressourcen eine langfristige Strategie umsetzen zu können, kann eine Auslagerung sinnvoll sein.

**Umsetzung**

Und wie läuft die Umsetzung? Jedes Unternehmen muss sich die Frage stellen, welche Prozesse sich besonders für die Automatisierung eignen. Ideale Kandidaten sind sich wiederholende Massenprozesse mit:

- langfristiger Laufzeit und absehbar geringen Anpassungen in den Abläufen,
- hohem manuellen Arbeitsanteil,
- großer Fehleranfälligkeit,
- gleichförmiger Informationsgrundlage bzw.
- regelbasierten Entscheidungskriterien.

**Ergebnisse**

Was letztendlich zählt, sind natürlich die Ergebnisse. Und da ergibt sich aus den Erfahrungswerten:


- Steigerung der Prozessproduktivität um 50 bis 80 Prozent
- Amortisierung der Einführungskosten (Lizenzkosten plus unternehmensindividuelle Konfiguration) innerhalb kürzester Zeit – oftmals in nur wenigen Monaten
- Erhöhung der Mitarbeiterzufriedenheit durch sinnstiftende Aufgaben
- Gewinnbringender Einsatz ohnehin knapper Personalressourcen
- Steigerung der Prozessgeschwindigkeit
- Senkung der Fehlerrate
- Betrieb rund um die Uhr – unabhängig von Feierabend, Urlaub oder Krankheit
- Keine aufwändige Einarbeitung in wenig lukrative Begleitprozesse
- Erhöhte Konkurrenzfähigkeit am Markt
- Notwendige Transparenz für Audits und Zertifizierungen

**Fazit**

Die Automatisierung von Prozessen ist inzwischen zum echten Wettbewerbsvorteil geworden, die Identifizierung und Umsetzung von Prozesspotenzialen durch ein unternehmensweit verantwortliches Center of Automation jedoch ist (noch) nicht weit verbreitet. Die Etablierung eines solchen Teams ist die wichtigste organisatorische Entscheidung, um Automatisierung systematisch umzusetzen und so Wertschöpfungspotenziale am Markt und bei der Fachkräfteentlastung zu heben.

***Steffen Weiers***

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

# No SurpRISE with SAP

## Strategie & Operations

04. Mai 2023 | ab 9:00 Uhr | Digitalevent

SCAN ME

https://www.it-daily.net/sap/

#SAPdigital23

# Hürden der Digitalisierung

## ... UND WIE MAN SIE NIMMT

Die interne Logik der Digitalisierung rückt die IT in das Zentrum strategischer und taktischer Unternehmensentscheidungen. Bei der Umsetzung der digitalen Transformation in eine erfolgreiche Praxis besteht aber vor allem im Mittelstand noch reichlich Handlungsbedarf.

Digitale Geschäftsmodelle sind ohne eine innovative und effiziente IT weder vorstell- noch umsetzbar. Die IT soll die komplementären Rollen als Vordenker, Ideenlieferant, Taktgeber und ausführendes Organ parallel ausfüllen, dabei kosteneffizient und flexibel genug sein, um jederzeit für die Volatilität digitaler Entwicklungen gerüstet zu sein.

WÄHREND KONZERNE UND GROSSUNTERNEHMEN FÜR DIE DIGITALE TRANSFORMATION IN DER REGEL AUF GROSSE INTERNE IT-ABTEILUNGEN UND EINE AUSDIFFERENZIERTE, BESTENS QUALIFIZIERTE PARTNERLANDSCHAFT ZURÜCKGREIFEN KÖNNEN, FEHLT ES IM MITTELSTAND OFT NOCH AN EINER AUSGEPRÄGTEN IT-EXPERTISE.

**Dr. Christoph Ehlers, Leiter DevOps, ConSol, www.consol.de**

Dieses komplexe Anforderungsprofil wird in der Praxis durch den Unternehmensalltag oft konterkariert. Im Alltag wird die IT nach wie vor als eher limitierender Faktor gesehen und nicht als der notwendige Motor der Digitalisierung. Dahinter stecken jedoch weder böser Wille noch Unfähigkeit, sondern schlicht und einfach die Tatsache, dass Aufbau und Struktur der in der Regel internen IT-Ressourcen bereits vor der Digitalisierungswelle chronisch überlastet waren – und nach wie vor sind. Schon immer stand die IT unter dem ständigen Druck, den laufenden Betrieb aufrechtzuhalten und sich dabei gleichzeitig innovativ auf die Anforderungen von morgen einstellen zu müssen.

**Wege aus der Sackgasse**

Die zusätzlichen typischen Anforderungen der Digitalisierung, wie etwa kurze Time to Market und die damit verbundene Agilität und Skalierbarkeit, sind so nicht zu erfüllen. Die bestehenden Konzepte, Kompetenzen und Ressourcen müssen also überdacht werden. Besonders im Mittelstand herrscht in Sachen digitales Rüstzeug noch großer Nachholbedarf.

Immerhin, die Tragweite dieser Situation ist offensichtlich erkannt. So fördert die IDG-Studie «IT-Modernisierung» zutage, dass vor allem Unternehmen aus dem Mittelstand mit bis zu 500 Mitarbeitern Bedarf sehen, geschäftskritische IT-Umgebungen zu modernisieren. Die Impulse zur Implementierung von neuen Anwendungen, Systemen und Cloud-Computing-Strategien kommen primär aus den Reihen von Geschäftsführung und Management (43 Prozent). Die IT- und Fachabteilungen dagegen agieren eher verhalten – sei es nun, weil jede Änderung der Situation zunächst noch mehr Belastung verursacht oder weil die Modernisierungsbestrebungen als latente Kritik verstanden werden.

**Wege in die Digitalisierung**

Wie virulent dieses Thema dagegen in den Führungsetagen bereits ist, zeigt die Tatsache, dass die Kosten und Aufwände der digitalen Modernisierung nicht als ausschlaggebender Faktor angesehen werden. Technologische Aspekte (33 Prozent) und die IT-Sicherheit (35 Prozent) gelten als viel wichtiger, also Fragen, die eigentlich in den Kompetenz- und Wirkungskreis der IT-Abteilungen gehören. Um so bedenklicher ist es, dass die interne IT-Power dafür oft zu schwach ist: Nur rund 27 Prozent der befragten Unternehmen haben genügend eigene Fachleute, um eine Modernisierung der Systeme und Umgebungen durchzuführen. Das ändert allerdings nichts an der Tatsache, dass sie dafür dringend gebraucht werden. Die Lösung dieses Dilemmas kann daher nur durch externe Unterstützung kommen.

Die Aufgabenstellungen bei der digitalen Transformation sind komplex. Sie beginnen typischerweise mit der Fragen-Trias: Wo beginnen wir mit der Modernisierung? Wie können wir im Rahmen der bestehenden IT-Systemlandschaft mit einem begrenzten Risiko das meiste erreichen? Können wir das Ende der notwendigen Investition absehen? Aus diesen eher generischen Fragestellungen resultiert dann ein differenzierter Katalog, der auf die jeweiligen Besonderheiten und Spezifika des jeweiligen Unternehmens abgestimmt wird, und dessen Beantwortung dann als handlungsweisender Leitfaden die weiteren Digitalisierungsschritte definiert. Typischen Fragen sind: Wohin entwickelt sich mein Geschäft die nächsten fünf bis zehn Jahren? Wie agil und flexibel soll mein Geschäft sein? Rechne ich mit Lastspit-

zen? Wie kritisch sind meine Daten? Kommen Cloud-Services für mich überhaupt in Betracht – und wenn ja in welchem Rahmen? Wie amortisiert sich ein Infrastruktur-Update? Was passiert mit den Legacy-Systemen und postproduktiven IT-Ressourcen?

Aus der Beantwortung dieser Fragen ergeben sich die spezifischen Aufgabenstellungen, die dann zu einem Gesamtbild verknüpft werden. In der Umsetzung sollten dann unzureichend integrierte Lösungsinseln vermieden werden, auch wenn dann die digitale Reise einen längeren Atem erfordert.

So kann beispielsweise die als Lösung gefundene Containerisierung der Applikationen und die Einführung eines Container Management Systems nicht ihr volles Potential entfalten, wenn nicht gleichzeitig auch die Architektur der Applikationen entsprechend angepasst wird. Wird dieser Weg jedoch zu Ende gegangen und auch die Applikationen modernisiert, so kann das Unternehmen noch lange Jahre von der Zukunftsfähigkeit der Lösung profitieren.

**Wege in die Abteilungen**

IT ist kein Selbstzweck, sondern dient immer den unternehmerischen Prozessen. Dieses Mantra sollte auch bei der digitalen Transformation stets im Hinterkopf bleiben. Digitale Geschäftsmodelle und deren unendliche Möglichkeiten müssen operativ umgesetzt werden, um im Sales Cycle mit seinen kundenorientierten Marketing-, Sales- und Servicefunktionen, in den Abteilungen wie Human Resources oder Controlling und natürlich in der Leitungsebene mit den Strategie- und Stabsabteilungen anzukommen.

Bei allen Aktivitäten rund um die digitale Transformation gelten zwei Hürden als besonders schwer zu nehmen: Erstens die begrenzende Wirkung festgefahrener Denkweisen und zweitens die tradierte Rolle der IT als reiner Dienstleister für Workflows und Prozesse, die an anderer Stelle konzipiert worden sind. Bei der Überwindung dieser Hindernisse kann sich die Unterstützung durch externe Expertise als besonders hilfreich erweisen. Sie beginnt idealerweise schon im Planungs- und Evaluationsstadium, zum Beispiel beim Alignment von Business und IT, das für die Wettbewerbsfähigkeit der kommenden Jahre und die nachhaltige Wirkung der eingeleiteten Transformation ein wichtiger Grundstein ist. Sie hilft aber auch bei der operativen Umsetzung, etwa im Bereich der Software-Architekturen, in dem IT-Dienstleister naturgemäß über weitaus mehr Erfahrung und Kompetenz verfügen als mittelständische Unternehmen mit ihren, wie beschrieben, in der Regel begrenzten IT-Ressourcen. Die clevere Arbeitsteilung zwischen internen und externen Ressourcen ist daher eine der wichtigsten Grundlagen für die erfolgreiche Digitalisierung mittelständischer Unternehmen.

Der Mittelstand gilt zu Recht als tragendes und treibendes Element der deutschen Wirtschaft, und ist daher in seiner Bedeutung kaum zu überschätzen. Er ist für die aktuellen Herausforderungen insgesamt sehr gut aufgestellt. Für die anstehenden Aufgabenstellungen im Rahmen der digitalen Transformation allerdings muss er seine IT-Expertise dringend ausbauen und neu ordnen.

***Dr. Christoph Ehlers***

# Präzise Lokalisierung von Materialien

## LOGISTIKPROZESSE ALS ERP-KERNKOMPETENZ

Mit dem Ziel einer nachhaltigen Produktion und der Verschlankung von Produktions- sowie der Optimierung von Lagerprozessen hat die ams.Solution AG gemeinsam mit dem langjährigen Kunden SSI Schäfer ein strategisches Projekt zur Weiterentwicklung der ERP-Logistikfunktionalitäten aufgesetzt. Zum einen ging es darum, die Geschwindigkeit in der Fertigung sowie den Materialfluss im Produktionsprozess zu beschleunigen, zum anderen darum, Lagerflächen zu reduzieren, Überproduktion zu vermeiden und somit Ressourcen, Kosten und Zeit zu sparen. Über den aktuellen Projektstatus sprachen wir mit dem ams-Produktverantwortlichen Jurij Schmidt.

**it management:** *Herr Schmidt, inwieweit ist eine ERP-Software wie ams.erp prädestiniert für die Abbildung logistischer Prozesse?*

**Jurij Schmidt:** Die Abbildung von Logistikprozessen gehört zu unseren Kernkompetenzen, sie ist integraler Bestandteil des vernetzten, digitalen Wertschöpfungsprozesses, den unsere Kunden mit unserer Software steuern. Das Thema Logistik ist demnach kein Neuland für uns. In ams.erp steht unseren Kunden mit der Versandsteuerung seit vielen Jahren ein mächtiges Werkzeug zur Verfügung, über das wir sehr erfolgreich alle Materialströme vom Unternehmen nach außen darstellen.

Eine funktionale Besonderheit, die unser System als Ergebnis seiner Spezialisierung auf die Losgröße 1+ mitbringt, ist die Möglichkeit des Arbeitens mit O-Teilen, also mit Artikeln ohne Artikelnummern. Für den Logistikprozess erweist es sich als großer Vorteil, dass alle Materialien gleich behandelt werden, unabhängig davon, ob Artikel mit oder ohne Artikelnummern verwendet werden.

**it management:** *Warum ist dieser Aspekt so wichtig und was ist das konkrete, übergeordnete Ziel der laufenden Entwicklungsarbeit?*

**Jurij Schmidt:** Die große Stärke des O-Teile-Managements ist in den Augen der Logistik auch ihre Schwäche. Für herkömmliche Mittel ist die Existenz einer Artikelnummer essenziell, um die Nachvollziehbarkeit der Materialbewegung zu gewährleisten. Deswegen setzen wir bei ams auf ein von den Nutzern frei verwaltbares Platzkonzept, welches wir mit Ladungsträgern – den sogenannten Ladeeinheiten – kombinieren und so die homogene Verarbeitung von Materialien und Teilen ermöglichen.

Generell schaffen wir mit der Weiterentwicklung unserer Logistiklösung nun die Möglichkeit, nicht nur den exakten innerbetrieblichen Lagerort von Materialien zu ermitteln, sondern besitzen auch alle Informationen hinsichtlich ihres derzeitigen Zustands: Wir wissen beispielsweise, inwieweit diese Materialien bereits bearbeitet wurden oder ob eine Baugruppe fertig- oder teilfertiggestellt ist.

**it management:** *Das Projekt hat seinen Ursprung in der Praxis. Wie lauten die konkreten Anforderungen Ihres Kunden?*

**Jurij Schmidt:** SSI Schäfer geht es darum, mittels einer vollumfänglichen Materialflussnachverfolgung die maximale Kontrolle über die internen Materialbewegungen zu gewinnen. Unser Kunde betreibt ein sogenanntes Konsolidierungslager mit Anlieferungen aus unterschiedlichen Quellen. Dazu gehört zum einen ein Lager, von dem aus Material per Shuttle zum Konsolidierungslager gebracht wird, sowie zwei weitere externe Lieferanten. Aus dieser Konstellation ergibt sich, dass von einer Vielzahl an Materialien nicht bekannt ist, an welchem exakten Ort sie sich gerade befinden und ob das Material bereits vollständig in der Konsolidierungsfläche gesammelt ist.

> WIR SETZEN AUF EIN VON DEN NUTZERN FREI VERWALTBARES PLATZKONZEPT, WELCHES WIR MIT LADUNGSTRÄGERN KOMBINIEREN UND SO DIE HOMOGENE VERARBEITUNG VON MATERIALIEN UND TEILEN ERMÖGLICHEN.
>
> **Jurij Schmidt,**
> **Product Owner, ams.erp Logistics,**
> **www.ams-erp.com**

Die konkrete Vorgabe lautete vor diesem Hintergrund, den exakten Lagerort eines bestimmten Teiles zu einem bestimmten Zeitpunkt abzubilden. Die einzelnen Materialien sollen zudem effizienter organisiert werden können, was bedeutet, dass ermittelt wird, wann und wo welche Teile zu welchen Arbeitsschritten benötigt werden.

**it management:** *Wie kann dies gelingen?*

**Jurij Schmidt:** Dies gelingt, indem man vom bisherigen Push- auf das sogenannte

Pull-Prinzip umstellt. Anstelle das Material einfach auf Verdacht an die nächste Stelle in der Produktionskette weiterzuschicken (Push-Prinzip), wird es für den jeweiligen Produktionsschritt gezielt angefordert (Pull-Prinzip). Auf diese Weise ist der Materialfluss immer nur so schnell wie die Menschen, die mit dem Material arbeiten. Dies verhindert unnötige Materialstaus und stellt sicher, dass sich Materialien stets zur richtigen Zeit am richtigen Ort befinden, ohne dabei überflüssige Lagerbestände aufbauen zu müssen.

**it management:** *Wie läuft die Produktentwicklung ab? In welcher Weise wird der Pilotkunde eingebunden?*

**Jurij Schmidt:** Wir entwickeln in dem Projekt agil nach Scrum, also in sehr enger Zusammenarbeit mit SSI als Impulsgeber. In sogenannten Reviews präsentieren wir den Anwendern alle drei Wochen die neuentwickelten Features und erhalten noch während des Meetings die notwendige Rückmeldung. Die geäußerten Punkte setzen wir im folgenden Entwicklungsschritt, dem nächsten „Sprint", unmittelbar um – immer mit dem Fokus, eine stimmige Standardsoftware zu präsentieren.

**it management:** *Welche sind die nächsten Schritte?*

**Jurij Schmidt:** Wir denken im Rahmen der Weiterentwicklung nicht mehr nur in festen Orten, sondern auch in mobilen. Dies bedeutet, dass wir beispielsweise auch Transportfahrzeuge einbinden können, die nicht nur innerbetrieblich, sondern auch außerhalb unterwegs sind. Eine mögliche Variante zur Umsetzung in der Praxis könnte dabei sein, innerbetriebliche Checkpoints zu definieren, an denen mithilfe von RFID-Chips oder Scans Material, das eine Kreuzung oder ein Regal passiert, mit Koordinaten versehen wird und so exakt lokalisiert werden kann.

Denkbar wäre zudem die Platzierung von GPS-Trackern an den Fahrzeugen, um eine genaue Nachverfolgung zu ermöglichen. Unsere Vision von Logistik könnte man wie folgt formulieren: die einfachste und präziseste Verortung von Materialen an allen denkbaren Standorten in Echtzeit.


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

# Rethink Digital Growth

## WELCHE DIGITALTRENDS 2023 FÜR MEHR NACHHALTIGKEIT SORGEN

Welche Rolle spielt die Digitalisierung beim Klimaschutz? Welche Technologien sind vielversprechend? Christian Till Roga, Senior Vice President bei T-Systems, erklärt an welchen grünen Technologien 2023 kein Weg mehr vorbeigeht und wie Unternehmen effizient Nachhaltigkeitsziele nicht nur formulieren, sondern auch umsetzen können.

Hohe Energiekosten, geopolitische Spannungen, Fachkräftemangel, digitale Transformation – die Liste an Herausforderungen, denen sich Unternehmen auch 2023 stellen müssen, ist lang. Darüber dürfen sie die größte und wichtigste Aufgabe nicht vergessen: Nachhaltiger zu werden, um dem Klimawandel entgegenzuwirken. Nicht vergessen? Besser gesagt, sie sollten sie verinnerlichen. Denn wer von Anfang an Klima- und Umweltschutzkriterien zum Standard in seinen Prozessen macht, also „Sustainability-by-Design" praktiziert, kann seine Nachhaltigkeit deutlich stärken. Dieses Umdenken ist wichtig, damit Unternehmenswachstum, Digitalisierung und Nachhaltigkeit Hand in Hand gehen. Schließlich könnte eine nachhaltige digitale Industrie allein in Deutschland 64 Millionen Tonnen $CO_2$ einsparen, prognostiziert der Digitalverband Bitkom. Drei Digitaltrends stehen dabei dieses Jahr im Fokus.

WER VON ANFANG AN KLIMA- UND UMWELTSCHUTZKRITERIEN ZUM STANDARD IN SEINEN PROZESSEN MACHT, ALSO „SUSTAINABILITY-BY-DESIGN" PRAKTIZIERT, KANN SEINE NACHHALTIGKEIT DEUTLICH STÄRKEN.

**Christian Till Roga,**
**MD Integrated Account DT, T-Systems,**
**rethink-the-system.de**

### Daten-Wissen ist Macht

Mehr Nachhaltigkeit beginnt mit einer Bestandsaufnahme. Und die gelingt am besten mit einem Blick auf die Datensammlung des Unternehmens. Erst wenn ausreichend Daten über die bisherigen Geschäftsprozesse transparent einsehbar sind, können interne Teams die produzierten Emissionswerte und den Materialverbrauch ermitteln, Problemstellen entdecken und neue, energieeffizientere Strategien entwickeln. Je stärker Unternehmen die Funktionsweise von Produkten, Systemen oder Services durchdringen, umso einfacher können sie diese klimaschonend weiterentwickeln.

Außerdem liefern Daten die Grundlage für Innovationen und neu ausgerichtete Geschäftsmodelle – etwa basierend auf Künstlicher Intelligenz. Wer aber den Algorithmus einer KI trainieren möchte, braucht dazu eine ungeheuer große Zahl hochwertiger Daten. Sind diese vorhanden, dann lässt sich KI für den Klimaschutz nutzen – vorausgesetzt, dieses Ziel wird beim Training der KI und bei ihrer Weiterentwicklung konsequent mitgedacht. So kann die KI zur „Grünen KI" werden und in unterschiedlichen Bereichen zum Einsatz kommen. Beispielsweise in der nachhaltigen Stadtplanung: Mithilfe von KI und dem Internet of Things (IoT) wurde die spanische Stadt Gijón so zur Smart City. Heute steuert die Stadt zum Beispiel ihre Beleuchtung automatisiert. Diese besteht zudem aus LED-Lichtpunkten, die weniger Energie verbrauchen.

Von Rohstoffengpässen über Produktionsstillstände bis zu Transportblockaden in der Lieferkette: Technologien wie Automatisierung, Data Analytics oder Cloud-Dienste helfen, Ressourcen einzusparen und potenzielle Risiken zu ermitteln. Und es überrascht kaum: auch hier sind die Basis den Einsatz dieser Technologien im aktivem Nachhaltigkeitsmanagement hochwertige Daten. Qualität vor Quantität. Fehlen solch aussagekräftige Daten, dann können Unternehmen oder Kommunen ihre Analysefähigkeiten verbessern, indem sie Technologien miteinander verknüpfen.

### Grün in die Cloud

Auch mit der Cloud arbeitet es sich „grüner": Der Energieverbrauch würde enorm sinken, wenn häufig genutzte Softwareanwendungen in die Cloud verlagert würden. Studien haben ergeben, dass sehr große Rechenzentren Energie effizienter nutzen als kleine lokale Rechenzentren

oder Serverräume. Dennoch brauchen wir europaweite Richtlinien, was grüne Rechenzentren, Plattformen und Betriebsmodelle im Detail ausmacht. Derzeit gibt es zahlreiche Initiativen, die sich mit dieser Frage beschäftigen – vom „EU Code of Conduct for Energy Efficiency in Data Centres" über den „Pakt für klimaneutrale Rechenzentren" bis hin zum EU-Klimaplan „Fit for 55".

In diesem Zuge sollten wir den Souveränitätsbegriff in der IT erweitern: Er darf nicht nur Datensicherheit und -unabhängigkeit umfassen, sondern auch den Klimaschutz. Grüne Rechenzentren zeichnen sich durch eine hohe Energieeffizienz aus, können per digitaler Steuerung optimiert werden und nutzen Synergieeffekte sowie Strom aus erneuerbaren Energien.

Das Einsparpotenzial von Cloud-Technologie haben viele unserer Kund*innen aus Branchen wie der Automobilindustrie, dem Transportgewerbe oder der Energieversorgung längst erkannt: Mit dem Wechsel in die Cloud möchten sie nicht nur Prozesse schlanker gestalten und flexibel skalieren, sondern auch ihren $CO_2$-Fußabdruck und ihre Kosten erheblich reduzieren. So lassen sich mit einem KI-basierten Prozess in der Open Telekom Cloud etwa beim Glasfaserausbau – eine besonders energieeffiziente Technologie zum Datenverkehr – die Kosten viel genauer, schneller und skalierbarer als zuvor kalkulieren.

**Besser mit den Beschäftigten**

Der dritte Trend ist nicht zu unterschätzen. Und dabei geht es nicht um Technologie, sondern darum, Mitarbeitende ins Thema Nachhaltigkeit einzubinden. CIOs und das IT-Team wählen zwar grüne IT-Lösungen aus und tragen so maßgeblich dazu bei, dass das gesamte Unternehmen klima- und umweltgerechter arbeitet. Aber sie sollten noch in eine weitere Rolle schlüpfen: in die der Motivator*innen. Damit innovative Technologien ihre Wirkung entfalten können, spielen die Motivation und das digitale Know-how der Beschäftigten eine zentrale Rolle. Sie sind diejenigen, die Tools für die täglichen Geschäftsprozesse nutzen. Sie setzen den Nachhaltigkeitswandel Schritt für Schritt um – sei es in der Produktion, im Einkauf oder der Entwicklung. Deshalb gilt auch: Maßnahmen sollten begreifbar gemacht werden. Das Stichwort lautet Visualisierung.

T-Systems bietet ihren Kund*innen beispielsweise das Dashboard „Syrah Sustainability" an. Damit behalten öffentliche und private Organisationen ihre Nachhaltigkeitsindikatoren im Blick und können anhand der aggregierten Informationen fundierte Entscheidungen treffen. Und der nächste Schritt? Auf die digitale Umsetzung folgen im besten Fall neue Ideen und Initiativen der Mitarbeitenden.

Ziehen alle Beschäftigte an einem Strang, können sie nicht nur die Nachhaltigkeit des eigenen Unternehmens verbessern, sondern tragen damit gleichzeitig durch die Reduzierung des $CO_2$-Fußabdrucks auch ökologische Verantwortung für ihre Kund*innen. Suchen Unternehmen also nach dem viel besagten Purpose, so wäre dieser Weg ein guter Start.

***Christian Till Roga***

# IT Service Provider

## DIE 5 TOP-HERAUSFORDERUNGEN UND DAS NÄCHSTE GROSSE DING

Was sind die kommenden Herausforderungen für IT Service Provider? Wir haben fünf aktuelle Themen herausgegriffen, die bei der Lieferung von IT-Services eine enorm wichtige Rolle spielen. Einige Punkte sind alte Bekannte, teilweise in neuen Gewändern. Aber Achtung: Mit einer neuen EU-Richtlinie kommt ein Thema in Dimensionen der DSGVO, dass IT Service Provider für die nächsten Jahre unbedingt auf dem Schirm haben sollten.

**Standardisierung vs. Anpassbarkeit vs. Automatisierung**

IT Service Provider müssen immer besser den Spagat hinbekommen zwischen Standardisierung einerseits und der individuellen Anpassung an Kundenlandschaften und -prozesse andererseits. Für das Management solcher IT-Strukturen sind flexible IT Service Management Lösungen gefragt. Diese sollten das Deployment und Mandantisierung in einer Art ermöglichen, welche den Compliance-Anforderungen der Kunden gerecht werden. Gleichzeitig brauchen die IT Service Provider eine zentralisierte Sicht auf die Gesamtsituation, um kosteneffizient eine Vielzahl von Kunden gleichzeitig verwalten und steuern zu können. Ein weiteres wichtiges Merkmal solcher ITSM-Tools ist die Möglichkeit zu flexibel konfigurierbaren Schnittstellen, über die Daten mit Kundensystemen ausgetauscht werden können. Alles muss dabei so standardisiert gestaltet sein, dass sich die Prozesse hochgradig automatisieren lassen.

**IT Security Awareness**

Im renommierten Allianz Risk Barometer für 2023 sind Cybervorfälle erneut als größtes globales Risiko für Unternehmen benannt, zusammen mit dem Risiko von Betriebsunterbrechungen. Es gilt also weiterhin massiv in IT-Sicherheit zu investieren, denn Angriffe, vor allem durch Ransomware-Gangs, sind an der Tagesordnung und können erhebliche Schäden verursachen. Aber auch Datendiebstahl und die Offenlegung personenbezogener Daten können zu hohen Schadensersatzansprüchen und Strafen sowie zu Reputationsschäden führen. Daher bleiben regelmäßige und praxisorientierte Maßnahmen wie Awareness-Schulungen und -Tests, aktives Patch Management und Penetration Tests sowie der Betrieb eines Security Operations Center (SOC) mit einem Security Information and Event Management (SIEM) auch in den kommenden Jahren eine lohnende Investition. Eine gute Grundlage zur Strukturierung dieser Maßnahmen ist ein unternehmensweites Information Security Management System (ISMS), welches mit einem IT-Service-Management-Tool integrierbar ist.

**Fachkräftemangel, Mitarbeiter-Gewinnung und Business Cases für AI**

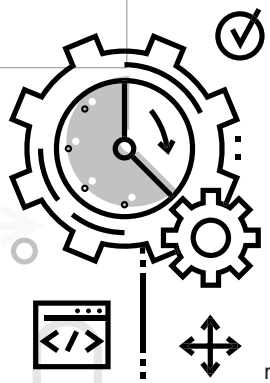
Experten sagen voraus, dass uns der Mangel an qualifizierten Mitarbeitenden auch in den nächsten Jahren begleiten wird. Deshalb bleibt das Outsourcing mittels Nearshoring und Offshoring eine mögliche Alternative, um der steigenden Nachfrage und dem Leistungsdruck gerecht zu werden. Objektiv einfacher ist es, den Nachwuchs selbst auszubilden und sich zu einem attraktiven Arbeitgeber mit einer Kultur zu entwickeln, in der sich auch die Digital Natives zu Hause fühlen. Gerade die hohe Dynamik der IT-Branche macht die Mitarbeiter-Gewinnung zu einer Marathon-Aufgabe. Dabei gibt es schon heute viele bekannte Aspekte, um dem Fachkräftemangel zu begegnen,

wie beispielsweise die IT-Berufe für Frauen attraktiver zu machen oder für mehr Inklusion zu sorgen. Eine weitere Chance bietet auch die schnelle Integration von IT-Fachkräften, die auf Grund von politischen Gegebenheiten als Flüchtlinge in Deutschland leben.

Ein anderer Ansatz, um dem Fachkräftemangen entgegenzuwirken, entsteht durch die Nutzung von AI im IT Service Management. Beispielsweise im Incident und Problem Management unterstützt intelligente Software bei der Klassifizierung von Störungen. So lassen sich Prozesse beschleunigen und entlasten bestehende Service Desk Mitarbeiter. Anpassungsfähige AI Desk Agents können intelligente Chats mit Kunden führen und lernen aus diesen Interaktionen. Darüber hinaus können AI-Tools wie Chat GPT auch im Knowledge Management eingesetzt werden und unterstützen hier bei den Formulierungen und der Strukturierung von Wissensdokumenten. Wobei hier die AI in der Regel nicht das eigentliche Wissen liefert, aber smarte Hilfestellung leistet. Es können Wissenslücken vermieden werden, da wichtige Informationen im Unternehmen bestehen bleiben. Das vereinfacht und beschleunigt beispielsweise Onboarding-Prozesse von neuen Mitarbeitern.

IT SERVICE PROVIDER WERDEN ERST DANN ZUM VERLÄSSLICHEN LÖSUNGSANBIETER, WENN SIE FLEXIBLE IT SERVICE MANAGEMENT SYSTEME EINSETZEN UND DIE GEFORDERTEN IT SERVICE DELIVERY PROZESSE STANDARDISIEREN UND AUTOMATISIEREN KÖNNEN.

**Bert Kondruß, Director Product Management, Service Management, USU Software AG, www.usu.com**



**„Hybrid" wird noch lange die Realität bleiben**

Auch IT Sevice Provider müssen sich neu ausrichten und sich an die Anforderungen an eine hybride IT-Umgebung anpassen. Eine große Rolle spielen hierbei die aktuellen Kundenanforderungen hinsichtlich der digitalen Transformation und dem Switch hin zu Cloud-Umgebungen. Gartner prognostiziert für 2023 weltweite Ausgaben von Public Cloud-Diensten von fast 600 Milliarden US$. Damit steigen die Cloud-Ausgaben im Vergleich zum Vorjahr erneut um 20% und machen somit den größten Teil der IT-Ausgaben aus. Der Wechsel in die Cloud wird sich also weiter fortsetzen, denn das verleiht den Kunden mehr geschäftliche Flexibilität. Aktuell ist die Welt aber noch hybrid und für manche Anforderungen wird sie es auch in Zukunft bleiben. Es braucht IT-Lösungen, die alte Anforderungen und neue verknüpfen können und die es ermöglichen, IT-Prozesse zu optimieren, egal ob im Rechenzentrum oder in der Cloud. Daher benötigen IT Service Provider auch Management-Systeme, um solche Umgebungen in allen Aspekten zu beherrschen: Ressourcen, Kosten und Governance. Die große Herausforderung: Es muss noch mehr als heute in Echtzeit geschehen.

**EU CSRD und EU-Taxonomie**

Mit der am 5. Januar 2023 in Kraft getretenen „Corporate Sustainability Reporting Directive (CSRD)" der Europäischen Union ist das nächste große Ding im Anmarsch. Ähnlich wie bei der Einführung der Datenschutz-Grundverordnung (DSGVO) kommen hier auf viele Unternehmen umfangreiche Berichtspflichten zur Nachhaltigkeit zu. Sie müssen dokumentieren, welchen Beitrag ihre Wirtschaftstätigkeit zum Klimaschutz oder zur Anpassung an den Klimawandel leistet. Dieses Thema wird viele Unternehmensbereiche durchziehen und ist nicht nur für große Konzerne relevant, sondern auch für eine Vielzahl von kleinen und mittleren Betrieben. Damit wird es sich auch direkt und indirekt auf alle IT Service Provider auswirken - in Dimensionen wie bei der Einführung der DSGVO. Diese sollten es deshalb als strategisches Thema für die kommenden Jahre einplanen.

**Fazit**

Unternehmen und Organisationen werden künftig noch stärker auf effiziente und transparente IT-Services angewiesen sein. IT Service Provider sind dann verlässliche Lösungsanbieter, wenn sie flexible IT Service Management-Systeme einsetzen und damit die geforderten IT Service Delivery-Prozesse standardisieren und automatisieren. Ein leistungsfähiges ITSM-Tool unterstützt bei all den genannten Herausforderungen.

***Bert Kondruß***

# Nutzungsdaten erfassen und analysieren

## KRITERIEN FÜR ERFOLGREICHE SOFTWARE USAGE ANALYTICS (SUA)

Nutzungsdaten zeigen schwarz-auf-weiß, ob ein Produkt beim Kunden ankommt oder ob es Zeit wird, die Geschäftsstrategie zu überdenken. Bei der Implementierung von Software Usage Analytics gibt es jedoch zentrale Kriterien zu beachten.

Wie lässt sich Kundenzufriedenheit messen? Um diese Frage zu beantworten, setzen Unternehmen oft eine ganze Batterie an Feedback-Instrumenten ein. Dazu gehören qualitative Methoden wie das klassische Kundengespräch, die E-Mail-Umfrage, die Auswertung von Anrufen im Support-Center oder die Rücksprache mit dem Vertrieb. Web Analytics Tools (Google Analytics, Microsoft App Insights) kommen zum Einsatz, um rudimentäre Daten über den User Flow in einer Software zu erfassen. Was diese Vorgehensweisen gemein haben: Sie geben häufig nur den Blick auf einen Teilausschnitt frei, sind selten repräsentativ und liefern kaum Kontext, um Rückschlüsse auf einzelne Kundensegmente zu ziehen.

Software-Anbieter haben daher in den letzten Jahren verstärkt in die Software Usage Analytics investiert und holen Kundenfeedback damit direkt über die Nutzung der Anwendung ein. Die Nachverfolgung und Auswertung von Benutzerinteraktionen gibt einen sehr detaillierten und datenbasierten Einblick in die Art und Weise, wie Anwender die Software in der Praxis nutzen. Was wird die Software beim täglichen Arbeiten genutzt? Und für welche Funktionen wäre ein Kunde eventuell bereit mehr zu zahlen?

### REIFEGRAD VON SUA NIMMT ZU

Laut einer weltweiten Umfrage von Revenera (Monetization Monitor: Software Usage Analytics 2022) setzen bereits 62 Prozent der Softwareanbieter auf Software Usage Analytics und sammeln und erfassen methodisch Telemetriedaten. Bis 2024 soll der Anteil auf 80 Prozent ansteigen. Dazu trägt auch der anhaltende Trend in Richtung nutzungsbasierte Geschäftsmodelle bei – allen voran SaaS. 41 Prozent der Produktmanager gehen davon aus, dass sich die Adoption von Lösungen rund um Usage Analytics in den nächsten eineinhalb Jahren weiter fortsetzt.

Dabei verbessert sich der Reifegrad der Lösungen zusehends – vor allem, was die Automatisierung der Datenerfassung angeht. Nur noch rund ein Drittel der Anbieter greift hier auf manuelle, zeitaufwändige Prozesse zurück (2022: 44%).

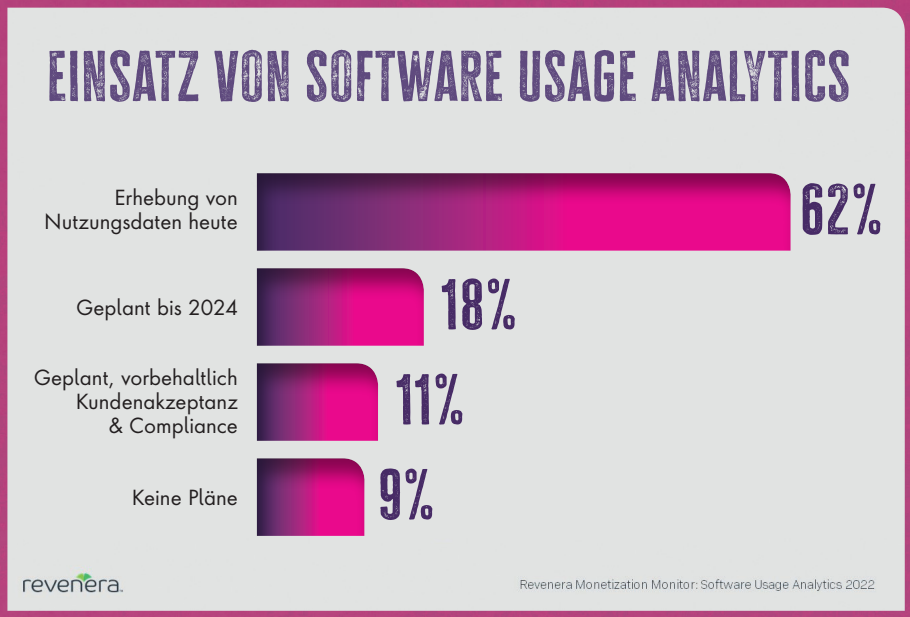



**Bild 1: Einsatz von Software Usage Analytics in Unternehmen weltweit.** (Quelle: Revenera)

## FÜNF ANFORDERUNGEN ZUR IMPLEMENTIERUNG

Die Implementierung solcher automatisierten Systeme setzt allerdings Zeit, Ressourcen und Expertise voraus. Entwicklerteams stehen vor der Frage, ob sie das Analysetool Inhouse entwickeln oder sich lieber auf eine kommerzielle Lösung verlassen sollen. Egal für welchen Weg sich Unternehmen letztendlich entscheiden, sie sollten in jedem Fall die folgenden Kriterien berücksichtigen.

### #1 Klarer Fahrplan & Zielsetzung

Die Entwicklung komplexer Softwaresysteme erfordert eine umfassende Vorab-Planung und eine genaue Zielsetzung. Der Aufbau eines Systems zur Software Usage Analytics ist da keine Ausnahme. Hier gilt es im ersten Schritt, abteilungsübergreifend eine Methodik festzulegen, um sicherzustellen, dass Fragen unterschiedlicher Stakeholder mit Hilfe des Analysetools auch tatsächlich beantwortet werden können. Idealerweise gehören daher sowohl Entwicklerchefs als auch C-Level Produktmanager, IT-Leiter sowie Vertriebs- und Marketingverantwortliche ins Team.

Gemeinsam lässt sich klären, wer Zugang zu welchen Informationen benötigt und wie das System Ad-hoc-Analysen (Exploration & Discovery) unterstützt. Darüber hinaus werden eindeutige Metriken und Metadaten für das Reporting definiert. Dazu zählen beispielswiese Informationen über die Hardware, auf der die Software läuft, Statistiken über Installationen und Laufzeiten sowie generelle und Feature-bezogene Nutzungsdaten.

Eine Kernfrage der Planung betrifft die Konfiguration der Telemetrie. Der Zeitpunkt der Datenübertragung ist hier maßgebend. Entwickler müssen zu diesem Zweck Ereignisse (Events) beziehungsweise Benutzeraktionen identifizieren, die von besonderem Wert für die Nutzungsanalyse sind, und festlegen, welche Daten beim Eintreten dieser Events gesammelt werden sollen. Darüber hinaus beinhaltet die Konfiguration das Einrichten von Protokollformaten, Kommunikationsprotokollen, Prozessen, Synchronisierungszeitplänen, Caching und Handhabung bei Offline-Nutzung.

> ENTWICKLERTEAMS STEHEN VOR DER FRAGE, OB SIE DAS ANALYSETOOL INHOUSE ENTWICKELN ODER SICH LIEBER AUF EINE KOMMERZIELLE LÖSUNG VERLASSEN SOLLEN.
>
> **Nicole Segerer, SVP und General Manager, Revenera, www.revenera.de**

Schließlich geht es bei der Planung auch darum, die Verfügbarkeit von Ressourcen zu klären. Um Software Usage Analytics in der Cloud zu betreiben, fallen Kosten für Instanzen an. Soll das System hingegen intern gehostet werden, sind neben einer skalierbaren Hardware-Infrastruktur auch weitere Software, Backup, Firewalls, Anti-Malware nötig.

### #2 Daten sammeln: Konfiguration der Telemetrie

Die automatisierte Datenerfassung ist das A&O von Software Usage Analytics. Dementsprechend umfangreich ist die To-Do-Liste für den Aufbau der Telemetrie zwischen Client und Server. Gefragt sind sichere und schlanke Kommunikationsprotokolle, um sensible Daten zu verschlüsseln und so zuverlässig und unterbrechungsfrei zurück an den Softwareanbieter zu übertragen. Die Client-Server-Protokolle müssen dabei in der Lage sein, Proxies, Firewalls, Webfilter-Gateways und anderen Netzwerkkonfigurationen zu umgehen. Für das Aggregieren, Komprimieren und Optimieren der Datenübertragung ist zudem eine individuelle Anwendungslogik erforderlich, die auch bei Kommunikationsfehlern (zum Beispiel: „Netzwerk nicht verfügbar") greift.

Im Vergleich zu anderen quantitativen Methoden punktet die Software Usage Analytics mit einer sehr genauen Segmentierung von Benutzerprofilen. Voraussetzung dafür ist, dass die Systeme automatisch Kunden- oder Benutzer-Installations-IDs generieren. Dieser (anonyme) Maschinenfingerabdruck ermöglicht es, Trends bei der Nutzung für jede Installation nachzuverfolgen und Installationsprofile mit Download-Quellen oder Marketingkampagnen zu verknüpfen. Softwareanbieter erhalten so auf unterschiedlichen Aggregationsebenen einen Einblick darüber, wie Anwender ihre Produkte nutzen – egal ob es sich dabei um ein bestimmtes Kundensegmente oder alle User innerhalb eines Kundenkontos handelt.

### #3 Daten speichern und verwalten: Auswahl der Datenbank

Bei der Software Usage Analytics steht Qualität vor Quantität. Doch selbst bei einer kleinen Zahl an definierten Metriken, entstehen in der Regel Terabytes an

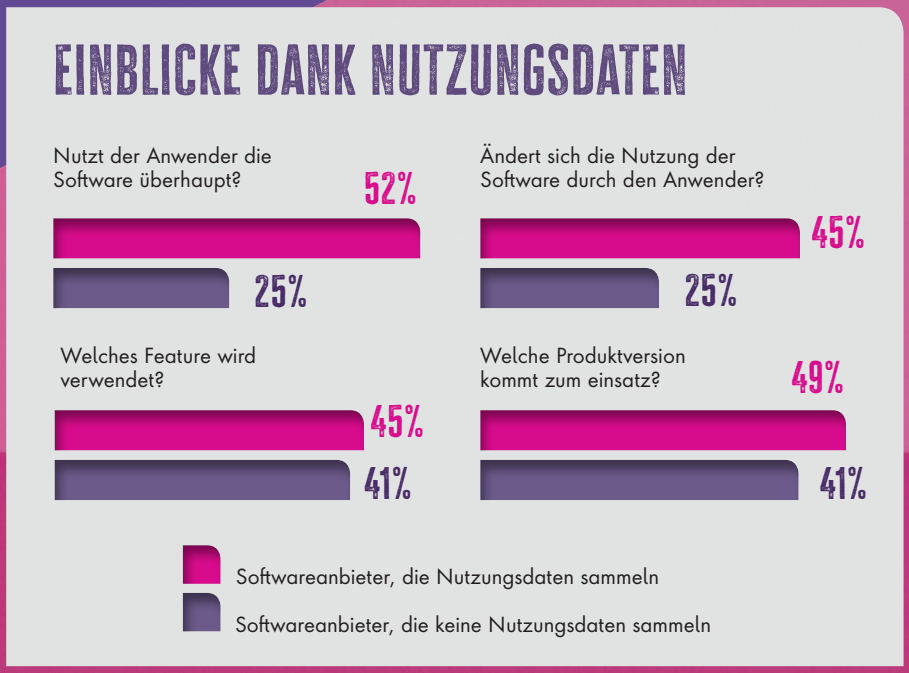



**Bild 2:**
**Software Usage Analytics erlaubt einen tiefen Einblick in die Nutzung von Software**
(Bilder: Revenera)

Daten, die es zu speichern, zu verknüpfen und zu analysieren gilt. Die zu Grunde liegenden Datenbanken sollten daher über eine hohe Skalierbarkeit verfügen.

Zwischen kommerziellen Lösungen und Eigenentwicklungen gibt es hier noch weitere Unterschiede: So ist bei vielen Dritt-Systemen eine individuelle Anpassung der zu verfolgenden und zu erfassenden Metriken nur begrenzt möglich. Im schlimmsten Fall werden nur Daten erfasst, die für das Produktmanagement-Team keine echte Relevanz besitzen und als „Datenmüll" in den Speichersystemen verbleiben. Inhouse entwickelte Systeme wiederum sind oft zu einseitig auf bestimmte Nutzungsdaten ausgerichtet. Ändern sich dann im Laufe der Zeit die Anforderungen, kann es schwierig sein, neue Metriken einzubinden, ohne den Client-Code komplett umschreiben zu müssen. Einen guten Mittelweg stellen daher in der Software hinterlegte Remote-Control-Funktionen dar: So können Anwender über ein Dashboard das Tracking von Metriken flexibel stoppen, starten oder anpassen.

## #4 Daten visualisieren: Erstellen von Reports

Um der Komplexität der Datenmenge Herr zu werden, sind neben hoher Skalierbarkeit und Flexibilität auch Visualisierungs-Frameworks entscheidend. Denn selbst der größte Datenpool hilft nur wenig, wenn es an der visuellen Aufbereitung und dem Kontext fehlt, um Analysen einordnen und nutzen zu können. Interaktive Dashboards, aussagekräftige Berichte mit Drill-Down-Funktionalität sowie Export-Möglichkeiten gehören daher zur Grundausstattung einer jeden Software Usage Analytics-Lösung.

Da die Analyse der Softwarenutzung zudem für unterschiedliche Abteilungen sowie ein breites Spektrum an Führungskräften, Managern und Entwicklern von Wert ist, sollten die Systeme idealerweise auch individuelle, anwenderspezifische Ansichten ermöglichen – und zwar in Echtzeit. Lassen sich bei einer Benutzergruppe beispielsweise Updates der Software nicht mehr durchführen, können die technischen Verantwortlichen schneller reagieren, das Problem lösen und so den Support vor einer Flut an Kundenanfragen bewahren.

## #5 Datenschutz und Privatsphäre

Beim Erfassen, Speichern und Sammeln all dieser Daten, wie steht es da mit dem Datenschutz? Hier ist klarzustellen: Die Produktnutzungsanalyse basiert auf anonymisierten Daten und bewegt sich somit im Rahmen der Datenschutzbestimmungen. Der Blick auf den einzelnen Nutzer ist für die Evaluierung des Softwareprodukts weder relevant noch beabsichtigt. Vielmehr werden die Daten aggregiert, um übergeordnete Trends und Muster im Nutzerverhalten aufzudecken.

Um ein hohes Maß an Datensicherheit zu garantieren, sollten die Systeme über granulare Zugangskontrollen auf allen Ebenen verfügen. Opt-in/Opt-out Optionen stellen zusätzlich sicher, dass Anwender das Tracking ihrer Softwarenutzung jederzeit beenden oder einschränken können. Darüber hinaus müssen bei der Konzeption von Usage Analytics-Systemen regionale Datenschutzbestimmungen genau verfolgt und Compliance-konform umgesetzt werden. In der EU heißt das u. a. eine lokale Speicherung der Daten, um einen DSGVO-konformen Umgang zu garantieren.

### FAZIT

Wie erfolgreich die Software Usage Analytics tatsächlich ist, hängt wie immer stark vom Buy-in der beteiligten Teams, den technischen Rahmenbedingungen sowie anderen Faktoren ab. Ist die Implementierung jedoch erstmal erfolgreich, gewinnen Unternehmen wertvolle KPIs, um ihre Roadmap bedarfsorientiert zu planen und die Zufriedenheit ihrer Kunden nicht nur zu messen, sondern kontinuierlich zu verbessern.

***Nicole Segerer***

# Customer Relationship Management

## DAS SYSTEM IST SELTEN SCHULD!

Viele Unternehmen hadern mit ihrem aktuellen Customer Relationship Management (CRM)-System, warum eigentlich?

Die User sagen, es sei umständlich zu bedienen, es fehlen wichtige Funktionen, es stehle ihnen die Zeit und es arbeite sogar fehlerhaft. Ein gruppendynamischer Prozess setzt ein, der dazu führt, dass alles, was im Unternehmen schiefläuft, dem CRM angeheftet wird.

Doch nicht die Software ist schuld, sondern vielmehr sind es die Verantwortlichen, die nicht in der Lage sind, für eine sinnvolle Nutzung zu sorgen. Das CRM wird zum Sündenbock für eine unterlassene oder missglückte Analyse- und Konzeptionsphase. Bedenkt man, dass Analyse und Konzeption zusammen nur etwa 10 Prozent der Zeit und rund 10 Prozent der Kosten ausmachen, ist es schon ein unverantwortliches Risiko, diese Phase zu überspringen.

SYSTEMATISCHES KUNDENMANAGEMENT BEDEUTET, UNTERNEHMEN BENÖTIGEN GANZHEITLICHE, ZUKUNFTSORIENTIERTE CRM-KONZEPTE, BASIEREND AUF DEN VIER KLASSISCHEN EBENEN: STRATEGIE, PROZESSE, MENSCHEN UND SYSTEME.

**Stephan Bauriedel, CRM-Experte, www.erfolg-mit-crm.de**

**Ursache: Die Analyse- und Konzeptionsphase**

Bei einer Fehleranalyse ertönt häufig derselbe Einwand: „... mein CRM ist wirklich schlecht!" Es gibt sicher viele CRM-Systeme, die technologisch veraltet oder funktional mangelhaft sind. Doch der Markt hat sich in den vergangenen fünf Jahren konsolidiert und zählt nur noch sechs Premium CRM. Es ist nahezu unmöglich, in eine schlechte CRM-Software zu investieren, wenn man seinen individuellen Anforderungskatalog erstellt und die möglichen Systeme daraufhin evaluiert.

Mit der Konzeption des Systems und dessen Anwendung erlangen Unternehmen Sicherheit und Orientierung. Wichtig ist, zu verstehen, wie das Unternehmen heute arbeitet (Ist-Analyse) und wie es sich zukünftig mit einem modernen CRM-System (Soll-Konzept) aufstellen möchte. Es geht um höchste Qualität an allen Punkten mit Kundenkontakt und die Optimierung der internen Prozesse in Bezug auf Effizienz, Transparenz und Professionalisierung.

Das CRM zeigt in der 360-Grad-Kundensicht alle Vorgänge und unterstützt die kundennahen Prozesse vom Erstkontakt bis zum Auftrag und in der Zeit danach. Das gesamte Kundenmanagement wird schneller, besser und einfacher. Die Ausrichtung und Verzahnung der Strategie, der Prozesse und Systeme sorgen dabei für den Unterschied. Zahlreiche Referenzen belegen dies.

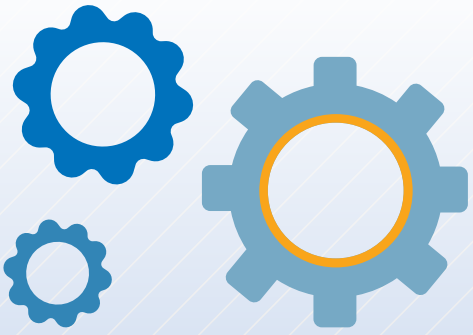
**Projekthürden**

Auf dem Weg zum Erfolg gibt es jedoch noch weitere Hürden, die ein Projektleiter kennen sollte. Das richtige CRM-System auszuwählen, ist dabei noch die einfachere Sache. Weitaus schwieriger ist, den organisatorischen Wandel zu gestalten. Ein CRM-System erfolgreich einzuführen, bedeutet, die Mitarbeiter mitzunehmen. Dabei gilt es, den Nutzen immer wieder hervorzuheben und – besonders wichtig – die Systemanbieter zu führen. Die härteste Nuss, die es dabei zu knacken gilt, ist das Management.

**PLUS**

Die größten Fallen bei der CRM-Software Auswahl:
**https://bit.ly/3jmruCB**

Tipps zur CRM Auswahl:
**https://bit.ly/3jiSkf1**



**CRM ist nicht nur Software**

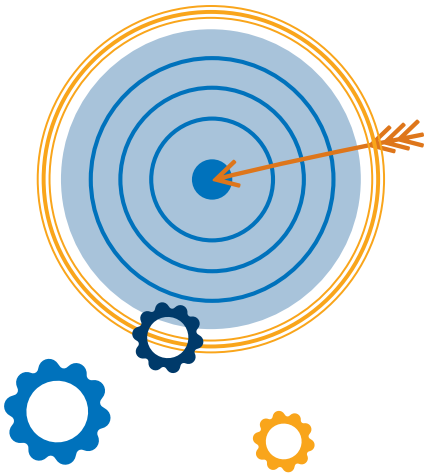
Bei der Einführung von CRM handelt es sich im Kern um ein Veränderungsprojekt. Obwohl der Projektleiter circa 80 Prozent seiner Zeit in die Implementierung investieren wird, sind die restlichen 20 Prozent entscheidend für den Erfolg. In der Praxis hat sich gezeigt, dass Projekte, die sich nur auf die Technik fokussieren, schnell scheitern. Ist das Vorhaben dagegen als Projekt zur Veränderung der Prozesse angelegt, konzentrieren sich alle Kräfte vorrangig auf den Nutzen. Hierfür ist es erforderlich, die Ziele zu kennen, einen Bauplan zu haben, prozessorientiert zu denken, die Mitarbeiter zu motivieren und zu schulen. Die Vorarbeiten der Analyse- und Konzeptionsphase können nun genutzt werden, um das CRM sukzessive von innen nach außen zu verkaufen.

**Customizing ist Pflicht**

Die erwähnten Premium-CRM-Systeme basieren auf moderner Technologie, haben eine hohe funktionale Reife, sind benutzerfreundlich und hochgradig anpassbar. Ein ausgereiftes CRM-System besitzt „im Standard", also ohne Anpassung, bereits mehr als 80 Prozent der erforderlichen Funktionalität. Die fehlenden 20 Prozent werden im Rahmen des Customizings umgesetzt. Der Systemanbieter individualisiert das CRM-System nach den Anforderungen des Unternehmens. Dazu gehören Masken, Einstellungen in den Funktionen und Schnittstellen. Dieses Customizing benötigt eine Anleitung, etwa ein prozessorientiertes Lastenheft, damit der Systemanbieter das CRM bauen kann.

**Vertrauen in den Partner**

Bei der Auswahl des Systempartners zählen vorrangig die Kompetenz, Erfahrungen und Sympathie. Bei den Verhandlungen ist zu bedenken, dass die Systempartner bei ihren Präsentationen häufig blumig von Customer Experience sprechen, von Strategie- und Prozessberatung. Am Ende der Gespräche und Verhandlungen verkaufen sie ein üppiges Paket an Manntagen für das Customizing.



Die vielen Anglizismen der Systemanbieter sind jedoch nur Blendwerk, die Erfolgsfaktoren bleiben leere Versprechungen. Es bleibt Aufgabe des Unterneh-

mens, die Zukunft des Kundenmanagements zu planen und in die Realität umzusetzen. Dazu sollte das Management – von der Unternehmensführung bis zur Projektleitung – über die Möglichkeiten des CRM-Systems und die Fähigkeiten der Mitarbeiter informiert sein. Nur dann kann der Projektleiter den Implementierer führen und das Ergebnis seiner Arbeit prüfen. CRM lässt sich nicht kaufen, nicht beim Systemanbieter und auch nicht beim Implementierer.

**Resilienz des Managements**

Die Nutzung des CRMs als Informations- und Kommunikationsinstrument ist über alle Hierarchiestufen hinweg erforderlich, jedoch aufgrund der strukturellen Abhängigkeiten schwierig einzufordern. Ein Beispiel für Resilienz im Management ist, dass das Führungsverhalten der persönlichen Berichterstattung „er berichtet an mich" weiter praktiziert wird. Diese veralteten Machtstrukturen ruinieren die neu gewonnene Effizienz. Die treffende Antwort eines Kundenbetreuers beschreibt, wie CRM gelebt werden sollte: „Lieber Vorgesetzter, alle meine Verkaufschancen stehen im CRM und sind aktuell. Bitte öffne dein CRM und informiere dich selbst, denn ich bin beim Kunden!"

**Erfahrung**

Kann eine gescheiterte Projekteinführung gerettet werden? Ich habe es noch nicht erlebt, denn in den Köpfen der Mitarbeiter ist das vorhandene System bereits komplett verbrannt. Aus meiner Sicht braucht es einen Neuanfang mit neuen Playern und neuem Vorgehen.

Als Autor dieses Artikels – mit mehr als 20 Jahren Erfahrung – kann ich sagen, es liegt nie am CRM-System, sondern an der CRM-Einführung. Fehlkäufe und schlechte CRM-Einführungen entstehen, weil Verantwortliche das Vorhaben unterschätzen. Modernes Kundenmanagement erfordert ein Umdenken: Die Strategie, die Prozesse und die Menschen sind Teil des Projektes genau wie das System.

***Stephan Bauriedel***

# MESSBARE ERFOLGE DIGITALER STRATEGIEN

## UNTERNEHMEN FÜR MULTI-CASE-STUDY GESUCHT

Digital-Experte Stephan Bauriedel sucht im Rahmen seiner Doktorarbeit zu betriebswirtschaftlichen Erfolgen digitaler Strategien in der Industrie Unternehmen für eine Multi-Case-Study. Die mittelständischen Unternehmen oder Konzerne sollten die digitale Transformation bereits abgeschlossen haben und ihre Erfolge präsentieren wollen. Die Teilnehmer der Studie erhalten belastbare Erkenntnisse und einen neuen Blickwinkel auf mögliche Potenziale.

- Die Multi-Case-Study untersucht die drei wichtigsten Fragen rund um die Digitalisierung der Geschäftsmodelle: Woher kam der Impuls für die Digitalisierung? Welches Vorgehen wurde verfolgt? Was waren die betriebswirtschaftlichen Erfolge? Anhand eines Fragebogens werden der initiale Impuls, die Instrumente und die Wirkung der Digitalisierung gemessen. Hierfür ist es notwendig, die betriebswirtschaftlichen Kenngrößen vor und nach dem Projekt zu erheben.
- Die Studie bietet die Möglichkeit, die digitale Transformation objektiv und aus einem betriebswirtschaftlichen Blickwinkel bewerten zu lassen. Daraus ergeben sich Impulse für die teilnehmenden Unternehmen, weitere Potenziale zu nutzen. Darüber hinaus bewertet Stephan Bauriedel die digitale Strategie, gibt Feedback und steht als externer Sparringspartner zur Verfügung.

**Weitere Informationen und Anmeldeformular:**
**www.digital-action.de**

# Kleiner Finger, ganze Hand

## WAS EIN MODERNES CRM-TOOL ALLES KÖNNEN MUSS

Das moderne CRM ist mehr als die Datenbank von früher. Doch die Anforderungen an das Sales-Tool steigen und steigen. Kann ein CRM da noch Schritt halten? Die Anforderungen an ein CRM-Tool der Moderne – und was dieses tatsächlich leisten kann.

Mit dem Beginn der Pandemie endete 2020 ein Jahrzehnt der relativen wirtschaftlichen Stabilität und begründete eine Zeit der wirtschaftlichen Unsicherheit: steigende Energiekosten, Inflation, ein abnehmendes Konsumklima. Summa Summarum: die Spendierfreudigkeit der Privat- und Geschäftskunden nahm und nimmt ab.

Dementsprechend rückt und rückte der Vertrieb in den Mittelpunkt vieler Unternehmen; denn dieser ist in Krisenzeiten der maßgebliche Umsatztreiber vieler Firmen. Er muss die Bestandskunden bei Laune und ihr Auftragsniveau hochhalten – und das, obwohl deren Budgetgürtel aufgrund der wirtschaftlich schwierigen Zeiten garantiert enger geschnallt werden müssen. Und wenn bestehende Partner doch wegbrechen oder ihr Invest zurückfahren, liegt es am Ver-

trieb, diesen Umsatzrückgang durch die Akquise neuer Leads aufzufangen.

Um dieser Verantwortung gerecht zu werden, sind heutzutage viele Vertriebler*innen und Unternehmen auf die Nutzung von Customer-Relationship-Management-Tools (CRMs) angewiesen. Das zeigt beispielsweise eine Umfrage des estnischen Unternehmens Pipedrive. Dieses befragte für den Report „The State of Sales & Marketing" über 1.000 Vertriebsexperten und analysierte den Status Quo zu Vertrieb und Marketing in kleinen und mittelständischen Unternehmen. Eines der Ergebnisse: Die Wahrscheinlichkeit, mit der Vertriebsteams ihre Umsatzziele erreichen, ist um ganze 16 Prozent höher, wenn sie im Arbeitsalltag auf digitale Hilfsmittel zurückgreifen können. 76 Prozent der Unternehmen, die CRM-Tools verwenden, wuchsen stärker als im Vorjahr. Auf der anderen Seite stagnierten ein Drittel der Unternehmen, die auf das Tool verzichten, beziehungsweise sie schrumpften sogar.

**Der Vertrieb, neu erfunden**

Das liegt vor allem darin begründet, dass der Vertrieb heute immer mehr in den digitalen Raum rückt. Diese Entwicklung begann natürlich schon vor Jahren, wurde aber mit der Corona-Pandemie auf ein neues Level gehoben. Die Website einer Firma ist deren Visitenkarte, die erste Anlaufstelle potenzieller Kunden und der Ort der ersten Kontaktaufnahme. Dieses Beispiel lässt sich mit dem asiatischen Internetriesen Alibaba veranschaulichen: Dessen Chatbot beantwortete 2021 über 300 Millionen (!) Kundenanfragen. Natürlich kommt das durchschnittliche mittelständische Unternehmen nicht ansatzweise auf solche Zahlen, doch selbst hier reden wir inzwischen von teils mehreren hundert Anfragen pro Woche.

Zeitgleich – und hier wird die eigentlich erfreuliche Zunahme der Kontaktanfragen für viele Unternehmen zum Problem – hat sich der Anspruch vieler Kunden, ganz egal, ob im Privat- oder Geschäftskundensegment, drastisch verändert.

Zum einen wäre da die wachsende Ungeduld vieler potenzieller Kunden. Stellen diese eine Online-Anfrage an ein Unternehmen, beträgt die optimale Reaktionszeit laut einer Studie des Harvard Business Review und Insight Sales gerade einmal fünf mickrige Minuten. Gleichzeitig betont das Harvard Business Review, dass nur 37 Prozent der Vertriebsmitarbeiter*innen ihren Leads innerhalb einer Stunde antworten; die durchschnittliche Reaktionszeit liegt bei 42 Stunden.

Mehr noch: Interessenten wollen nicht nur zügige Antworten auf ihre Anfragen, sondern auch noch individuelle, personalisierte Betreuung und keine Stangenware. Kurzum, nicht nur der Druck auf, sondern auch der Workload ist für Vertriebler*innen heutzutage immens. Und dies beeinflusst alle Phasen der Vertriebspipeline. Von der Leadgenerierung bis zur Bestandskundenpflege. Ohne ein CRM lässt sich dieser Aufwand kaum bewältigen oder betreiben.

**Was ein modernes CRM können muss – und der Realitätscheck**

Auch unser Verständnis von CRMs hat sich dementsprechend in den vergangenen Jahren deutlich verändert. Von einer Art Übersichtstool, einer Datenbank, in welcher Vertriebsexpert*innen ihre Leads einpflegen, Informationen hinterlegen und ihre Vertriebspipeline visualisieren konnten, zu einer aktiven, automatisierten Unterstützung, die jede wertschöpfende Aufgabe und Phase in der Customer Journey des Vertriebs abdeckt. Was also muss ein modernes CRM alles können?

DAS CRM-TOOL DER MODERNE IST EIN ALLESKÖNNER: EINE ALL-IN-ONE-PLATTFORM, DIE JEDEN SCHRITT DER CUSTOMER JOURNEY ABDECKT. EIN HELFER, DER AKTIV UND AUTOMATISIERT MITARBEITET.

**Shaun Shirazian,**
**Chief Product Officer, Pipedrive,**
**www.pipedrive.com**

Foto: Helis Hämarsalu

**#1 Digitale Kundenakquise: Die Lead-Generierung**

Jene Customer Journey beginnt mit der Akquirierung und der Qualifizierung neuer Kunden. Das umfasst die Recherche potenzieller Leads, die Recherche wichtiger Informationen über eben diese Kontakte, ja sogar die Kontaktaufnahme.

Denn moderne CRMs bieten beispielsweise integrierte, kuratierte und filterbare Lead-Datenbanken. Sie sind damit nicht nur eine Datenbank bestehender, sondern auch ein Sourcing-Tool für noch nicht vorhandene Kunden. Automatisch durchsucht die Technologie Tausende von Kundenprofilen nach den gewünschten Kriterien und präsentiert dem Verkäufer in kurzer Zeit passende Kandidaten, anstatt dass diese ressourcenintensiv das eigene Netzwerk abgrasen, Google-Recherchen betreiben oder manuell Kontaktdatenbanken nach möglichen Leads durchforsten müssen.

Und auch, wenn der mögliche Interessent von selber auf den Plan tritt und eigen-

ständig die Website des verkaufenden Unternehmens aufruft, handeln moderne CRMs. Denn, analog zum eingangs erwähnten Alibaba-Beispiel, bieten viele CRM-Unternehmen inzwischen selbst eigene Chatbots, die sich auf die Website integrieren lassen, an – oder API-Schnittstellen zu der Software anderer Anbieter. Der Clue an dieser Verknüpfung von Chatbot zu CRM: Informationen, die im Gespräch des Bots und des Interessenten abgeklappert werden, können so direkt in das Kundenprofil im CRM übertragen und aufgeführt werden. Tritt dann der Vertriebsexperte mit diesem Lead in Kontakt, kann er ohne Umschweife auf diesen Wissensfundus zurückgreifen. Zudem analysieren Tools das Verhalten von Website-Besucher*innen, lernen aus Verweildauer und Klickverhalten und sprechen dem Mitarbeiter so intelligente Empfehlungen aus, zum Beispiel bei welchem Lead sich die direkte Ansprache lohnt.

Apropos Automatisierung: Moderne CRMs nehmen den Vertriebler*innen auch mühselige Admin-Aufgaben ab; etwa die Datenübertragung, Automatisierung oder Synchronisierung. Denn diese zeitintensiven, kleinteiligen Tasks lenkten viele Vertriebsmitarbeiter*innen in der Vergangenheit entweder von ihrer eigentlichen Aufgabe, dem Verkaufen, ab oder wurden von diesen gerne auf die lange Bank geschoben – was unvollständige oder unsaubere Kundendatensätze zur Folge hatte.

### #2 Der Austausch mit dem Kunden: Lead-Qualifizierung, Verhandlungen und der Deal-Abschluss:

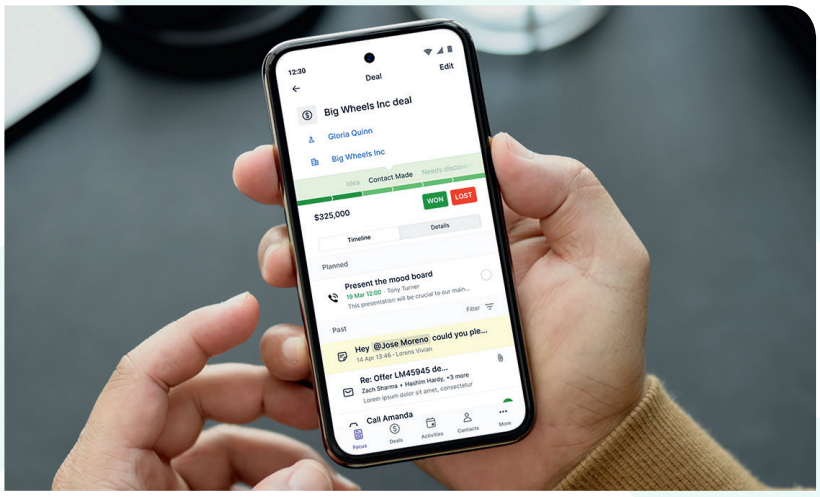
Ist der Kontakt zum Lead durch den Einsatz technischer Hilfsmittel einmal aufgewärmt, beginnt die eigentliche Sternstunde des Vertrieblers. Und hier ist der Faktor Mensch besonders wichtig: laut einem gemeinsamen Bericht von Google und der Unternehmensberatung BCG geben 40 Prozent der Konsument*innen online mehr aus als geplant, wenn der Webshop-Betreiber den personalisierten Kontakt bietet. Und auch B2B-Kunden verlangen an diesem Punkt der Customer-Journey laut einer McKinsey-Untersuchung gerne den „Human Touch".

Doch das bedeutet nicht, dass das CRM hier keine gewichtige Rolle im Prozess spielt. Vielmehr rückt es nun – vorerst – in den Hintergrund und arbeitet dem Experten zu, beziehungsweise macht diesem den Job so einfach wie nur irgend möglich.

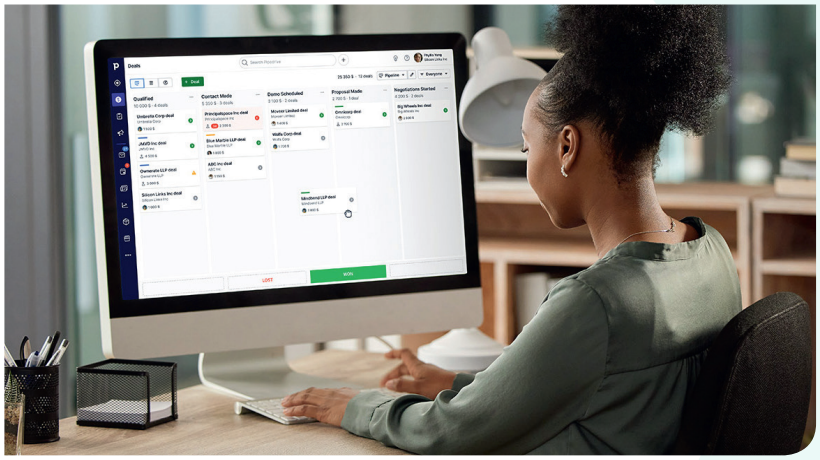
Etwa in dem es zum einen alle möglichen Kommunikationskanäle mit dem Kunden in einer Übersicht bündelt – ganz egal ob Chats mit dem Bot, Emails, WhatsApp oder Social Media Messenger. So hat der Vertriebler jeden Gesprächsverlauf schnell vor Augen. Zudem sollte ein modernes CRM die Posteingänge des ganzen Teams bündeln können. Denn in vielen Unternehmen ist Sales kein Solo, sondern Teamwork. Sprich: oft stehen mehrere Vertriebsmitarbeiter*innen mit einem Unternehmen in Kontakt. Und in diesen Fällen ist eine zentrale Übersicht über die Gesprächsverläufe elementar, um zu vermeiden, dass eventuell wichtige Informationen im Team untergehen.

Und auch in dieser Verkaufsphase spielt die Automatisierung eine immer größere Rolle. Etwa in Form automatisierter E-Mail-Sequenzen, die für Vertriebsmitarbeiter*innen automatisch Follow-Ups übernehmen, damit, etwa in stressigen Zeiten, kein Lead in der Aufgaben-Flut untergeht. Sind diese automatisierten Follow-Ups nicht gewollt, bieten viele moderne CRMs als Alternative an, selbstständig Reminder an die jeweiligen Sales-Expert*innen zu schicken.

Und, zu guter Letzt, sollte ein modernes CRM in dieser Phase des Verkaufszyklus auch über ausgeprägte Analyse-Fertigkeiten verfügen und dementsprechend




Quelle: Pipedrive



Quelle: Pipedrive

die Verkäufer*innen beraten, was sie wann tun müssen, um den Deal in die nächste Phase zu schieben – oder warum im Worst Case ein Deal gescheitert ist.

## #3 Nach dem Deal ist vor dem Deal: After-Sales und Lead-Pflege

Idealerweise sorgt ein reibungsloser Deal-Abschluss dann natürlich dafür, dass der Kunde kein „One and Done" ist, also kein einmaliger Einkauf. Das Ziel ist natürlich, jenen Lead zu einem dauerhaften Kunden zu machen. Und somit beginnt die Phase des After-Sales-Betreuung und der Lead-Pflege.

46 Prozent der deutschen Konsumenten befürworten personalisierte Werbung, so das Ergebnis einer Studie der Beratungsgesellschaft McKinsey. Gerade bei großen Kundenstämmen liegt es jedoch fern des menschlich Machbaren, alle Kunden und deren Bedürfnisse persönlich und regelmäßig abzufragen. So wundert es nicht, dass die meisten Werbebotschaften für 42 Prozent der Befragten nach wie vor wie Massenware wirken. Auch hier hilft Technologie, die die Kundenbedürfnisse stetig analysiert, gewisse Trends aus Branchen ableitet und Learnings aus früheren E-Mails, wie Click-Rate oder bevorzugte Produkte, an den Vertriebsmitarbeiter für das Leadmanagement weitergibt.

**Mobile ist wichtiger denn je**

Beinahe jedes dritte deutsche Unternehmen berichtet von mehr Anfragen für Fernarbeit, so der State of Spending Report des Unternehmens Pleo. Damit wird eine Vermutung bestätigt, die viele Expert*innen bereits zum Start des Lockdowns äußerten: das Home Office ist gekommen, um zu bleiben. Damit müssen moderne CRMs eben jenen Remote-Work-Aspekt berücksichtigen und außerhalb der klassischen Büro-Räume und Firmenserver sowie auf mobilen Endgeräten funktionieren. Cloud-Applikationen, die sich von überall öffnen lassen sowie Plug-and-Play-Produkte, die ohne aufwendiges Software-Setup direkt aus dem Browser geöffnet und verwendet werden können, sind hier hervorzuheben.

Das CRM-Tool der Moderne ist somit, summa summarum, ein Alleskönner: eine All-in-One-Plattform, die jeden Schritt der Customer Journey abdeckt. Ein Helfer, der aktiv und automatisiert mitarbeitet. Ein Teamplayer, der über die eigenen Kernfunktionalitäten Zusatzfeatures – oder zumindest Schnittstellen zu weiteren Anbietern offeriert. Ein Weiterdenker, der nicht in der starren, veralteten Sales-Philosophie operiert, sondern das Marketing mit einschließt. Und ein Mobile-Enabler, der immer und von überall einfach und schnell bedient werden kann. Ein hoher Anspruch an ein CRM? Bestimmt! Aber dennoch genau das, was der moderne Vertrieb braucht.

***Shaun Shirazian***


# Revolution der Chatbot-Technologie

## EINSATZ IM B-TO-B-BEREICH

WICHTIG IST, DASS ANWENDER SICH NICHT DAS DENKEN ABNEHMEN LASSEN, DENN AKTUELL NEIGT CHATGPT NOCH DAZU, INFORMATIONEN NACH GUTDÜNKEN NEU ZU SORTIEREN. EIN GRÜNDLICHER FAKTENCHECK IST DAHER UNVERZICHTBAR..

**Raoul Plickat, Gründer, CopeCart, www.copecart.com**

ChatGPT hat in den letzten Monaten die Schlagzeilen dominiert: Die AI-basierte Chatbot-Technologie sorgt aus gutem Grund für Aufregung, denn ihre Antworten sind praktisch nicht von den Aussagen eines Menschen zu unterscheiden. In Zukunft soll das Tool kostenpflichtig werden – gute Nachrichten für B2B-Unternehmen, die die Technologie langfristig für ihre Zwecke nutzen möchten.

„Derzeit ist ChatGPT für professionelle Anwender kaum benutzbar, weil es ständig mit minderwertigen Daten gefüttert wird", erklärt Raoul Plickat. „Die geplante Kostenpflichtigkeit sehe ich daher als ein positives Signal für die Zukunft des Marketings." Im Folgenden, zeigen wir wie ChatGPT das Marketing revolutionieren wird und warum gerade B2B-Unternehmen davon profitieren können.

**Die aktuelle Situation**

Schon jetzt bietet künstliche Intelligenz unzählige Möglichkeiten, den Arbeitsalltag zu vereinfachen. So sind Helfer wie ChatGPT zum Beispiel dazu in der Lage, persönliche Notizen zu ergänzen oder ganze Power-Point-Präsentationen zu erstellen. All diese Dinge wären noch vor einigen Jahren unvorstellbar gewesen.

Das soll nicht heißen, dass KIs in Zukunft massenhaft Jobs gefährden werden – im Gegenteil: Experten gehen davon aus, dass Artificial Intelligence die heutigen Aufgabenfelder erweitern und neue Jobs entstehen lassen wird. Denn trotz aller Leistungsfähigkeit ist eine KI immer nur so smart wie der Mensch, der sie für ihre Zwecke nutzt. Es braucht also eine Person, die sich ausführlich mit der Thematik beschäftigt hat – und daher weiß, welche Fragen sie stellen muss, um beispielsweise einen detaillierten Marketingplan zu erhalten.

**Zukünftige Weiterentwicklung und Qualitätssteigerung**

Aktuell ist die Chatbot-Technologie noch nicht ausgereift und verlässlich genug,

um in jedem Bereich sinnvoll eingesetzt werden zu können. Dass ChatGPT kostenpflichtig wird, ist jedoch ein positives Signal, das darauf hindeutet, dass OpenAI die Weiterentwicklung des Tools durch finanzielle Mittel vorantreiben möchte. Hochwertigere Anfragen werden die Folge sein, was die KI letztendlich vielerorts zu einem wertvollen Helfer machen wird. Der Preis von 20 Dollar pro Monat für die Plus-Version beinhaltet einen garantierten Zugriff auch bei hoher Nachfrage, des Weiteren soll die Reaktionsgeschwindigkeit von ChatGPT auch etwas höher sein als für User der kostenlosen Variante.

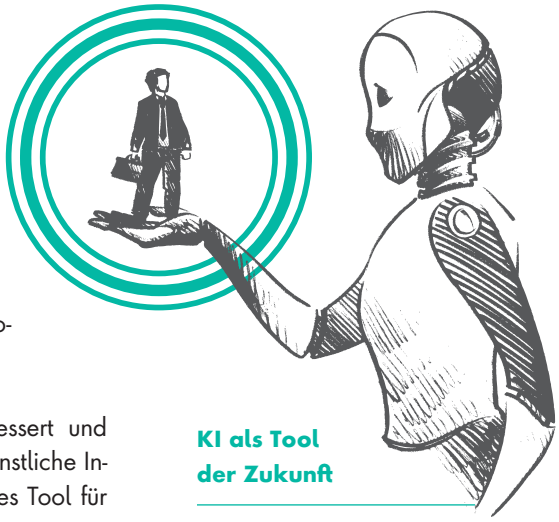
Verantwortliche im B2B-Bereich können die Technologie theoretisch schon jetzt für tägliche Arbeiten wie die Kommunikation mit Kunden, die Erstellung von Texten für Social Media oder die Analyse von Kundenfeedback einsetzen. Wichtig ist, dass sie sich dabei nicht das Denken abnehmen lassen, denn aktuell neigt ChatGPT noch dazu, Informationen nach Gutdünken neu zu sortieren. Ein gründlicher Faktencheck ist daher unverzichtbar.

**KI als Tool der Zukunft**

Die aktuelle Version ChatGPT-3, die derzeit in aller Munde ist, ist erst der Anfang: Noch dieses Jahr soll mit ChatGPT-4 eine aktualisierte Version auf den Markt kommen, die erneut für eine starke Disruption sorgen wird. In den nächsten zwei bis drei Jahren sind weitere Fortschritte zu erwarten: Schon jetzt wird die Technologie jeden Monat besser.

Sofern sie durchgehend verbessert und richtig eingesetzt wird, kann künstliche Intelligenz durchaus ein nützliches Tool für die Zukunft sein, das neue Geschäftsfelder im gesamten Marketingsektor schaffen könnte. Damit wird sie direkten Einfluss auf tägliche Arbeitsabläufe nehmen. Man darf also gespannt sein, was der Release von ChatGPT-4 mit sich bringt.

***www.copecart.com***



**KI als Tool der Zukunft**


Das **eBook** umfasst 46 Seiten und steht zum kostenlosen Download bereit.
**www.it-daily.net/download**

# STORAGE

## WHAT`S NEW?

Daten entwickeln sich in der modernen digitalen Wirtschaft zur wichtigsten Währung. Gleichzeitig steigen Kosten, Komplexität und Bedrohungen für die Datensicherung. Ein effizienter Schutz der Daten tut Not, unabhängig davon soll der Nutz- und Mehrwert dieser „Assets" als Active Archive voll ausgeschöpft werden.

Das Backup hat sich zu einer existentiellen Anforderung für Unternehmen in der digitalen Transformation und angesichts der bekannten Cyber-Bedrohungen entwickelt. Doch wie sieht die Zukunft des Backups aus? Diese und weitere Fragen werden im eBook „Storage: What`s new?" beantwortet.

**Weitere Artikel aus dem eBook**

- Storage-Strategie: Der richtige Mix macht`s
- PPR: Prevention, Protection & Recovery
- Zukunftssichere Speicherinfrastrukturen
- Always on: Unveränderbare Snapshots

# Prediction of everything

## ZUKUNFTSTRENDS DER NÄCHSTEN JAHRE

Und das sind die Themen: zunächst ChatGPT. Vorsicht Falle! Quantencomputer und KI läuten das Zeitalter der Predictive Economy ein und neue Botformen ersetzen die Apps. Klingt doch spannend oder?

Bei allem Hype um ChatGPT hier ein paar kritische Anmerkungen zu dem Thema. Warum jetzt der Hype um dieses Tool der Künstlichen Intelligenz, schließlich ist es ja nicht erst seit heute verfügbar?

Wie so oft ist das Thema wie eine Art Schneeballsystem oder sollte ich besser sagen Schneeballlawine ins Rollen gekommen. Einer entdeckt es als Thema, viel andere springen auf den Zug auf, schreiben mehr oder weniger voneinander ab, fügen etwas hinzu und auf einmal gibt es einen Hype, wie um 1900 am Klondike. Aus ein paar Nuggets werden Goldklumpen, die am Wegesrand liegen und die man nur aufzusammeln braucht und schon ist man reich. Bekannterweise, so die Geschichte, ist das für Viele alles andere als glücklich ausgegangen.

Aber: man muss keine Angst vor der Zukunft haben. Diese Form der KI wird keine Arbeitsplätze vernichten, sie wird die Arbeitsinhalte verändern und das hat Innovation schon immer mit sich gebracht.

**Das Wesen des Hypes**

Was wird also geschehen? Ehrlich gesagt weiß das keiner so genau, jedenfalls keiner der nicht in die Kategorie Scharlatan gesteckt werden will. Was wir hören sind Annahmen, Prognosen, Ideen. Aber steckt dahinter auch die Wahrheit? Natürlich nicht.

Insofern war es erquickend am Zukunftstag von 2bAHEAD teilzunehmen, wo auch dieses Thema diskutiert wurde. In circa 20 Jahren werden wir wahrscheinlich wissen, welche Aussagen seinerzeit tatsächlich zutreffend waren. Die Zukunftsforscher verweisen darauf, dass jede Innovation natürlich eine Inspiration sei und eine MEINUNG. Und es gibt Meinungen, die als wichtig und weniger wichtig erachtet werden. Die Umsetzungswahrscheinlichkeit ist also bei Themen und Meinungen unterschiedlich hoch. Aber: Meinung kann man nicht messen, das ist der wichtige Unterschied.

**Ist da noch was außer KI?**

Ja, in der Tat. Zwei IT-Themen waren noch inspirierend. Zum einen die Verbindung von KI und Quantencomputern, die uns in ein paar Jahren auf den Weg zur Predictive Economy führen wird. Das bedeutet, das uns aus Datenpunkten, Sensoren und einer Unmenge von Messpunkten in naher Zukunft Waren geliefert werden, die wir gerade im Begriff waren zu bestellen. Nicht mehr nur Predictive Maintenance und Predictive Analytics, sondern Predictive Delivery, also Lieferung on demand, also den Liefertag quasi antizipieren. Das zeigt wie wichtig Daten und die richtige Interpretation in Zukunft werden.

Und noch etwas Dramatisches wird passieren: Die Prognosefähigkeit wird dazu führen, dass sich ganze Organisationen und Strukturen verändern werden. Denn wenn Prognosen und Bestellungen automatisiert werden, dann entfallen zum Großteil auch Akquise und Auftragsbear-

beitung, Suchmaschinen verlieren an Bedeutung. Warum? Weil Menschen dann Computern mehr vertrauen als Menschen.

**Prediction of everything**

Was bedeutet das für die Zukunft und wie weit ist sie entfernt? Nun, das wird nicht von heute auf morgen geschehen, aber stellen Sie sich darauf ein, dass wir in etwa um 2030 soweit sein werden. Vielleicht nicht auf breiter Front, aber in den ersten Ausprägungsformen sicherlich.

**Die Bot Revolution**

Schon heute sprechen wir viel über Bots und meinen damit kleine Maschinen, die unsere Böden reinigen oder die Chatbots, die uns auf immer mehr Webseiten begegnen. Nun ehrlich gesagt, der Nutzen ist überschaubar, jedenfalls dann, wenn es um spezifische Probleme geht. Dann geht es für den Chatbot in den

Loop, weil er keine Antwort weiß, uns aber unbedingt auf der Website halten will und irgendwann ist für den Bot Schluss und der Anwender gibt entnervt auf. Ein bisschen erinnert mich das an die Anfänge des Internetzugangs auf Mobiltelefonen vor dem iPhone, dann kam die Revolution und hat selbst einen als unbezwingbar geltenden Hersteller wie Nokia eliminiert.

Wie sehen die Zukunftsforscher diesen Markt? Nun, der Bot wird zum künstlichen Assistenten. Neben einem Personal Bot pro Person wird es künftig Service Bots geben, sie übernehmen quasi die Aufgabe der Apps, die wir bisher schon zum Teil via Alexa oder Siri steuern. Der Personal Bot wird zwischen 30 und 50 Service Bots steuern. Eine Bot-to-Bot Ökonomie entsteht, die Bots kommunizieren ergänzt durch Sprache untereinander. Zukunftsmusik? Wenn ich mir die Dynamik und die Geschwindigkeit des technologischen Wandels der letzten dreißig Jahre anschaue, wohl kaum. Muss ich Angst haben? Nein, die hatte ich vor 30 Jahren auch nicht. Und Sie?

***Ulrich Parthier – www.it-daily.net***

---

# KI UND DIE DISRUPTION DER ARBEIT

## TÄTIG JENSEITS VON JOB UND ROUTINE

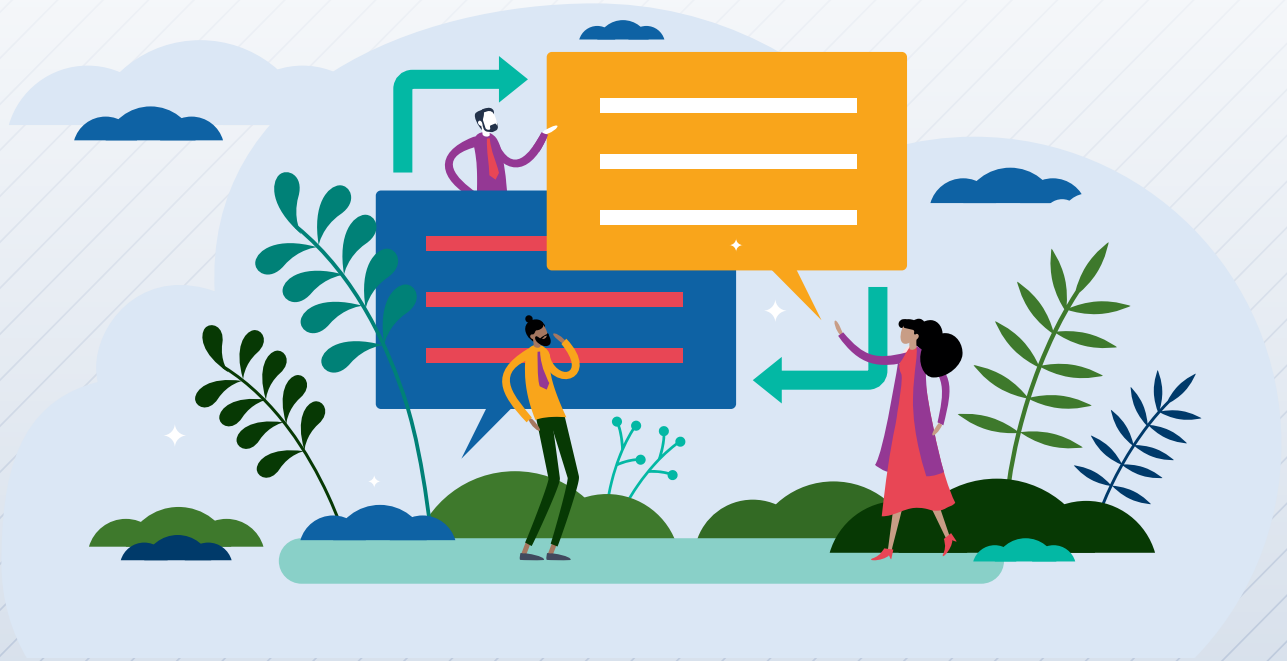
Mittlerweile ist allen klar geworden: Künstliche Intelligenz wird die Arbeitswelt in Zukunft grundlegend verändern. Schon jetzt zeichnet sich ab, wozu diese Technologie in der Lage ist, aber das ist wohl nichts im Vergleich zu dem, was uns erwartet. Müssen wir Angst vor diesen Veränderungen haben oder dürfen wir sie begrüßen? Sind wir wirklich hilflos einer unaufhaltsamen Macht ausgeliefert? Nein, schließlich sind wir alle, die Experten wie Konsumenten, auch diejenigen, die diese Entwicklung entfesselt haben und deshalb für ihre Gestaltung mit verantwortlich sind. Dennoch gibt es eine große Unsicherheit und das allgegenwärtige Gefühl des Kontrollverlusts.

Was viel zu selten geschieht, leistet dieses Buch: Die Betrachtung der anstehenden Veränderungen wird auf eine solide Basis gestellt, die sich schon oft bewährt hat: Wenn wir uns ansehen, woher wir kommen, verstehen wir besser, wohin wir gehen, besser noch, wohin wir wollen sollten. Wenn man verantwortlich mitgestalten will, darf man nicht wie das Kaninchen vor der Schlange verharren, so faszinierend oder erschreckend das alles sein mag.

Der Autor überträgt dieses Prinzip auf die Arbeitswelt. Er betrachtet mit Hilfe von Szenarien die Felder, auf denen die größten Umwälzungen zu erwarten sind, und zeigt, dass auch in der Vergangenheit schon oft große Brüche stattgefunden haben. Daraus kann man Schlüsse ziehen und lernen, was die heutigen Entwicklungen bedeuten, welche technischen, ökonomischen und sozialen Triebkräfte diese Innovationen in der Künstlichen Intelligenz und der Robotik vorantreiben. Das erlaubt dem Autor eine mögliche Arbeitswelt der Zukunft zu entwerfen, die eine Welt der gestaltenden und überwiegend überwachenden Tätigkeiten sein könnte.


**KI und die Disruption der Arbeit**

– Tätig jenseits von Job und Routine;
Prof. Klaus Kornwachs,
Carl Hanser Verlag GmbH & Co.KG; 07-2023



# Value Stream Mapping

## MIT DER WERTSTROMANALYSE DEN BUSINESS VALUE DER IT ERHÖHEN

Unternehmen fragen sich, wie ihre IT Business Values für das Tagesgeschäft erzielen kann. Das gelingt mit Value Stream Mapping, der Analyse von Wertströmen. Damit werden Prozesse in ihrer Gesamtheit erfasst und ihre Auswirkungen nachvollziehbar – es entsteht Klarheit, wo Wertschöpfung entsteht und welche Aktivitäten oder Anpassungen erfolgen müssen, um sie immer mit dem Kundennutzen im Blick zu optimieren. Eine solche Wertstromanalyse ist kein einmaliges Projekt – sie wird am besten mit einem externen Partner begonnen und mit dem Ziel des Wissenstransfers durchgeführt.

Wollen Mitarbeitende in Unternehmen Prozesse optimieren, passiert das häufig mit lokalem Fokus. Dieser Mikroblick erfolgt mit engen Grenzen und erfasst Details als Mosaiksteine statt der Gesamtheit mitsamt ihren Zusammenhängen. Zwar können damit Fragen etwa nach Standardisierungsmöglichkeiten beantwortet werden, doch der Wertbeitrag und damit der Kundennutzen stehen nicht im Vordergrund der Analyse. Die Wertstromanalyse, Value Stream Mapping, nimmt hier die Vogelperspektive ein und fokussiert auf das Gesamtbild. Sie ermittelt den Wertstrom und die Wertschöpfung, die vom Kunden bezahlt wird - angefangen von der Abteilungs- bis zur Unternehmensperspektive. Damit kann die Visualisierung, Analyse und Optimierung aller Schritte in einem Produktlieferungsprozess verbessert werden.

Mit dem Ansatz gelingt es zum Beispiel, Prozesse hinsichtlich übergeordneter Ziele wie schnellerer Reaktionszeiten und höherer Flexibilität, kürzerer Produktionszyklen und zufriedenerer Kunden zu optimieren. Mit Blick auf das Enterprise Service Management (ESM) und darunterliegende IT-Prozesse können Abläufe ganzheitlich ausgerichtet und beschleunigt werden. Damit bereitet die Wertstromanalyse die Grundlage für effiziente IT-Prozesse: Der Flow wird identifiziert und kann optimiert werden, was die Grundlage für eine sinnvolle Automatisierung darstellt: Durch die vollständige Sicht wird deutlich, was automatisiert und was besser eliminiert werden sollte. Damit zahlt Value Stream Mapping in den ersten Weg bei DevOps ein, die Optimierung des Flows.

Beim Entwicklungs- und Softwarebereitstellungsprozess können durch Value Stream Mapping und Automatisierung (im Sinne von Continuous Integration und Deployment) die Adaptions- und Bereitstellungszeiten minimiert werden, wenn Fragen nach einer sinnvollen, automatisierten und regelbasierten Prüfung und Freigabe bestimmter Teilschritte beantwortet werden können. Darüber hinaus werden Verschwendungen erkannt und können eliminiert werden. Insgesamt ist es möglich, IT-Prozesse zu

schaffen, die direkt auf die Wertschöpfung fokussieren.

**Herangehensweise**

Als erster Verfahrensschritt des Value Stream Mappings wird ein Blick auf alle Schritte geworfen, die vom Bedarf des Kunden bis zum gelieferten Nutzen gegangen werden. Dabei kann es sich um einen einzelnen, durchgängigen Prozess oder um eine Vielzahl kombinierter Prozesse handeln. In den Folgeschritten Value Stream Design und Value Stream Planning werden diese Erkenntnisse zur Optimierung des Wertstroms genutzt.

Start der Analyse ist die umfassende Betrachtung des Ist-Ablaufs: Es wird geklärt, wer die am Wertfluss Beteiligten sind und die fünf bis sieben wesentlichen Aktivitäten und Prozessschritte definiert. Hier gilt es, datengestützt Antworten auf Fragen zu finden wie: Wo liegen Übergabepunkte? Welche Informations- und Materialflüsse liegen vor? Wie sind die Durchlaufzeiten? Wie effektiv sind Iterationen? Wo kommt es zu Verschwendungen, zu Fehlern, Wartezeiten oder Übererfüllung? Im IT-Servicemanagement bedeutet das unter anderem festzustellen, wie die Produktions-IT genutzt wird und wer ihre Kunden sind; was das Team vor Ort benötigt, um an den Kunden ausliefern zu können; wie lange die Erbringungsprozesse in Anspruch nehmen, was ihre Teilschritte und Wege sind, wo es Warte- und Liegezeiten oder ob es Rückfragen gibt.

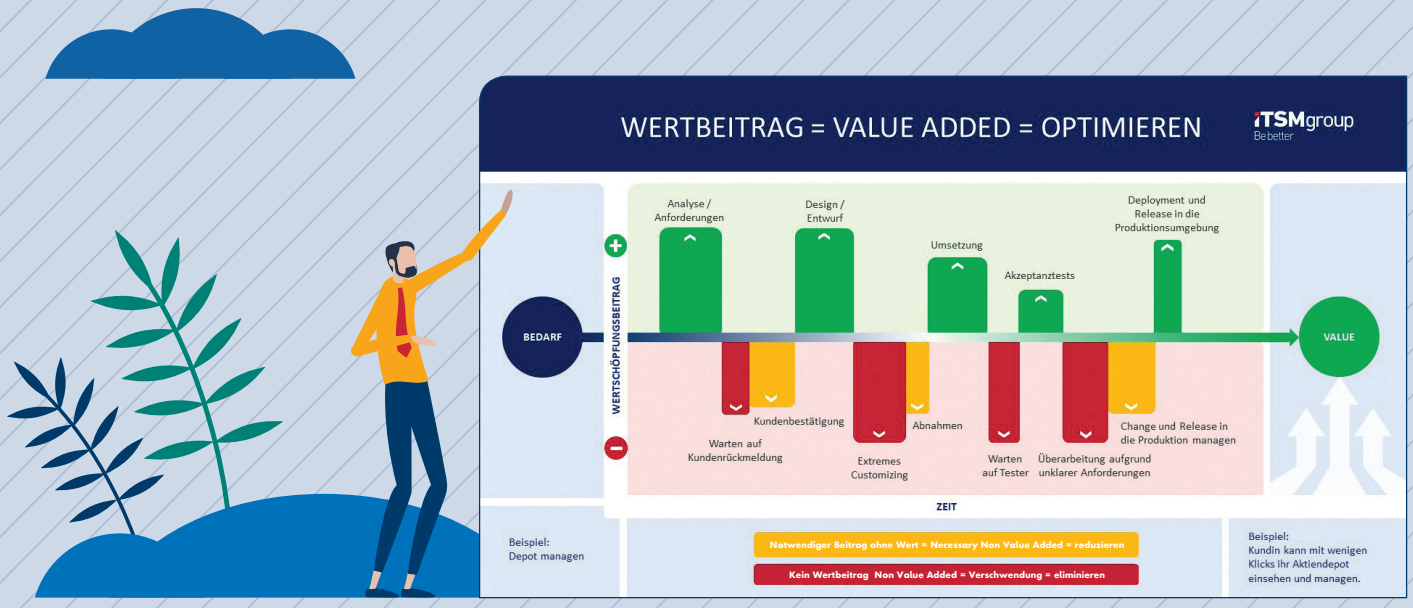
Um diese Informationen zu erhalten, werden Interviews geführt, die Aktivitäten und Prozesse vor Ort am Arbeitsplatz in Augenschein genommen. Auch Process Mining kann ein Werkzeug sein. Nach der Sammlung der Daten beginnt das Mapping. Begonnen wird mit den Aktivitäten und Durchlaufzeiten, dazu kommen Wiederholungszyklen. Die Visualisierung der Ergebnisse erfolgt über unterschiedliche Verfahren: Eine Symbolbibliothek kann zum Beispiel digital Material- und Informationsflüsse darstellen.

Vor Ort am Whiteboard kann eine Darstellung aber auch über verschiedenfarbige Zettel erfolgen, die Schritte und Aktivitäten repräsentieren, aber auch Störungen im Ablauf und IT-Systeme. Im Diskurs mit den Beteiligten werden Schritte, Reihenfolgen und Informationsflüsse ermittelt und eine Kette visualisiert. So werden Ergebnisse und ihre Auslöser ersichtlich. Mit diesen unterschiedlichen Informationsbausteinen wird die Wertschöpfungskette sukzessive und ebenenweise zum IST-Stand abgebildet und angereichert. Es entsteht ein Makrobild.

**Die Wertbeiträge ermitteln**

Jeder Schritt wird nun in Bezug auf seinen Wertbeitrag, das heißt aus Sicht der Werthaltigkeit für den Kunden, hinterfragt: Worum geht es diesem konkret – um kürzere Lieferzeiten, eine bessere Qualität oder um bedarfsgerechte Funktionen? Die Ermittlung der Wertbeiträge erfolgt binär durch die Beantwortung der Frage, ob ein Prozess oder Teilschritt zur Wertschöpfung beiträgt oder nicht. Die Antwort lautet ja, wenn der Kunde Geld dafür bezahlen würde oder wenn der Schritt notwendig ist – zum Beispiel aus legalen Gründen, weil Informationen erhoben werden müssen oder wegen fiskalischer Anforderungen.

Die übergeordnete Ende-zu-Ende Sicht hilft zu verstehen, wie Services erbracht werden und wo wertstiftende Aktivitäten stattfinden. Das Ziel ist es dann, notwendige Schritte ohne Wertbeitrag soweit wie möglich zu reduzieren, nicht notwendige wie überflüssige Schleifen, die dem Kunden nicht helfen, zu eliminieren und jene Schritte, die einen Wertbeitrag dar-



stellen, zu optimieren. Im Bereich der IT spielen Durchlauf- und Wartezeiten sowie Loop- und Cycletime bei der Betrachtung eine große Rolle, weil sie Indikatoren für die Effizienz darstellen.

**Störfelder und Handlungsoptionen identifizieren**

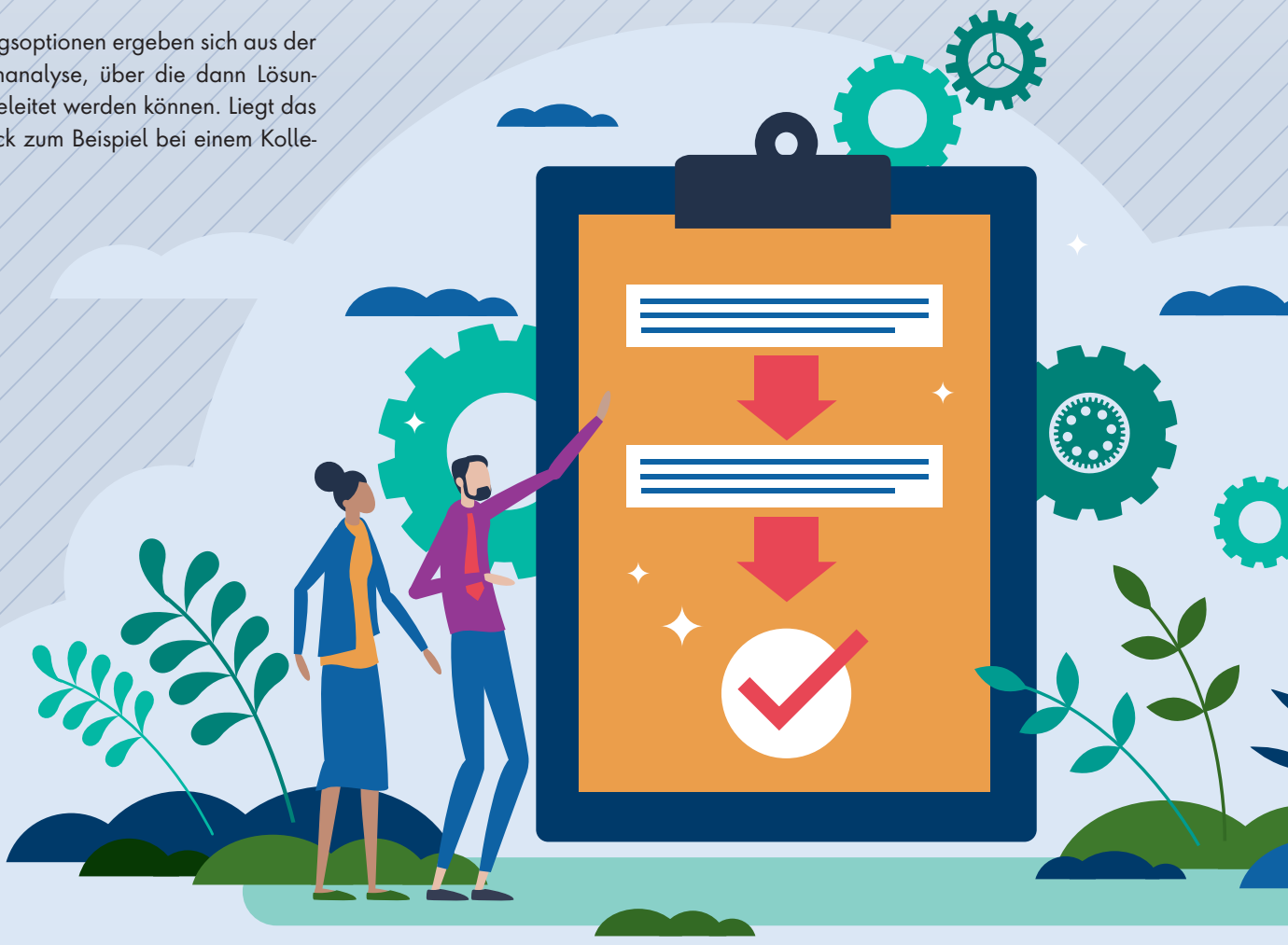
Auch Störfelder und Handlungsoptionen werden im Diskurs mit den Beteiligten identifiziert. So können zum Beispiel sieben Arten der Verschwendung festgestellt werden, darunter etwa eine zu große Variation im Prozess oder Fehler wie Störungen, zu viele Iterationen oder Rückfragen. Bei Behörden liegen klassische Probleme etwa in Vorgängen, die die Eingabe von bereits systemseitig vorhandenen Informationen erneut erfordern. Insgesamt werden Brüche im System durch die Visualisierung deutlich.

Handlungsoptionen ergeben sich aus der Ursachenanalyse, über die dann Lösungen abgeleitet werden können. Liegt das Bottleneck zum Beispiel bei einem Kollegen, der nicht wie erwartet liefern kann, stellt sich die Frage, wodurch die Verzögerung entsteht. Vielleicht, weil der Kollege diverse Aufträge parallel bearbeiten muss und die Priorisierung fehlt. Oder weil Krankenstände oder Personalengpässe den Zeitdruck erhöhen. Diese Überarbeitung und Überlastung von Menschen und System führen zu Fehlern und Störungen im Ablauf. Sie werden mit der Wertstromanalyse identifiziert.

**Gelingende Prozessoptimierung**

Nach dem Mapping setzt die Phase des Value Stream Designs beziehungsweise Plannings ein: Hierbei wird der Wertstrom der Zukunft ermittelt – ohne Störstellen in seinem Idealzustand. Es wird festgelegt, welche Schritte man konkret gehen muss, um diesen Soll-Zustand zu erreichen, sowie die Voraussetzungen und Notwendigkeiten. Der Ist-Zustand kann zum Beispiel darin bestehen, dass ein Kunde bei der Vermarktung seiner Leistung acht Wochen benötigt, bis Angebot und Vertrag aufgesetzt sind und vier weitere Wochen bis zur Unterschrift vergehen.

Der Soll-Zustand kann festlegen, statt zwölf nur noch sechs Wochen zu benötigen, etwa, indem Einkaufs- und Unterschriftsprozesse vereinfacht werden. Im Bereitstellungsprozess der Services können außerdem Lieferzeiten verkürzt und verlässlichere Qualität sowie Freiraum für weitere Verbesserungen geschaffen werden.



Den Abschluss bildet die Vorbereitung der Maßnahmen, um zu diesem Soll-Zustand zu kommen.

**Was bringt Value Stream Mapping?**
Mit Value Stream Mapping werden Prozesse in ihrer Gesamtheit erfasst und in ihren Ausprägungen und Auswirkungen nachvollziehbar. Der Fokus liegt auf den wichtigsten Handlungsfeldern und es entsteht ein klarer Ansatz, welche Ergebnisse mit welchen Aktivitäten erzielt werden müssen, um die Wertschöpfung zu optimieren.

Oftmals wächst erstmalig ein gemeinsames Verständnis aller Prozessbeteiligten für die Zusammenhänge.

Durch den Dialog, auch mit Externen, werden Abhängigkeiten und Übergänge sichtbar und der eigene Wertbeitrag zum Gesamtsystem deutlich. Kollegen sprechen manchmal zum ersten Mal überhaupt miteinander – der Blick weitet sich weg von den eigenen Aufgaben hin zur Gesamtheit: Der Beginn des Wertschöpfungsprozesses wird erkennbar, sein Ende und die Schritte dazwischen. Der Austausch schafft Transparenz, die gemeinsamen Ergebnisse rücken in den Fokus.

Darüber hinaus können Störfelder identifiziert und Handlungsoptionen für die Verbesserung oder Neugestaltung der Abläufe abgeleitet werden. Damit wird Value Stream Mapping zur Grundlage, um Probleme und Störungen im Ablauf zu eliminieren und Verschwendungen zu beheben. Dieser Blick nach außen auf den Wertbeitrag für den Kunden wird zum Leitfaden. Der Blick nach innen hat in der Regel die interne Performance und die damit einhergehende Standardisierung zum Ziel – dabei wird aber deren Notwendigkeit nicht hinterfragt.

Mit Value Stream Mapping kann dagegen sichergestellt werden, dass nur relevante Elemente und keine Altlasten automatisiert werden: Es geht also nicht mehr darum, individuelle Arbeitsleistung zu maximieren, sondern mit Blick auf die Gesamtheit das auszuwählen, was tatsächlich sinnvoll ist.

Value Stream Analysis schafft darüber hinaus Raum und Zeit für die Beteiligten, sich um wertschöpfende Arbeit zu kümmern. Damit können die Produktivität erhöht, Silos aufgelöst und Zusammenhänge aufgezeigt werden. Die Zusammenarbeit verbessert sich, Effizienz und Effektivität steigen. Gleichzeitig entsteht Raum für Innovation, wenn Mitarbeitende nicht mehr unter Alltagsaufgaben begraben werden. Unternehmen können Kosten senken und ihre Antwortgeschwindigkeit erhöhen.

**Value Stream Mapping einführen**
Eingeführt wird Value Stream Mapping mit Blick auf die Frage, wie man Abläufe verbessern kann. Dabei muss geklärt werden, ob der Blick auf das Produkt oder den Durchlauf gerichtet werden soll. Der Impuls muss zudem vom Management ausgehen oder von diesem aufgegriffen werden. Der Prozess wird am besten von einem neutralen und erfahrenen Moderator geleitet. Er weiß, worauf es ankommt und kennt die Vorgehensweise.

MIT VALUE STREAM MAPPING KANN SICHERGESTELLT WERDEN, DASS NUR RELEVANTE ELEMENTE UND KEINE ALTLASTEN AUTOMATISIERT WERDEN.

**Bernd Ebert,**
**Management Consultant Enterprise Service Management, iTSM Group,**
**bit.ly/3KjLC3p**

Neutralität ist notwendig, damit alle an einem Strang ziehen können und nicht der Eindruck entsteht, dass sich einzelne profilieren wollen. Der Einstieg in die Wertstromanalyse gelingt mit externer Unterstützung leichter, der übergeordnete Unternehmensanspruch wird deutlich. Da Value Stream Mapping keine einmalige Anwendung ist, sollten Unternehmen langfristig Expertise aufbauen – die vorgenommenen Änderungen müssen regelmäßig evaluiert und optimiert werden.

**Fazit**
Value Stream Management in der IT ermittelt die Wertbeiträge von Prozessen für den Kunden mit ganzheitlichem Blick. Der Wertstrom wird ersichtlich, seine Hindernisse, sowie sein Verlauf. Unternehmen verstehen, wo sie ansetzen können, um Optimierungen anzustoßen und innerhalb der Belegschaft entsteht ein Verständnis über den eigenen Beitrag, was die Zusammenarbeit und Effektivität insgesamt verbessert.

***Bernd Ebert***

# Business Performance Management

## IM SPANNUNGSFELD VON IT & BUSINESS

Ob Krisen- oder Wachstumsphase: Effektives Business Performance Management ist der Schlüssel für die Zukunftsfähigkeit eines jeden Unternehmens. Damit ist gemeint: Die Planung, Integration, Umsetzung und Überwachung langfristiger Ziele, Strategien und Ressourcen innerhalb eines Unternehmens, um dessen Produktivität und Wirtschaftlichkeit kontinuierlich zu verbessern. Diese Aspekte sind üblicherweise nicht unmittelbar Kernaufgaben der IT-Abteilung. Dabei könnte sie aufgrund ihrer Einbindung in beinahe alle Prozesse und ihrem Zugriff auf fast alle Datenpunkte der Organisation oftmals wertvolle Insights für das Performance Management liefern.

Um das Potenzial der IT in strategischen Fragen voll auszuschöpfen, muss die Geschäftsleitung allerdings ihren bisherigen – womöglich überladenen – Fokus auf die Key-Performance-Indikatoren (die sogenannten KPIs) des Unternehmens erweitern und sich für neue Performance-Management-Methoden, öffnen. Dann kann die IT mit ihrer ganzen Stärke in strategische Prozesse eingebunden und das volle Potential der verfügbaren Daten zur Ressourcen- und Prozessplanung ausgeschöpft werden.

**Strategien**

Ein wichtiger Aspekt im Business Performance Management ist die Entwicklung, Umsetzung und Erfolgsmessung von Unternehmensstrategien. Sie geben die Richtung vor, die das Unternehmen einschlagen sollte, um langfristige Ziele zu erreichen und beinhalten eine Kalkulation der dafür notwendigen Ressourcen.

Abhängig vom Entwicklungsgrad der jeweiligen Organisation, aber auch von Branche und Wettbewerbsumfeld, können sich verschiedene Strategien anbieten. In vielen Konstellationen verfolgen Unternehmen eine Wachstumsstrategie, die auf eine Vergrößerung des eigenen Marktanteils und auf eine Steigerung der Einnahmen abzielt. Die einzelnen Aktionen einer solchen Strategie sind typischerweise etwa Investitionen in Forschung und Entwicklung, die Einführung neuer Produkte oder Dienstleistungen oder der Eintritt in neue Märkte.

Alternativ könnte das Unternehmen eine Kostensenkungsstrategie verfolgen, um seine Rentabilität zu verbessern. Dabei liegt der Fokus häufig auf der Rationalisierung von Prozessen, der Reduzierung von Ausgaben oder der Auslagerung oder Aufgabe bestimmter Geschäftsbereiche. Das kann die Trennung von einer unprofitablen Unternehmenssparte sein, oder

auch die Senkung der Ausgaben für IT- und Digitalisierungsprojekte.

Eine Strategie muss dabei auf die langfristigen Unternehmensziele ausgerichtet sein und alle Anstrengungen in diese Richtung lenken. Ob dies tatsächlich der Fall ist, macht das Performance Management anhand der Messung, Überwachung und Analyse essenzieller Leistungsindikatoren fest – die vielen unter dem gängigen Begriff KPIs bekannt sein dürften. Anhand dieser können die Strategieverantwortlichen den Erfolg des Unternehmens ableiten, aber auch, worauf sie oder die jeweiligen Abteilungen ihre Anstrengungen konzentrieren sollten, um auf Kurs zu bleiben.

**Frage der Messbarkeit**

Kann dieser Kurs zum Beispiel aufgrund einer Rezession oder anderen geopolitischen Herausforderungen nicht zufriedenstellend gehalten werden, drängt sich häufig die Frage nach der Sinnhaftigkeit solcher KPIs auf. Tatsächlich ist es gerade in solchen Phasen, in denen zum Beispiel aufgrund sinkender Nachfrage Kostensenkungsmaßnahmen zu ergreifen sind, wichtig, einen klaren Überblick über die finanzielle Gesundheit und Produktivität des Unternehmens zu behalten. KPIs können hier Orientierung bieten, indem sie Momentaufnahmen von Schlüsselkennzahlen wie Umsatz und Rentabilität liefern.

**Nachteile von KPIs**

In Krisenzeiten, oder wenn eine strategische Transformation erforderlich ist, können KPIs ihre Rolle oftmals jedoch nur bedingt erfüllen. Zwar sind sie oft an bestimmte kurzfristige Ziele gebunden, was in turbulenten Phasen, in denen Unternehmen sich schnell auf Veränderungen am Markt konzentrieren müssen, hilfreich sein kann. Doch gerade deshalb neigen KPIs auch dazu, die langfristige Gesundheit und Nachhaltigkeit eines Unternehmens, sowie die Herausforderungen, Chancen und die dafür erforderlichen Abschreibungen oder Investitionen nicht (ausreichend) zu berücksichtigen, auf die es in solchen Phasen gerade ankommt.

Mehr noch: Der häufig KPI-getriebene Überfokus auf bestimmte Bereiche geht in vielen Fällen auf Kosten anderer, ebenso wichtiger Werttreiber. Konzentriert sich eine Firma etwa zu sehr auf die Maximierung des Umsatzes, kommt es aufgrund der nicht ausbalancierten Ressourcenallokation womöglich zu Abstrichen im Kundenservice oder beim Wohlbefinden der Mitarbeiter, was langfristig ebenso schädlich ist.

AUS GRÜNDEN DER ÜBERSICHT UND EFFIZIENZ SOLLTEN SOWOHL OKRS ALS AUCH KPIS GERADE IN GRÖSSEREN UND KOMPLEXEN ORGANISATIONSSTRUKTUREN AUF EINER DIGITALEN PLATTFORM ABGEBILDET UND VISUALISIERT WERDEN.

**Seth Elliot,**
**Chief Operating Officer, Quantive,**
**https://quantive.com/**

## BEISPIELE FÜR KPIs IN IT-ABTEILUNGEN

- Erreichbarkeit
- Reaktionszeit
- Servicequalität
- Wirksamkeit des Kontrollsystems
- Effizienz der Störungsbeseitigung
- Auslastungsgrad
- Transparenz der IT-Betriebskosten
- Berücksichtigung von Daten- und Cybersicherheit
- Häufigkeit nicht-autorisierter Konfiguration

Statt sich also allein auf finanzielle Kennzahlen zu beschränken, sollte das Business Performance Management deshalb seine traditionellen KPIs weiterentwickeln und transformative Messgrößen wie die Resilienz oder Adaptionsfähigkeit des Geschäftsmodells, die Kundenzufriedenheit, das Mitarbeiterengagement oder auch die Innovationskraft als Leistungsindikatoren mitberücksichtigen.

Trotzdem stellt sich auch dann die Frage, welche und wie viele KPIs angemessen sind, um ein klares und realistisches Bild der Unternehmensleistung zu erhalten. Zudem bleiben KPIs immer nur Indikatoren, die im komplexen Ökosystem eines Unternehmens weder Probleme bis zur Wurzel verfolgen noch Aufschluss darüber geben können, welche Gegenmaßnahmen auf Management-Ebene notwendig wären. Auch die Frage nach Verantwortlichkeiten für die Probleme und deren Lösung können sie nicht geben.

## BEISPIELE FÜR OKRs IN IT-ABTEILUNGEN MIT FOKUS AUF INFORMATIONSSICHERHEIT

**Objective: „Wie wir unsere Kompetenzen, Sensibilisierung und Effektivität im Bereich Cybersicherheit steigern."**

**Key Results:**

1) „Wir müssen die Quantität und Qualität Schulungen zum Thema Cybersicherheit pro Quartal von einer auf drei erhöhen."
2) „Wir müssen die Öffnungsrate von Junk- und Phishing-Emails von 3 Prozent auf 1 Prozent verringern."
3) „Wir müssen die Zugriffsversuche auf nicht autorisierte Websites reduzieren, von zehn auf fünf pro Monat und Mitarbeitendem."
4) „Wir müssen die Häufigkeit von Cloud-Sicherungen und Daten-Backups von zwei auf vier pro Quartal erhöhen."

**OKRs als zusätzliche Methode**

Zur Umgehung dieser Fallstricke setzen zahlreiche Unternehmen zunehmend auf die sogenannte OKR-Methode (Objectives and Key Results). Von Intel CEO Andy Grove entwickelt, wurde diese Performance-Managementmethode im Jahr 1999 von John Doerr, ehemals Mitarbeiter bei Intel, bei Google eingeführt. Der Weltkonzern nutzt die OKR-Methodik bis heute und viele andere Firmen folgten im Laufe der Zeit nach.

Wichtigster Bestandteil dieser Management-Philosophie ist die Formulierung von ambitionierten, motivierenden Kernzielen (Objectives). Auf diese Weise soll ein Rahmen konstruiert werden, der die Festlegung auf eindeutig definierte und messbare Ziele, die Ausrichtung von Teams auf diese Ziele und die Verfolgung des Fortschritts bei der Zielerreichung erleichtern soll. Durch die Formulierung von OKRs werden abstrakte Unternehmensvisionen („Unser Betrieb soll bis 2030 vollständig digitalisiert sein") in systematische Teilaufgaben untergliedert, die auf diese Ziele einzahlen („Wir statten unsere Logistik bis 2025 mit einem neuen ERP-System aus"). Diese Key Results teilt das Management gemeinsam mit den jeweiligen Teams in drei bis fünf Schlüsselergebnisse auf („Wir identifizieren alle verfügbaren ERP-Systeme am Markt"). Anschließend werden gemeinsam einzelne Teilziele für jeden Mitarbeitenden definiert, die dieser in einem bestimmten Zeitraum (in der Regel im nächsten Quartal) bestmöglich erreichen sollte. Dieser Prozess wird wiederholt, bis das gewünschte Ziel erreicht ist.

Zwar belastet die Umstellung auf die OKR-Methodik zunächst Kapazitäten. Die Unternehmensstrategie – zuvor ein abstraktes und theoretisches Konstrukt – wird damit aber greifbar und ihre Umsetzung quantifizierbar: Optimal aufgesetzt hat das Management durch die Transparenz der OKR-Methodik einen genauen Überblick über den Status einzelner Projekte, Kapazitäten und potenzielle Krisenherde. Und auch die Mitarbeiter können ihre Verantwortlichkeiten, Aufgaben und deren Wirkung nun genau nachvollziehen.

Mit einem derart umfassenden Überblick können Unternehmen im nächsten Schritt tatsächlich sinnvolle KPIs definieren, an denen die Performance einzelner Bereiche gemessen werden kann. Damit sind OKRs nicht etwa eine Alternative, sondern eine natürliche Erweiterung zur Erfolgsmessung auf Basis von KPIs, die in einem OKR-Rahmen deutlich mehr Aussagekraft versprechen. Sie helfen Unternehmen dabei, ihre Business Ziele in Zeiten von Umbruch und Wachstum zu erreichen.

**Die IT ist Dreh- und Angelpunkt**
Aus Gründen der Übersicht und Effizienz sollten sowohl OKRs als auch KPIs gerade in größeren und komplexen Organisationsstrukturen auf einer digitalen Plattform abgebildet und visualisiert werden. Hier kommt die IT-Abteilung ins Spiel. Natürlich kann sie selbst, in der eigenen Planung, auch von einem OKR-basierten Projektmanagement profitieren.

Eigentlich spielt sie ihre Rolle im Business Performance Management aber dort, wo sie die technologische Infrastruktur zur Unterstützung des unternehmensweiten OKR-Prozesses, bereitstellt. Performance- oder OKR-Management-Software kann ihre Wirkung umso besser entfalten, je mehr Datenbanken und Datenpunkte aus den verschiedenen Unternehmensbereichen an sie angedockt sind. Das können Informationen aus den einzelnen Prozessmanagement-Systemen sein, etwa die Content-Management-Software des Marketing-Teams, oder das CRM-System des Kundensupports.

Abteilungen, deren Digitalisierungsgrad womöglich noch in den Kinderschuhen steckt, sollten dabei priorisiert und parallel die entsprechenden Schnittstellen für eine spätere, abteilungsübergreifende Performance-Management-Lösung vorbereitet werden. Erst dann kann die IT im letzten Schritt entweder selbst ein skalierbares, für alle Mitarbeiter transparentes, nutzerfreundliches und sicheres Dashboard zur Visualisierung aller OKRs in allen Abteilungen bauen, oder sich alternativ – nach einer entsprechenden rechtlichen und Compliance-Prüfung – für ein externes Tool entscheiden, um die OKR-Strategie zu visualisieren und so ihre Umsetzung zu erleichtern.

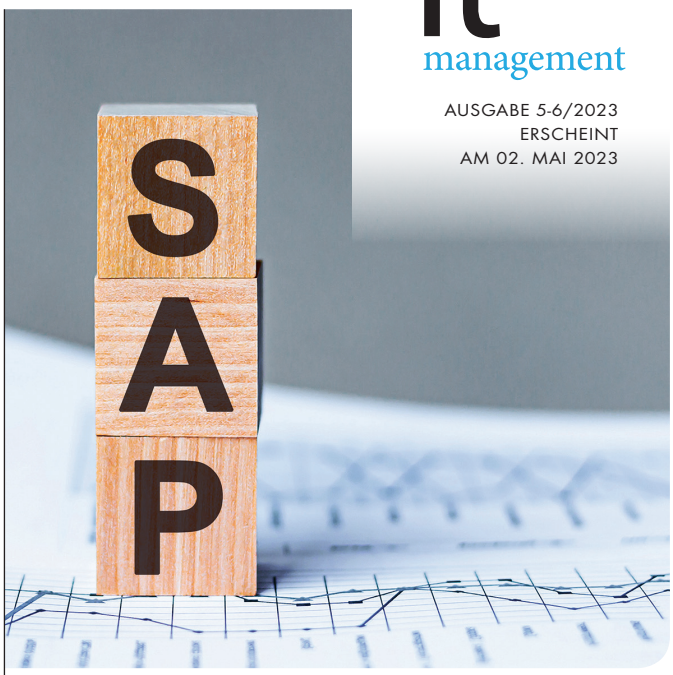
**Fazit**
Modernes Business Performance Management kommt ohne die Beobachtung und Evaluation von KPIs nicht mehr aus. Sie sind jedoch keine Universallösung der Erfolgsmessung und greifen in komplexen Organisationsstrukturen zu kurz. Die zusätzliche Implementierung von OKRs kann eine Möglichkeit sein, Unternehmensstrategien greifbarer zu machen, Ressourcen effizienter zu nutzen und einen transparenten Überblick über den Fortschritt von Projekten und Maßnahmen zu erlangen. Der IT-Abteilung kommt bei der Einführung von OKRs eine entscheidende Rolle zu, weil sie die erforderlichen technischen Grundlagen schafft. Gelingt die Einführung, ist das Unternehmen für herausfordernde Transformationsprojekte künftig besser gerüstet.

***Seth Elliot***

| DIE UNTERSCHIEDE | KPIs | OKRs |
|---|---|---|
| **Sinn und Zweck im Business Performance Management** | Erfolgs- und Aktivitätsmessung | Setzen strategischer Schwerpunkte, Fokussierung, Engagement, Verbindlichkeit und Transparenz |
| **Strategischer Anwendungsumfang** | Sehr punktuell | Breit und abteilungsübergreifend |
| **Kontrollzeitraum** | Langfristig | Kurzfristig (Key Results) und Langfristig (Objectives) |
| **Flexibilität und Adaptionsmöglichkeiten** | Kaum, sind eher statisch | Viele, können und sollten regelmäßig aktualisiert werden |
| **Funktionalität** | Idealerweise gleichgewichtet, aber voneinander isoliert und nur bedingt verknüpfbar | Können verschiedene Hierarchien abbilden, aufeinander aufbauen und durch unterschiedliche Gewichtung ineinander verschachtelt sein |

it management

AUSGABE 5-6/2023
ERSCHEINT
AM 02. MAI 2023




## UNSERE THEMEN

SAP-Partnerlösungen
Data Center & Data Management
IT & Service Management

it security

AUSGABE 5-6/2023
ERSCHEINT
AM 02. MAI 2023

## UNSERE THEMEN

Privileged Access Management
Zero Trust einfach einführen
Künstliche Intelligenz & Security



## INSERENTENVERZEICHNIS



## IMPRESSUM

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

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

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

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

***Autoren:*** Stephan Bauriedel, Philipp von der Brüggen, Bernd Ebert, Dr. Christoph Ehlers, Seth Elliott, Bert Kondruß, Carina Mitzschke, Mirjam Müller, Silvia Parthier, Ulrich Parthier, Raoul Plickat,Christian Till Roga, Shaun Shirazian, Nicole Segerer, Thomas Timmermann, Florian Vees, Steffen Weiers, Ralph Weiss

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

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

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

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

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

***Anzeigenpreise:*** Es gilt die Anzeigenpreisliste Nr. 30. Preisliste gültig ab 1. Oktober 2022.

***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
Marena Avila (nur per Mail erreichbar), avila@it-verlag.de

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

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

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

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

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

Das E-3 Magazin

## SUMMIT DER SAP-COMMUNITY

# COMPETENCE CENTER

## Salzburg, 1. und 2. Juni 2023


**April 2023:**

**Das Magazin zum Competence Center Summit 2023**

Der E-3 Verlag veranstaltet einen Summit zum Thema CCC/CCoE, SolMan, ALM, Lizenzen und vielen weiteren Basisthemen. Dieses E-3 Extra ist der Kongressband.

*Beteiligen Sie sich jetzt an der CC-Summit-Bildungsarbeit 2023.*
*Ansprechpartnerin:*
*Andrea Schramm,*
*Telefon: +49/8654-77130-15,*
*andrea.schramm@b4bmedia.net*

### Liebe Mitglieder der SAP-Community in D-A-CH,

die SAP-Basis und damit das Customer Competence Center und Customer Center of Expertise sind sowohl für den On-prem- als auch für den Cloud-Betrieb die Garantie für nachhaltigen Erfolg. Wir greifen die Tradition des CCC-Forums auf und präsentieren den Competence Center Summit 2023.

Auf dem Weg nach Hana und S/4 entstehen viele Fragen hinsichtlich Betriebsmodell, Architektur, Lizenzen und natürlich Basissupport. Viele dieser Fragen werden am 1. und 2. Juni in Salzburg auf dem Summit 2023 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 1st/2nd Support, Sourcing-Strategien, Automatisierung und Modifikationen, DB-Management und Berechtigungsmanagement etc.

Wir laden alle CCC-Leiter, CIOs und IT-Experten herzlich nach Salzburg ein, um an zwei Tagen alle relevanten SAP-Basisthemen mit Partnern und Spezialisten zu diskutieren.

Jetzt anmelden: Die Teilnahmegebühr exkl. USt. sowie exkl. Übernachtungs- und Reisekosten beträgt 590,– Euro mit einem Early-Bird-Angebot von 440,– Euro bis Montag, 27. März 2023.

Alle Infos unter e-3.de/summit-cc

E-3 Summit **COMPETENCE CENTER** wird gesponsert von:

new relic. itesys

**e-3.de/summit-cc/**

15.–16. MÄRZ

Aagon

CLIENT MANAGEMENT PLATFORM

AUF DER

secIT by Heise

HANNOVER 2023

# WIR SIND DABEI!

Eilenriedehalle

Stand-Nr.: 55

Live

**Vortrag**

"Wie können (Cloud) Security Lösungen optimal ergänzt und zentral gemanagt werden?"

15.03.2023 | 13:25 Uhr

Bühne 2 | Eilenriedehalle

Mehr Infos: www.aagon.com/secit2023

ACMP ist 4fach Champion

PUR 2023
Professional User Rating

Aagon

it security

Detect. Protect. Respond.
März/April 2023

ZEITKRITISCHE PRODUKTIONSVERFAHREN

# Die Industrie sicherer machen

Uwe Gries, Stormshield

RBAC VS. PBAC

Warum Policies allein den Zugriff nicht sichern

ANOMALIEN

KI-basierte Angriffserkennung

SAP-LIZENZMODELL

Gefahr ungeprüfter Berechtigungen

www.it-daily.net

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

SAVE THE DATE

# CYBERSECURITY
# DIE GEFAHR AUS DEM OFF

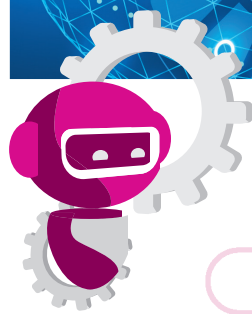
## Digitalevent
## 22. März 2023

**#cybersec23**

SCAN ME

https://www.it-daily.net/cybersecurity/





# Inhalt

# Die Industrie sicherer machen

## SICHERHEIT IN ECHTZEIT FÜR ZEITKRITISCHE PRODUKTIONSVERFAHREN

Cyberkriminelle stellen eine immer größere Herausforderung für die Cybersicherheit in der digitalisierten Industriewelt dar. Die große Frage ist: Wie schütze ich meine OT-Umgebung am besten? Uwe Gries, Country-Manager DACH bei Stormshield, sprach mit uns über essenzielle Faktoren für die IT-Sicherheit im Industrieumfeld.

**it security:** *IT- und OT-Umgebungen. Wo liegen die Unterschiede?*

**Uwe Gries:** IT-Systeme sind für die Zusammenarbeit mit Menschen konzipiert. In einer OT-Umgebung hingegen müssen die Geräte in der Lage sein, meistens ohne Zutun eines Anwenders eine Schnittstelle zu „physikalischen" Systemen und Prozessen zu bilden. Beispielhaft genannt seien eine chemische Reaktion, der Fluss einer Flüssigkeit, ein Heiz-/Kühlprozess oder die Validierung eines Prozesses. Auch die Prioritäten der beiden Umfelder sind unterschiedlich. In der IT wird die Integrität der Daten geschützt, in der OT gilt der Schutz der Kontinuität des Prozesses. Es ist also nicht verwunderlich, dass OT-Umgebungen ursprünglich komplett von IT-Umgebungen getrennt waren, weshalb man keinen Bedarf an einer zusätzlichen Absicherung solcher „Silos" empfand. Doch im Zuge der Digitalisierung koppelt man zunehmend IT-Systeme mit OT-Geräten, sei es zur Fernüberwachung, zur prädiktiven Instandhaltung oder zur Analyse der generierten, immer größer werdenden Datenmengen. Ohne geeignete Absicherung wirkt sich aber die Konvergenz von Betriebstechnologie (OT) und Informationstechnologie (IT) negativ auf die Sicherheit der gesamten Infrastruktur aus, denn IT-Umgebungen werden bereits seit Jahrzehnten von Cyberkriminellen ins Visier genommen – OT-Umgebungen erst, seitdem die IT darin Einzug hält.

> DIE ENGE VERZAHNUNG VON IT UND OT SETZT DIE WEICHEN FÜR DIE INDUSTRIE DER ZUKUNFT UND IST ZUGLEICH DEREN GRÖSSTE BEDROHUNG.
>
> **Uwe Gries, Country-Manager DACH, Stormshield, www.stormshield.com**

**it security:** *Würden Sie sagen, es stand ohne IT besser um die Sicherheit von OT-Infrastrukturen?*

**Uwe Gries:** Ich würde es so formulieren: Das „Industrial Internet of Things" (IIoT) macht erst die „Operational Technology" (OT) und damit die Hardware sowie Embedded Software zur Überwachung und Steuerung physischer Geräte, von Prozessen und Events zukunftsfähig. Die enge Verzahnung von IT und OT setzt die Weichen für die Industrie der Zukunft und ist deren größte Bedrohung zugleich: Der Einzug der IT in die OT-Welt darf nicht ohne die Implementierung von Cybersicherheitsmaßnahmen und -strategien erfolgen, die weit über den klassischen IT-Ansatz hinausgehen und den Eigenschaften von SCADA- und ICS-Systemen gerecht werden.

**it security:** *Thema Hannover Messe, hier ist Stormshield präsent. Der Prozess- und Industriesicherheit wird wieder große Bedeutung beigemessen.*

**Uwe Gries:** Das ist genau der Grund, warum wir an der Hannover Messe teilnehmen. Wir stellen dort nicht nur unsere für OT-Umgebungen entwickelten IPS- und Endpoint-Sicherheitslösungen aus, sondern wollen aktiv zur Erkenntnis beitragen, dass mehr zur Industriesicherheit gehört als eine IT-Firewall aus dem Regal.

**it security:** *OT-Sicherheit umfasst tatsächlich ein breites Spektrum an industriellen Steuerungssystemen wie SCADA-Systeme, Sensoren, Aktoren und viele andere technische Anlagen. Welches sind aus Ihrer Erfahrung die wichtigsten Maßnahmen für die OT-Sicherheit?*

**Uwe Gries:** Angesichts der Hypervernetzung und der Vergrößerung der Angriffsfläche von OT-Infrastrukturen durch den wahllosen Einsatz von IT-Komponenten im Zeichen von Industrie 4.0 müssen IPS- und Firewall-Lösungen in der Lage sein, sowohl industrielle als auch IT-Protokolle in Echtzeit zu analysieren. Dabei darf es nicht nur um den Inhalt jeder Kommunikation gehen, sondern auch um die korrekte Bewertung des Verhaltens der überwachten Komponenten. Dieses Monitoring gehört sicherlich zu den Basics, um Be-

**Uwe Gries, Country-Manager DACH bei Stormshield (2.v.r) und sein Team.**

drohungen und Angriffe frühzeitig zu erkennen.

Eine weitere unerlässliche Maßnahme ist die Segmentierung der verschiedenen Produktionsbereiche und deren Isolierung von reinen IT-Bereichen wie Verwaltung, Vertrieb, Technik uvm. Das sind alles Elemente, die klar von den Produktionssystemen getrennt sein müssen, um die Ausbreitung von Angriffen auf die gesamte Infrastruktur durch laterale Bewegungen auszuschließen. Unsere Empfehlung: Auch die verschiedenen Bereiche der OT-Umgebung sollten segmentiert werden, deren Prozesse nicht voneinander abhängen oder für die keine Interkommunikation vorgesehen ist.

**it security:** *Was sollten Industrieunternehmen zudem beachten?*

**Uwe Gries:** Über die Notwendigkeit einer Datensicherung zur Bewältigung von Schäden am Datenbestand durch Verschlüsselung beziehungsweise der physikalischen Trennung der Backups vom Netzwerk hinaus empfehlen wir die Einrichtung von Zero-Trust-Architekturen (ZTA) durch genau ausgearbeitete Zugriffskontrollregeln. Diese sollten aus Benutzerauthentifizierung und Berechtigungen, zugelassenen Zeiträumen und Geräten bestehen. Firewalling-Systeme der Industrieklasse gestatten die Realisierung solcher ZTAs auch mit Geräten, die nicht mit HIPS-Lösungen oder anderer systemstärkender Software ausgestattet werden können.

**it security:** *Im IT-Bereich ist aktuell das Thema Phishing und damit verbunden Ransomware-Attacken der Top-Angriffsvektor. Zunehmend sehen wir das auch im industriellen Umfeld.*

**Uwe Gries:** Wir betrachten das ebenfalls mit Sorge. Schulungen und Awareness-Maßnahmen helfen auch hier. Unternehmen müssen ihre Mitarbeiter über die Bedrohungen und Angriffe, die auf OT-Systeme zielen, und über die richtigen Verhaltensweisen informieren und sie schulen, damit die Mitarbeiter selbst die erste Verteidigungslinie bilden können.

**it security:** *Wie kann Stormshield Anwendern aktuell helfen, ihre OT-Netzwerke zu schützen und den Anforderungen an IoT sowie IT-/OT-Konvergenz gerecht zu werden?*

**Uwe Gries:** Unsere Firewall-Reihe Stormshield Network Security (SNS und SNi) bietet wichtige Funktionen zum Schutz industrieller Netzwerke vor Cyberbedrohungen. Anwender können vor allem auf eine „Intrusion Prevention Engine" (IPS) vertrauen, die bösartige Datenströme innerhalb des Netzwerks sowie abnormales Verhalten identifiziert und blockiert. Die Lösungen basieren auf der IPS-Stateful-DPI-Technologie, die eine kontextbezogene Paketanalyse des Netzwerkverkehrs ermöglicht und das Risiko der Beeinträchtigung von Geschäftsabläufen und Anwendungen reduziert. Mithilfe von IDS-Regeln („Intrusion Detection System") erkennen Stormshields Firewalls für die Industrie Cyberbedrohungen, ohne dass die Produktion unterbrochen werden muss. Ergebnis: Das Schutzniveau der Infrastruktur wird erhöht. Dazu gibt es viele weitere Tools wie etwa den „Stormshield Log Supervisor" (SLS), eine neue Log-Management-Lösung unserer Stormshield-Network-Security-Firewalls. Kurz gesagt: ein Sicherheitsversprechen in Echtzeit.

**it security:** *Herr Gries, wir danken für das Gespräch!*

# Gravierende Folgen des neuen SAP-Lizenzmodells

## UNGEPRÜFTE BERECHTIGUNGEN: GEFÄHRLICH – UND NUN AUCH TEUER!

Es war zuvor bereits kaum empfehlenswert, wenn Unternehmen ihre Bestandsrollen einfach 1:1 nach S/4HANA migrieren. Mit dem neuen Lizenzmodell sind zu großzügig gesetzte Berechtigungen künftig aber nicht mehr allein sicherheitstechnisch brisant, sondern führen zur regelrechten Kostenexplosion. Worauf ist beim Umstieg mit Blick auf das neue Lizenzmodell also mehr denn je zu achten?

Eine Unternehmensumfrage im Rahmen der IT-Onlinekonferenz Ende Januar zur Überprüfung von SAP-Berechtigungsrollen bestätigt den Eindruck folgenreicher Unkenntnis: Gut 65 Prozent der Unternehmen prüfen diese nur unregelmäßig, teilweise oder überhaupt nicht. Und bezeichnende 20 Prozent wollen oder können dazu keine Angaben machen, was erfahrungsgemäß auf Ersterem beruht. Denn viele sind sich der Konsequenzen des neuen Lizenzmodells für die Migration einfach nicht bewusst, und das sollte sich schleunigst ändern.

**Der Status quo**

Betrachtet man, wie Berechtigungsprojekte über die letzten 25 Jahre SAP verliefen, ergibt sich: Klassischerweise wurde kurz vor knapp ein Berechtigungskonzept definiert, das irgendwie compliant funktioniert, und Rollen dann so gebaut, dass die Anwender nutzen konnten, was sie sollten. Niemand hat Gedanken daran verschwendet, dass es verschiedene Zugriffstechnologien geben und welche monetären Auswirkungen dies haben könnte. Aber genau das ist jetzt der Fall in S/4HANA-Projekten: Neue Technologien setzen entsprechende Szenarien voraus, das SAP-Lizenzmodell wurde immer komplexer und ändert sich nun grundlegend.

Klar ist, dass die Frage der Lizenzierung bei der technischen Zuweisung von Berechtigungen in den meisten Unternehmen vernachlässigt wird. In vielen werden Lizenzkosten überhaupt erst seit Kurzem an einzelne Abteilungen weiterverrechnet, was im Endeffekt dazu geführt hat, dass Berechtigungen ausufern. Bei manchen Projekten trifft man auf User mit 200 bis 500 Berechtigungen. Benötigt werden davon allenfalls 25 Prozent. Werden Kunden nun gefragt, mit welchem Lizenzmodell und Berechtigungskonzept sie den Wechsel zu S/4HANA vorbereiten, dann wissen diese meist gar nicht, was die Wahl zwischen einer Product- und einer Contract Conversion in letzter Konsequenz bedeutet. Wo liegen also die Herausforderungen bei S/4HANA-Umstellungen und neuem Lizenzmodell?

DIE TIEFGREIFENDEN FOLGEN DES WECHSELS VON VERBRAUCHS- ZU BERECHTIGUNGSBASIERTER LIZENZIERUNG WERDEN VON DEN MEISTEN SAP-KUNDEN FATAL UNTERSCHÄTZT.

**Ralf Kempf, CTO, Pathlock Deutschland, www.pathlock.com/de**

**Die Contract Conversion**

Contract Conversion bedeutet vereinfacht gesagt die Ablösung der Bestandsverträge. Hier nimmt man die bestehenden Verträge, den Lizenz- und auch den Softwarewert, der in diesen Lizenzen und Verträgen steht, zusammen und bewertet sie. Dieser Wert kann mit bis zu 98 Prozent auf die Neuanschaffung angerechnet werden. Es wird dann für S/4HANA ein neuer Vertrag erstellt und dieser gilt fortan mit all seinen Folgen. Entscheidend ist dabei: Im Bereich S/4HANA basiert die Lizenzierung nun auf theoretischen Berechtigungen und nicht mehr auf der tatsächlichen Nutzung, die vom User verursacht wurde. Dafür zeichnet die SAP über einen Zeitraum von per Standardeinstellung drei Monaten auf, auf welche Berechtigungen ein User im System Zugriff gehabt haben könnte, wofür dann allein aufgrund potenzieller Nutzung eine Lizenz fällig wird. Relevant ist dann nicht mehr die tatsächlich genutzte Transaktion, sondern alles, was man theoretisch mit seinen Berechtigungen hätte tun können. Und das kann bei einem großzügig gesetzten Berechtigungskonzept äußerst problematisch werden. Zusätzlich sind Tools, die bis dato sehr verlässliche Ergebnisse zur Optimierung von SAP-Lizenzen lieferten, mit dem neuen Lizenzmodell obsolet geworden.


**Die Product Conversion**

Product Conversion bedeutet, dass alte Verträge (zunächst) bestehen bleiben. Im Gegensatz zur Contract Conversion ist es hier möglich, die bestehenden Verträge mit der SAP und damit eben auch deren Bedingungen zur Lizenzierung beizubehalten. Neue Produkte aus S/4HANA werden dann hinzugefügt, das heißt, wer eine neue Engine nutzen will, die es nur unter S/4HANA gibt, kauft diese hinzu und lizenziert sie entsprechend. Aber er verbleibt mit seinen Nutzungslizenzen mehr oder weniger im ECC-Bereich und vermisst weiterhin nach Verbrauch und nicht nach Berechtigung. Es findet damit natürlich aber auch keine Wandlung aus bestehenden Lizenzen wie bei der Contract Conversion statt. Zunächst wird also an das Bestehende einfach nur ein Vertrag über den konkreten Zukauf angefügt und die Lizenzierung basiert weiterhin auf tatsächlicher Nutzung.

**Die Konsequenzen**

Das Bisherige könnte zu dem Schluss verleiten, wenn man die Product Conversion wählt, bleibt alles, was das Thema Berechtigungen angeht, erst mal beim Alten, nur mit der Contract Conversion holt man sich die geschilderte Problematik ins Haus. Das ist aber in vielerlei Hinsicht zu kurz gedacht. Zum einen, weil es in den neuen Modellen neue Anwendungen gibt, während andere wegfallen, und wenn man dann Rollen baut, die kleinste Änderung dazu führen kann, dass diese nicht mehr lizenzkompatibel sind, was die entsprechenden Konsequenzen hat.

Zum anderen: Wenn man eine Product Conversion betreibt, zeigt die Erfahrung, dass die benötigten Berechtigungen für die neu hinzugekauften Produkte meist einfach zu den alten Rollen hinzugefügt werden. Das heißt, es findet kaum eine Auseinandersetzung mit den bestehenden SAP-Rollen statt, mit der Folge, dass nicht mehr benötigte Berechtigungen weiterhin nicht entfernt werden. Was die Rolle angeht, wird diese erweitert, statt sie auf ein gesundes Maß zu reduzieren.

Selbst wenn man die eindringlichen Warnungen der Sicherheitsexperten weiterhin ignoriert, gilt: Ausufernde Berechtigungen werden mittelfristig sehr, sehr teuer. Dabei zeigt die Erfahrung: Im Schnitt braucht ein User 75 Prozent der ihm zugewiesenen Berechtigungen überhaupt nicht. Das ist zumindest finanziell noch unproblematisch, solange auf Verbrauch lizenziert werden kann. Da man aber später auf Berechtigungen lizenzieren muss, und das wird passieren, entscheidet ja nicht mehr das Did-do eines Users, sondern ausschließlich das Could-do. Und dann werden diese 75 Prozent, die nie benutzt wurden, mit eingerechnet. Die Erfahrung der letzten Jahre im Bereich ECC hat gezeigt, dass diese Änderungen definitiv kommen werden, auch wenn der Aufschrei in der DSAG und anderen Gremien groß sein wird.

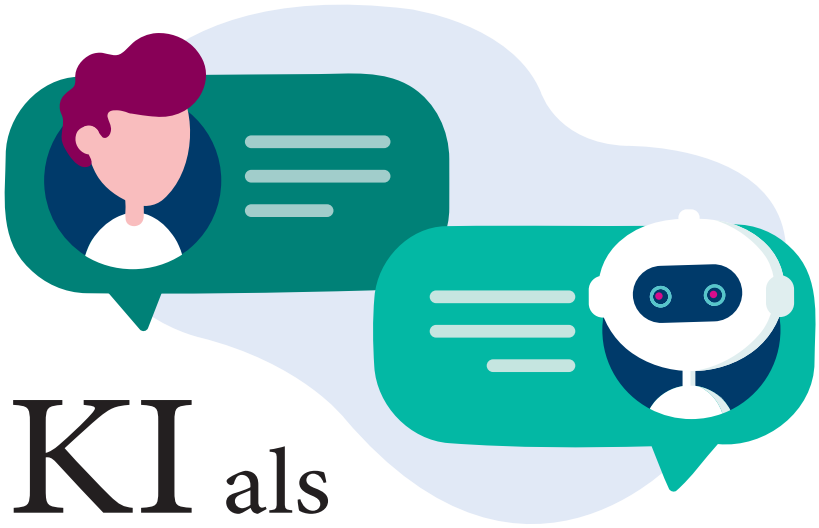
**Der Best Practice Ansatz**

Wie achtet man dann aber zukunftssicher auf Berechtigungen und Lizenzen im Projekt Rollenmigration? Die klare Antwort ist: Alles außer einem Greenfield-Ansatz macht bei S/4HANA-Berechtigungen nun keinen Sinn mehr! Hier bringt es auch nichts zu sagen, wir räumen auf, weil dies nicht so gründlich erfolgt wie eine Neuerstellung. Der richtige Ansatz eines Best Practice ist, über eine Verbrauchsanalyse aller Nutzer im aktuellen System festzustellen, was haben wir wirklich gebraucht, sowie eine Rollenanalyse im Nachgang der Verbrauchsanalyse durchzuführen. Und dann zu klären, wie bilden die aktuellen Rollen den tatsächlichen Verbrauch ab? Dann erfolgt die Neuzuordnung der Lizenzen aufgrund der Verbrauchsanalyse. Und dafür sind zum jetzigen Zeitpunkt Tools wie die von Pathlock unverzichtbar für die kontinuierliche Kontrolle der Ergebnisse. Das bezieht sich sowohl auf die Analyse dessen, was gebraucht wird, als auch auf die Ergebnisse bei der Neuerstellung der Rolle und der Berechtigungen.

**Eine Empfehlung zum Schluss**

Die SAP bietet jetzt ein Tool, mit dem man auf Knopfdruck ermittelt, ob eine Rolle teuer wird. Man kann sich dafür unverbindlich registrieren und die dazugehörige Excel-Tabelle zeigt, welches Berechtigungsobjekt in welcher Ausprägung welchem Lizenztyp zugeordnet ist. Und man kann einen Testlauf nutzen, der ausgibt, aktuell wäre eine S/4HANA-Lizenz exakt so teuer. Gut möglich, dass dieses Tool für die meisten Unternehmen einen erheblichen Schreckmoment und notwendigen Weckruf bereithält.

***Ralf Kempf***



# KI als Betrugsszenario

## POTENZIELLE GEFAHREN DURCH CHATBOTS UND TEXT-TO-SPEECH

Im Bereich der künstlichen Intelligenz (KI) hat sich in den letzten Monaten viel getan. Vor allem der seit vergangenem November verfügbare Chatbot ChatGPT von OpenAI sorgt für Aufregung. Das textbasierte Dialogsystem basiert auf maschinellem Lernen und beantwortet Fragen in natürlicher Sprache.

Im Januar hat Microsoft zudem seine neue KI „Vall-E" vorgestellt. Das Sprachsynthesemodell kann menschliche Stimmen imitieren. Dafür reicht eine Aufnahme der Originalstimme von nur drei Sekunden. Die KI simuliert die menschliche Stimme sehr genau und kann sogar emotionale Betonungen des Sprechers nachahmen.

Die Entwickler beider Systeme sind sich allerdings bewusst, dass ihre KI-Modelle nicht nur Vorteile bieten. Mit der zunehmenden Beliebtheit solcher Programme steigt auch das Betrugspotenzial.

Welche Betrugsszenarien durch den Einsatz von KI-Modellen zukünftig möglich sind:

### #1 Phishing und Social Engineering mithilfe von KI

ChatGPT nutzt die Verarbeitung natürlicher Sprache (Natural Language Processing, NLP). Das könnten Cyber-Kriminelle für Phishing- und Social-Engineering-Kampagnen ausnutzen. Es lassen sich beispielsweise E-Mail-Konversationen authentisch nachstellen, ohne dass Grammatik- oder Rechtschreibfehler erkennbar sind. Dabei sorgt ein natürlicher Sprachfluss für Vertrauen bei den potenziellen Opfern: Der vermeintliche Bankmitarbeiter, der den Kunden per E-Mail auffordert, seine Kontodaten zur Verifizierung anzugeben, wirkt durch die natürliche Sprache authentisch. Auf diese Weise können Betrüger problemlos Daten abgreifen oder komplette Konten übernehmen.

### #2 Herausforderung: Geldwäschebekämpfung

Auch die Bekämpfung der Geldwäsche stellt eine Herausforderung dar und ist oft mit hohen Kosten verbunden. Hier bleibt die erste Überweisung meist unentdeckt. Entweder wird sie vom Überwachungssystem übersehen, oder der „Kunde" beziehungsweise der AML-Analyst (Anti-Money Laundering) bestätigt die Transaktion als unverdächtig. Denn mithilfe von KI-gestützten Chatbots wie ChatGPT können Geldwäscher Gespräche generieren, die scheinbar legitime Geschäftsaktivitäten zum Gegenstand haben. In Wirklichkeit dienen sie jedoch dazu, Geldtransfers zu verschleiern. Dadurch wird es für Finanzinstitute immer schwieriger, die gängigen Muster von Geldwäscheaktivitäten zu erkennen.

Ein weiteres Problem ist die Rekrutierung ahnungsloser Personen zur Geldwäsche. Viele der Konten werden von arglosen Personen eröffnet, die glauben, einen ertragreichen Nebenjob gefunden zu haben. Dabei wissen die Betroffenen oft nicht, dass sie als Geldwäscher agieren und ihr Konto für kriminelle Aktivitäten nutzen, oder es dafür zur Verfügung stellen. Denn die Betrüger geben sich als legitime Unternehmen aus und versprechen schnelles Geld. Und mit ChatGPT lässt sich die vermeintliche Stellenanzeige und der nachfolgende Rekrutierungsprozess noch überzeugender gestalten.

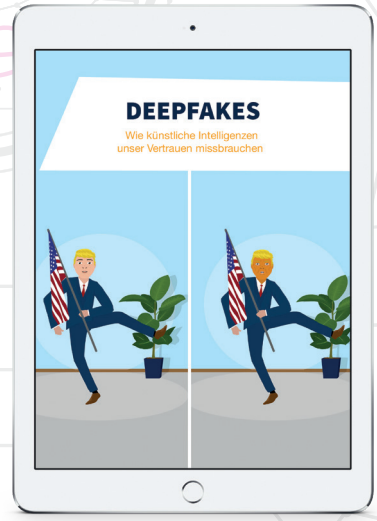
### #3 Verhaltensbiometrie schafft Abhilfe

Verhaltensbiometrie kann eine wichtige Rolle beim Aufdecken von Betrugsversuchen und Geldwäsche spielen. Durch die Analyse des Benutzerverhaltens, etwa der Tippgeschwindigkeit, den Tastenanschlägen und Mausbewegungen kann das normale Verhalten eines Benutzers festgelegt werden. Anhand davon kann die Software erkennen, ob es sich tatsächlich um den angemeldeten Benutzer handelt, oder um einen Betrüger. Auch viele andere Betrugsversuche lassen sich so erkennen. Auf diese Weise können auch Konten ausfindig gemacht werden, die zu einem späteren Zeitpunkt für Geldwäsche genutzt werden sollen.

***www.biocatch.com***

# Fälschung oder Realität?

## WIE KÜNSTLICHE INTELLIGENZEN UNSER VERTRAUEN MISSBRAUCHEN




Deepfake ist eine Wortschöpfung aus „Deep Learning" und „Fake". Sie beschreibt eine Methode, die Bilder, Videos oder Audioformate mithilfe künstlicher Intelligenz so manipulieren kann, dass das menschliche Auge oder Ohr kaum noch in der Lage ist, diese Fälschungen zu erkennen.

Deepfakes werden mit neuronalen Netzen erstellt: Füttert man diese Netze mit ausreichend Daten, können sie vorhersagen, wie Daten der gleichen Art aussehen könnten. So zum Beispiel das GAN (Generative Adversarial Network): Es besteht aus einem ermittelnden Algorithmus, der versucht, die Fälschung eines anderen Algorithmus zu identifizieren und daraus zu lernen (Deep-Learning).

Die wohl weitverbreitetste Art ist das Austauschen von Gesichtern in Bildern oder Videos (Face Swapping). Expert:innen warnen, Deepfakes könnten bald so perfekt sein, dass wir nicht mehr in der Lage sein werden, sie als solche zu identifizieren. Von 2018 bis 2020 verdoppelte sich die Zahl der Fake-Videos alle sechs Monate und brachte es im Dezember 2020 so auf über 85.000 Videos im Netz. Das schockierende: Laut einer Studie waren 96 Prozent aller Deepfake-Videos pornografisch.

Die Folgen von Deepfakes reichen bis in die Politik wie im Fall des Präsidenten von Gabun, bei dem ein gefälschtes Video einen Putschversuch auslöste, oder dem der US-Demokratin Nancy Pelosi, in dem sie als betrunken dargestellt wurde, um sie zu diffamieren.

Neben der missbräuchlichen Verwendung bieten Deepfakes auch Positives. Sie bieten zum Beispiel die Möglichkeit, Filme mit bereits verstorbenen Schauspieler:innen zu produzieren oder werden von KIs genutzt, um Videos aus geschriebenem Text, für Präsentationen oder E-Learning zu erzeugen.

***www.increaseyourskills.com***

# Moderne Cybersecurity

## DER BLICK NACH INNEN

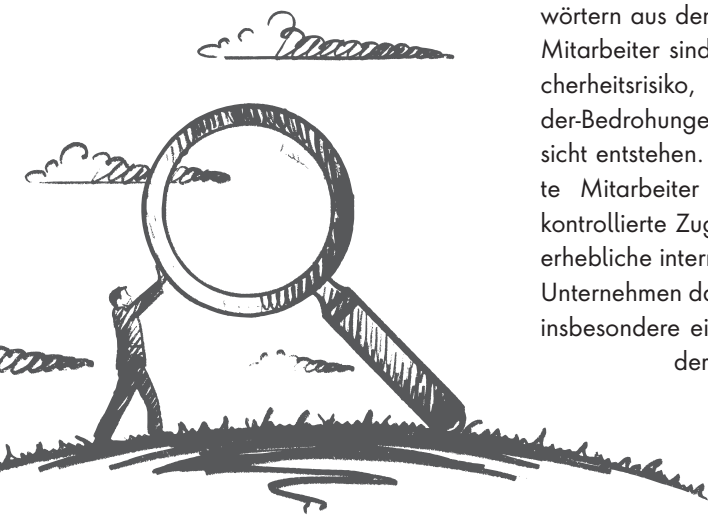
Unternehmen sind mit einem Ansturm von Cyberangriffen konfrontiert. Laut dem Cybersecurity Census Report 2022 von Keeper Security ist fast ein Viertel (24 Prozent) jährlich mehr als 251 Angriffen ausgesetzt; 14 Prozent erleben mehr als 500 Angriffe pro Jahr. Die Situation wird sich voraussichtlich noch weiter verschlechtern. 81 Prozent der IT-Führungskräfte gehen davon aus, dass die Gesamtzahl der Cyberangriffe auf deutsche Unternehmen im nächsten Jahr zunehmen wird, wobei 47 Prozent der deutschen Unternehmen sogar davon ausgehen, dass auch die Zahl der erfolgreichen Angriffe steigen wird.

**Sensibilisierung für Bedrohungen und Security**

Der Keeper Cybersecurity Census Report 2022 wurde in Zusammenarbeit mit Sapio Research in mehreren Ländern erstellt. In Deutschland wurden 514 IT-Manager befragt. Diese explosionsartige Zunahme der Angriffe von 24 Prozent und die künftigen Aussichten von noch mehr Angriffen veranlassen Unternehmen beziehungsweise deren IT-Manager zur Reaktion: IT-Teams stocken ihre Sicherheitsvorkehrungen und Ausgaben auf. Im Cybersecurity Census Report 2022 fand Keeper fand heraus, dass 66 Prozent der IT-Leiter im vergangenen Jahr neue Mitarbeiter im Bereich Cybersicherheit eingestellt und 83 Prozent ihre Ausgaben für Cybersicherheitssoftware erhöht haben. 70 Prozent erwarten, dass ihre Cybersicherheitsbudgets in den nächsten zwölf Monaten steigen werden.

**Verschwiegenheit und die Gefahr von innen**

Die Wirksamkeit von Budgeterhöhungen und Investitionen wird jedoch begrenzt sein, wenn ein entscheidender Schwachpunkt in der Abwehr bestehen bleibt. Viele Unternehmen sind so sehr damit beschäftigt, nach äußeren Gefahren Ausschau zu halten, dass sie einen wichtigen Punkt vergessen – sie sind auch mit ernsthaften Bedrohungen von innen konfrontiert.



Bei einer Insider-Bedrohung geht es nicht nur darum, dass sich ein unzufriedener Mitarbeiter mit wichtigen Passwörtern aus dem Staub macht. Solche Mitarbeiter sind zwar durchaus ein Sicherheitsrisiko, allerdings können Insider-Bedrohungen auch ohne böse Absicht entstehen. Unzureichend geschulte Mitarbeiter oder nur rudimentär kontrollierte Zugänge stellen ebenfalls erhebliche interne Bedrohungen für ein Unternehmen dar. Darüber hinaus birgt insbesondere eine Unternehmenskultur der Angst oder Unsicherheit ein erhebliches Risikopotenzial, über das jedoch nur selten gesprochen wird. Alarmierend beispielsweise ist, dass laut der Umfrage von Keeper mehr als die Hälfte (51 Prozent) der Befragten deutschen IT-Führungskräfte von einem Cyberangriff wussten und diesen für sich behielten und nicht den zuständigen Behörden meldeten.

In der IT-Branche weiß man, dass eine nicht gemeldete Sicherheitsverletzung verheerende Folgen für ein Unternehmen aber auch für Partner und Kunden haben kann. Die DSGVO sieht eine Meldepflicht für die Verletzung personenbezogener Daten vor und Kritische

DIE SCHAFFUNG EINER STARKEN KULTUR DER CYBERSICHERHEIT ERFORDERT AUCH, DASS UNTERNEHMEN IHRE SICHERHEITSSCHULUNGEN STRATEGISCH UND GEZIELT DURCHFÜHREN UND DASS GEEIGNETE LÖSUNGEN FÜR DIE SECURITY ZUM EINSATZ KOMMEN.

**Darren Guccione, CEO und Mitbegründer, Keeper Security, KeeperSecurity.com**


Infrastrukturen sowie einige weitere Bereiche haben eine besondere Meldepflicht. Ein Verschweigen von Datenschutzverletzungen kann also rechtliche Konsequenzen und gegebenenfalls empfindliche Strafen nach sich ziehen. Das kann Unternehmen nicht nur in eine finanzielle Katastrophe führen, sondern zusätzlich einen nicht zu vernachlässigenden Image- und Reputationsverlust zur Folge haben, der sich zusätzlich negativ auf das Geschäft auswirken kann. Mehr noch: Verschwiegene und nicht detailliert untersuchte Angriffe führen oft dazu, dass Cyberkriminellen Tür und Tor offen stehen. Sie können einen weiteren Angriff starten, indem sie Malware aus ihren vorherigen Angriffen in den Netzwerken unbemerkt zurücklassen. Durch die Verheimlichung werden die Unternehmen der Möglichkeit beraubt, eine Schwachstelle genau zu analysieren und zu beheben sowie aus einem Vorfall zu lernen. Wenn die Behörden nicht benachrichtigt werden, bleiben zudem die Cyberkriminellen auf freiem Fuß und können mit derselben Taktik neue Opfer angreifen.

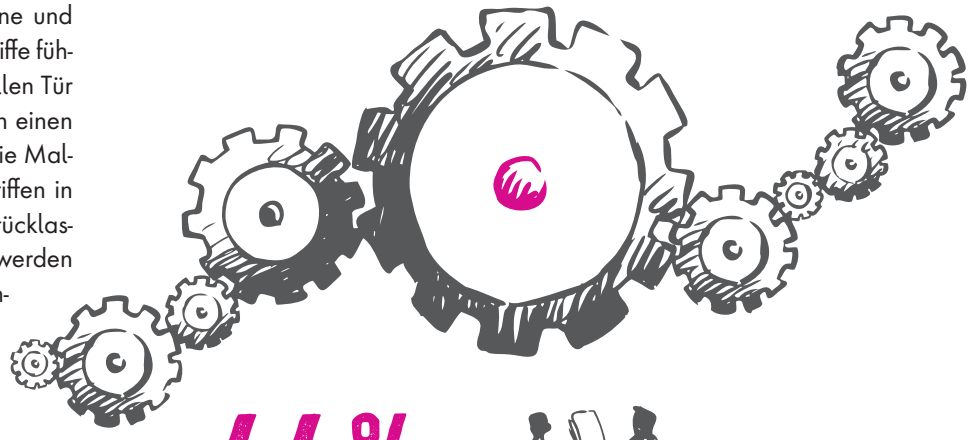
**Sicherheitskultur der Offenheit**

Wenn IT-Experten ihr Unternehmen vor Cyberangriffen schützen wollen, müssen sie auch die Kultur der Geheimniskrämerei abschaffen. Sie sollten für eine Umgebung sorgen, die von Transparenz, Unterstützung und Verantwortungsbewusstsein geprägt ist und in der sich jeder Mitarbeiter traut, sich zu melden, sobald ein Vorfall eintritt – auch wenn es ein Fehlalarm sein könnte.

**Zu wenig Wissen über moderne Security-Konzepte**

Die Schaffung einer starken Kultur der Cybersicherheit erfordert auch, dass Unternehmen ihre Sicherheitsschulungen strategisch und gezielt durchführen und dass geeignete Lösungen für die Security zum Einsatz kommen. Keeper hat im Cybersecurity Census Report 2022 herausgefunden, dass 78 Prozent der deutschen IT-Fachleute über einen Einbruch in ihrem eigenen Unternehmen besorgt sind - und das aus gutem Grund: Es gibt immer noch einen beunruhigenden Mangel an Wissen über wichtige Sicherheitskonzepte, sowohl in den IT-Teams als auch im gesamten Unternehmen. Mehr als ein Drittel der deutschen IT-Leiter (35 Prozent) geben an, dass sie die Konzepte „Zero Trust" und „Zero Knowledge" im Zusammenhang mit der Cybersicherheit „einigermaßen", „minimal" oder „gar nicht" verstehen. 37 Prozent behaupten, dass sie diese Konzepte zwar vollständig verstehen, aber nicht glauben, dass der Rest ihres Unternehmens sie nachvollziehen kann. Es ist klar, dass mehr Aufklärung nötig ist. Unternehmen sollten sicherstellen, dass sie die Lücken im Security-Wissen erkennen und schließen.

**Wurde in Ihrem Unternehmen schon einmal eine Sicherheitslücke innerhalb Ihrer Organisation festgestellt und macht Ihnen das Sorgen?**



**44 %**

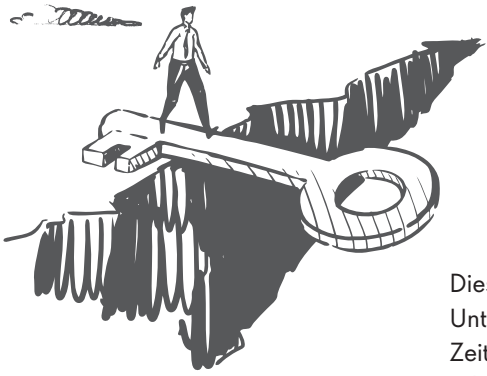
Ja, ich habe einen Verstoß innerhalb meiner Organisation erlebt, daher macht mir das Sorgen

**22 %**

Nein, ich habe noch keinen Verstoß innerhalb meiner Organisation erlebt und ich mache mir auch keine Sorgen darüber

**34 %**

Ja, ich bin besorgt über die Gefahr einer Sicherheitsverletzung innerhalb meiner Organisation, aber ich habe noch keine erlebt



Neben den klassischen Maßnahmen zur Security, wie beispielsweise Security-Lösungen für Endgeräte, Server, das Netzwerk oder für die Arbeit in der Cloud ist auch ein Umdenken bei der Einstellung der Unternehmen zur Identitätssicherheit erforderlich. Passwortsicherheit ist hierbei das zentrale Thema. Zu viele Unternehmen haben bisher keinen geeigneten Passwort-Schutz inklusive dessen Management etabliert. Die Zahlen des Keeper Cybersecurity Census Report 2022 belegen dies: In der Umfrage geben 31 Prozent der IT-Leiter an, dass ihre Organisation es den Mitarbeitern überlässt, ihre eigenen Passwörter festzulegen und dass die Mitarbeiter ihre Anmeldedaten häufig gemeinsam nutzen.

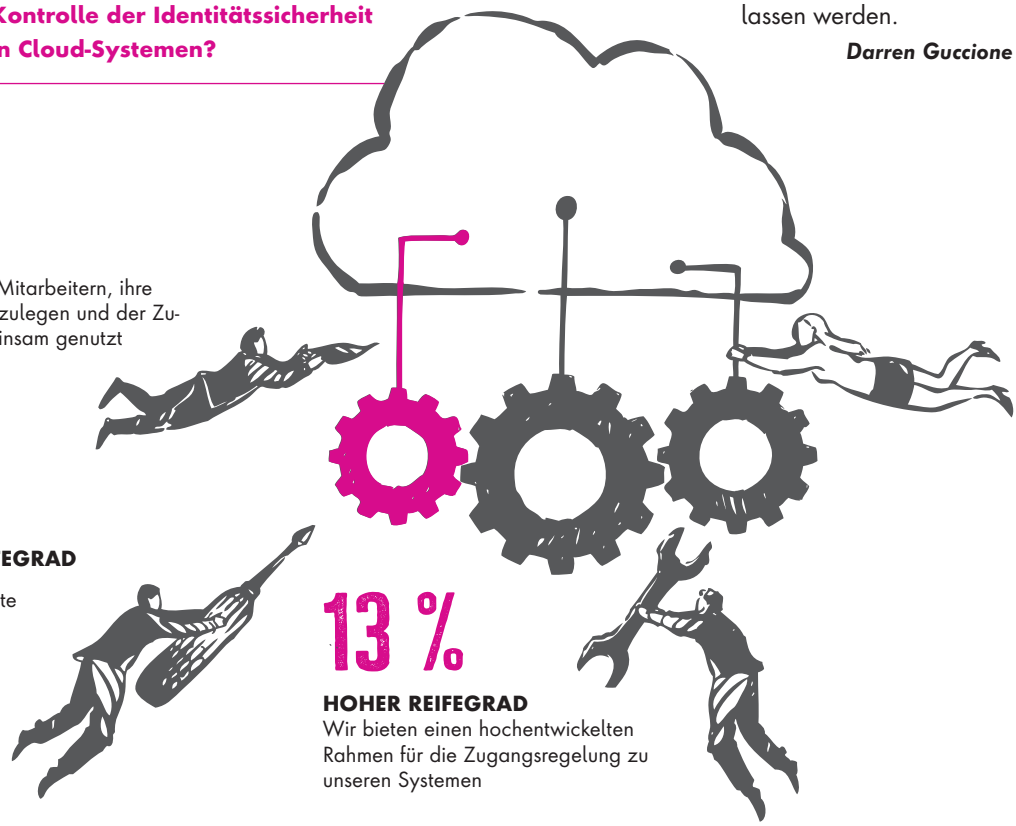
Dies stellt eine enorme Bedrohung für Unternehmen dar, insbesondere im Zeitalter der Remote-Arbeit, in der Mitarbeiter von verschiedenen Standorten aus und mit unterschiedlichen Geräten Zugang zu den Unternehmenssystemen benötigen. Das Mindeste, was Unternehmen tun sollten, ist ihren Mitarbeitern Leitlinien und bewährte Verfahren für die Verwaltung von Passwörtern und Zugängen an die Hand zu geben. Der sicherste Weg besteht allerdings darin, ein ausgereiftes System zur Zugangsregelung zu den Systemen zu implementieren. Passwort-Manager für Unternehmensumgebungen sind für diese Anforderung eine zuverlässige Lösung. Der Anwender kann von jedem seiner Geräte aus auf den Passwort-Manager zugreifen, um seine Passwörter zu erstellen und sicher zu nutzen. Anerkannte Verschlüsselungstechnologien und die Zero-Knowledge-Architektur sorgen dafür, dass niemand außer dem Nutzer Zugriff auf die Inhalte des Passwort-Tresors bekommt. Bei den Passwortmanager-Lösungen für Unternehmen sind die Tresore der einzelnen Mitarbeiter separiert und in SaaS- oder Cloud-Umgebungen mit zusätzlichen Schutzmechanismen ausgestattet.

**Security ist gleichbedeutend mit einem 360-Grad-Blick**

Angesichts der zunehmenden Zahl von Cyberangriffen müssen Unternehmen erkennen, woher die Gefahr kommt. Dabei sind Bedrohungen von innen ein ebenso großes Risiko wie von außen. Durch eine nicht zeit- und situationsgemäße IT- und Security-Kultur sind viele Unternehmen extrem anfällig. Wenn Unternehmen ihre Netze und digitalen Werte schützen wollen, sollten sie dafür sorgen, dass ausschließlich die Cyberkriminellen im Dunkeln stehengelassen werden.

***Darren Guccione***

**Welchen Reifegrad hat Ihr Unternehmen in Bezug auf die Transparenz und Kontrolle der Identitätssicherheit On-Premises und in Cloud-Systemen?**



**31 %**

**GERINGE REIFE**

Wir überlassen es den Mitarbeitern, ihre eigenen Passwörter festzulegen und der Zugang wird häufig gemeinsam genutzt

**56 %**

**DURCHSCHNITTLICHER REIFEGRAD**

Wir bieten Leitlinien und bewährte Verfahren für Passwörter und Zugangsverwaltung

**13 %**

**HOHER REIFEGRAD**

Wir bieten einen hochentwickelten Rahmen für die Zugangsregelung zu unseren Systemen

# ENDPUNKTSICHERHEIT FÜR MODERNES ARBEITEN

## SCHUTZ DER GERÄTEFLOTTE VOR CYBERANGRIFFEN

Endgerätesicherheit wird allgemein als Schutz Ihrer Geräteflotte vor Cyberangriffen verstanden. Obwohl dies ein wesentlicher Bestandteil ist, gehört zur erfolgreichen Implementierung und Gewährleistung der Endpunktsicherheit in Unternehmen noch mehr. Dabei handelt es sich nämlich um eine Reihe von Funktionen, die Ihre Geräte sowie Benutzer*innen vor einer sich ständig weiterentwickelnden Bedrohungslage schützen. In dem Sinne müssen auch Sie handeln und die richtigen Tools für Ihre Geräte auswählen.

**Mit diesem Whitepaper können Sie:**

- Unternehmensrisiken verstehen
- Endgerätesicherheit modernisieren
- Basislinien etablieren
- vor moderner Malware schützen
- Schwächen von All-in-One-Lösungen erkennen
- Sicherheit und Leistung vereinbaren


**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 12 Seiten und steht kostenlos zum Download bereit.
**www.it-daily.net/Download**

# KPIs für Cyber Resilienz

## CYBERANGRIFFE WERDEN MITTLERWEILE ALS NOTWENDIGES ÜBEL VON VIELEN WAHRGENOMMEN. WAS KANN MAN DAGEGEN TUN?

Cyber-Resilienz bedeutet, die Funktionsfähigkeit zentraler Prozesse und Infrastrukturen selbst unter außergewöhnlichen Umständen auf ausreichendem Niveau aufrechtzuerhalten. Ein 100prozentiger Schutz ist in der Realität eh ein Wunschdenken. Es muss in den Unternehmen mehr Bewusstsein für die reale Wirkung von IT-Sicherheitsmaßnahmen entwickelt werden.

Ransomware war im Vorjahr eines der Topthemen. Bei vielen dieser Angriffe handelte es sich um doppelte Erpressungen, bei denen der Angreifer nicht nur mit der Verschlüsselung, sondern auch mit der Herausgabe von Daten drohte.

Bei dem Versuch, mit Ransomware-Banden und anderen Angreifern Schritt zu halten, sahen sich die Unternehmen häufig mit den Herausforderungen einer komplexen Umgebung konfrontiert, die Cloud-Dienste und auch lokal verteilte Mitarbeiter umfasst. Die Aufrechterhaltung der Sichtbarkeit und Kontrolle über Benutzer, Anwendungen und Daten war wohl noch nie komplizierter als heute gewesen.

**WAS ERWARTET UNS AKTUELL? FÜNF KONKRETE ANGRIFFSVEKTOREN RÜCKEN IN DEN FOKUS.**

1

### Cybersicherheit von zu Hause wird für Unternehmen zur Priorität

Um die relativ neue Verlagerung zur entfernten Mitarbeit zu unterstützen, mussten viele Unternehmen zunächst den Ansatz „erst umziehen, später planen" verfolgen und ihre netzwerkzentrierte Sicherheitswelt hinter sich lassen, die es den IT-Teams erlaubt hatte, den Großteil des Netzwerks zu beherrschen und zu kontrollieren. Da inzwischen immer deutlicher wird, dass das Arbeiten von überall aus nicht mehr aufzuhalten ist (und die Anzahl der Orte, an denen Geräte des Unternehmens installiert sind, stetig zunimmt), haben Unternehmen damit begonnen, von kurzfristigen Taktiken zu langfristigen Strategien überzugehen, die sich darauf konzentrieren, die uneinheitliche Sichtbarkeit und Kontrolle der IT-Teams über Endgeräte und Netzwerkzugriff zu überwinden. Dies trägt wiederum zu ihrer Fähigkeit bei, Probleme der Endbenutzer zu diagnostizieren und drohende Risiken zu korrigieren. Um diese Probleme anzugehen, müssen Unternehmen auch Maßnahmen für strenge Zugriffskontrollen ergreifen. Was uns zu unserem nächsten Trend bringt.

2

### Zunehmende Einführung von software-definierten Maßnahmen, die Zero Trust Network Access in der Praxis umsetzen

Da 51 Prozent der Unternehmen Beweise dafür besitzen, dass angegriffene Endpoint-Geräte für den Zugriff auf Unternehmensdaten über entfernte Zugriffsverbindungen verwendet wurden, ist Zero Trust für viele Unternehmen bereits zu einem wichtigen strategischen Schwerpunkt geworden. Wir gehen davon aus, dass sich dieser Trend im aktuellen Jahr 2023 fortsetzen wird. Overlay-Netzwerke und software-definierte Architekturen tragen aufgrund der Seg-

mentierung des Datenverkehrs dazu bei, Zero Trust zu ermöglichen. Laut einem Bericht von Gartner treten die Vorteile von Zero Trust Network Access unmittelbar zutage und „bieten erhebliche Vorteile in Bezug auf Benutzerfreundlichkeit, Agilität, Anpassungsfähigkeit und einfache Richtlinienverwaltung".

## 3 Wirtschaftliche Bedingungen erhöhen das Risiko von Insider-Bedrohungen

Politische Umstände und Preisschocks im Einzelhandel haben die Aufmerksamkeit der Öffentlichkeit stärker auf die Wirtschaft gelenkt. Im neuen Jahr 2023 werden diese Bedingungen ein Umfeld schaffen, das für Cyber-Kriminelle günstig ist, die auf der Suche nach unberechenbaren Mitarbeitern sind: Diese sind eventuell bereit, mit dem Verkauf von Daten oder dem Zugriff auf Unternehmens-Ressourcen zusätzliches Geld zu verdienen. Um sich vor dieser Möglichkeit zu schützen, muss der Schwerpunkt auf strategische Vorbereitungen gegen Insider-Bedrohungen gelegt werden. Dies bedeutet, dass Wege gefunden werden müssen, um die Sichtbarkeit und die Kontrolle über die Geräte der Mitarbeiter zu erhöhen, insbesondere bei Unternehmen, in denen ein großer Teil der Belegschaft von zuhause aus arbeitet. IT- und Sicherheitsexperten müssen zu jedem Zeitpunkt wissen, ob die Endgeräte ihrer Mitarbeiter sensible Daten enthalten, die ihr Unternehmen einem Insider-Risiko aussetzen.

## 4 Ransomware-Angriffe richten weiterhin großen Schaden an

Wenn etwas funktioniert, warum sollte man es dann ändern? Das Geschäft mit Ransomware läuft gut für die Angreifer, und das Modell von Ransomware-as-a-Service (RaaS) hat den Start von Angriffen sehr viel einfacher gemacht. Wir gehen davon aus, dass diese Art von Angriffen weiterhin Organisationen im öffentlichen und privaten Sektor betreffen wird. IT-Führungskräfte in Unternehmen müssen sich unbedingt auf die Vorbereitung in Sachen Ransomware konzentrieren, was insbesondere auch die Fähigkeit betrifft, Endpunkte und geschäftskritische Infrastrukturen wie zum Beispiel Active Directory im Falle eines Angriffs wiederherzustellen.

CYBER-WIDERSTANDS-FÄHIGKEIT WIRD EINE NEUER KEY PERFOR-MANCE INDICATOR (KPI) FÜR UNTERNEHMEN.

**Torsten George, Cybersecurity-Evangelist, Absolute Software, www.absolute.com/de**

## 5 Cyber-Widerstandsfähigkeit wird eine neue Key Performance Indicator (KPI) für Unternehmen

Trotz der langjährigen Annahme, dass der Einsatz von mehr Sicherheitslösungen zu einem besseren Schutz vor Bedrohungen führt, kann die Wahrheit ganz anders aussehen. Das liegt daran, dass jede Sicherheitsanwendung, die einem Endgerät hinzugefügt wird, die Komplexität und das Risiko erhöhen kann, zur Gefährdung und zur Anfälligkeit von Anwendungen beizutragen und den Gesamtzustand des Geräts zu beeinträchtigen. Letztendlich kommt es nicht auf die Anzahl der Sicherheitskontrollen an, sondern auf deren Wirksamkeit. Dies gilt insbesondere unter schwierigen wirtschaftlichen Bedingungen, in denen Unternehmen ihr Verteidigungsarsenal wahrscheinlich eher verkleinern werden. Wir gehen wiederum davon aus, dass sich die Cyber-Widerstandsfähigkeit zu einem neuen wichtigen Leistungsindikator (KPI) für Unternehmen entwickeln wird.

MITRE definiert diese Cyber-Resilienz als „die Fähigkeit, ungünstige Bedingungen, Belastungen, Angriffe oder Beeinträchtigungen von Cyber-Ressourcen zu antizipieren, ihnen zu widerstehen, sich an sie anzupassen oder sich von ihnen zu erholen". Durch die Konzentration auf proaktives Handeln und die Fähigkeit, Angriffen zu widerstehen und sich von ihnen zu erholen, stellt die Cyber-Resilienz eine Erweiterung der Art und Weise dar, wie Unternehmen häufig über Cyber Security denken. Es geht nicht nur um den einfachen Schutz von Systemen und Daten, sondern auch um die Verringerung des Risikos von Geschäftsunterbrechungen aufgrund von Cyber-Attacken.

Es ist unwahrscheinlich, dass die Bedrohungslage für Unternehmen abnehmen wird, und es wird weiterhin an IT-Leitern und Sicherheitsexperten liegen, Benutzer und Unternehmen aktiv zu schützen. Genauso wie im Jahr 2022 wird es eine Kombination aus umfassender Sichtbarkeit, effektiven Zugriffskontrollen und einer Verlagerung von defensiven Strategien der Cyber Security auf das Management von Störungen durch mehr Widerstandsfähigkeit erfordern. Grundsätzlich sollten wir alle darin übereinstimmen, intensiver auf Sicherheit zu achten und die Best Practices zu befolgen, die uns, unsere Daten und unsere Systeme weiterhin auf einem sicheren Niveau halten.

***Torsten George***


# Ransomware

## SO SCHÜTZEN SICH KLEINE UND MITTLERE UNTERNEHMEN EFFEKTIV

Plötzlich sind alle Systeme unter Verschluss und werden nur gegen ein Lösegeld wieder freigegeben: Ransomware gehört mittlerweile zu den Top-Angriffsmethoden von Cyber-Kriminellen. Jedes Unternehmen kann ins Visier geraten – auch kleine und mittelständische. Daher muss ein vielschichtiger Sicherheitsansatz her.

Das lukrative Geschäft mit Ransomware bildet im Untergrund sein eigenes kriminelles Ökosystem. Neben eigenmächtigen Kampagnen bieten Cyber-Kriminelle ihre Dienste, Tools sowie Wissen als Ransomware-as-a-Service auf dem Schwarzmarkt an und entwickeln ihre Vorgehensweisen stetig weiter. Der Ransomware-Markt ist im Laufe der Jahre gewachsen – innerhalb eines Jahres sogar um 13 Prozent – und ist mittlerweile zu einem der beliebtesten Cyber-Crime-Werkzeuge avanciert.

Das verwundert nicht, immerhin ist die Aussicht auf Profit vielversprechend. Laut einer aktuellen IDC-Studie sind oder waren mehr als 50 Prozent der von Ransomware betroffenen Unternehmen (70 Prozent) bereit, das geforderte Lösegeld zu zahlen. Die durchschnittliche Summe beläuft sich auf mehr als 253.000 Euro.

**Cyber-Kriminelle haben es auf die Schwächeren abgesehen**

Es sind jedoch nicht immer nur namhafte Großkonzerne, die Cyber-Kriminelle zu ihren Zielen erklären. Unternehmen jeder Branche und Größe sind potenzielle Opfer – kleine und mittelständische Unternehmen (KMUs) sind sogar besonders gefährdet. 2021 waren 70 Prozent der KMUs weltweit von Ransomware-Angriffen betroffen, in Deutschland sind diese mit der Hälfte aller Angriffe am stärksten gefährdet. Die Gründe leuchten ein:

ES GIBT KEIN ONE-SIZE-FITS-ALL-ALLHEILMITTEL GEGEN RANSOMWARE-ATTACKEN.

**Dr. Dieter Kehl, Director Sales DACH/ CEE/MEA, OpenText Cybersecurity, www.opentext.de**

KMUs verfügen nicht über die gleichen ausgereiften Schutzmechanismen wie große Unternehmen, was vor allem durch mangelndes IT-Budget und fehlende IT-Fachkräfte bedingt ist. Außerdem erregen sie weniger Aufmerksamkeit und machen dadurch seltener Schlagzeilen. Vor diesem Hintergrund ist eine ganzheitliche, vielschichtige Cyber-Sicherheitsstrategie, die ihren individuellen Anforderungen entspricht, unerlässlich.

**Die vier Säulen eines starken Cyber-Schutzes**

Der alleinige Einsatz von Antivirus-Programmen und/oder Firewalls reicht nicht aus, um sich umfassend vor Ransomware-Angriffen zu schützen. Vielmehr greifen mehrere Faktoren ineinander, denen auch KMUs im Rahmen ihrer Cyber-Sicherheitsstrategie Beachtung schenken müssen, um einen vielschichtigen Schutzmechanismus aufzubauen.

### 1. Schwachstellen ausfindig machen

In einem ersten Schritt gilt es, jene Schwachstellen zu identifizieren, über die sich Ransomware einschleusen lässt. Viele denken oftmals als erstes, dass es

sich dabei um ein technisches Problem handelt. Die Suche sollte sich jedoch bewusst über das gesamte Unternehmen erstrecken und sich nicht nur auf die IT selbst beschränken, da Schwachstellen verschiedene Formen annehmen können – wie die Mitarbeiter selbst. Die Zugangskontrolle spielt hier eine wichtige Rolle. Wie gehen Mitarbeiter mit ihrem Zugang um und welche Zugriffsprivilegien haben sie? Unternehmen müssen den Zugang so eingrenzen, dass ein Mitarbeiter, der Opfer einer Phishing-Attacke wurde, den Schadcode nicht über die gesamte Unternehmens-IT verteilt.

## 2. Über Social Engineering aufklären

Eine besonders populäre Methode, um Ransomware in ein Unternehmen zu bringen, ist Social Engineering. Dafür nutzen Cyber-Kriminelle alle Informationen, die sie über ihre Opfer ausfindig machen können, um vertrauenswürdig zu wirken. Die sozialen Medien sind eine beliebte Quelle: Hier finden sie Details zur Management-Hierarchie und zu einzelnen Führungskräften, die sie in Phishing-E-Mails einarbeiten. In den meisten Fällen ist es dann zu spät, wenn der Empfänger bemerkt, dass er hinters Licht geführt wurde.

In einem vielschichtigen Sicherheitssystem bildet E-Mail-Security die erste Abwehrlinie, die sich mithilfe von Künstlicher Intelligenz und Machine Learning stärken lässt. Die Technologien helfen dabei, den Großteil der schädlichen E-Mail-Eingänge zu blockieren, herauszufiltern und folglich zu verhindern, dass Mitarbeiter sie öffnen.

Außerdem sollten in Abständen von drei bis sechs Monaten Security-Awareness-Schulungen stattfinden. Anhand von echten Praxisbeispielen wird die Belegschaft für Cyber-Bedrohungen wie Phishing, Social Engineering und Ransomware sensibilisiert.

## 3. Notfallstrategien schützen

Viele Unternehmen haben mittlerweile Backup- und Recovery-Pläne in ihre Cyber-Sicherheitsstrategie aufgenommen – eine wichtige Maßnahme. Jedoch fällt dabei oftmals die Tatsache vom Tisch, dass diese Informationen während eines Ransomware-Angriffs durch die verantwortlichen Akteure ebenfalls verschlüsselt oder entfernt werden können. Um dieses Desaster zu umgehen, sollten Unternehmen vorab mehrere Kopien der Pläne anlegen und an verschiedenen Orten ablegen – wie zum Beispiel in Form einer lokalen und einer Cloud-Version. Außerdem empfiehlt es sich, auf Backup-Lösungen zu setzen, die verhindern, dass Angreifer Backup-Daten editieren, verschlüsseln oder anderweitig modifizieren.

## 4. Vielschichtigen Schutz implementieren

Es gibt kein One-size-fits-all-Allheilmittel gegen Ransomware-Attacken. Unter anderem liegt das an der Dynamik der Cyber-Crime-Landschaft: Akteure entwickeln ihre Angriffsmethoden, -taktiken und -Tools kontinuierlich weiter. In diesem Bedrohungsumfeld fällt es Unternehmen zunehmend schwerer, mit den Fortschritten im Untergrund mitzuhalten. Der beste Weg, um sich dieser Herausforderung zu stellen, ist ein Sicherheitsansatz, der aus vielen unabhängigen Schichten besteht. Auch wenn es Akteure durch die erste und vielleicht sogar zweite Schicht schaffen, müssen sie immer noch die restlichen überwinden. Teil dieser Aufstellung sollten Endpoint- und E-Mail-Security-Lösungen, Security-Schulungen, DNS-Schutz sowie eine Backup- und Recovery-Strategie sein. Damit alle Schichten effizient und langfristig ihren Zweck erfüllen können, sind regelmäßige Prüfungen und Updates notwendig.

**Fazit**

Cyber-Kriminelle wissen, dass KMUs oftmals nicht über die notwendigen Ressourcen Budget, Fachpersonal und Wissen verfügen, um sich den Cyber-Bedrohungen von heute zu stellen. Daher geraten sie zunehmend ins Visier von Angreifern. Sie können sich daher am effektivsten vor Ransomware-Angriffen schützen, wenn sie ihre Sicherheitsstrategie von Grund auf auf den vier Säulen aufbauen: Schwachstellen kennen, über Bedrohungen aufklären, Backups schützen und auf vielschichtige Sicherheitsmechanismen setzen.

***Dr. Dieter Kehl***

**Inwieweit betrachten Sie die Ransomware als zukünftige Bedrohung für die IT-Sicherheit Ihres Unternehmens?**

59 %
Sehr bedrohlich

33 %
eher bedrohlich

5 %
eher nicht bedrohlich

(Quelle: Bitkom Research 2022)

# Wie vermeidet man MFA-Fatigue Angriffe?

## WAS STECKT HINTER DIESEM BEGRIFF, WELCHE VARIANTEN TRETEN DERZEIT AUF UND WELCHE ABWEHRMASSNAHMEN HELFEN?

Cyberkriminelle nutzen eine neue Taktik, um auch Multifaktor-Authentifizierung (MFA) zu knacken. Sie fordern hartnäckig die nötige Authentifizierung, bis das Opfer aus purer „Ermüdung" irgendwann bestätigt. Unser Rat: Sensibilisieren Sie Ihre Mitarbeiter für die Gefahren!

Fast täglich sind dabei neue Varianten zu beobachten. Derzeit gibt es vor allem verstärkt MFA-Fatigue-Angriffe, wie die Hackerattacke auf den Fahrdienstleister Uber zeigt, um nur einen prominenten Namen zu nennen. Die CyberArk Labs haben fünf gängige Phishing-Attacken der jüngsten Vergangenheit identifiziert. Darauf aufbauend gibt das Unternehmen Tipps zur Verringerung der Cyberrisiken.

**#1 SMS- und Voice-Phishing**

Diese MFA-Fatigue-Attacken werden genutzt, um sich als vertrauenswürdige Quellen auszugeben – dabei „ermüden" Angreifer die Nutzer mit zahlreichen MFA-Pushes bis sie Zugang zu den Zielsystemen erhalten.

Angreifer finden immer wieder neue Wege, um MFA-Anwendungen und Sicherheitskontrollen zu umgehen. Die Nutzung von Phishing-resistenten MFA-Faktoren wie FIDO, QR-Codes oder physischen Token kann dabei helfen, diese Bemühungen zu vereiteln.

Eine wirkungsvolle Abwehrmethode gegen MFA-Fatigue-Attacken ist auch die Änderung der MFA-Konfiguration. So können zum Beispiel Push-Benachrichtigungen durch One-Time Passwords (OTPs) ersetzt werden. Die OTP-Nutzung ist zwar weniger komfortabel, kann aber das MFA-Fatigue-Risiko minimieren.

Ein benutzerfreundlicherer Ansatz besteht darin, für eine erfolgreiche MFA-Authentifizierung einen Nummernabgleich zu verlangen. Dabei wird Nutzern, die auf MFA-Push-Benachrichtigungen mit der Authenticator-App antworten, eine Zahlenfolge angezeigt. Diese muss in die App eingeben werden, um den Prozess abzuschließen.

**#2 Social-Engineering-Angriffe**

Eine wirksame Methode zum Schutz vor Social Engineering sind Security-Awareness-Trainings für die Mitarbeiter. Routinemäßig sollten Schulungen durchgeführt werden, um das sicherheitsbewusste Verhalten in der Unternehmenskultur zu verankern und die Mitarbeiter über die Entwicklung von Social-Engineering- und Phishing-Angriffstechniken zu informieren. Aber auch technische Schutzmaßnahmen müssen getroffen werden. Dazu zählt etwa die Nutzung von Spam-Filtern, die verhindern, dass verdächtige E-Mails oder unerwünschte Anhänge wie Gewinnspiele oder infizierte Bewerbungen in die Posteingänge der Mitarbeiter gelangen.

**#3 Identitätskompromittierung**

Der Diebstahl von Zugangsdaten ist eine weitere beliebte Phishing-Methode, bestes Beispiel dafür sind Man-in-the-Middle-Angriffe.

Awareness-Kampagnen können nicht immer verhindern, dass ein Benutzer Opfer von Phishing wird. Folglich muss eine Verteidigungsstrategie auch ein Endpoint Privilege Management beinhalten, das die clientseitigen Credentials schützt und den Diebstahl von Cookies verhindert, der ein MFA-Bypassing ermöglichen kann.

**#4 System- und Serverkompromittierung**

Mit Seitwärtsbewegungen können Angreifer tiefer in kompromittierte Umge-

bungen eindringen und Zugriffsrechte ausweiten – bis hin zu Domain Controllern.

Eine Abwehrmaßnahme ist die Durchsetzung des Least-Privilege-Prinzips in der gesamten Infrastruktur, auch im Hinblick auf Anwendungen und Daten. Hier kommen intelligente Berechtigungskontrollen ins Spiel, die den Zugriff für alle Identitäten verwalten, sichern und überwachen.

**#5 Datenexfiltration**

Bei einem der jüngsten Phishing-Vorfälle versuchten Angreifer, wieder in das Netzwerk einzudringen, nachdem sie Daten gestohlen hatten, aber anschließend entdeckt worden waren. Dabei zielten sie auf Mitarbeiter ab, die nach dem obligatorischen Zurücksetzen der Anmeldedaten möglicherweise nur einzelne Zeichen an ihren Passwörtern geändert hatten. Die

EIN WIRKSAMER ANTI-PHISHING-SCHUTZ MUSS EINERSEITS TECHNISCHE LÖSUNGEN UMFASSEN UND ANDERERSEITS AUCH DIE MENSCHLICHE KOMPONENTE BERÜCKSICHTIGEN.

**Michael Kleist, Area Vice President DACH, CyberArk, www.cyberark.de**

Angreifer waren in diesem Fall nicht erfolgreich, aber er zeigt, wie wichtig sichere Passwortverfahren sind. Idealerweise wird dabei eine Lösung genutzt, die automatisch eindeutige und sichere Passwörter generiert und regelmäßig rotiert.

**Fazit**

Phishing hat eine neue Stufe der Innovation erreicht. Die jüngsten Ereignisse zeigen, wie weit Angreifer gehen, um ihre ahnungslosen Opfer zu täuschen. Betroffen sind auch solche Mitarbeiter, die denken, dass sie dank MFA gefahrlos agieren. Ein wirksamer Anti-Phishing-Schutz muss deshalb einerseits technische Lösungen umfassen und andererseits auch die menschliche Komponente berücksichtigen. Schließlich ist davon ausgehen, dass unerwünschte Klicks letztlich immer unvermeidlich sind. Folglich sollten auch Bedrohungen prinzipiell frühzeitig erkannt werden, bevor ein größerer Schaden entsteht. Außerdem muss die Security mehrstufig aufgebaut sein, um im Falle des Falles den Angreifer in der nächsten Verteidigungslinie abfangen zu können.

***Michael Kleist***

# Passwörter

## ZWEI-FAKTOR-AUTHENTIFIZIERUNG NIMMT ZU

In einer von KnowBe4 im Januar 2023 durchgeführten Umfrage wurden 106 Personen zum Thema „Passwörter vs. Passwordless" befragt. Die Mehrheit der Befragten (61 Prozent) verwendet beim Online-Banking eine Zwei-Faktor-Authentifizierung und 46 Prozent beim Online-Shopping. Die Befragten scheinen großes Vertrauen in diese Methode der Authentifizierung zu setzen, denn deutlich mehr als die Hälfte hält sie für sicher und nur rund ein Viertel hat Bedenken wegen der Sicherheit. Es ist interessant zu beobachten, dass etwa ein Drittel (34 Prozent) ein jeweils leicht modifiziertes Passwort für verschiedene Konten nutzt und ebenso fast ein Drittel (32 Prozent) für jedes Konto ein komplett anderes Passwort verwendet.

**Was macht die Sicherheit von Passwörtern aus?**

Die steigende Bedeutung der Zwei-Faktor-Authentifizierung zeigt sich auch darin, dass es viele Bedenken in Bezug auf die grundsätzliche Sicherheit von klassischen Passwörtern, egal wie komplex sie sind, gibt. So halten nur 30 Prozent komplexe Passwörter für sehr sicher, während fast ein Viertel (24 Prozent) nicht weiß, wie sie die Lage einschätzen sollen. Und fast ein Drittel der Befragten (29 Prozent) halten selbst komplexe Passwörter für eher unsicher.

Nutzer sollten einige Grundregeln verinnerlichen:

1. Komplexere Passwörter sind besser als kurze – Passphrasen sind eine geeignete Methode zur Steigerung der Komplexität.

2. Multifaktorauthentifizierung verfügt über bessere Sicherheit als einfache Authentifizierung.

3. Im Schnitt schützen Nutzer ihre Accounts durch die Verwendung von Passwortmanagern mehr, als dass sie sie verwundbar machen.

***www.knowbe4.de***

# Anomalieerkennung

## KI-BASIERTE ANGRIFFSERKENNUNG: MÖGLICHKEITEN UND GRENZEN

Anomalieerkennung gilt als eine Methode der Angriffserkennung für die IT- und OT-Sicherheit. Cyberkriminelle versuchen jedoch häufig, unter dem Radar solcher Systeme zu operieren. Was kann KI in diesem Zusammenhang leisten?

Strom, Wasser, Lebensmittel oder Gesundheitsversorgung: Selbst kritische Infrastrukturen sind heute Bestandteil digitaler Ökosysteme. Mit zunehmender Digitalisierung und Vernetzung wächst deren Komplexität und damit die Verwundbarkeit gegenüber Cyberangriffen. Gleichzeitig steigt unsere Abhängigkeit von der Verfügbarkeit, Integrität und Vertraulichkeit solcher Systemlandschaften. Eine hohe Cyberresilienz wird damit zunehmend zur Grundlage einer stabilen Gesellschaft. Wichtiger Bestandteil dieser Widerstandsfähigkeit ist das Erkennen und die Abwehr von Angriffen. Dem trägt auch der Gesetzgeber immer mehr Rechnung und verpflichtet Betreiber von KRITIS-Anlagen mit dem IT-SIG 2.0 ab dem 1. Mai 2023 zum Einsatz von Systemen für die Angriffserkennung.

**Angriffserkennung vs. Anomalieerkennung**

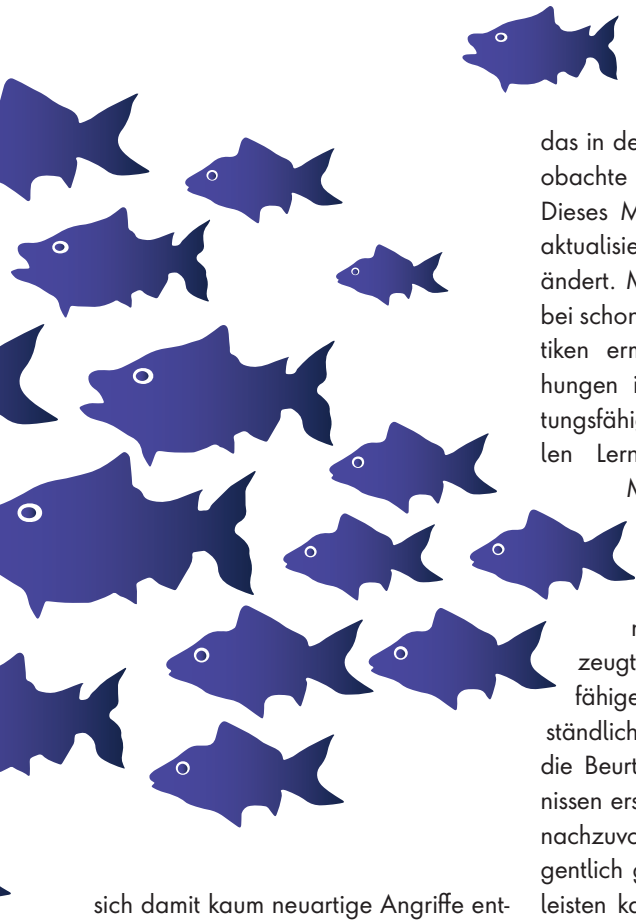
Im Zusammenhang mit der Angriffserkennung wird oftmals der Begriff der Anomalieerkennung als Synonym verwendet. Allerdings ist eine Anomalie nur eine Abweichung von dem normal Erwarteten. Dabei kann es sich um eine Störung handeln, der kein Angriff zugrunde liegt, sondern zum Beispiel eine Fehlfunktion oder der Ausfall einer Komponente. Zwar ist es unter dem Aspekt einer hohen Verfügbarkeit und Integrität wichtig, derartige betriebliche Probleme frühzeitig zu erkennen und zu behandeln, sie sind aber nicht Bestandteil der Abwehr von Cyberangriffen.

Im Gegensatz zu solch sporadisch auftretenden Fehlfunktionen mit klarem Fehlerbild versuchen Angreifer gezielt, ihre Cyberattacken unter dem Radar klassischer Anomalieerkennung durchzuführen. Eine generische Anomalieerkennung ist damit als primäres Mittel einer Angriffserkennung eher ungeeignet. Stattdessen sind Systeme erforderlich, die explizit auf die Erkennung von Angriffen ausgelegt wurden.

**Regelbasiert vs. KI-basiert**

Ein klassischer Ansatz bei Angriffserkennungssystemen ist die Nutzung manuell bzw. semi-automatisch erstellter kuratierter Regeln auf Basis von Expertenwissen und Datenanalysen. Dazu gehören die in Intrusion-Detection-Systemen genutzten Signaturen bekannter Angriffspakete. Aber auch Schwellwerte für Paketgrößen oder Paketmengen, deren Überschreiten einen Angriff nahelegt, oder komplexere Heuristiken zur Erkennung von Aufklärungstechniken wie Portscanning, können mit geeigneten Regelwerken abgebildet werden.

Derartige Regeln sind im Allgemeinen auf klare Angriffsmuster fokussiert. Ihre Bedeutung ist dadurch selbst für Nicht-Experten zu verstehen und auf ein durch die Regel gemeldetes Ereignis kann entsprechend zügig und fokussiert reagiert werden. Allerdings haben diese aufwändig kuratierten Systeme Probleme mit den zunehmend komplexen Daten umzugehen und müssen bei Änderungen der Umgebungen erneut manuell angepasst werden. Auch lassen



sich damit kaum neuartige Angriffe entdecken, für deren Verhalten noch keine spezifischen Regeln erstellt wurden.

Bei KI-basierten Systemen wird hingegen aus einer längeren Beobachtung des Datenverkehrs automatisiert ein Modell der Umgebung generiert, welches das in der betrachteten Umgebung beobachte Normalverhalten beschreibt. Dieses Modell lässt sich automatisiert aktualisieren, wenn sich die Umgebung ändert. Manche Hersteller betiteln dabei schon mit Hilfe von einfachen Statistiken ermittelte Kommunikationsbeziehungen im Netz als KI-Modell. Leistungsfähigere Verfahren des maschinellen Lernens erlauben jedoch eine Modellierung deutlich komplexerer Zusammenhänge.

Allerdings werden bei zunehmender Komplexität die erzeugten Modelle nicht nur leistungsfähiger, sondern auch schwerer verständlich für den Menschen, wodurch die Beurteilung von gemeldeten Ereignissen erschwert wird. Es ist auch kaum nachzuvollziehen, was das Modell eigentlich gelernt hat, das heißt, was es leisten kann und wo es Probleme hat. Diese Nachteile sind besonders in hochkomplexen, dynamischen Umgebungen spürbar, in denen auch regelbasierte Systeme schwächeln.

Die Integration von mehr fachlicher Expertise über das Problemfeld kann Abhilfe schaffen. Über die Einbeziehung von fach- und umgebungsspezifisch kuratierten Regeln, das heißt Signaturen, Schwellwerten und Heuristiken als Teil der von einem KI-Modell berücksichtigten Merkmale, ist es möglich, die erzeugten Modelle sowohl verständlicher zu machen, als auch sie zielgerichteter auf eine Angriffserkennung statt nur generische Anomalien auszurichten.

**Grenzen der netzbasierten Erkennung**

Mit der zunehmenden Verschlüsselung von Daten sinkt die Menge an zuverlässigen Informationen, welche einer Angriffserkennung im Netz zur Verfügung stehen. Zwar kann man Meta-Informationen wie Zeitverhalten und Paketgrößen der Kommunikation einbeziehen oder auch Details aus dem Verbindungsaufbau kryptographischer Sessions. Aber diese sind deutlich weniger aussagekräftig als die eigentlichen übertragenen Inhalte und lassen sich von Angreifern auch leichter simulieren, um die Erkennung zu umgehen.

Viele netzbasierte Angriffserkennungen arbeiten nur auf der Ebene einzelner

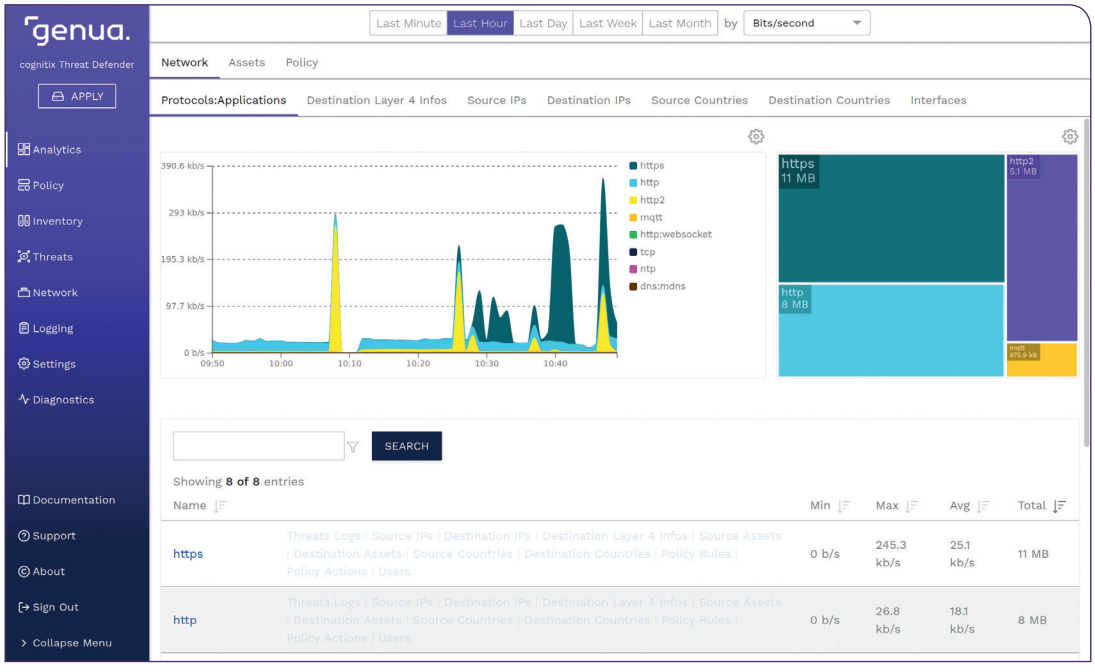
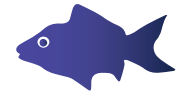



**Bild 1:**
**KI-basierte Systeme zur Anomalieerkennung generieren aus dem Datenverkehr automatisiert ein Modell zur Beschreibung des Normalverhaltens. Zusätzlich fach- und umgebungsspezifisch kuratierte Regeln erhöhen die Verständlichkeit der Modelle und erlauben eine zielgerichtete Angriffserkennung.**



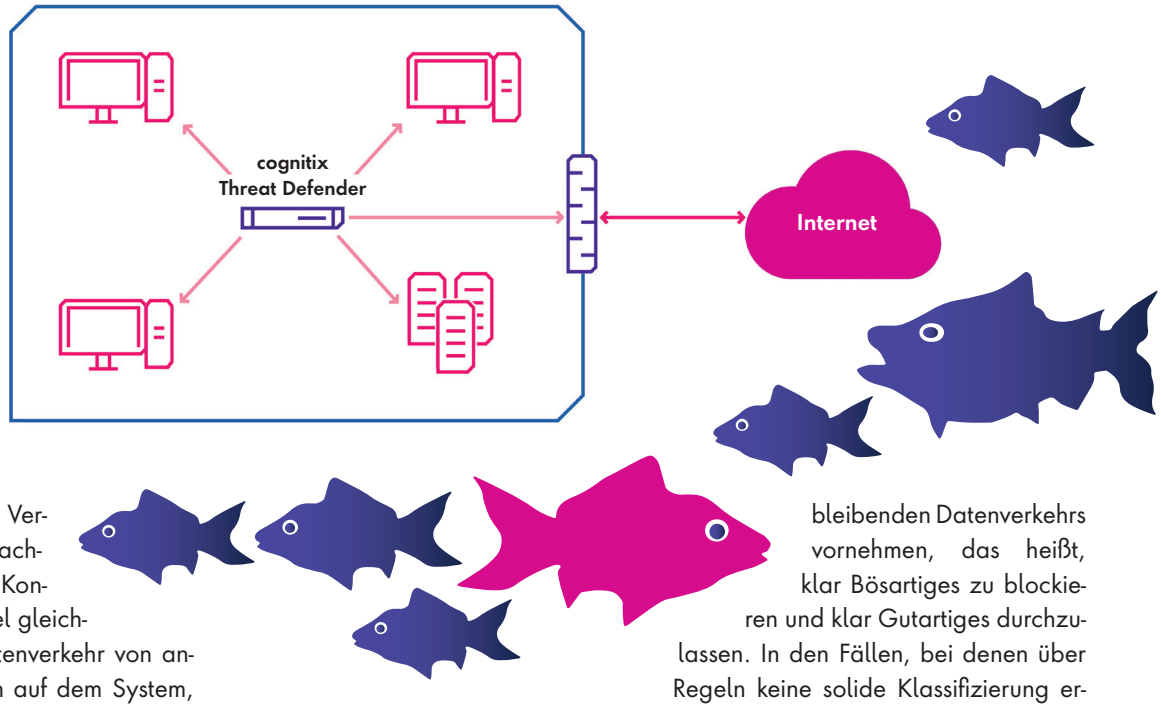
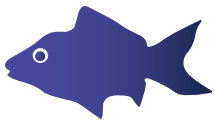



**Bild 2:**
**Trotz Angriffserkennungssystemen sollte der Fokus in der IT-Sicherheit auf einer proaktiven Absicherung der Systeme im Netz liegen, zum Beispiel mittels einer Zero-Trust-basierten Mikrosegmentierung.**

Datenpakete oder Verbindungen. Sie betrachten keinen größeren Kontext, wie zum Beispiel gleichzeitig laufenden Datenverkehr von anderen Anwendungen auf dem System, vorhergehende und nachfolgende Kommunikation oder Steuerkommunikation wie DNS-Anfragen. Sie haben auch keine Informationen über den Anwendungskontext innerhalb der einzelnen Applikationen und Systeme. Sie können nur spekulieren, welche Auswirkungen die übertragenen Daten auf das Zielsystem haben werden. Eine netz-, system- und anwendungsübergreifende Aggregation und Korrelation dieser Information in Analyse-Systemen kann zwar tiefere Einblicke geben, führt allerdings wiederum zu steigender Komplexität. KI-basierte Analysen können auch hier wieder helfen, die Komplexität handhabbar zu machen.

**Optimale Einsatzumgebung**

Angriffserkennungssysteme, egal ob regelbasiert, KI oder hybrid, werden mit zunehmender Komplexität der zu analysierenden Kommunikation immer weniger hilfreich. Der Fokus sollte daher auf einer proaktiven Absicherung der Systeme im Netz liegen, also einer Beschränkung der Kommunikationsmöglichkeiten im Netz auf das erforderliche Minimum, zum Beispiel mittels einer Zero-Trust-basierten Mikrosegmentierung. Dieses Vorgehen senkt sowohl die Angriffsfläche für eine initiale Infektion als auch die Möglichkeiten für eine nachfolgende laterale Ausbreitung des Angreifers und reduziert damit das Schadenspotential.



Aufbauend darauf sollten klar verständliche kuratierte Regeln, idealerweise kontextübergreifend über Pakete, Verbindungen, Anwendungen und Systeme hinweg, eine Klassifikation des verbleibenden Datenverkehrs vornehmen, das heißt, klar Bösartiges zu blockieren und klar Gutartiges durchzulassen. In den Fällen, bei denen über Regeln keine solide Klassifizierung erfolgen kann, können dann KI-Modelle herangezogen werden. Auf diese Weise spielen proaktive Sicherheit, einfache aber verständliche Regeln und komplexe aber leistungsfähigere KI-Modelle ihre jeweiligen Stärken optimal aus.

KI-BASIERTE ANGRIFFSERKENNUNGSSYSTEME IN NETZEN KÖNNEN HILFREICH SEIN. SIE SIND ABER KEIN MAGISCHER ZAUBERSTAB, DER DIE PROBLEME ALLEINE LÖST.

**Steffen Ullrich, IT-Sicherheitsexperte, genua GmbH, www.genua.de**

**Fazit**

KI-basierte Angriffserkennungssysteme in Netzen können hilfreich sein. Sie sind aber kein magischer Zauberstab, der die Probleme alleine löst. Sie sollten kombiniert werden, und zwar mit einer proaktiven Absicherung des Netzes zur Minimierung von Angriffsflächen, lateraler Ausbreitung und Schadenspotential sowie einer regelbasierten Angriffserkennung zur Behandlung offensichtlicher Fälle und der Eliminierung von False Positives der nachfolgenden KI. Beim Design der Merkmale für die KI sollte fachspezifische Expertise über das konkrete Netz und die verwendeten Kommunikationsmuster und -protokolle und die erwarteten Angriffsmuster einfließen – was im OT-Umfeld oft anders aussieht als in der IT. Nur wenn sie möglichst gut an die Arbeitsumgebung angepasst und nicht von Komplexität überfordert ist, kann Angriffserkennung ihr Potential optimal ausspielen.

***Steffen Ullrich***

# File-basierte Bedrohungen mit CDR abwehren

## SICHERE NEUVERPACKUNG VON DATEI-INHALTEN

RANSOMWARE UND ANDERE SCHADPROGRAMME ZÄHLEN NACH WIE VOR ZU DEN GRÖSSTEN SICHERHEITSBEDROHUNGEN FÜR UNTERNEHMEN.

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

Cyberkriminelle nutzen gern manipulierte PDF- und Office-Dokumente, um Malware bei Unternehmen einzuschleusen. Content Disarm and Reconstruction (CDR) lässt solche Bedrohungen ins Leere laufen, indem es die Dateien auseinandernimmt und neu aufbaut. Dabei bleiben alle gefährlichen Bestandteile auf der Strecke – auch unbekannte.

Ransomware und andere Schadprogramme zählen nach wie vor zu den größten Sicherheitsbedrohungen für Unternehmen. Häufig stecken sie in manipulierten PDF-Dateien und Office-Dokumenten, die Mitarbeiter via E-Mail erhalten oder aus dem Internet herunterladen. Vielschichtige Abwehrtechnologien sollen zwar verhindern, dass die verseuchten Files ins Unternehmen gelangen, doch das gelingt nicht immer. Schließlich tarnt sich Malware heute äußerst geschickt – etwa indem sie ihren Code verändert, um signaturbasierte Lösungen zu umgehen, oder ihre Schadfunktionen erst verzögert startet, um Sandboxes und andere verhaltensbasierte Lösungen auszutricksen.

Regelmäßig mahnen IT-Abteilungen daher die Belegschaft, Dateien unbekannter Herkunft keinesfalls zu öffnen. Einen richtigen Schutz bietet das indes nicht, denn im hektischen Tagesgeschäft ist ein verdächtiger Mail-Anhang schnell angeklickt. Zumal die Mails, mit denen die Malware verbreitet wird, heute oft so gut gefälscht sind, dass es selbst IT-Profis schwerfällt, sie als Fälschung zu erkennen. Außerdem kann sich Malware durchaus auch in Dateien bekannter Herkunft verstecken.

Unternehmen brauchen deshalb zusätzliche Schutzmechanismen, um dateibasierte Bedrohungen zuverlässig abzuwehren. Eine Möglichkeit wäre, die verschiedenen Dateiformate zum Beispiel in harmlose Bilder umzuwandeln. Im Arbeitsalltag ist so etwas natürlich unpraktisch, denn obwohl alle Informationen weiter vorhanden sind, lassen sie sich weder komfortabel lesen noch durchsuchen oder gar bearbeiten. Die Idee an sich ist jedoch gut und findet sich in ähnlicher Form in einer Technologie wieder, die schon seit

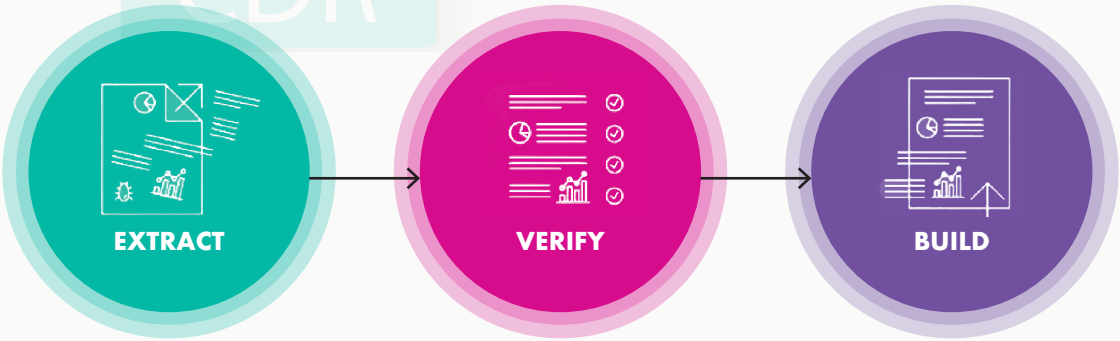



**Bild 1: Sichere Dateien in drei Schritten: CDR liest die eigentlichen Geschäftsinformationen aus, prüft sie auf eine gültige Struktur und erstellt daraus neue, garantiert malware-freie Dateien** (Quelle: Forcepoint)


**Bild 2:**
**Die Umwandlung von Dateien in Bilder oder PDFs kann gefährliche Inhalte entschärfen, erschwert aber die Arbeit mit den enthaltenen Daten – besser ist der Aufbau einer neuen Datei im ursprünglichen Format**

(Quelle: Forcepoint)

einigen Jahren existiert, hierzulande aber noch unter dem Radar fliegt: Content Disarm and Reconstruction, kurz CDR.

**So funktioniert CDR**

CDR extrahiert die unbedenklichen Daten aus einer Datei, also die für den Anwender nutzbaren Informationen sowie die Dateistruktur. Diese werden geprüft und anschließend zu einer neuen, voll funktionsfähigen Datei zusammengesetzt. Code, aktive Inhalte, versteckte Elemente und alle Bestandteile, die im entsprechenden Dateistandard nicht vorgesehen sind, bleiben dabei auf der Strecke – sie stellen keine Gefahr mehr dar und werden mit der Originaldatei gelöscht oder sicher aufbewahrt.

Durch diese Arbeitsweise hat CDR keine Schwierigkeiten mit unbekannten Bedrohungen und liefert stets absolut saubere und unbedenkliche Dateien – und das, ohne auf Signaturen oder andere Mechanismen zur Malware-Erkennung angewiesen zu sein. Demzufolge kommt die Technologie auch ohne regelmäßige Updates aus und produziert keine False Positives, deren Überprüfung bei anderen Security-Lösungen oft einen hohen Aufwand verursacht.

Der gesamte Prozess des Auseinandernehmens und Zusammenbauens dauert nur den Bruchteil einer Sekunde und bremst Arbeitsabläufe nicht aus – im Gegensatz beispielsweise zu Sandboxes, die häufig einige Minuten abwarten, bevor sie eine Datei als unbedenklich freigeben. Unternehmen können mit CDR also ihre sicherheitsrelevanten Prozesse beschleunigen und Sandbox-Umgebungen, die Ressourcen binden und Kosten verursachen, entlasten. Nur noch Dateien, die CDR nicht transformieren konnten, werden künftig zur Analyse an die Sandbox überstellt.

Manche CDR-Lösungen wandeln die verschiedenen Ausgangsformate, zu denen neben PDFs und Office-Dokumenten in der Regel auch Bilder, HTML-Dateien, Mail-Formate und Archive zählen, lediglich in PDFs um. Das erschwert es jedoch, Daten zu aktualisieren oder zu ergänzen. Besser sind daher Lösungen, bei denen das Endformat dem Ausgangsformat entspricht. Wobei es hier sogar Möglichkeiten gibt, das Format zu aktualisieren und einen Wildwuchs mit unzähligen alten Word-, Excel- und PowerPoint-Formaten einzudämmen. Die neu aufgebauten Dateien gleichen optisch dem Original, sodass es keinerlei Einschränkungen bei der User Experience gibt.

**CDR ergänzt andere Sicherheitslösungen**

Standardmäßig gehen bei der Transformation von Office-Dokumenten durch CDR alle Makros, die sich in den Ursprungsdateien befinden, verloren. Da einige Unternehmen allerdings Makros benötigten, sollten CDR-Lösungen flexible Optionen bieten, um bestimmte Dateien oder Kommunikationskanäle von der Neuverpackung der Inhalte auszunehmen. Hier kommen weiterhin die bestehenden Security-Tools zum Zuge, die CDR nicht ablösen will, sondern lediglich ergänzt. Idealerweise greifen alle Lösungen dabei auf einen zentralen Satz an Richtlinien zu, damit IT-Abteilungen nicht mehrere Sätze parallel pflegen müssen, was aufwendig ist und unweigerlich zu inkonsistenten Regeln führt.

Ähnlich wie der Umgang mit Makros lässt sich dann auch der Umgang mit

signierten und verschlüsselten Dateien richtliniengesteuert anpassen. Denn CDR kann zwar signierte Dokumente neu aufbauen und dadurch von möglichen Schadfunktionen bereinigen, doch der Neuaufbau bricht die Signatur. In der Praxis hat es sich bewährt, das bei Dokumenten aus unbekannten Quellen tatsächlich zu tun – aus Sicherheitsgründen. Auf die entfernte Signatur wird der Anwender hingewiesen. Bei klar definierten Prozessen jedoch, die auf signierten Dokumenten basieren, hält sich CDR hingegen zurück und überlässt anderen Security-Tools das Feld.


Schwieriger ist es bei verschlüsselten Dateien, die CDR nicht einzusehen vermag. Hier könnten IT-Abteilungen etwa die Zustellung via Mail bei vertrauenswürdigen Absendern gestatten – in allen anderen Fällen würde der verschlüsselte Dateianhang entfernt und ein Hinweis den Empfänger darüber informieren. Handelt es sich um verschlüsselte E-Mails, sollte sich die CDR-Lösung als Mail Transfer Agent beim Verschlüsselungsgateway einklinken können, um die dort entschlüsselten Nachrichten neu aufzubauen, bevor sie erneut verschlüsselt und final zugestellt werden.

Überhaupt sollten CDR-Lösungen sehr integrationsfreudig sein. Einerseits um die Arbeitsaufteilung mit anderen Security-Tools wie Firewall oder Sandbox abzustimmen. Andererseits um Zugriff auf alle Wege zu erhalten, auf denen gefährliche Dateien ins Unternehmen gelangen können. E-Mails und Downloads aus dem Internet sind zweifellos die Klassiker, dennoch kann sich Malware auch über Web-Anwendungen, Datei-Uploads, freigegebene Ordner, File-Sharing und Chat-Kommunikation einschleichen.

***Frank Limberger***


# Hannover Messe 2023

## DER WEG ZUR KLIMANEUTRALEN INDUSTRIE FÜHRT ÜBER HANNOVER

Auf der kommenden HANNOVER MESSE präsentieren die international führenden Unternehmen aus dem Maschinenbau, der Elektro- und Digitalindustrie sowie der Energiewirtschaft ihre Lösungen für eine ressourceneffiziente, klimaneutrale und resiliente Produktion. Unter dem Leitthema „Industrial Transformation – Making the Difference" zeigen sie, welche Veränderungen die Industrie vorantreiben kann, um den $CO_2$-Ausstoß spürbar und im großen Maßstab zu reduzieren.

**Klimawandel, Energieknappheit, unterbrochene Lieferketten**

Das sind nur einige der Herausforderungen, vor denen Gesellschaft und Wirtschaft heute stehen. Herausforderungen, die eines gemeinsam haben: Ihre Bewältigung liegt im konsequenten Einsatz von Hochtechnologie und innovativen industriellen Lösungen. Hightech und Lösungen, die auf der HANNOVER MESSE 2023 gezeigt werden. Denn die Weltleitmesse der Industrie ist die einzige Veranstaltung, auf der das Zusammenspiel der führenden Unternehmen aus dem Maschinenbau, der Elektro- und Digitalindustrie sowie der Energiewirtschaft erlebbar wird. Als industrielles Ökosystem machen sie die notwendigen Veränderungen möglich – Veränderungen in der Art, wie wir produzieren, wirtschaften, zusammenarbeiten.

**Making the Difference**

„Unter dem Leitthema ‚Industrial Transformation – Making the Difference' wird die Messe zeigen, welchen Unterschied die ausstellenden Unternehmen machen können, welche Veränderungen sie vorantreiben und welche Innovationen sie entwickeln – auf dem Weg zu einer klimaneutralen Industrie", sagt Dr. Jochen Köckler, Vorsitzender des Vorstands der Deutschen Messe AG. „Konzerne, Mittelstand, Startups sowie Wissenschaft, Politik und Gesellschaft sind gemeinsam gefordert. Nur im Zusammenschluss kann es gelingen, die industrielle Produktion und damit unseren Wohlstand und unsere Zukunft nachhaltig zu sichern und gleichzeitig den Klimaschutz voranzutreiben."

Rund 4.000 Aussteller aus aller Welt präsentieren hochtechnologische Lösungen für die Produktion und Energieversorgung der Zukunft. Von der Digitalisierung von komplexen Produktionsprozessen über den Einsatz von Wasserstoff zum Betrieb ganzer Produktionsanlagen bis hin zur Anwendung von Software zur Erfassung und Reduzierung des $CO_2$-Fußabdrucks bietet die HANNOVER MESSE ein ganzheitliches Bild der technologischen Möglichkeiten für die Industrie von heute und morgen.

**Industrial Security Circus**

Neu ist in diesem Jahr der Industrial Security Circus. Auf dem Gemeinschaftsstand präsentieren Unternehmen eine völlig neue Mischung aus Technologien, Angeboten, Produkten und Dienstleistungen. Dazu zählen unter anderem IT-Sicherheitstrainings und erklärendes Entertainment mit innovativen Wegen der Wissensvermittlung im Kontext von IT/OT Security in der industriellen Fertigung. Auf der Messe selber bieten mehr als 350 Unternehmen Produkte und Lösungen zum Thema IT-Sicherheit.

**Making Indonesia 4.0**

Mit Indonesien präsentiert sich die größte Wirtschaftsmacht in der ASEAN Region als Partnerland der HANNOVER MESSE 2023. Das Motto lautet: Making Indonesia 4.0. Bis 2030 möchte Indonesien eine der zehn größten Volkswirtschaften der Welt sein. Der Anteil der Erneuerbaren Energien an der Stromerzeugung soll bis dahin 51,6 Prozent am Gesamtzubau ausmachen. Davon entfällt knapp die Hälfte auf Wasserkraft und etwa ein Viertel auf Photovoltaik. In Hannover präsentiert sich das aufstrebende Land als zuverlässiger Partner für Unternehmen rund um den Globus.

***www.hannovermesse.de***

HANNOVER MESSE

**17. bis 21. April 2023**

Laden Sie sich jetzt Ihr kostenloses eTicket herunter.

***https://bit.ly/3DSwQg9***

# Sichere optische Datenkommunikation

## QUANTENKRYPTOGRAPHIE UND LI-FI HELFEN DABEI

Die moderne Quantentechnologie eröffnet viele neue Anwendungsgebiete. Aber sie birgt auch Risiken. So könnten Quantencomputer dank ihrer enormen Rechenleistung selbst modernste Daten-Verschlüsselungsverfahren aushebeln. Um diesem Szenario zuvorzukommen, entwickeln mehrere Partner unter Führung der KEEQuant GmbH einen neuen Ansatz zur sicheren optischen Datenübertragung in drahtlosen Netzwerken mit Hilfe von Licht und Quantenschlüsseln. Das Projekt „QuINSiDa" wird vom Bundesministerium für Bildung und Forschung BMBF mit einer Summe von zwei Millionen Euro gefördert.

Mit der Quantentechnologie stehen in vielen technischen Bereichen die nächsten großen Sprunginnovationen bevor. Neben Quantencomputern, Quantenbildgebung und Quantenuhren steht vor allem die Quantenkommunikation und die Quantenverschlüsselung für eine sichere und private Datenkommunikation im Fokus der Entwicklungen. Dabei sollen klassische Verschlüsselungsansätze, die auf rechnerischer Komplexität beruhen, durch neuartige Quantenschlüsselverteilungs-Ansätze in Kombination mit Post-Quanten-Kryptographie ersetzt werden. Diese Art von Kodierung kann selbst mit beliebig viel Zeit und Rechenleistung nicht geknackt werden. Da die existierende Kryptographie bereits in naher Zukunft durch die immer größeren Rechenpower von Quantencomputer bedroht ist, müssen Lösungsansätze rechtzeitig entwickelt werden, um einer unsicheren Übergangszeit vorzubeugen.

Die bisherige Forschung konzentrierte sich auf eine sichere Datenkommunikation über weite Strecken für Anwendungen in der globalen Dateninfrastruktur, zur Vernetzung von behördlichen oder militärischen Einrichtungen oder zum Informationsaustausch mit Satelliten. Die Verbindungen zum Endnutzer auf dem letzten Kilometer werden bislang jedoch noch immer mit den klassischen Technologien bedient und sind damit weiterhin angreifbar. Um dies zukünftig zu verhindern, wurde das Projekt „QuINSiDa – Quantenbasierte Infrastruktur Netze für Sicherheitskritische drahtlose Datenkommunikation" ins Leben gerufen.

### Verknüpfung von Technologien

Mit der Li-Fi-Technologie können sich Nutzer über kurze Distanzen mittels optischer Signale miteinander vernetzen. Im Vergleich zur bekannten Wi-Fi-Technologie, die auf Funkwellen basiert, durchdringen die optischen Signale keine Wände und können so auf einen definierten Bereich ausgelegt werden. Damit erlaubt die Li-Fi-Technologie die volle

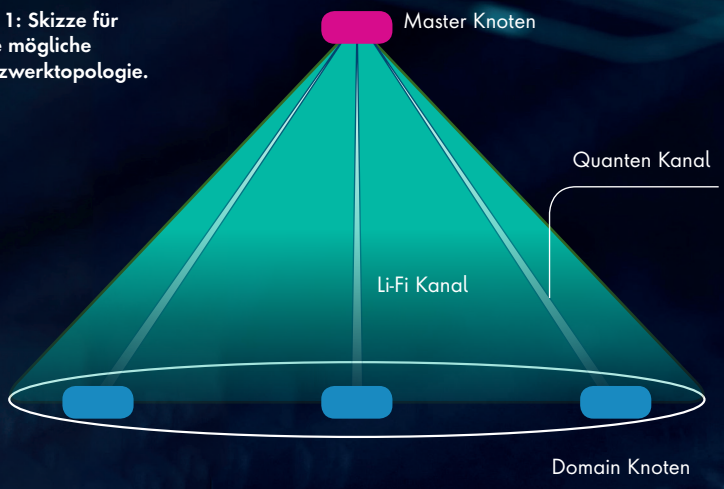



**Bild 1: Skizze für eine mögliche Netzwerktopologie.**

Ausnutzung der verfügbaren spektralen Datenbandbreite in diesem Bereich ohne Störungen von außen.

Unabhängig davon wird die neuartige Technologie der Quantenkryptographie weltweit vorangetrieben. Im Speziellen geht es hier um die Quantenschlüsselverteilung (engl.: quantum key distribution, QKD), welche es ermöglicht, einen kryptographischen Schlüssel zu verteilen, dessen Sicherheit informationstheoretisch bewiesen werden kann. Dies steht in Kontrast zu bestehenden kryptographischen Verfahren, deren Sicherheit auf rechnerischer Komplexität beruht und durch aufkommende Quantencomputer gefährdet wird.

Bei der Quantenschlüsselverteilung werden beim Erzeugen der Schlüssel Quantenzustände in Form von Licht präpariert und zwischen den Teilnehmern im Netzwerk ausgetauscht. Beim Empfang der Quantenzustände werden diese gemessen und nachbearbeitet, so dass auf beiden Seiten identische, aber gegenüber einem Angreifer geheime Schlüssel entstehen.

Das Vorhaben QuINSiDa kombiniert erstmals beide Technologien zu einem „QKD over Li-Fi"-System. Dies ermöglicht es die bisher typischerweise eher im Gebäude-zu-Gebäude-Szenario angedachte QKD auch bis zum Endnutzer zu tragen.

„Intention des Projekts ist die Demonstration eines quantenbasierten Datenkommunikationsnetzwerks, welches drahtlos und flexibel mehrere Endnutzer an eine sichere Backbone-Infrastruktur anschließt oder welches separat als sicheres Campus-Netzwerk eingesetzt werden kann", sagt Dr. Imran Khan Managing Director der KEEQuant GmbH. Dabei soll unter Nutzung eines flexiblen drahtlosen Datenkommunikationsnetzwerks im Punkt zu Multipunkt Szenario eine gleichzeitige Absicherung

**Im Projekt entwickeln die Forschenden Technologien zur drahtlosen Quantenkommunikation zwischen mehreren Geräten innerhalb eines Raumes.**
(Bilder: Fraunhofer IPMS)

der einzelnen Kommunikationskanäle auf Basis von Quantenschlüsseln gewährleistet werden.

## Anwendung der Technologie

Die Nutzung eines optischen Kommunikationsnetzwerkes bietet im Gegensatz zu funkbasierten Ansätzen den Vorteil, dass jeder Teilnehmer, der sich im optisch drahtlosen Kommunikationskanal (Li-Fi Kanal) anmeldet auch für den Quantenkanal sichtbar ist. Damit ist sichergestellt, dass es auch zu einem sicheren Schlüsselaustausch kommen kann. Um den Li-Fi Kanal und den Quantenkanal voneinander zu trennen werden dabei unterschiedliche Wellenlängen des Lichts verwendet. Diese Trennung lässt sich durch den Empfänger mittels einer entsprechenden optischen Filterung gegen Interferenzeinflüsse optimieren.

## Quantenbasiertes Infrastrukturnetz

Das vorgestellte Konzept eines quantenbasierten Infrastrukturnetzes für sicherheitskritische, drahtlose Datenkommunikation ist ein völlig neuer interdisziplinärer Ansatz, der bisher weder in wissenschaftlichen Veröffentlichungen noch in aktuellen Marktlösungen vorgestellt wurde. Der Ansatz soll von den Projektpartnern vor allem im Hinblick auf sicherheitskritische Anwendungen, wie etwa die Ausstattung öffentlicher Versorgungseinrichtungen, wie Banken, Krankenhäuser, Energieversorger, öffentliche Dienste, Telekommunikationsknoten und Regierungseinrichtungen, untersucht werden.

Hierbei wird besonderes Augenmerk auf die Sicherheit des Gesamtsystems bei gleichzeitiger, interdisziplinärer Integration von Netzwerk-Management-Software, klassischer Kryptographie (Stichwort: Post-Quanten-Kryptographie), QKD-Technologie und Li-Fi-Technologie gelegt. Gleichzeitig ist das Projekt vor dem Hintergrund der technologischen Souveränität für den Standort Deutschland von gesellschaftlicher Bedeutung.

Am Ende des Projekts ist eine entsprechende Demonstration des Gesamtsystems geplant, welche die Technologien im Verbund zusammenführen soll und damit bisher unerforschte und unerreichte Anwendungsfälle ermöglich kann. Diese sollen im Anschluss an das Vorhaben durch die beteiligten Firmen verwertet und in die sicherheitskritischen Anwendungen eingebracht werden. Durch den Endnutzerfokus ist eine breite Anwendung und damit ein sehr großes Marktpotenzial und Innovationspotenzial erkennbar. Die in den nächsten Jahren entstehende drastische Kostenreduktion in der QKD durch Produktion in mittleren Stückzahlen wird zudem eine breitere Marktdurchsetzung erlauben.

Weiterhin führt die interdisziplinäre Vernetzung zwischen den verschiedenen Communities (QKD, Optik, Telekommunikation, Sicherheit) zu einer nahtlosen Integration der neuartigen Technologien in bestehende Sicherheitstechnologien. Dies macht es Endnutzern leicht die Technologie in bestehende Infrastruktur zu übernehmen.

***www.forschung-it-sicherheit-kommunikationssysteme.de***

**MEHRWERT**

Weitere Informationen zum Projekt finden Sie unter:
**https://bit.ly/3XtCQCX**

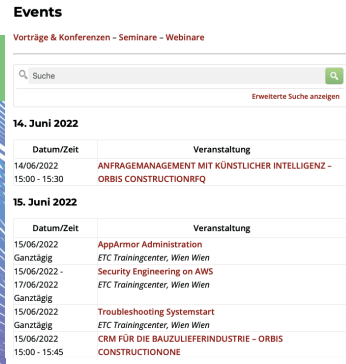
# IT WELT.at is IT

## IT NEWS


Der tägliche Newsletter der ITWELT.at bringt die aktuellen IT Nachrichten aus Österreich und dem Rest der Welt. Wer immer up to date sein will, bestellt den kostenlosen Newsletter itwelt.at/newsletter und ist damit jeden Tag schon am Morgen am neuesten Informationsstand.

itwelt.at

## IT TERMINE




In Österreichs umfangreichster IT-Termindatenbank gibt es Termine für IT-Events wie Messen, Konferenzen, Roadshows, Seminare, Kurse und Vorträge. Über die Suchfunktion kann man Thema und Termin suchen und sich bei Bedarf auch gleich anmelden. Mit Terminkoordination und Erinnerung per E-Mail.

itwelt.at/events

## IT UNTERNEHMEN

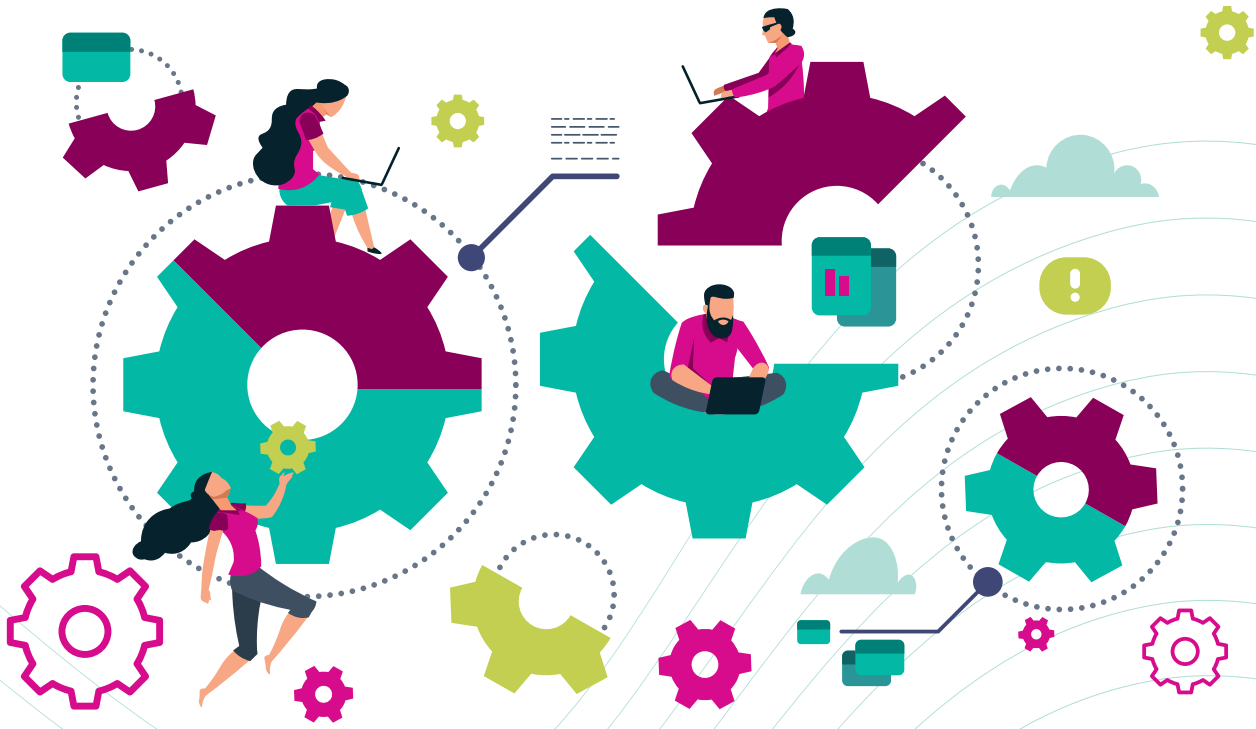

TOP 1001 ist Österreichs größte IT-Firmendatenbank. Mit einer Rangliste der umsatzstärksten IT- und Telekommunikations-Unternehmen. Die Datenbank bietet einen Komplettüberblick der TOP IKT-Firmen und ermöglicht die gezielte Abfrage nach Tätigkeitsschwer-punkten, Produkten und Dienstleistungen.

itwelt.at/top-1001

## IT JOBS


Hier sind laufend aktuelle IT Job-Angebote zu finden. In Zu-sammenarbeit mit der Standard.at/Karriere, dem Jobportal der Tageszeitung Der Standard, findet man auf dieser Plattform perma-nent hunderte offene Stellen aus dem Bereich IT und Telekom. Eine aktive Jobsuche nach Tätigkeits-feld und Ort ist natürlich möglich.

itwelt.at/jobs



# RBAC ist tot – lang lebe PBAC?

## WARUM RBAC NICHT STIRBT UND POLICIES ALLEIN DEN ZUGRIFF NICHT SICHERN KÖNNEN

Als im Jahre 2019 auf der USENIX ATC ein Papier mit dem Namen „Zanzibar: Google's Consistent, Global Authorization System" vorgestellt wurde, nahm man dies außerhalb der Filterblase der IAM-Vordenker und Cloud-Enthusiasten zunächst eher wenig zur Kenntnis. Spannend waren für viele eher aus dem Cloud-IT Operations stammenden Leser vermutlich die Aussagen über die extreme Geschwindigkeit der Zugriffsentscheidungen (unter 10 Millisekunden) und die sehr hohe Verfügbarkeit eben jener ominösen „Access Control List Maschine", gepaart mit der Aussage, dass dies auf Millionen von Autorisierungs-Anfragen pro Sekunde skaliert funktioniert. Jeder Anwender mit einer Freigabe auf ein Dokument in einem Google-Drive eines Kollegen oder mit Zugriff auf das gemeinsame Foto-Share vom Familienurlaub mit den Nachbarn nutzt diese Leistung täglich, und macht sich wenig Gedanken darüber, warum und wieso das nun funktioniert.

Warum soll es also uns im klassischen Identity & Access Management interessieren, dass ein Hyperscaler wie Google intern eine tolle neue Autorisierungs-Engine an den Start gebracht hat? Und wieso behaupten jetzt einige Gurus, dass das Ende der Rollen-basierten Zugriffe gekommen wäre? Hierfür müssen wir ein wenig historische Analyse im Access Management betreiben, die Evolution der Entwicklungsmethoden von Software in Unternehmen von Wasserfall bis agil betrachten um endlich bei den Auswirkungen des Paradigmenwechsels rund um DevOps anzukommen. Ein weit gespannter Bogen, der erstaunliche Schlussfolgerungen zulässt!

**Am Anfang war die Applikation**

In grauer Vorzeit, als weder Novell Netware noch Microsoft Active Directory zugegen waren, mussten die Benutzerkonten und deren Zugriffsrechte im Mainframe oder in den Applikationen

direkt erstellt und verwaltet werden. Damalige Ansätze für das Identity & Access Management begrenzten sich darauf, existierende Benutzer mit Rechten zu finden, die dem Bedarf eines neu eingestellten Mitarbeiters nahe kamen, diesen Benutzer zu kopieren, umzubenennen und diese Änderungen halbwegs automatisch in die angeschlossenen Systeme zu übertragen. Komplex, fehleranfällig und vor allem dazu neigend, viel zu viele Rechte zu vergeben. Gepaart mit der ebenfalls lokalen Entscheidung, was der Benutzer denn nun in der Anwendung tun soll (lokale Access Matrix im System), war an zentrale Kontrolle und Governance kaum zu denken. Ein Audit einer solchen Landschaft setzte tiefe Kenntnisse der Applikationen und ihrer Berechtigungsmodelle voraus; der Aufwand war astronomisch und Audits konnten nur in kleinen Stichproben erfolgen.

**Dann kam der Verzeichnisdienst**

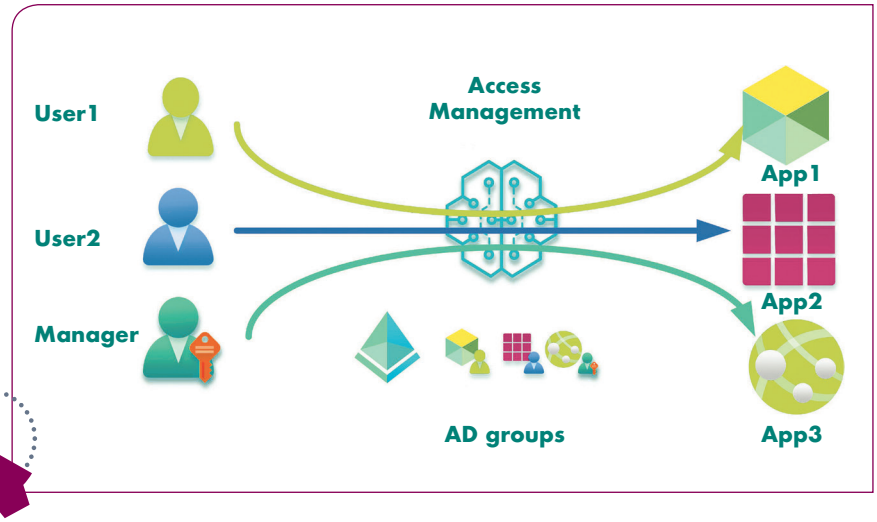
Eine deutliche Verbesserung (aus administrativer Sicht und auch für die Anwender) ergab sich durch die Verbreitung von Verzeichnisdiensten, und der Verbindung von Applikationen mit den Verzeichnisdiensten. In den Applikationen musste nicht mehr unbedingt eine Tabelle der Anwender mit ihren Passworten hinterlegt sein, denn der Vorgang der Identifikation und Authentisierung konnte an den Verzeichnisdienst, etwa das Active Directory, ausgelagert werden. Microsoft hat hierfür das Kerberos Protokoll adaptiert, dass noch heute den Zugriff auf Applikationen durch die Mitgliedschaft in (Sicherheits-)Gruppen steuert, und dem Anwender eine einfache Art des Single Sign-Ons ermöglicht, da er nunmehr seine AD-Anmeldung per Kerberos-Token mit den Anwendungen teilt. In diesen Zeitraum fällt auch die Adaption des in den frühen 1990er Jahren vom US-Verteidigungsministerium entwickelten „Role Based Access Control" (RBAC). Anhand dieses Modells wurde in einer – oftmals hierarchisch ausgelegten – Struktur ein Set an abstrakten Rechte-Bündeln so zugeschnitten, dass den zugeordneten Personen genau der Zugriff auf Applikationen verfügbar wurde, den sie für ihre jeweilige Aufgabe im Unternehmen brauchten. Teilweise konnte dies sogar bis auf die Berechtigungen in Anwendungen verfeinert werden, wie die in SAP oftmals genutzten „Profile" zeigen. Dies wurde oftmals mit Ansätzen des „least privilege" kombiniert und konnte – im Idealfall – sogar zur Abgrenzung toxischer Kombinationen über „segregation of duty" genutzt werden. Eine Vielzahl (gescheiterter) RBAC-Projekte hat jedoch gezeigt, dass eine rein auf Rollen basierende Zuweisung von Rechten in der Praxis nicht funktioniert, da der Abdeckungsgrad der jeweiligen Rollen je Position einen Zielkonflikt zwischen „need to do" und „least privilege" hervorruft. Man will schließlich nicht 1.000 Rollen für 1.000 Mitarbeiter haben – folglich sind Kompromisse mit Einzelberechtigungen, Projektberechtigungen und administrativen Sonderrechten in „just in time" oder „on-demand" Modi erforderlich.

**Rechte: Verwaltung vs. Zugriff oder RBAC vs xBAC**

Spätestens an der Stelle mit „on-demand" wird deutlich, dass man den wenig zeitkritischen Verwaltungsakt der Zuordnung einer (eher statischen) Rolle zum Anwender von dessen versuchten Zugriff zur Laufzeit (dynamisch) unterscheiden muss. Die unabhängige IDpro Organisation hat in ihrem (lesenswerten) Book of Knowledge dazu die Unterscheidung zwischen „Admin Time" (zeit-unkritischer Verwaltungsakt) und „Runtime" (zeitkritischer Zugriff) für die Berechtigungen eines An-

DIE KERNIDEEN RUND UM DYNAMISCHERE VERWALTUNG VON ZUGRIFFSRECHTEN KÖNNEN IN NAHEZU JEDEM AUF DEVOPS AUSGELEGTEN IT-BETRIEB SINNVOLLE ANWENDUNG FINDEN.

**Sebastian Rohr, CSO, umbrella.associates GmbH, www.umbrella.associates/de**



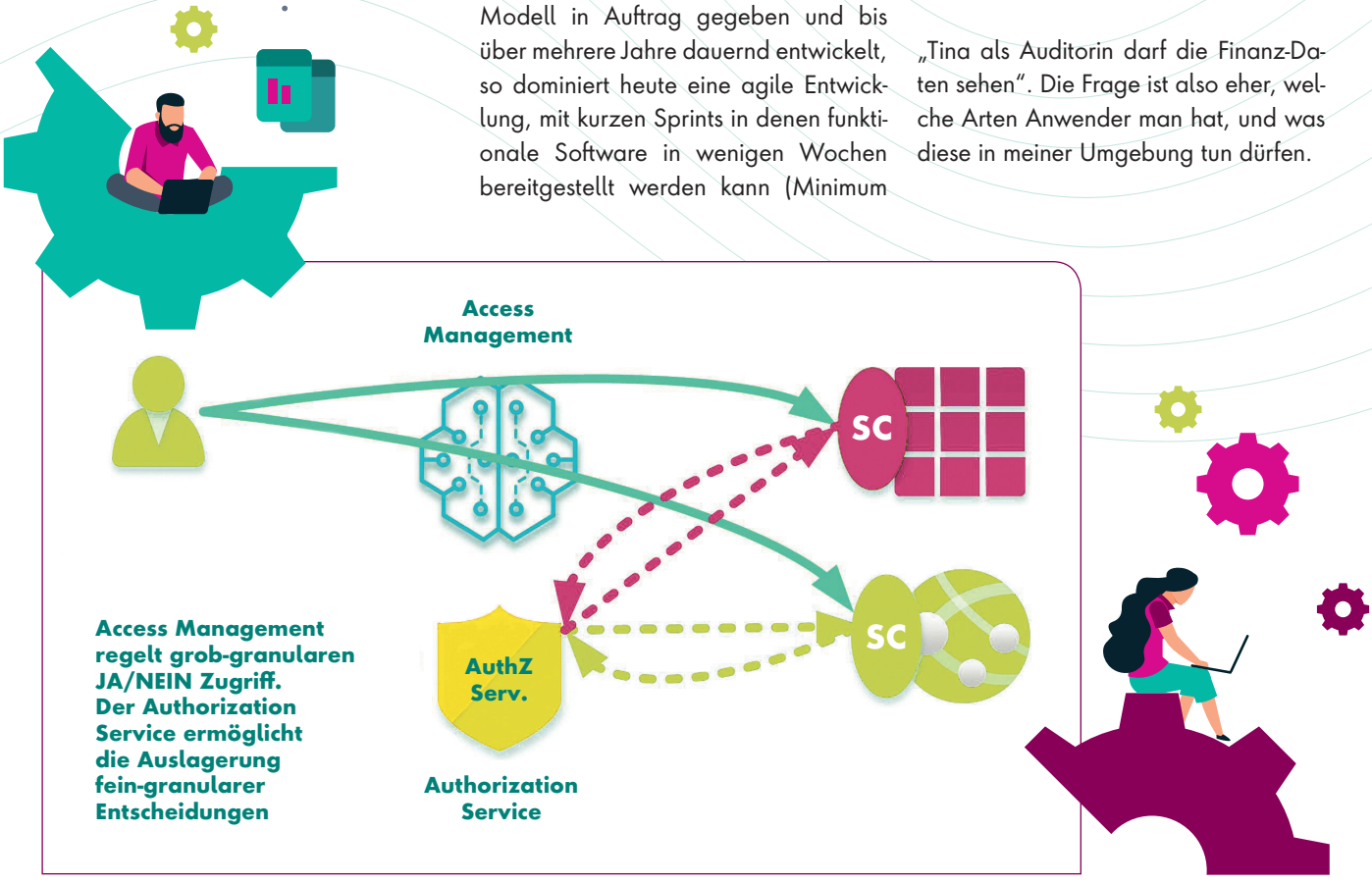
wenders definiert – und hier liegt auch einer der Problempunkte der vielen Berechtigungsmodelle. Während die Rollen eines RBAC Modells im Identity Management eher dem statischen Verwaltungsteil zuzuordnen sind, und etwa die Rollen, ihr Zuschnitt und die Zuordnung zu Personen zyklisch geprüft werden sollten, sind andere Akronyme wie ABAC, CBAC und auch PBAC (Attribute-, Context- und Policy Based Access Control) mehr der Runtime zuzuordnen, denn sie werden verwendet um bei tatsächlichem Zugriff(-sversuch) zu klären, ob das handelnde Subjekt tatsächlich autorisiert ist, auf das betreffende Objekt zuzugreifen. Fast alle Access Management Werkzeuge prüfen dabei die Mitgliedschaft eines Subjektes in einer LDAP-Gruppe oder ob bestimmte definierte Attribute die erforderlichen Werte enthalten (etwa: „ist Mitglied der Gruppe Marketing" oder „Angestelltentyp ist gleich Manager"). Dies wird bei modernen Web- oder SaaS Applikationen nicht mehr über Kerberos abgebildet, sondern verwendet die Security Assertion Markup Language, kurz SAML in der Version 2.0. Diese Mitgliedschaften oder Attribute werden üblicherweise durch das rollenbasiert arbeitende Identity Governance Werkzeug im Vorweg gesetzt – aber diese Zuweisungen sind eher statisch und werden nur bei Positionswechseln (Mover) oder Entlassungen (Leaver) angepasst. Bei Anpassungen an den Zuständigkeiten einer Funktion, etwa durch eine Re-Organisation, muss der Zuschnitt der Rollen angepasst werden – dies wird über eine Rezertifizierung der Rolle selbst, oder des Rollenmodells realisiert, jedoch selten öfters als einmal pro Jahr oder eben „bei Bedarf".

An dieser Stelle kommt die Historie der Softwareentwicklung ins Spiel! Wurden noch bis in die 2000er Jahre größere Software Projekte nach Wasserfalls Modell in Auftrag gegeben und bis über mehrere Jahre dauernd entwickelt, so dominiert heute eine agile Entwicklung, mit kurzen Sprints in denen funktionale Software in wenigen Wochen bereitgestellt werden kann (Minimum Viable Product, MVP). Hatten die IAM Fachleute also nach GoLive einer nach Wasserfall entwickelten Software etliche Jahre Zeit, das darin enthaltene Berechtigungsmodell in ihr eher statisches Rollenmodell zu integrieren, so werden heute nahezu wöchentlich neue Software Produkte mit sich teilweise dramatisch unterscheidenden Funktionsumfängen in Betrieb genommen. Es fällt schwer sich vorzustellen, wie ein auf jährliche Überarbeitung ausgelegtes Rollen-Management diese sich stets im Wandel befindlichen Zielsysteme abdecken können soll – ganz zu schweigen von den Ansätzen eines Continous Integration / Continous Delivery (CI/CD), in dem zu jeder Zeit kleine Änderungen an Microservices direkt in die Produktion übernommen werden.

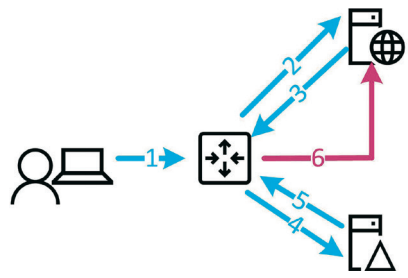
**Wie PBAC bei DevOps helfen kann**

Das RBAC-Modell betrachtet Berechtigungen vornehmlich aus Sicht des Anwenders:

„Tina als Auditorin darf die Finanz-Daten sehen". Die Frage ist also eher, welche Arten Anwender man hat, und was diese in meiner Umgebung tun dürfen.



**Das PBAC-Modell fragt aus Sicht der Ressourcen:**
„Intranet-Einträge können von Entitäten editiert werden, die »Editor« als Attributwert in ihrer Jobbeschreibung haben,…" und diese können auch noch um Bedingungen ergänzt werden: „wenn sie von Firmengeräten aus zugreifen." Hier wird die Frage gestellt, welche Ressourcen ich habe, und durch wen oder wie diese genutzt und verwaltet werden.




1. Non-Kerberos Authentisierung
2. Authentisierungs-Versuch
3. Kerberos-unterstützt!
4. Service Ticket Request
5. Service Ticket ausgestellt
6. Kerberos-Authentisierung

Damit steht der Anwendungsentwickler in viel engerer Beziehung mit den Objekten, die in seiner Applikation zugreifbar und veränderbar angeboten werden. Der Entwickler kann – ganz den Anforderungen der Spezifikation entsprechend – einen Satz an Zugriffspolicies für „seine Objekte" anlegen und stetig anpassen. Kommen neue Objekte hinzu, werden neue Policies ergänzt. Das kann sowohl einmal im Jahr passieren, als auch jeden Sprint oder nahezu im Minutentakt, falls erforderlich. In diesen Policies kann natürlich auch der etablierte Rollenbegriff und das bestehende Rollenmodell weiter genutzt werden: „Das Objekt kann gelesen werden, wenn das Subjekt den Mitarbeiter-Typ ´Angestellter´ hat. Das Objekt kann aktualisiert werden, wenn das Subjekt die Rolle ´Editor´ hat."

Dies führt zur angenehmen Situation, dass RBAC mit PBAC-Ansätzen kombiniert werden kann, und eine Koexistenz mittelfristig sinnvoll erscheint.

**Wo eignet sich PBAC?**
Die Nutzung von PBAC erfordert eine Anpassung der Berechtigungsverwaltung in den Zielsystemen – folglich ist PBAC nur dann sinnvoll umsetzbar, wenn eigene neue Software-Entwicklungsvorhaben anstehen, oder eine existierende (Webanwendungs-)Software einem Refactoring unterzogen werden soll. Überall dort, wo eher dynamische Entwicklung mit sich schnell ändernden Anforderungen zu finden sind, oder sehr große Mengen an Objekten sich im wechselnden Zugriff durch viele Subjekte finden, kann ein PBAC-Ansatz hilfreich sein. PBAC kann aber auch in eher statischen Umgebungen eine sinnvolle Ergänzung zu RBAC-Modellen sein, wenn moderne Neuentwicklungen parallel zu Altsystemen betrieben und geschützt werden müssen. Hierbei kann der Pflegeaufwand für die Administration der etablierten Rollen erheblich reduziert werden, und die Anwendungslandschaft erhält eine zukunftsweisende, dynamische Autorisierungsplattform.

**Was ist für eine Umsetzung notwendig?**
Eine ganze Anwendungslandschaft auf PBAC zu transformieren wäre ein Mammutaufgabe – viele Entwickler haben die Ideen rund um Zanzibar und PBAC jedoch in Form von Open Source Bausteinen adaptiert und stellen diese für andere Entwickler frei zur Verfügung. Genannt seien hier die Projekte „KETO" und die überaus erfolgreiche Policy Engine „Open Policy Agent" (OPA) Software, die mit Fördermitteln entstanden ist und sich im Umfeld der hoch-dynamischen Zugriffsverwaltung auf Kubernetes Container einen Namen machen konnte. Zur Umsetzung kommen sogenannte Application Side Cars zum Einsatz, die eingehende Zugriffsanfragen an die zentrale Policy Decision Points leiten, über die zentral verwaltete Policies abgefragt werden können. Hierbei finden sich weitgehend Analogien zu abstrakten Web Access Management Komponenten (PAP, PIP, PDP), die wiederum über moderne Protokolle wie OAuth 2.0 mit den entsprechenden Flows eingebunden werden können.

**Fazit**
Komplexe Modelle wie im „Zanzibar" Papier beschrieben sind nur für wenige Unternehmen und Anwendungsfälle interessant. Die Kernideen rund um dynamischere Verwaltung von Zugriffsrechten können jedoch in nahezu jedem auf DevOps ausgelegten IT-Betrieb sinnvolle Anwendung finden und lassen sich mit modernen Open Source Komponenten auch verhältnismäßig einfach in den Entwicklungsprozess und die Werkzeuglandschaft des IT-Betriebs einbinden. Die etwas angestaubten RBAC-Ansätze werden nicht obsolet, sondern finden mit PBAC eine dynamische und flexible Ergänzung, mit der moderne Autorisierungsmodelle behutsam Einzug in die IT finden können.

***Sebastian Rohr***

1) Zu finden unter https://research.google/pubs/pub48190/
2) Zu finden unter https://github.com/ory/keto
3) Zu finden unter https://www.openpolicyagent.org/

# Vier Fragen zu EDR und NDR

## KOMMUNIKATION UND INTERAKTION DURCH INFORMATION HELFEN EINE UMFASSENDE CYBERABWEHR ZU ORGANISIEREN

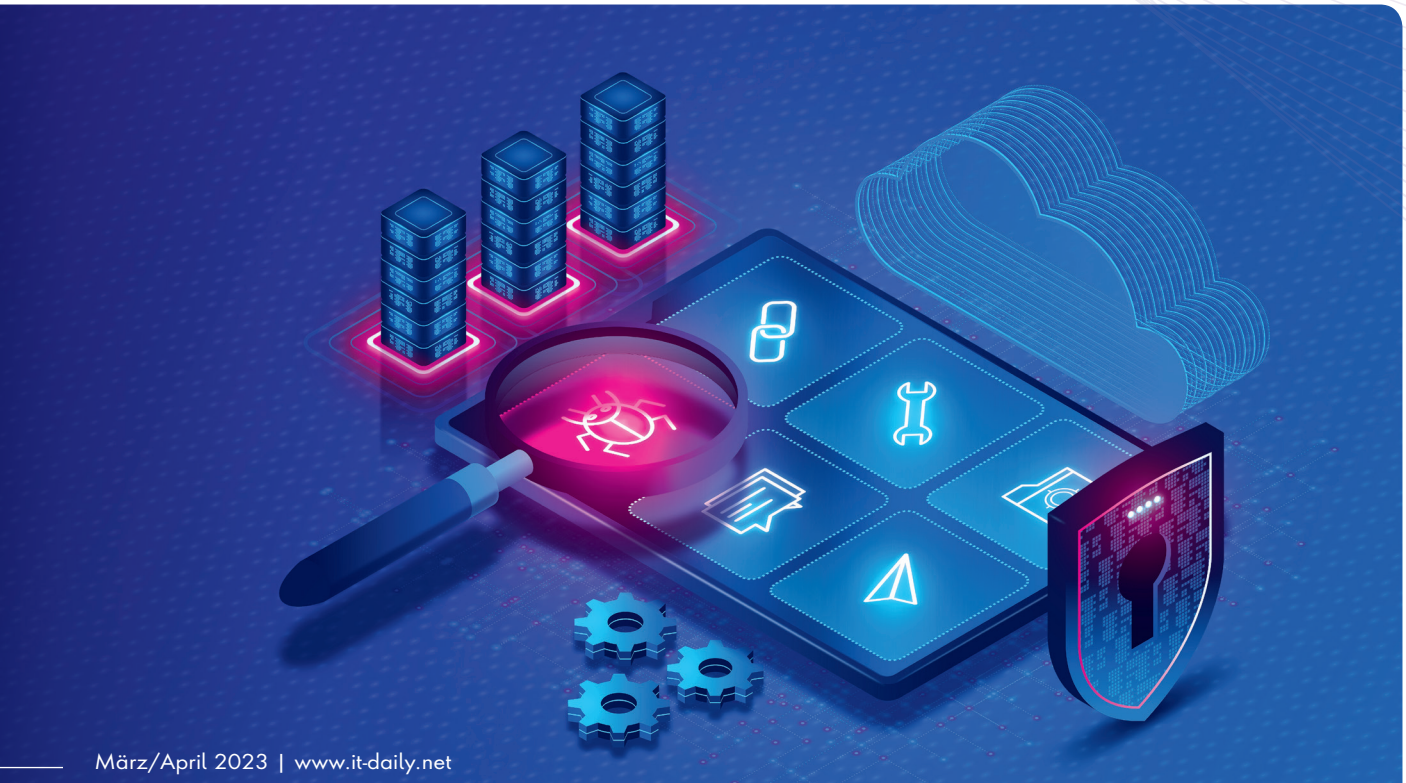
DURCH DAS ZUSAMMENSPIEL VON EDR UND NDR WERDEN AUCH DIE RANDBEREICHE DER IT-UNSICHERHEIT – NICHT VERWALTETE IOT- ODER OT-GERÄTE – ZUMINDEST ETWAS KLEINER.

**Paul Smit, Director Professional Services, ForeNova Technologies B.V., www.forenova.com**

Cyberangriffe, die Datenverluste oder längere IT-Ausfallzeiten verursachen, beruhen auf der Kenntnis der Hacker über die Gegebenheiten und das Geschehen in der Opfer-IT. Wer diese komplexen Attacken abwehren will, benötigt eine gut informierte und tief gestaffelte IT-Sicherheit. Diese sollte den Datenverkehr, die Endpunkte sowie Informationen aus beiden Bereichen im Blick haben. Eine Network Detection and Response (NDR) und eine Endpoint Dectection and Response (EDR) entfalten einen wirklichen Schutz in ihrer Kombination. Mit Interaktion und Koordination beantworten beide Systeme vier zentrale Fragen für die Cyberabwehr.

Viele Angriffe starten meist immer noch mit einer einfachen Phishing-Mail. Nach einer Studie von ForeNova und Cyber Security Insiders aus dem Herbst 2022 starteten Ransomware in 58 Prozent der Fälle durch eine Phishing-Mail, 52 PRozent durch infizierte E-Mail-Attachements. Diese sorgen aber nur für die initiale Infektion eines Systems. Die Urheber gefährlicher Advanced Persistent Threats (APTs) suchen anschließend nach kritischen Systemen sowie nach Informationen als Ansatzpunkte effizienter Attacken. Ihr Ziel ist es bei einer Ransomware-Attacke zum Beispiel, die größtmögliche Drohkulisse aufzubauen, damit Opfer ein Lösegeld bezahlen.

Die Spuren gestaffelter Angriffe verteilen sich im ganzen Netzverkehr und auf verschiedene Endpunkte. Ihre Abwehr



beruht vor allem auf Wissen und der kontinuierlichen Überwachung der gesamten IT. Eine Kombination aus NDR und EDR verbessert den notwendigen Wissensaustausch und beantwortet vier entscheidende Fragen:


**Bild 1: Ein Beitrag der Network Detection and Response: KI erkennt den ungewöhnlichen Aufbau von Verbindungen nach außen.** (Quelle: ForeNova)

**#1 Was befindet sich wo?**

NDR sieht den Aufbau neuer Verbindungen mit bisher unbekannten IP-Adressen wie unbekannten externen Servern. Zudem erkennt sie, wenn Daten in unüblichen Mengen oder zu ungewöhnlichen Zeiten zwischen bekannten Systemen fließen. Ebenso zeigt sie unbekannte Assets im Netz – wie Schatten-IT oder einmal angelegte und eventuell wieder vergessene virtuelle Maschinen. Eine EDR wiederum sieht alle zentral verwalteten Endpunkte mit einer IP-Adresse, wie einen Windows-PC- oder Mac-Systeme im Büro, remote im Home Office oder unterwegs. Auf einem zentral verwalteten Arbeitsnotebook installiert, erkennt ein EDR-Agent die Quelle gefährlicher Prozesse, wenn ein Mitarbeiter remote arbeitet: Ist das Notebook oder das WLAN im Hotel oder zuhause für ein Risiko verantwortlich? Auch eine angemietete Cloud-Server-Instanz lässt sich überwachen, indem Administratoren einen Agenten auf dieser Unternehmensressource in der angemieteten Cloud installierten.

**#2 Was geschieht wo?**

Menschliche Beobachter sind mit der Analyse der Aktivitäten im Netz und auf den Endpunkten überfordert. Künstliche Intelligenz (KI) unterstützt daher beim Monitoring und der Interpretation der IT- Vorgänge. Sie definiert die normalen und damit erlaubten Modelle des Datenverkehrs oder der Endpunktaktivitäten. Daraus abgeleitet definiert sie zutreffend, schnell und effizient neue und damit eventuell illegitime Abläufe, die auf einen Angriff hindeuten. KI von EDR und von NDR beobachten komplementär die verschiedenen Bereiche.

NDR hilft, die Muster im Datenverkehr und damit die Wege der Hacker im System zu erkennen und als potenziell gefährlich einzustufen. Wichtig ist, auffällige Wege nachzuzeichnen. Denn Hacker tarnen ihre Aktivitäten und Seitwärtsbewegungen mit legitimen Tools, die ein Administrator nutzen würde. Trotzdem ziehen sie dabei durch ihr Verhalten verräterische Spuren. Geht ein Tool etwa einzelne Systeme der Reihe nach ab, deutet dies darauf hin, dass ein Unbekannter, der sich in der IT nicht auskennt, nach Schwachstellen oder Informationen sucht. Ein Administrator, der Probleme lösen will, würde gezielt einzelne Systeme ansteuern, die er untersuchen muss.

Ein Endpunktschutz hilft unmittelbar bei der Exekution einer Attacke auf den Endpunkt, unterbindet also die Datenexfiltration oder den Verschlüsselungsprozess. EDR bietet zudem eine bessere Aufsicht der Endpunkte. Die Analyse von Prozessen, Verbindungen sowie von Aktivitäten der Nutzer oder von Prozessen, die vielleicht noch keine unmittelbaren Folgen zeigen, lässt sich oft erst durch die KI am Endpunkt interpretieren. Eine intelligente EDR unterscheidet zum Beispiel legitime von illegitimen Kompressionen oder Verschlüsselungen von Informationen.

**#3 Wann greift die Abwehr?**

Wer Endpunkt und Netzwerk beobachtet, erkennt verschiedene Zeitpunkte und Notwendigkeiten, vielstufige Angriffe abzuwehren. Eine Threat Intelligence einer EDR wehrt eine bekannte Phishing-Website in einer Mail ebenso ab wie eine Malware, deren Signatur bekannt ist. Die Dunkelziffer, wie viele Ransomware-Attacken so schon im Keim erstickt wurden, ist erfreulich hoch.

Eine NDR erkennt sofort den Aufbau der Kommunikation zwischen einem infizierten System und einem bösartigen Command-and-Control-Server. Sie sieht langfristige Manöver der Hacker, die etwa auf eine weitere Schwachstellenanalyse oder eine Eskalation von Privilegien digitaler Identitäten hindeuten.

Von einer EDR als Honeypot-Lockvögel angelegte Dateien in Verzeichnissen veranlassen verräterische Prozesse wie ein Verschlüsseln oder ein Löschen dieser Köder-Dateien. EDR löst einen sich verratenden Angriff frühzeitig aus und stoppt ihn. Ebenso blockiert sie Systeme. Ein auf Grund der Analyse des Netzverkehrs durch NDR erstellter Notfallplan legt fest, welche Systeme eine EDR im Ernstfall blocken soll, um Infektionswege abzuschneiden.

### #4 Wer übernimmt welche Maßnahmen?

Eine NDR sieht durch die KI-gestützte Definition von Angriffsmustern Gefahren frühzeitig kommen, doch sie benötigt die konkrete Hilfe vor Ort am Endpunkt. NDR und EDR tauschen nicht nur Informationen aus, sie arbeiten Hand in Hand. Die NDR veranlasst eine effiziente Mikrosegmentierung durch ihre Kenntnis des Datenverkehrs, die der Endpunkt auch ohne Firewall umsetzt. Sie bemerkt eine Datenexfiltration am Datenverkehr, die EDR stoppt diese. Ebenso alarmiert sie eine Firewall, um den Datenverkehr zu stoppen. NDR zeigt Schwachstellen auf, deren Ausnutzen eine EDR dann blockt – auch bevor ein Patch des Softwareanbieters bereitsteht oder eingespielt wird.

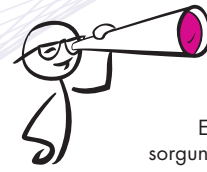
Nur ein Zusammenspiel der beiden Abwehrkomponenten erzeugt umfassende Sicherheit – einschließlich der Interaktion mit anderen Abwehrtechnologien wie SIEM oder einer Firewall. Zusammengestellte und im Kontext interpretierte Informationen aus mehreren Quellen erfassen das Gesamtgeschehen in der IT-Infrastruktur. Eine gestaffelte Abwehr bedeutet mehr, als nur viele Auffangnetze zu spannen. Sie erweitert den Schutzbereich, verbessert die Analyse von Angriffen und das Schließen einmal ausgenutzter Schwachstellen gegen zukünftige Angriffe. Sie beschleunigt die Reaktionszeit der Cyberabwehr.

### Abwehrhorizonte erweitern

Durch das Zusammenspiel von EDR und NDR werden auch die Randbereiche der IT-Unsicherheit – nicht verwaltete IOT- oder OT-Geräte – zumindest etwas kleiner. Indirekt reduzieren sich die Gefahren oder möglichen Angriffsfolgen durch das Überwachen des Netzverkehrs und durch den Schutz der Endpunkte. Ein intakter Endpunktschutz oder eine Firewall senken das Risiko etwa eines nicht verwaltbaren Routers im Homeoffice. Die wirkliche nahtlose Integration dieser Systeme bleibt aber noch eine gemeinsame Aufgabe der IT-, OT- und IoT-Architekten. EDR und NDR können Gefahren für die Systeme der IT senken: Durch das Erkennen ungewöhnlicher Prozesse auf dem Endpunkt und im Datenverkehr.

NovaCommand ist ein solches innovatives Tool, das Unternehmen hilft, die Cyberabwehr effizienter zu organisieren. Es wurde aus diesem Grund vom renommierten Sans-Institute getestet. Mit ForeNova NovaGuard steht auch ein EDR-Agent zur Verfügung. Der Dienst ForeNova MDR kombiniert aktuelle, auf Künstlicher Intelligenz basierende Sicherheitstechnologien mit dem Know-how, der Expertise und dem Urteilsvermögen von menschlichen Sicherheitsanalysten.

***Paul Smit***



**PLUS**

Eine kostenfreie Testversorgung von NovaCommand finden Sie hier:
**https://www.forenova.com/free-trial**

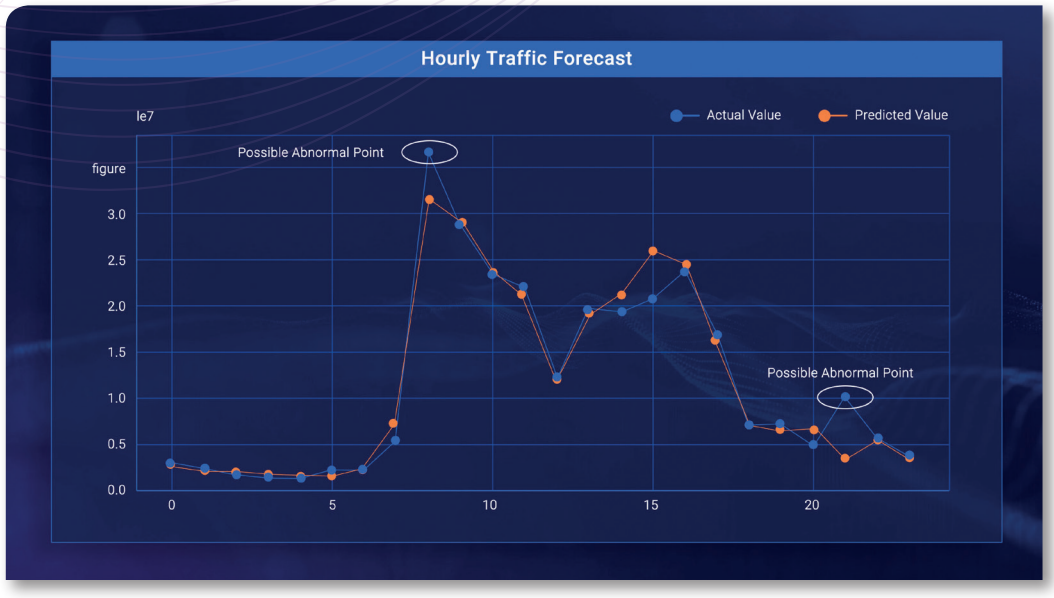
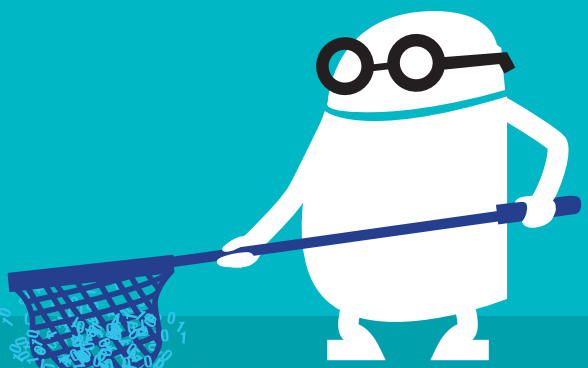



**Bild 2:**
**NDR erkennt die Exekution einer Datenexfiltration durch erhöhten Datenverkehr.**
(Quelle: ForeNova)

Data Lake:

# Die etwas ANDERE ART des PHISHINGS....



# ChatGPT: Chancen und Sicherheitsrisiken

## HOHER NUTZEN, VERSTECKTE GEFAHREN

OpenAI, im Dezember 2015 gegründet, ist ein non-profit Unternehmen für die KI-Forschung und -den KI-Einsatz. Deren Mission ist es, sicherzustellen, dass künstliche allgemeine Intelligenz der gesamten Menschheit zugutekommt. Daran arbeiten über 100 Mitarbeiter.

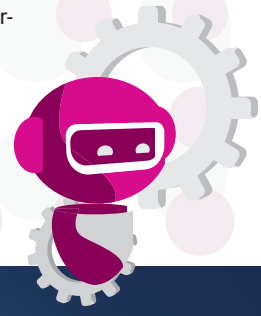
Eines der zur Zeit interessantesten Projekte ist ChatGPT. Ziel ist die Optimierung von Sprachmodellen für Dialoge.

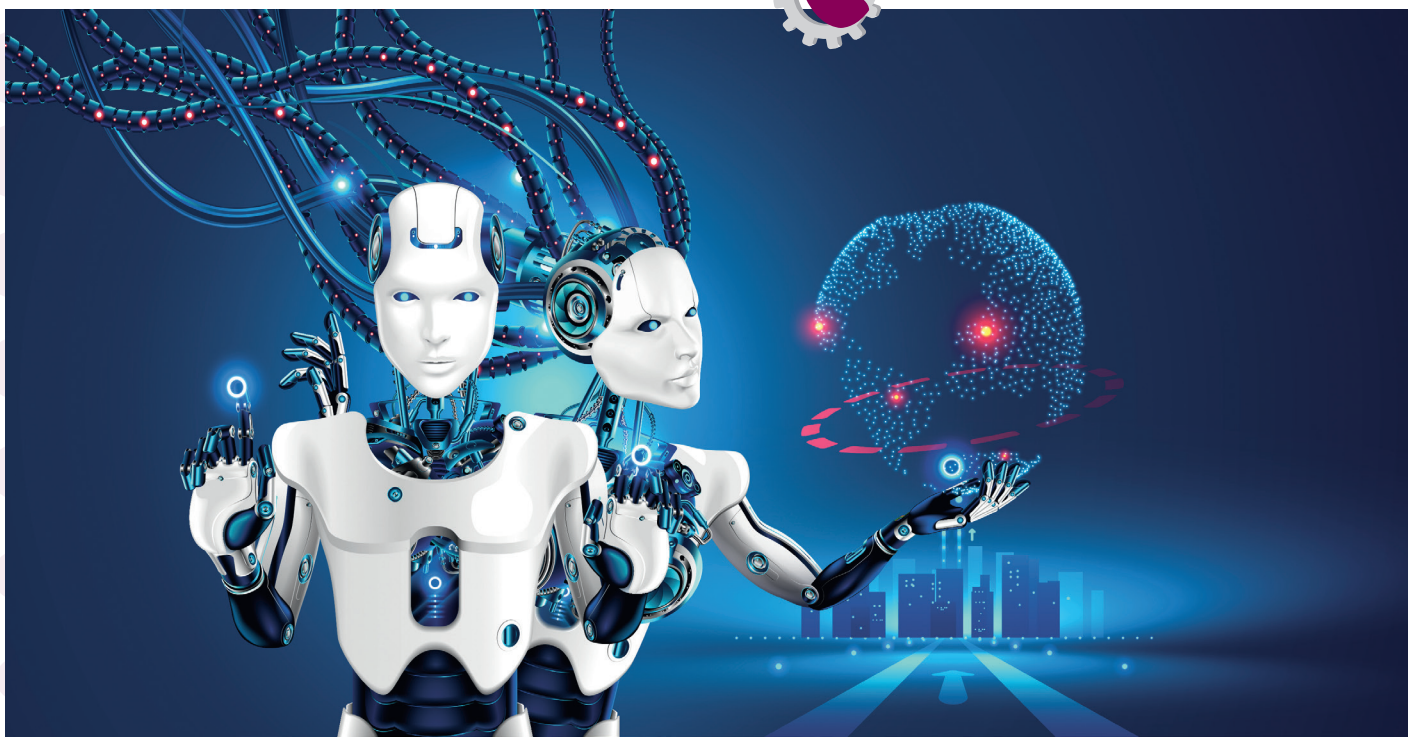
Den Experten ist es gelungen, ein Modell zu trainieren das Interaktion ermöglicht. Das Dialogformat ermöglicht es, Folgefragen zu beantworten, Fehler zuzugeben, falsche Prämissen in Frage zu stellen und unangemessene Anfragen zurückzuweisen. ChatGPT ist ein Geschwistermodell von InstructGPT, das darauf trainiert ist, einer Anweisung in einer Eingabeaufforderung zu folgen und eine detaillierte Antwort zu geben. Wer sich für die Details interessiert, wird hier fündig: https://openai.com/blog/chatgpt/

Soweit so gut. Bei allen Innovationen passiert es immer wieder, dass dort wo große Chancen sind, auch große Risiken liegen, oft im Verborgenen.

**Warum der Hype?**

Bei Trellix ist man der Ansicht, dass ChatGPT der Begriff für innovative Chattechnologie schlechthin geworden ist. Während seine Vorgänger in der Data-Science-Branche zwar auf Interesse stießen, erkannten nur sehr wenige einen praktischen Nutzen für den Durchschnittsverbraucher. Damit sei jetzt Schluss, denn der „intelligenteste Textbot aller Zeiten" hat Tausende von innovativen Anwendungsfällen inspiriert, die in fast allen Branchen zum Einsatz kommen. Im Cyber-Bereich reichen die Beispiele von der E-Mail-Generierung über die Code-Erstellung und -Prüfung bis



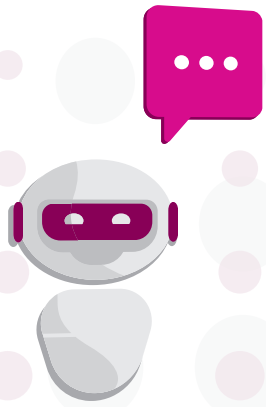


hin zur Entdeckung von Sicherheitslücken und vielem mehr.

Mit den bahnbrechenden Fortschritten in der Technologie sind jedoch auch die unvermeidlichen Sicherheitsbedenken nicht weit entfernt. Während ChatGPT bemüht ist, böswillige Inhalte einzuschränken, sieht die Realität so aus, dass Cyber-Kriminelle bereits nach Möglichkeiten suchen, das Tool für schadhafte Zwecke zu nutzen. Es ist zum Beispiel nicht schwer, realistische Phishing-E-Mails oder Exploit-Code zu erstellen, indem man einfach die Benutzereingabe ändert oder die erzeugte Ausgabe leicht anpasst.

**Die Kehrseite der Medaille**

Während textbasierte Angriffe wie Phishing weiterhin das Social Engineering dominieren, wird die Entwicklung von datenwissenschaftlichen Tools unweigerlich zu anderen Medien führen, einschließlich Audio und Video, die ebenso effektiv sein könnten. Darüber hinaus könnten Bedrohungsakteure versuchen, Datenverarbeitungs-Engines so zu verfeinern, dass sie ChatGPT nachahmen, während sie gleichzeitig Beschränkungen aufheben und sogar die Fähigkeiten dieser Tools zur Erstellung bösartiger Ergebnisse verbessern.



**Das Potenzial**

Auch wenn Bedenken hinsichtlich der Cyber-Sicherheit aufgekommen sind, darf nicht vergessen werden, dass dieses Tool ein noch größeres Potenzial hat Gutes zu tun. Es kann unter anderem dazu beitragen, kritische Programmierfehler zu erkennen, komplexe technische Konzepte in einfacher Sprache zu beschreiben und sogar Skripte und widerstandsfähigen Code zu entwickeln. Forscher, Hochschulen und Unternehmen in der Cyber-Sicherheitsbranche können sich die Vorteile von ChatGPT für Innovation und Zusammenarbeit zunutze machen. Daher wird es interessant, diese Entwicklung für computergenerierte Inhalte zu verfolgen, da es die Fähigkeiten sowohl für gutartige als auch für bösartige Absichten verbessert.

**Die Lücken**

Sicherheitsforscher von Check Point Research (CPR) haben just in Experimenten herausgefunden, dass ChatGPT auch dafür verwendet werden könnte, bösartige Mails und Code zu generieren und so mit wenig Aufwand ausgefeilte Cyberangriffe zu initiieren. Das ist natürlich weniger schön.

Sie warnen vor Hackern, die ChatGPT und Codex von OpenAI nutzen könnten, um gezielte und effiziente Cyberangriffe durchzuführen. CPR hat in experimentellen Korrespondenzen getestet, ob sich mithilfe des ChatBots schädlicher Code zur Initiierung von Cyberangriffen erstellen ließe. ChatGPT (Generative Pre-trained Transformer) ist ein frei nutzbarer KI-ChatBot, der seinen Nutzern auf der Grundlage im Internet zu findender Daten kontextbezogene Antworten liefern kann. Bei Codex wiederum handelt es sich um eine ebenfalls von OpenAI entwickelte Künstliche Intelligenz, die in der Lage ist, natürliche Sprache in Code zu übersetzen.

**Das Vorgehen verlief wie folgt:**

- CPR verwendete ChatGPT, um eine Phishing-E-Mail zu erstellen, die sich als Hosting-Unternehmen ausgab
- CPR wiederholte ChatGPT, um eine Phishing-E-Mail zu verfeinern und die Infektionskette zu erleichtern
- CPR verwendete ChatGPT, um VBA-Code zum Einbetten in ein Excel-Dokument zu generieren

**Mit ChatGPT Infektionsketten erzeugen**

Um die Gefahren beider Technologien zu demonstrieren, hat CPR ChatGPT und Codex verwendet, um bösartige E-Mails, Code und eine vollständige Infektionskette zu erzeugen, die die Computer von Nutzern angreifen kann. CPR dokumentiert seine Korrespondenz mit ChatGPT in einer neuen Veröffentlichung mit Beispielen für die erzeugten Inhalte. Das Ergebnis unterstreicht, wie wichtig es ist, wachsam zu sein, da die Entwicklung von KI-Technologien wie ChatGPT die Cyber-Bedrohungslandschaft erheblich verändern kann.

Mit ChatGPT von Open AI konnte CPR eine Phishing-E-Mail mit einem angehängten Excel-Dokument erstellen, das bösartigen Code zum Herunterla-

den von Reverse-Shells enthielt. Reverse-Shell-Angriffe zielen darauf ab, eine Verbindung zu einem entfernten Computer herzustellen und die Ein- und Ausgabeverbindungen der Shell des Zielsystems umzuleiten, damit der Angreifer aus der Ferne darauf zugreifen kann.

**Die durchgeführten Schritte:**

**#1 ChatGPT bitten, sich als ein Hosting-Unternehmen auszugeben**

**#2 ChatGPT bitten, den Vorgang zu wiederholen und eine Phishing-E-Mail mit einem bösartigen Excel-Anhang zu erstellen**

**#3 ChatGPT bitten, bösartigen VBA-Code in einem Excel-Dokument zu erstellen**

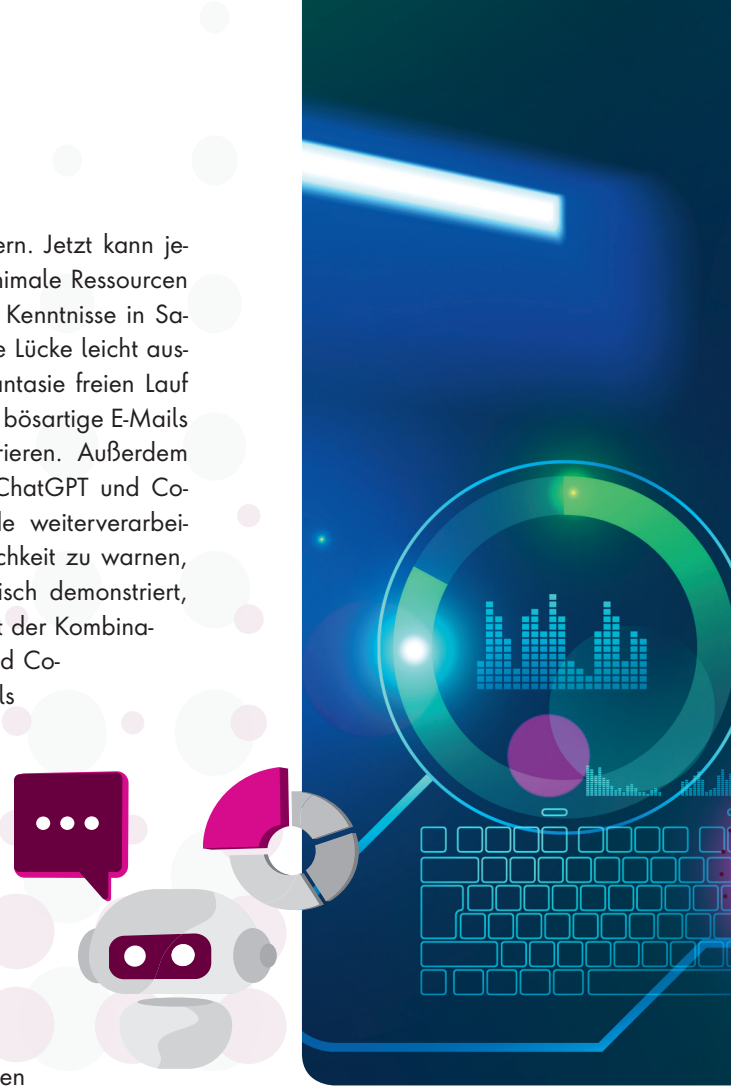
**Erstellung von schadhaftem Code**

CPR war auch in der Lage, mit Codex bösartigen Code zu erzeugen. CPR gab Codex dafür diverse Befehle, darunter:

- Ausführen eines Reverse-Shell-Skripts auf einem Windows-Rechner und Herstellen einer Verbindung zu einer bestimmten IP-Adresse.
- Prüfen, ob eine URL für SQL-Injection anfällig ist, indem man sich als Administrator anmeldet.
- Schreiben eines Python-Skripts, das einen vollständigen Port-Scan auf einem Zielcomputer durchführt.

Der bösartige Code wurde anschließend umgehend von Codex generiert.

Fazit von Sergey Shykevich, Threat Intelligence Group Manager bei Check Point Software: ChatGPT hat das Potenzial, die Cyber-Bedrohungslandschaft erheblich zu verändern. Jetzt kann jeder, der nur über minimale Ressourcen verfügt und keinerlei Kenntnisse in Sachen Code hat, diese Lücke leicht ausnutzen und seiner Fantasie freien Lauf lassen. Es ist einfach, bösartige E-Mails und Code zu generieren. Außerdem können Hacker mit ChatGPT und Codex bösartigen Code weiterverarbeiten. Um die Öffentlichkeit zu warnen, haben wir exemplarisch demonstriert, wie einfach es ist, mit der Kombination von ChatGPT und Codex bösartige E-Mails und bösartigen Code zu erstellen. Ich glaube, dass diese KI-Technologien einen weiteren Schritt in der gefährlichen Entwicklung von immer ausgefeilteren und effektiveren Cyberfähigkeiten darstellen. Die Welt der Cybersicherheit verändert sich rasant, und wir möchten betonen, wie wichtig es ist, wachsam zu bleiben, da diese neue und sich entwickelnde Technologie die Bedrohungslandschaft sowohl zum Guten als auch zum Schlechten beeinflussen kann.



**Was kann man dagegen tun?**

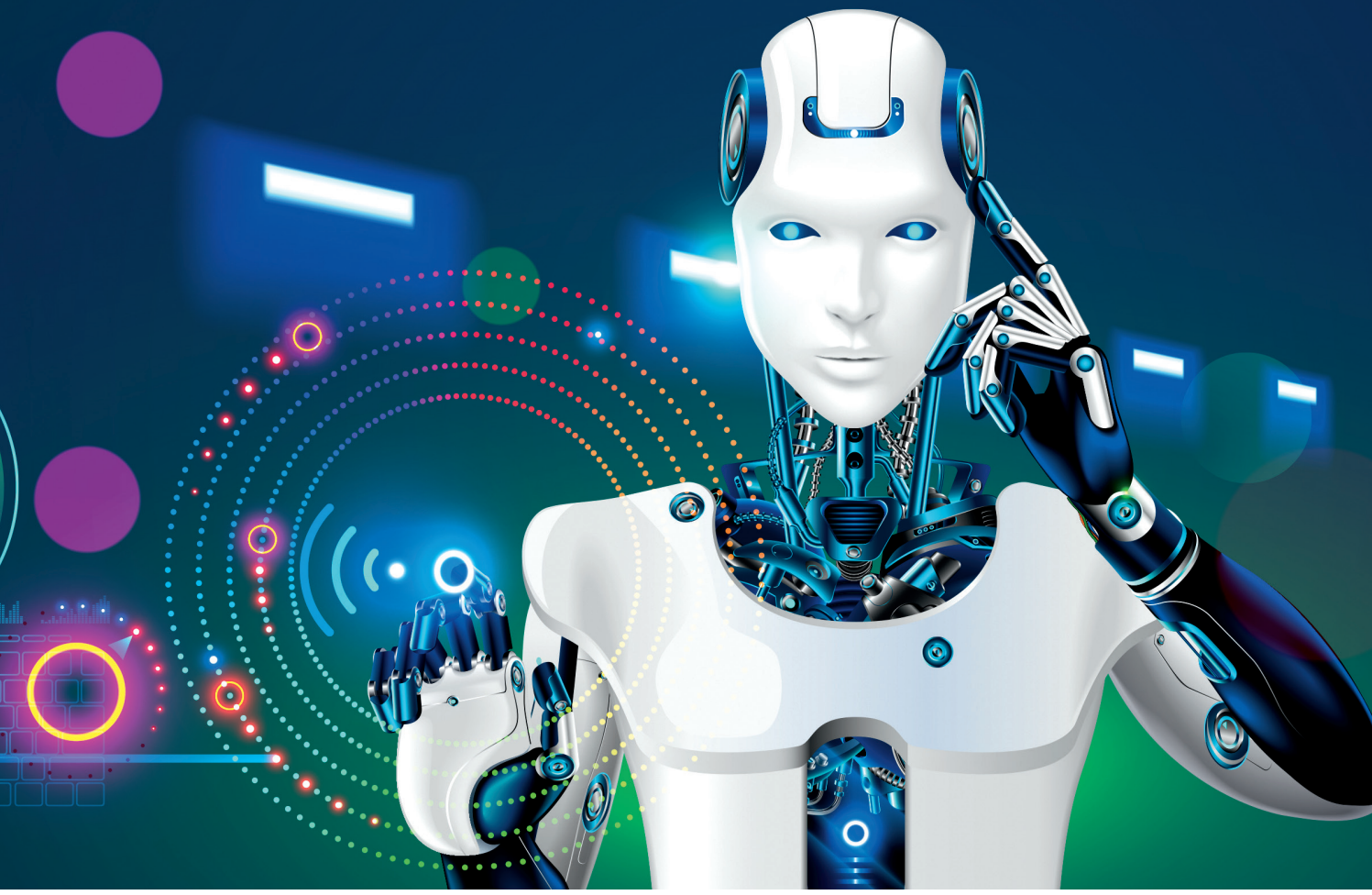
Wir haben einfach bei CheckPoint nachgefragt. Die Antwort: Im Prinzip sind die Schutzmaßnahmen grundsätzlich die gleichen wie auch bei anderen Phishing-/Cyberangriffen. Nachfolgend einige der bewährtesten Tipps:

**#1 Denken Sie nach, bevor Sie auf einen Link klicken.**

Phishing-Angriffe zielen häufig darauf ab, persönliche Daten zu stehlen. Aus diesem Grund ist bei URLs, die per E-Mail, SMS oder Messaging-Apps wie WhatsApp verschickt werden, besondere Vorsicht geboten. Um zu vermeiden, dass Sie zum nächsten Opfer werden, gehen Sie immer zur offiziellen Website des Absenders, anstatt auf einen unbekannten Link in der Nachricht zu klicken.

**#2 Verwenden Sie für jeden Zugang ein anderes Passwort.**

Für einen Cyberkriminellen gibt es keine größere Freude, als einen Benutzer zu finden, der ein Universal-Passwort verwendet. Sobald es einem Angreifer gelingt, auch nur ein Passwort zum Zugang einer etwaigen Plattform zu entschlüsseln, wird er versuchen, mit demselben Schlüssel auf alle Konten des Opfers zuzugreifen. Daher ist es wichtig, für jede App oder jeden Dienst ein eindeutiges Passwort mit mindestens acht Zeichen zu erstellen, das Buchstaben (Groß- und Kleinschreibung), Zahlen und Symbole kombiniert. Um den Überblick über die verschiedenen Passwörter zu behalten, kann ein sicherer



Passwortmanager wie Dashlane oder LastPass verwendet werden.

### #3 Verwenden Sie Multifaktor-/ Benutzerauthentifizierung.

Cyberkriminelle verwenden häufig das Remote-Desktop-Protokoll (RDP) um mit erratenen oder gestohlenen Anmeldedaten Fernzugriff auf die Systeme eines Unternehmens zu erhalten. Sobald der Angreifer in das System eingedrungen ist, kann er darüber hinaus Ransomware auf dem Rechner ablegen und diese ausführen. Dieser potenzielle Angriffsvektor kann durch strenge Passwortrichtlinien, die Einführung von Multi-Faktor-Authentifizierung und die Aufklärung der Mitarbeiter über Phishing-Angriffe geschlossen werden.

### #4 Vermeiden Sie das Herunterladen von Anhängen von Fremden.

Ein E-Mail-Anhang eines unbekannten Absenders kann Einfallstor für alle Arten von Cyberangriffen – sei es Malware oder Phishing - die Informationen und Daten stehlen können. Wird ein infiziertes Endgerät darüber hinaus für Fernarbeit genutzt oder ist es an ein größeres Netzwerk angeschlossen, kann es schwerwiegende Schäden verursachen. Prüfen Sie daher genau die Herkunft einer Datei und laden Sie nichts herunter, was Ihnen verdächtig vorkommt.

### #5 Etablieren Sie Schulungen zum Cyber-Bewusstsein.

Phishing-E-Mails sind eine der beliebtesten Methoden zur Verbreitung von Ransomware. Sie verleiten Nutzer dazu, auf einen Link zu klicken oder einen bösartigen Anhang zu öffnen. So können sich Cyberkriminelle dann Zugang zum Computer des Mitarbeiters verschaffen und mit der Installation und Ausführung des Ransomware-Programms beginnen. Deshalb sollten die Mitarbeiter in regelmäßigen Schulungen zu klassischen Best Practices angehalten werden, wie der Prüfung der Legitimität von Links, bevor diese angeklickt werden.

### #6 Installieren Sie Anti-Ransomware-Lösungen.

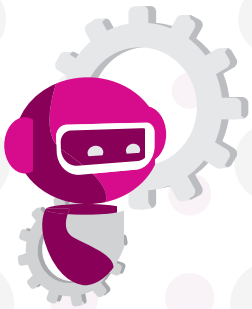
Um ihr Ziel zu erreichen, muss Ransomware bestimmte anomale Aktionen durchführen, wie das Öffnen und Verschlüsseln einer großen Anzahl von Dateien. Anti-Ransomware-Lösungen überwachen Programme auf für Ransomware typische, verdächtige Verhaltensweisen. Wenn diese Verhaltensweisen erkannt werden, kann das Programm Maßnahmen ergreifen, um die Verschlüsselung zu stoppen, bevor weiterer Schaden angerichtet werden kann.

### Einflüsse auf die IT

Natürlich machen sich viele derzeit Gedanken über Einsatzgebiete und den

Einfluss auf die IT-Welt. Auch die Hersteller. So zum Beispiel Omada, ein Anbieter im Bereich Identity & Access Management.

Für die Anwender sei es natürlich verlockend mit ChatGPT ein neues Tool für das Arbeiten zur Verfügung zu haben, mit dem Programmierer ihre Fragen einem Chatbot stellen können und dieser dann eine fast menschlich anmutende Antwort gibt, die wie eine Unterhaltung präsentiert wird.



Das Tool kann sich die gesamte Diskussion merken und verwendet frühere Fragen und Antworten, um wiederum künftige Antworten zu ermitteln und diese zu optimieren. ChatGPT wählt die Antworten wiederum aus, indem es riesige Datenmengen aus dem Internet verarbeitet – aller Art. Es kann sogar skurrile Befehle recht akkurat umsetzen, wie das Schreiben einer Geburtstagskarte im Tonfall einer beliebigen Berühmtheit.

ChatGPT selbst sagt jedoch auf Nachfrage über sich: „Ich bin nicht perfekt und habe vielleicht nicht immer die richtige Antwort auf jede Frage. Außerdem sind die Informationen, die ich zur Verfügung stelle, nur so genau wie die Daten, auf die ich trainiert wurde und die einen festen Stichtag haben. Das bedeutet, dass ich möglicherweise nicht in der Lage bin, Informationen über aktuelle Ereignisse oder Entwicklungen zu liefern, die seit der Erfassung der Trainingsdaten eingetreten sind", und unterstreicht die Tatsache, dass KI immer noch auf menschliche Komponenten angewiesen ist sowie eine hohe Datenqualität erfordert, um ordnungsgemäß zu funktionieren. Das Gleiche gilt für den Einsatz von KI in der Identitätsverwaltung: Sie eröffnet viele spannende Möglichkeiten, erfordert aber noch menschliches Eingreifen, damit sie funktioniert.

Aus dem Phänomen ChatGPT lassen sich laut Omada-Experten drei wichtige Lehren ziehen, die auf jedes Programm zur Identitätsverwaltung angewendet werden können:

### #1 Menschen sind immer noch wichtig

Viele sehen hinter ChatGPT auch den Versuch, eine neue Art von Suchmaschine zu etablieren und den derzeitigen Markt aufzurütteln. Wie bei Suchmaschinen ist jedoch sowohl der Mensch, der die Frage stellt, wichtig, als auch die Menschen hinter der Programmierung der KI selbst. Im Bereich der Identitäten kann man an KI denken, die Zugriffsrechte empfehlen kann, die auf der Grundlage von Zugriffsrechten in Peer-Gruppen generiert wurden. In diesem Fall kann die Software-Lösung diese Empfehlungen zwar auf der Grundlage dessen, was andere Personen im gesamten Netzwerk tun, kuratieren, doch ist zu Beginn trotzdem noch menschliches Eingreifen erforderlich, denn vorher muss festgestellt werden, wer die wahren Peers sind und welche Arten von Zugriffsrechten und Berechtigungen auf der Grundlage von (stets neu zu bewertenden) Rollen gewährt werden dürfen.

### #2 Datenqualität ist entscheidend

Betrachten wir noch einmal das oben genannte Beispiel der Geburtstagskarte: Angenommen, ein Nutzer erhält auf diese Anfrage hin eine ganze Reihe gefälschter Reden eines Politikers, den er sich wünschte, die ebenfalls im Netz kursieren – dann ist das Ergebnis nicht sehr genau und wird den Fragesteller verwirren. Ähnlich ist es bei der Identitätsverwaltung, daher ist es nicht so einfach, schlicht ein KI-Tool anzuschließen, denn man bedenke: In diesem wichtigen Segment der IT-Sicherheit spielen Governance, Compliance, Prüfkontrollen und reibungslose Arbeitsabläufe eine wichtige Rolle. Damit ein Identitätsmanagement-Tool funktioniert, muss es mit hochqualitativen Daten gefüttert werden, um überwachen zu können, wer Zugriff auf welche Bereiche hat, warum dieser Zugriff gewährt wurde, für wie lange – und so weiter. Für ein leistungsfähiges Identitätsmanagement kann die Einspeisung von Daten aus mehreren Quellen sehr schnell pro-

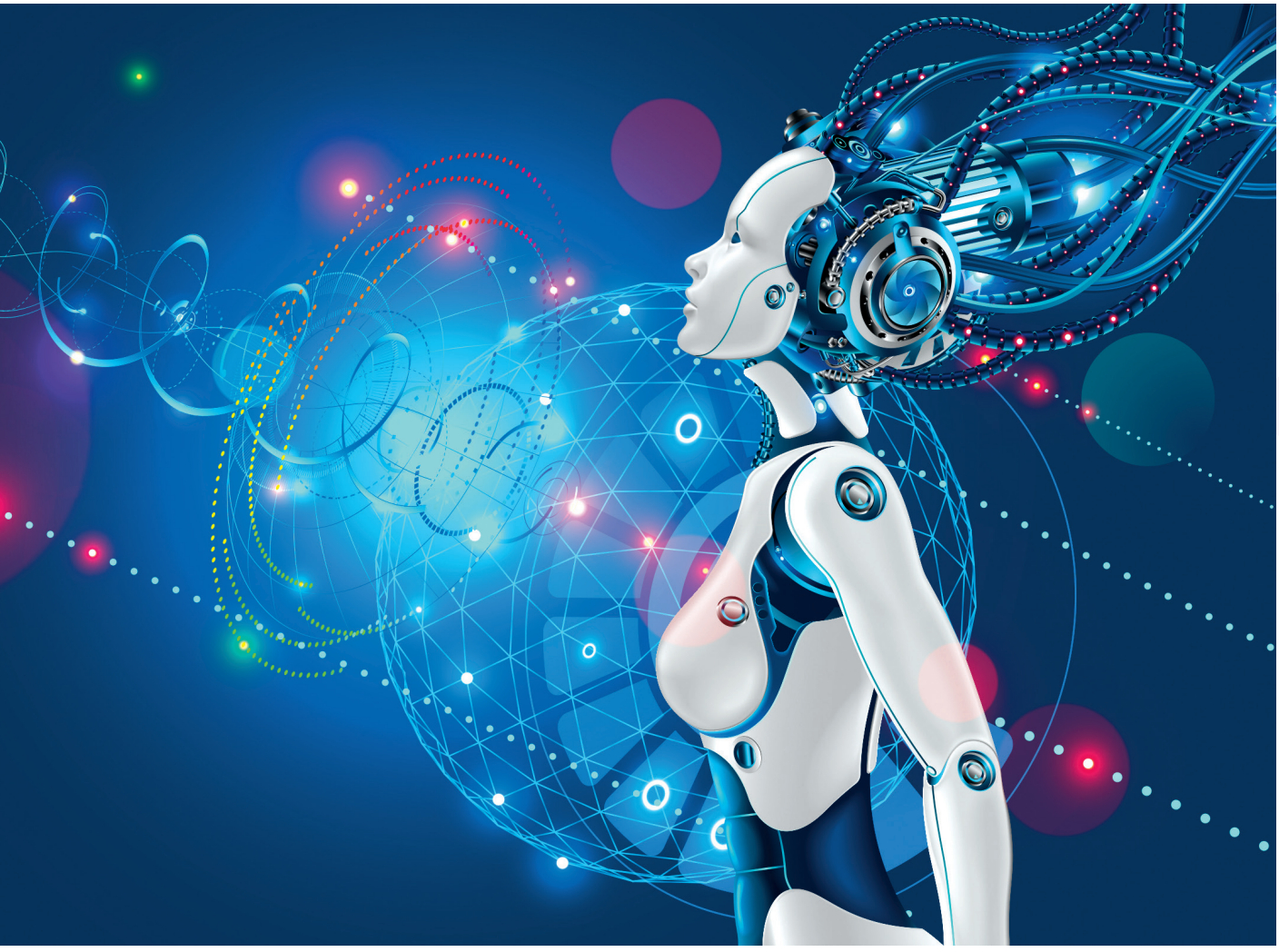
blematisch werden, insbesondere dann, wenn die Daten in unterschiedlichen Formaten oder Modellen gespeichert wurden.

### #3 KI ist kein Allheilmittel

Viele befürchten, dass ChatGPT bedeutet, Kinder bräuchten ihre Hausaufgaben nicht mehr selbst erledigen, oder Fachartikel, Gedichte, ganze Bücher, Komposition, Gemälde oder Kommentare (wie dieser) würden automatisch generiert werden. In einigen Fällen mag dies zutreffen, doch in den meisten Fällen sollte KI nur zur Optimierung der Entscheidungsfindung oder der Prozesse eingesetzt werden, neben dem Menschen, damit sie ihre volle Wirkung entfalten kann. Eine wichtige Erkenntnis aus der jüngsten Begeisterung für KI lautet daher, dass sie auf solide Grundprozesse aufgesetzt werden sollte, um den größten Nutzen zu erzielen. Auch bei ChatGPT muss man wissen, welche Fragen man stellen will und wie man sie zu stellen, damit man die besten Informationen erhält.

Mit anderen Worten: Im Identitätsmanagement müssen die KI-Funktionen von IAM-Administratoren und Sicherheitsverantwortlichen in die richtige Richtung gelenkt werden. Um KI optimal nutzen zu können, muss sie in Verbindung mit Menschen eingesetzt werden, damit bessere Entscheidungen getroffen werden können. KI kann zwar problemlos zur Automatisierung manueller oder sich wiederholender Prozesse eingesetzt werden, aber es wird immer menschliches Eingreifen erforderlich sein, um eine große Anzahl von Identitäten verwalten zu können, die Zugriff auf eine wachsende Liste von Cloud-basierten Anwendungen und Infrastrukturen benötigen.

***Ulrich Parthier | www.it-daily.net***



# Homeoffice

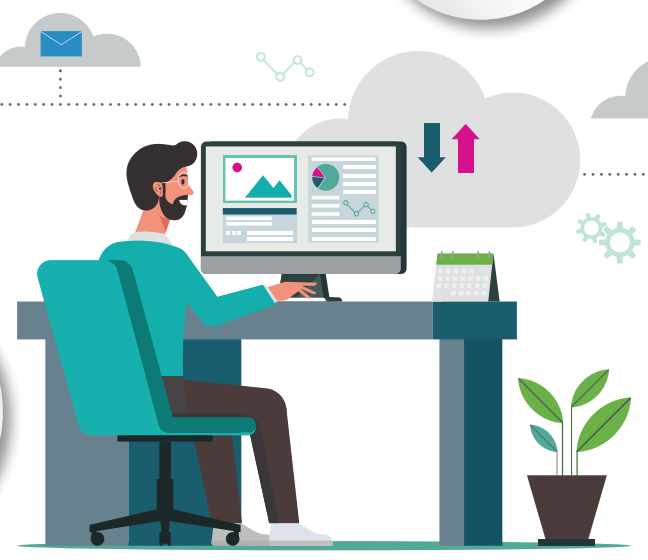
## MANGELNDES SICHERHEITSBEWUSSTSEIN

Die Verlagerung Richtung Remote-Arbeit und Homeoffice in deutschen Unternehmen bringt neue, vielfältige Sicherheitsbedrohungen mit sich – so sieht das auch eine klare Mehrheit der IT-Expertinnen und -experten in Unternehmen. In einer Umfrage von SoSafe, gaben 9 von 10 Befragten an, dass sich die Cyber-Bedrohungslage verschlechtert habe. 75 Prozent der Befragten nennen mobiles Arbeiten als einen Grund dafür – und das nicht zu Unrecht: Denn Mitarbeitende, die im Homeoffice arbeiten, klicken fast dreimal so häufig (30 %) auf Phishing-E-Mails wie Angestellte, die im Büro sind (12 %).

Laut SoSafe zählen mangelnde Kommunikation im Homeoffice, die Nutzung eigener Technik als Arbeitsgeräte sowie ungesicherte Arbeitsumgebungen zu den größten Sicherheitsrisiken des mobilen Arbeitens. Während diese den meisten Unternehmen durchaus bewusst sind, ist das bei den Mitarbeitenden selbst nicht immer der Fall – sie haben im Homeoffice oft ein falsches Gefühl von Sicherheit. Gerade jetzt während der Winter- und Krankheitszeit arbeiten immer mehr Arbeitnehmende von zu Hause aus. SoSafe warnt daher vor den größten Risiken der mobilen Arbeit und teilt einfache Tipps sowie Lösungen, um diese zu mindern.

## DIE TIPPS FÜR SICHERES ARBEITEN IM HOMEOFFICE:

- **Vergewissern Sie sich, dass Ihr System und Ihre Programme auf dem neuesten Stand sind**
- **Schulen Sie sich regelmäßig zum Thema Cybersicherheit**
- **Bewahren Sie Dokumente und tragbare Datenspeichergeräte an einem sicheren Ort auf**
- **Überprüfen Sie Informationen und geforderte Maßnahmen**
- **Sperren Sie immer Ihren Bildschirm oder Computer, wenn Sie ihn nicht benutzen**
- **Stellen Sie sicher, dass vertrauliche oder sensible Dokumente zerstört, unkenntlich oder unleserlich gemacht werden, bevor Sie sie wegwerfen**



## DIE GRÖSSTEN RISIKEN DER MOBILEN ARBEIT

**#1 Unzureichend geschützte Arbeitsbereiche:** Mehr Mitarbeitende im Homeoffice bieten Cyberkriminellen auch mehr Angriffsfläche. Unternehmen müssen daher weitere Endpunkte, Netzwerke und Software sichern. Für die Cybersecurity-Teams ist das eine schwer zu überblickende Lage. Denn sie können nicht alle im Homeoffice verwendeten Technologien überprüfen. So ist mehr denn je die Aufmerksamkeit jedes einzelnen Mitarbeitenden zu Hause gefragt, um Sicherheitslücken zu erkennen und entsprechend zu reagieren.

**#2 Optimale Bedingungen für Social Engineering und Phishing:** Die mobile Arbeit verstärkt außerdem die Abhängigkeit von digitalen Kommunikationsmitteln. Mitarbeitende gewöhnen sich daran, dass sie Geschäftsanfragen nur noch per E-Mail erhalten. Cyberkriminellen bietet das optimale Bedingungen, um ausgeklügelte Phishing-Angriffe zu starten – und das mit Erfolg, da mehr Mitarbeitende Phishing-Mails zuhause öffnen oder mit ihnen interagieren.

**#3 Fehlende Kommunikation mit Kolleginnen und Kollegen:** Hohe Klickraten im Homeoffice lassen sich unter anderem durch einen Mangel an direkter Kommunikation mit den Kolleginnen und Kollegen erklären. Direkte Kommunikation ist schließlich notwendig, um Informationen oder geforderte Handlungen zu überprüfen – oder auch, um über alle Entwicklungen im Unternehmen auf dem Laufenden zu bleiben.

**#4 Bedarf von neuen Kommunikations- und Kollaborationswerkzeugen:** Da die persönliche Kommunikation deutlich reduziert ist, kommen neue Kommunikations- und Kollaborationstools wie Slack oder Zoom zum Einsatz. Diese bieten wiederum neue Einfallstore für Cyberkriminelle – nicht nur für den Angriff selbst, sondern auch zum Abfangen von Informationen für ihren nächsten Social-Engineering-Angriff. Insbesondere Voice Cloning und Deepfakes sind derzeit auf dem Vormarsch.

**#5 Bring-Your-Own-Device:** Viele Angestellte kompensieren das Fehlen von Firmengeräten im Homeoffice, indem sie ihre privaten Laptops oder Smartphones für Arbeitszwecke nutzen. Das Problem: Die IT-Abteilung kann diese Geräte nicht auf Unregelmäßigkeiten überprüfen. Ebenso wenig kann sie sicherstellen, dass die erforderlichen technischen Abwehrsysteme vorhanden sind.

**#6 Anfällige Mitarbeitende aufgrund von Unsicherheit und ständiger Veränderung:** Neue Arbeitsbedingungen und ein unvorhersehbares Umfeld ermüden Mitarbeitende – und machen sie damit anfälliger für Cyberangriffe, die diese Veränderung für anlassbezogenes Phishing laufend instrumentalisieren. So kümmern sich Mitarbeitende beispielsweise weniger um Sicherheitsrichtlinien, hinterfragen Inhalte seltener und machen eher Fehler.

***www.sosafe-awareness.com***



## IMPRESSUM

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

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

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

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

***Autoren:***
Torsten George, Darren Guccione, Dr. Dieter Kehl, Ralf Kempf, Michael Kleist, Frank Limberger, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Sebastian Rohr, Paul Smit, Steffen Ullrich

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

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

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

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

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

***Anzeigenpreise:***
Es gilt die Anzeigenpreisliste Nr. 30.
Preisliste gültig ab 1. Oktober 2022.

***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
Marena Avila (nur per Mail erreichbar),
avila@it-verlag.de

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

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

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

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

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

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

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

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

# We secure IT

## 11.05.23 | Digitalevent

SAVE THE DATE

SCAN ME

https://www.it-daily.net/wesecureit/


#WesecureIT2023