itmanagement
NOVEMBER 2020


TRANSFORMATION AUF ALLEN EBENEN

# RETHINK YOUR WORK!

Joerg Hartmann, Konica Minolta

## DAS TEC MODELL

Der Code agiler Organisationen

## ZERO TRUST

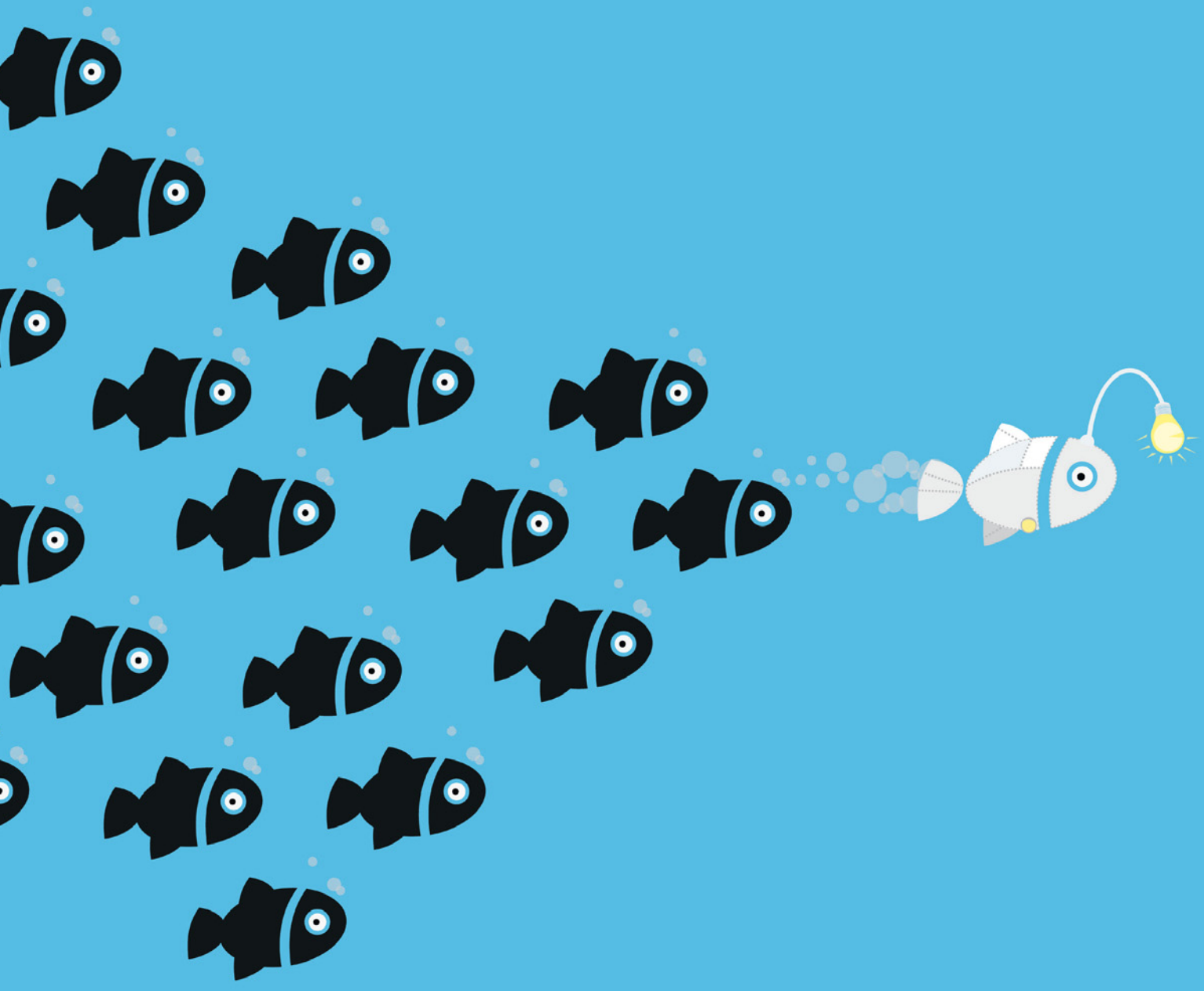
Buzzword oder praktischer Ansatz?

## CUSTOMER CENTRICITY

Ein Muss im digitalen Zeitalter

www.it-daily.net

# Thought Leadership



## POSITIV BLEIBEN

Und auf einmal stehen wir da, wo wir Anfang des Jahres bereits einmal standen und nie wieder hinwollten. Eigentlich hatte ich mir fest vorgenommen zum Thema Pandemie auf keinen Fall ein Editorial zu schreiben, eigentlich … Aber man kommt einfach nicht um das Thema herum. Egal, wo man ist, mit wem man sich trifft – virtuell wie in der realen Welt – irgendwann kommt man immer auf Covid-19 zu sprechen.

Dass das Virus da ist und uns sicherlich noch weiterhin begleiten wird, darüber bedarf es keiner Diskussion. Wie man damit umgeht, besonders im beruflichen Umfeld, dagegen schon. Klar ist, dass die Pandemie enorme negative Auswirkungen auf viele Branchen hat, viele dieser Auswirkungen werden sich wahrscheinlich auch erst wesentlich später klar benennen lassen. Aber: Es gibt auch positive Punkte.

Laut einer aktuellen Studie von Qualtrics stieg die Kreativität und die Produktivität der Arbeitnehmer im Homeoffice tatsächlich an (www.qualtrics.com/de). Das mag erst einmal verwundern, aber bei genauerer Betrachtung zeigt dies, dass Arbeitnehmer durchaus gewillt sind, sich schwierigen Situationen zu stellen und das Beste daraus zu machen. Aufgrund mangelnder technischer Unterstützung zu Beginn der Pandemie, musste sich oft selbst geholfen werden – was allerdings schnell zu einem Problem für die Sicherheitsabteilungen der Unternehmen wurde. Aber auch dafür haben die meisten Firmen mittlerweile Lösungen gefunden, die Digitalisierung und auch das Thema „Mobile Working" weiter vorangetrieben.

Ähnlich sehen es auch viele Autoren dieser Ausgabe: Machen Sie das Beste aus der Situation oder wie unser Titelthema so schön sagt: rethink your work!

In diesem Sinne, viel Spaß beim Lesen

Carina Mitzschke | Redakteurin it management

COVERSTORY 10

# INHALT

36


34

32

49

26


38

# DATA SCIENCE

## VERSCHENKTE POTENZIALE MANGELS DATENSTRATEGIE?

Die Disziplin Data Science eröffnet neue Möglichkeiten, messbare Erkenntnisse und datengestützte Vorhersagen zu generieren. Damit hat sich die Datenwissenschaft als wichtiger Hebel positioniert, mit dem Unternehmen Wettbewerbsvorteile sicherstellen können. In der Praxis jedoch sammeln viele Organisationen einfach möglichst viele Informationen in riesigen Datenpools, in der Hoffnung, datengesteuerter zu werden. Das dies nicht funktionieren kann und welche Potenziale Unternehmen durch eine unzureichende Auswertung ihrer Daten verschenken, zeigen aktuelle Studien. Um das volle Potenzial von Daten effektiv auszuschöpfen, benötigen Unternehmen nicht nur die passenden Technologien und Prozesse, sondern auch Fachkräfte mit den passenden Fähigkeiten. Skillsoft hat fünf Schritte zusammengefasst, mit denen sie ihre Datenstrategie weiterentwickeln können.

### 1. Datenkontaminierung reduzieren

Um Datenkontamination zu minieren, müssen Mitarbeiter besser über nachgelagerte Datenprozesse informiert werden. Einige Informationen sind geschäftskritisch, aber viele Daten entstehen auch unstrukturiert und undefiniert als Nebenprodukt täglicher Büroarbeiten als sogenannte „Dark Data". Um den Nutzen zu erhöhen, müssen Daten besser bereinigt, relevante Daten definiert sowie aus ihren Silos befreit und für Analysen zugängig gemacht werden.

### 2. Transformative Technologie nutzen

Ein wichtiger Schritt dazu ist es, Technologien wie maschinelles Lernen und künstliche Intelligenz für die Datenanalyse zu nutzen. Algorithmen und Plattformen für „Machine Learning" und „Deep Learning" helfen dabei, die riesigen Datenmengen – Stichwort „Big Data" – auszuwerten. Die Investition in entsprechende Werkzeuge, Technologien und Mitarbeiterfähigkeiten ist daher eine wichtige strategische Entscheidung.

### 3. Anreize für Data Science Rollen setzen

Der Fachkräftemangel in vielen Bereichen hat Unternehmen laut Gartner dazu ermutigt, Mitarbeiter als interne Kunden zu betrachten. Top-Arbeitgeber formulieren spezifische Angebote mit klaren Wertversprechen („Employer Value Proposition") und Karriereperspektiven anstelle von „Jobs", um Datenprofis anzuziehen und zu halten.

### 4. Datenrollen diversifizieren

Es ist sinnvoll, die Aufgaben und Rollen frühzeitig zu spezifizieren, um auch intern entsprechende Fähigkeiten aufbauen zu können. Eine vorausschauende Strategie ist es daher, vielversprechende Mitarbeiter oder Kandidaten frühzeitig zu identifizieren und sie mithilfe von Schulungen für die Weiterentwicklung ihrer Karriere im Bereich Data Science zu qualifizieren.

### 5. Karrierechancen aufzeigen

Durch Angebote für Qualifizierung, Vorqualifizierung und Umschulung von Mitarbeitern entwickeln Organisationen auch intern Fähigkeiten, die aktuell oder in Zukunft benötigt werden. Mit der internen Förderung von Mitarbeitern bleibt außerdem wertvolles institutionelles Wissen erhalten, statt karriereorientierte Mitarbeiter an andere Arbeitgeber zu verlieren.

***www.gcpr.de***

# KÜNSTLICHE INTELLIGENZ

## GESETZLICHE REGELN GEFORDERT

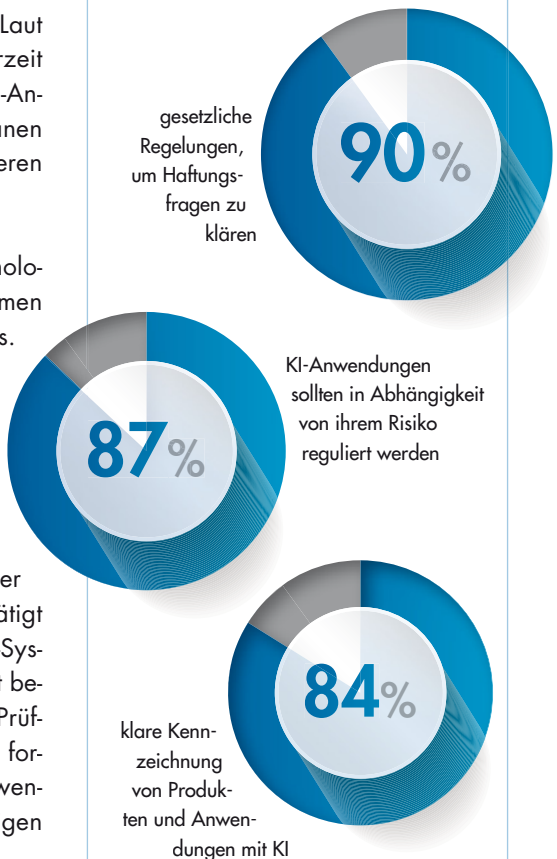
Die deutschen Unternehmen stehen Künstlicher Intelligenz sehr positiv gegenüber und erhoffen sich durch die Nutzung der Technologie entscheidende Wettbewerbsvorteile. Gleichzeitig befürwortet eine große Mehrheit gesetzliche Vorgaben für den Einsatz Künstlicher Intelligenz. Das hat eine repräsentative Studie ergeben, für die im Auftrag des TÜV-Verbands 500 Unternehmen ab 50 Mitarbeiter/innen befragt wurden.

„Künstliche Intelligenz ist eine Schlüsseltechnologie der Digitalisierung mit enormen Chancen, die aber einen gesetzlichen Rahmen braucht", sagte Dr. Dirk Stenkamp, Präsident des TÜV-Verbands (VdTÜV). „KI-Anwendungen sollten bestimmte Sicherheitsanforderungen erfüllen, wenn bei ihrer Nutzung die Gesundheit von Menschen oder ihre elementaren Grundrechte wie Privatsphäre oder Gleichberechtigung in Gefahr sind." Stenkamp: „Nur mit klaren gesetzlichen Vorgaben können wir Vertrauen in Künstliche Intelligenz schaffen und eine breite Nutzung ermöglichen." Laut den Studienergebnissen nutzen derzeit erst 11 Prozent der Unternehmen KI-Anwendungen. Weitere 4 Prozent planen die Nutzung und 15 Prozent diskutieren darüber.

Wenn es um die Nutzung der Technologie geht, wünschen sich Unternehmen mehr Orientierung für ihr Business. „KI-Systeme sind häufig eine Art Blackbox, deren Entscheidungen die Nutzer nicht nachvollziehen können", sagte Stenkamp. Daher würden es mehr als vier von fünf Unternehmen befürworten (84 Prozent), wenn die Zuverlässigkeit einer KI von unabhängigen Experten bestätigt würde. Bei der Anschaffung eines KI-Systems würden 86 Prozent ein Produkt bevorzugen, das über ein neutrales Prüfzeichen verfügt. Und 85 Prozent fordern, dass die Sicherheit von KI-Anwendungen von herstellerunabhängigen Stellen geprüft wird.

***www.vdtuev.de***

### DAS FORDERN UNTERNEHMEN



# TECHNOLOGIEFRUSTRATION

## ADIEU TALENTE?

Eine Vielzahl kleiner Unternehmen sind noch nicht ausreichend mit Remote-Working-Technologien ausgestattet, wie eine neue Studie von Ricoh Europe ergab: Die Wahrscheinlichkeit, dass europäische Kleinunternehmen Arbeitnehmer aufgrund von Frustration über die technischen Voraussetzungen für Remote Work verlieren, ist 42 Prozent höher als bei großen Unternehmen.

Während sich Kleinunternehmen aktuell von den Folgen der Coronavirus-Pandemie erholen, erwarten die Arbeitnehmer von ihren Arbeitgebern zunehmend moderne und flexible Arbeitskonzepte.

Diese technischen Defizite stellen nicht nur ein Risiko für die Bindung von Talenten dar. Besorgniserregend ist, dass gerade in dieser Zeit, in der Wachstum entscheidend ist, ein Viertel der Befragten berichtet, dass ihnen nicht die notwendigen Mittel zur Verfügung stehen, um die besten Ergebnisse für Kunden zu erzielen oder aus dem Homeoffice effektiv mit ihrem Team zu kommunizieren.

***www.ricoh.de***

**27 %**
der Befragten in europäischen Kleinunternehmen ziehen einen Arbeitsplatzwechsel in Betracht

**69 %**
gaben an, dass sie über die für Remote Working benötigten Fähigkeiten verfügen

**29 %**
sagen, dass es ihnen aufgrund von Problemen mit der Kommunikation und Technik schwerfalle, im Homeoffice motiviert und engagiert zu bleiben

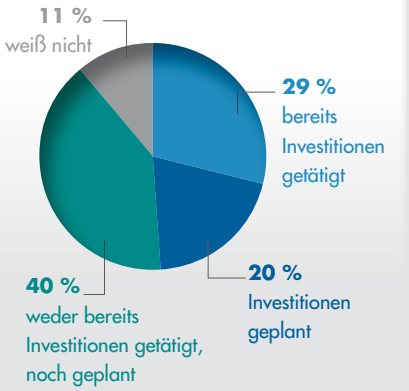
**48 %**
berichtete, dass sie für die Arbeit im Homeoffice auf ihre private technische Ausstattung angewiesen waren, da ihr Unternehmen ihnen das benötigte Equipment nicht bereitstellte

**22 %** erklärte, aufgrund dieser Einschränkungen das Gefühl zu haben, weniger produktiv zu sein

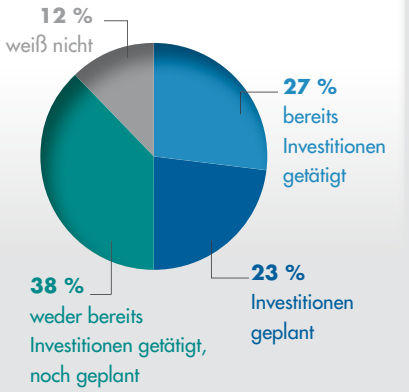
## DIGITALISIERUNGSSCHUB

**Welche der folgenden digitalen Investitionen hat Ihr Unternehmen bereits getätigt/plant Ihr Unternehmen in Folge der Krise?**

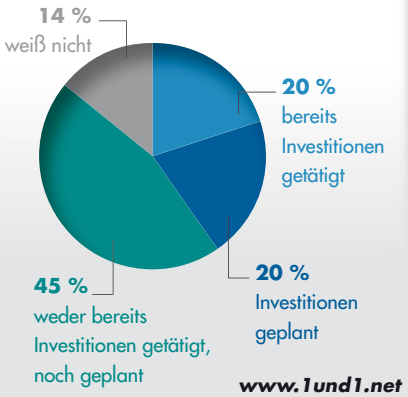
**Neue Vernetzungslösungen**
(VPN-Zugänge, Cloud Services)




**Verstärkter Schutz**
von Daten und Infrastruktur




**Digitale Workflows**




***www.1und1.net***

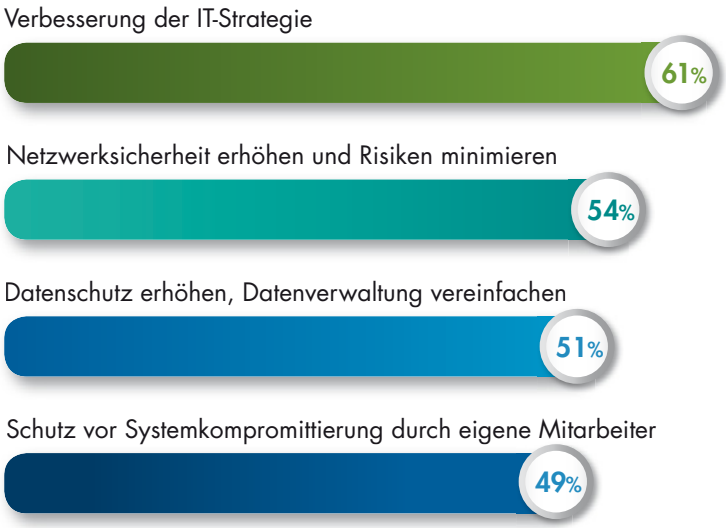
# ZERO TRUST

## FÜR MEHR IT SICHERHEIT

Unsichere Endgeräte, Phishing-Attacken und Datenpannen nehmen deutlich zu. Das ist ein Ergebnis der aktuellen Studie von Gigamon, einem Anbieter für Netzwerktransparenz und -Analyse für hybride Cloud-Strukturen. Vor dem Hintergrund der aktuellen digitalen und wirtschaftlichen Lage zeigen die Ergebnisse der Studie die künftigen Herausforderungen, vor der IT- und Sicherheitsentscheider stehen, ihre Prioritäten für die nächsten 12 Monate und insbesondere ihre Einstellung zu Zero Trust.

***www.gigamon.com***

**DIE WICHTIGSTEN GRÜNDE FÜR DIE IMPLEMENTIERUNG VON ZERO TRUST**



# RETHINK YOUR WORK

## TRANSFORMATION AUF ALLEN EBENEN IST DAS GEBOT DER STUNDE

Die Arbeitswelt in den Unternehmen wird immer komplexer. Einen Stillstand kann sich kein Unternehmen leisten. Joerg Hartmann, Geschäftsführer bei Konica Minolta in Deutschland und Österreich im Gespräch mit Ulrich Parthier, Publisher it management, über die vielfältigen Veränderungen der Geschäftswelt.

**Ulrich Parthier:** *Herr Hartmann, Sie selbst sind jetzt seit einem Jahr bei Konica Minolta Geschäftsführer. Welche Veränderungen haben Sie erlebt, positiv wie negativ?*

**Joerg Hartmann:** Einmal abgesehen von Corona war das für mich eine Zeit, die ich als sehr positiv erlebt habe. Die schwierigen Monate seit März 2020 haben uns als Unternehmen sicher fokussiert und wenn wir uns am Anfang des Jahres vorgenommen hatten, uns noch mehr zu einer digitalen Company zu entwickeln, dann haben wir das schon wenige Monate später besser als jemals erwartet umgesetzt.

**Ulrich Parthier:** *Konica Minolta hat also das erste halbe Jahr in der Corona-Krise gut überstanden? Wie schwierig war der Schritt ins Homeoffice? Und was wird das #newnormal der Zukunft sein?*

**Joerg Hartmann:** Als Pionier in Sachen digitaler Transformation haben wir schon frühzeitig auf das Thema „Mobile Working" gesetzt, sowohl intern als auch extern. Das kam uns natürlich im Frühjahr zugute, die Mehrheit unserer Mitarbeiter konnte einfach im Homeoffice weitermachen. Dass unsere Servicetechniker auch während des Lockdowns vor Ort bei Kundeneinsätzen tätig waren, beweist die Flexibilität unserer Organisation. Das #newnormal sehe ich für viele Unternehmen als hybride Arbeitsform – kreative Zusammenarbeit im Office, daily work – wo es möglich ist – als „Mobile Working". In Zeiten von Corona bedeutet das natürlich Homeoffice.

**Ulrich Parthier:** *In jeder Krise gibt es Gewinner und Verlierer. Wie hat Konica Minolta als weltweit agierendes Unternehmen auf die Krise reagiert?*

**Joerg Hartmann:** Ich denke nicht, dass wir uns als typischen Gewinner bezeichnen können. Dennoch haben wir die vergangenen Monate, auch dank sinnvollem Einsatz von Kurzarbeit, gut gemeistert. Als Organisation, und das ist mir besonders wichtig, sehe ich uns auf jeden Fall als Gewinner. Nur ein Beispiel: Wir haben sehr schnell Tools für unsere Kunden zur Verfügung gestellt, die es Ihnen erlauben, Konica Minolta Systeme auch ohne Vor-Ort-Besuch eines Servicetechnikers im Fehlerfall selbst zu reparieren. Viele Kunden waren sehr dankbar, dass Firmenfremde nicht in das Unternehmen kommen mussten. Ohne die Corona-Krise hätten wir solche Unterstützungs-Tools, die auf Augmented Reality basieren, vielleicht erst viel später angeboten.

**Ulrich Parthier:** *Für viele Ihrer Kunden waren die vergangenen Monate schwierig. Was benötigen diese am dringendsten?*

**Joerg Hartmann:** Was die meisten Kunden benötigen ist das, was wir als den „intelligenten vernetzten Arbeitsplatz" bezeichnen. Basis dafür ist eine vernünftige, stabile Netzwerkinfrastruktur, die mit einem soliden IT-Security- Konzept abgesichert wird. Im nächsten Schritt sollte dann überprüft werden, ob die Prozesse und Abläufe im Unternehmen auch tatsächlich für den „new way of work" geeignet sind. Ob es, zum Beispiel, eine digitale Lösung gibt, die Unterschriften auf dem Papier ersetzen kann, wenn die Verantwortlichen nicht im Haus sind. Zudem muss auch die Unternehmenskultur überprüft werden, ob ein Modell der Vertrauensarbeit, wie im mobile work benötigt, auch tatsächlich im Unternehmen umgesetzt werden kann.

**Ulrich Parthier:** *Das Anbieterbewertungsmodell von IDC MarketScape verschafft Anwendern einen Überblick über die Wettbewerbsfähigkeit von ITK-Anbietern. Nun ist ihr Unternehmen ja im aktuellen IDC MarketScape zu einem der weltweit führenden Unternehmen für Print-Transformation ernannt*

ICH BIN DAVON ÜBERZEUGT, DASS NACHHALTIGKEIT FÜR UNTERNEHMEN DER SCHLÜSSEL ZU EINER SICHEREN UND ERFOLGREICHEN ZUKUNFT IST.

Joerg Hartmann, Geschäftsführer, Konica Minolta Deutschland und Österreich, www.konicaminolta.de


STILLSTAND
KANN SICH KEIN
UNTERNEHMEN LEISTEN!

*worden. Was kann sich der Leser darunter vorstellen?*

**Joerg Hartmann:** Die Anfänge von Konica Minolta liegen im Bereich der Fotografie und in den fast 150 Jahren unseres Bestehens haben wir uns ständig damit auseinandergesetzt, wie wir mit unserem Know-how unsere Kunden und deren Kunden bestmöglich unterstützen können. So haben wir im Lauf der Jahre Medizintechnik und Drucksysteme in unser Programm aufgenommen und sind heute ein weltweit agierender IT-Konzern mit Angeboten im Bereich Security, Voice-over-IP, Enterprise Content Management, Outsourcing von Geschäftsprozessen und spezifischen vertikalen ERP- und CRM-Lösungen. Diese ständige Bereitschaft zum Wandel zeichnet Konica Minolta aus. Das wird uns auch immer wieder bestätigt, in diesem Jahr erzielten wir Top-Platzierungen als bestes Systemhaus Deutschlands und als bester Managed Service Provider. Und eben auch die Bestätigung des IDC MarketScape, wo in der Auszeichnung festgehalten wird, dass „.....Kunden, die nicht nur eine Aktualisierung ihres Drucker-/MFP-Portfolios, sondern eine Vision von der Entwicklung des Arbeitsplatzes in die Zukunft wollen, Konica Minolta in Betracht ziehen sollten".

**Ulrich Parthier:** *Immer bedeutender wird in Organisationen die Security-Komponente. Jetzt in der Krise und in der Zukunft: Wie wird sich das Arbeiten verändern? Und: Wie stellen wir sicher, dass Unternehmen ganzheitlich gesichert sind?*

**Joerg Hartmann:** Konica Minolta sichert seine MFPs mit bizhub SECURE ab. Diese Services enthalten Sicherheitsfunktionen wie Zugriffssteuerung und -kontrolle ebenso wie Festplattenverschlüsselung oder automatisiertes Löschen gespeicherter Daten. Aber für uns ist das erst der Anfang: Wir bieten umfassende „Endpoint Protection"-Leistungen, die nicht nur mobile Endgeräte, sondern auch Workstations und Server vor Malware-, Trojaner- oder Ransomware-Befall schützen. Dazu überprüfen wir die Netzwerk-Security und helfen, eine funktionierende Balance zwischen Sicherheit, Flexibilität, Innovation, Komfort und Geschwindigkeit zu erreichen. Und wenn einmal doch etwas passiert, kann eine von uns erstellte IT-Notfallplanung den möglichen Schaden minimieren. Schließlich sollten auch unbewachte Gebäude nicht vergessen werden, hier können wir mit Video Security Services hohe Sicherheit bieten.

**Ulrich Parthier:** *Beim Thema Umwelt kommen wir zwangsläufig auf die Aspekte Green IT und Nachhaltigkeit. Welche Rolle spielen die für ihre Kunden wie für das Unternehmen Konica Minolta?*

**Joerg Hartmann:** Ich bin davon überzeugt, dass Nachhaltigkeit für Unternehmen der Schlüssel zu einer sicheren und erfolgreichen Zukunft ist. Nachhaltiges Wirtschaften und Umweltschutz sind schon lange wichtige Handlungsfelder bei Konica Minolta, die in unserer Eco Vision 2050 verankert sind. Beispielsweise sind wir in der FTSE4Good-Indexreihe, einem der bekanntesten Indizes der Welt für verantwortungsbewusstes Investieren, seit 17 Jahren in Folge vertreten.

**Ulrich Parthier:** *Zu guter Letzt noch ein Ausblick – Was wird sich verändern, was wird bleiben?*

**Joerg Hartmann:** Ich habe zuvor schon den intelligenten vernetzten Arbeitsplatz als das neue Modell erwähnt, das „Mobile Working" und eine hybride Arbeitswelt beinhaltet, die es auch ohne Corona als treibende Kraft noch geben wird. Er bedingt auch, dass sich Unternehmen digital transformieren und die Chancen, die darin liegen, wahrnehmen. Schließlich werden Unternehmen noch viel mehr auf Sicherheit achten müssen, die ein zentraler Bestandteil der Unternehmensstrategie werden wird. In all diesen Bereichen begleiten wir schon heute viele unserer mehr als 30.000 Kunden in Deutschland und sind ein geschätzter Partner bei diesen Themen.

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

# SELBSTORGANISATION BRAUCHT FÜHRUNG

## DIE EINFACHEN GEHEIMNISSE AGILEN MANAGEMENTS


**Selbstorganisation braucht Führung – Die einfachen Geheimnisse agilen Managements; Boris Gloger, Dieter Rösner, Carl Hanser Verlag, 2017**

Dieses Buch räumt mit dem Klischee auf, dass Scrum und andere agile Managementmethoden funktionieren, wenn man Teams einfach sich selbst überlässt. Agilität befreit vor allem die mittleren Manager nicht von ihrer Verantwortung. Ganz im Gegenteil: Agile Selbstorganisation braucht Führung in ihrer besten Form – sie braucht Manager, die sich ihrem Menschsein stellen.

**Vom Anreizsystem zum Anerkennungssystem**

- Erfahren Sie, warum agile Unternehmenskulturen mehr Führung denn je brauchen
- Systemisches Hintergrundwissen hilft Ihnen, die Prinzipien der Selbstorganisation zu verstehen
- Schaffen Sie mit einfachen Werkzeugen den Rahmen für Selbstorganisation
- Lernen Sie aus den Erfahrungen, Erfolgen und Misserfolgen der Autoren als Manager
- Nutzen Sie die Tipps und Übungen, um Ihr persönliches Führungsverständnis zu formen

Boris Gloger und Dieter Rösner zeigen, wie eng Agilität, Teamentwicklung und Führung miteinander verwoben sind. Die Theorie bleibt im Hintergrund – es ist keine „agile Führungslehre", die hier entworfen wird. Erzählt wird von den persönlichen Krisen, vom eigenen Scheitern und dem Erkennen, wie Selbstorganisation gelingt.


**Content Design – Durch Gestaltung die Conversion beeinflussen; Robert Weller, Ben Harmanus; Carl Hanser Verlag, 01/2021**

# CONTENT DESIGN

## DURCH GESTALTUNG DIE CONVERSION BEEINFLUSSEN

Die Autoren erklären Ihnen, wie Sie mit psychologischen Triggern aus Besuchern Ihrer Website Newsletter-Abonnenten, Leads und Kunden machen und wie Sie durch Content-Optimierung nachhaltig Ihre Umsätze steigern.

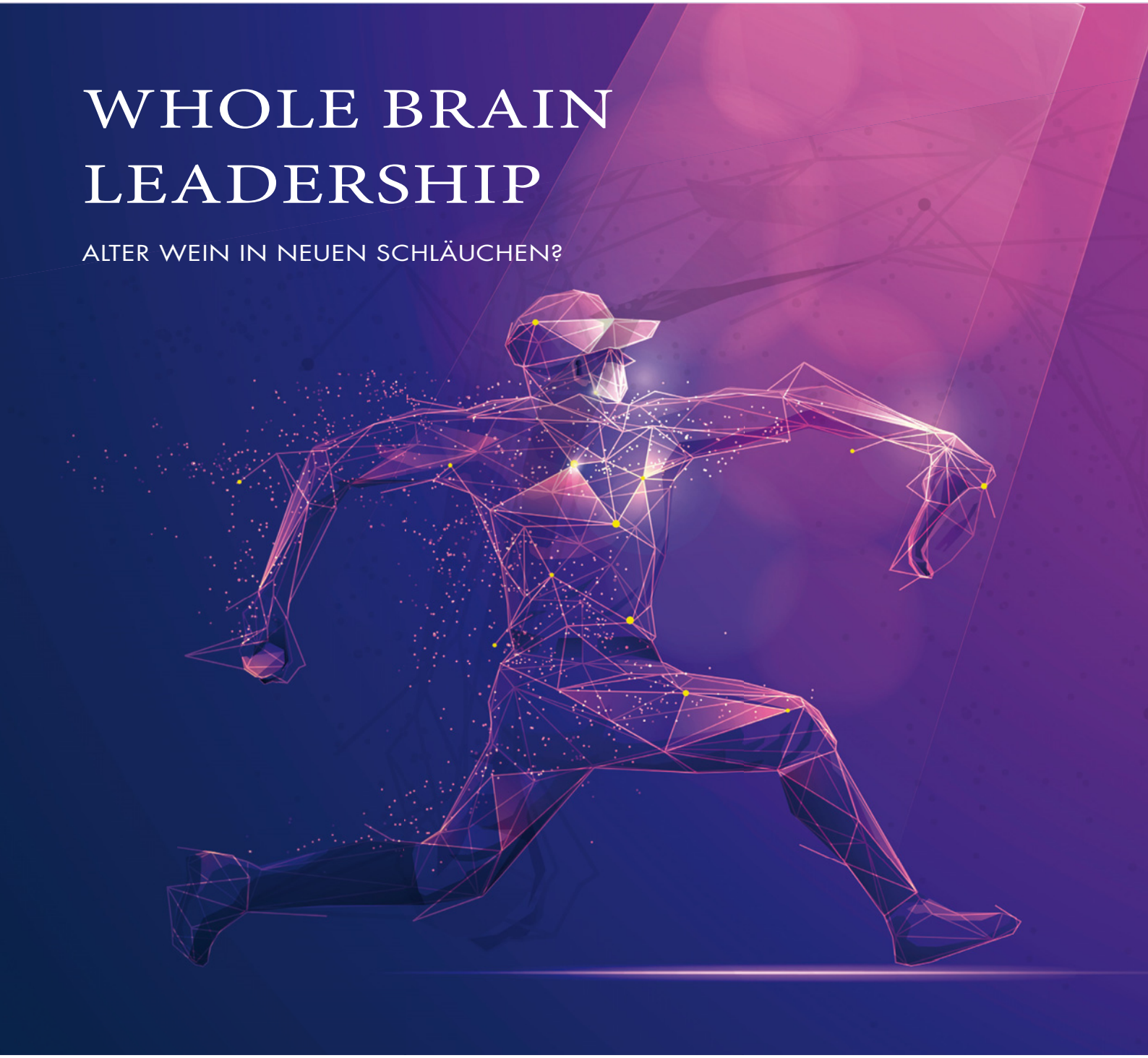
Sie erhalten eine Übersicht über die Voraussetzungen für erfolgreiches Content Design sowie eine klar strukturierte Einführung in die Gestaltung und Konzeption digitaler Inhalte – insbesondere Text, Bild, Video und Audio.

Profitieren Sie nicht nur vom Expertenwissen der Autoren, sondern auch von erfahrenen Marketingverantwortlichen bei Facebook, Zalando, Pixum und LogMeIn. Mithilfe der Tipps zur Content- und Conversion-Optimierung sowie passenden Tool-Empfehlungen haben Sie alles was Sie brauchen, um Ihr eigenes Content Marketing auf den nächsten Level zu heben.

Mit ihrem Buch richten sich Robert Weller und Ben Harmanus sowohl an Einsteiger als auch an erfahrene Online-Marketing-Manager, die nicht nur einzelne Aufgaben schnell umsetzen, sondern den Zusammenhang von Content und Design in Bezug auf das Marketing in seiner Vielschichtigkeit verstehen wollen. Zahlreiche visuelle Beispiele, bewährte Tipps aus der Marketingpraxis sowie Erfahrungsberichte, Worksheets und Checklisten helfen dabei.

# WHOLE BRAIN LEADERSHIP

## ALTER WEIN IN NEUEN SCHLÄUCHEN?



Thought Leadership, Market Leadership, Situational Leadership, Whole Brain Leadership, es gibt viele Variationen von Leadership. „Whole Brain Leadership" ist ein relativ neuer Begriff, der im vergangenen Jahr in einer Studie von Accenture Strategy untersucht wurde und deren wichtigsten Ergebnisse wir nachfolgend zusammengefasst haben.

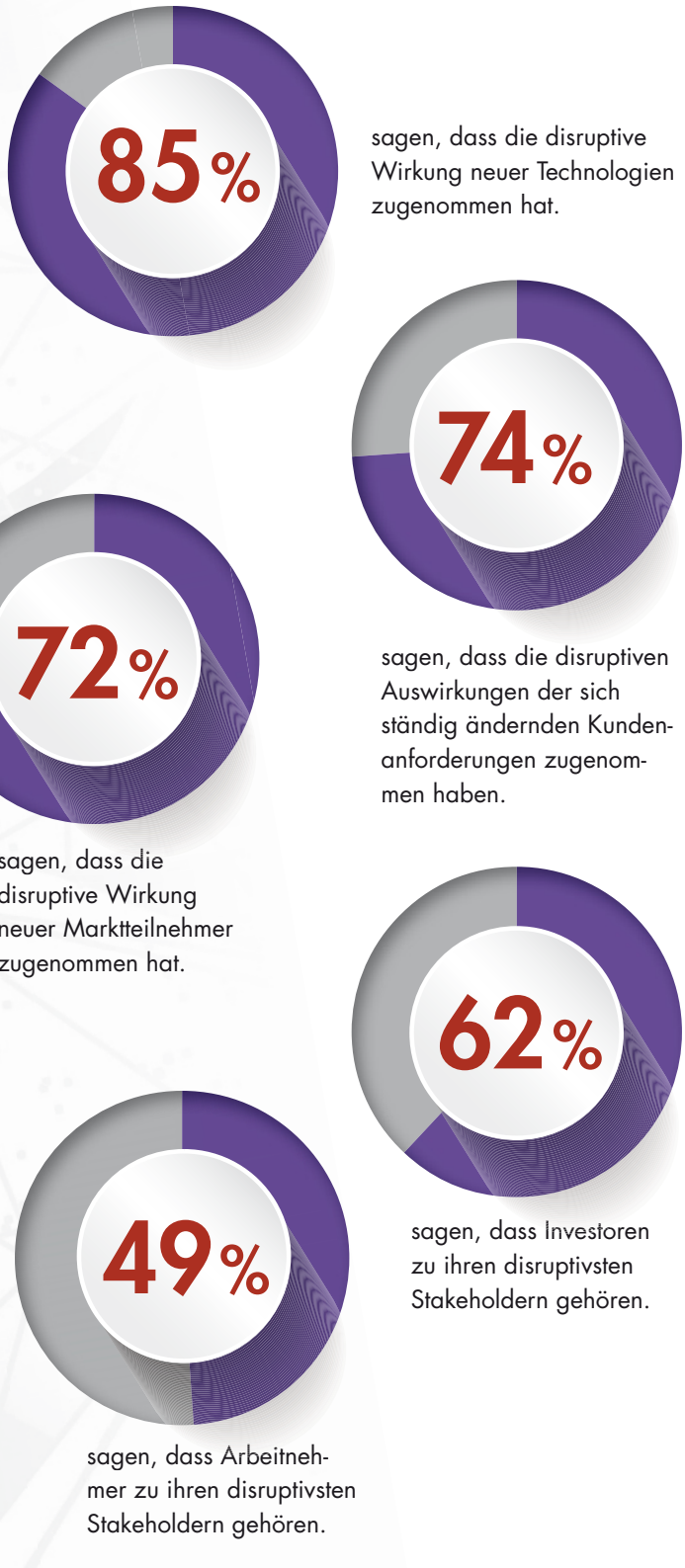
Zunächst einmal beschreibt er einen ganzheitlichen Ansatz, der die traditionellen datenbasierten (rationalen) Ansätze mit emotional orientierten Aspekten ausbalanciert. Im Kontext von Digitaler Transformation und disruptiven Technologien gilt es, wettbewerbsfähig und agil zu bleiben. Davon betroffen ist natürlich auch die IT.

Die Zahlen sprechen für sich. Nach Angaben von Accenture erzielen Top-Manager die einen solchen Ansatz verfolgen, im Durchschnitt 22 Prozent mehr Umsatz und eine um 34 Prozent bessere Rentabilität. Das ist beeindruckend.

**BILD 1:**

## DIE DISRUPTIONSWELLE UND IHRE FOLGEN

– DAS C-MANAGEMENT STEHT VON VIELEN SEITEN GEHÖRIG UNTER DRUCK UND MUSS LIEFERN.




Die Studie unterscheidet verschiedene Gruppen von Kunden und Mitarbeitern, abhängig von a) ihrer Selbsteinschätzung, welchen Einfluss sie auf die Geschäftsaktivitäten von Unternehmen haben und b) ob ihnen ihr eigener Vorteil oder der der Allgemeinheit wichtiger ist. Die wichtigste Gruppe für Top-Manager ist dabei diejenige, die im folgenden „Pathfinders" genannt wird. Ihnen sollten Unternehmen eine besondere Bedeutung beimessen.

Denn „Pathfinders" sind Mitarbeiter und Kunden, die der Meinung sind, dass sie selbst Veränderungen in Unternehmen, für die sie arbeiten oder deren Produkte und Services sie kaufen, bewirken können. Statt sie nur als eine weitere destabilisierende Kraft wahrzunehmen, sollte man sie als wichtige Impulsgeber für Veränderungen betrachten.

Die Gruppe definiert sich mehr durch ihre besondere Denkweise, als durch demografische Gemeinsamkeiten. Sie sind über alle Altersgruppen hinweg vertreten. Wenn Top-Führungskräfte mit „Pathfinders" interagieren, werden sie feststellen, dass diese besondere Gruppe die Macht besitzt, die Art von Veränderung herbeizuführen und zu beschleunigen, die auch Unternehmensführer schaffen müssen, um wettbewerbsfähig zu bleiben.

Denn die Studie zeigt, das fast Dreiviertel der „Pathfinder" überzeugt sind, dass sie das Potenzial haben, den wirtschaftlichen Wert eines Unternehmens zu zerstören. Sollten ihre Erwartungen ignoriert werden, dann darf man ihnen trotzdem getrost einen gewissen Hang - mindestens zur Selbstüberschätzung - wenn nicht zum Größenwahn attestieren.

Spitzenmanager sind sich der Macht und des Potenzials dieser Gruppe selten bewusst. Das ist ein weiterer wichtiger Faktor und gleichzeitig eine schlechte Nachricht. Die gute Nachricht: „Pathfinder" haben großen Einfluss. Als Mitarbeiter machen sie schnell Karriere auf Führungsebene, denn sie verfügen über entscheidende Kompetenzen. Der Vorteil: Wenn

sich Top-Manager auf die Gruppe der „Pathfinder" einstellen, gewinnen sie wertvolle Verbündete und können mit ihrer Unterstützung die digitale Transformation besser vorantreiben. Eine wichtige Voraussetzung, damit die Führungskräfte selbst und auch ihre Unternehmen auf Erfolgskurs gehen können.

Derzeit geben allerdings nur acht Prozent der Top-Manager an, dass sie einen Whole Brain-Ansatz in ihren Unternehmen verfolgen. 82 Prozent räumen ein, dass sie zukünftig einen solchen Ansatz implementieren werden.

**Erwartungen**

Die Accenture Studie zeigt, dass die „Pathfinder" das Top-Management dazu antreiben, neue Wege der Führung, des Wachstums und der Nachhaltigkeit zu gehen. Denn sie wünschen sich eine Unternehmensführung, die ihre Anliegen, Prinzipien und Fähigkeiten teilt und umsetzt. „Pathfinder" wünschen Führungskräfte, die einen ausgewogenen Mittelweg zwischen Analytics-getriebenen und menschlichen Fähigkeiten schaffen.

Der Whole-Brain-Leadership-Ansatz verbindet Fähigkeiten der logisch-rationalen linken Gehirnhälfte wie Datenanalyse und kritische Beweisführung mit den kreativen Fähigkeiten der rechten Gehirnhälfte, die für Intuition und Empathie zuständig ist. Werden die beiden Kompetenzbereiche zusammengeführt, können Probleme besser gelöst und Mehrwert geschaffen werden.

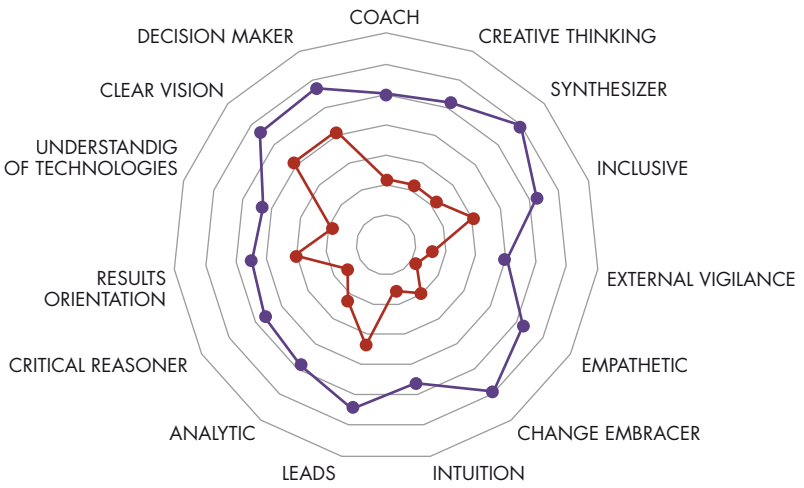
**Top-Management vs. Pathfinder**

Top-Manager schätzen Whole-Brain-Fähigkeiten - jedoch nicht in dem Maße, wie die „Pathfinder". Hier können Führungskräfte ansetzen, um die Lücke zwischen dem, was ist und dem, was erwartet wird, zu schließen.

65 Prozent der Top-Manager denken, dass die Fähigkeiten ihrer rechten Gehirnhälfte schwächer ausgeprägt sind und erkennen, dass sie die Fähigkeiten dieser Gehirnhälfte – wie Empathie oder Intuition – für einen ausgeglichenen Whole-Brain-Ansatz stärken müssen.

**BILD 2:**
**UNTERSCHIEDE IN DER BEURTEILUNG VON SCHLÜSSELQUALIFIKATIONEN**

DEUTSCHLAND




Quelle: Accenture

**Was ist zu tun?**

Die Autoren der Studie um Peter Lacy, Katherine LaVelle und Alberto Zamora sind der Meinung, dass folgende Punkte zu planen und umzusetzen sind:

**1.** Kompetenzlücken schließen. Neun von zehn Top-Manager ergreifen Maßnahmen und nutzen interne und externe Möglichkeiten, um eine Balance ihrer Whole-Brain-Fähigkeiten zu erreichen. Mehr als die Hälfte der befragten Führungskräfte berichten, dass sie sich selbst aktiv bemühen, neue Fähigkeiten zu erlernen. 46 Prozent setzen auf externe Ressourcen und neue Mitarbeiter.

**2.** Traditionelle Führungsrollen neu definieren: Es ist überlebenswichtig, dass Potenzial der „Pathfinder" zu nutzen. Wenn Führungskräfte diese Gruppe ernst nehmen, ihre Stimme auch bis in die obersten Vorstandskreise gehört und sich auf ihre Erkenntnisse gestützt wird, gewinnen sie Verbündete und stärken außerdem die eigene Glaubwürdigkeit und Führungsrolle. Wenn „Pathfinder" mit den Werten eines Unternehmens einverstanden sind, sind sie hochmotiviert. Dann geben sie nicht nur das Beste für ihren Arbeitgeber, sondern werden auch einer teureren Marke den Vorzug geben. Unternehmen können also von den „Pathfinders" als natürlichen Motor für Veränderung profitieren.

**3.** Grundlegende und weitreichende Veränderungen vorantreiben: Die richtige Kombination verlangt Fingerspitzengefühl. Top-Manager müssen ein ausgewogenes Kompetenzspektrum verinnerlichen und dies in ihrer Organisation und auch persönlich einsetzen. Damit wird es möglich, einen Whole-Brain-Ansatz durchzusetzen, um die komplexen Probleme der Disruption zu lösen. Wenn Führungskräfte datengetriebene und menschliche Fähigkeiten in einem ausgewogenen Verhältnis als neue Norm im Unternehmen nutzen, erreichen sie mehr kurz- und langfristige Geschäftserfolge und steigern ihre Wettbewerbsfähigkeit.

***Ulrich Parthier***

Weitere Infos finden Sie hier:
***https://accntu.re/3jkp6ad***

# KREATIVE KONZEPT-FINDUNG

## PROJEKTE STARTEN MIT DESIGN THINKING

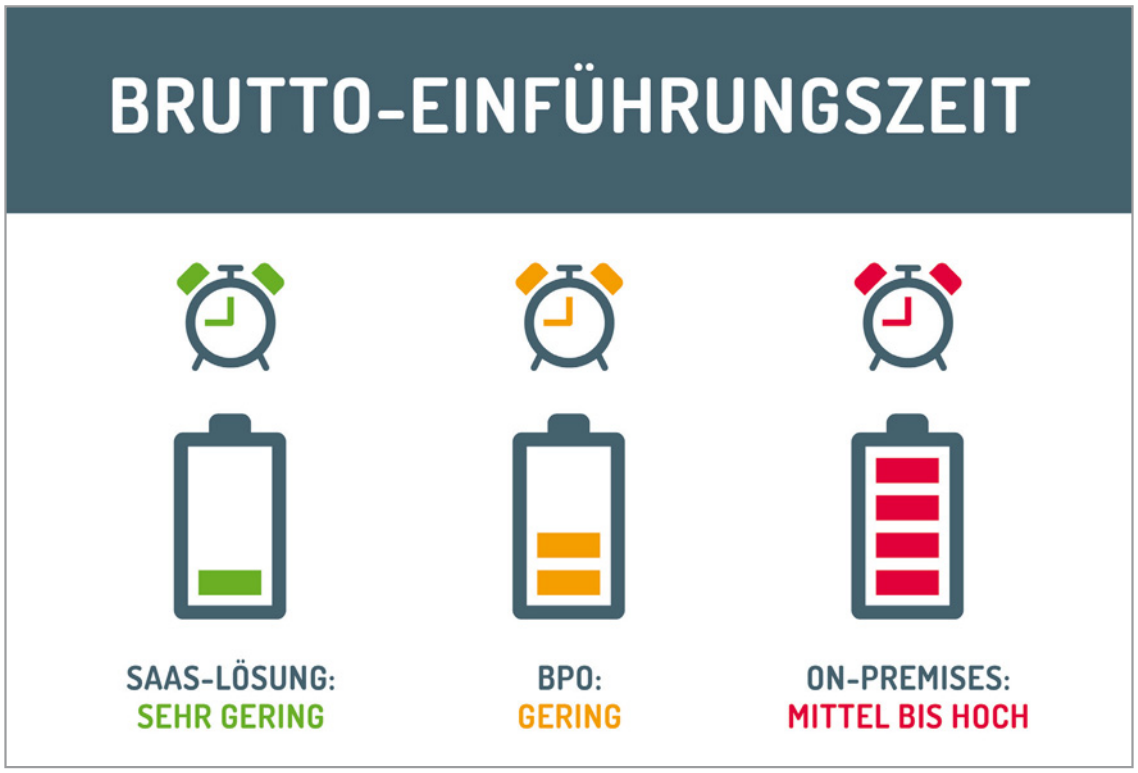
Projektarbeit gehört in vielen Unternehmen zur Tagesordnung. Ob Digitalisierung, Innovationsvorhaben, Change oder neue Produkte und Services, sie haben eins gemein: Sie starten als Projekt. Design Thinking hilft, sie zum Erfolg zu führen.

Doch für welche Projektthemen eignet sich Design Thinking? Wie lassen sich cross-funktionale Teams aufstellen? Welche Voraussetzungen braucht die Kreativarbeit noch?

Jens Otto Langes Buch gibt Antworten auf diese Fragen. Konkret und anschaulich illustriert es den Einsatz von Design Thinking für den Start und das Scoping von Projekten. Schritt für Schritt zeigt es auf, wie du Design Thinking-Workshops planst, um schnell Konzeptideen für komplexe Fragestellungen zu entwickeln.

Langes Playbook lädt zum Mitmachen und Mitdenken ein und vermittelt praxisorientiert die Anwendung der wichtigsten Denkwerkzeuge für die Gestaltung kreativer Konzeptfindungsprozesse zur Lösung komplexer Problemstellungen.


Projekte starten mit Design Thinking, Jens Otto Lange, Business Village 2020




# ON-PREMISES, SAAS ODER OUTSOURCING

## HABEN WIR EINE WAHL? ODER SIND WIR NICHT LÄNGST GETRIEBENE? (TEIL 2)

Untersuchungen zeigen, dass die Veränderungsgeschwindigkeit seit über einhundert Jahren kontinuierlich zunimmt. Im letzten Jahrhundert ist sie bereits „schneller" geworden als die durchschnittliche Reaktionsgeschwindigkeit von Unternehmen. Umso wichtiger ist es, dass Unternehmen die Veränderung strategisch angehen. Welche Vorteile Business Process Outsourcing (BPO) und Software as a Service (SaaS) dabei bieten, wurde im ersten Teil dieses Artikels (erschienen in der it-management Ausgabe 10-2020) beleuchtet. Dieser Beitrag widmet sich dem praktischen Einsatz.

**Cloud-Service oder BPO**

Für beide Konzepte gilt: Die Mitspieler müssen an der richtigen Position spielen. Der Einsatz cloudbasierter Services genauso wie das Outsourcing von Geschäftsprozessen bergen vor allem die Chance, Veränderungsprozesse selbstbestimmt zu gestalten, ohne von außen getrieben zu sein. Der Erfolg stellt sich dann ein, wenn Anbieter und Servicenutzer klare, verbindliche Erwartungshaltungen abstimmen. Bei einem einfachen cloudbasierten Service ist das gegebenenfalls schnell erledigt. Bei der Auslagerung von Prozessen muss mehr Zeit investiert werden, um die Übergänge und vorhandenen Erwartungen abzugleichen. Denn auch in einer scheinbar kurzlebigen Welt möchten weder der Anbieter noch der Servicenutzer das Rad ständig neu erfinden, sondern eine erfolgreiche und langfristige Geschäftsbeziehung auf Augenhöhe führen. Das bedeutet keinesfalls, dass immer alles harmonisch verlaufen muss und wird. Ein fairer Umgang führt jedoch dazu, dass beide Seiten auf Dauer erfolgreich bleiben und Spaß dabei haben. Das ist insbesondere bei BPO-Projekten ein wesentlicher Garant fürs Gelingen.

Ein Service-Level-Agreement (SLA) schafft hier Klarheit für alle Beteiligten, was genau an Leistung, Verfügbarkeit, Funktionalität und Performance auf beiden Seiten erwartet wird.

**Drei Strategien**

Ein gutes Beispiel zur Veranschaulichung der Ansätze in der Praxis ist die Digitalisierung von Dokumenten. Im Purchase-to-Pay- oder Order-to-Cash-Prozess erreichen unstrukturierte Daten die Unternehmen. Das sind Papierbelege, Faxe oder auch E-Mails. Teilweise liegen die

Belege zwar in digitaler Form vor, jedoch sind die prozessrelevanten Informationen nicht strukturiert vorhanden.

Die Digitalisierung beschreibt, welche Informationen von einem Beleg zum Beispiel in ein ERP-System übertragen werden müssen. Bei einer Rechnung sind das die Angaben, die etwa nach dem Umsatzsteuergesetz erforderlich sind, bei einer Auftragsbestätigung ist es der Bezug zur Bestellung oder das abweichende Lieferdatum, bei einem eingehenden Kundenauftrag liegt das Augenmerk eher auf den zu liefernden beziehungsweise zu fertigenden Positionen.

Selbstverständlich kann heutige Software Daten auslesen und bereitstellen. Zumal standardisierte Formate wie EDIFACT, ZUGFeRD oder XRechnung genau dabei unterstützen sollen. Völlig ohne Personal geht es jedoch in den seltensten Fällen, denn irgendjemand muss zumindest die Post bearbeiten.

In dem hier beschriebenen Teilprozess geht es also um die Aufbereitung eingehender Belege und die Erfassung aller relevanten Daten aus dem Dokument:

## On-Premises

Bei einer On-Premises-Lösung übernimmt das Unternehmen diesen Job komplett selbst. Es kauft die Software zur Digitalisierung, stellt die IT-Infrastruktur, die Serverrechenleistung, die Prozessorganisation sowie das Fachpersonal für die komplette Anwendungs- und Betriebsbetreuung. In den vergangenen 15 Jahren war dies das bevorzugte Modell des Mittelstands.

## SaaS

Bei einer Cloud-Lösung kann das Unternehmen, die vorher On-Premises betriebene Software aus der eigenen Verantwortung in die Verantwortung des Cloud-Anbieters geben. Die Vorteile sowie Herausforderungen einer solchen SaaS-Lösung wurden bereits im ersten Teil des Artikels näher erläutert: Verfügbarkeit, Funktionalität und neueste Technologien sind immer in der aktuellen Nutzung.

UNTERNEHMEN MÜSSEN SICH DIE FRAGE STELLEN, OB ES NOCH ZEITGEMÄSS IST, ADMINISTRATIVE GESCHÄFTSPROZESSE IM EIGENEN HAUS DURCHZUFÜHREN.

Sven Schal, Geschäftsführer AFI Solutions GmbH, www.afi-solutions.com

Der On-Premises-Anteil entfällt und der Betrieb der Lösung in Bezug auf den Teilprozess wird erheblich leichter. Das Know-how, wie genau mit den digital gewonnenen Daten umgegangen wird oder wie die eingehende Post vorsortiert werden muss, liegt weiterhin beim Fachpersonal des Unternehmens.

## BPO

In der BPO-Variante wird der Teilprozess komplett ausgelagert. Für die reine Digitalisierung im obigen Sinne ist nur noch der Serviceanbieter zuständig. Ein SLA regelt auch hier, wie mit der eingehenden Post – egal ob elektronisch oder in Papierform – umzugehen ist, welche Zeiträume für die Bearbeitung zur Verfügung stehen, und welche Datenqualität im Zielsystem erwartet wird.

## Aktuelles Beispiel: Mehrwertsteuersenkung

Ein schönes aktuelles Beispiel, um alle Ansätze nochmal zu verdeutlichen, ist die Mehrwertsteuersenkung seit 1. Juli 2020. Diese Umsetzung musste nun kurzfristig in allen drei Umgebungen eingerichtet werden.

➤ Im Falle des ausgelagerten Prozesses (BPO) hat das Unternehmen schlichtweg kein To-Do: Es liegt komplett in der Verantwortung des Servicedienstleisters, sich um die technische Umsetzung zu kümmern und die entsprechenden, korrekten Daten ans Unternehmen zu liefern.

➤ Beim SaaS muss das Unternehmen den Fall innerhalb des Prozesses lösen, aber es kann sich darauf verlassen, dass die Software in der Cloud pünktlich in der Lage ist, die neuen Mehrwertsteuersätze zu erkennen und zuzuordnen.

➤ In der On-Premises-Welt bleiben alle Aufwände am Endkunden hängen, dieser muss es in der Software und im Prozess umsetzen. Hier braucht es dann Beratung, Unterstützung bei den entsprechenden Software-Einstellungen sowie eventuell anstehende Software-Updates. Gerade bei On-Premises könnte die Zeit zum kritischen Faktor werden.

## Fazit: Sie haben die Wahl

Sie haben eine starke IT und ausreichend Personal? Dann kann auch On-Premises die richtige Lösung für Sie sein. Unsere Erfahrung ist, dass die meisten Unternehmen nicht möchten, dass die eigenen Fachleute ihre wertvolle Zeit damit verschwenden, Belege anzuschauen und zu vergleichen, hier werden Teilprozesse gerne ausgelagert. Zumal es oft auch Schwankungen nach oben im Belegaufkommen gibt, die dann der Servicedienstleister auffangen muss.

Auf der anderen Seite gibt es Kunden, die beim Abgleich oder der Validierung von Belegen sehr viel Spezialwissen einsetzen, da passt dann Software as a Service. Das Unternehmen muss sich nicht mehr um die IT-Betriebsthemen kümmern, sondern kann sich darauf verlassen, dass die Software auf dem neuesten technologischen Stand ist – inklusive Compliance, Datensicherheit und Datenschutz.

Unternehmen haben die Wahl. Sie müssen sich nur die Frage stellen, ob es noch zeitgemäß ist und der eigenen Kernkompetenz entspricht, administrative Geschäftsprozesse im eigenen Haus durchzuführen.

***Sven Schal***

# CLOUD UND REGULATORIK

## COMPLIANT CLOUD COMPUTING

Wachsende Erwartungen der Kunden an digitale Services und der Zwang zur effizienten Prozessautomatisierung treiben die Modernisierung der IT voran. Die Finanzbranche muss dabei zusätzliche strenge Regularien erfüllen. Damit Audits effizient ablaufen, braucht es branchenerfahrene Dienstleister, die technische und regulatorische Anforderungen gleichermaßen im Blick haben.

Will ein Unternehmen die Übersetzung von Geschäftsprozessen in Cloud-native-Software auf Basis von Microservices vorantreiben, so braucht es Platform-as-a-Service-Provider. In Deutschland ist noris network so ein Anbieter, der in eigenen Hochsicherheitsrechenzentren Platform as a Service „Made in Germany" mit einem Technologie-Stack aus Docker-, Kubernetes- und Continuous-Delivery-Technologien bietet. „Wir wollen Unternehmen eine Lösung bieten, die sich auf den Migrationspfad Richtung Cloud begeben und eine sichere Umgebung für die agile Entwicklung und die hochskalierbare Bereitstellung von Microservices suchen", erläutert Stefan Keller, CMO bei der Nürnberger noris network AG. „Wir helfen auch dort, wo Cloud-Lösungen die performante Anbindung an Legacy-Lösungen brauchen, wo Entwicklerteams die Hilfe von erfahrenen DevOps bei Aufbau und Betrieb von Continuous Delivery Pipelines wünschen oder spezielle Sicherheitsbedürfnisse bestehen."

### Es gehört mehr dazu

Wenn bei der Modernisierung von IT-Plattformen einzig Fragen der technischen Umsetzung behandelt werden, kann es leicht passieren, dass Sicherheitsaspekte übersehen werden. Und IT-Sicherheit ist in vielen Branchen direkt mit der nachweislichen Einhaltung von Standards und Regelwerken verbunden. Wie kann ein IT-Dienstleister gewährleisten, dass Anforderungen, die nicht direkt mit der Funktion der betreuten Lösungen zusammenhängen, erfüllt werden – ja mehr noch, in einer Weise erfüllt werden, die effiziente Compliance-Nachweise erlaubt? Die Herausforderung: Banken und Versicherungen müssen im Bereich der IT eine große Zahl branchenspezifischer Audits bestehen. Diese werden von unterschiedlichen Organisationen durchgeführt: von Wirtschaftsprüfern über BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) und Bundesbank bis zu Experten der Anlagensicherungsfonds. So stehen Finanzdienstleistern nicht selten pro Jahr zehn große IT-Audits ins Haus, bei denen sich die Anforderun-

> WIR WOLLEN UNTERNEHMEN EINE LÖSUNG BIETEN, DIE SICH AUF DEN MIGRATIONSPFAD RICHTUNG CLOUD BEGEBEN UND EINE SICHERE UMGEBUNG FÜR DIE AGILE ENTWICKLUNG UND DIE HOCHSKALIERBARE BEREITSTELLUNG VON MICROSERVICES SUCHEN
>
> Stefan Keller, Chief Marketing Officer, noris network AG, www.noris.de

gen in der Praxis zudem laufend verschärfen. Ohne Kenntnis der sich aus der Regulatorik ergebenden praktischen Anforderungen und deren Auslegung durch die Prüfer, ohne echte Transparenz und eine detaillierte Dokumentation der Plattformen und Prozesse schon beim Aufbau der Cloud-Plattformen entstehen sehr schnell „Minenfelder", die die Unternehmen und deren IT-Verantwortliche später vor große Probleme stellen. Probleme bei Audits sind in der Finanzbranche keine „Schönheitsfehler", sondern werden bankenintern schnell eskaliert.

**Compliance-Durchsetzer**

Es braucht jemanden, der MaRisk (Mindestanforderungen an das Risikomanagement), MaComp (Mindestanforderungen an die Compliance-Funktion), MaSI (Mindestanforderungen an Sicherheitsmaßnahmen für webbasierte Bezahlsysteme und webbasiertes Onlinebanking), BAIT (Bankaufsichtliche Anforderungen an die IT) und all die anderen Rahmenbedingungen kennt und zugleich ein umfassendes Verständnis für die praktischen Implikationen der Vorschriften mitbringt. noris network hat dazu ein eigenes Servicekonzept entwickelt. Als sogenannte IT-Service-Manager stehen spezialisierte Mitarbeiter und Mitarbeiterinnen Finanzinstituten nicht nur als zentrale Ansprechpartner für alle von noris network bezogenen IT-Services, sondern zugleich als Fachleute mit Praxiswissen zu Compliance zur Seite. Die IT-Service-Manager übersetzen die spezifischen betriebswirtschaftlichen, geschäftsstrategischen und regulatorischen Anforderungen der Kunden in technische Anforderungen. Zu den Aufgaben gehören aktive Prozess- und Qualitätsoptimierung, Service-Continuity-Managementleistungen, Dokumentenlenkung, Begleitung des Risikomanagements und die Vorbereitung und Steuerung von Audits. Der Umfang der Dienstleistungen ist ausgehend von den Koordinations- und Kommunikationsaufgaben skalierbar.

Bildquelle noris network

Die Mitarbeiter, die den Kunden als IT-Service-Manager zur Seite gestellt werden, haben langjährige Erfahrung mit der Betreuung von Banken-IT und sind mindestens als IT-Service-Manager nach ISO 20000 oder als Auditoren von Managementsystemen nach ISO 19011 qualifiziert. „Mit der Auswahl eines IT-Dienstleisters wollen Banken die eigene Organisation entlasten. Diese Einsparungen sollten somit nicht durch aufwendige Kommunikationswege und Steuerung des IT-Dienstleisters aufgefressen werden. Aus diesem Grund bieten wir Banken kompetente Ansprechpartner, die deren geschäftliche und oft sehr spezifische regulatorische Anforderungen verstehen", erläutert Stefan Keller das Dienstleistungsangebot.

**Das müssen Cloud-Anbieter können**

Zur Erfüllung der strengen Auflagen, die der Finanzwirtschaft auferlegt sind, müssen Cloud-Anbieter ein enormes Leistungsspektrum abdecken können. Dazu zählen eben diese Compliance-Teams, die über ausreichende Erfahrungen im Umgang mit den speziellen Regularien verfügen. Noch besser ist es, branchenerfahrene Spezialisten des Dienstleisters in interne Gremien wie Service Review Boards, Change Advisory Boards, Information Security Management Boards oder in das Notfallmanagement im Rahmen des Business Continuity Managements zu integrieren. Sie können so Praxisaspekte und Lösungsvarianten direkt in die Beratungen einbringen und als Schnittstelle zum Dienstleister zugleich die Umsetzung beschleunigen.

Kompetentes Personal allein aber reicht nicht. Es besteht ein Unterschied zwischen IT-Sicherheit herstellen und dies auch jeweils Audit-gerecht dokumentieren zu können. Hierbei kommt dem Reifegrad des internen Kontrollsystems (IKS) des Dienstleisters eine zentrale Bedeutung zu. Lässt es kundenindividuelle Prozesse überhaupt zu oder sichert es lediglich allgemeine Standards? Wie schnell ist der Dienstleister tatsächlich zu kundenspezifischen Prozessdetails auskunftsfähig? Wie ist der Kunde eingebunden? In welchem Umfang sind Kontrollen von kundenspezifischen Maßnahmen technisch unterstützt und automatisiert? Wie werden die manuellen Prozesse tatsächlich beim Dienstleister gelebt?

**Fazit**

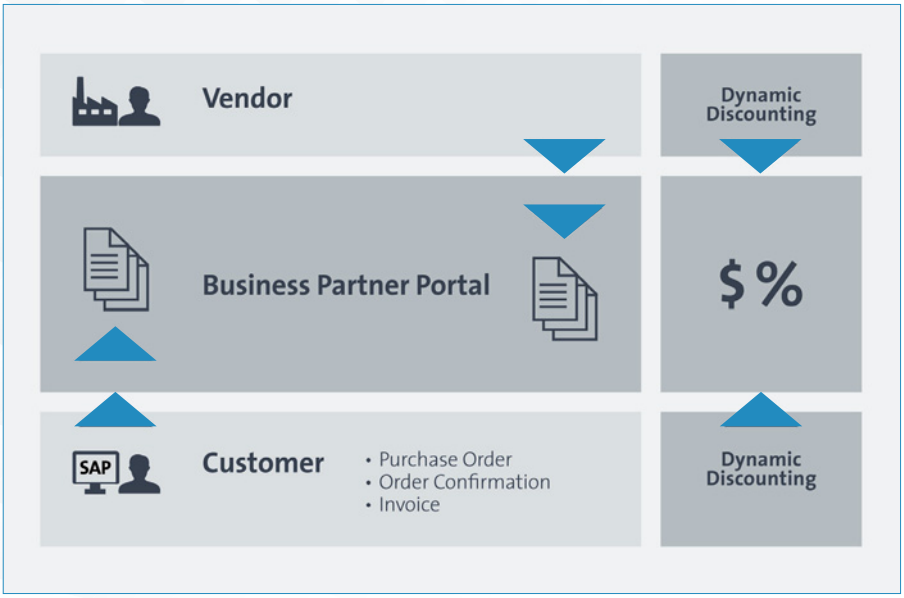
Höchste Sicherheitsstandards müssen nicht nur erfüllt, sondern in regulierten Branchen auch auditierfähig dokumentiert werden. Audits sollten als Teil der IT-Anforderungen verstanden werden. Cloud- und IT-Dienstleister sollten ein Unternehmen bei Audits fachlich und personell kompetent unterstützen.

***Peter Kronfeld***

# HYBRIDE CLOUD

## GESCHÄFTSPARTNERPORTAL IN DER SAP CLOUD PLATFORM

Wie man SAP mit eigenen Lösungen aus der Cloud verbindet, zeigt der Ahrensburger Softwarehersteller xSuite Group jetzt mit dem „xSuite Business Partner Portal Sphere" – einer Cloudanwendung für Unternehmen mit SAP ERP oder SAP S/4HANA im Einsatz. Diese können damit ihre Kommunikation sowie den Daten- und Dokumentenaustausch mit Lieferanten im Procure-to-Pay-Prozess automatisieren und zentralisieren. Durchgängiges Bestellen und Bezahlen in der Zusammenarbeit mit Lieferanten werden darüber digitalisiert und standardisiert.




### Automatische Datenübernahme

Einkauf, Buchhaltung und Lieferanten tauschen über das Portal alle mit der Beschaffung zusammenhängenden Daten und Dokumente aus, eine automatische Übernahme von Daten und Dokumenten aus dem Portal in das SAP-System entlastet Einkauf und Buchhaltung – eine Hybrid-Architektur wie aus dem Lehrbuch, die abermals zeigt: Wesentlich sinnvoller als ein reiner Public-Cloud-Betrieb ist es, wenn man Kernsysteme für individuelle Anforderungen on-premises einsetzt und sie um flexible Dienste aus der Cloud erweitert.

Betrieben wird das „xSuite Business Partner Portal Sphere" über die SAP Cloud Platform (SCP). Das ist ganz im Sinne des ERP-Herstellers, der es am liebsten sähe, wenn alle seine Kunden ihre Aktivitäten möglichst rasch und umfassend in die Cloud verlagern. Für die Entwicklung von Erweiterungen und Eigenprogrammierungen stellt der Konzern deshalb die SCP bereit. Vorteil für Unternehmen wie xSuite, die auf den Zug aufspringen: Die Kompatibilität ihrer Lösung mit aktuellen und zukünftigen SAP-Releases ist damit sichergestellt. Und für die Anwenderunternehmen entfällt die Aufgabe, mit jedem Release, mit jedem Update nachzuprüfen, ob noch alles stimmig läuft.

### Plattform für Dokumentenaustausch und Kommunikation

Einkaufsabteilungen arbeiten, wenn sie das neue Portal nutzen, wie gewohnt in ihrer SAP-Umgebung. Dort erzeugen sie ihre Bestellung und stellen sie anschließend dem Lieferanten automatisch im Portal zur Verfügung. Der hat sie damit sofort vorliegen und kann aus ihr heraus alle Folgedokumente selbständig direkt im Portal erzeugen und an den Einkauf übergeben: Auftragsbestätigungen, Lieferavise, Rechnungen und Gutschriften. Alternativ kann der Lieferant diese Dokumente auch hochladen. In beiden Fällen übernimmt das SAP-System des Bestellers die Dokumente und Daten automatisch aus dem Business Partner Portal. Für die Beteiligten im Einkaufsprozess entfallen damit Ausdrucke und Versendung. Der gesamte P2P-Prozess verläuft schneller und bekannte Fehlerquellen wie Medienbrüche werden umgangen.

### Self Service und Dynamic Discounting

Lieferanten bietet das Business Partner Portal hilfreiche Funktionen wie die Self-Service-Option. Damit können Lieferanten ihre Kontaktdaten oder Bankverbindung hinterlegen beziehungsweise aktualisieren. Nach Freigabe werden die Stammdaten im SAP-System entsprechend angepasst. Das Portal ermöglicht es über die Funktion „Dynamic Discounting" ferner, Liquidität gezielt zu steuern: Lieferanten können individuell und flexibel einen zusätzlichen Rabatt anbieten, wenn eine Rechnung früher bezahlt wird. Die Rabatthöhe sowie das zugehörige Zahlungsziel wählt das Unternehmen beliebig aus, ebenso ist es möglich, mehrere Zahlungsziele mit unterschiedlichen Rabatthöhen anzubieten.

Die xSuite Group folgt damit den Anforderungen ihrer wachsenden internationalen Kundschaft. Insbesondere in den USA, aber auch in vielen anderen Ländern, verfestigt sich in den letzten Jahren der Trend zum Dynamic Discounting.

***Dina Haack | www.xsuite.de***

# WETTBEWERBSFAKTOR NACHHALTIGKEIT

Die Digitalisierung treibt den Stromverbrauch nach oben und damit den Ausstoß von Treibhausgasen. Zudem sorgt die Vielzahl neuer elektronischer Geräte für einen steigenden Ressourcenverbrauch und führt zu einer wachsenden Belastung der Umwelt mit Elektroschrott. Dell Technologies und Intel engagieren sich daher seit Langem gemeinsam für eine nachhaltige Produktion und umweltbewusstes Handeln.

Geht es um Nachhaltigkeit, kommt der IT-Industrie eine besondere Verantwortung zu, ist sie doch Treiber der Digitalisierung, die durch eine wachsende Zahl digitaler Endgeräte und immer größere Rechenzentren den Stromverbrauch und die Ressourcennutzung massiv ansteigen lässt. Dell Technologies und Intel haben daher bereits in den vergangenen Jahren umfangreiche Maßnahmen eingeleitet, um Emissionen und Müll zu reduzieren und den Energieverbrauch ihrer Produkte zu senken. Für die kommenden zehn Jahre haben sich beide Unternehmen sehr ambitionierte Ziele gesetzt.

- Schon heute verwendet Dell Technologies bei seinen Produktverpackungen zu 85 Prozent recycelte oder wiederverwertbare Materialen. Bis 2030 sollen es sogar 100 Prozent sein.
- Die Produkte selbst sollen bis 2030 zu mehr als der Hälfte aus Komponenten bestehen, die recycelte oder erneuerbare Materialien nutzen.
- Für jedes verkaufte Produkt soll ein gleichwertiges recycelt werden. In einem Pilotprojekt wurden aus alten Produkten bereits mehr als 2.000 Kilogramm Kunststoffharze gewonnen und in der Displayproduktion genutzt.

**Sparsame Komponenten**

Zudem soll über die komplette Lieferkette hinweg der Ausstoß von Treibhausgasen weiter sinken – auch beim Kunden durch den Einsatz energieeffizienter Geräte. Diese Energieeffizienz wird dabei vor allem durch sparsame Komponenten verbessert, wie Intel sie liefert.

- Bis 2030 will Intel die Effizienz seiner Client- und Server-Prozessoren verzehnfachen und damit zu Energieeinsparungen auf Kundenseite beitragen.
- Die gesamten Emissionen des Unternehmens sollen im gleichen Zeitraum um 10 Prozent verringert und in allen Produktionseinrichtungen ausschließlich erneuerbare Energien genutzt werden.
- Seit Mitte der 1990er Jahre hat Intel die Recyclingrate von ungefährlichen Abfällen von 25 auf 93 Prozent erhöht, seit 2015 wurde die direkte Wiederverwertung von Produktionsabfällen um 275 Prozent gesteigert. Das neue Ziel lautet nun, die Umsetzung von Kreislaufwirtschaftsstrategien entscheidend voranzutreiben.

**Umweltschutz von Anfang an**

In einer globalisierten Welt reicht es jedoch nicht, wenn sich nur wenige Unternehmen um nachhaltiges Wirtschaften bemühen. Vielmehr ist der Einsatz jedes Einzelnen gefragt, um einen lebenswerten Planeten zu hinterlassen. In den Führungsetagen darf nicht mehr nur darüber diskutiert werden, dem eigenen Unternehmen einen grünen Anstrich zu verpassen – notwendig sind vielmehr konkrete und wirkungsvolle Maßnahmen zum Umweltschutz auf breiter Basis.

Sowohl Privat- als auch Geschäftskunden verlangen heute nach sauberen und ressourcensparenden Lösungen und meiden Anbieter, die diesem Anspruch nicht gerecht werden. Ein nachhaltiges wirtschaftliches Handeln wird damit für Unternehmen zum Wettbewerbsfaktor.

***www.DellTechnologies.com/DE/Nachhaltigkeit***

# CLOUD INFRASTRUKTUREN

## HERAUSFORDERUNGEN IM MANAGEMENT

Nach Prognosen von Gartner-Analysten wird sich das Verhältnis „on premises" zu Cloud-Services in den nächsten 5 Jahren dramatisch ändern. Daher ist es Zeit, sich über eine Lösung Gedanken zu machen, um beide Welten bestmöglich und zukunftssicher zu koppeln. Dabei geht es um das parallele Managen von Cloud-Infrastrukturen und traditionellen Rechenzentrums-Landschaften. Durch den stark steigenden Cloud-Anteil ergeben sich dabei ganz neue Herausforderungen in Bezug auf Compliance, Kostenkontrolle und Transparenz. Hybrid Cloud Computing-Lösungen unterstützen hierbei. Unser Überblick zeigt Möglichkeiten und Herausforderungen dieser neuen Technologie.

### Hybrid Cloud Computing – was ist das?

Der Aufbau, die Implementierung und die Ausreifung von Cloud-Strategien werden auch in den kommenden Jahren auf der Agenda von CIOs ganz oben stehen. Gartner rät, sich dabei auf den Aufbau einer flexiblen Infrastruktur zu konzentrieren. Wenn man wie Gartner davon ausgeht, dass der Anteil von „On premises" betriebenen Enterprise-Systemen zwar kontinuierlich von heute 80 Prozent auf 30 Prozent im Jahr 2025 zurückgeht, aber nicht komplett ersetzt wird, ist dabei vor allem das Konzept der Hybrid Cloud Erfolg versprechend. Hybrid Cloud Computing stellt nicht nur eine Brücke zwischen dem traditionellen Rechenzentrum und diversen Cloud-Diensten (Public Cloud) dar – sie vereint beide Welten bestmöglich. Das Ziel-Szenario einer Hybrid Cloud ist eine integrierte, skalierbare und sichere Plattform für das nahtlose Bereitstellen und die Nutzung von Geschäftsanwendungen oder anderen Technologie-Services, die aus internen oder externen Quellen stammen können. Denn Anwender und Kunden verlassen sich heute auf agile und automatisierte Services, darunter viele cloudbasierte und Self-Service-orientierte Leistungen.

Die Vorteile liegen auf der Hand, vor allem:

- eine hohe Flexibilität und günstige Kostenmodelle der Public-Cloud
- ein hoher Grad an Sicherheit und Datenschutz im eigenen Rechenzentrum
- das kurzfristige Buchen zusätzlicher Rechen- und Speicherkapazität

Doch einige dieser Vorteile bleiben aufgrund eines mangelnden Überblicks über die eingesetzten Ressourcen auf der Strecke. Sollte bereits die Infrastruktur im eigenen RZ einem sorgfältigen Management unterliegen, wird diese Notwendigkeit umso dringlicher, sobald zusätzlich verschiedene Cloud-Infrastrukturen im Unternehmen zusammenkommen. Bei der Umsetzung einer Hybrid Cloud sind kaufmännische, technische und sicherheitsrelevante Herausforderungen zu meistern.

### Hybrid Cloud Management – die vier Herausforderungen für die IT

Betrachten wir zuerst die Kosten. In diesem Jahr werden nach Einschätzungen von Gartner 80 Prozent der Organisationen ihre Cloud-IaaS-Budgets aufgrund fehlender Kostenoptimierungs-Ansätze überziehen. Bei Unternehmen ohne einen Plan für das Cloud-Kostenmanagement können sich die Mehrausgaben sogar auf 70 Prozent oder mehr summieren.

Die Gründe für die Kostenexplosion sind vielfältig. Meist führt die Flexibilität der Cloud-Nutzung zu einem Overkill bei der Nutzung. Denn viele Nutzer geben cloudbasierte Rechnerkapazität, Speicherplatz oder Lizenzen nicht mehr zurück, wenn sie sie nicht mehr benötigen. Dazu kommen die verschiedensten Preismodelle der Cloud-Infrastruktur-Anbieter, in denen die Abrechnungsdetails je nach Anbieter dramatisch variieren. Wer beispielsweise Rabattprogramme oder sogenannte Reserved Instances von Cloud-Herstellern nutzt, kann viel Geld sparen.

Die IT benötigt Tools zur Kostentransparenz und Kontrolle und muss damit Fragen beantworten wie zum Beispiel:

- Gibt es ein praxiserprobtes Modell für eine verursachergerechte Kostenverrechnung, auch für die Cloud-Services?
- Wie lassen sich zahlreichen Cloud-Service-Angebote wirtschaftlich optimieren?
- Welche Cloud-Ressourcen, ob Hardware oder Software, werden zwar voll bezahlt, liegen aber brach oder werden nur teilweise genutzt?
- Wie lassen sich Cloud-Infrastrukturkosten auf Services oder Projekte verteilen und Service-Stückkosten einfach ermitteln und planen?
- Ist auf Knopfdruck ein Soll/Ist-Vergleich von Plankosten und tatsächlichen Kosten möglich?

**„Untersuchungen haben ergeben, dass Unternehmen ohne einen Plan für das Cloud Management die Ausgaben um 70 Prozent oder mehr übersteigen könnten."**

Ron Blair, Gartner

Einschätzung von Gartner zu Cloud-Kosteneinsparpotentialen.

Voraussetzung für die Kostentransparenz ist die Transparenz über die komplette IT-Landschaft und -Struktur. IT-Abteilungen kennen heute oft nur Teile der Infrastruktur, die Fachbereiche selbständig bei den Cloud-Anbietern bestellt haben. Nur über volle Kenntnis der IT-Infrastruktur ist eine effektive Ressourcen-Steuerung möglich. Zu beachten sind Aspekte wie zum Beispiel:

- zentrale Erfassung und Darstellungsmöglichkeit der Cloud-Komponenten als auch der IT-Komponenten im eigenen Rechenzentrum und deren Beziehungen und Abhängigkeiten untereinander
- Management sämtlicher Cloud-Infrastrukturen und Cloud-Software über ihren kompletten Lebenszyklus: Von der Anforderung über die Genehmigung, die Instanziierung bis hin zur Abschaltung der Cloud-Instanzen.
- Monitoring der tatsächlichen Nutzung der Cloud Infrastrukturen, um nicht genutzte Kapazitäten zu identifizieren und abschalten zu können.

Eine dritte zentrale Herausforderung ist das Sicherstellen von Guidance und Compliance. Kennen denn Fachabteilungen die Cloud-Policy ihres Unternehmens, die genehmigten Cloud-Anbieter und die Länder, in denen die IT-Infrastruktur ihres Unternehmens gehostet werden darf? Und hat die zentrale IT-Abteilung, Kenntnis darüber, wo Applikationen und Daten liegen und wer Zugriff darauf hat? Oft fehlt zudem der Prozess, der sicherstellt, dass Ex-Mitarbeiter nicht mehr auf Firmendaten in der Cloud zugreifen können.

Voraussetzungen für Compliance-Konformität sind:

- Vollumfängliche Transparenz über angeforderte und im Einsatz befindliche Cloud-Infrastruktur-Komponenten
- Reporting über die Erfüllung von Vorgaben der unternehmensindividuellen Cloud-Policy
- Abgleich zwischen lizensierter und tatsächlich installierter Software
- Anzeige von Abweichungen bei Unter- bzw. Überlizenzierungen oder unerlaubten Installationen

DER HYPE IST VORBEI. CLOUD COMPUTING IST DAS „NEW NORMAL". FÜR ÜBER 90 PROZENT DER ORGANISATIONEN SIND CLOUD-TECHNOLOGIEN INZWISCHEN DIE ERSTE OPTION. DIE IT WIRD ZU GUNSTEN VON CLOUD SERVICES HYBRIDER.

Peter Stanjeck,
Senior Vice President, USU GmbH,
www.usu.com

Last but not least ist die Effektivität in der Organisation ein wichtiger Erfolgsfaktor für ein funktionierendes Hybrid Cloud Management. IT-Abteilungen brauchen das nötige Know-how für das Management von hybriden-Umgebungen, um zahlreiche Services unterschiedlicher Herkunft und Beschaffenheit in ein einheitliches Bereitstellungs- und Überwachungskonzept zu integrieren. Zu oft werden inzwischen doppelte Betriebsstrukturen für das Management von Cloud und Rechenzentrums-Infrastrukturen hochgezogen. Für die notwendige Effizienz gilt es, Organisationsstrukturen anzupassen und das Cloud Management in das bisherige IT Service Management zu integrieren. Insbesondere müssen die internen IT-Abteilungen in Sachen Hybrid-Cloud ihre eigene Expertise aufbauen und Tools einsetzen, die beide Welten parallel managen können. Gartner geht davon aus, dass Unternehmen in 2022 etwa 60 Prozent ihrer Infrastruktur bei Cloud-Anbietern betreiben lassen.

***Martin Landis***


Die 4 Herausforderungen des Hybrid Cloud Managements.

**VIDEO HYBRID CLOUD MANAGEMENT**

Herausforderungen und Lösungsmöglichkeiten des Hybrid Cloud Managements werden in folgendem Video leicht verständlich erläutert: http://bit.ly/cm-video-itm

Aufbruch in neue Welten: Bei der Migration auf das neuen SAP-System S/4HANA gilt es, das Thema IT-Security direkt bei der Planung mit zu berücksichtigen.

# GANZHEITLICHE ABSICHERUNG VON SAP-SYSTEMEN

## DIE WICHTIGSTEN BAUSTEINE EINER CYBERSECURITY-STRATEGIE

In Zeiten wie diesen sind die IT-Verantwortlichen eines Unternehmens besonders gefragt: Nicht nur der coronabedingte Umzug vieler Mitarbeiter ins Home Office musste bewältigt werden, bei den meisten steht mit der Migration auf das neue SAP-System S/4HANA eines der größten und umfangreichsten Projekte der vergangenen Jahre an – und nebenbei muss die ganzheitliche Absicherung der IT-Systeme gegen bewusste Angriffe von außen und das Fehlverhalten eigener Mitarbeiter sichergestellt werden. „Im Rahmen der Corona-Pandemie ist eher noch eine Zunahme von Angriffen auf die Unternehmens-IT zu verzeichnen", berichtet der Security-Experte Ralf Kempf (CTO SAST SOLUTIONS bei der akquinet AG). „Allerdings kommen nahezu zwei Drittel aller Bedrohungen für SAP-Systeme mittlerweile von innen." Oft sind diese internen Bedrohungen auf fahrlässiges Verhalten von Mitarbeitern in Bezug auf E-Mail- und Website-Funktionen zurückzuführen. „Die meisten Unternehmen bezahlen hier erhebliches Lehrgeld, weil sie ihre Security-Hausaufgaben nicht gemacht haben", ergänzt Kempf. In diesem Beitrag beschreibt er mit seiner Erfahrung im Bereich der SAP-Sicherheit die wichtigsten Bausteine einer Cybersecurity-Strategie und was für eine sichere Migration der Systeme auf S/4HANA zu berücksichtigen ist.

Eine ganzheitliche Cybersecurity-Strategie, die dann zu einer bestmöglichen Resilienz gegen Angriffe und unbefugte Zugriffe von innen und außen führt, besteht aus drei Bausteinen, die aufeinander aufbauen. Zuerst wird mit der Systemhärtung die Grundlage geschaffen, dann folgt das Netzwerk-Zoning und im letzten Schritt das kontinuierliche Security-Monitoring, um in Echtzeit kritische Schwachstellen zu erkennen und vor allem schnell darauf zu reagieren. Aufgrund der gesteigerten Komplexität der IT- und vor allem der SAP-Landschaften sowie der zunehmenden Geschwindigkeit und Heterogenität der Angriffe auf diese, ist es ratsam, für eine zeitgemäße und ständig aktuelle Sicherung der Systeme auf Unterstützung von erfahrenen externen Partnern im Bereich Security zu setzen.

### 1. Systemhärtung: Einschränkung der Benutzer und ihrer Rechte

In diesem Prozessschritt werden alle Softwarebestandteile und Funktionen, die nicht zwingend notwendig sind, rigoros entfernt. Für die Härtung sind folgende Methoden empfehlenswert: Die Deaktivierung und Entfernung von für den Betrieb nicht zwingend erforderlichen Softwarekomponenten, die Verwendung unprivilegierter Benutzerkonten zur Ausführung von Server-Prozessen, die Reduzierung der Benutzer-Rechte und -Accounts sowie die Anpassung von Dateisystemrechten und ihrer Vererbung. Hierbei ist vor allem darauf zu achten, dass das Betriebssystem und die Software regelmäßig aktualisiert und für die Übertragung von Daten eine entsprechende Verschlüsselung (zum Beispiel SSL oder SNC) genutzt wird. Darüber hinaus sollte möglichst fehlerfreie Soft-

ware ohne bekannte Verwundbarkeiten eingesetzt werden.

**Für eine effiziente Systemhärtung werden die folgenden Methoden und Tools benötigt:**

- Inventarisierung über Configuration Management Database (CMDB) Systeme
- Richtlinien und Standards definieren, basierend auf dem aktuellem „Stand der Technik"
- Server- und Systemhärtung, wahlweise manuell oder per Script
- Nutzung der Windows-Gruppenrichtlinien:
  - Blockade aller Office Macros
  - Einschränkung der Anwendungen (Whitelisting)
  - Anzeige Datei-Extensions = Standard
- Netzwerktrennung und Firewall
- Mail-Scan und Blockade von Office- und ZIP-Formaten
- Schwachstellen- und Konfigurationsscanner und zyklische Auswertung

## 2. Netzwerk-Zoning: Getrennte Systeme zur Vermeidung der „Brandausbreitung" im Krisenfall

Die Netzwerk-Trennung ist eine sehr günstige, aber vor allem auch sehr effektive Form der Sicherung der IT-Systeme. Zoning hat vor allem ein Ziel: Das Vermeiden einer „Brandausbreitung" im Falle eines kritischen Zwischenfalls. Im Rahmen dieses Bausteins erfolgt eine Trennung aller unsicheren Netze von kritischen Anwendungen sowie einer Filterung durch Perimeter (Router oder Firewall). Alle wichtigen Anwendungen wie Backend-, Backup- oder Applikations-Server sollten in einer gesicherten Zone, der sogenannte Restricted Zone (RZ), lokalisiert sein. Im Rahmen dieses Bausteins erfolgt die Definition weiterer Bereiche: Public Zone, Public Access Zone und Operations Zone.

**Alle Zonen sollten folgende Charakteristiken besitzen:**

- Jede Zone enthält eines oder mehrere routbare Subnetze
- Jede Zone kommuniziert über Perimeter-Filter
- Jede Zone hat zwei Eingänge:
  - Normale Kommunikation der Anwendungen
  - Administration der Systeme

## 3. Security-Monitoring

Wenn alle Hausaufgaben im Bereich der Härtung und des Zonings gemacht sind, beginnt die Phase, in der man im laufenden Betrieb die Fortdauer der Sicherheit überwachen muss. Das Security-Monitoring der SAP-Systeme ist eine umfassende, komplexe Aufgabe, die durch ein SIEM/Monitoring-Tool alleine nicht realisiert werden kann. Die besonderen Herausforderungen liegen unter anderem in der hohen Anzahl der verschiedenen Systeme und Anwendungen sowie in der Tatsache, dass der „Verteidiger" des SAP-Systems alle Angriffsmuster kennen muss, ein „Angreifer" jedoch nur ein funktionierendes.

Beim Security-Monitoring wird dann zwischen einer zyklischen Konfigurations-Überwachung und einer permanenten Event-Überwachung in Echtzeit unterschieden. Diese Echtzeit-Überwachung wertet die einzelnen Logs der Systeme aus und braucht Indikatoren, um einschätzen zu können, was auf eine Schwachstelle hinweisen könnte. Dafür sind entsprechende Regeln notwendig. Auch hier sind externe Analysten gefragt, um Anomalien zu erkennen und zu definieren.

Sind diese drei Bausteine alle berücksichtigt und im Idealfall mit einem spezialisierten externen Partner geplant und entsprechend implementiert, verfügt das Unternehmen über einen ganzheitlichen Schutz seiner SAP-Systeme.

## Spezialfall S/4HANA

Darüber hinaus sind IT-Verantwortliche aktuell mit der Vorbereitung der anstehenden Migration der SAP-Systeme auf S/4HANA gefordert. Auch hier ist eine besondere Berücksichtigung der sicherheitsrelevanten Aspekte absolut notwendig. Fakt ist, fast ein Drittel der Unternehmen, die eine Migration auf S/4HANA planen, vernachlässigen hierbei die Absicherung der neuen Systeme und das führt nicht nur zu neuen, ungesicherten Schwachstellen, sondern auch zu erheblichen Folgekosten. Eine Situation, die Cyberkriminellen beliebte Hintertüren öffnet und nur zu gerne ausgenutzt wird.

JE EHER UNTERNEHMEN MIT EINER GANZHEITLICHEN CYBERSECURITY-STRATEGIE STARTEN, DESTO BESSER SIND SIE IN DER LAGE, SICH GEGEN BEDROHUNGEN VON INNEN UND AUSSEN ABZUSCHIRMEN.

Ralf Kempf, CTO SAST SOLUTIONS bei der akquinet AG, www.sast-solutions.de

Die Empfehlung ist daher, sich jetzt um einen ganzheitlichen Schutz der SAP-Systeme zu kümmern – ganz gleich ob für SAP ERP oder schon für S/4HANA. Je eher Unternehmen mit einer ganzheitlichen Cybersecurity-Strategie starten, desto besser sind sie in der Lage, sich gegen Bedrohungen von innen und außen abzuschirmen.

***Ralf Kempf***

Weitere Informationen rund um das Thema Sicherheit der SAP-Systeme oder auch sichere Migration auf S/4HANA sind im Blog von SAST SOLUTIONS zu finden (https://sast-blog.akquinet.de/).

# DAS TEC MODELL

## DER CODE AGILER ORGANISATIONEN

Erfolgreiche agile Organisationen haben erstaunlich wenig gemein in ihrer Struktur. Umso mehr Gemeinsamkeiten findet man dafür in ihrer Kultur: ein Modell. Das wir eigentlich schon leben.

Eine zukunftsfähige Kultur muss vor allem Anpassungsfähigkeit der Organisation ermöglichen.

Reaktionsfähigkeit. Schnelligkeit. Organisationaler Agilität.

Die richtige Kultur ist Möglichmacher, Treiber und Förderer von Agilität in Organisationen. Die Unternehmenskultur erfolgreicher agiler Organisationen weist dabei ein bestimmtes Muster auf, wie es im TEC-Modell TEC-Model (Puckett, 2020) in Form eines Kultur-Codes entschlüsselt ist. Eine agile Organisationskultur stützt sich auf drei Pfeiler, die in einem ungefähren Gleichgewicht stehen: Transparenz, Empowerment und Kollaboration (Collaboration).

### Transparenz

Transparenz in Organisationen ist die Basis für funktionierendes agiles Arbeiten, das jeden Kopf in der Belegschaft als Antenne zum Markt/ Kunden/ Trends nutzt und das kollektive geistige Potenzial und das kollektive Wissen ausschöpft. Drei Aspekte zählen.

#### Transparenz mit Informationen und Daten

Es besteht offener Zugang zu Informationen und Daten, die das Unternehmen betreffen (etwa KPI Metriken, strategische Überlegungen und Pläne, Zahlen) und das externe Umfeld (Wettbewerbsanalysen, technologische Entwicklungen, Entwicklungen bei Kunden, Trends auf dem Markt). Hiermit können alle Mitarbeitenden strategische und taktische Überlegungen anstellen, relevante Ideen entwickeln und Entscheidungen sachkundig treffen.

> MÜSSEN ALLE BETEILIGTEN BEIM WANDEL ZU EINER AGILEN ORGANISATIONSKULTUR IHR „MINDSET" ÄNDERN? LEBEN WIR NICHT BEREITS NACH DEM TEC-KULTUR-CODE?
>
> Stefanie Puckett, Diplom Psychologin, Beraterin und Executive Coach, www.agilethroughculture.com

#### Transparenz von Ergebnissen und Wirkung der eigenen Arbeit

Mitarbeitende können die Entwicklung der Ergebnisse ihrer Arbeit (Erfolg), ihre Leistung anhand von qualitativen und quantitativen Daten verfolgen. Hierzu gehört Feedback von Kollegen und internen und externen Kunden genauso wie Zugang zu Zahlen (Absatzzahlen, Ratings von Kunden) die durch die eigene Arbeit beeinflusst werden. Dies ermöglicht nicht nur Selbstkorrektur und -steuerung, sondern vermittelt auch Sinn (was bewirke ich mit meiner Arbeit, welche Relevanz hat meine Arbeit) und damit eine Quelle der Motivation und Zufriedenheit.

#### Transparenz von Plänen und Absichten

Jeder kann sich darüber informieren, wie die strategischen und operativen Pläne des Unternehmens aussehen. Darüber hinaus besteht auch Transparenz in der Kommunikation der Absichten. Was soll mit der Strategie erreicht werden? Warum ist welche geplante Initiative, welche Entscheidung relevant und was soll sie im Einzelnen und insgesamt bewirken? Was ist der dahinter stehende Sinnzweck (Purpose)? So kann sich der Einzelne am Warum und Wohin selbstständig ausrichten. So entsteht auch Vertrauen und eine Identifikation mit dem Arbeitgeber wird gefördert.

### Empowerment

Empowerment ist der zweite Pfeiler der agilen Kultur. Er ermöglicht es den Mitarbeitenden, anhand ihrer eigenen (Er-) Kenntnisse auf Basis des ersten Pfeilers (Transparenz) zu agieren und gibt ihnen die Kontrolle über ihre Arbeit und Möglichkeiten größerer Selbstbestimmung.

Ausführende werden zu Gestaltern. Drei Facetten zählen.

### Freiheit zum Adaptier- enund Kreieren.

Die Mitarbeitenden haben als Meister ihrer Arbeit die Kontrolle über die Arbeit. Teams organisieren und managen sich selbst. Es besteht der notwendige Handlungsspielraum, die eigene Arbeit zu optimieren, an die eigenen Vorlieben anzupassen und sich auf Veränderungen einzustellen. Dies ermöglicht eine unmittelbare Reaktion auf sich verändernde Kundenbedürfnisse, auf neue technologische Möglichkeiten oder sich auftuende Chancen, die eigene Arbeit noch erfolgreicher zu machen. Im Großen geht Freiheit mit mehr Wahl- und Gestaltungsmöglichkeiten einher. Flexibilität statt Vorschriften, auch in Aspekten wie Gestaltung der Arbeitszeit, des Arbeitsortes, Wahl der Arbeitsmethode und Managen der eigenen Arbeit aber auch Wahl der Aufgaben oder des Teams.

### Empowerment zum (Selbst-)Führen.

Hier geht es nun nicht mehr darum, Dinge richtig zu tun zu können, sondern darum, die richtigen Dinge tun zu können. Selbststeuerung. Mitarbeitende bzw. Teams übernehmen nicht nur das sich selbst Managen und Organisieren, sondern auch das Steuern. Ziele werden autonom aus der Unternehmensstrategie abgeleitet und verfolgt, Methoden, Prioritäten und Arbeitsergebnisse (Produkte, Services, Prozesse) werden eigenständig angepasst. Das Team überwacht die jeweilige Wirkung und adaptiert, stoppt oder weitet aus.

### Ownership mit der Tendenz zum Handeln

Ownership übertragen zu bekommen bzw. zu übernehmen ist der Königsweg des Empowerments. Mitarbeitende erhalten und übernehmen die End-to-End Verantwortung eine Idee unabhängig zu verwirklichen. Unternehmertum im Unternehmen. Im Idealfall handelt sich um eine eigene Idee, die verwirklicht werden

## DAS TEC MODELL

darf. Der Einzelne bzw. das Team verfügt über den notwendigen Handlungsspielraum und die Befähigung, alle notwendigen Entscheidungen selbst zu treffen und verpflichten sich gleichzeitig dem Ziel.

**Kollaboration**

Kollaboration ist der dritte Pfeiler des TEC-Modells agiler Unternehmenskultur. Eine Organisation kann ein hohes Maß an Digitaler Geschäftsagilität aufweisen und trotzdem den Überlebenskampf verlieren. Die Komplexität und der Umfang der heute verfügbaren Daten können von Organisationen voller Einzelkämpfern nicht bewältigt werden. Auch kann ohne Flexibilität in der Zusammenarbeit nicht schnell und schlagkräftig reagiert und agiert werden, wenn Kräfte nicht kurzfristig gebündelt werden können. Drei Facetten sind notwendig:

### Zusammenarbeit über Austausch und Teilen

Das ganze Potenzial kollektiven Wissens, vorhandener und verfügbarer Information und Daten, die Erfahrungsschätze und Kompetenzen Einzelner, wird erst dann voll realisiert, wenn ein Bündeln und Kombinieren möglich wird. Die Qualität der Entscheidungen wird durch die Vielfalt der Perspektiven erhöht, Innovation ermöglicht. Vernetzte Menschen führen zu vernetztem Denken. Vernetzte Lösungen entstehen. Auch die Effizienz wird gesteigert, wenn durch den Austausch Möglichkeiten sichtbar werden, Synergieeffekte zu nutzen. Die Erfolgswahrscheinlichkeit steigt, wenn Wissen und Erfahrungen dort ausgetauscht werden, wo sie gebraucht werden.

**DER CODE AGILER ORGANISATIONEN**


Das Playbook für den Wandel zur agilen Organisationskultur
1. Auflage
BusinessVillage
2020

### Zusammenarbeit über Beiträge und Flexibilität

Bei der schnellen Ausarbeitung und Umsetzung von Ideen müssen die richtigen Leute zeitnah zusammengebracht werden und sich dem Thema widmen können. Dies erfordert eine Organisation in flexiblen Netzwerken, die sich zielbedingt immer wieder neu organisiert.

Darüber hinaus wird Spitzenleistung erst dann möglich, wenn Mitarbeitende Beiträge basierend auf ihren Talenten leisten und zwar dort, wo sie den größten Mehrwert stiften. Unabhängig davon, für welche Abteilung, in welchem Team und in welcher Rolle oder auch Tätigkeit.

### Zusammenarbeit über gemeinsames Lernen und Wachsen

Anpassungsfähigkeit einer Organisation setzt Lernfähigkeit voraus. Und diese beginnt im Kleinen. Die regelmäßige gemeinsame Reflektion im Team, die kontinuierliche Verbesserung im Team bewirkt. Reflektion oder die Auswertung von Misserfolgen über Teamgrenzen hinweg erlaubt das Identifizieren systematischer Erfolgshemmnisse und deren Beseitigung. Dies setzt voraus, dass die Menschen offen über Fehler und Scheitern sprechen, gemeinsam reflektieren und Vorgehensweisen, Prozesse und Zusammenarbeit anpassen und ständig gemeinsam weiterentwickeln.

Denken Sie an einen Bereich, oder ein Vorhaben aus Ihrem Privatleben, in/bei dem Sie besonders erfolgreich und zufrieden sind. Blicken Sie auf die Umstände. Finden Sie die drei Pfeiler wieder?

In einer solchen Situation sind wir meistens recht gut über das Thema informiert bzw. wissen, wo wir alle benötigte Information finden. Wir sind uns bewusst darüber, warum wir hier investieren und was wir erreichen wollen. Der Effekt des Erfolges ist direkt spürbar. (Transparenz)

In solchen Situationen agieren wir in der Regel selbstbestimmt. Wir treffen relevante Entscheidungen gestalten unsere Arbeit selbst. (Empowerment)

Dann sind solche Situationen dadurch gekennzeichnet, dass wir Personen in unserem Netzwerk haben, die uns Inspiration oder Rat geben und mitunter tatkräftig unterstützen. (Kollaboration)

***Stefanie Puckett***

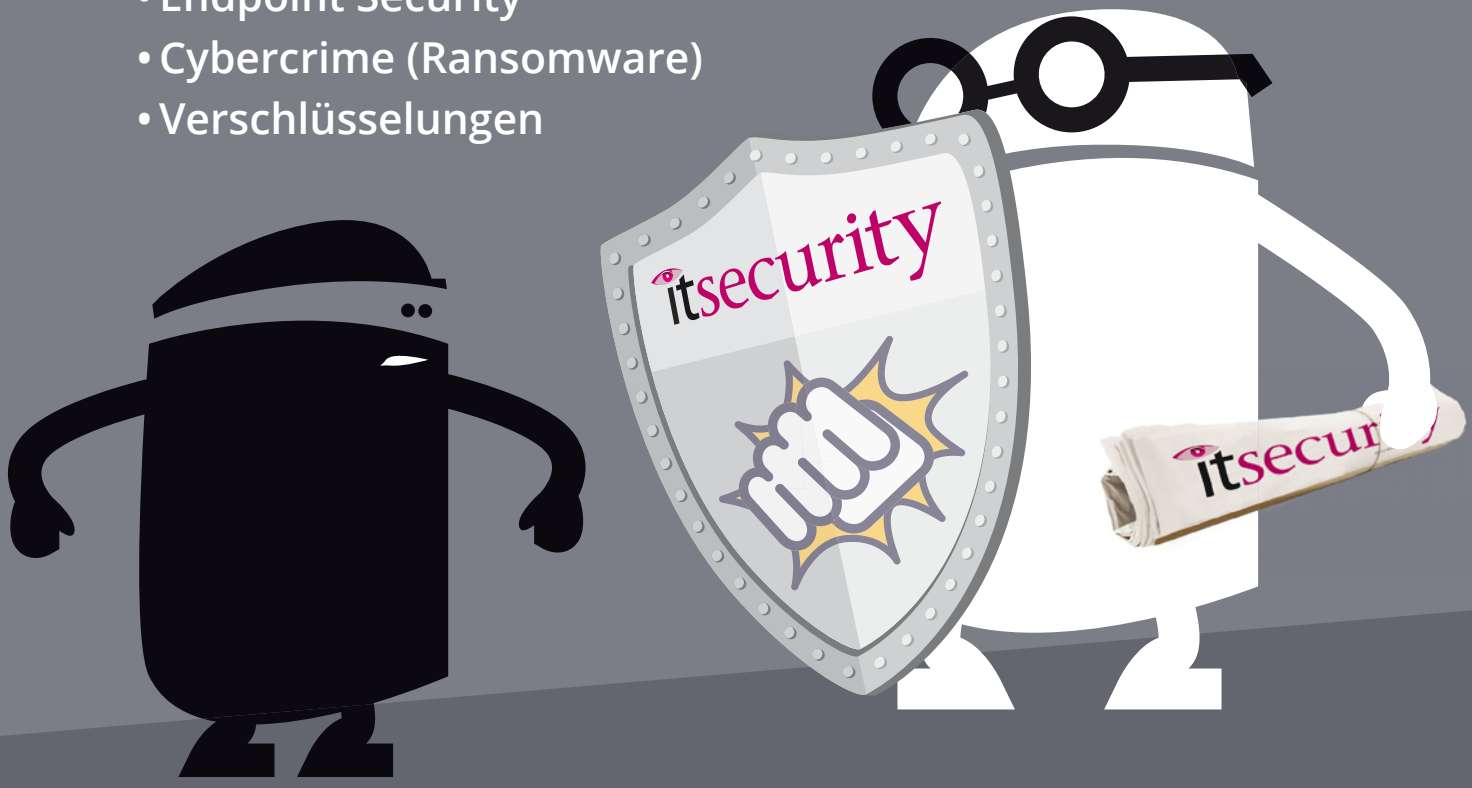
# We secure IT

## IT Security 2020 Digitalevent

## 17. November 2020

Die virtuelle, interaktive Konferenz mit Live Vorträgen, Diskussionsrunden und Interviews zu den Themen:

- Cybersecurity
- Security Awareness
- Cloud Security
- Endpoint Security
- Cybercrime (Ransomware)
- Verschlüsselungen




**Jetzt anmelden**

**www.it-daily.net/wesecureit/**

# DAS ZEITALTER DER QUANTENCOMPUTER

## BEDEUTEN SIE DAS ENDE DER KRYPTOGRAPHIE?

Als Google Ende 2019 bekanntgab, dass ihr Quantencomputer eine Aufgabe in 200 Sekunden löste, für welche der schnellste Supercomputer der Welt 10.000 Jahre benötigt hätte, schien sich das Rennen der Quantenüberlegenheit der Ziellinie zu nähern. Dieser erste Erfolg von Google zeigt auch, dass das Quantenzeitalter näher ist, als wir oft denken. Umso wichtiger ist es daher, die möglichen Auswirkungen dieser Technologie aufzuzeigen. Dabei erscheint keine Bedrohung größer, als die potenziellen zerstörerischen Auswirkungen dieser Technologie auf die Kryptographie und Cybersicherheit.

**Der Tod der Kryptographie**

Eine wichtige Rolle bei der Verschlüsselung von Daten spielen Primzahlen. Asymmetrische Verschlüsselungssysteme wie zum Beispiel RSA basieren darauf, dass es für die Primfaktorzerlegung kein effizientes Verfahren gibt. Zum Beispiel beansprucht bei einem herkömmlichen Computer die Primfaktorzerlegung einer 240-stelligen Nummer (RSA-240) circa 900 Jahre Rechenleistung. Die Schwere dieses Problems ist das Kernstück weit verbreiteter Algorithmen in der Kryptographie wie RSA.

Anders als traditionelle Computer brillieren Quantencomputer jedoch darin, genau diese Algorithmen zu knacken. Shor, ein amerikanischer Mathematiker, stellte 1994 einen Algorithmus vor, welcher mit Hilfe eines Quantencomputer in Polynomzeit die Primfaktorzerlegung einer großen Zahl berechnen kann. Da die Sicherheit der heutigen Verschlüsselungs- und Signaturschemata der Primfaktorzerlegung zugrunde liegt, könnte das den Tod dieser kryptographischen Systeme bedeuten.

DER SCHUTZ KRITISCHER DATEN IM QUANTENZEITALTER IST MÖGLICH; ERFORDERT JEDOCH EINEN MULTIDISZIPLINÄREN ANSATZ.

Florian Wiedmann,
Secure Analytics Manager, CYSEC SA,
www.cysec.com

Damit kann die Kryptographie im Zeitalter von Quantencomputern weder die Übertragung von Daten, noch deren sichere Speicherung garantieren. Experten gehen davon aus, dass schon im Jahr 2031 ein Quantencomputer existieren könnte, der groß genug ist, um die kryptographischen Algorithmen zum Schutz von Kreditkarten (RSA) zu knacken. Mit anderen Worten: Große Datenmengen, wie zum Beispiel von Finanztransaktionen, E-Mail-Kommunikation, kritischer Infrastruktur oder Transportsystemen werden mit der Erfindung des Quantencomputers unsicher.

**Die heutige Bedrohung**

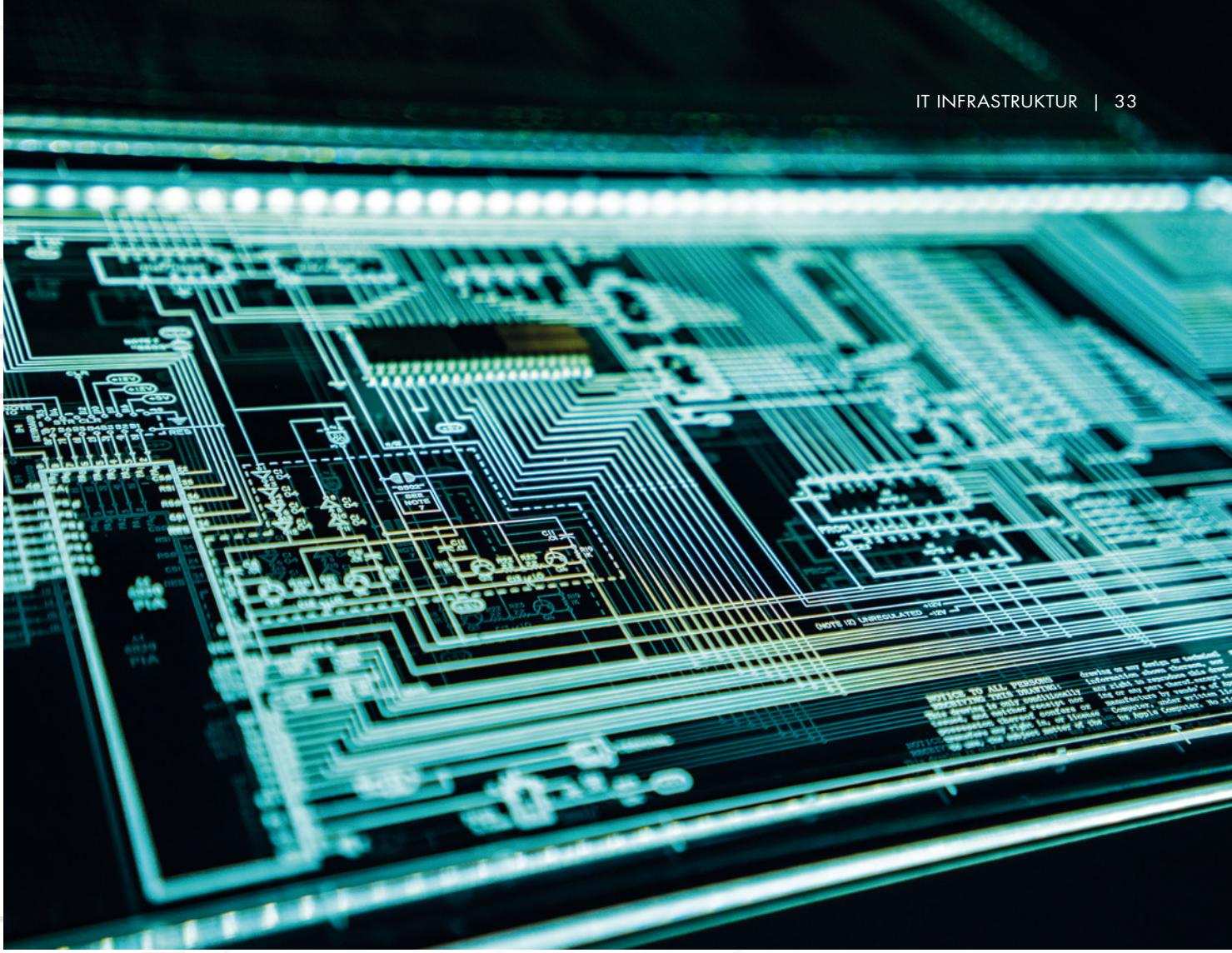
Quantencomputer stellen eine ernsthafte Bedrohung für die Verschlüsselung dar – und das schon heute. Das liegt daran, dass verschlüsselte Informationen auch in Zukunft rückwirkend entschlüsselt werden können. Hacker, ob privat oder staatlich, könnten schon jetzt sensible und verschlüsselte Daten sammeln und diese entschlüsseln, sobald Quantencomputer verfügbar sind.

Unternehmen und Regierungen können es sich nicht leisten, dass ihre Kommunikationskanäle rückwirkend entschlüsselt werden, selbst wenn dieser Zeitpunkt in ferner Zukunft liegt. Denn das könnte erhebliche geschäftliche, geopolitische und diplomatische Auswirkungen haben. Deshalb ist im Umgang mit sensiblen Daten schon heute große Vorsicht geboten. Daten müssen mit Algorithmen verschlüsselt werden, welche nicht nur den besten gegenwärtigen Standards entsprechen, sondern auch resistent gegen Quantencomputer sind. Wenn die Datensicherheit auch in Zeiten von Quantencomputern bewahrt werden soll, müssen deshalb schon jetzt Maßnahmen ergriffen werden.

**Post-Quanten-Kryptographie**

Post-Quanten-Kryptographie (engl. PQC) Lösungen folgen einem algorithmischen Ansatz und könnten eine Lösung gegen die Bedrohung durch Quantencomputer in der traditionellen Kryptographie bieten. Solche Lösungen basieren auf mathematische Funktionen, bei welchen Quantenalgorithmen keinen komparativen Vorteil haben.

Die theoretischen Arbeiten im Zusammenhang mit solchen PQC-Lösungen sind recht weit fortgeschritten und es gibt bereits heute zahlreiche Beispiele für mög-



liche quantenresistente Verschlüsselungen. Da PQC die am weitesten verbreitete Anwendung ist und relativ geringe Kosten mit sich bringt, scheint es die vielversprechendste Lösung für die Entwicklung einer quantenresistenten Verschlüsselung zu sein.

Doch die Frage bleibt, wie solche Lösungen implementiert und standardisiert werden sollen. Organisationen wie das National Institute for Science and Technology (NIST) versuchen aktiv, Antworten auf diese Fragen zu finden. Das NIST ist an den Standardisierungsbemühungen von PQC-Algorithmen beteiligt, die den Weg für die Massenanwendung ebnen werden.

## Kryptographische Algorithmen reichen nicht aus

In der Praxis hängt die Sicherheit dieser kryptographischen Primitive jedoch auch Stark von ihrer Hardware-Implementierung ab. Das liegt daran, dass ein Angriff auch gelingen kann, ohne dass das mathematische Problem geknackt wird. Bei sogenannten Seitenkanalattacken wird das Gerät, auf welchem die kryptographischen Algorithmen gehostet werden, beobachtet. Der Angreifer analysiert dann beispielsweise die Laufzeit des Algorithmus, den Energieverbrauch des Prozessors oder die elektromagnetischen Ausstrahlung. Diese Informationen können genutzt werden, um geheime Schlüssel zu extrahieren und sensitive Daten zu entschlüsseln.

Herkömmliche Hardware hat sich wiederholt als unzureichend erwiesen, um kryptographische Primitive sicher zu implementieren. Sogar bekannte Lösungen wie SGX von Intel erwiesen sich als unsicher gegen die oben genannten Seitenkanalattacken. Angesichts dieser Bedrohungen ist es wichtig, quantenresistente kryptographische Bibliotheken auf robuster Hardware zu implementieren. Solche Lösungen sind als vertrauenswürdige Ausführungsumgebungen (englisch: Trusted Execution Environments, TEEs) bekannt und nutzen nicht-konventionelle Hardware wie Hardware-Sicherheitsmodule (HSMs) zum Schutz digitaler Daten.

## Schlussfolgerung

Der Schutz kritischer Daten im Quantenzeitalter ist möglich; erfordert jedoch einen multidisziplinären Ansatz. Die derzeit verwendeten kryptographischen Primitive müssen durch sogenannte Post-Quanten-Kryptographische Primitive ersetzt werden, denn diese sind bei Angriffen auf Quantencomputer widerstandsfähiger. Gleichzeitig müssen kryptographische Primitive in einem Trusted Execution Environment gehostet werden, um gegen Seitenkanalattacken gesichert zu sein. Folglich müssen Organisationen schnell handeln und auf Post-Quanten-Kryptographie, als auch auf vertrauenswürde Ausführungsumgebungen setzen, um Vertraulichkeit, Integrität und Authentizität ihrer Daten und Anwendungen im Quantenzeitalter zu gewährleisten.

***Florian Wiedmann***

# „ZERO TRUST“

## BUZZWORD ODER PRAKTISCHER ANSATZ?

Der Begriff „Zero Trust“ zeigt in aktuellen Studien, Marktanalysen, IT-Sicherheitsstrategien und Fachbeiträgen eine gewisse Dauerpräsenz. Ob es nun das „Zero Trust Maturity Model“ ist, ein „Zero Trust Network Access (ZTNA)“ oder das „Continous Adaptive Risk and Trust Assessment (CARTA)“ – alle Ansätze versprechen höhere Sicherheit und besseren Schutz gegenüber aktuellen Bedrohungen. Wirklich neu ist das Konzept aber nicht: Der Begriff wurde von Analysten bereits im Jahr 2010 geprägt; der Ursprung geht sogar noch weiter zurück bis in die 2000er, als das Jericho Forum eine Initiative startete, die eine Zukunft nach der klassischen Perimetersicherheit beschreibt.

### Warum ist die Vertrauensfrage so aktuell?

Generell entstammen die Konzepte der Netzwerk- und Perimetersicherheit einer Zeit, in der von einer vollständigen Kontrolle über das Netzwerk und den damit verbunden Kommunikationswegen ausgegangen wurde. Geräte und Netzwerkanschlüsse befanden sich allesamt innerhalb der Firmengebäude. Drahtlose Technologien waren kaum im Einsatz und die Kupferverkabelungen in öffentlich zugänglichen Bereichen galten als bedenklich, da sie im Gegensatz zu Glasfaserverbindungen abhörbar waren. Die größte Gefahr sah man in dieser Zeit in den eigenen Mitarbeitern oder Personen, die grundsätzlich Zugang zum Gebäude hatten und Industriespionage betrieben.

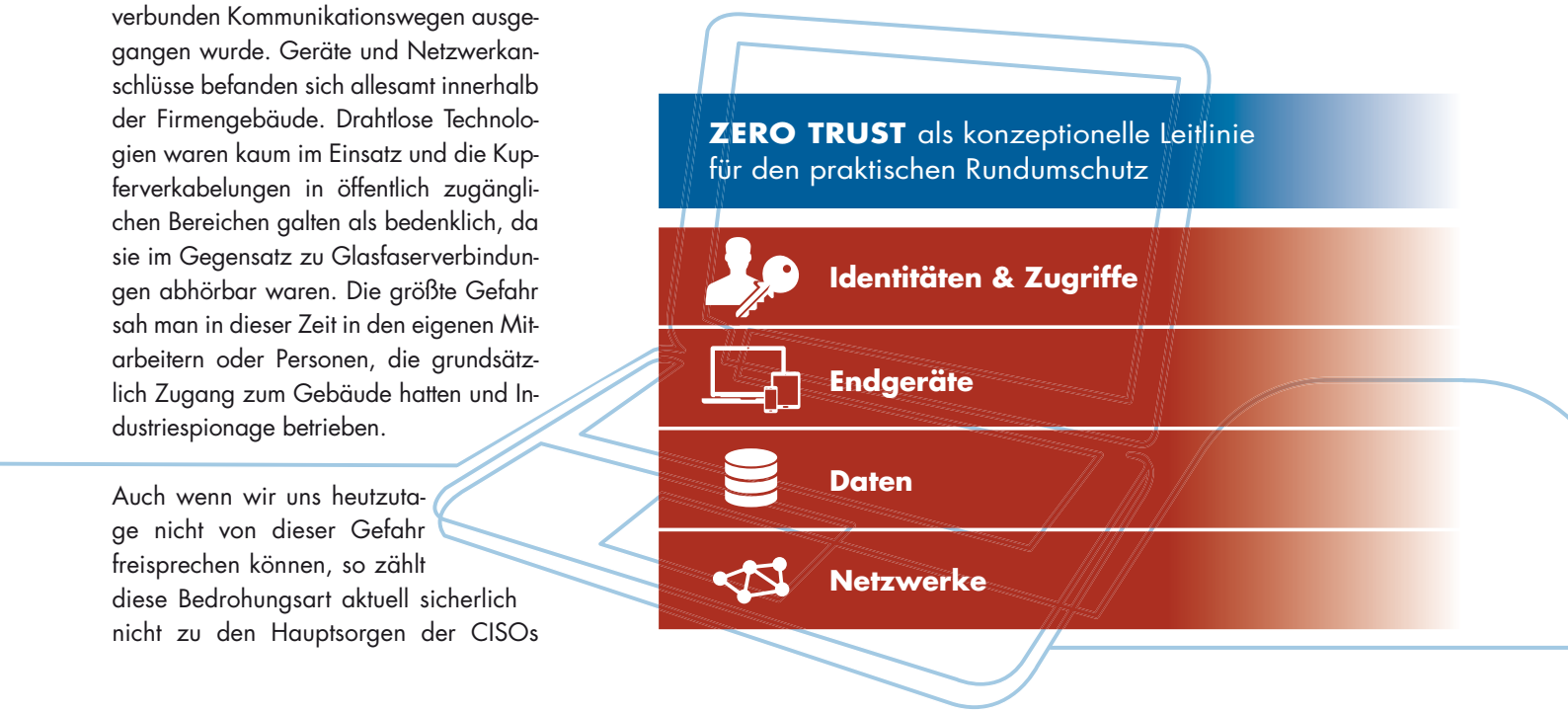
Auch wenn wir uns heutzutage nicht von dieser Gefahr freisprechen können, so zählt diese Bedrohungsart aktuell sicherlich nicht zu den Hauptsorgen der CISOs weltweit. Vielmehr entwickelt sich die Bedrohungslage in rasantem Tempo und schier grenzenlos weiter. Die Dezentralisierung von Daten und Zugriffen, die durch den Einsatz von Cloudservices und die Notwendigkeit des uneingeschränkten mobilen Arbeitens bedingt wird, verschärft die Situation zunehmend. Es liegt auf der Hand, dass die beschriebenen Ansätze der Netzwerksicherheit in dieser Zeit keinen adäquaten Schutz mehr bieten können.

### Was kann man sich unter Zero Trust vorstellen?

Zero Trust beschreibt weder eine dedizierte Technologie noch ein genormtes Verfahren. Vielmehr handelt es sich hierbei um eine konzeptionelle Leitlinie, die auf Vorsicht, Umsicht und einer gewissen Skepsis beruht. Untermauert wird diese häufig durch Claims wie „Never Trust, always verify“ oder „Application Access ≠ Network Access“.

Worin liegt also der Unterschied zu den bisherigen Security-Ansätzen? Das grundsätzliche Ziel besteht darin, möglichst viele Informationen zu sammeln: Mit deren Hilfe werden aktuelle Zugriffe bewertet und entsprechend zugelassen oder abgewehrt. Das bedeutet: Auch eine erfolgreiche Authentifizierung gewährt daher nicht automatisch einen Datenzugriff, da zusätzlich weitere Signale berücksichtigt werden wie Zugriffsort, -gerät oder die Risikobewertung des Nutzers per se. Das Bewertungsergebnis entscheidet schließlich darüber, ob der erfolgreich authentifizierte Benutzer einen eingeschränkten (also auf seine Nutzerrolle angepassten) oder sogar gar keinen Zugriff auf bestimmte Applikationen und Daten erhält.

Neben solch einer fallbezogenen Entscheidung gilt grundsätzlich das Minimalprinzip. Das bezieht sich sowohl auf Zugriffsrechte innerhalb einer Applikati-



on, den restriktiven Umgang mit privilegierten Benutzern (administrative Accounts) als auch auf den Verzicht auf nicht notwendige Netzwerkzugriffe.

**Was unterscheidet Zero Trust Ansätze?**

Am Beispiel des durch das Marktforschungsinstitut Gartner beschriebenen aktuellen ZTNA-Modells lässt sich die Besonderheit dieses Ansatzes gut herausstellen.

Schaut man sich herkömmliche Netzwerke an, gibt es in der Regel ein Urvertrauen (Level of Trust). Der Zugriff aus dem Unternehmensnetzwerk erfolgt erst einmal uneingeschränkt über das gesamte Netzwerk. Modernere Netzwerkarchitekturen arbeiten mit groben Netzsegmentierungen nach dem Ausschlussprinzip: Demnach schließt ein Unternehmen aus, dass ein Mitarbeiter von seinem Device aus direkten Zugriff auf das Datensicherungsnetz benötigt – und entzieht es ihm somit. Aufgrund des notwendigen Zugriffs auf den zentralen Fileserver und die fehlende Mikrosegmentierung (also ein Segment pro Applikation und Anwendungsfall) hat jedes Gerät im Firmennetz erstmal übergreifenden Netzzugriff. Die Authentifizierung des Benutzers und die Überprüfung der Zugriffsrechte erfolgen erst im Anschluss. Die Netzsicherheit wird zusätzlich durch die Notwendigkeit der mobilen Arbeit beeinflusst. VPN-Zugriffe ermöglichen in der Regel den vollständigen Netzwerkzugriff aus der Ferne und schaffen so häufig weitere – teils unkontrollierte – Netzübergabepunkte zwischen dem Unternehmensnetz und dem Internet. Nicht umsonst stellen Ransomware-Angriffe eine der aktuell größten Bedrohungsszenarien dar, da sie genau diese Schwachstellen ausnutzen.

Beim ZTNA wird der Ansatz umgekehrt. Der Benutzer muss sich erst unter Berücksichtigung verschiedener Einflussfaktoren authentifizieren, um dann in einem vollständig segmentierten Netz Zugriff auf einzelne Applikationen zu erhalten. Die ihm gewährten Zugriffe richten sich an einem Rollenkonzept aus und werden immer wieder aufs Neue bewertet. Das oben genannte Prinzip des „Urvertrauens" wird ausgehebelt.

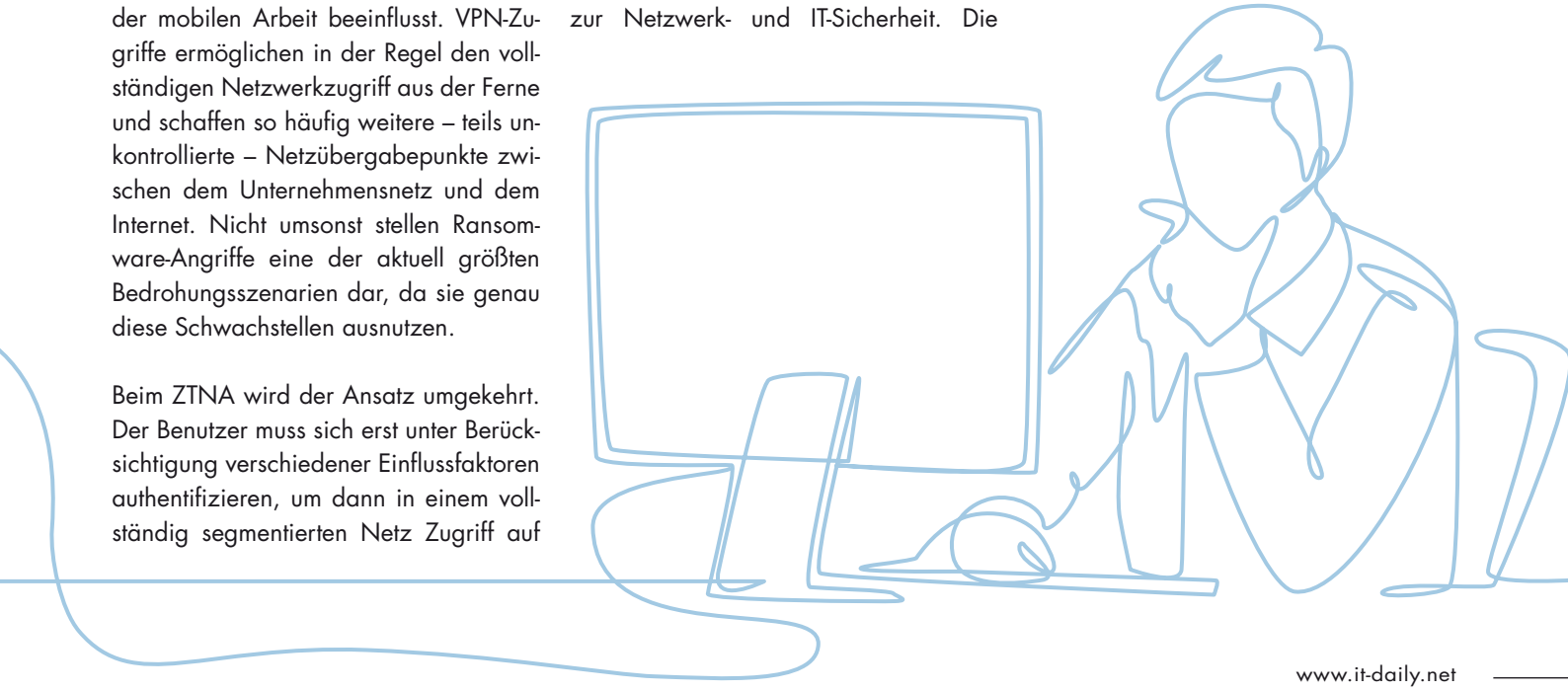
> DIE ZEITEN, IN DENEN EIN UNTERNEHMEN BEHAUPTEN KANN, ALLE SYSTEME, DATEN UND APPLIKATIONEN DIREKT KONTROLLIEREN UND STEUERN ZU KÖNNEN, SIND LEIDER EBENSO ÜBERHOLT WIE VIELE DER BISHERIGEN ANSÄTZE ZUR NETZWERK- UND IT-SICHERHEIT.
>
> Daniel Philips, Head of CIS, synalis GmbH & Co.KG, www.synalis.de

Die Praxis verlangt zusammenfassend weniger eine exakte Umsetzung eines vollständigen Konzeptes als vielmehr ein Umdenken in Bezug auf grundsätzliche Annahmen und konzeptionelle Ansätze.

Die Zeiten, in denen ein Unternehmen behaupten kann, alle Systeme, Daten und Applikationen direkt kontrollieren und steuern zu können, sind leider ebenso überholt wie viele der bisherigen Ansätze zur Netzwerk- und IT-Sicherheit. Die grundsätzliche Idee, Zugriffe kritisch zu hinterfragen und zu beurteilen, ein sicheres Identitäts- und Zugriffsmanagement zugrunde zu legen und eben nur die absolut notwendigen Ressourcen zugänglich zu machen ist eine Interpretation von Zero Trust, die einen praktischen Ansatz liefert und eine gute Grundlage novellierter Sicherheitskonzepte bildet.

Fazit: Wenn Sie das Prinzip Never trust, always verify in die Tat umsetzen und in Sicherheitsfragen beherzigen, verhilft Ihnen das vermeintliche Buzzword „Zero Trust" zu einem praktikablen Ansatz für moderne IT-Security.

***Daniel Philips***



# SCHWACHSTELLEN-MANAGEMENT

## FOKUS AUF DEN START DER CYBERSICHERHEITSKETTE

In Zeiten der digitalen Transformation hängt Erfolg davon ab, wie zuverlässig Menschen, Unternehmen und Dienste vor Cyberangriffen und vor dem Verlust wertvoller Daten geschützt werden.

Die Gründe für einen Cyberangriff oder einer Datenverletzung sind unterschiedlich. In einigen Fällen, wie zum Beispiel beim US-Finanzdienstleister Equifax erlangten Angreifer durch die Ausnutzung einer Schwachstelle unbefugten Zugang zu ihrem Netzwerk und ihren Systemen. Fatal war, dass es sich um eine bekannte Schwachstelle handelte, die nicht innerhalb einer angemessenen Zeitspanne behoben wurde. Der „Data Breach" bei Equifax ist ein typisches Beispiel für einen bedeutenden Cyberangriff, bei dem persönliche Daten von fast 150 Millionen Kunden offengelegt wurden.

In anderen Fällen können ungesicherte, dem Internet ausgesetzte Daten ein Problem darstellen. Zero-Day-Schwachstellen können nach Belieben ausgenutzt werden, bevor Korrekturen verfügbar sind, oder in einigen der schlimmsten Fälle kann eine Organisation oder eine Einzelperson von staatlich finanzierten Advanced Persistent Threat (APT)-Gruppen ins Visier genommen werden, die über beträchtliche Ressourcen und Werkzeuge verfügen.

Tatsächlich reicht ein einziger anfälliger Endpunkt, ein Netzwerk, ein Server oder eine Anwendung aus, um Millionen von Menschen zu beeinträchtigen. Shellshock, Heartbleed, Poodle und EternalBlue sind nur einige der berüchtigten Schwachstellen, die dem Datendiebstahl durch Malware und anderen Angriffen Tür und Tor geöffnet haben. Es gibt unzählige weitere - im Jahr 2017 gab es 1.522 öffentlich gemeldete Schwachstellen. Die Zero Day Initiative [ZDI] hat aufgedeckt, dass 929 davon als „kritisch" oder „hoch" eingestuft wurden.

Neben der Bedrohungslandschaft spielen auch die Kosten für Unternehmen, die einem Angriff oder einer Datenverletzung ausgesetzt sind, eine große Rolle. Cyberkriminalität ist ein profitables Geschäft, mit relativ geringen Risiken im Vergleich zu anderen Formen der Kriminalität.

Laut dem Lagebericht des Ponemon Institute dauerte es im Jahr 2019 im Durchschnitt 279 Tage, bis ein Verstoß entdeckt und eingedämmt wurde. Die durchschnittlichen Gesamtkosten eines „Datenverstoßes" beliefen sich weltweit auf 3,9 Millionen US-Dollar, in Deutschland sogar 4,08 Millionen US-Dollar, wenn man die Meldekosten, die mit der Untersuchung, Schadensbegrenzung und Schadensbehebung verbundenen Ausgaben sowie die Bußgelder und Gerichtsverfahren berücksichtigt. Die Kosten für einen Datenverstoß sind steigend (12 Prozent in 5 Jahren). Unbeabsichtigte Data Breaches durch menschliches Versagen und Systemfehler sind immer noch die Ursache für fast die Hälfte (49 Prozent) der im Bericht untersuchten Datenverletzungen. Hierzu zählen „unbeabsichtigte Insider", etwa Mitarbeiter, die durch Phishing-Angriffe kompromittiert werden oder deren Geräte infiziert oder verloren/gestohlen werden können.

### Was können Unternehmen präventiv tun?

Schwachstellen können in den Betriebssystemkomponenten oder Softwareanwendungen liegen. IT-Administratoren müssen die mit diesen Schwachstellen verbundenen Risiken identifizieren und verwalten können. Angesichts des oben genannten Schadenspotenzials muss eine Organisation ein deutliches Gewicht auf das Management der Schwachstellen und damit verbundenen Risiken legen. Die Cyber-Abwehr muss mit einem ständigen Strom neuer Informationen operieren: Software-Updates, Patches, Sicherheitshinweise, Threat-Bulletins oder ähnli-

VULNERABILITY-MANAGEMENT-LÖSUNGEN MACHEN DEN PROZESS DES VULNERABILITÄTS-MANAGEMENTS ZU EINER TÄGLICHEN ROUTINE, VEREINFACHEN DIE BESEITIGUNG UND BERICHTERSTATTUNG UND SENKEN DIE GESAMTBETRIEBSKOSTEN (TCO).

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

ches. Es ist wichtig, Schwachstellen zu identifizieren, die die sofortige Aufmerksamkeit erfordern. Zu den Grundlagen eines Vulnerability-Managements gehört eine vollständige Bestandsaufnahme aller Hardware- und Software-Assets im gesamten Unternehmensnetzwerk.

Bevor Sie Ihre Angriffsfläche angemessen schützen können, müssen Sie alle darin enthaltenen Assets identifizieren. Ein effektives risikobasiertes Schwachstellenmanagement erfordert einen klar definierten Prozess.

## Hoher Aufwand des Schwachstellenmanagements

Die Verwaltung der unzähligen Konfigurationen innerhalb der Systemkomponenten mit manuellen Methoden ist zu einer unmöglichen Aufgabe geworden. Deshalb besteht dringender Bedarf nach automatisierten Lösungen, die langfristig Kosten senken, die Effizienz steigern und zuverlässig sind.

Vulnerability-Management-Lösungen machen den Prozess des Vulnerabilitäts-Managements zu einer täglichen Routine, vereinfachen die Beseitigung und Berichterstattung und senken die Gesamtbetriebskosten (TCO). Diese Lösungen helfen, Schwachstellen in einem Unternehmen zu identifizieren, zu klassifizieren, zu beseitigen und zu mindern.

Schwachstellen-Management-Anwendungen können aber sehr komplex sein, beanspruchen viel Netzwerkbandbreite und Systemressourcen. Deshalb zögern immer noch Unternehmen, tägliche Schwachstellen-Scans durchzuführen. Und selbst nachdem ein Scan abgeschlossen ist, stehen IT-Abteilungen vor der Frage, wie sich Schwachstellen leicht beheben lassen.

## Welche Normen sollten erfüllt werden?

Für Organisationen mit einer großen Anzahl von Systemkomponenten liegt die einzige praktische und effektive Lösung darin, automatisierte Lösungen zu verwenden, die standardisierte Berichtsmethoden verwenden. Sie sind gut beraten, sogenannte SCAP-validierte Lösungen in die engere Auswahl zu nehmen. SCAP bedeutet Security Content Automation Protocol (Protokoll zur Automatisierung von Sicherheitsinhalten) und bietet eine gemeinsame „Sprache" zur Beschreibung von Schwachstellen, Fehlkonfigurationen und Produkten. SCAP umfasst eine Reihe von Spezifikationen, die das Format und die Nomenklatur standardisieren, mit denen Informationen über Software-Fehler und sichere Konfigurationen übermittelt werden können.

Beispielsweise ist das Common Vulnerability Scoring System (CVSS) eine Spezifikation innerhalb von SCAP, die einen offenen Rahmen für die Kommunikation der Merkmale von Softwareschwachstellen und für die Berechnung ihres relativen Schweregrads bietet. Die CVE-Spezifikation vergibt eindeutige gemeinsame Namen für öffentlich bekannte Schwachstellen in Informationssystemen.

## Der DriveLock Schwachstellen-Scanner

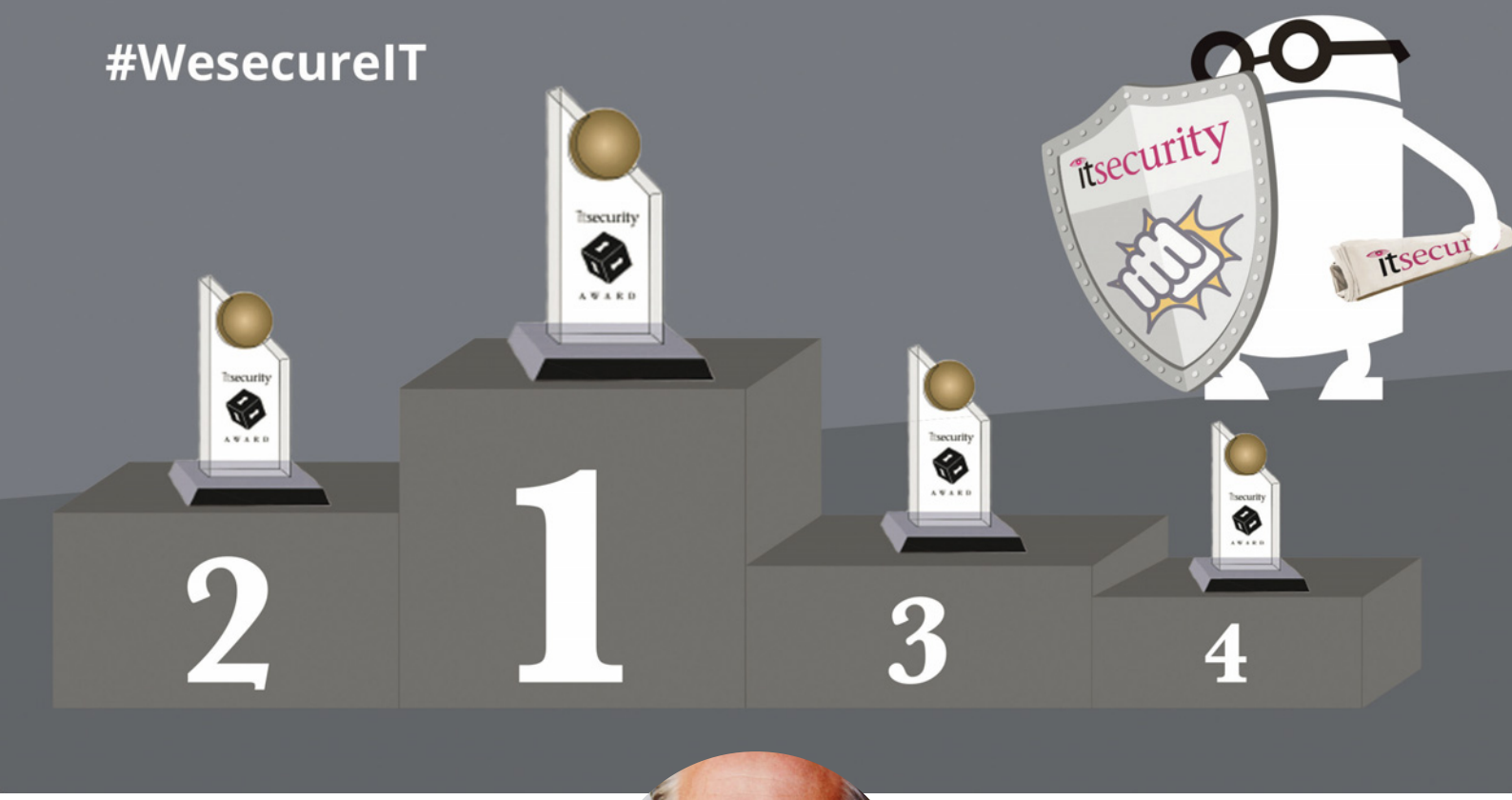
Die DriveLock Vulnerability-Management Lösung identifiziert Schwachstellen auf den Endpoints und trägt zur Verhinderung potenzieller Malware-Angriffe bei. IT-Administratoren können die mit Schwachstellen verbundenen Risiken identifizieren und kontrollieren.

So ist eine kontinuierliche Bewertung von Sicherheits- und Risiko-Position möglich, unbekannte Assets und Schwachstellen werden entdeckt und Schwachstellen priorisiert, um das Cyberrisiko zu minimieren und Verletzungen zu verhindern. Die Lösung baut auf einer täglich aktualisierten SCAP Feed-Datenbank auf und enthält unter Verwendung eines OVAL-Scanners eine Sprache zur Kodierung von Systemdetails. Der DriveLock-Schwachstellen-Scanner sucht automatisch nach Schwachstellen in einem Computersystem. Er tut dies ad-hoc oder auf geplanter regelmäßiger Basis.

***Andreas Fuchs***

# itsecurity AWARD 2020

## GEWINNER IM RAHMEN DER „WE SECURE IT“ AUSGEZEICHNET




Der erste Digitalevent von it security war am 1. Oktober auch Schauplatz für die Verleihung der IT SECURITY AWARDS. Bereits seit 2007 verleiht das Fachmagazin it security jährlich diese Preise. Eine hochkarätige Jury wählt die besten Projekte und Produkte in den Kategorien Web/Internet Security, Identity & Access Management, Cloud Security und Management Security aus. Nun stehen die Preisträger der vier IT SECURITY Awards 2020 fest. Es sind Fortinet, Attivo Networks, Thycotic und Forcepoint.

### Management Security: Fortinet

Die FortiGate 4400F ist die erste Hyperscale-Firewall der Welt. Sie nutzt sicherheitsorientierte Netzwerkprinzipien, um hochskalierbare, sichere verteilte Netzwerke und Hyperscale-Rechenzentren zu ermöglichen. Die FortiGate 4400F setzt neue Maßstäbe für Security Compute Ratings und liefert konkurrenzlose Performance, Skalierbarkeit und Sicherheit in einer einzigen Appliance. Sie basiert auf Fortinets neuestem NP7-Netzwerkprozesser der siebten Generation, der Hardware-Beschleunigung bietet. Als einzige Firewall auf dem Markt ist sie dadurch schnell genug, um Hyperscale-Rechenzentren und 5G-Netzwerke abzusichern.

FORTINET ERMÖGLICHT DANK IMMER BESSERER, HARDWARE-BESCHLEUNIGTER PERFORMANCE DIE KONVERGENZ VON SICHERHEIT UND VERNETZUNG. WIR NENNEN DIES EINEN SICHERHEITSORIENTIERTEN NETZWERKANSATZ.

Christian Vogt, VP DACH, Fortinet, www.fortinet.com

Damit ist die Absicherung von Hpyerscale-Netzwerk-Infrastrukturen etwa im Online-Handel möglich sowie die sichere Übertragung auch von Elephant Flows und die SecGW-Implementierung von 5G.

IMMER MEHR UNTERNEHMEN WÜNSCHEN SICH EFFEKTIVE LÖSUNGEN, UM PRIVILEGIERTE ZUGRIFFE NACHHALTIG ABZUSICHERN UND FUNKTIONIERENDE APPLIKATIONSKONTROLLEN SOWIE LEAST PRIVILEGE-STRATEGIEN UMZUSETZEN.

Stefan Schweizer, Regional Vice President Sales DACH, Thycotic, www.thycotic.com

## Web/Internet Security: Attivo Networks

Attivo Networks bietet eine umfassende Deception-Plattform, die in Echtzeit Einbrüche in Netzwerke, öffentliche und private Datenzentren und spezialisierte Umgebungen wie SCADA, Industrial Control Systems (ICSs), Internet of Things (IoT) und POS-Umgebungen (Point of Sale) erkennt. Ausgehend von der Prämisse, dass selbst die besten Sicherheitssysteme nicht alle Angriffe verhindern können, bietet Attivo die erforderliche Visibilität und verwertbare, fundierte Warnmeldungen, um Cyberangriffe zu erkennen, zu isolieren und abzuwehren. Im Gegensatz zu herkömmlichen Präventions-Systemen geht Attivo davon aus, dass sich der Angreifer innerhalb des Netzwerks befindet. Es verwendet hochgradig interaktive Köder am Endpunkt, in Server-Umgebungen und Anwendungen.

Diese werden allgegenwärtig im Netzwerk platziert, um Bedrohungsakteure so zu täuschen, dass sie sich preisgeben. Der BOTsink-Deception-Server ist so konzipiert, dass er die Seitwärtsbewegung fortgeschrittener Bedrohungen im Netzwerk sowie den Diebstahl von Berechtigungsnachweisen präzise und effizient erkennt. Ferner erkennt er Ransomware, Man-in-the-Middle- und Phishing-Angriffe, ohne von Signaturen oder dem Abgleich von Angriffsmustern abhängig zu sein.

Die Attivo Multi-Correlation Detection Engine (MCDE) erfasst und analysiert Angreifer-IP-Adressen, Methoden und Aktionen, die dann im Attivo Threat Intelligence Dashboard angezeigt, und für die forensische Berichterstattung im IOC-, PCAP-, STIX- und CSV-Format exportiert werden können. Sie können ebenfalls zur automatischen Aktualisierung von SIEM- und Präventionssystemen zur Blockierung, Isolierung und Bedrohungsverfolgung verwendet werden können. Das ThreatOps-Angebot vereinfacht die Vorfallsreaktion durch Informationsaustausch, Automatisierung und die Erstellung wiederholbarer Playbooks.

Insgesamt gesehen ergibt sich eine Verkürzung der Verweildauer (Dwell-Time), die schnelle Erkennung maliziöser Insider und eine Erhöhung der Visibilität von Angreifern in einem Netzwerk.

## Identity & Access Management: Thycotic

80 Prozent aller Sicherheitsvorfälle sind auf den Missbrauch von kompromittierten Zugangsdaten für Privileged Accounts zurückzuführen, da diese meist nur unzureichend geschützt werden.

Mit Thycotics Secret Server und Privilege Manager profitieren Unternehmen von sofort einsatzbereiten, benutzerfreundlichen und skalierbaren Enterprise-Lösungen für Passwortmanagement und die Verwaltung von Benutzerrechten. Sie unterstützen IT-Abteilungen dabei, privilegierte Unternehmenskonten effektiv vor Missbrauch durch Hacker und Insider-Angreifer zu schützen, und ermöglichen ihnen eine effiziente Administration aller Zugriffe.

Privilegierte Accounts wie Administrator-, Service-, Maschinen- oder Datenbank-Konten sind Hauptangriffsziel für Cyberkriminelle, da Angriffe über diese Accounts großes Potenzial für weitreichenden Datenmissbrauch eröffnen. Dieses Risiko wird mit Thycotic drastisch minimiert: Zum einen bietet der Secret Server Unternehmen ein effektives Passwortmanagement, bei dem privilegierte Unternehmenskennwörter sicher erstellt, kontrolliert und automatisch gewechselt werden. Dabei werden die Teammitglieder in Echtzeit über Passwortänderungen informiert, um Beeinträchtigungen zu vermeiden. Zum anderen sorgen spezielle Privileged Behavior Analytics-Fähigkeiten für eine vollständige Transparenz über die Aktivitäten sämtlicher administrativer Benutzer sowie alle Zugriffe. Dabei kommen Machine Learning-Technologien zum Einsatz, mit deren Hilfe Benutzeraktivitäten auf Basis von individuellen Verhaltensmustern analysiert und verdächtige Zugriffe automatisch gemeldet werden.

Mit Thycotics Privilege Manager können Unternehmen zudem bequem eine minimale Rechtevergabe umsetzen und den potenziellen Missbrauch privilegierter Accounts weiter einschränken. Dabei unterstützt die Lösung IT-Abteilungen beim sorgfältigen Löschen aller lokalen Adminrechte, einschließlich verborgener und hartcodierter Berechtigungsnachweise, sowie beim Einrichten von White- und Blacklists, die festlegen, welche Anwendungen unter welchen Bedingungen ausgeführt werden.

Als Fazit können automatisierte Prozesse bei der Identifizierung von privilegierten Konten helfen und eine vollständige Transparenz aller Zugriffe entlasten die IT-Abteilungen nachhaltig.

Um den hohen Anforderungen von DevOps hinsichtlich Geschwindigkeit und Skalierbarkeit nachzukommen, hat Thycotic seine Lösung um einen DevOps Secret Vault erweitert, der eine sichere Verwaltung von dynamischen (automatisch wechselnden) Zugangsdaten er-

möglicht, ohne den Entwicklungsprozess zu stören.

## Cloud Security: Forcepoint

Ausgezeichnet wurde das Forcepoint Cloud Security Gateway – SASE. Vorgestellt im Juli 2020, handelt es sich um eine echte Security Access Service Edge (SASE)-Lösung, die Web, Cloud- und Data-Security in einer einzigen converged Plattform verbindet.

Unternehmen waren 2020 von einem Tag auf den anderen gezwungen, Remote Working drastisch auszubauen. Spätestens damit wurden physische Grenzen aufgelöst, klassische Sicherheitstools können diese dezentrale Organisation nicht mehr absichern. Dazu kommt, dass ein normales Unternehmen schon zuvor im Durchschnitt ca. 50 verschiedene Sicherheits-Anbieter nutzt, was schnellen Wandel noch zusätzlich erschwert.

Forcepoint CSG fasst zentrale Cloud-Security-Lösungen (Data Loss Prevention, Cloud Access Security Broker und Secure Web Gateway) in einer Plattform zusammen und schafft Sichtbarkeit, Kontrolle und Bedrohungsschutz für Nutzer und Daten, unabhängig davon, wo diese sind. Eine Reduktion von Einzel-Lösungen spart Kosten und verringert die Komplexität sowie den Verwaltungsaufwand.

NICHT NUR DATEN, SONDERN AUCH NUTZER SIND HEUTE NICHT MEHR AN EINEN STANDORT GEBUNDEN – UND CISOS MÜSSEN SIE SCHÜTZEN: ÜBERALL IMMER UND AUF JEDEM GERÄT. DAFÜR MUSS IT-SICHERHEIT DAHIN GEHEN WO NUTZER MIT DATEN INTERAGIEREN. DIE ZUKUNFT DER IT-SECURITY LIEGT IN DER CLOUD.

Frank Limberger,
Data and Insider Threat Specialist,
Forcepoint, www.forcepoint.com

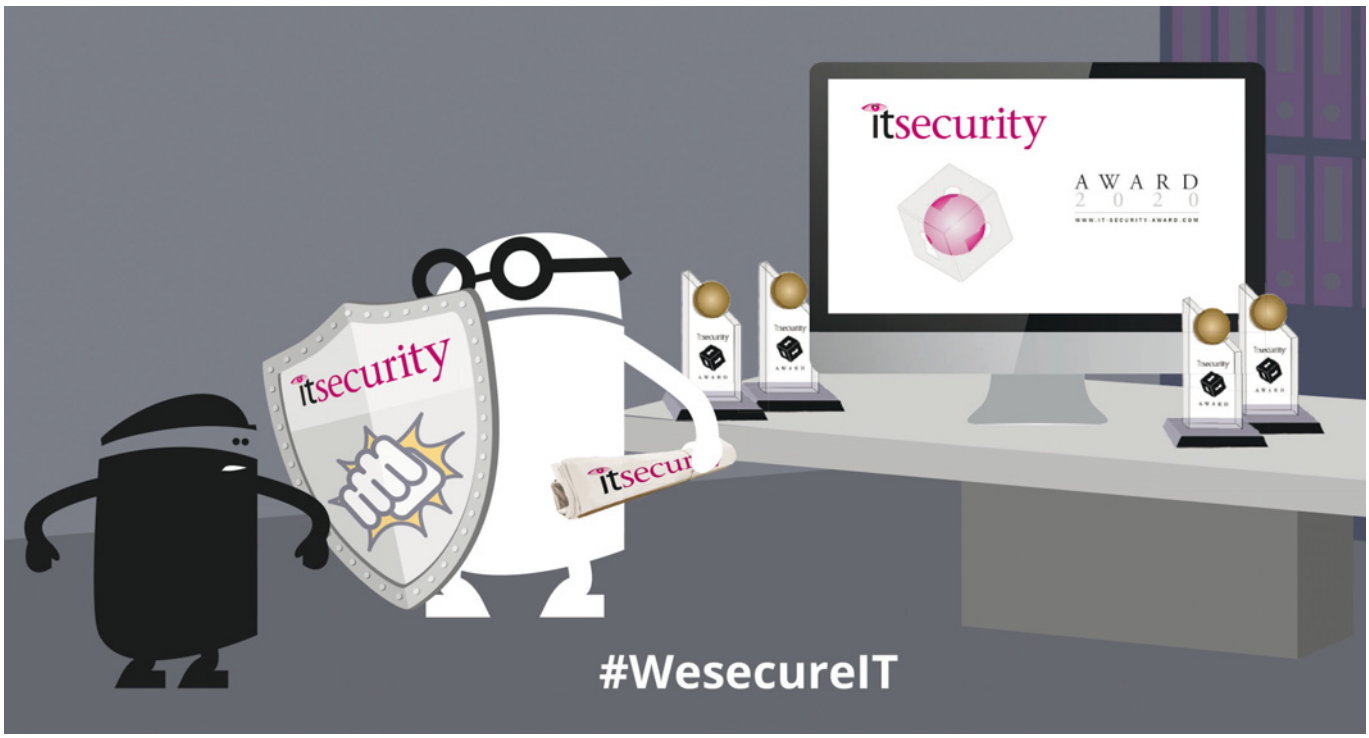
**Vorteile von Forcepoint CSG sind unter anderem:**

- Einheitliche Web-Protection und -Policies für alle Nutzer, innerhalb und außerhalb klassischer Unternehmens-Grenzen
- Schutz vor Bedrohungen aus Web und Cloud (CASB, DLP, SWG)
- Sichtbarkeit für Schatten-IT und sicherheitsrelevante Abläufe im Unternehmen
- Kosteneinsparung und einheitliche Verwaltung von Policies
- Schnellere Durchsetzung von Compliance-Vorgaben

## Fazit

Die Unternehmens-IT verändert sich kontinuierlich. Nutzer und Daten sind nicht mehr an einen Standort gebunden – und CISOs müssen sie schützen.
Das neue Credo lautet: überall, immer und auf jedem Gerät bei voller Abdeckung hybrider Umgebungen.

***Ulrich Parthier***




# ICH BRAUCHE KEINE CLOUD

## ICH BRAUCHE EINE LÖSUNG

Um die Cloud kommt am Ende kein Unternehmen mehr herum. Die Frage ist nicht, ob, sondern in welchem Umfang. Aber Sie haben recht: Nicht alles muss in die Cloud. Stattdessen kann man auch die eigene IT so elastisch, schlagkräftig und günstig aufstellen, dass sie von den angeschlossenen Cloud-Diensten mit bloßem Auge nicht zu unterscheiden ist.

**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 15 Seiten und steht kostenlos zum Download bereit.

***www.it-daily.net/download***

# DAS ERP-INNOVATIONSDILEMMA

## ERKENNTNISSE ZUR ERP-MODERNISIERUNG


Trotz all der Vorteile durch Innovationen und Modernisierungen stehen Unternehmen immer noch vor Problemen, die durch Hybrid-IT entstehen. 42 Prozent gaben Hybrid-IT als Grund dafür an, nicht die heutzutage von Unternehmen erwartete Geschwindigkeit bieten zu können.

Es überrascht also nicht, dass Unternehmen in EMEA Herausforderungen mit Hybrid-IT direkt angehen. Die drei wichtigsten Projekte sind dabei Standardisierung und Konsolidierung von Anwendungen (76 %), Migration der Infrastruktur zur Cloud (75 %) und Konsolidierung der Legacy-Infrastruktur (69 %).

Diese Projekte untermauern die kritischen Geschäftsanforderungen von Unternehmen in EMEA, die da lauten: Bereitstellung einzigartiger Kundenerfahrungen, Anwendungsintegration und Agilität. Nur intelligente Technologie kann dies leisten. Die größte Herausforderung besteht darin, die Jahrzehnte alten ERP-Kernsysteme hinter sich zu lassen.

CIOs haben derzeit die Wahl: Entweder sie investieren viel und folgen dem Trend cloudbasierter ERP-Systeme oder sie üben sich in Zurückhaltung und riskieren dabei, den Anschluss zu verpassen.

**WHITEPAPER DOWNLOAD**

Das Whitepaper umfasst 20 Seiten und steht kostenlos zum Download bereit.

***www.it-daily.net/download***

# HYPERAUTOMATION UND ÖKOSYSTEME

## ALLES WIRD MITEINANDER VERNETZT

Die Digitale Transformationen und ihre Technologien durchdringen nahezu jede Branche und jede Abteilung. Digitale und miteinander vernetzte Ökosysteme bringen mit intelligenten Anwendungen und Services Kunden und Partner näher zusammen. Mit Hilfe dieser Ökosysteme können Unternehmen beziehungsweise deren Systeme miteinander kommunizieren. Mittels Hyperautomation können Unternehmen sogar noch einen Schritt weitergehen: Unterschiedliche Systeme können sowohl innerhalb als auch außerhalb miteinander verbunden werden, so dass diese autonom, also automatisiert, miteinander kommunizieren, Prozesse anstoßen und gegebenenfalls Projekte handhaben.

Hyperautomation geht über die typische Automatisierungsstrategie hinaus und ist eine Kombination fortschrittlicher Technologien wie Künstliche Intelligenz, Maschinelles Lernen, Process Mining sowie Robotic Process Automation. Alles ist darauf ausgerichtet, die Automatisierung von Prozessen und Arbeitsabläufen in einem Unternehmen zu verbessern. Software-Roboter übernehmen dabei wiederkehrende oder monotone Aufgaben eines Mitarbeiters, so dass der beispielsweise mehr Zeit für die Kundenberatung haben.

Der nächste Schritt in Sachen Automatisierung ist die Implementierung und Integration weiterer Ökosysteme. Wenn also Roboter in ein Ökosystem eines Unternehmens integriert werden, können sie beispielsweise auch in einem weiteren externen Ökosystem eingebaut werden, so dass ein gemeinsames übergeordnetes System entsteht, das dann zusammenarbeitet und wenn nötig, dennoch autark ist.

### Automatisierung des Kundenservice

Die Implementierung von Automatisierung im Kundenservice bietet zahlreiche Vorteile für den Wertschöpfungsprozess im Unternehmen und steigert die Effizienz und Produktivität der Mitarbeiter. Die eingesetzten Software-Roboter sind wartungsarm, flexibel, skalierbar und eine ri-

sikoarme Alternative zu anfälligen API-Integrationen, die nur schwer zu aktualisieren sind, wenn sich Prozesse ändern.

Im Kundenservice geschieht Automatisierung entweder im Hintergrund durch eine Steigerung der Prozesseffizienz oder im direkten Kontakt mit den Kunden. Automatisierung beziehungsweise Hyperautomation und die Vernetzung weiterer Ökosysteme ermöglicht es Mitarbeitern durch das Zusammenführen der Daten aus verschiedenen Systemen und Anwendungen, sich auf die Interaktion mit den Kunden zu konzentrieren, anstatt sich durch ineffiziente Prozesse zu navigieren, bei denen sie manchmal zwischen mehreren Systeme wechseln und auf Antwort von angegliederten Partnern warten müssen. Mittels Automatisierung können Unternehmen den Umfang der Datenverarbeitung, die von den Menschen durchgeführt werden muss, reduzieren. Die Nachbearbeitungszeit kann durch Roboter minimiert werden. Denn die automatische Erfassung und Weitergabe von Daten sorgt für Optimierung und Effizienz. Die durch die Automatisierung verkürzte Bearbeitungszeit, sorgt dafür, dass Kundenanliegen schneller bearbeitet werden können, was wiederum den Kunden und dem Unternehmen zugutekommt. Das Kundenerlebnis kann somit verbessert, Prozesse beschleunigt, IT vereinfacht und Compliance sichergestellt werden.

## Das intelligente, vernetzte Ökosystem

Nehmen wir als Beispiel den Möbelkauf: Abstrakt lässt sich dieser runterbrechen auf: Kunde kommt ins Möbelfachgeschäft, sucht sich beispielsweise eine neue Küche aus, hat eventuell noch einen Sonderwunsch bezüglich Ausstattung, den er mit dem Verkäufer abklärt, kauft die Küche und lässt sich diese ein paar Wochen später nach Hause liefern.

Was zunächst einfach klingt, ist im Back-End komplex. Denn der Verkäufer muss die Daten des Käufers prüfen (zum Beispiel: ist er überhaupt liquide), die Sonderausstattung oder andere Details mit dem Hersteller beziehungsweise sogar mit dem Zulieferer des Herstellers (können die Details überhaupt so umgesetzt werden) abklären, der Liefertermin muss überprüft und der Kauf-Vertrag fertig gemacht werden. Hier müssen also unterschiedliche Unternehmen und Abteilungen miteinander kommunizieren. Bisher geschieht das häufig noch manuell, da die verwendeten Systeme nicht miteinander vernetzt sind und daher nicht kommunizieren können. Teilweise werden Daten manuell noch aufbereitet, damit diese von einem System ins anderes übertragen werden können.

DURCH HYPERAUTOMATION WERDEN KOSTEN REDUZIERT UND DIE ANZAHL VON FEHLERN MINIMIERT. EIN VERNETZTES ÖKOSYSTEM BRINGT NEUE MÖGLICHKEITEN FÜR UNTERNEHMEN UND DEREN KUNDEN.

Sabine Obermayr,
Marketing Director Central Europe, UiPath,
www.uipath.com/de

Software-Roboter eines intelligenten und umfassend vernetzten Ökosystems könnten viele dieser Aufgaben erledigen. Dabei können sie beispielsweise nicht nur die Datenübertragung von einem Format ins andere übernehmen, sondern auch einen Schritt weiter „denken." Anhand des Beispiels mit der Sonderausstattung könnte das wie folgt aussehen: der Mitarbeiter des Möbelfachgeschäfts gibt den Wunsch des Kunden, beispielsweise eine Geschirrspülmaschine mit LED-Anzeige, ins System ein. Anstatt dass ein weiterer Mitarbeiter nun im Back-End die nötigen Informationen manuell einholt und dabei unter Umständen stunden- oder gar tagelang warten muss, kann diese der Software-Roboter bei seinem Pendant beim Hersteller oder Zulieferer anfragen. Dieser prüft daraufhin, ob die Konfiguration so möglich ist und vor allem bis wann diese lieferbar wäre. Diese Informationen werden an den Software-Roboter im Möbelfachgeschäft zurückgespielt. Der Mitarbeiter sieht somit direkt, ob der Wunsch des Kunden möglich ist. Gibt der Kunde dann sein „go", kann der Mitarbeiter den Software-Roboter die weiteren Schritte anschieben lassen. Er bestellt die Küche inklusive aller Sonderwünsche, gibt seinen digitalen Kollegen in der Rechtsabteilung Bescheid, dass ein Vertrag für den Kauf aufgesetzt werden muss und lässt den Mitarbeiter diesen dann direkt in den Druck bringen, so dass er dem Kunden ausgehändigt werden kann.

## Hyperautomation

Durch Hyperautomation werden Kosten reduziert und die Anzahl von Fehlern minimiert. Ein vernetztes Ökosystem bringt neue Möglichkeiten für Unternehmen und deren Kunden. Denn Mitarbeiter können deutlich schneller auf die Bedürfnisse der Kunden reagieren und eine personalisierte und optimierte Customer Experience schaffen.

Das Beispiel des Küchenkaufs lässt sich selbstverständlich auf weitere Szenarien adaptieren: Patienten in einem Krankenhaus, ein Neukunde einer Bank, eine Schadensmeldung bei einer Versicherung oder die Bestellung eines Autos im Autohaus. Mittels vernetzter Ökosysteme entstehen ungeahnte Möglichkeiten für Unternehmen, sich wettbewerbsfähig für die Zukunft zu rüsten. Den Faktor Mensch wird Automatisierung jedoch in der Arbeitswelt und speziell im Kundenservice insbesondere bei komplexen Anliegen nicht ersetzen – der Einsatz von Automatisierung wird in Kooperation mit den Mitarbeitern geschehen, um ihn zu entlasten und ihm die Zeit verschaffen, die er für einen erstklassigen Kundenservice benötigt.

***Sabine Obermayr***

# IAM CONNECT 2020

## Die Brücke zu neuen Geschäftsmodellen

**Auf der deutschsprachigen Konferenz zum Thema Identity & Access Management teilen erfahrene Praktiker, Vordenker und Querdenker ihre Erfahrungen und Visionen mit Ihnen.**

## Hybride Konferenz
## 30.11. bis 02.12.2020
## in Berlin

**www.iamconnect.de**

Sie haben die Wahl

- vor Ort im **Berliner Hotel Marriott** teilzunehmen oder
- die Veranstaltung per **Video Stream** zu verfolgen.

In virtuellen Meetingräumen können Sie die Aussteller besuchen, mit ihnen sprechen und sich Produkte vorführen lassen.

### Hauptsponsor

ipg
EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

### Speed Demo Sessions

AIRLOCK®
SECURE ACCESS HUB

Auth0

betasystems

DIERICHSWEILER
Unternehmens- und Prozessberatung

Eine Veranstaltung von itmanagement & itsecurity

# Highlights aus der Agenda

## Vorträge

**Wie alles begann**

Prof. Dr.-Ing. habil. Horst Zuse ist der Sohn des Erfinders des Computers Konrad Zuse. Er berichtet von den frühesten Entwicklungen.

**Kundenorientiertes Projekt-management mit Design Thinking**

Prof. Dr. Falk Uebernickel, Hasso-Plattner-Institut für Digital Engineering gGmbH

**Ordnung im Berechtigungs-Dschungel: Erfahrungsbericht**

Dr. Peter Katz,
KPT Krankenkasse

**Einführung einer neuen IAM-Lösung bei der Thüringer Aufbaubank**

Cindy Schöneck,
Thüringer Aufbaubank

**Individualisierung, oder: Muss es immer die Oberfläche des Herstellers sein?**

Clemens Wunder,
Bundesagentur für Arbeit

**IAM im industriellen IoT-Umfeld: Erfahrungsbericht zur Digitalisierung in Fertigung und Produktion**

Mathias Winter,
PI Informatik GmbH Berlin

## Workshops

**Minimaler Aufwand, maximale Sicherheit: Dos and Don'ts für erfolg-reiches Berechtigungsmanagement**

Dr. Ludwig Fuchs,
Nexis GmbH

**IAM für Internet-Dinger (IoT)**

Peter Weierich,
IPG GmbH Deutschland

**Rechtliche Herausforderungen im IAM**

Ralf Schulten, Rechtsanwalt,
avocado rechtsanwälte

NEXIS ONE IDENTITY Ping Identity. Telia

# CUSTOMER CENTRICITY

## EIN MUSS IM DIGITALEN ZEITALTER

Kunden-Hotlines, Chatbots und personalisierte Ansprachen gehören heute zum Standard-Repertoire im Customer Service eines jeden Unternehmens. Denn: Die Kunden sind kritischer geworden. Welcher Marke, welchem Produkt und welcher Dienstleistung sie ihr Vertrauen schenken und warum, entscheiden allein sie. Die Sieger sind diejenigen Unternehmen, die von Beginn an die Bedürfnisse ihrer Kunden verstanden und berücksichtigt haben und darauf aufbauend einen herausragenden Service bieten. Die Digitalisierung unterstützt Unternehmen dabei, ihre Strategien und Wertschöpfungsketten auf die Wünsche ihrer Kunden auszurichten. Customer Centricity lautet hier das Zauberwort. Wer also auch in Zukunft wettbewerbsfähig bleiben will, tut gut daran, sich mit diesen Themen auseinanderzusetzen.

### Hand in Hand gehen

Märkte werden transparenter und schnelllebiger – was heute im Trend ist, kann morgen schon längst wieder veraltet sein. Lokale Retailer konkurrieren mit internationalen Playern, neue Kommunikationskanäle, das Internet of Things und neue Methoden zur Echtzeitanalyse von riesigen Datenbeständen durchdringen den Markt. Kurzum: Die Art und Weise, Handel zu treiben, hat sich verändert und ruft damit auch neue Geschäftsmodelle hervor.

Man kann die Digitalisierung heute als Grundvoraussetzung sehen, um die stetig wachsenden Herausforderungen für den Einzelhandel und Online-Retail sowie die digitale Informationsbeschaffung in Wirtschaft und Gesellschaft zu meistern. Für Einzelhändler und Retailer ist sie die Basis, um Customer Centricity nachhaltig in der eigenen Unternehmensstruktur und -kultur zu verankern. Im Zentrum stehen natürlich die Kunden. Denn nur wer eine enge Beziehung zu ihnen aufbaut, sammelt Daten, die – richtig eingesetzt – einen Rund-um-Blick auf die Kundenbedürfnisse ermöglichen. Diese Insights können Unternehmen für die Weiterentwicklung ihrer Produkte und Dienstleistungen nutzen und die Customer Journey optimieren. Die logische Konsequenz lautet also: Einzelhändler und Retailer sollten sich auf ihre eigene digitale Transformation fokussieren, um sich auf dieser Basis zu einer kundenzentrierten Organisation zu entwickeln.

DER WEG ZU EINEM DIGITALEN KUNDENORIENTIERTEN UNTERNEHMEN IST KOMPLEX UND GESCHIEHT NICHT VON HEUTE AUF MORGEN.

Marc Bohnes,
Product Management Director, Episerver,
www.episerver.de

### Wo liegen die Herausforderungen?

Viele Unternehmen neigen dazu, diese Themen zu sehr zu analysieren und komplett durchdringen zu wollen, bevor sie diesen Schritt wagen. Aber gerade im Bereich Digitalisierung ist das in dieser schnelllebigen Zeit beinahe unmöglich. Oft genügt es, loszulegen, zu experimentieren und Schritt für Schritt vorzugehen. Und ja, dabei dürfen Fehler gemacht werden. Hier gilt es eine Resilienz gegenüber der Furcht vor dem Unbekannten zu etablieren. Das alte Sprichwort „learning by doing" hält in dieser Hinsicht etwas durchaus Erfrischendes bereit.

Unternehmen sollten außerdem darauf achten, dass es bei der Transformation nicht in erster Linie um die eigenen Produkte und Dienstleistungen geht, sondern darum eine fundierte Strategie zur digitalen Transformation zu entwickeln, die die entsprechenden Möglichkeiten zur technischen Umsetzung schafft. Dazu gehören beispielsweise die IT-Infrastruktur, technisches Equipment oder Mobile-First-Ansätze. Darauf aufbauend gilt es, eine digitale offene Kultur zu entwickeln, in der das Unternehmen in der Lage ist, sich gemeinsam mit seinen Kunden auszuprobieren und entsprechende Projekte umzusetzen. Dabei muss natürlich stets gewährleistet sein, dass Privatsphäre und Kundendaten geschützt werden.

Einen großen Vorteil haben dabei Unternehmen, die die Transformation aus eigenem Antrieb starten. Sie haben ausreichend Zeit zur Verfügung, um eine solide Strategie zu entwickeln und die notwendigen Budgets und Ressourcen zu schaffen. Kommt der Druck von außen, beispielsweise durch die aktuelle Corona-Krise oder neue Regularien, wird es häufig schwierig, adäquat (und vor allem zeitnah) zu reagieren, da womöglich finanzielle Engpässe vorliegen oder die notwendige Infrastruktur noch nicht vorhanden ist. So erging es beispielsweise der norwegischen Supermarktkette Coop, als die norwegische Regierung im Rahmen der Corona-Krise beschloss, dass Lebensmittel nun verstärkt online angeboten werden sollen, um das Social Distancing zu fördern. Coop hat es allerdings geschafft, eine Customer Experien-


Die Digital Experience Platform ermöglicht es, von den Kunden zu lernen, ihr Vertrauen zu gewinnen und ihnen mithilfe von KI das beste digitale Kundenerlebnis zu bieten.

ce zu schaffen, die dem Einkauf im stationären Einzelhandel schon sehr nahekommt. So hat der Kunde die Möglichkeit, schnell und jederzeit sichtbar seinen Warenkorb zu betrachten oder dem Mitarbeiter eine Nachricht zu hinterlassen, was beim Einpacken der Waren beachtet werden soll (beispielsweise Alternativen zu bereits vergriffenen Produkten).

**So klappt der Change-Prozess**

Change-Prozesse sind kompliziert, erfordern Flexibilität und einen großen Transformationswillen. Dabei stoßen sie nicht selten auf Widerstand, da sie gnadenlos aufdecken, an welchen Stellen es im Unternehmen hapert. Oftmals können sich Mitarbeiter nicht mit den anstehenden Veränderungen identifizieren, fühlen sich übergangen und vor vollendete Tatsachen gestellt. Um das zu verhindern, muss das Unternehmen transparent, klar und glaubwürdig kommunizieren, warum Veränderungen anstehen, welche Vorteile diese für das Unternehmen und die Mitarbeiter haben und dass diese vor allem aktiv mitgestalten können und sollen. Dieses Versprechen muss das Management anschließend sukzessive und gemeinsam mit den Mitarbeitern umsetzen. Ein offenes Ohr für Anmerkungen, Feedback und Sorgen ist dabei unerlässlich. Nur so entsteht ein konstruktiver Prozess. Je nach Unternehmensgröße ist das natürlich mit einem großen Organisationsaufwand verbunden, aber er lohnt sich. Denn wenn das ganze Unternehmen an einem Strang zieht, entsteht die Transformation von innen heraus. Und nur eine intrinsische Strategie, die jeden Mitarbeiter mitnimmt und ihm aufzeigt, weshalb Progression nötig beziehungsweise notwendig ist, kann am Ende auch erfolgreich sein.

**Customer Centricity in der Praxis**

Der Premiumschokoladenhersteller Neuhaus aus Brüssel hat sich ebenfalls auf das Abenteuer digitale Transformation und Customer Centricity eingelassen. Das Unternehmen setzte lange Zeit auf eigene Boutiquen in Belgien und Deutschland sowie den Vertrieb über verschiedene Luxuskaufhäuser. Im Zuge der wachsenden Digitalisierung stellte sich Neuhaus allerdings die Frage, wie sich das Geschmackserlebnis und die Beratung vor Ort auch online umsetzen lassen. Das oberste Ziel: Alle Kunden sollen sowohl online als auch offline vom selben Shopping-Erlebnis profitieren.

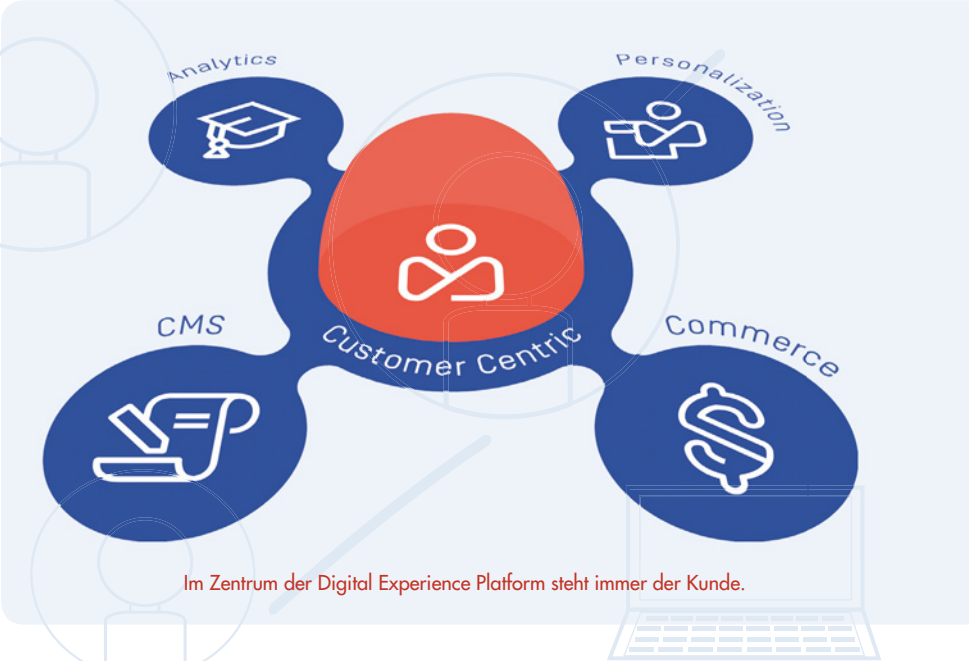
Personalisierung ist dabei ein ausschlaggebender Faktor. Durch individuelle Produktempfehlungen via E-Mail und im Webshop sowie auf Basis der Kundenkonten analysiert Neuhaus nun Schokoladengeschmack, Vorlieben und Kaufgewohnheiten und kann so die Kunden gezielt ansprechen. Das Unternehmen hat auf der Webseite außerdem einen Chatbot implementiert, der die User berät, Informationen zu den verschiedenen Schokoladenkreationen bereithält oder über Themen wie ethische Bezugsquel-

len, Nachhaltigkeit und Umweltauswirkungen informiert. Für den Versand hat Neuhaus eine spezielle Verpackung entwickelt, um den Kunden ein hochwertiges „Unboxing"-Erlebnis zu bieten.

Damit auch Online-Kunden das Sortiment von Neuhaus kennenlernen, hat das Unternehmen Neuhaus Insiders – eine Art Newsletter-Club – gegründet. Die Mitglieder profitieren hier von kostenlosen Kostproben, um neue Kollektionen kennenzulernen, sie erhalten ein Geburtstagsgeschenk oder werden zu exklusiven VIP-Events eingeladen.

Wir sehen: Der Weg zu einem digitalen kundenorientierten Unternehmen ist komplex und geschieht nicht von heute auf morgen. Doch gerade die Möglichkeiten der Digitalisierung, Big Data und das Einbeziehen von Kunden und Usern eröffnen neue Wege, das Thema Customer Centricity anzugehen. Am Ende kommt es dabei auf genau drei Dinge an: Kultur (Dinge ausprobieren), Struktur (Technologien nutzen und die interne Digitalisierung vorantreiben) und Strategie (maximale Orientierung am Kunden). So gelingt der Weg hin zu einer erfolgreichen Customer Centricity in Zeiten schnelllebiger digitaler Prozesse.

***Marc Bohnes***




Im Zentrum der Digital Experience Platform steht immer der Kunde.

# BIG DATA UND ANALYTICS

## KI UND ML AUF DEM VORMARSCH

Die Datenmenge schwillt rasant an und Prognosen werden immer schwieriger. Hinzu kommen immer mehr unstrukturierte Daten, die auch irgendeine Form der Integration in den Unternehmenskontext bedürfen.


Dieses eBook weist den Weg in die Zukunft.

Das eBook „Big Data und Analytics" ist deutschsprachig, 44 Seiten lang und das PDF ca. 7 MB groß. Es steht unter diesem Link kostenlos zum Download bereit:

***www.it-daily.net/download***

**Highlights aus dem eBook**

**• BI & Analytics in der Cloud**

Wir zeigen Möglichkeiten analytischer Lösungen in der Cloud. Darüber hinaus werden Vorteile als auch Nachteile der Cloud Services kritisch gegenübergestellt. Es werden die drei wichtigen Architekturkomponenten vorgestellt, auf denen Cloud Services in der Regel basieren und konkrete Services sowie deren Anbieter beispielhaft vorgestellt, um Vergleiche zu ermöglichen.

**• Datenstrategien für Big Data**

Die Verarbeitung von Metadaten wird immer wichtiger, um Daten anhand relevanter Kriterien zu finden. Mit ihnen lassen sich beispielsweise verschiedene Daten zusammenführen, ungleiche Daten unterscheiden oder Ortsangaben machen. Saubere Daten inklusive der passenden Metadaten machen es Organisationen einfacher, einen Wert aus den Daten zu ziehen.

**• Next Dimension Big Data**

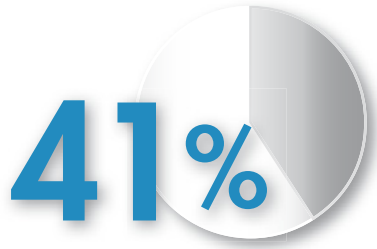
Es geht hier um die Synchronizität von Information und Aktion. Durch performante und frei skalierbare In-Memory-Lösungen wird auf die teuren Multi-Core-Server verzichtet. Stattdessen werden über eine neuartige Technologie leistungsfähige Cluster geschaffen. Viele Standard-Computer werden über nur einen speziell dafür entwickelten Hypervisor zu einem System zusammengefasst.

# AKTUELLE STUDIE

## ARBEITNEHMER SIND TROTZ KRISE PRODUKTIVER

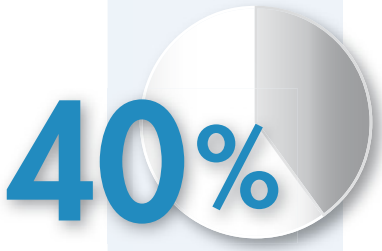
Angesichts von Kurzarbeit, Homeoffice und Quarantäne machen sich viele Arbeitgeber Sorgen, wie es in Zeiten der Pandemie um die Arbeitsmoral im Lande bestellt ist.
Wie eine aktuelle Umfrage von Qualtrics zeigt, sind diese aktuell nicht begründet.

Befragte gaben an:



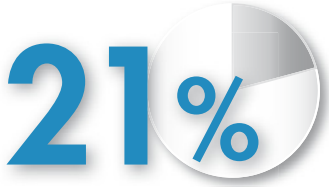
**41%**

Krise hat sich weder positiv noch negativ ausgewirkt



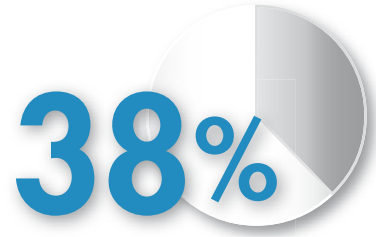
**40%**

seit der Krise bin ich kreativer geworden



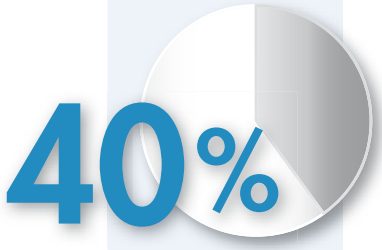
**21%**

sind in der Krise weniger produktiv



**38%**

Krise hat sich positiv auf Produktivität ausgewirkt



**40%**

Kommunikation zwischen Führungsetage und Arbeitnehmern hat sich verbessert.

Weitere Ergebnisse der Studie:

***www.qualtrics.com/de***

# FEHLER ERLAUBT

## VORAUSSETZUNGEN FÜR DEN ERFOLG VON DEVOPS

Eine schnellere Software-Entwicklung bei gleichzeitiger Verbesserung der Software-Qualität? Was sich nach konträren Zielen anhört, soll DevOps möglich machen. IT-Dienstleister Avision erklärt, welche Voraussetzung erfüllt sein müssen, damit die Umsetzung gelingt.

**KURZE RELEASE-ZYKLEN**

**AUTOMATISIERTE TESTS**

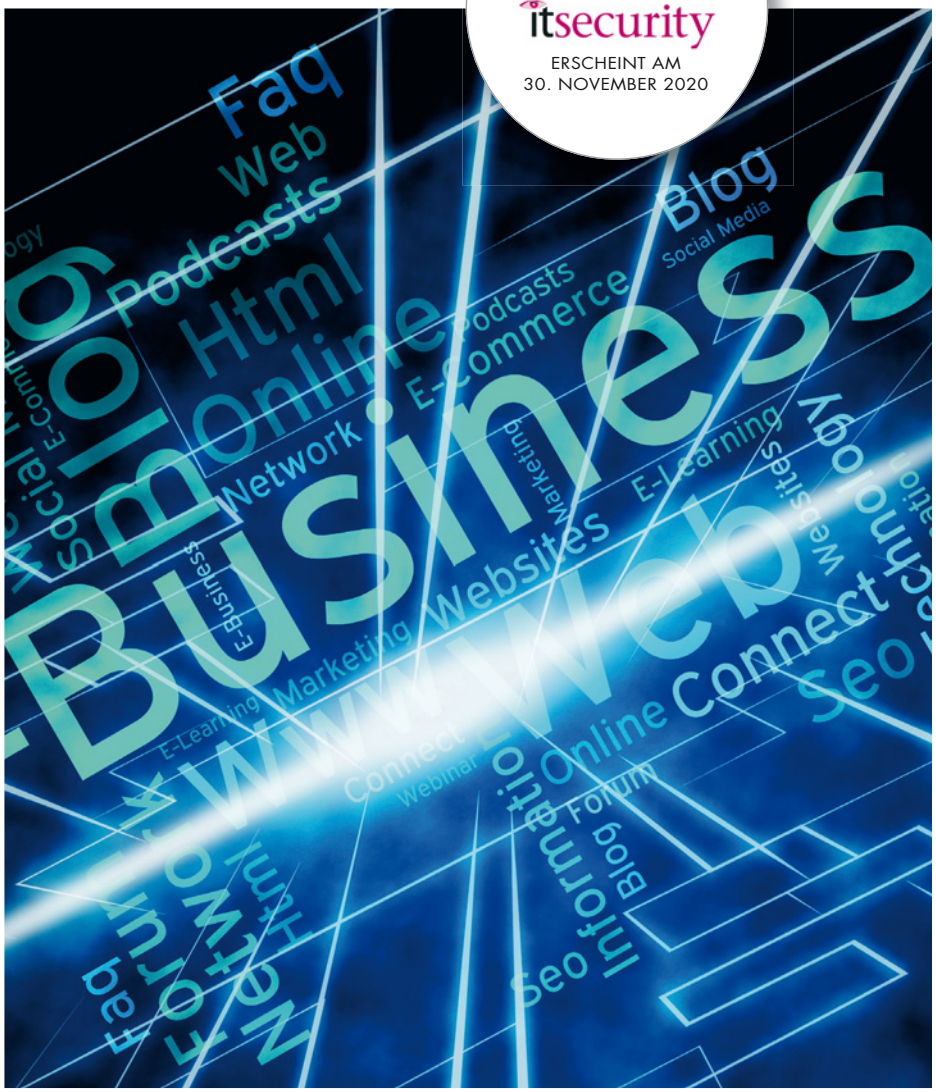
**FEHLER SIND EXPLIZIT ERLAUBT**

**EIGENVERANTWORTUNG FÜR DIE ENTWICKLER**

„Anwender erwarten heutzutage von Software-Anbietern ein schnelles Bugfixing sowie regelmäßige Funktions- und Usability-Verbesserungen“, erklärt Nadine Riederer, CEO bei Avision. „DevOps ist perfekt geeignet, diesen hohen Anforderungen gerecht zu werden. Kleinere Entwicklungsschritte und automatisierte Tests erlauben es, Fehler leichter zu entdecken, schneller zuzuordnen und zügig zu beheben, und das sogar ohne große Fehlersuche und aufwändige User-Tests.“

***www.avision-it.de***

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
30. NOVEMBER 2020




## IT TRENDS 2021

Wieder KI, ML, IoT und Blockchain?

## WORKPLACE 4.0 – EIN HYPE?

Smart und schnell in die Zukunft

## eBUSINESS LEICHT GEMACHT

Evolution voraus oder alles wie gehabt?

**DIE AUSGABE 12/2020 VON IT MANAGEMENT ERSCHEINT AM 30. NOVEMBER 2020.**

## INSERENTENVERZEICHNIS



## IMPRESSUM


***Chefredakteur:***
Ulrich Parthier (-14)

***Redaktion:***
Carina Mitzschke, Silvia Parthier (-26)

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

***Autoren:***
Marc Bohnes, Andreas Fuchs, Dina Haack, Ralf Kempf, Peter Kronfeld, Martin Landis, Carina Mitzschke, Sabine Obermayr, Silvia Parthier, Ulrich Parthier, Daniel Philips, Stefanie Puckett, Sven Schal, Florian Wiedmann

***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 veröff entlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenver arbeitungsanlagen 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 Veröff entlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

***Herausgeberin:***
Dipl.-Volkswirtin Silvia Parthier

***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. 28.
Preisliste gültig ab 1. Oktober 2020.

***Mediaberatung & Content Marketing-Lösungen it management | it security | it daily.net:***
Kerstin Fraenzke
Telefon: 08104-6494-19
E-Mail: berthmann@it-verlag.de

Karen Reetz-Resch
Home Office: 08121-9775-94,
Mobil: 0172-5994 391
E-Mail: reetz@it-verlag.de

***Online Campaign Manager:***
Vicky Miridakis
Telefon: 08104-6494-21
miridakis@it-verlag.de

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

***Erscheinungsweise:***
10x pro Jahr

***Verkaufspreis:***
Einzelheft 10 Euro (Inland),
Jahresabonnement, 100 Euro (Inland),
110 Euro (Ausland), Probe-Abonnement
für drei Ausgaben 15 Euro.

***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 Bezugs zeitraumes 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


IMPROVING DATA. BUILDING SUCCESS.
zetvisions
SPOT – DER DATENHÜTER
SUPERKRÄFTE FÜR IHR
STAMMDATENMANAGEMENT
Lassen Sie Ihre Unternehmensprozesse nicht länger von fehlerhaften und redundanten Daten bestimmen. SPoT macht damit Schluss. Unermüdlich im Einsatz und mit außergewöhnlichen Fähigkeiten, erkennt er die Unruhestifter in Ihrer Datenherde und besiegt sie.
Lernen Sie SPoT jetzt kennen!
WWW.ZETVISIONS.DE/SPOT