itmanagement

MÄRZ 2020

INKLUSIVE 32 SEITEN

IT SECURITY SPEZIAL

ENTERPRISE CONTENT MANAGEMENT

Herzstück der Digitalisierung

WORKSPACE 4.0

Sicher Zusammenarbeiten in der Cloud

DIGITAL WORKPLACE

DER WEG IST DAS ZIEL

Niculae Cantuniar, Ricoh Deutschland

MANAGED SERVICES THOUGHT LEADERSHIP

VENDOSOFT

Kostenneutrale Cloud-Migration

ab Seite 20

www.it-daily.net

DILK

Deutscher IT-Leiter-Kongress
28.–30. September 2020
Kongresszentrum CCD | Düsseldorf

3. Deutscher IT-Leiter-Kongress 2020

IT geht in Führung – mit mehr als 2.000 Teilnehmern, 100 Vorträgen & Workshops und über 80 Top-Referenten ist der DILK der größte Fachkongress für IT-Entscheider in ganz Deutschland. Seien Sie dabei und lernen Sie von den Besten!

- Sofort anwendbare Lösungen für Ihren Arbeitsalltag von über **80 Top-Referenten in über 100 zukunftsweisenden Vorträgen & Workshops!**
- Intensiver Austausch & wertvolle Networking-Gelegenheiten mit Deutschlands renommiertesten Experten und **2.000 Kolleginnen und Kollegen!**
- **All-inclusive-Verpflegung** einschließlich aller Getränke – ohne Extrakosten in einem Kongresszentrum der gehobenen Premiumklasse!
- **Jetzt ganz ohne Risiko** bis 31.05.2020 zum DILK 2020 **anmelden mit 50 % Frühbucherrabatt** und kostenloser Rücktrittsgarantie!

Hier eine kleine Auswahl unserer über 80 Top-Referenten:


Walter Kohl


Lutz Herkenrath


Christian Lindemann


Ulrike Winzer


Mario Brandenburg


Anna Abelein


Prof. Dr. Matthias Trier


Christoph Holz


Prof. Dr. Dr. Jivka Ovtcharova


Kai Diekmann


Alexander Herrmann


Dr. Carsten Lekutat


Dr. Dr. Justinus C. Pech


Prof. Dr. Julian Kawohl


Felix Thönnessen


Dr. Matthias Wittfoth


Dr. Christiane Bierekoven


Prof. Dr. Dr. Ayad Al-Ani


Andreas Kuffner


Dr. Mai Thi Nguyen-Kim

Eine gemeinsame Veranstaltung von: Wolters Kluwer, panda

Exklusiver Gesundheitspartner: Die Techniker

Platin-Partner: zetvisions

Gold-Partner: Synology

Silber-Partner: Pentalog

Medien-Partner: IT DIRECTOR, it-daily.net

Ausführliche Informationen zum DILK 2020 unter: www.deutscher-it-leiterkongress.de

WIESO, WESHALB, WARUM?

Die Generation Y ist Ihnen doch sicher ein Begriff? Kennen Sie auch die dahinter stehende Diskussion über eben jene Generation? Y steht in diesem Kontext für „Why", also für eine Generation, die alles hinterfragt - was per se ja nicht unbedingt schlecht ist. Sie hinterfragt demzufolge Sinn und Unsinn von Arbeit und inwieweit diese Arbeit mit der individuellen Freizeitgestaltung vereinbar ist. Sie sucht nach sozialer Sicherheit, arbeitet lieber in Teams als in tiefen Hierarchien, sie improvisiert gern und schätzt „alle wichtigen Lebensentscheidungen nach den unmittelbaren Vor- und Nachteilen für die eigene Person ab." (Wikipedia: Generation Y – Improvisation und Lebensplanung)

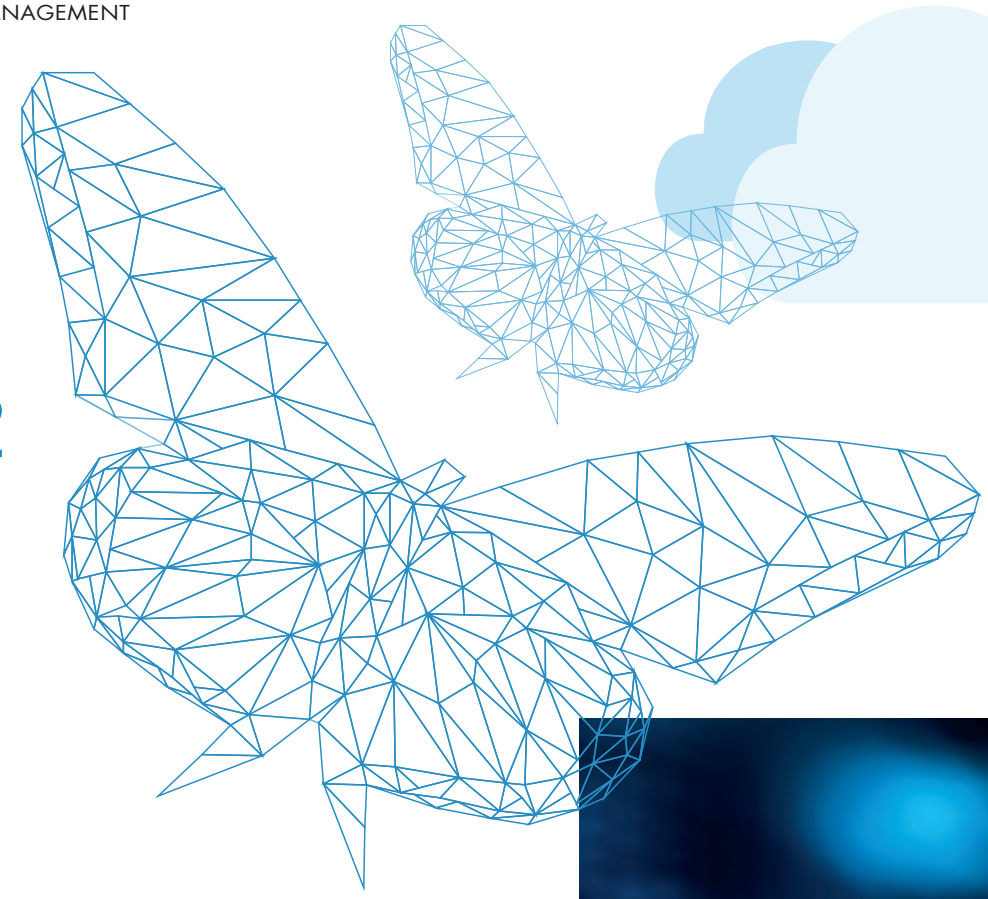
Will man so einen Egomanen wirklich einstellen, ist das unsere zukünftige Führungsriege? Die Antwort lautet: Ja. Aber machen Sie sich keine Sorgen, laut weiterführender Studien, gibt es besagte Generation Y gar nicht beziehungsweise kann man ihnen keine signifikanten Merkmale zuordnen, die sie von älteren oder jüngeren Generationen unterscheiden würden!

Den Vorteil, den diese Generation allerdings hat, ist die hohe Technik- und Medienaffinität. Quasi mit dem Smartphone in der Hand aufgewachsen, wissen sie, welche Tools man für welche Aufgabe sinnvoll nutzen kann und wollen diese dementsprechend auch in ihren Arbeitsalltag integrieren. Das Thema Workplace 4.0 steht da nicht zur Debatte – es wird erwartet und gelebt!

Wieso, weshalb, warum – weil neue Technologien schon immer Einfluss auf unsere Arbeitsweisen hatten und man der Zukunft gegenüber offen sein sollte, auch, wenn man sie nicht immer gleich versteht.

In diesem Sinne viel Spaß beim Lesen!

Carina Mitzschke
Redakteurin it management



INHALT

8

COVERSTORY

24

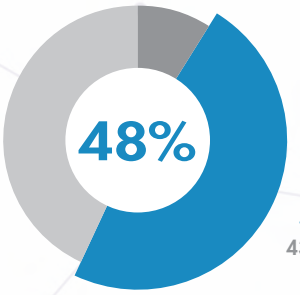
Inklusive 32 Seiten

IT SECURITY SPEZIAL

INDUSTRIE 4.0

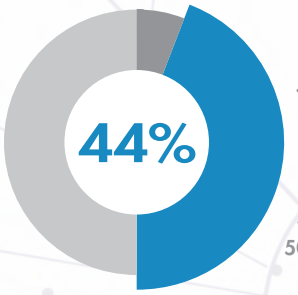
HEMMNISSE FÜR DIE EINFÜHRUNG

Die Einführung von Industrie 4.0-Technologien verzögert sich in unserem Unternehmen,…



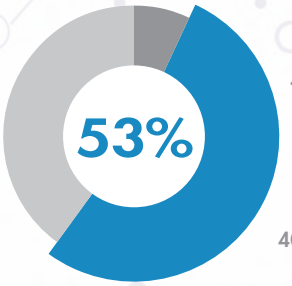
…weil etablierte, historisch gewachsene IT-Systeme die Integration erschweren.

9 % Stimme nicht zu
48 % Stimme zu
43 % nicht sicher



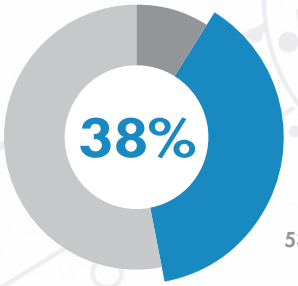
…da funktionsbedingte und historisch gewachsene Datensilos die Umsetzung bereichsübergreifender Lösungen erschweren.

6 % Stimme nicht zu
44 % Stimme zu
50 % nicht sicher



…weil durch das Tagesgeschäft nicht genug Kapazitäten zur Verfügung stehen.

7 % Stimme nicht zu
53 % Stimme zu
40 % nicht sicher



…aufgrund von Schwierigkeiten für Industrie 4.0 qualifizierte Mitarbeiter einzustellen.

9 % Stimme nicht zu
38 % Stimme zu
53 % nicht sicher

(Quelle: www.mhp.com; Industrie 4.0 Barometer)

SCHWACHSTELLEN-ÜBERBLICK 2019

KEINE LÖSUNG IN SICHT

Die Gesamtzahl der neuen Schwachstellen steigt: Im Jahr 2019 ist die Anzahl an Schwachstellen (20.362) um 17,6 Prozent gegenüber 2018 (17.308) und um 44,5 Prozent gegenüber 2017 (14.086) gestiegen.

Die Anzahl mittelschwerer bis kritischer Schwachstellen ist hoch: Bei der Einteilung der Schwachstellen nach dem CVSS wurden 8 Prozent als gering oder gar nicht schwer eingestuft, 61 Prozent wurden als mittel eingestuft, während 18 Prozent als hoch und 13 Prozent als kritisch eingestuft wurden.

Bislang keine Lösung greifbar: Bei über einem Drittel (40,2 Prozent) der Schwachstellen ist aktuell keine Lösung – wie beispielsweise ein Softwareupgrade, eine Software zum Umgehen der Schwachstelle oder ein Software-Patch – verfügbar.

www.imperva.com

BUSINESS TRANSFORMATION

AUF DEM WEG ZU DEVOPS

Die Nutzung von DevOps setzt sich durch – mittlerweile nutzen beinahe vier von fünf Unternehmen DevOps, viele weitere planen den Einsatz in naher Zukunft. Das ist eines der zentralen Ergebnisse der aktuellen IDC-Studie „DevOps in Deutschland 2020", die Consol zusammen mit anderen IT-Unternehmen unterstützt hat. Das DevOps-Modell kombiniert Prozesse, Methoden und Werkzeuge, mit denen Unternehmen schneller und einfacher Anwendungen und Services bereitstellen können. Wesentlich sind dabei unter anderem Cloud-Nativität, Agilität und Automatisierung. Die IDC-Prognosen belegen darüber hinaus, dass die Verwendung von Cloud-nativen Werkzeugen und Applikationen, Microservices und Containern zunehmen wird. So sollen bereits 2024 rund 80 Prozent aller neu entwickelten Applikationen über Container bereitgestellt werden. Zudem werden in absehbarer Zeit Machine Learning und Künstliche Intelligenz bei der Entwicklung und dem Deployment von Applikationen eingesetzt.

www.consol.de

GRÖSSTE HERAUSFORDERUNGEN BEI DER UMSETZUNG VON DEVOPS:

34 % **IT-Kultur und Beharrungsvermögen**

33 % **Integration von Anwendungsentwicklung und IT-Operations (Prozesse und Personal)**

29 % **Reife der Tools und Anwendungen**

27 % **Festlegen und Beschließen gemeinsamer KPIs**

27 % **Fehlendes Budget**

(Quelle: IDC)

DER WEG ZUM DIGITAL

DER WEG IST DAS ZIEL (KONFUZIUS)

Auf dem Weg zum Ziel braucht man vor allem drei Dinge: Geduld, Kontinuität und Gelassenheit. Über das Erreichen seiner Ziele und der Mittel sprach it management-Herausgeber Ulrich Parthier mit Niculae Cantuniar, CEO bei Ricoh Deutschland.

Ulrich Parthier: *Durch die Digitalisierung rückt auch das Thema Digital Workplace zunehmend in den Fokus der Unternehmen. Wie wird sich der Arbeitsplatz durch die Einführung neuer Technologien wie etwa KI und Robotik verändern? Welche Auswirkungen wird es auf das Unternehmen und die Mitarbeiter haben?*

Niculae Cantuniar: Die Auswirkungen werden massiv und tiefgreifend sein. Sie sind ja schon heute wahrnehmbar, vor allem in der Arbeitswelt. Fest steht: Die Geschwindigkeit, mit der die Digitalisierung in die Arbeitswelt eindringt und diese verändert, nimmt stetig zu. KI und Robotik sind längst keine Zukunftsmusik mehr, sondern gehören zur Realität. Als Technologieunternehmen sehen wir aber ganz klar die Chancen und das Potenzial dieser Entwicklung. Eben diese Technologien ermöglichen es Menschen, flexibler und kooperativer zu arbeiten. Sie schaffen kreative Freiräume, indem sie dazu beitragen, zeitintensive administrative Routineaufgaben zu übernehmen. Die Herausforderung besteht vor allem in der Frage, wie man sich diesen Veränderungen stellt und den Wandel organisatorisch und strategisch verankert. Das betrifft auch und vor allem das Mindset der Mitarbeiterinnen und Mitarbeiter. Gleichzeitig steigt der Handlungsdruck. Das gilt besonders für den Mittelstand. Wer sich als Unternehmen heute nicht oder nicht intensiv genug mit der Digitalisierung auseinandersetzt, setzt unmittelbar die Wettbewerbs- und Zukunftsfähigkeit aufs Spiel.

Ulrich Parthier: *Welche Handlungsempfehlung können Sie geben?*

Niculae Cantuniar: Aus unserer Sicht ist klar: Die Digitalisierung ist keine Kür, sondern eine Pflichtaufgabe. Das ist zwar längst vielen Unternehmen bewusst, aber die vermeintliche Komplexität, die viele damit verbinden, scheint viele mittelständische Chefetagen nach wie vor zu überfordern – das lähmt und macht vor allem den Einstieg für viele so anspruchsvoll. Wir dürfen nicht vergessen, dass es eben nicht nur um neue Technologien geht, sondern darum, Arbeitsweisen zu verändern. Deshalb ist es unserer Meinung nach wichtig, genau jetzt zu handeln. Wer das erkennt und diesen Schritt heute macht, schafft die wichtigste Grundlage für eine erfolgreiche Zukunft. Genau an diesem Punkt setzen wir an: Unser Ziel ist es, unsere Kunden bei diesem Einstieg in die Digitalisierung effektiv zu unterstützen und den Wandel voranzutreiben. Nicht nur mit unseren Technologien, sondern auch durch eine ganzheitliche Beratung und Unterstützung. Das meinen wir, wenn wir von „Empowering Digital Workplaces" sprechen.

Ulrich Parthier: *Der „Digital Workplace" macht auch beim eigenen Unternehmen nicht halt. Welche Bedeutung hat die Digitalisierung für Ricoh als Unternehmen (intern) und für das Business?*

Niculae Cantuniar: Das ist ein ganz wichtiger Punkt. Tatsache ist, dass die Entwicklung, die wir als Technologieunternehmen vorantreiben, dieselbe Entwicklung ist, der wir selbst als Unternehmen unterliegen. Anders gesagt: Den Druck spüren wir auch. Selbst wenn wir als Tech-Company damit vielleicht etwas selbstverständlicher umgehen, auch wir müssen uns dieser Herausforderung stellen. Es heißt nicht umsonst: Practice what you preach! Wir arbeiten bei uns im Unternehmen gerade mit Hochdruck an der Umsetzung eines Projekts zur Implementierung neuer Arbeitsweisen, den so genannten „New Ways of Working". Dazu gehören nicht nur Investitionen in die IT-Infrastruktur, sondern auch die Modernisierung der Bürorarchitektur bis hin zu Programmen für Digital Skills. Wir hätten am Markt nicht diesen Erfolg und auch keine Glaubwürdigkeit, wenn dieser Transformationsprozess bei Ricoh strategisch nicht so konsequent vorangetrieben würde.

Ulrich Parthier: *Das Thema Kollaboration & AV-Integration war eines der Hauptthemen auf der diesjährigen ISE 2020 in Amsterdam. Wie stellt sich Ricoh hier für die Zukunft auf?*

Niculae Cantuniar: Gerade im Zusammenhang mit dem digitalen Arbeitsplatz spielen die Technologien, die wir auf der ISE vorgestellt haben, eine ganz wichtige Rolle. Kommunikation und Kollaboration stehen hier im Fokus. Ricoh investiert viel in die Forschung und Entwicklung neuer Technologien, die bei uns im Geschäftsbereich Communication Services gebündelt sind. Dieser Bereich wird zukünftig noch wichtiger, insbesondere an der Schnittstelle zu unserem Kerngeschäft Office Printing. Damit meine ich etwa die Verbindung und Integration unserer Interactive Whiteboards mit Workflow-Lösungen, an die auch unsere intelligenten Multifunktionssysteme angeschlossen sind, alles Cloud-basiert. Das alles haben wir auf

WORKPLACE

der ISE einem breiten Fachpublikum gegenüber in Szene gesetzt. Ich glaube, es ist uns gut gelungen, unsere Rolle als globaler Technologiepartner für den Digital Workplace glaubhaft zu unterstreichen.

? **Ulrich Parthier:** *Office Printing ist nach wie vor das Kerngeschäft von Ricoh. Wie wirkt sich hier die fortschreitende Digitalisierung aus?*

Niculae Cantuniar: Fest steht, dass im Zuge des Vormarschs digitaler Arbeits- und Kommunikationsprozesse weniger gedruckt wird. Fest steht aber auch, dass das Druckvolumen bei weitem nicht so schnell zurückgeht, wie prognostiziert wurde. Der Stellenwert unseres Kerngeschäfts, vor allem auf Kundenseite, hat sich aber stark verändert. Dort, wo wir unsere Multifunktionssysteme installieren, arbeiten diese primär als Digitalisierungs-Hub. Es geht dabei vor allem um Input und Throughput von Information, nicht nur um den Output. Besonders durch die Anbindung an ECM-Systeme hat unser Kerngeschäft eine enorme Hebelwirkung, wenn es um die Digitalisierung von Geschäftsprozessen geht. Mit diesem Bereich steigen wir bei vielen unserer Kunden in die Digitalisierung ein, vor allem im Mittelstand. Seit der Übernahme von DocuWare im letzten Jahr haben wir nun eine der marktführenden Lösungen in unserem Portfolio. Unser Ziel, ein führender Digitalisierungspartner für den Mittelstand zu sein, erreichen wir so vor allem über unser Kerngeschäft und die Tatsache, dass wir unseren Kunden darüber hinaus ein Technologie- und Service-Portfolio bieten können, das in diesem Umfang, dieser Tiefe und auch dieser Reife am Markt einzigartig ist.

? **Ulrich Parthier:** *Wie fügt sich die Übernahme von DocuWare (2019) in dieses Puzzle ein? Was waren die Gründe und wie entwickelt sich das Geschäft mit Prozesslösungen seitdem?*

Niculae Cantuniar: Ricoh und DocuWare haben ja schon vor der Übernahme über viele Jahre gut, eng und vor allem sehr erfolgreich als Partner zusammengear-

> TATSACHE IST, DASS DIE ENTWICKLUNG, DIE WIR ALS TECHNOLOGIEUNTERNEHMEN VORANTREIBEN, DIESELBE ENTWICKLUNG IST, DER WIR SELBST ALS UNTERNEHMEN UNTERLIEGEN. ANDERS GESAGT: DEN DRUCK SPÜREN WIR AUCH.
>
> Niculae Cantuniar, CEO, Ricoh Deutschland, www.ricoh.de

beitet. Die Übernahme im vergangenen Sommer ist aus meiner Sicht eine strategisch sehr intelligente Entscheidung des Konzerns, weil sie unser Lösungsangebot für die Digitalisierung des Arbeitsplatzes unglaublich stärkt, und zwar an einer ganz entscheidenden Schnittstelle in unserem Portfolio. Gerade im deutschen Markt hat uns diese Übernahme im Digitalisierungsgeschäft einen kräftigen Schub nach vorne gegeben. Die Nachfrage speziell nach Cloud-basierten ECM-Lösungen wächst im Mittelstand rapide. Hier ist DocuWare führend.

Ulrich Parthier: *Die IT-Welt ist eine dynamische. Wie sieht die Zukunft des Printings aus Ihrer Sicht aus?*

> WENN WIR ÜBER DAS DRUCKEN SPRECHEN, GEHT ES SCHON LÄNGST NICHT NUR DARUM, TONER ODER TINTE AUF PAPIER ZU BRINGEN, SELBST WENN DAS NACH WIE VOR EIN WESENTLICHER TEIL UNSERES GESCHÄFTS IST. DAS MOTTO LAUTET „PRINT ON ANYTHING".
>
> Niculae Cantuniar,
> CEO, Ricoh Deutschland,
> www.ricoh.de

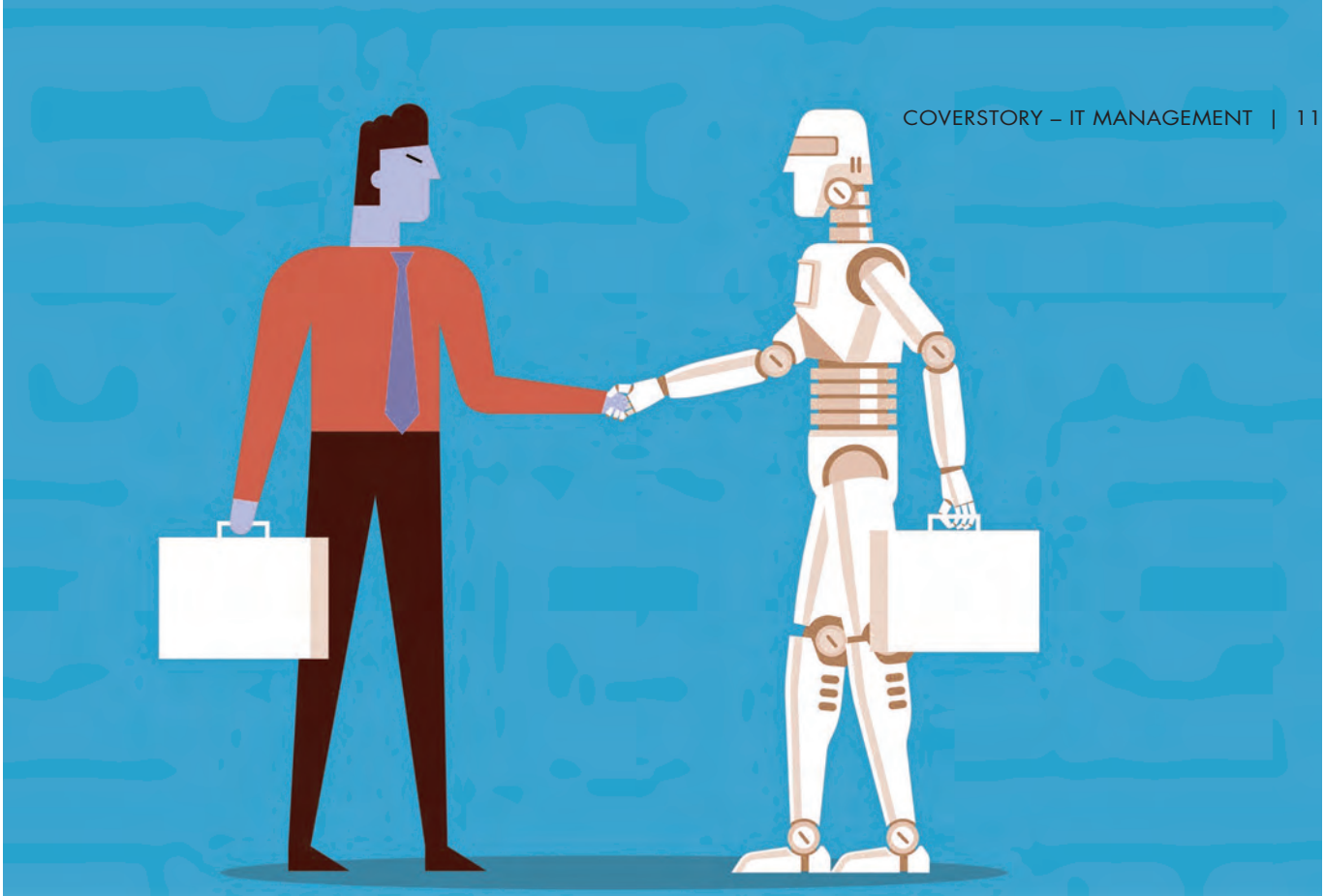
Niculae Cantuniar: Ich kann Ihnen an dieser Stelle sagen: Sehr lebendig und vielfältig! Wenn wir über das Drucken sprechen, geht es schon längst nicht nur darum, Toner oder Tinte auf Papier zu bringen, selbst wenn das nach wie vor ein wesentlicher Teil unseres Geschäfts ist. Das Motto lautet „Print on anything". Mit unseren Technologien drucken unsere Kunden inzwischen auf Materialien wie Glas, Metall, Stoff, Holz und Keramik. Vom 3D-Druck oder Bioprinting, wo Ricoh auch ganz massiv in die Forschung und Entwicklung investiert, ganz zu schweigen. Wenn es um Drucktechnologie geht, gehört Ricoh seit Jahrzehnten zu den absoluten Innovationstreibern am Markt. Für uns bedeutet das ganz konkret, dass wir unsere Technologien nutzen und einsetzen, um an den Produktions- und Wertschöpfungsketten unserer Kunden eine ganz zentrale Rolle einzunehmen. Hierbei geht es nicht mehr darum, nur ein Produkt zu verkaufen, sondern zusammen mit dem Kunden ganze Produktionsabläufe auf Basis unserer Technologien zu entwickeln und umzusetzen. Das ist ein wirklich spannendes Thema und wir treiben diese Entwicklung seit Jahren erfolgreich voran. Auf der diesjährigen Drupa in Düsseldorf werden wir einige dieser Drucktechnologien präsentieren, die hierbei eine Schlüsselrolle spielen.

Ulrich Parthier: *Ihr Unternehmen ist eine Partnerschaft mit dem Bildungswerk der Niedersächsischen (BNW) Wirtschaft eingegangen. Was verbirgt sich dahinter?*

Niculae Cantuniar: Im Grunde geht es darum, den „DigitalPakt Schule", den der Bund im letzten Jahr gestartet hat, voranzutreiben. Wir möchten so gemeinsam unseren Teil dazu beitragen, dass die notwendigen Investitionen in die digitale Infrastruktur in Schulen getätigt werden können. Es gibt ja Gründe dafür, warum von den bereitgestellten fünf Milliarden Euro an Mitteln offenkundig erst ein kleiner Bruchteil an die Schulen abgeflossen ist. Fest steht indes: Offenbar brauchen gerade Schulen ganz konkrete und handfeste Unterstützung, um das Thema anzugehen. In Niedersachsen haben wir mit dem BNW einen Partner, der vor allem im Bereich der Konzeption und Medienbildung stark ist. Das BNW unterstützt die Schulen bei der Entwicklung und späteren Umsetzung des individuellen Medienbildungskonzeptes, das eine wesentliche Grundvoraussetzung für die Bereitstellung der Gelder aus dem DigitalPakt Schule ist. Als exklusiver Technologiepartner helfen wir anschließend bei der technischen Ausstattung der Schulen mit digitalen Kommunikationslösungen. Im Fokus stehen hierbei unsere Interactive Whiteboards. Allein in Niedersachsen geht es um die mögliche Ausstattung von 2.700 Schulen. Wir finden: Das ist ein guter Anfang.

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

THANK YOU



FUTURE OF WORK

WELCHE BEDEUTUNG HABEN KI UND DIGITALE SKILLS FÜR DIE ZUKUNFT DER ARBEIT?

Neue Technologien haben seit jeher großen Einfluss auf unsere Arbeitsweisen. Doch keine Revolution hat unsere Arbeitswelt bisher so drastisch verändert wie die Digitalisierung. Dabei wirkt sich der zunehmende Einsatz von künstlicher Intelligenz ganz wesentlich auf die Zukunft der Arbeit aus und bietet enorme Chancen für Unternehmen und Arbeitnehmer. Doch die Arbeitsplätze der Zukunft erfordern neue Fähigkeiten und Kompetenzen – hier sind Initiativen zum lebenslangen Lernen am Arbeitsplatz gefragt.

Durch die Digitalisierung verändert sich unsere Art zu arbeiten grundlegend, doch es ist nicht das erste Mal, dass technologische Innovation sich radikal auf unsere Arbeitsweise auswirkt. Der Einsatz von Wasserdampf hat während der ersten industriellen Revolution Ende des 18. Jahrhunderts zu einer leistungsstarken mechanisierten Produktion geführt, die zweite industrielle Revolution nutzte Elektrizität für die Massenproduktion. Die dritte industrielle Revolution kombinierte Elektronik und Informationstechnologie für Computer, um die Produktion zu automatisieren und Menschen weltweit miteinander zu vernetzen. All diese Entwicklungen haben die Art und Weise, wie wir Menschen arbeiten, grundlegend und für die Zukunft verändert.

Aktuell befinden wir uns inmitten der vierten industriellen Revolution, die sich vor allem um die Digitalisierung früherer analoger Techniken und die Integration cyber-physischer Systeme dreht. Die Interaktion zwischen Menschen und Maschinen prägt die Arbeitswelt seit jeher, doch im Vergleich zu ihren Vorgängern entwickelt sich die vierte industrielle Revolution vielmehr exponentiell als linear. Die Vielzahl digitaler Schnittstellen zwischen Menschen und diesen neuen Technologien – von Tablets über Wearables bis hin zu Augmented und Virtual Reality – markieren den Beginn weiterer Veränderungen. Die Bedeutung der Beziehung von Mensch und Maschine nimmt mit der raschen Entwicklung neuer Technologien weiter zu, die Grenzen werden immer unschärfer.

KI am Arbeitsplatz: Eine große Chance

Um sich den sich schnell ändernden Gegebenheiten anzupassen, entwickeln Unternehmen nicht nur neue Geschäftsmodelle, sondern verwenden auch am Arbeitsplatz neue digitale Technologien, um nicht nur die Produktivität zu steigern, sondern auch die Qualität der Arbeit und mit ihr die individuelle Erfahrung bei der Arbeit für die Mitarbeiterinnen und Mitarbeiter zu verbessern. Eine der bedeutendsten Veränderungen am Arbeitsplatz ist unbestritten der zunehmende Einsatz von künst-

licher Intelligenz. Derzeit können wir noch nicht genau absehen, wie sich KI in Zukunft auf unsere Arbeitswelt auswirken wird. Schätzungen des Weltwirtschaftsforums zufolge könnten bis 2022 über 75 Millionen Arbeitsplätze durch die Verlagerung der Arbeitsteilung zwischen Mensch und Maschine verdrängt werden. Das ist für unsere Gesellschaft eine große Herausforderung, aber auch eine enorme Chance. Derselbe Bericht ergab nämlich auch, dass im gleichen Zeitraum 133 Millionen neue Jobs entstehen werden.

KI und Automatisierung werden Mitarbeiter bei zeitintensiven administrativen Aufgaben entlasten und es ermöglichen, sich auf kreativere und strategisch relevante Aufgaben zu konzentrieren. Auch die Einstellung der Arbeitnehmer zu neuen Technologien hat sich inzwischen gewandelt, diese sehen KI am Arbeitsplatz zunehmend als Bereicherung an. Über die Hälfte der Arbeitnehmer ist sich sicher, dass Arbeitgeber Technologien wie KI nutzen werden, um die Erfahrung am Arbeitsplatz zu verbessern. Und nur knapp 30 Prozent der Arbeitnehmer machen sich Sorgen, dass sie durch neue Technologien wie KI und Robotik am Arbeitsplatz ersetzt werden. Das geht aus der aktuellen Studie „Future of Work" hervor, die wir gemeinsam mit Arup durchgeführt haben.

Kompetenzen für die Arbeit der Zukunft

Die neu entstehenden Arbeitsplätze werden neben traditionellen auch verstärkt digitale Kompetenzen und Skills erfordern, die den steigenden Anforderungen entsprechen, sowohl durch den technologischen Fortschritt, als auch durch die dynamischen und sich kontinuierlich verändernden Bedürfnisse der Arbeitgeber. Der Bericht des Weltwirtschaftsforums legt nahe, dass analytisches und logisches Denken, Kreativität und Führungsqualitäten zu den wichtigsten Skills für die kommenden Jahre zählen werden.

Um mit den technologischen Entwicklungen Schritt zu halten, müssen Arbeitnehmer entsprechend geschult werden und sich kontinuierlich weiterbilden. „Lifelong learning" lautet somit das Mantra der Zukunft der Arbeit. Laut der Future of Work-Studie sind mehr als drei Viertel der Befragten der Meinung, dass sie bereits die Fähigkeiten besitzen, um in den nächsten zehn Jahren nicht nur ihren Job zu behalten, sondern sich auch innerhalb ihrer Rolle weiterzuentwickeln. Gerade in Zeiten des Fachkräftemangels sind hier nun die Unternehmen gefragt: Vier von fünf Arbeitnehmer erwarten, dass ihre Arbeitgeber ihnen Support und Schulungen zur Weiterbildung zur Verfügung stellen, um die Fähigkeiten zu erlernen, die sie im Hinblick auf die Einführung neuer Technologien am Arbeitsplatz benötigen.

Lebenslanges Lernen und Flexibilität am Arbeitsplatz

Der Schlüssel zum erfolgreichen Lernen am Arbeitsplatz wird darin liegen, zu verstehen, welche Qualifikationen in Zukunft benötigt werden. Beispielsweise werden traditionelle Abschlüsse und Zertifikate nicht mehr allein ausschlaggebend sein – das Ziel ist ein System, bei dem das lebenslange Lernen im Vordergrund steht. Online-Kurse und digitale Tools bieten heute viele Möglichkeiten zur Weiterbildung, was auch immer mehr von den Mitarbeitern selbst gefordert wird. Über zwei Drittel der Beschäftigten in Europa sind der Ansicht, dass die besten Arbeitsplätze in digitale Technologien zur Weiterbildung investieren, so die Future of Work-Studie. 60 Prozent der Arbeitnehmer vertrauen außerdem darauf, dass ihr Unternehmen Technologien bereitstellt, die den Anforderungen an die Arbeitsplätze der Zukunft entsprechen. Im Fokus sollten hierbei die Bereiche Zusammenarbeit und Flexibilität stehen. Generell profitieren Unternehmen davon, sich von herkömmlichen Arbeitsweisen zu lösen, um ihre Fachkräfte zu unterstützen, zu motivieren und letztendlich langfristig zu binden.

Der Mensch steht im Mittelpunkt

Die Arbeit der Zukunft wird die individuellen Bedürfnisse und Ambitionen der Arbeitnehmer aller Generationen unterstützen und fördern. Neue Technologien und KI werden es ermöglichen, produktiver zu arbeiten und mehr Zeit für kreative Aufgaben schaffen, die maßgeblich zum Geschäftserfolg beitragen. Denn Technologie allein entscheidet nicht über den Geschäftserfolg – der Mensch ist und wird auch in Zukunft unverzichtbar sein. Doch mit der richtigen Art der Zusammenarbeit und den richtigen Partnerschaften kann die Zukunft der Arbeit gestaltet und in Angriff genommen werden.

Niculae Cantuniar

MANAGED SERVICES IM WANDEL

MANAGED SERVICES THOUGHT LEADERSHIP

Auch die Managed Services sind im Wandel. Schuld an allem ist die Cloud-Revolution. Zusammen mit der Digitalisierungswelle stellt sie Althergebrachtes und Eingeschliffenes auf den Prüfstand. Egal ob Organisation, Prozesse, Technologien, Betreibermodell, Unternehmenskultur, Kosten, alles ändert sich.

Was liegt in Zeiten des Personalmangels näher, als nicht lebensnotwendige Dinge outzusourcen? Aufgaben, die andere vielleicht sogar besser beherrschen und Skaleneffekte verzeichnen.

So gesehen sind Managed Services nichts anderes als die nächste Evolutionsstufe der IT-Dienstleistungen. Denn IT-Infrastrukturen sind nicht statisch, sie wachsen und das dynamisch. Und sie können helfen, Probleme zu beseitigen: Legacy-Systeme, Zeit-, Personal- und Budgetprobleme sind allgegenwärtig. Die Wartung von Altsystemen verschlingt den größten Teil der Budgets, es bleibt kein Handlungsspielraum mehr für neue Entwicklungen. Die Folgen: Stress in Projekten und oft Notlösungen. Diese wiederum verursachen mittelfristig Probleme. Es entsteht ein Teufelskreis, der Innovationen hemmt, Mitarbeiter frustriert und Ressourcen weiter verknappt.

Und jetzt sollen auch noch Transformationsprojekte den Speed beschleunigen? Wie soll das gehen? Die Antwort lautet: Konzentration auf die Kernkompetenzen. Die Anforderungen an die Digitalisierung lauten: freie Kapazitäten, ständige Verfügbarkeit und optimale Performance.

So entsteht die Vision einer barrierefreien IT-Infrastruktur für alle im Unternehmen! Aber Vorsicht: Managed Services wird oft missverstanden, es ist keine Form von Outsourcing. Das Outsourcing bedeutete früher: Arbeitsplätze im Unternehmen gehen verloren, weil mitunter ganze Abteilungen ausgegliedert werden. Wie unschön, daher sprechen wir heute auch kaum mehr vom Outsourcing oder haben Sie den Begriff in letzter Zeit öfter gehört?

Besser klingt: Die Aufgabe von Managed Services sollte darin liegen, Mitarbeiter von Routineaufgaben und von ad-hoc-Aufgaben zu befreien, dem typischen „Hey Joe-Prinzip". Natürlich sollten immer wiederkehrende, manuelle Aufgaben zu einem Großteil schon vorher durch Automatisierungsprozesse und -tools erledigt werden. Das Ziel heißt damit Entlastung von Routineaufgaben, um das Leben der IT-Mitarbeiter abwechslungsreicher und produktiver zu machen. So macht die Arbeit auch wieder mehr Spaß!

Ulrich Parthier

MODERN IT-TIMES

MANAGED SERVICES IN ZEITEN DER DIGITALISIERUNG – WARUM SOLLTEN IT-CHEFS TEILE IHRER VERANTWORTUNG AN DIENSTLEISTER ABGEBEN?

Nachfolgend ein Blick auf die Themen, die IT-Verantwortliche heute bei der Wahl zwischen „Make or Buy" umtreiben und wie sich IT-Dienstleister darauf einstellen.

Eigentlich sind Managed Services inzwischen ja zu einer völlig unspektakulären Dienstleistung geworden - wenn es da nicht Entwicklungen gäbe, die die Spannung sowohl auf Anwender- als auch auf Anbieterseite hochhalten würden. Der digitale Wandel beschäftigt Unternehmen und deren Belegschaften, modifiziert ganze Branchen und hält CIOs und IT-Abteilungen auf Trab. Neue Technologien, Konzepte und Player am Markt - wie die drei großen Cloud-Hyperscaler Amazon, Microsoft und Google – ändern das Zusammenspiel von IT-Anbietern und -Nutzern. Vor diesem Hintergrund hat sich auch das Szenario „Managed Service" in den letzten Jahrzehnten grundlegend verändert.

MANAGED SERVICES – UNSPEKTAKULÄR ODER SPANNEND?

Effizienz und Kostenvorteile

Dazu ein kurzer Rückblick auf die Anfänge. In den 1990er Jahren waren IT-Verantwortliche hauptsächlich damit beschäftigt, ihre Systeme auf die bevorstehende Jahrtausendwende vorzubereiten. Den „Millenium Bug" zu verhindern, erforderte enorme personelle und technische Ressourcen, die mit Bordmitteln oft nicht bereitgestellt werden konnten und zugekauft wurden.

KOSTENVORTEILE ALS MOTIV IN DER ZEITEN GLOBALISIERUNG

Die zeitgleich aufkommende Globalisierung vergrößerte das Einzugsgebiet und brachte die lokale Ausrichtung der IT-Delivery ins Wanken. Rechenkapazitäten und Fachpersonal wurden vermehrt in Schwellenländer eingekauft - zu Konditionen, die auf den geschützten Binnenmärkten nicht zu haben waren.

Effizienz, Kostenvorteile und der Transfer von IT-Mitarbeitern waren damals ausschlaggebend für die Entscheidung, IT-Dienstleistungen von externen Providern übernehmen zu lassen. Zunächst wurden operative Routinetätigkeiten und -Prozesse, später immer häufiger auch komplette Rechenzentren ausgelagert. Das beachtliche Einsparungspotential machte die Themen „IT-Outsourcing" und „Managed Services" für viele Unternehmen attraktiv.

Die Digitalisierung verändert IT-Prozesse und -Dienstleistungen

Als vor rund zehn Jahren mit der Digitalisierung eine weitere Komponente ins Spiel kam, wurden die Karten neu gemischt. Der Einzug digitaler Technologien in nahezu alle Lebensbereiche änderte vieles. Unser Konsum- und Kommunikationsverhalten, die Abläufe in der Arbeitswelt und die Wertschöpfungsprozesse in der Wirtschaft.

Und aktuell: Dass das Managed Services-Segment inzwischen zu einer festen Größe innerhalb der IT- Branche geworden ist und enormes Wachstumspotential

besitzt, belegen aktuelle Untersuchungen. So schätzt IDC in der Studie Managed Services 2019 die Umsätze im deutschen Markt auf 32 Milliarden €, Bitkom sogar auf 40 Milliarden €.

Was bedeutet das nun konkret für Managed Services? Die digitale Disruption verändert die Geschäftsprozesse, die zugrundeliegenden IT-Prozesse und damit auch die traditionellen IT-Dienstleistungen.

HEUTE FORDERT DIE DIGITALISIERUNG DIE IT

„AKTUELLE TECHNOLOGIETRENDS MÜSSEN ANALYSIERT, ADAPTIERT UND VOR ALLEM SICHER IMPLEMENTIERT WERDEN. DIE KOMPLEXITÄT ABER NIMMT ZU, GLEICHZEITIG STEIGEN DIE ERWARTUNGEN AN FLEXIBILITÄT, SKALIERFÄHIGKEIT, KURZE UMSETZUNGSZEITEN UND EINE PUNKTGENAUE LEISTUNGSVERRECHNUNG."

Markus Sieber, Vorsitzender der Geschäftsführung, SPIRIT/21 GmbH, www.spirit21.com

FACHKRÄFTE-MANGEL ALS HERAUSFORDERUNG

Digitale Technologien und Fachkräftemangel fordern die IT

Soll ein Unternehmen für den digitalen Wandel fit gemacht werden, ist zunächst die eigene IT-Organisation gefordert: Aktuelle Technologietrends wie Cloud Computing, Internet of Things oder Mobility-Lösungen, müssen analysiert, adaptiert und vor allem sicher implementiert werden.

Die Komplexität nimmt zu, gleichzeitig steigen die Erwartungen: Flexibilität, Skalierfähigkeit, kurze Umsetzungszeiten und eine punktgenaue Leistungsverrechnung auf Verbraucher- beziehungsweise Fachbereichsebene sind heute der erklärte Standard. Dass sich viele IT-Mitarbeiter nach wie vor primär um den Betrieb historisch gewachsener Architekturen und die damit verbundenen Legacy-Anwendungen kümmern müssen, verschärft die Lage.

Die Schwierigkeit liegt also wieder in den mangelnden Ressourcen. Fehlt es an IT-Fachkräften, können die Digitalisierung von Geschäftsprozessen, die Entwicklung neuer Geschäftsmodelle und Unternehmenswachstum zu einem massiven Problem werden.

Leider lässt sich diese Problematik heute nicht so einfach lösen. Der Arbeitsmarkt für IT-Spezialisten ist leergefegt. Laut einer aktuellen Studie des Digitalverbands Bitkom waren Ende letzten Jahres allein in Deutschland rund 124.000 IT-Jobs unbesetzt – ein neuer Höchststand.

Neben dieser personellen, kommt häufig auch noch eine organisatorische Herausforderung auf das IT-Management zu: Investitionsentscheidungen müssen heute viel schneller getroffen werden und werden nicht mehr ausschließlich in der IT-Organisation gefällt. Immer häufiger bestimmen die Fachbereiche über ihr eigenes IT-Projektbudget und mischen sich in die IT-Entwicklung ein.

Managed Services helfen, den digitalen Wandel zu gestalten

Eine Möglichkeit – trotz des steigenden IT-Aufwands und fehlender Ressourcen- Betriebsabläufe zu sichern, sich wieder auf seine Kernkompetenzen zu konzentrieren und dadurch neue Marktchancen zu nutzen, bieten Managed Services. Durch

SPIRIT/21

Das Unternehmen wurde 1998 als IT-Startup in der Nähe von Stuttgart gegründet. Heute ist das mittelständische Beratungs- und IT-Dienstleistungsunternehmen an neun Standorten in Deutschland, Österreich und der Schweiz vertreten. Mit rund 500 Consulting-, Software- und Service-Experten ist SPIRIT/21 in der Lage, seine Kunden in jeder Phase ihrer digitalen Transformation zu unterstützen. Dabei geht es um aktuelle Trendthemen wie Internet of Things, Cloud Consulting & Services sowie Enterprise Mobility & Collaboration. Zum Portfolio gehören aber auch klassische IT-Dienstleistungen wie SAP- und Infrastruktur-Services. Innerhalb des SPIRIT/21 Leistungsspektrums gewinnen Managed Services-Lösungen zunehmend an Bedeutung. Das Angebot erstreckt sich hier auf nahezu alle Services der IT wie Applikationen, Backup und Storage, Netzwerkmanagement, Mobile Content und Device Management, SAP, Cloud- und Customer Help Desk Services.

MANAGED SERVICES ALS LÖSUNG?

die Verlagerung der Verantwortung für Teilbereiche der IT auf externe Dienstleister können Unternehmen die notwendige technologische und personelle Flexibilität erlangen, um sich auf den digitalen Wandel einzustellen. Soweit die Theorie.

Welcher Provider ist der richtige?

In der Praxis gelingt dies aber nur, wenn der Managed Services Provider auch tatsächlich in der Lage ist, das erforderliche Know-how, termingerecht und in den benötigten Kapazitäten zur Verfügung zu stellen. Denn der aktuelle Fachkräftemangel stellt auch die IT-Dienstleister vor neue Herausforderungen. Sie müssen ihr eigenes Unternehmen konsequent auf die digitale Transformation ausrichten, notwendige Kompetenzen auf allen Unternehmensebenen aufbauen und kontinuierlich weiterentwickeln. Und sie müssen versuchen, ihre eigenen Mitarbeiter dauerhaft zu binden, indem sie als Arbeitsgeber attraktiv bleiben. Nur denjenigen Providern, denen dies gelingt, werden in der Lage sein, ihre Kunden effektiv zu unterstützen.

Anforderungen an Dienstleister

Die Erwartungshaltung an den externen Dienstleister ist dabei klar – er muss die IT-Prozesse besser, flexibler und kostengünstiger abbilden können als die eigene IT. Dazu gehört die Fähigkeit, die zunehmende Komplexität der IT-Prozesse zu managen, aktuelle Technologietrends zu

ATTRAKTIVE DIENSTLEISTER GESTALTEN DEN DIGITALEN WANDEL

berücksichtigen, Risiken rund um die Themen IT-Sicherheit und Datenschutz zu reduzieren und gut ausgebildetes IT-Fachpersonal zur Verfügung zu stellen. Doch auch hier steigen die Anforderungen: Schnelle Bedienung von Bedarfen, Skalierfähigkeit, Hybrid-Cloud-Lösungen, effektive Automation und hoch flexible Services sind die neuen Standards, die ein Provider heute beherrschen muss.

Antwort der IT-Anbieter: Flexibilität und Kundennähe

Aus Kundensicht sind Flexibilität und Kundennähe heute die entscheidenden Erfolgsfaktoren. Und hier unterscheiden sich die Managed Service Provider erheblich.

FLEXIBILITÄT UND KUNDENNÄHE MACHEN DEN UNTERSCHIED

Nah am Kunden zu sein bedeutet, Bedarfe und Trends zu erkennen und darauf schnell reagieren zu können. Dies geht nur mit einer sehr gut ausgebildeten, erfahrenen und vor allem motivierten Belegschaft. Sie muss in der Lage sein, die Anforderungen aus einem Managed Service-Vertrag „in Time" umzusetzen und auf eventuell notwendige Erweiterungen oder Anpassungen schnell und flexibel zu reagieren.

Der Kunde muss Nähe allerdings auch zulassen. Ohne ein gewisses Maß an Offenheit und die Bereitschaft, den IT-Dienstleister als Partner in seine Wertschöpfungsketten und Entscheidungsprozesse zu integrieren, funktionieren Managed Services auf Dauer nicht.

Soft-Skills machen den Unterschied

Seriosität, Nachhaltigkeit und Leadership können helfen, das notwendige Vertrauen aufzubauen. Auch die Kommunikationskultur unter den beteiligten Parteien ist eine nicht zu unterschätzende Kompo-

SOFT-SKILLS SOURCING-ENTSCHEIDUNGEN PRÄGEN

nente. Der persönliche Kontakt ist auch im Zeitalter der Sozialen Medien für den Erfolg einer Transition oder einer Dienstleistung oft entscheidend. Diese sogenannten „Soft-Skills" werden bei Sourcing-Entscheidungen künftig immer mehr an Bedeutung gewinnen.

Managed Services bieten viele Chancen

Um für ihre Kunden relevant zu bleiben, müssen sich Managed Services Provider ständig weiterentwickeln. Ich bin sicher, dass alle Stakeholder, die das Thema nicht nur durch die technische Brille betrachten, sondern ihre gesamte Organisation und über die eigenen Unternehmensgrenzen hinaus alle Parteien ihres Ecosystems im Blick haben, künftig im Wettbewerb die Nase vorn haben werden.

MANAGED SERVICES ENTWICKELN SICH UND BIETEN ENORMES POTENTIAL

Aus unserer Sicht bieten Managed Services in Zukunft viele Chancen – verbunden mit einem signifikanten Business-Potential. Interessante Arbeitsplätze auf technisch anspruchsvollem Niveau, gepaart mit unterschiedlichen Kundenanforderungen und wechselnden Ansprüchen entwerfen ein attraktives Berufsbild, das Innovationen und viel eigene Kreativität zulässt.

Markus Sieber

TWENTY2X

NEUE IT-MESSE FÜR DEN MITTELSTAND IST STARTKLAR

Mit dem neuen Format, der klaren B2B-Ausrichtung und dem Fokus auf die Lösungen, die kleine und mittlere Unternehmen für die Digitalisierung wirklich brauchen, hat die Deutsche Messe eine Lücke im Messemarkt geschlossen. Bis jetzt haben sich für die Veranstaltung vom 17. bis 19. März in Hannover bereits mehr als 180 Unternehmen aus zwölf Ländern angemeldet, darunter 35 Startups.

Passgenaue Angebote für mittelständische Unternehmen

Ziel der TWENTY2X ist es, mittelständische Unternehmen mit einem passgenauen Angebot, praxisnahen Beispielen und Gesprächen auf Augenhöhe bei der notwendigen Digitalisierung zu unterstützen. Das Angebot reicht von Datenanalyse-Tools und neuen Arbeitsmethoden über Social-Media-Strategien bis zum Umgang mit Bedrohungen im Netz. Es geht um intelligente Technologien und anwendungsreife Lösungen zur Erneuerung von Geschäftsmodellen, für innovative Produkte und Services, für effiziente Strukturen, optimierte Prozesse und moderne Zusammenarbeit.

Mittelstand als wichtigste Kundengruppe

Der überwiegende Teil der Aussteller kommt selbst aus dem Mittelstand beziehungsweise sieht den Mittelstand als sein wichtigstes Kundensegment. Der DATABUND ist allein mit rund 30 Mitausstellern dabei. Weitere IT-Anbieter sind unter anderem Inotec, Synology, Grün Software und Topdesk. Der ECM-Anbieter DocuWare beispielsweise nutzt die TWENTY2X, um mit Kunden, Partnern und Interessenten persönlich in Kontakt zu treten

Auch einige „Big Player" sind an Bord, wie beispielsweise Materna auf eigener Fläche. Die Unternehmen Dell und VMware präsentieren ihr Angebot gemeinsam mit dem Systemhaus Global Information Distribution. IBM ist auf der TWENTY2X mit eigenem Stand vertreten und geht mit anerkannten Experten im Konferenzprogramm zu den Themen Blockchain, Cloud, New Mobility, Public Security und New Work an den Start.

Raum für Information, Inspiration und Austausch

Besucher finden auf der TWENTY2X nicht nur konkrete Angebote und Lösungen, sondern auch Raum für Information, Inspiration, Wissensvermittlung und Erfahrungsaustausch. Auf fünf Bühnen präsentieren rund 200 Sprecher an den drei Messetagen in unterschiedlichen Formaten Grundlagenvorträge, praxisorientierte Erfahrungsberichte, kontrovers besetzte Podiumsdiskussionen, Themen-Summits und Pitches. Neu sind innovative und interaktive Formate, die gemeinsam mit Ausstellern und potenziellen Besuchern entwickelt und extra auf die neue B2B-Digitalmesse und die Zielgruppe Mittelstand zugeschnitten wurden.

Sprecher aus Politik, Wirtschaft und Gesellschaft

Bei der Eröffnungs-Session am Dienstagmorgen, 17. März, spricht unter anderem Thomas Jarzombek, der Beauftragte des Bundeswirtschaftsministeriums für Digitale Wirtschaft und Start-ups. Der Autor, Internet-Unternehmer und Blogger Sascha Lobo erörtert in seiner Eröffnungs-Keynote die Frage „Digitalisierung im Mittelstand – und wie jetzt weiter?". Anschließend steht Hagen Rickmann, Geschäftsführer Geschäftskunden bei der Deutschen Telekom, auf dem Programm. Am Mittwoch, 18. März, referiert der frühere Chief Technology Officer von IBM Prof. Gunter Dueck über den Wandel in der digitalen Arbeitswelt.

www.twenty2X.de

TWENTY2X
NEW TECH. NEW BUSINESS.

DIGITALE TOOLS IM VORSTAND

LIVE WEBINAR AM 20.03.2020, 11-12 UHR

Beim Austausch von Daten – ganz gleich ob per Mail oder über das Smartphone – besteht immer auch das Risiko, dass Informationen in die falschen Hände geraten. Das sorgt gerade auf Vorstandsebene für Unsicherheiten. Vorstände und Aufsichtsräte vertrauen daher oft auf ihre herkömmlichen Arbeitsweisen und auf Sitzungsunterlagen aus Papier. Auf diese Weise entfällt zwar das Risiko auf digitale Datenlecks, doch haben wir damit die sicherste Lösung? Leider nein.
Wie also sicher kommunizieren und vertrauliche Daten richtig austauschen? Die Antwortet lautet: Digitale Board-Portale.

Live-Demo eines Board-Portals
In dem Webinar „Digitale Tools im Vorstand" stellt Michael Jacob von der Brainloop AG in einer Live-Demo ein digitales Board-Portal vor. Er geht dabei auf folgende Fragen ein:

- Welche Vorteile hat ein Board-Portal für die Vorstands- und Aufsichtsratskommunikation?
- Wie kann man eine Datenumgebung schaffen, in der wichtige Sitzungsunterlagen sicher sind?
- Worauf sollte man bei der Auswahl eines Board-Portals achten?

Interessenten können sich hier zum dem kostenlosen Webinar anmelden:
https://www.it-daily.net/webinar

Der Sprecher
Michael Jacob ist seit knapp drei Jahren bei Brainloop als Senior Pre-Sales Consultant beschäftigt. Schwerpunkte seiner Tätigkeit sind Produktdemos für Modern Governance Lösungen sowie die fachliche Betreuung und Unterstützung der Kunden während der gesamten Projektphase.

Zuvor hat Michael Jacob mehrere Jahre im IT-Umfeld als IT-Trainer, Consultant und Projektmanager im DMS-Bereich gearbeitet.

ETHIK IN KI UND ROBOTIK

WAS DARF KI EIGENTLICH?

Unser Leben wird zunehmend von Künstlicher Intelligenz (KI) und Robotik beeinflusst. Autonome Fahrzeuge kommen auf unsere Straßen, Roboter werden für eine Vielzahl von Aufgaben im Gesundheitswesen vorgeschlagen – von der Unterstützung älterer Menschen bis zum Einsatz bei Operationen – und Algorithmen entscheiden über Kreditanträge sowie sogar über den Einsatz automatische Waffensysteme. Viele Menschen befürchten, dass KI langfristig die Kontrolle über unser Leben übernimmt.

Vor diesem Hintergrund wird es immer wichtiger, die ethischen Grundlagen und Auswirkungen des Einsatzes von KI und Robotik in unserer Gesellschaft zu diskutieren. Dieses Buch bietet eine Einführung in das Thema, die keine technischen, rechtlichen oder philosophischen Kenntnisse voraussetzt. Es behandelt Fragen, die zur Diskussion von KI-Anwendungen einladen, von der Gesundheitsfürsorge bis zur Kriegsführung.

Die Autoren veranschaulichen die Themen im gesamten Buch anhand von Beispielen. Am jeweiligen Kapitelende befinden sich Fragen, die zur Diskussion von KI-Anwendungen einladen. Weiterführende Literatur dient ebenfalls als Anregung für den Leser.

Ethik in KI und Robotik;
Christoph Bartneck, Christoph Lütge, Alan R. Wagner, Sean Welsh; Carl Hanser Verlag GmbH & Co. KG
2019

KUNDENZUFRIEDENHEIT

WISSEN SIE, WIE ZUFRIEDEN IHRE KUNDEN* SIND?

Wann haben Sie das letzte Mal innerhalb Ihres Unternehmens die Zufriedenheit Ihrer Kunden gemessen? Wissen Sie, was Ihre Kunden gut oder schlecht finden und wo sie Optimierungspotenzial sehen?

Viel schlimmer ist, dass in den meisten Fällen die evaluierten Daten nicht weiterverarbeitet werden. Kunden werden sich bei weiteren Zufriedenheitsumfragen deshalb genau überlegen, ob sie nochmals Feedback geben. Denn sie fühlen sich dann nicht ernst genommen. Kundenzufriedenheit, die zwar gemessen, aber mit der am Ende nichts passiert, fördert letztlich eine zunehmende Unzufriedenheit.

Gehen Sie auf Kritik ein

Beauftragen Sie jemanden in Ihrem Unternehmen, der aktiv und zeitnah nach dem Erhalt von Feedback, vor allem negativem, reagiert. Nehmen Sie die erhaltene Kritik ernst und geben Sie dem Kunden das Gefühl, dass auch negative Kritik wertgeschätzt und – falls nachvollziehbar – umgesetzt wird. Binden Sie den Kunden, der negative Kritik geäußert hat, ein! Fragen Sie ihn, was aus seiner Sicht notwendig ist, um Ihren Service zu verbessern. Auch sollten Sie aktiv kommunizieren, wenn sich etwas verbessert hat, was zuvor bemängelt wurde. Ein Self Service Portal eignet sich hervorragend, um Kundenfeedback einzuholen.

Nutzen Sie ein Servicemanagement-Tool

Mit Hilfe eines Self Service Portals lässt sich erhaltenes Feedback zentral hinterlegen und verarbeiten. Haben Sie einen definierten Feedback-Prozess, bei dem mehrere Abteilungen involviert sind? Nutzen Sie die Abläufe des Changemanagements und bilden den Prozess in einem standardisierten Workflow ab! So stellen Sie sicher, dass jedes Feedback bearbeitet wird und die Kunden stets auch eine Rückmeldung erhalten. Wie erwähnt, gibt es nichts Schlimmeres, als Feedback einzufordern, dann aber nicht auf das erhaltene Feedback zu reagieren.

Lassen Sie die Umfrageergebnisse in Ihre Produkte einfließen

Sehen Sie Kundenfeedback auch immer als Chance Ihre Services zu hinterfragen und zu verbessern. Umso wichtiger ist es, dass Sie das dem Kunden Versprochene auch zeitnah umsetzen. Informieren Sie ihn bspw. über einen Projektstart und damit verbundene Zwischenziele. Offenheit und Transparenz sind wichtig, um bei Ihren Kunden Vertrauen zu stärken.

Felix Heintz | www.topdesk.de

PRAXISBEISPIEL:

Kundenzufriedenheits-beauftragter bei der TOPdesk Deutschland GmbH

Bei meinem Arbeitgeber, der TOPdesk Deutschland GmbH, haben wir vor etwa drei Jahren die Rolle des Kundenzufriedenheitsbeauftragten eingeführt. Unsere Kunden können uns jederzeit über den Support Feedback geben. Insbesondere wenn ein Feedback negativ ausfällt, meldet sich unser Kundenzufriedenheitsbeauftragter zeitnah telefonisch, um zu verstehen, was bemängelt wurde. Anschließend wird dieses Feedback mit den relevanten Abteilungen besprochen und nach Verbesserungsmöglichkeiten geschaut. Der Kunde erhält anschließend eine Rückmeldung zu seinem Feedback. Wichtig ist uns, dass wir möglichst transparent agieren. Seit der Einführung dieser Rolle, haben unsere Kunden sehr positiv reagiert. Sie schätzen es aktiv involviert zu werden, wenn sie Kritik äußern.

Service Excellence Blog: https://blog.topdesk.de

TOPdesk

* Da Services sowohl aus interner als auch externer Sicht von einer Serviceabteilung angeboten werden, ist unter dem Begriff Kunde in diesem Artikel sowohl der interne Mitarbeiter als auch der Ansprechpartner eines externen Kunden gemeint.

CLOUD-MIGRATION

KOSTENNEUTRALER UMSTIEG BEI DER GLÖCKLE GRUPPE

Als die Geschäftsleitung der Firmengruppe Glöckle 2019 beschloss, auf Cloud-Produkte von Microsoft zu migrieren, stellte sie zwei Fragen: Was passiert mit unserer alten Software und wie lässt sich ein solches Projekt finanzieren?

Beide Fragen waren zum Zeitpunkt der Entscheidung nicht geklärt. Klar war jedoch, dass im ersten Schritt die Büroanwendung Office sowie Teile der Serverlizenzen auf Cloud-Produkte von Microsoft umgestellt werden sollten. Schnell stand zur Debatte, was mit den bis dato verwendeten Softwarelizenzen passieren sollte, schließlich stellten sie einen beachtlichen Vermögenswert dar.

Der bei Glöckle für Einkauf, Betriebsorganisation und Lizenzmanagement zuständige Peter Klemmer informierte sich online über die Möglichkeiten, gebrauchte Software Assets zu veräußern.

„Die Suche gestaltete sich schwierig, weil für uns nicht erkennbar war, was ist seriös, was nicht", beschreibt er sein Vorhaben. Erfahrungswerte gab es keine. Dafür die klare Vorgabe der Geschäftsleitung, dass beim Verkauf der alten Lizenzen die Rechtmäßigkeit oberste Priorität habe.

Das hieß für Peter Klemmer, sich in die rechtlichen Begebenheiten einzuarbeiten – oder einen vertrauenswürdigen Partner zu finden.

Einen verlässlichen Gebrauchtsoftware-Händler finden

Eine Empfehlung gab den entscheidenden Hinweis und das gute Gefühl, einen Profi zur Seite zu haben. Seit 20 Jahren arbeitet Glöckle mit dem Systemhaus CANCOM zusammen. Nachdem ihm verschiedene Ankaufsangebote vorlagen, fragte Klemmer den langjährigen IT-Partner um Rat. Dort nannte man ihm VENDOSOFT als seriösen Gebrauchtsoftware-Händler.

„Das war für uns eine wertvolle Empfehlung, denn als Mittelständler brauchen wir einen Partner, bei dem wir gut aufgehoben sind – auch für den Fall, dass es mal zu Problemen kommt."

Bereits das erste Gespräch mit einem Microsoft Licensing Professional der VENDOSOFT GmbH bestätigte ihn in seiner Wahl. Auch das Angebot überzeugte –

ÜBER DEN RESELLER

Als Silver Microsoft Partner und Adobe Certified Reseller handelt die VENDOSOFT GmbH neue und gebrauchte Software sowie Cloud-Lösungen.

Bezugsquellen sind Unternehmen, deren Lizenzen nicht länger benötigt werden – sei es durch Umstrukturierung, das Zusammenlegen von Abteilungen oder die Migration in die Cloud. VENDOSOFT führt diese Altlizenzen – die so wertig sind wie neu – dem Zweitmarkt für gebrauchte Software zu.

Um eine rechtssichere Lizenzierung zu gewährleisten, beraten bei VENDOSOFT zertifizierte Microsoft Licensing Professionals.

obwohl der Preis für Glöckle nicht ausschlaggebendes Kriterium sein sollte.

Der Software-Verkauf lohnt sich

Insgesamt ging es um 250 Microsoft-Lizenzen, darunter Office 2019 und verschiedene Server und Zugriffslizenzen aus SA-Verträgen – und damit um Software der 2019er Versionen.

Rund 100.000 Euro erwirtschaftete Glöckle mit dem Verkauf der Software Assets an VENDOSOFT. Der Ertrag wurde zu 100 Prozent in das Cloud-Projekt reinvestiert und deckt einen Großteil der entstehenden Migrationskosten.

Von links nach rechts: Sven Rudisch, Gruppenleiter IT, und Peter Klemmer, Leiter Einkauf und Lizenzmanagement, Glöckle.

Bei Glöckle ist man sehr zufrieden mit der Umwandlung der obsolet gewordenen Vermögenswerte in bares Geld. Auch in puncto Beratung, Betreuung und Abwicklung durch VENDOSOFT fühlt sich das Unternehmen gut aufgehoben. Insbesondere was die rechtlich wichtigen Aspekte wie Deinstallation der Altlizenzen und Dokumentation des Verkaufsprozesses angeht.

Der vereinbarte Betrag ging nur drei Tage nach Übergabe der letzten Dokumente auf dem Glöckle-Firmenkonto ein. Darüber zeigten sich Peter Klemmer und die Geschäftsleitung ebenso begeistert wie über die nahezu kostenneutrale Migration der gesamten Firmengruppe in die Cloud.

www.vendosoft.de

ERFOLGREICHE MIGRATION

Das Ziel:

- Umstellung auf Microsoft-Cloud-Produkte
- Gegenfinanzierung des Projekts
- Verwertung der bisherigen Software Assets
- Wahrung aller rechtlichen Vorgaben

Die Lösung:

- ✔ Veräußerung von etwa 250 Microsoft-Lizenzen im Wert von knapp 100.000 Euro an die VENDOSOFT GmbH.

Die Vorteile:

- ✚ Professionelle Beratung und Abwicklung
- ✚ Refinanzierung der Cloud-Migration
- ✚ Auflösung werthaltiger Wirtschaftsgüter
- ✚ Verschlankung des SAM
- ✚ Nachhaltige Nutzung von Software

OPTIMALE WORKLOADS

DEN CLOUD-UMZUG IN GESCHÄFTSERFOLG UMMÜNZEN

Das Thema Cloud-Migration steht bei beinahe allen Unternehmen auf der Tagesordnung. Viele Workloads laufen allerdings erst optimal, wenn sie auf geteilte Filesysteme zugreifen – das muss auch für den Cloud-Betrieb erreicht werden. Dabei helfen die richtigen NAS (Network Attached Storage)-Dienste.

Vor dem Umzug in die Cloud braucht es eine gute Vorbereitung: Die Geschäftsziele müssen abgesteckt, Workloads identifiziert sowie katalogisiert und schließlich Compliance und Datenschutz gewährleistet werden. Doch auch die beste Organisation vorab kann keinen reibungslosen Applikations- und Datenbankbetrieb in virtuellen Umgebungen gewährleisten.

Denn in der Regel sind dutzende bis hunderte Spezial-Anwendungen auf Shared Storage angewiesen. Dieser wird meist als NAS umgesetzt. Der Vorteil dabei: Die Festplatten sind eigene Fileserver und nicht an einen Server gebunden. Der Zugriff erfolgt dann über verschiedene Protokolle wie beispielsweise NFS (Network File System) oder die Microsoft-Variante SMB (Server Message Block). Das erlaubt einen schnelleren Zugriff auf Snapshots, Backups in Sekundenschnelle sowie ein kürzeres RTO (Recovery Time Object).

Viele Anwender erwarten diesen Standard auch in der Cloud. Das Data-Fabric-Konzept von NetApp schafft dafür die bestmöglichen Voraussetzungen: Der Ansatz ermöglicht es Unternehmen, ihre Datenbestände sicher über alle Infrastrukturen hinweg zu transferieren – unabhängig davon, wo sich die Daten befinden. Dadurch können sie die leistungsfähigen IT-Ressourcen der Public-Cloud-Anbieter nutzen, aber gleichzeitig die Kontrolle über die eigenen Daten bewahren.

Cloud und Storage als Einheit

Besonders wichtig sind für den NAS-Betrieb dabei Cloud-Data-Services, beispielsweise von NetApp. Cloud Volumes ONTAP erleichtert den Zugang zum NAS und Cloud Volumes Service verbessert die Verwaltung. Wenn Anwender NetApp-Speichersysteme auch im eigenen Rechenzentrum einsetzen, können sie mit Cloud Volumes ONTAP ihre Daten zwischen On-Premises und Cloud synchronisieren. Cloud und Storage bilden so eine Einheit und das Datenmanagement wird massiv vereinfacht.

Der Dienst wird dabei einfach auf dem Hypervisor von AWS oder Google installiert und sorgt für eine effiziente Speichernutzung beim Cloud-Provider. Über zusätzliche Features wie Snapshots, SnapMirror, Cloning, Datenreplikation und Datenreduktion wird außerdem auch die Datenbankadministration effizienter.

Mit Cloud Volumes Service übernimmt der Anbieter sogar in Gänze den NAS-Betrieb. Bei diesem Dienst handelt es sich um einen Cloud-nativen File-Storage: Nutzer geben vorab lediglich an, welche Kapazitäten sie bei AWS oder Google benötigen und welches Protokoll verwendet werden soll. Eine möglichst schlichte Benutzeroberfläche unterstützt Anwender außerdem dabei, intuitiv Snapshots und Klone zu erstellen. Auch Exportrichtlinien lassen sich mit Cloud Volumes Services bequem festlegen.

Einfachere Migration in die Cloud

Eine Anwendung, die ein geteiltes Filesystem benötigt, lässt sich somit auch in der Cloud betreiben. Sie steht einer Cloud-Migration grundsätzlich nicht im Weg. Mit Cloud Volumes ONTAP und Cloud Volumes Service unterstützt das Unternehmen Anwender zudem dabei, auch im NAS-Betrieb in der Cloud den bestmöglichen Service zu erhalten. Auch für Anwendergruppen ohne profundes Speicherwissen ist es so möglich, ihre Anwendungen ohne großen Mehraufwand in die Cloud zu migrieren.

Oliver Krause | www.netapp.com/de

Quelle: NetApp

Der Umzug in die Cloud erfordert Vorbereitung – und die richtigen Services.

UNTERNEHMENSPROZESSE DIGITALISIEREN

AUF DEM WEG ZUM PAPIERLOSEN UNTERNEHMEN

Die Hafner Bau GmbH ist ein mittelständischer Familienbetrieb mit Tradition, der seit 1971 besteht. Neben den klassischen Hochbautätigkeiten wie Maurer-, Beton- und Verputzarbeiten sowohl für Eigenheime als auch in der Industrie hat sich das Unternehmen auf die Planung und Erstellung schlüsselfertiger Bauaufgaben spezialisiert – und zwar in den Bereichen Neubau, Umbau und Modernisierung. Von der Baugenehmigung bis hin zur Erstellung von Plänen für Ein- und Mehrfamilienhäuser sowie Garagen kann alles übernommen werden. Besonderen Wert legt Hafner Bau auf eine individuelle Planung, eine ganzheitliche energetische Betrachtung und die solide handwerkliche Ausführung ihrer Objekte.

Ausgangssituation

Daher war eines der primären Ziele in der effizienten Unternehmensführung die Übersicht über Prozesse, Aufträge, Einkäufe und Mitarbeiter. Insbesondere soll es eine einfache Übersicht über alle Eingangsrechnungen geben, gleichzeitig sollen alle Belege behalten und archiviert werden.

Vorgehensweise

Um die wachsende Komplexität der Anforderungen besser abdecken zu können, wurde eine Erweiterung des Workflow-Management-Systems implementiert. Dabei legte die Hafner Unternehmensgruppe großen Wert auf Zuverlässigkeit sowie eine möglichst benutzerfreundliche Oberfläche, um einer hohen Anwenderakzeptanz den Weg zu ebnen.

Zunächst wurde der Eingangs-Workflow einschließlich Standard-Stempel und Aufgabenliste realisiert. Alle Dokumente werden mit einem Barcode versehen, bevor sie den Scan-Prozess durchlaufen. Über den Barcode wird bereits ein Hinweis gegeben, um welchen Dokumenttyp es sich handelt. Die Prozessarten sind definiert und lösen den nachgelagerten Workflow, zum Beispiel die Rechnungsstellung, aus.

Die Kombination von DocuWare und JobRouter stellte sich im Arbeitsalltag als die perfekte Lösung heraus. Beide Systeme ergänzen sich in ihrem Leistungsspektrum ideal. Auch die Integration mit dem bereits vorhandenen ERP-System verlief reibungslos: Rechnungen und Belege sind so mit dem ERP verknüpft, dass sie auch aus diesem System innerhalb eines Rechnungsdialogs heraus angezeigt werden können. Per Mausklick auf das entsprechende Dokument öffnet sich der DocuWare Web-Client und zeigt dann das verknüpfte pdf an.

Unternehmensnutzen

- Transparenz:
  Jeder Mitarbeiter gemäß dem Berechtigungskonzept sowie die Geschäftsführung haben Einsicht in die Dokumente und können den Status einzelner Vorgänge problemlos nachvollziehen beziehungsweise nachverfolgen.
- Schneller Zugriff auf die Dokumente, besonders in der Finanzbuchhaltung
- Prozessvereinheitlichung:
  Es gibt nun eine klar definierte Prozess-Struktur. Diese führt zu einer besseren Nachvollziehbarkeit und Dokumentation der Unternehmensvorgänge.
- Standortunabhängiges Arbeiten:
  Hafner Bau skaliert das Projekt für mehrere Mandanten. Insgesamt sind DocuWare und JobRouter in vier Büros im Einsatz, mehrere Firmen arbeiten standort-unabhängig damit.

Fazit

Routinemäßige Arbeitsabläufe wurden bei Hafner Bau automatisiert. Der konstante Zugriff auf Dokumente wurde gewährleistet, höhere Transparenz und kürzere Liegezeiten kamen hinzu – Rechnungen können theoretisch innerhalb von zwei Tagen ab der Erfassung durch die Finanzbuchhaltung freigegeben werden.

Axel Schneider | www.alos.de

BEDIENKONZEPTE 4.0

WIE BUSINESS-SOFTWARE DIE ANFORDERUNGEN DER GENERATION Y ERFÜLLEN KANN

Enterprise-Resource-Planning-Systeme (ERP) zählen zu den mächtigsten Anwendungen, die der Markt für Business-Software bereithält. Zusätzlich zu den betriebswirtschaftlichen Prozessen und dem Produktlebenszyklusmanagement (PLM) decken sie die Bereiche Kundenbeziehungsmanagement (CRM), Lieferkettenmanagement (SCM) und Aftersales ab. Mehr Komplexität geht nicht.

Vor diesem Hintergrund galt es lange Zeit als das Nonplusultra des Bedienkomforts, wenn Anwendern Fenstertechniken zur Verfügung standen, über die sie ihre Aufgaben und Vorgänge in exakt derjenigen Reihenfolge erledigen konnten, die ihrem persönlichen Arbeitsverständnis entsprach. Inzwischen vollzieht sich jedoch ein tief greifender Wandel. Erstmals treffen wir auf Anwendergruppen, die eine völlig andere Vorstellung davon haben, welche Prozess- und Entscheidungsunterstützung ihr ERP ihnen geben soll. Mit wachsendem Selbstbewusstsein fordern sie rein intuitiv nutzbare Zugriffsmöglichkeiten, die ein Minimum an Vorwissen erfordern und ein Maximum an Benutzerfreundlichkeit gewährleisten.

Mobile Einsatzszenarien treiben die Entwicklung

Wenig verwunderlich ist daher auch die Erwartungshaltung, dass sich das Bedienkonzept einer ERP-Lösungen möglichst eng an die Philosophien anlehnen soll, welche die mobilen Betriebssysteme iOS und Android vorgeben. Aus Sicht der Entwicklungsabteilungen verdoppeln sich damit die Anforderungen. Sie müssen das Look & Feel beider Systeme nachbilden. Nur dann bekommen ERP-Anwender die Usability der Plattformwelt ihrer Wahl.

> ERSTMALS TREFFEN WIR AUF ANWENDERGRUPPEN, DIE EINE VÖLLIG ANDERE VORSTELLUNG DAVON HABEN, WELCHE PROZESS- UND ENTSCHEIDUNGSUNTERSTÜTZUNG IHR ERP IHNEN GEBEN SOLL.
>
> Martin Hinrichs, Produktmanager, ams.Solution AG, www.ams-erp.de

Besonders stark vollzieht sich diese Entwicklung in all jenen Bereichen, wo Mitarbeiter in direktem Kundenkontakt stehen und ihre IT-Aufgaben auf mobilen Endgeräten erledigen. Der Vertrieb und das Servicemanagement bilden daher die Speerspitze der Entwicklung. Beispiel Kundendienst: Mehr und mehr Servicetechniker greifen per Webbrowser oder App auf die ERP-Informationen zu, die sie für ihre aktuellen Reparatur- oder Wartungsaufträge brauchen. Technologiebedingt bietet die App-Anbindung an das ERP eine Reihe funktioneller Vorteile. Sie ermöglicht eine integrierte Kameranutzung, so dass die Techniker ihre Arbeit dokumentieren können, ohne das Bildmaterial per Hand hochladen und mit dem laufenden Auftrag verknüpfen zu müssen.

Personalisierbare Dashboards

Über die prozessbegleitende Aufbereitung, sowohl der technischen als auch der auftragsbezogenen Daten, entstehen durchgängige Workflows, die weitgehend automatisiert ablaufen. In der Folge können sich die Anwender auf das Handling von Planabweichungen konzentrieren. Sowie auf all jene Aufgaben, bei denen es um betriebswirtschaftliche Entscheidungen geht, die die Kompetenzen und das Fingerspitzengefühl erfahrener Mitarbeiter erfordern.

Um all diese Handlungsbedarfe frühestmöglich transparent zu machen, eignet sich der Einsatz personalisierbarer Dashboards. Zusätzlich zu ihrer Funktion als Früherkennungssystem dienen Dashboards als eine Art digitaler Steuerstand: Wechselt darin zum Beispiel eine Kennzahlenampel von Grün auf Gelb, gelangt der Anwender in genau diejenigen Bereiche seiner ERP-Lösung, in der er die Ursachenanalyse vertiefen und erforderliche Ausgleichsmaßnahmen einleiten kann.

Martin Hinrichs

UNTERNEHMENSSPEZIFISCHE PROZESSE

„DIE HATTEN VERSTANDEN, WAS WIR WOLLTEN“

Unternehmensspezifische Prozesse bieten ERP-Systeme meist erst nach Anpassungen. Mit dem richtigen System lassen sich aber sogar komplett neue Produkte ohne teure Unterstützung durch den Software-Anbieter relativ einfach abbilden.

Die Wuppertaler HUEHOCO-Gruppe ist ein Global Player für die Veredelung von Metallprodukten. Mit über 1.000 Mitarbeitern und Mitarbeiterinnen an 14 Fertigungsstandorten beliefert man 40 Länder und über 30 Branchen. Durch die Vernetzung aller Unternehmen bietet die familiengeführte Unternehmensgruppe branchenübergreifende Systemlösungen für veredelte Metallbänder. Größter Abnehmer ist die Automobilindustrie, wobei nicht die OEMs direkt beliefert werden, sondern deren Zulieferer, die dann wiederum die OEMs mit ihren Produkten beliefern. Weitere Kunden sind Elektronikfirmen und die Nahrungsmittelindustrie.

Überzeugend dank Testsystem

Bis zum Jahr 2007 gab es bei HUEHOCO lediglich eine rein kaufmännische Software, die etwa einen Lieferschein oder eine Rechnung erzeugen konnte. Trotz Ausbau konnte das Programm die Anforderungen, die man an moderne Unternehmen stellt, nicht mehr erfüllen. Es war kaum möglich, die Daten in einen Gesamtzusammenhang zu bringen, also sich etwa mit den Themen Preisen und Disposition zu beschäftigen oder vorausschauende Planungen durchzuführen. In einem Auswahlprozess wollte man darum herauszufinden, welche Anbieter mit einem geeigneten Software-Produkt es überhaupt gab. Die großen Anbieter wie SAP hatte man grundsätzlich ausgeschlossen, weil sich deren Systeme relativ starr präsentierten und man eher die eigenen Prozesse an das ERP-System angleichen musste als umgekehrt.

Die Wahl fiel rasch auf die ERP-Lösung caniasERP des Softwarehauses Industrial Application Software GmbH (IAS). Das System überzeugte bei der Präsentation außer durch seine Flexibilität direkt mit einem Testsystem, sodass IT-Leiter Klaus Peter Schönfeld sicher war: „Die hatten verstanden, was wir wollten.“ Zunächst programmierten die Berater des IAS-Projektteams die meisten Anpassungen und übergaben sie der IT-Abteilung zum Testen, damit kleine Fehler beseitigt werden konnten. Es entstand gleich so etwas wie eine Individualprogrammierung. Aber schnell konnte sich Schönfeld selbst intensiver mit der Programmierung beschäftigen und eigenständige Lösungen entwickeln. Denn das Highlight von caniasERP ist für den IT-Profi der Zugriff auf den kompletten Source Code und die Entwicklungsumgebung mit der Programmiersprache TROIA, die von IAS mitgeliefert werden. „Wir können alles abdecken, von der FiBu über die Anlagenbuchhaltung bis zur Konzernkonsolidierung erledigen wir alles in caniasERP“, so Schönfeld.

Keine Grenzen

„Man kann mit logischem und mathematischem Verständnis alles selbst programmieren. Die Anpassungen, die wir bis jetzt schon programmiert haben, hätten wir mit keiner anderen Software realisieren können“, weiß Schönfeld und resümiert: „caniasERP ist wirklich eine tolle ERP-Lösung. Wenn sie mal in unsere Transaktionsliste schauen, stellen sie fest, dass die Anzahl der Neuentwicklungen inzwischen größer ist, als die der Standardfunktionalitäten. Es ist ein absolutes Highlight für uns, dass wir über den gesamten Source Code inklusive der Prüftabellenwerte, die hinterlegt sind, verfügen. Und das Tollste daran ist: Ich habe noch keine Grenzen entdeckt, die sich nicht mit eigenen Mitteln überwinden ließen.“

Volker Vorburg | www.caniaserp.de

Von links nach rechts: Klaus-Peter Schönfeld, IT-Leiter und Mike Schirrmacher, ERP-Programmierer.

UNATTENDED SETUP

DAS CLIENT MANAGEMENT ALS TRAGENDE ROLLE BEI DER IT-ZENTRALISIERUNG

„Turnschuh-Administration" wäre noch eine krasse Untertreibung gewesen: Für die IT-Abteilung der Rieck Logistik-Gruppe, inhabergeführtes Familienunternehmen mit Hauptsitz in Großbeeren (südl. von Berlin), hätte es früher wohl eher einer mehrtägigen Reise bedurft, um IT-Probleme an ihren Standorten in China zu beheben. Deshalb kümmerte sich bisher natürlich ein Kollege vor Ort darum. Doch genau das war das Problem: Der zentralen IT oblag zwar die Aufsicht, sie gab die grundlegende Richtung vor. Einfluss auf den Betrieb vor Ort hatte sie jedoch nicht. So schraubte jeder (Teil- oder Vollzeit-)Administrator in den Niederlassungen an den Clients herum; verschiedene Groupware-Lösungen an den Standorten verschleierten den Überblick, was überhaupt an Software und Hardware installiert ist. Prozessoren verschiedenster Generationen und unterschiedliche Festplattenarten waren im Einsatz. Eine solche Heterogenität macht den IT-Betrieb wenig kontrollierbar und unüberschaubar.

Schon seit 2009 sind diese Zustände bei Rieck allerdings Vergangenheit. Zu diesem Zeitpunkt hatte das Unternehmen seine komplette IT erneuert. Neben der Virtualisierung von rund 45 Applikationsservern im Rechenzentrum Großbeeren sowie der Einführung von Citrix-Terminalclients für alle Standorte außerhalb des Großraums Berlins, gehörte dazu auch die Standardisierung der Hard- und Software aller Arbeitsplatz-PCs im Unternehmensverbund sowie die Einführung eines standortübergreifenden Client Managements. Zu den Aufgaben der 14 Team-Mitglieder der Rieck-IT zählen seitdem nicht nur die Weiterentwicklung und Pflege der selbstentwickelten Speditionssoftware, sondern auch die Planung und Betreuung der gruppenweiten Netzwerk- und Client-Infrastruktur.

Tabula rasa anstatt Stückwerk

Allein 300 PCs wurden damals neu angeschafft und mittels der Client-Management-Lösung von Aagon mit Betriebssystem und Software bestückt. „Tabula rasa zu machen, war für uns die wirtschaftlichste Alternative", sagt Tom Polten, IT-Leiter der Rieck Logistik-Gruppe. Für die ACMP Suite als neu-

Quelle: Rieck Logistik-Gruppe

es Client-Management-System hatte sich die Rieck-Gruppe entschieden, „weil uns das Produkt durch seine Einfachheit im Umgang überzeugte. Die Art der Softwareverteilung sucht ihresgleichen", erklärt Tom Polten. Dem IT-Leiter gefällt auch das kollegiale Miteinander. „Für angeblich falsche Fragen abgekanzelt zu werden, wie man es von manchem großen US-Hersteller kennt, geschieht einem bei Aagon nicht. Man agiert auf Augenhöhe – von Mittelständler zu Mittelständler."

Software-Paketierung als fortdauernder Prozess

Im ersten Schritt installierte die IT-Abteilung den ACMP-Agenten auf allen bestehenden Clients, um die bestehende Hard- und Software zu inventarisieren. Die dabei gewonnenen Informationen dienten der Ausstattungsplanung der neuen Client-PCs; außerdem ließen sich so auch Anwendungen identifizieren, die nicht gebraucht und somit entfernt werden können. Im nächsten Schritt ging es daran, Softwarepakete für die automatische Verteilung der Anwendungen auf die neuen Arbeitsplatzrechner zu erstellen. „Paketieren von Software ist kein einmaliger Vorgang, sondern ein Prozess, der eigentlich nie abgeschlossen ist", erklärt Tom Polten. „Wir haben unsere Anwendungen zunächst priorisiert und dann damit begonnen, die Applikationen der Reihe nach zu verpacken".

Entsprechend seinem Rollout-Profil erhält ein neuer Client-PC bei Rieck immer genau die Softwareausstattung, die der jeweilige User benötigt, bevor der Rechner an dessen Arbeitsplatz aufgestellt wird. Für die spätere Versorgung mit Updates oder sogar eine Neuinstallation des Betriebssystems reicht es dann aus, dass der PC mit dem Netzwerk verbunden ist. Alle Softwareinstallationen finden als „unattended Setup" statt, was im Gegensatz zum Imaging-Verfahren deutlich mehr Flexibilität bietet. Der Rechner wird dabei automatisiert im laufenden Betrieb bespielt, ohne dass der User davon beeinträchtigt wird.

KURZ NOTIERT:

Um die Kontrolle über ihre weltweit verteilte IT-Landschaft zurückzugewinnen, hat die Rieck Logistik-Gruppe schon im Jahr 2009 ein großes Zentralisierungsprojekt gestartet. Dazu gehörte auch die Einrichtung des Client-Management-Systems von Aagon, das die Administration seitdem sichtlich erleichtert.

Angebundene Arbeitsplatzstationen:
500 Windows Clients

Eingesetzte Produkte:
ACMP Inventory, ACMP Desktop Automation, ACMP OS Deploy-ment, ACMP Lizenzmanagement, ACMP Security Detective

Projektstart:
Herbst 2018 (Lizenzmanagement)

Nutzen:
- Client-Rollout dauert statt vier Stunden nur noch 30 Minuten
- Softwareinstallationen finden als „unattended Setup" statt
- Rollenprofile im Client-Management-System schnell anpassbar

500 Rechnerarbeitsplätze optimal verwaltet

Fünf verschiedene Rollen haben Tom Polten und sein Team im Client-Management-System definiert, darunter als wichtigste ein Logistikprofil mit verschiedenen Logistik-ERP-Systemen, ein Buchhaltungsprofil mit SAP sowie ein Vertriebsprofil mit den vertriebsrelevanten Systemen. „Diese Rollen ändern sich aber auch ständig", erläutert der IT-Leiter. „Mit der ACMP-Suite können wir dies sehr gut anpassen, ohne dafür gleich das Image des Rechners auf den Kopf zu stellen" – für ihn ein klarer Vorteil gegenüber reinen Imaging-Lösungen.

Inzwischen sind es 500 Rechnerarbeitsplätze, die unter permanenter Aufsicht des Client Managements stehen. Das Rollout eines neuen Clients dauert heute statt vier Stunden nur noch 30 Minuten. 16 Clients kann das IT-Team mit dem Client-Management-System parallel betanken und erfüllt so den selbst gesteckten Anspruch: Ist ein PC defekt, steht bereits am nächsten Werktag ein neuer bereit, und zwar an allen Standorten weltweit. In der Zentrale in Großbeeren ist ein solcher Hardwareaustausch – also das Bereitstellen eines neuen Rechners mit aktueller Softwareausstattung – sogar innerhalb von zwei bis drei Stunden der Fall.

Die Mehrheit der 14 Beschäftigten in der IT-Abteilung ist ohnehin im Wesentlichen mit Softwareentwicklung und Datenintegration befasst. Das Administrations-Team kann – dank Unterstützung des Client-Management-Systems – klein gehalten werden, und vor Ort in China, Tschechien und anderswo ist niemand mehr erforderlich, der sich um Softwareupdates und dergleichen kümmert. Lediglich neue Hardware muss im Bedarfsfall aufgestellt werden – um den Rest kümmert sich die zentrale IT. Für Tom Polten sind die wertvollsten Komponenten das Softwaredeployment und die Übersichten in ACMP, beziehungsweise die Client Commands. Bei Rieck wird keine Software mehr ohne Client Command installiert. „Dies hilft uns ungemein, die Systemlandschaft homogen zu halten." Mehrere 100 eigene Commands wurden seit Einführung des Systems erstellt.

Lizenzmanagement im Vorfeld erspart das Audit

Automatische Verteilung von Betriebssystemen sowie Anwendungen auf einheitliche Hardware in allen Standorten ist aber nicht alles, was die Rieck Logistik-Gruppe mit dem Client-Management-System erledigt. Im Vorfeld eines angekündigten Audits von Microsoft wurde auch das Lizenzmanagement-Modul der Aagon-Software implementiert und mit Unterstützung des Herstellers eine unternehmensweite Übersicht der installierten Softwarelizenzen erstellt. „Diese wurde Microsoft übermittelt, seitdem haben wir Ruhe", so Tom Polten zufrieden.

www.aagon.de

GERÄTEAUSWAHLPROGRAMME FÜR MITARBEITER

HOCHQUALIFIZIERTE UND MOTIVIERTE FACHKRÄFTE GEWINNEN UND HALTEN

Zufriedene Mitarbeiter, die produktiv arbeiten und dem Unternehmen treu bleiben - welcher Personalmanager wünscht sich das nicht? Jeder hat von den großartigen Angeboten der Tech-Unternehmen im Silicon Valley gehört, bei denen Mitarbeiter unter anderem kostenlose Massagen, Vollverpflegung und regelmäßige Sabbaticals genießen. Wie die etwas traditionsreichere US-Firma IBM kürzlich demonstrierte, sind für die Mitarbeiterschaft daneben auch die „hard facts", genauer gesagt die Hardware, ein wichtiges Argument: Apple-Geräte erfreuen sich demnach als Arbeitsgeräte im Beruf immer größerer Beliebtheit. Seit 2015 lässt IBM im Rahmen des Mac@IBM-Programms Mitarbeitern die Wahl, ob sie für ihre Arbeit Mac oder PC nutzen wollen. Die Ergebnisse stellte IBM CIO Fletcher Previn im November 2019 auf der Jamf Nation User Conference in Minneapolis vor. Sie zeigen, dass IBM-Mitarbeiter, die Mac verwenden, länger im Unternehmen bleiben und ihre Leistungen im Vergleich zu PC-Nutzern höher sind.

Die Bedeutung von Technologieauswahl in Großunternehmen (Copyright: Jamf)

Konkret brachte das Geräteauswahlprogramm eine nachweislich verbesserte Mitarbeiterleistung: 22 Prozent mehr macOS- als Windows-Benutzer haben die von ihnen erwartete Leistung übertroffen. Außerdem waren hochvolumige Verkaufsabschlüsse bei macOS-Anwendern in der Regel um 16 Prozent höher als bei Windows-Anwendern.

Auch die Mitarbeiterzufriedenheit fiel höher aus: macOS-Anwender erzielten einen höheren Net Promoter Score als Windows-Nutzer: 47,5 im Vergleich zu 15. Außerdem ist es um 17 Prozent weniger wahrscheinlich, dass sie IBM verlassen. macOS-Anwender sind zufriedener mit der Verfügbarkeit von Drittanbieter-Software bei IBM. Nur 5 Prozent der macOS-Nutzer fragen zusätzliche Software an, verglichen mit 11 Prozent der Windows-Nutzer.

Zusätzlich wirkte sich das Wahlprogramm positiv auf die laufenden Kosten und die Beanspruchung der IT-Abteilung aus: IBM stellt fest, dass nur 5 Prozent der Mac-Anwender Anfragen an den Helpdesk richten, verglichen mit 40 Prozent der PC-Anwender im gleichen Zeitraum. Aktuell sind daher nur sieben IT-Mitarbeiter mit dem Support von 200.000 macOS-Geräten befasst, während für 200.000 Windows-Geräte 20 IT-Mitarbeiter nötig sind. Das entspricht einem 186 Prozent höheren Support-Aufkommen für Windows-Geräte. Insgesamt sparte IBM - über einen Zeitraum von vier Jahren gerechnet - pro Mac zwischen 273 und 543 US-Dollar im Vergleich zu einem PC.

IT-Wahlfreiheit für Mitarbeiter

Neben diesem Einzelbeispiel bestätigt auch eine von Jamf durchgeführte Studie* den Trend zu Wahlprogrammen. Mehr als die Hälfte der befragten Unternehmen (52 Prozent) bietet ihren Mitarbeitern die Möglichkeit, den für die Arbeit genutzten Computertyp selbst zu bestimmen. Wenn Unternehmen ihren Mitarbeitern die Möglichkeit bieten, die Technologie selbst zu wählen, entscheiden diese sich überwiegend für Apple: 72 Prozent im Gegensatz zu 28 Prozent, deren Wahl auf einen PC fällt. Ähnlich ist der Trend bei Mobilgeräten: Fast die Hälfte (49 Prozent) der Unternehmen ge-

stattet ihren Mitarbeitern, ihr mobiles Arbeitsgerät selbst auszuwählen. 75 Prozent der Befragten gaben an, dass sie sich für ein iPhone oder iPad entscheiden. Nur 25 Prozent wählen ein Android-Gerät und weniger als 1 Prozent einen Blackberry.

Mit der Unternehmensgröße wächst auch die Bedeutung der Technologieauswahl. So ist in Unternehmen mit mehr als 500 Mitarbeitern der Wunsch nach Auswahlmöglichkeiten der Technologie deutlich größer. So gaben in Großunternehmen 86 Prozent der Mitarbeiter an, dass es ihnen wichtig ist, mit einem Gerät ihrer Wahl arbeiten zu können. 50 Prozent der Befragten sagten, dass die Wahlmöglichkeiten ihnen sogar sehr oder extrem wichtig sind.

Auch den Einfluss auf die Arbeitgeberauswahl belegt die Studie: So sagen 77 Prozent der Mitarbeiter, in deren Unternehmen es derzeit ein solches Programm gibt, dass sie sich wieder für einen Arbeitgeber entscheiden bzw. eher bei ihm bleiben würden, der ihnen hinsichtlich der Geräte ebenfalls die Wahl lässt. Dies zeigen auch zahlreiche aktuelle Stellenangebote auf deutschen Job-Portalen, wie eine Freitextsuche nach „iPhone“ oder „iPad“ zeigt:

IT-Wahlfreiheit ist keine Momentaufnahme, sondern ein eindeutiger Trend: 80 Prozent der Studienteilnehmer glauben, die Wahlfreiheit sei mehr als nur eine Modeerscheinung und fordern, sie solle in der Geschäftswelt zur Norm werden.

Sechs Schritte zur Realisierung eines Geräteauswahlprogrammes

Für die Einführung eines Wahlprogrammes empfehlen sich folgende sechs Schritte:

1. Pilotprojekt starten

Wählen Sie eine Abteilung oder Gruppe aus, die ihren Arbeitscomputer bzw. ihr Mobilgerät auswählen darf. So können Sie die Einführung testen und feststellen, welche Lücken hinsichtlich Software und Support eventuell noch bestehen.

2. Bedarf ermitteln

Klären Sie mit der Personalabteilung, wie oft die Frage nach Auswahlmöglichkeiten in Bewerbungsgesprächen auftaucht. Oder führen Sie eine interne Umfrage zum Betriebssystem bzw. zur Hardware durch, für die sich die Mitarbeiter entscheiden würden, wenn sie die Wahl hätten. So können Sie den Umfang Ihres zukünftigen Projekts besser abschätzen.

3. Software aktualisieren

Nicht jede Software funktioniert auf jedem Gerät und jeder Plattform gleich gut. Oft gibt es Alternativen zu bereits vorhandenen Tools, die für eine höhere Produktivität der Mitarbeiter sorgen. Sehen Sie sich im Apple App Store nach (kostenlosen) Softwarelösungen um, die bereits auf dem Markt sind. Halten Sie Ausschau nach cloudbasierten Lösungen, die im Browser ausgeführt werden und veraltete Desktop-Software ersetzen können.

4. Den gesamten Benutzerkomfort einbeziehen

Versetzen Sie sich in die Lage der Benutzer: Wie sieht es mit der Benutzerfreundlichkeit aus – von den Anforderungen eines neuen Geräts, über den Empfang von Benachrichtigungen, bis hin zum Support für neue Software oder Betriebssysteme? Erwägen Sie die Einführung eines Portals, auf dem Benutzer ihr neues Gerät auswählen und bestellen können. Schauen Sie sich andere Support-Seiten an, die Ihnen gefallen, und orientieren Sie sich an deren Benutzeroberfläche. Die Support-Seiten von Apple sind dafür ein hervorragender Ausgangspunkt. Apple bietet zudem eine Fülle von Ressourcen, angefangen bei macOS Einführungshandbüchern bis hin zur Unterstützung für Ihr internes Portal.

5. Flexibilität bieten

Wenn Sie bereit sind, Ihr Programm für die breite Masse einzuführen, gehen Sie das Projekt richtig an, indem Sie Offenheit zeigen. Gehen Sie davon aus, dass nicht alle Mitarbeiter das gleiche Gerät wählen oder mit ihrer ersten Entscheidung zufrieden sein werden. Erwägen Sie, eine Rücktrittsmöglichkeit anzubieten. IBM bot bei seinem Auswahlprogramm eine 60-Tage-Rücktrittsfrist an. So haben die Mitarbeiter die Freiheit, ihre Geräteentscheidung erst einmal zu testen.

80 PROZENT DER TEILNEHMER EINER JAMF-STUDIE ZU MITARBEITERWAHLPROGRAMMEN GLAUBEN, DIE WAHLFREIHEIT SEI MEHR ALS NUR EINE MODEERSCHEINUNG UND SIE SOLLE IN DER GESCHÄFTSWELT ZUR NORM WERDEN.

Oliver Hillegaart,
Regional Sales Manager DACH, Jamf,
www.jamf.com

6. Auswirkungen messen

Nachdem die Mitarbeiter ihre Geräte erhalten haben, sollten Sie anschließend ermitteln, was die Benutzer von dem gewählten Gerät und dem Geräteauswahlprogramm halten. Dies kann zum Beispiel bei der jährlichen Mitarbeiterbefragung eruiert werden. Wichtig zur Befragung: Die gleichen Fragen sollten vor - und nach Einführung des Programms gestellt werden – nur so erhalten Sie ein aussagekräftiges Ergebnis.

Oliver Hillegaart

*Quelle: Umfrage „Der Einfluss von Geräteauswahlprogrammen auf die Mitarbeiterzufriedenheit“, Jamf Software, 2018.

WORKSPACE 4.0

SICHER ZUSAMMENARBEITEN IN DER CLOUD

Auch im Hinblick auf die Arbeitswelt der Zukunft kann die Digitalisierung enorme Vorteile ausspielen. Das gilt insbesondere für das Arbeiten in der Cloud. Nichtsdestotrotz sind die Hemmungen hier und da nach wie vor groß, wenn es etwa darum geht, die Grundlage für digitale Arbeitsstrukturen zu schaffen.

Das Thema Arbeitswelt 4.0 gewinnt immer stärker an Bedeutung. Denn mit ihm verknüpfen sich große Hoffnungen, die gegenwärtigen und zukünftigen Herausforderungen einer dynamischen Wirtschaftswelt zu lösen. Dazu zählen etwa der Fachkräftemangel, das Angebot flexibler, moderner Arbeitsmodelle, die Vereinbarkeit von Familie und Beruf oder der Austausch auf globaler Ebene. Als einer der wichtigsten Hebel hierfür gilt die Cloud. Hierüber herrscht längst Konsens. Gleichzeitig befeuern schlechte Erfahrungswerte in Sachen Verfügbarkeit und Sicherheit die Zurückhaltung vieler Verantwortlicher und verhindern Entwicklungsschritte, die dringend notwendig sind. Doch woran erkennen Unternehmer geeignete Angebote? Welche technischen Voraussetzungen muss eine Cloud-Lösung mitbringen, um maximale Sicherheit zu gewährleisten? Welche Funktionen sollte sie unterstützen? Und welche Risiken können mit Cloud-Lösungen verbunden sein? Bei all diesen Fragen ist es lohnenswert, sich Zeit für das Kleingedruckte zu nehmen.

Zusammenarbeit über klassische Grenzen hinweg

Bevor diese Fragen beantwortet werden können, gilt es einen Blick auf die Definition einer Arbeit 4.0 zu werfen. Was bedeutet sie konkret? Wie ist sie ausgestaltet? Und wo schlummern Potenziale?

Arbeit 4.0 bedeutet hohe Flexibilität in Bezug auf den Arbeitsort und den Austausch von Daten in sämtlichen Prozessen. Die Mitarbeiter können folglich jederzeit über eine zentral bereitgestellte Wissensdatenbank auf alle für sie relevanten Prozesse und Dateien zugreifen. Auf diese Weise kann der intensive Austausch von Wissen nach innen wie nach außen gelingen, und es entsteht eine einheitliche Wissensbasis. Dieses ortsunabhängige Arbeiten ist allerdings nur dann möglich, wenn die entsprechende Cloud-Infrastruktur im Unternehmen vorhanden ist. Dafür ist vor allem auch eines besonders ausschlaggebend: Vertrauen in Anbieter und Technologie. Denn ein Unternehmen hat wenig davon, seinen Mitarbeitern flexibles Arbeiten und digitale Prozesse zu ermöglichen, wenn diese Bemühungen gleichzeitig potenziellen Angreifern Tür und Tor öffnen. Im Ergebnis versprechen Flexibilisierungsvorhaben mit der Hilfe von Cloud-Lösungen einen Mehrwert für Arbeitgeber und Mitarbeiter gleichermaßen. Flexiblere Arbeitszeitgestaltung, die bessere Verein-

DIGITALE ARBEIT 4.0 IST AUF DEM VORMARSCH. WER IN ZEITEN VON FACHKRÄFTEMANGEL UND DEM SOGENANNTEN „WAR FOR TALENTS" ENTSPRECHENDE STRUKTUREN IMPLEMENTIERT, KANN SICH EINEN ECHTEN WETTBEWERBSVORTEIL VERSCHAFFEN.

Luc Mader,
CEO und Geschäftsführer, luckycloud,
www.luckycloud.de

barkeit von Beruf und Familie, die am Ende des Tages zu höherer Leistungsfähigkeit und Motivation führen.

Potenziale und Risiken adäquat einschätzen

Trotz des offenkundigen, enormen Potenzials herrscht noch immer große Cloud-Skepsis – gerade in kleinen und mittelständischen Unternehmen, die jeden Wettbewerbsvorteil für sich nutzen müssen, um langfristig erfolgreich zu sein. Im Zentrum der Zurückhaltung stehen vor allem Fragen nach den technischen Voraussetzungen. Betrachtet im Kontext von DSGVO & Co., Cyber-Spionage und Datenmonetarisierung sind diese Sorgen auch berechtigt. Dabei sind die Mindestanforderungen für eine sichere Workspace 4.0-Lösung auf den ersten Blick wenig überraschend. Der Teufel liegt jedoch im berühmten Detail.

Ein zentrales Sicherheitskriterium ist der Serverstandort, den der Cloud-Anbieter offeriert. Der sollte ausnahmslos in Deutschland liegen, um eine mögliche Datenverarbeitung in Drittländern auszuschließen. Im gleichen Zuge gilt es auf eine hochverfügbare und ausfallsichere IT-Infrastruktur zu achten, etwa durch georedundante Verteilung der Rechenzentren oder eine Verwendung von SDS-Clustern. Weil sich auch in der Cloud manche Anbieter ein Hintertürchen offenhalten, sorgen der konsequente Einsatz von Open Source Software sowie die strenge Einhaltung des Zero-Knowledge-Prinzips für weitere Sicherheit und Flexibilität im Gesamtsystem. Diese schließt zum Beispiel die clientseitige Verschlüsselung ein, bei der die Schlüsselhoheit allein beim Nutzer liegt. Nur auf diese Weise bleibt die Datenhoheit in Hand des eigenen Unternehmens, denn nicht einmal die Administratoren des Anbieters können dann auf den Code-Schlüssel zugreifen – ganz im Gegensatz zu einigen Angeboten mit Ende-zu-Ende Verschlüsselung. Nicht zuletzt gilt es auf plattformübergreifende Clients und Apps zu achten, die das zeit- und ortunabhängige Arbeiten ermöglichen.

Empfehlenswert sind zweifelsohne Gesamtlösungen, deren Funktionsumfang zudem online wie offline abrufbar ist. Auch Lese- oder Schreiberechte lassen sich hier in der Rechteverwaltung anpassen. Ein weiterer Pluspunkt ist ein Administrations-Dashboard, das schnell und einfach einen Überblick verschafft und die Möglichkeit bietet, Benutzerverwaltung und Datenorganisation flexibel zu handhaben – und das unabhängig vom Standort des Mitarbeiters.

Entschlossen zum Workspace 4.0

Digitale Arbeit 4.0 ist auf dem Vormarsch. Wer in Zeiten von Fachkräftemangel und dem sogenannten „War for Talents" entsprechende Strukturen implementiert, kann sich einen echten Wettbewerbsvorteil verschaffen. Immerhin erzeugt ein cloudbasiertes Arbeiten 4.0 überzeugende Flexibilitäten in Form ortsunabhängiger Arbeitsmodelle für potenzielle Kandidaten. Wer dabei auf einige technische Eckpfeiler cloudbasierter Arbeitslösungen achtet, muss auch vor bösen Überraschungen keine Angst haben.

Luc Mader

CHECKLISTE
ARBEITEN 4.0 IN DER CLOUD

Hochverfügbarkeit und Geo-Redundanz:

- ☐ hoch-skalierbares SDS-Cluster
- ☐ ISO-zertifizierte Rechenzentren in Deutschland
- ☐ Hybrid Cloud Ansatz bzw. NAS Einbindung + Backup

Schlüsselhoheit und Sicherheitsfeatures:

- ☐ Open Source
- ☐ 3-fach-Verschlüsselungen
- ☐ Block-Versionierung
- ☐ 2-Faktor-Authentisierung
- ☐ stündliche Backups

Orts- und zeitunabhängiges Arbeiten:

- ☐ Mobile App
- ☐ Sync-Client / Drive-Client/ Web-Client / WebDAV
- ☐ RESTful API

Teamwork und Datenaustausch:

- ☐ Web-Office
- ☐ Chat
- ☐ Wikis
- ☐ Aktivitäten
- ☐ Rollenmanagement
- ☐ Freigabelinks
- ☐ verschlüsselte Benutzerfreigaben

Betreuung:

- ☐ individuelle Beratung
- ☐ persönliches Onboarding
- ☐ 24/7-Support bei systemkritischen Anfragen

ENTERPRISE CONTENT

HERZSTÜCK DER DIGITALISIERUNG

Der digitale Arbeitsplatz ist kein Selbstzweck der digitalen Transformation, sondern soll konkreten Geschäftsnutzen bringen. Auch wenn nicht alle das Gleiche unter einem digital Workplace verstehen, sind die Hauptanforderungen in allen Unternehmen gleich. Er erfordert einen zentralen Informationszugang, die Einbindung vereinbarter Kommunikationsmittel, effektive Collaboration, sicheres Dokumentenmanagement und transparente Prozesse. Eine ECM-Lösung als Herzstück des digital Workplace erfüllt diese Geschäftsanforderungen für ein integriertes Informations- und Prozessmanagements – flexibel anytime & anywhere. Der digitale Arbeitsplatz baut Informationssilos in Unternehmen ab und öffnet sich für die Zusammenarbeit mit Kunden und Lieferanten. Er vernetzt alle Mitarbeiter, fördert den Wissensaustausch und verbessert die Effizienz der Arbeitsprozesse.

Ganzheitlich denken

Am Anfang des digital Workplace steht die Digitalisierungsstrategie. Was soll mit dem digitalen Arbeitsplatz erreicht werden? Eine höhere Produktivität, eine bessere Zusammenarbeit, ein moderner Arbeitsplatz für Mitarbeiter? Eine Digitalisierungsstrategie enthält personenbezogene Überlegungen zu Organisation, Arbeitsstil und Unternehmenskultur. Sie zieht die Anpassungsfähigkeit von Mitarbeitern auf die Digitalisierung (digital Dexterity) und die Benutzerfreundlichkeit der Softwarelösungen in Betracht. Ausstattung, Geschäftsanwendungen, Collaboration, Sicherheit und digitale Infrastruktur sind ebenfalls elementare Bestandteile der Strategie.

Welche Komponenten und Funktionalitäten sind wichtig? Kann die Infrastruktur durch APIs und Konnektoren relativ einfach erweitert werden, um mit neuen Technologien Schritt zu halten und sich an Marktanforderungen anzupassen? Die unternehmensweite Einführung des digital Workplace ist eine große Chance zur IT-Konsolidierung. Die Anzahl der Tools lässt sich fast immer reduzieren und die Lösungen unterschiedlicher Anbieter können besser aufeinander abgestimmt werden. Auf diese Weise schaffen Unternehmen nicht nur eine einheitliche Plattform für die Zusammenarbeit, sondern sparen unnötige Lizenz- und Wartungskosten.

Informationen zentral vorhalten und mit Enterprise Search finden

Der Informationsbestand eines Unternehmens ist heterogen über verschiedene Systeme und Standorte verstreut, oft isoliert und schwer auffindbar. Strukturierte Daten aus Business-Systemen wie ERP, CRM, HR, PDM gehören ebenso dazu wie Briefe, Konzepte, E-Mails, kaufmännische Belege oder Produktbeschreibungen – also die große Masse der unstrukturierten, teilweise gar noch papierbasierten Dokumente. Mit Enterprise Content Management ECM lassen sich diese Teile des Puzzles zu einem Ganzen verknüpfen.

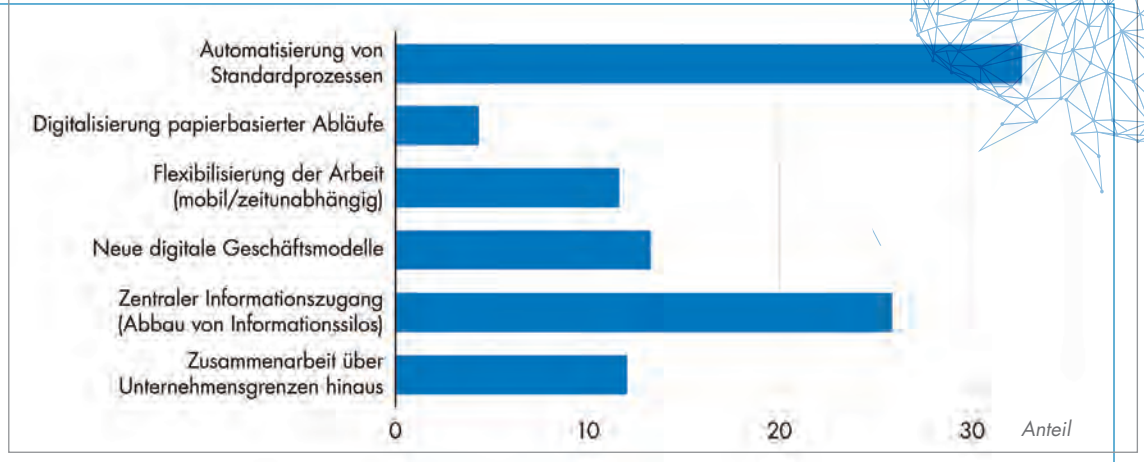
Die ECM-Lösung Doxis4 der SER Group für den digital Workplace bringt Dokumente, Daten und Vorgänge systemübergreifend und kontextbasiert zusammen. Sie erfasst, sammelt, strukturiert, archiviert, findet und verteilt Informationen proaktiv. Wo diese liegen, spielt dabei keine Rolle. Ist die ECM-Basisanwendung mit den Standard-Funktionen implementiert, kann man sie in jede beliebige Abteilung ausrollen und muss sie nur noch an abteilungsspezifische Charakteristika und Anforderungen anpassen.

Kunden und Mitarbeiter erwarten am digitalen Arbeitsplatz Informationen on demand, also zu jeder Zeit und an jedem Ort über ihre (mobilen) Endgeräte hinweg. Hier kommt Enterprise Search als zentrales, unternehmensweites Suchen und vor allem Finden ins Spiel, ohne zwischen verschiedenen Repositories wechseln zu müssen.

DIE SOFTWARE HILFT, EXPERTEN FÜR BESTIMMTE BEREICHE ZU FINDEN UND ÄHNLICHE ODER ERGÄNZENDE DOKUMENTE UND AKTEN ZU IDENTIFIZIEREN. SIE KANN ZUM PERSÖNLICHEN ASSISTENTEN DES ANWENDERS WERDEN.

Franziska Thomas, Head of Group Marketing, SERgroup Holding International GmbH, www.sergroup.com

MANAGEMENT



(Quelle: Marktforschungsreihe SER ECM Insights, 1/2019 – 02/2020)

Welche Aspekte sind für Sie im Rahmen Ihrer Digitalisierungsstrategie besonders wichtig?

Das ECM-System findet systemübergreifend die benötigten Informationen und zeigt die Suchergebnisse transparent in einer einheitlichen, strukturierten Trefferliste an: unabhängig davon, ob es sich um Dokumente, Daten, elektronische Akten, Aufgaben oder Vorgänge handelt. Die zugehörige Quelle wird sofort erkannt und die Benutzer können direkt dorthin abspringen. Das aufwendige Suchen in zahlreichen Informationssilos hat ein Ende – die Basis, um alle Informationen aktiv ohne Medienbrüche in Geschäftsprozessen zu nutzen.

Wo der Schuh noch drückt

Wiederkehrende Prozesse und Workflows sollten möglichst automatisiert sein. Informationen zwischen Systemen sollten selbstständig ausgetauscht und Arbeitsaufträge dokumentiert werden können. Die Wirklichkeit sieht in vielen Fällen noch anders aus. Es gibt zu viele Tools und Anwendungen, die keine unternehmensweiten durchgängigen Prozesse zulassen. Unternehmen sollten die Digitalisierung nutzen, um Prozesse umzustellen, zu automatisieren und nicht mehr manuell suchen, finden, verschieben, versenden … So entsteht ein großes Optimierungspotential. Digitale Workflows statt Umlaufmappen sparen Bearbeitungs- und Durchlaufzeiten und sorgen für transparente Prozesse. Fragen wie „wer hat wann welchen Vorgang wie bearbeitet, was ist die letzte Version, wo liegt sie" gehören dann der Vergangenheit an.

Sinnvoll automatisiert, enorm kollaborativ

Mit einer durchgängigen digitalen ECM-Lösung werden typische Geschäftsprozesse vereinheitlicht, wie die Schadensbearbeitung bei Versicherungen, die Kreditbearbeitung in Banken oder das Vertragsmanagement. Bei der Rechnungseingangsverarbeitung als Querschnittprozess lassen sich Belege automatisiert erfassen, Lieferanten zuordnen, prüfen, mit Bestellungen abgleichen und intern freigeben.

Das Vernetzen von Fachabteilungen, das Bereitstellen von richtigen Daten und Dokumenten zum richtigen Zeitpunkt an die richtigen Personen fördert die Produktivität und schafft Wachstumspotenziale. Auch inspirierte und motivierte Mitarbeiter sind die Folge: kein Frust mehr über zu lange Wartezeiten und fehlende Informationen für schnelle Kundenauskünfte.

Unternehmen sind heute in Business-Ökosysteme eingebunden. Sie interagieren nicht nur mit Kunden und Lieferanten, sondern auch mit Projektpartnern oder Entwicklungskooperationen weltweit. Eine ECM-Lösung muss sich gezielt für externe Partner öffnen lassen, damit alle Beteiligten auf eine verlässliche gemeinsame Informationsbasis zugreifen können. In virtuellen Projekt- und Datenräumen organisieren und bearbeiten sie zusammen Dokumente, Aufgaben und Vorgänge – fristgerecht und für alle nachvollziehbar. Alle Informationen stehen jederzeit aktuell und genau in dem Projektkontext bereit, in dem Teams diese benötigen. Die Verantwortlichen steuern, welche Mitglieder Zugang in die geschützten virtuellen Räume erhalten und wer welche Informationen – auch temporär – einsehen und bearbeiten darf.

Zukunftsfähig

Unternehmen werden immer stärker disruptive digitale Technologien nutzen, um schneller Ideen zu entwickeln und zu skalieren, Produkte herzustellen und so auch in Zukunft gut aufgestellt zu sein. Digitale Geschäftsmodelle und kollaborative Business-Ökosysteme brauchen ein solides integriertes Informations- und Datenfundament, automatisierte Prozesse und sichere Lösungen zur Interaktion mit Kunden, Lieferanten und Partnern. Dies bietet ECM als digital Workplace – ob hybrid, on-premise oder in der Cloud.

Franziska Thomas

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
30. APRIL 2020

TRIO INFERNALE

Low-Code-Plattformen, BPM und RPA

SAP S/4HANA

Auf der Erfolgsspur bleiben

INDUSTRIE 4.0

Der Zukunft entgegen

DIE AUSGABE 04/2020 VON IT MANAGEMENT ERSCHEINT AM 31. MÄRZ 2020.

INSERENTENVERZEICHNIS

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Jeff Aaron, Nicuale Cantuniar, Uwe Gries, Jens Heidland, Felix Heintz, Oliver Hillegaart, Martin Hinrichs, Oliver Krause, Jonathan Knudsen, Darrell Long, Luc Mader, Martin Mangold, Carina Mitzschke, Marcel Mock, Klaus Nemelka, Silvia Parthier, Ulrich Parthier, Axel Schneider, Markus Sieber, Sebastian Spethmann, Alexander Steiner, Franziska Thomas, Volker Vorburg, Elmar Witte

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. 27.
Preisliste gültig ab 1. Oktober 2019.

Mediaberatung & Content Marketing-Lösungen it management | it security | it daily.net:
Kerstin Berthmann
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

G DATA

TRUST IN
GERMAN
SICHERHEIT

Kaffee geholt. Daten weg.

Desktop sperren rettet Unternehmen.

Schaffen Sie IT-Sicherheitsbewusstsein

gdata.de/kaffee

itsecurity

MÄRZ 2020

DAS SPEZIAL

PASSWORD SAFE

WAS IST HEUTE SCHON SICHER?

Sascha Martens, MATESO

CYBERSICHERHEIT IM JAHR 2020

Drei konkrete Bedrohungsszenarien

BERECHTIGUNGS-KONTROLLE

Analyse & Überwachung

VORTEILE VON ZERO TRUST

Sichere Netzwerkumgebung

www.it-daily.net

LOGICALIS
Architects of Change

Setzen Sie auf eine starke Abwehr

- **Endpoint Protection**
- **Office 365 E-Mail Security**
- **Cloud-based Security**

secIT by Heise
HANNOVER 2020

Stand 20

logicalis.de

INHALT

WAS IST HEUTE SCHON

WOZU EIN PASSWORD SAFE NÜTZLICH SEIN KANN

Sascha Martens, CTO & Cybersecurity Evangelist bei MATESO im Gespräch mit Ulrich Parthier, Publisher it security zum Titelthema.

Ulrich Parthier: *Wir hören immer wieder von automatisierten Brute-Force-Angriffen, die zum Ziel haben, Passwörter zu stehlen. Wie groß schätzen Sie die tatsächliche Gefahr ein?*

Sascha Martens: Enorm. Heutige Angriffe, bei denen auch Brute-Force-Angriffe zum Einsatz kommen, werden immer intelligenter und ausgereifter. Denn die Technik entwickelt sich immer weiter und die Angreifer schlafen nicht. Während also die Welt aktuell vom Corona-Virus spricht, hält das Viren-Trio Emotet, Trickbot und Ryuk die IT in Atem.

Ulrich Parthier: *Dabei ist das ja erst der Anfang. Wenn Quantencomputer erst einmal auf dem Markt sind, steigt dann nicht das Diebstahlrisiko erheblich an?*

Sascha Martens: Quantencomputer werden für den gesamten InfoSec-Bereich eine ungemeine Herausforderung. Als Spezialist für Verschlüsselungen beschäftigen wir uns schon lange mit dem Thema und untersuchen den Einfluss auf verschiedene sicherheitsrelevante Bereiche. Alle mit asynchronen Verschlüsselungs-Techniken geschützten Daten und Übertragungswege sind hier besonders gefährdet. Dabei geht es natürlich auch wieder viel um zentrale Passwort- beziehungsweise Zugangs-Lösungen.

Ulrich Parthier: *Password Safe – hört sich erst einmal sicher an. Können Sie die Lösung, die sich hinter diesem Namen verbirgt, erklären?*

Sascha Martens: Password Safe ist sicher – das ist unser Fokus und wir machen bei der Sicherheit auch keine Kompromisse. Natürlich lässt sich Sicherheit nur durch diverse Mechanismen herstellen. Als Beispiel können wir einen Blick auf die Verschlüsselung oder auch Back-End-Architektur im Vergleich zu anderen Lösungen werfen: Während bei den meisten Lösungen die Datenbank verschlüsselt wird und ein Knacken dieser zum Zugriff auf alle Geheimnisse führt, ist bei uns jedes Geheimnis für sich geschützt. Zudem werden die Daten Ende-Zu-Ende-geschützt bis zur Verwendungsstelle (dem Client) übertragen. Wir vertrauen in puncto Sicherheit dabei nicht nur auf unsere Erfahrung, sondern setzen auch immer auf die Expertise externer Spezialisten.

Ulrich Parthier: *Wie kann der Anwender feststellen, ob sein Passwort sicher ist oder, noch besser, zu wie viel Prozent?*

Sascha Martens: Bei der Passwort-Sicherheit selbst gelten an sich super einfache Regeln und eigentlich kann ein Passwort gar nicht sicher genug sein! Password Safe gibt dem User dabei immer sofort Rückmeldung zu der Sicherheit des Passwortes. Zudem können wir zentrale Berichte für den User erstellen und einen CISO oder Auditor damit versorgen.

SO SCHNELL WERDEN PASSWÖRTER GEKNACKT:

FYD*8F	**ca. 5 Sekunden**
W!BCVM)5	**ca. 9 Stunden**
(UN?V*UG7P!9	**ca. 485 Jahre**

Beispielrechner mit 4 Milliarden Passwörtern pro Sekunde inklusive Wörterbuch.

BELIEBT
EINFACH EIN PAAR ZAHLEN DAHINTER SETZEN:

passwordexample1:	**23,84 %**
passwordexample2:	**6,72 %**
passwordexample3:	**3,86 %**
passwordexample4:	**3,19 %**
passwordexample5:	**3,35 %**

SICHER?

Auch können eigens Passwort-Richtlinien hinterlegt werden, um die Sicherheitsstufen zusätzlich individuell zu erhöhen.

Ulrich Parthier: *Können Sie einige Szenarien für den Unternehmenseinsatz skizzieren?*

Sascha Martens: Uns ist wichtig, dass wir nicht als die eine, wichtigste Sec-Lösung wahrgenommen werden. Vielmehr gehört Password Safe zum elementaren Baustein in einer ganzheitlichen Sec-Strategie – schließlich können wir als Experten nicht jedes Gebiet abdecken. Somit wird Password Safe als Password Management Tool entsprechend für Admins und End-Anwender und zusätzlich als Credential Provider für andere Anwendungen und zur Automatisierung notwendiger Prozesse im Hintergrund eingesetzt. Für die restlichen Themen bieten wir die perfekte Schnittstelle und können einfach an schon bestehende Systeme wie etwa Security Information Management Tools angebunden werden.

Ulrich Parthier: *Auf den Punkt gebracht bedeutet die sichere Kommunikation durch Ende-zu-Ende-Verschlüsselung (E2EE) …?*

Sascha Martens: … den durchgängigen Schutz der Daten. Es gibt einfach keine Lücke zwischen Speicher- und Verwendungsort, weshalb die Daten durchgehend geschützt sind. Erst auf dem Client wird das Geheimnis entschlüsselt und ein Angreifer hat keine Chance.

Ulrich Parthier: *Stichwort Segregation of Duties und Privileged Accounts: Wie sieht es mit der Rechtetrennung funktional und technisch aus – macht diese Trennung Sinn?*

Sascha Martens: Ja, absolut. Allerdings müssen alle Privileged Accounts besonders geschützt werden! Und aktuell werden aufgrund von Dokumentationspflicht und im Sinne der Nachvollziehbarkeit immer mehr Privileged Accounts angelegt. Mit so genannten named Accounts erhält jeder User, der einen Verwaltungsauftrag haben könnte, einen solchen Account. Damit ist immer nachvollziehbar, wer welche Änderungen durchgeführt hat. Wir können mit Sicherheitsfunktionen an vielen Stellen zurück auf generische Accounts gehen und dadurch die Angriffsfläche massiv verringern.

Ulrich Parthier: *Wie sehen diese Sicherheitsfunktionen aus? Kann man Passwörter noch besser schützen?*

Sascha Martens: Definitiv. Zum Beispiel kann ein Passwort, das von mehreren Personen genutzt werden muss, ausschließlich von einer Person verwaltet werden. Alle anderen können es wiederum nutzen, ohne es gesehen zu haben. Bei besonders sensiblen Accounts kann als zusätzliche Hürde die Genehmigung eines Verantwortlichen als erforderliche Maßnahme ergänzt werden, um ein Passwort verwenden zu können.

Ulrich Parthier: *Gibt es so etwas wie eine Historie und/oder Versionsnachverfolgung für Auditing-Zwecke?*

Sascha Martens: Alle Aktionen innerhalb von Password Safe werden im Logbuch dokumentiert. Aus diesen Informationen generieren wir aktive Benachrichtigungen und ein Admin oder Auditor kann das Nutzer-Verhalten analysieren. Die Benutzer können natürlich auch auf alle alten Versionsstände zurückgreifen. Gerade zur Umsetzung von DSGVO-Richtlinien sind diese Funktionen maßgebend.

MIT ÜBER 20 JAHREN ERFAHRUNG SIND WIR DIE EINZIGE ENTERPRISE LÖSUNG, DIE ON-PREM BEIM KUNDEN ODER IN DER CLOUD BETRIEBEN WERDEN KANN, SICH ABER AUF JEDEN FALL IMMER NACH EINER COOLEN CLOUD-LÖSUNG ANFÜHLT!

Sascha Martens,
CTO & Cybersecurity Evangelist, MATESO,
www.passwordsafe.de

Ulrich Parthier: *Welche besonderen Features unterscheiden Password Safe von anderen Produkten?*

Sascha Martens: Ich denke, dass wir uns besonders durch unsere konsequente Haltung zum Thema Sicherheit differenzieren. Mit über 20 Jahren Erfahrung sind wir die einzige Enterprise Lösung, die On-Prem beim Kunden oder in der Cloud betrieben werden kann – volle Kontrolle also – sich aber auf jeden Fall immer nach einer coolen Cloud-Lösung anfühlt!

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

THANK YOU

ANALYSE UND ÜBERWACHUNG

BERECHTIGUNGSKONTROLLE IN MICROSOFT-UMGEBUNGEN

Systemadministratoren haben zahlreiche Aufgaben zu bewältigen. Dabei ist es wichtig, die IT-Sicherheit stets im Blick zu behalten. Arbeiten sie innerhalb einer Microsoft-Umgebung, gehört dazu auch die Überwachung der Richtlinien und Benutzerkonstellationen in dem Active Directory (AD) und den NTFS-Fileserversystemen. Um auch bei großen Umgebungen nicht den Überblick zu verlieren, unterstützen geeignete Softwarelösungen bei der detaillierten Auswertung und grafischen Darstellung der Berechtigungsvergaben im Bereich AD und NTFS.

Kommt keine derartige Software zum Einsatz, müssen AD-Objekte und Fileserver-Strukturen manuell analysiert und auf Konformität geprüft werden. Dies ist äußerst aufwendig und birgt hohes Fehlerpotenzial. Damit es zu keinen falschen Benutzerkonstellationen kommt, die die IT-Sicherheit gefährden, ist daher eine softwarebasierte Auswertung der Zugriffsberechtigungen anzuraten. Bei der Auswahl einer solchen Lösung gilt es jedoch, einige Anforderungen zu beachten.

Wesentliche Features

Zunächst ist es essenziell, dass sich die Software ohne zusätzliche Dienstleistungen einfach installieren und konfigurieren lässt. Dazu sollte das Tool in der Lage sein, die Zugriffsberechtigungen der einzelnen Benutzer und Gruppen innerhalb der firmeninternen Microsoft-Infrastruktur zu identifizieren und zu erfassen. Nach der Analyse der zentralen Benutzerdatenbank (AD) sowie der Microsoft-Dateisysteme (NTFS) können die ermittelten Daten zur Visualisierung in ein leistungsfähiges Datenbanksystem importiert werden. Gleichzeitig erfolgt auf Basis von hinterlegten Policies eine automatisierte Überprüfung der Berechtigungen auf Konformität zu Best-Practice-Vorgaben. So lassen sich Abweichungen feststellen und korrigieren.

MODERNE LÖSUNGEN SOLLTEN EIN BENUTZERFREUNDLICHES WEB-DASHBOARD INTEGRIEREN, DAS INFORMATIONEN ÜBERSICHTLICH DARSTELLT.

Sebastian Spethmann,
Account Manager, G+H Systems
www.daccord.de/microsoft

Alle Infos auf einen Blick

Moderne Lösungen sollten ein benutzerfreundliches Web-Dashboard integrieren, das Informationen übersichtlich darstellt. Dabei ist eine personalisierte Sicht auf die entsprechenden Analyseinformationen und Hinweise bezüglich Abweichungen von Best-Practice-Richtlinien von Vorteil. Aus dem AD sollten beispielsweise aktive Benutzerkonten, vorhandene, geschachtelte oder leere Gruppen und Gruppenmitgliedschaften sowie deren Berechtigungsvergabe angezeigt werden. Der zusätzliche Abgleich mit einem vorhandenen Personalsystem gestattet es hierbei zu validieren, ob Mitarbeiter noch aktiv sind, um Zugriffsrechte entsprechend managen zu können, „Karteileichen" zu entfernen oder neue Berechtigungen festzulegen.

Neben den Benutzerinformationen sollten auch NTFS-Filesysteme bis auf Dateiebene visualisierbar und deren Zugriffs- und Freigabeberechtigungen sichtbar sein. Auf diese Weise lässt sich sofort erkennen, welche Shares auf welchen Servern angeboten werden und welche User beziehungsweise Gruppen darauf Zugriff haben. Greift hier ebenfalls die Auswertung gemäß Policy ein, sind etwaige Missstände sofort erkennbar.

Skalierbarkeit

Ein weiterer wichtiger Aspekt ist die Skalierbarkeit. So sollte es möglich sein, auch Systemumgebungen mit sehr großen AD- und Fileserverstrukturen zu analysieren, bei denen große Datenmengen anfallen können. Weder die Datenerhebung noch deren Abspeicherung in der benutzten Datenbank dürfen hier zu Engpässen bei der Speichergröße oder zu Performance-Problemen führen. Dazu sollte eine performante Datenbank zum Einsatz kommen, die hinsichtlich der einzulesenden Datenstrukturen und der Vergleichs- beziehungsweise Auswertungsleistung optimiert ist.

Sebastian Spethmann

RUNDUM SICHER ALS SERVICE

IDENTITY MANAGEMENT MIT LASTPASS

Durch die Vielzahl von Anwendungen und Geräten, die im gesamten Unternehmen im Einsatz sind, ist es fast unmöglich, den Überblick darüber zu behalten, wer wo und wann worauf zugreift. Ganz klar: Die neuen Strukturen, die durch „New Work" unseren Arbeitsalltag bestimmen, stellen neue Anforderungen auch an die IT-Sicherheit. Faktoren wie mobile Endgeräte, Bring-your-own-device, neue Apps und Home Office erfordern mehr Kontrolle für die IT aber gleichzeitig einfache Handhabung für die Mitarbeiter - also weitreichendere Sicherheit, ohne damit Nutzer zu frustrieren oder bei der täglichen Arbeit zu behindern. LastPass Identity ist dafür die All-in-one Lösung, die alle wichtigen Funktionen bietet:

- Identitätsmanagement
- Passwortmanagement
- Multifaktorauthentifizierung
- Single Sign On

IDaaS als Lösung

Identity-as-a-Service (IDaaS) von LastPass bietet eine Authentifizierungs-Infrastruktur, die Unternehmen als Managed Service abonnieren. Die 2019 bei den CyberSecurity Breakthrough Awards als „Overall ID Management Solution of the Year" ausgezeichnete Lösung bietet reibungslose Abläufe und eine einfache Bereitstellung durch eine zentralisierte Ansicht für Mitarbeiterzugriff und Authentifizierung. Durch die Nutzung biometrischer und kontextueller Faktoren bietet sie Mitarbeitern passwortfreies Arbeiten ohne zusätzliche Komplexität. Und: IT-Sicherheitsexperten verwalten alle Zugriffspunkte transparent in einer Lösung ohne umständliches Hin- und Herwechseln. Unternehmen integrieren die Lösung in ihre vorhandene Infrastruktur und haben sofort die Kontrolle über ihr Business. LastPass ermöglicht Unternehmen jeder Größe ein vollständiges, sicheres Identitätsmanagement aus der Cloud.

Alles, was Sie für Zugriff und Authentifizierung brauchen

Die erweiterte LastPass-Business-Suite besteht aus LastPass Enterprise, das neben der Passwortverwaltung eine Single-Sign-on-(SSO)-Lösung samt Katalog von 1.200 Anwendungen umfasst, aus der Multifaktor-Authentifizierungslösung (MFA) LastPass MFA, die biometrische und kontextuelle Authentifizierungsfaktoren nutzt, sowie aus LastPass Identity, das Passwortverwaltung, SSO und MFA in einer einzigen Lösung kombiniert. Die Business-Suite lässt sich laut Anbieter leicht in bestehende Infrastrukturen integrieren.

Ein paar Tatsachen für IT-Verantwortliche

Diese Ergebnisse aus dem LastPass Sicherheitsreport sollten IT-Verantwortliche kennen:

- Mehr als 50 Prozent der Unternehmen auf der ganzen Welt setzen bereits Multifaktor-Authentifizierung für ihre Mitarbeiter ein.
- IT-Administratoren nutzen Richtlinien (wie etwa DSGVO) als Anlass für mehr Sicherheit und optimiertes Management, es könnten insgesamt aber mehr Admins die Nutzung der Multifaktor-Authentifizierung vorschreiben.
- Die Möglichkeit Passwörter auf Mobilgeräten abzurufen, führt zu besseren Nutzer-Erfahrungen und höherer Mitarbeiternutzung.

Hier finden Sie weitere interessante Informationen zu LastPass:

www.lastpass.com

LastPass ••• | by LogMeIn

CYBERSICHERHEIT 2020

DREI KONKRETE BEDROHUNGSSZENARIEN

Jedes Jahr erstellt Cybersecurity-Hersteller Stormshield eine Analyse der Tendenzen, die sich für das angebrochene Jahr abzeichnen. Auf den Prüfstand werden selbst schwache Angriffssignale aus dem Vorjahr gestellt, die jüngsten Branchenanalysen und die Meinungen der Stormshield-Sicherheitsspezialisten. Daraus resultiert ein Ausblick für 2020 mit drei auf Industrieumgebungen zugeschnittenen Hypothesen und Szenarien, die alles andere als realitätsfremd sind.

2020 WERDEN WIR SEHR WAHRSCHEINLICH NOCH HÄUFIGER ATTACKEN AUF DIE LEBENSMITTELINDUSTRIE, SOWIE AUF DEREN ZULIEFERER ODER GAR KUNDEN VERZEICHNEN.

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

1. Die Malware von morgen ist heute bereits am Werk

„Die Cyberkriminalität wird allmählich zum Massenphänomen", so der Geschäftsführer der französischen ANSSI (wie unser BSI) in einem Interview über die Entwicklungen im Jahr 2019. Ein Jahr, in dem sowohl komplexe, gezielte und hochwirksame Cyberangriffe gegen große Fernsehsender, Krankenhäuser und Industrieanlagen kursierten, als auch für großflächigere Angriffe entwickelte Malware wie LockerGoga und Ruyk. Selbst die Folgen der manchmal von den Staaten unterstützten Cyberkriminalität wurden der Öffentlichkeit spätestens im März 2019 deutlich gemacht, als die USA einen Angriff auf ein venezolanisches Kraftwerk ausübten.

Im November 2019 wurde durch eine Studie nachgewiesen, dass gewisse Schwachstellen seit über zehn Jahren und noch heute von Cyberangreifern ausgenutzt werden. Einigen betroffenen Unternehmen sind die Sicherheitslücken in ihrem System bekannt, jedoch können oder dürfen die entsprechenden Anwendungen nicht ausgetauscht werden, wie etwa im Gesundheitswesen oder im Finanzsektor, wo Anwendungen zum Einsatz kommen, die nur auf veralteten Betriebssystemen laufen. In der Industrie werden ebenfalls gewisse Bestandteile der Hardware weiterverwendet, obwohl sie veraltet sind. Dadurch erhöht sich das Risiko, einem Angriff zum Opfer zu fallen, der schon Jahre zuvor initiiert wurde. Daher die Frage: Potenziert das Alter der Schwachstellen ihr Schadenspotenzial? 2020 dürfte uns Antworten bringen.

Mögliche Szenarien für 2020:

Wie bei latenten Viren im menschlichen Körper sind einige Angriffsvektoren bereits vor Jahren in empfindlichen Computersystemen installiert worden. Es ist daher leicht, Hypothesen aufzustellen, in denen bestimmte Schlüsselsektoren (Gesundheit, Nahrungsmittel, Energie) mit seit Jahren inaktiver Malware infiziert worden sein könnten (APT = Advanced Persistant Threats). Ebenso einfach ist es, die katastrophalen Folgen zu hypothetisieren: Was würde passieren, wenn mitten in der Nacht alle weltweit verteilten Produktionsstätten eines großen lebensmittelverarbeitenden multinationalen Unternehmens gleichzeitig gestoppt würden? Es würde Wochen dauern, das Problem zu identifizieren und lösen. Die Produktion würde eingestellt und alle verderblichen Waren weggeworfen werden. Ein katastrophales Bild in den TV-Nachrichten und der sichere finanzielle Ruin wären die Folge.

Die wahrscheinliche Quelle eines solchen Unfalls? Eine erfolgreiche Phishing-Kampagne, die Jahre zuvor durchgeführt wurde, wodurch mehrere Firmennetzwerke mit latenter Malware infiziert wurden. Diese Schadsoftware konnte sich unbemerkt lokal auf alle Endgeräte mit älteren Windows-Versionen verbreiten und wird nach Jahren per Fernzugriff aktiviert. Da sie bereits auf allen Terminals vorhanden ist, ist es nicht mal hilfreich, die Geräte im Notfall vom Netz zu trennen. Und alle sitzen vor schwarzen Bildschirmen.

2. Generalisierte Cyberangriffe auf die Agrar- und Lebensmittelindustrie

Im April 2019 wurde der französische Branchenriese Fleury Michon Opfer einer erfolgreichen Cyberattacke und musste fünf Tage lang alle Tätigkeiten einstellen. Im Dezember 2019 waren die italienische Feinkostmarke Fratelli Beretta und der belgische Bierbrauer Busch an der Reihe, als sie mit der Ransomware Maze erpresst wurden. Die Nahrungsmittelindustrie scheint mehr denn je Begehrlichkeiten von Cyberangreifern jeder Art zu wecken.

Mögliche Szenarien für 2020:
Ein hypersensibler Sektor, eine größtenteils automatisierte Produktionskette und eine Qualitätssicherung, die eine der Säulen der Branche ist: Hier sind alle Elemente vereint, die die Lebensmittelindustrie auch in den nächsten Jahren zu einer mit hohen Risiken behafteten Branche machen.

Ganz gleich, ob die Cyberangriffe von staatlich geförderten Akteuren (Reaktion auf einen offenen Konflikt) oder von Cyberterroristen (Angriff auf Bevölkerungsgruppen mit gesundheitsgefährdenden Lebensmitteln) ausgehen, 2020 werden wir sehr wahrscheinlich noch häufiger Attacken auf die Agrar- und Lebensmittelindustrie sowie auf deren Zulieferer oder gar Kunden verzeichnen.

Ein guter alter USB-Stick oder eine Phishing-Kampagne reichen, um einen Arbeitsplatz-PC zu infizieren und ins Netzwerk einzudringen. Einige der großen Konzerne haben dieses Szenario bereits in Betracht gezogen und wirksame Schutzmaßnahmen für ihre Produktionsanlagen ergriffen (zum Beispiel durch eine Segmentierung der Netzwerke). Kleine und mittlere Unternehmen dieser Branche scheinen hingegen anfälliger für diese Cyberangriffe zu sein, die hohe finanzielle Verluste und katastrophale Auswirkungen auf ihr Image zur Folge haben.

3. Deep-Fake als Brecheisen

Zahlreiche Softwarehersteller sind der Ansicht, dass 2019 der Anteil von Phishing an den meist genutzten Angriffsvektoren zunahm. Die eingesetzten Methoden entpuppten sich sogar teilweise aufgrund ihrer Komplexität zu einer echten Herausforderung, etwa mit falschen 404-Seiten oder Web-Portalen, die von Google indexiert wurden oder mit telefonisch von Geschäftsführern erteilten Aufträgen, die keine waren. Berichtet wurde sogar von Phishing-Kampagnen, die als Mitarbeiterbeurteilungsbögen getarnt waren (Quelle: Kaspersky Frankreich). Alles „Deep Fakes", eine Bedrohung, die 2019 sehr deutlich wurde.

Mögliche Szenarien für 2020:
Die Einführung des „Deep Fakes" in das Arsenal der Cyberkriminellen ist eine echte technische Herausforderung hinsichtlich Vorbeugung und Sicherheit. Es sind sogar Verbreitungsformeln wie „Deep Fake as a Service" denkbar, die eine deutliche Steigerung der Effizienz dieser Angriffsvektoren bewirken würden. Eine Bedrohung, die man durchaus ernst nehmen sollte. In seiner Studie prophezeit das Marktforschungsinstitut Forrester für das Jahr 2020 Schäden in Höhe von 250 Millionen US-Dollar aufgrund von Deep-Fake-Attacken. Dabei erweist sich die Entwicklung eines glaubwürdigen „Deep Fakes" als äußerst komplex und kostspielig. Der Kostenfaktor könnte deshalb die erwartete Explosion der „Deep Fakes as a Service" relativieren. Doch gilt dies gleichermaßen für Cyberkriminelle, die über umfangreichere Mittel als zum Beispiel ein Staat verfügen? Oder für unabhängige Spezialisten?

All dies lässt vermuten, dass 2020 das Jahr des mehrstufigen Phishings sein wird. Mit einfachen Kampagnen, die mit bereits bekannten Techniken auf die Gutgläubigkeit der Zielpersonen setzen, und komplexeren Kampagnen, die die aktuellsten Technologien nutzen, um auch erfahrene Profis hinters Licht zu führen.

Uwe Gries

Foto: 123rf.com | Olivier Le Moal

HANNOVER MESSE

DIE TRANSFORMATION IST ÜBERALL

Die industrielle Transformation ist bestimmt durch die Megathemen Digitalisierung, Individualisierung, Klimaschutz und demographischer Wandel. Darüber hinaus steht die Industrie vor großen wirtschaftspolitischen Herausforderungen wie Handelskriege, Nationalismus oder die zunehmend ungerechte Verteilung des Wohlstands. Die HANNOVER MESSE ist gerade in Zeiten des Umbruchs wichtigere denn je, denn sie ist die weltweit einzige Plattform, die die industrielle Transformation in all ihren Facetten abbildet.

Impulse

In dieser einen Woche im April 2020 geben rund 6 000 Aussteller zukunftsorientierte Impulse für eine global und digital vernetzte Industrie. Von Industrie 4.0, künstlicher Intelligenz und Robotik bis hin zu Leichtbau, Logistik und Sicherheit umfasst die Themenreihe alles, was die Industrie vorantreibt.

Beispielweise finden Besucher ein breites Angebot an Lösungen zur Sicherung der IT-Infrastruktur. Von der Absicherung sensibler Schnittstellen im Industriebereich bis hin zur Vernetzung hochkritischer Infrastrukturen, die zuverlässig verschlüsselte Datenkommunikation via Internet, Fernwartungs-Systeme sowie Remote Access-Lösungen für mobile Mitarbeiter ermöglichen.

Dabei gewinnen IT und Software für industrielle Anwendungen immer mehr an Bedeutung. Denn um eine smarte und flexible Fertigung sicherzustellen, müssen Maschinen und Systeme Daten autonom austauschen. Und das geht nur in hochdynamischen Ökosystemen, die eine vollständig individualisierte Produktion ermöglichen – Sprichwort „Business-Plattformen". Auf der HANNOVER MESSE sind die führenden Plattformanbieter vertreten, darunter Atos, Amazon Web Services, Dassault Systemes, Deutsche Telekom, IBM, Google, Huawei, Intel, Microsoft, SAP und Software AG.

Potenzial

Auch der Bereich Sensorik bietet der Industrie enormes Potenzial dank der schnellen Übertragung von Daten aus der Fabrikhalle in die Cloud. Die resultierende echtzeitige Sammlung, Verarbeitung und Analyse von solchen Daten ermöglicht gut informierte Entscheidungen seitens des Anwenders. Dabei kommt das Thema Retrofitting ins Spiel, denn mithilfe neuer Sensorik können Betreiber ihre bestehenden Industrieanlagen umrüsten und fit für die Zukunft machen. Dadurch steigt die Produktivität und Kosten sinken. Zu den Anbietern auf der HANNOVER MESSE zählen Unternehmen wie ABB, Endress+Hauser, ifm electronics, JUMO, Pepperl+Fuchs, SICK, Siemens oder Turck.

Expanded Reality findet immer häufiger im industriellen Umfeld Anwendung, beispielweise bei der Gestaltung von Triebwerken. Brauchten Ingenieure zuvor Tage, um die Parameter eines Entwurfes durchzurechnen, liefert ein Algorithmus im gleichen Zeitraum heute 2 000 Designs. Anschließend können 3D-Modelle in einem Virtual-Reality-Labor bis zur letzten Schraube auseinandergenommen, vermessen und zusammengesetzt werden.

HANNOVER MESSE

Neugierig auf mehr? Dann besuchen Sie die
HANNOVER MESSE
vom 20. bis zum 24. April 2020.
Hier geht es zum Ticketshop:
https://bit.ly/31yNr3Y

UMFASSENDE VERSCHLÜSSELUNG

E-MAIL-ANWENDUNGEN AUS DER CLOUD

Web- und Office-Programme aus der Cloud bieten Optionen, um E-Mails zu verschlüsseln. Warum sich dennoch eine zusätzliche Lösung empfiehlt, lässt sich am Beispiel von Microsoft Office 365 zeigen. Unternehmen gewinnen an Sicherheit und Nutzerfreundlichkeit, wenn sie totemomail einsetzen.

Vertraulichkeit und Integrität einer E-Mail sind schützenswert. Verschlüsselung gewährleistet beides, daher empfiehlt die DSGVO ihren Einsatz.

Grundsätzlich lassen sich der Transportweg per TLS (Transport Layer Security) und der Inhalt mit S/MIME (Secure/Multipurpose Internet Mail Extensions) oder PGP (Pretty Good Privacy) verschlüsseln. Doch wie sieht das im weitverbreiteten Microsoft Office 365 (O365) konkret aus?

Verschlüsselung in Office 365

Das Feature, das eine Nachricht in der Cloud verschlüsselt, nennt sich bei Microsoft Azure Information Protection (AIP). Die Mitteilung wird im E-Mail-Client des Absenders verschlüsselt und an den Empfänger gesendet. In Kombination mit der TLS-Verschlüsselung ergibt sich zwar ein hohes Sicherheitsniveau, allerdings hat der Cloud Provider in diesem Fall Zugriff auf die Schlüssel. Eine Alternative ist S/MIME, damit kann der Provider nicht auf das Schlüsselmaterial zugreifen. Wenn O365-Nutzer E-Mails mit einem S/MIME-Zertifikat auf ihrem Client verschlüsseln, müssen sie ihre Schlüssel jedoch selbst verwalten. Außerdem benötigt der Adressat ebenfalls S/MIME, um die verschlüsselten E-Mails lesen zu können.

Nutzerfreundliche Kommunikation

Nutzerfreundlichkeit und Sicherheit vereint erst eine zusätzliche E-Mail-Verschlüsselungslösung wie totemomail. Sicherheitsspezialist totemo bietet eine in Office 365 integrierte Verschlüsselung. Die Kommunikation innerhalb des Unternehmens wird mit S/MIME abgeschirmt. So wird Office 365 zum sicheren E-Mail-Speicher in der Cloud. Zudem erhöht totemomail die Nutzerfreundlichkeit, da es das Schlüsselmanagement übernimmt. Für die sichere Kommunikation nach außen stehen S/MIME, OpenPGP, TLS und Microsoft AIP (Azure Information Protection) zur Verfügung. Falls Empfänger diese Technologien nicht unterstützen, bietet totemo mit WebMail und Registered Envelope zwei alternative Methoden, mit denen sie verschlüsselte E-Mails lesen können, ohne über entsprechende Technik oder Know-how zu verfügen. Obwohl intern mit S/MIME verschlüsselt wird, liefert die Lösung dem Empfänger die verschlüsselte Nachricht also immer in einer für ihn passenden Form, so dass die Nutzerfreundlichkeit für Absender wie Empfänger sehr hoch ist.

Sicherer E-Mail-Speicher

totemo unterstützt auch bei der Migration von einer On-Premises-E-Mail-Infrastruktur in die Cloud. Mit seinem Verschlüsselungs- und Migrations-Tool verschlüsselt totemo bestehende Postfächer und Ordner in der On-Premises-Lösung, die meist im Klartext dort liegen. Anschließend werden diese nun verschlüsselten Nachrichten mit den Microsoft-Migrationstools nach Office 365 migriert.

Irrtümer der E-Mail-Verschlüsselung. (Quelle: totemo)

Lösung samt Tools und Optionen testen

Mit einer Testlizenz können Unternehmen die Lösung mit allen Funktionen kostenlos ausprobieren. Für den operativen Betrieb fallen Lizenzkosten pro interner E-Mail-Adresse an. totemomail lässt sich für O365 auf Wunsch bei Azure hosten und im Managed Service betreiben. Für welches Modell sich ein Unternehmen auch entscheidet, eins steht vorher fest: Die O365-Nutzer werden mit totemomail E-Mails durchgehend und nutzerfreundlich verschlüsseln, weil die Sicherheitsmaßnahmen im Hintergrund ablaufen.

Marcel Mock | www.totemo.com

totemo®
securing data in motion

DREI HERAUSFORDER

ISMS, NOTFALLPLANUNG & DATENSCHUTZ:

Die Zahl der Cyberattacken wächst seit Jahren. Unternehmen erleben immer häufiger Angriffe auf ihre IT- und OT-Infrastruktur. Ransomware-Angriffe nehmen weiter zu und verursachen Schäden in der „realen" Welt. Die Frage ist also nicht, ob es passiert, sondern wann es das eigene Unternehmen treffen wird.

Die vergangenen Monate haben zahlreiche Unternehmen wieder Opfer von geplanten und ungeplanten Cyberattacken werden lassen. Wie in diversen Medien bereits berichtet, hat es der aktuelle Trojaner unter dem Namen „Ursnif" auf Account-Daten wie Benutzernamen und Passwörter abgesehen. Die Geschäfts-E-Mails wirken dabei so echt, dass es selbst geübten Augen schwer fällt, die Fälschung zu erkennen. Die immer besser werdende Qualität solcher Spam- und Phishing-Mails stellt die Sicherheit der Unternehmen vor immer größere Herausforderungen. Mitarbeiter müssen also durch entsprechende Richtlinien für solche Gefahren sensibilisiert und im Umgang mit potenziell gefährlichen E-Mails geschult werden.

Eine weitere Gefahr: Angreifer nutzen oft Niederlassungen oder Zweigstellen größerer Unternehmen als Einfallstor. Üblicherweise ist die OT-Infrastruktur der kleineren Standorte mit dem größeren OT-Netzwerk verbunden. Bei Energieversorgern sind häufig die örtlichen Niederlassungen (Überlandwerke und Gemeindewerke) mit dem regionalen Stromnetz verbunden. Die Gefahr dabei: Ein erfolgreicher Angriff auf eine Zweigstelle oder kleinere Energieversorger wirkt wie eine Kettenreaktion und kann verehrende Folgen mit sich tragen, wie beispielsweise einen überregionalen Stromausfall.

Informationssicherheit zum Schutz der Unternehmenswerte

Behörden wie Unternehmen aller Größenordnungen profitieren von der Einführung und dem Einsatz eines ISMS. Viele Unternehmen sind für das Thema jedoch immer noch nicht bereit oder haben die Notwendigkeit der Informationssicherheit ausreichend verstanden. Tausende Euros werden in moderne Technik investiert. Eine rein technische Absicherung löst das Problem jedoch nicht. Denn die Informationssicherheit ist losgelöst von der Darstellungsform der schützenswerten Informationen: auch schriftliche Verträge, wichtige Dokumentationen oder Inhalte aus Kundengesprächen können schützenswert sein.

Oft sind sich die Mitarbeiter also dem Risiko für die IT bewusst. Anhänge von unbekannten Absendern in E-Mails werden nicht geöffnet. Auf der Dienstreise in der Bahn werden jedoch vertrauliche Dokumente gelesen, sensible Informationen auf dem Laptop angezeigt oder lautstark telefoniert. Was nützt mir also die beste Technik, wenn der Mensch, der sie bedient nicht ausreichend geschult ist, nicht genug Zeit hat oder die Zuständigkeit unklar ist. Wenn das Betreiben meines Kerngeschäfts jedoch davon abhängig ist, muss ich als Unternehmen die entsprechenden organisatorischen Maßnahmen ergreifen, damit dies gewährleistet wird.

Software-Bundle als dauerhafte Unterstützung

Ob BSI IT-Grundschutz oder DIN ISO/IEC 27001: Die Einführung eines ISMS nach nationalen oder internationalen Standards ist eine komplexe Aufgabe. Je nach Branche und Organisation müssen beim IT-Grundschutz über 1.500 Anforderungen erfüllt und bei mangelhafter Umsetzung durch geeignete Maßnahmen beseitigt werden. Bei der DIN ISO/IEC 27001 sind es im Vergleich nur etwas mehr als 100 Anforderungen. Je nach Unternehmensgröße und der Vorgehensweise bei der Einführung eines ISMS kann sich das Projekt über mehrere Jahre hinziehen. Mit einer entsprechen-

ISMS
INFORMATIONSSICHERHEIT
IT-NOTFALLPLANUNG
DATENSCHUTZ

UNGEN – EINE LÖSUNG

MIT SOFTWARE-EINSATZ ZUM ERFOLG

UNTERNEHMEN SOLLTEN SICH AUF DEN ERNSTFALL VORBEREITEN. DENN FRÜHER ODER SPÄTER KANN EINE CYBERATTACKE JEDES UNTERNEHMEN TREFFEN.

Jens Heidland, Leiter Produktion, CONTECHNET Deutschland GmbH, www.contechnet.de

den Tool-Unterstützung lässt sich der Arbeitsaufwand jedoch deutlich minimieren, sowohl bei der Einführung als auch im täglichen Betrieb. Zwar mögen die Anschaffungskosten beim Erwerb einer Softwarelösung die Management-Ebene davor zurückschrecken lassen, die Vorteile liegen jedoch auf der Hand:

Zentrale Plattform für das Managen von Informationssicherheit, Notfallplanung und Datenschutz:
Die Daten werden an einer Stelle gepflegt. Gibt es zum Beispiel Änderungen beim Personal, muss die Änderung nur einmal erfasst werden und wird überall automatisch übertragen.

Dokumentenverwaltung für Leit- und Richtlinien inklusive Vorlagensystem, Dokumentenlenkung und Freigabeverfahren:
Vorlagen für eine Informationssicherheitsleitlinie werden mit der Lösung ausgeliefert und können entsprechend angepasst werden. Leit- und Richtlinien können direkt in der Lösung erstellt und über das Freigabeverfahren den entsprechenden Verantwortlichen zur Verfügung gestellt werden. Wenn der Revisionszeitraum abgelaufen ist, werden automatisch der Autor sowie die freigebenden Personen benachrichtigt. Diese können dann entweder das Dokument anpassen oder direkt eine erneute Freigabe anstoßen.

Umfassendes und integriertes Risikomanagement:
Unternehmenswerte wie Informationen, Prozesse, Personal oder Infrastruktur, die jeweils dem gleichen Risiko zugeordnet sind, lassen sich in Gruppen zusammenfassen. Eine Risikoanalyse findet damit pro Gruppe statt und minimiert die Analysemaßnahmen. Wiederkehrende Behandlungsprozesse zur Risikoakzeptanz, Risikominimierung und Risikovermeidung können effizient über das Aufgabemanagement verwaltet werden. Die erstellten Maßnahmen zur Risikobehandlung werden über das Aufgabenmanagement gesteuert. Die Risikomatrix ist dynamisch. Organisationen können die Risikomethode im System auf ihre individuellen Bedürfnisse anpassen.

Intelligentes Auditmanagement vollständig integriert:
Ein integriertes Modul macht eine ganzheitliche Abwicklung von Audits mit übersichtlicher und benutzerfreundlicher Darstellung sowie einer automatisierten Berichtserstellung möglich. Ein standardisiert durchgeführter Auditprozess vereinfacht die Planung, Durchführung, Bewertung und Anpassung von Auditprogrammen und ermöglicht eine ordnungsgemäße Dokumentation. Die erkannten Abweichungen werden in die Risikoanalyse übertragen und können dort durch den Verantwortlichen bewertet und durch entsprechende Maßnahmen korrigiert werden.

Aufgabenverwaltung mit Mailing-Funktion:
Die angelegten Aufgaben und Maßnahmen werden übersichtlich in einem Kalender verwaltet und gesteuert. Dafür kann nach unterschiedlichen Kriterien gefiltert und der Bearbeitungsfortschritt der Aufgaben eingesehen werden.

Fazit
Unternehmen sollten sich auf den Ernstfall vorbereiten. Denn früher oder später kann eine Cyberattacke jedes Unternehmen treffen. Mit dem Einsatz einer ISMS-Lösung sparen Unternehmen Geld, Zeit und vor allem Nerven. Mit einer solchen Lösung erhält der Anwender ein zielorientiertes Werkzeug, das ihn in die Lage versetzt, selbst die Einführung und die Pflege eines ISMS in die Hand zu nehmen. Dokumentenvorlagen ersparen Arbeit und Hilfestellungen machen die komplizierten Normtexte verständlich. So können Verantwortlichkeiten übersichtlich festgelegt, Infrastrukturen einfach verknüpft und Risiken schnell identifiziert sowie minimiert werden. Mitarbeiter werden im Arbeitsalltag unterstützt und auch im Ernstfall ist das Unternehmen weiter handlungsfähig.

Eines der wesentlichen Mehrwerte ist jedoch, dass eine solche Softwarelösung nach der Implementierungsphase die tägliche Arbeit erleichtert. Damit ist die Organisation in der Lage, ein ISMS nicht nur einzuführen, sondern den gesamten Managementprozess lückenlos zu leben – denn darauf kommt es an!

Jens Heidland

PRIVILEGED ACCESS MANAGEMENT

ZUKUNFTSSICHERE INVESTITION IN NEUE TECHNOLOGIEN

CyberArk präsentiert eine Blaupause für ein erfolgreiches Privileged Access Management. Sie soll Unternehmen dabei helfen, einen zukunftssicheren, mehrstufigen Ansatz zur Verringerung der Risiken im Zusammenhang mit privilegierten Rechten zu verfolgen.

Die Erfahrungen der CyberArk Labs sowie aus Red-Team- und Incident-Response-Projekten von CyberArk zeigen eindeutig, dass fast jeder zielgerichtete Cyber-Angriff einem ähnlichen Muster folgt: der missbräuchlichen Nutzung privilegierter Zugangsdaten. Auf dieser Erkenntnis basieren die drei Leitprinzipien der neuen Blaupause: Unterbindung des Diebstahls von Zugangsdaten, Verhinderung von seitlichen und vertikalen Bewegungen des Angreifers im Netzwerk sowie Begrenzung von Privilegienvergabe und -missbrauch.

Die Blaupause verfolgt einen einfachen, präskriptiven Ansatz, um das Risiko eines Diebstahls und Missbrauchs von privilegierten Zugriffsrechten zu reduzieren. Dabei werden gleichermaßen interne und externe Angriffswege bedacht. Unternehmen, die die Cloud, SaaS, DevOps oder RPA nutzen, können mit den CyberArk-Empfehlungen Quick Wins realisieren, sukzessive weitere Anwendungsfälle adressieren und ihre Sicherheitsmaßnahmen bei Projekten der Digitalen Transformation kontinuierlich anpassen.

Zentrale Komponenten

Verhinderung des Diebstahls privilegierter Zugangsdaten: Zur Beseitigung interner und externer Risiken müssen Unternehmen in einem ersten Schritt den Diebstahl kritischer Credentials unterbinden; dazu gehören die Daten von IaaS-Administratoren, Domain-Administratoren oder API-Schlüsseln, die ein Angreifer für eine Ausbreitung im Netzwerk oder die Kompromittierung zentraler Infrastruktur-Accounts nutzen kann. Durch das Entfernen von hartkodierten Credentials, die Implementierung von Session-Isolierung und eine Lösung zur Diebstahlserkennung können Unternehmen privilegierte Zugriffe sowohl durch Personen als auch durch Applikationen sowie in CI/CD-Pipelines schützen.

Unterbindung von seitlichen und vertikalen Bewegungen des Angreifers im Netz: Um einen Zugriff von nicht vertrauenswürdigen Personen oder Geräten auf unternehmenskritische Cloud-Konsolen oder Domain-Controller zu verhindern, sollten im Privileged Access Management Just-in-Time-Methoden genutzt werden – mit einer temporären, bedarfsabhängigen Vergabe von privilegierten Zugriffsrechten.

Begrenzung von Privilegienvergabe und -missbrauch: Um Angreifer am Missbrauch von Privilegien zu hindern und die Angriffsfläche insgesamt zu verkleinern, müssen strikte Least-Privilege-Prinzipien gelten; Verhaltensanalysen können darüber hinaus auf Missbrauchsgefahren hinweisen.

Die Blaupause von CyberArk beinhaltet Templates und Roadmaps, mit denen Unternehmen jeder Größe in reglementierten oder nicht reglementierten Branchen die privilegierten Zugangskontrollen und die Privileged-Access-Management-Strategie nach und nach aufbauen und erweitern können.

UNABHÄNGIG VOM REIFEGRAD DES PRIVILEGED-ACCESS-MANAGEMENTS EINES UNTERNEHMENS ERMÖGLICHT DIE BLAUPAUSE EINE ZUKUNFTSSICHERE INVESTITION IN NEUE TECHNOLOGIEN.

Michaeö Kleist, Regional Director DACH, CyberArk, www.cyberark.com

Fazit

„Die einfache, aber gleichzeitig umfassende Blaupause bietet eine herstellerneutrale Anleitung, die Privileged-Access-Management-Initiativen eng mit einer Risikoreduzierung verzahnt und Unternehmen damit hilft, ihre größten Sicherheitsprobleme so schnell wie möglich zu lösen“, betont Michael Kleist, Regional Director DACH bei CyberArk. „Unabhängig vom Reifegrad des Privileged-Access-Managements eines Unternehmens ermöglicht die Blaupause eine zukunftssichere Investition in neue Technologien. Das Ergebnis ist eine kurz- und langfristige Verbesserung der Sicherheit, eine Verringerung der Angriffsfläche und eine Optimierung der betrieblichen Effizienz.“

www.cyberark.com/Blueprint

ALLES AUS EINER HAND

GANZHEITLICHES KONZEPT FÜR MEHR SICHERHEIT

Heutzutage stellt sich längst nicht mehr die Frage, ob, sondern wann ein Unternehmen Opfer eines Cyber-Angriffs wird. Das gilt für große Konzerne genauso wie für kleine und mittelständische Unternehmen, die meist über keine allzu hohen Sicherheitsstandards verfügen. Eines der jüngsten Opfer ist der belgische Webmaschinenhersteller Picanol: Dessen gesamte Produktion wurde aufgrund eines Ransomware-Angriffs lahmgelegt und die Cyber-Kriminellen stellten hohe Lösegeldforderungen, um die Daten wieder freizugeben.

Damit Unternehmen wie diese sich vor solchen Angriffen besser schützen beziehungsweise darauf reagieren können, sollte es trotz aller Vorkehrungen dazu kommen, hat Konica Minolta mit seinem 360-Grad-Sicherheitskonzept ein ganzheitliches Schutzkonzept entwickelt.

Die Cyber-Gefahren sind vielfältig: Angreifer nutzen neben Ransomware zunehmend intelligente Schadsoftware. Auch intern lauern Bedrohungen: Nicht selten sind es eigene Mitarbeiter, die meist unbewusst Einfallstor für Attacken sind oder wertvolle Informationen stehlen. Gleichzeitig sorgen die EU-DSGVO oder andere Compliance-Vorschriften für steigende Anforderungen an den Informationsschutz. Um einen angemessenen und passenden Schutzgrad der Informationen zu erzielen, ist eine strategische Herangehensweise in punkto Sicherheit notwendig, die Prozesse, Menschen und Technologien berücksichtigt.

Alle Sicherheitsaspekte im Blick

Konica Minolta hat sein 360-Grad-Sicherheitskonzept gezielt darauf ausgerichtet, sensible Bereiche zu schützen. Dazu gehören neben der IT-Infrastruktur mit zum Beispiel dem Netzwerk, Servern und Endgeräten, auch die angebundenen Multifunktionssysteme sowie die Videoabsicherung als auch die Mitarbeiter. Auf Basis des 360-Grad-Ansatzes wird zuerst eine Ist-Analyse durchgeführt und im Anschluss mit dem Kunden der Soll-Zustand definiert. Es folgen ein Maßnahmenkatalog und die Umsetzung einzelner Schritte. Neben der Definition einer Sicherheitsstrategie, der Implementierung von technischen und organisatorischen Maßnahmen, ist es im Zuge des Risikomanagements äußerst wichtig, die IT auf Schwachstellen zu untersuchen und diese vor allem zu verifizieren. Dies geschieht unter anderem mit Hilfe von Penetrationstests, die sowohl intern als auch extern von Konica Minolta durchgeführt werden. Da innerhalb einer Organisation stetig Veränderungen stattfinden, sollte dieser Prozess kontinuierlich wiederholt werden. Darüber hinaus finden professionelle Schulungen aller Mitarbeiter statt, damit diese verstehen, dass Informationssicherheit insbesondere in Zeiten des rasant wachsenden Datenvolumens und der steigenden Risiken ein zentraler Erfolgsfaktor ist. Dazu müssen Mitarbeiter alle Informationsstandards kennen und wissen, was bei einem sicherheitskritischen Vorfall zu tun ist.

Mit dem 360-Grad-Konzept von Konica Minolta erhalten Unternehmen alles aus einer Hand und profitieren von Ressourcen- und Kosteneinsparungen.

www.konicaminolta.de

KONICA MINOLTA

IAM CONNECT 2020

Die Brücke zu neuen Geschäftsmodellen

Die IAM CONNECT, die größte deutschsprachige Konferenz zum Thema Identity & Access Management, bietet Ihnen auch 2020 wieder ein praxisnahes Programm: IAM-Verantwortliche großer Unternehmen teilen ihre Erfahrungen mit Ihnen. In Speed Demo Sessions präsentieren Hersteller anhand von Business Cases ihre IAM-Lösungen.

Freuen Sie sich auf konstruktive Gespräche mit Kollegen auf hohem fachlichen Niveau.

Konferenz
16. bis 18. März 2020
in Berlin

Programm und Anmeldung unter
www.iamconnect.de

Hauptsponsor

ipg
EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Speed Demo Sessions

AIRLOCK® SECURE ACCESS HUB
Auth0
COGNITUM Software
IT CONCEPTS
_betasystems

Eine Veranstaltung von itmanagement & itsecurity

Highlights aus der Agenda

Vorträge

Wie alles begann

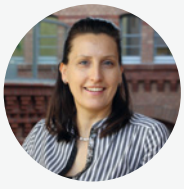
Prof. Dr.-Ing. habil. Horst Zuse ist der Sohn des Erfinders des Computers Konrad Zuse. Er berichtet von den frühesten Entwicklungen.

Einführung einer 2Faktor-Authentifizierung mit Hilfe eines Secure Access Hubs

Jörg Hartmann,
Johanniter-Unfall-Hilfe e.V.

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

Orchestrierung von IAM-Kontrollen und Bereinigungen

Thilo Richter,
KfW Bankengruppe

Workshops

Minimaler Aufwand, maximale Sicherheit: Dos and Don'ts für erfolgreiches 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

DIERICHSWEILER
Unternehmens- und Prozessberatung

NEXIS

Ping Identity.

Telia

ONE IDENTITY

IMMER ÄRGER MIT DEM

ZERO TRUST IST DIE NÄCHSTE STUFE

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist jetzt von seiner Empfehlung ab, Passwörter regelmäßig zu ändern. In der aktuellen Ausgabe des BSI-Grundschutz-Kompendiums wurde die entsprechende Textpassage gestrichen. Unter anderem hatte Heise Security über die Änderung berichtet.

Die BSI-Experten raten nun im Kapitel zur Regelung des Passwortgebrauchs nur für den Fall, dass ein Passwort in fremde Hände geraten sein könnte, das Kennwort zu ändern. Auch die dort bisher aufgeführte Verpflichtung, feste Regeln für Länge und Komplexität vorzuschreiben, ist verschwunden.

Bereits seit Jahren sind viele Sicherheitsexperten der Ansicht dass solche Regeln eher schaden als nützen. „Ein gutes Passwort kann man bedenkenlos über Jahre hinweg nutzen", schreibt etwa Heise Security. „Das regelmäßige Ändern führt eher dazu, dass man schwache Passwörter benutzt und diese beispielsweise nach einem Schema (geheim1, geheim2, ...) erzeugt."

Der Password Day

Anlässlich des „Change Your Password Days" am Samstag, dem 1. Februar, erinnerte das Hasso-Plattner-Institut (HPI) an die wichtigsten Regeln zur Erstellung starker Passwörter.

„Schwache Zahlenreihen wie etwa „123456" werden weltweit weiterhin viel zu häufig genutzt", kritisiert HPI-Direktor, Professor Christoph Meinel. „Viele Internetnutzer verwalten bereits mehr als hundert Online-Konten - da fällt die Wahl viel zu oft auf Passwörter, die man sich leicht merken kann", sagt Meinel. Auch die weit verbreitete Mehrfachnutzung von Passwörtern für unterschiedliche Dienste sei extrem leichtsinnig, wenn man bedenke, welche Schäden hierdurch entstehen könnten.

Die wichtigsten Regeln zur Erstellung starker Passwörter:

- Die Länge des Passworts sollte mindestens 15 Zeichen umfassen.
- Das Passwort sollte möglichst viele verschiedene Zeichentypen (Buchstaben, Ziffern, Sonderzeichen) sowie Groß- und Kleinschreibung mit einbeziehen.
- Keine Begriffe aus dem Wörterbuch oder andere „sinnvolle" Zeichenfolgen verwenden. Neben den Brute-Force-Attacken sind vor allem „Wörterbuchangriffe" üblich, um Passwörter zu knacken: Hierbei werden Listen mit Wörtern genutzt, um fremde Passwörter zu entschlüsseln.
- Nie dasselbe Passwort für mehrere Konten verwenden. Wird ein Passwort geknackt, ermöglicht es Kriminellen sonst den Zugang zu allen anderen Diensten.
- Niemals persönliche Informationen wie Namen, Geburtsdaten, Haustiernamen, Namen der Partner oder der jeweiligen Anwendung (zum Beispiel „Adobe") verwenden. Diese Daten könnten leicht erraten werden.

ZERO TRUST PRINZIPIEN

1. Erfordert sicheren und authentifizierten Zugang zu allen Ressourcen

2. Adaptierung eines Modells mit den geringsten Privilegien und Durchsetzung der Zugriffskontrolle

3. Überprüfen und protokollieren Sie alle Aktivitäten mit Hilfe von Datensicherheitsanalysen

(Quelle: varonis.com/blog/what-is-zero-trust/)

PASSWORT

- Wenn möglich, die 2-Faktor-Authentifizierung nutzen.
- Passwortmanager helfen bei der Generierung und der sicheren Aufbewahrung starker Passwörter

Ob man selbst Opfer eines Datendiebstahls geworden ist, lässt sich mit dem Identity Leak Checker, einem Online-Sicherheitscheck des Hasso-Plattner-Instituts (HPI), sehr leicht überprüfen. Seit 2014 kann dort jeder Internetnutzer unter https://sec.hpi.de/ilc kostenlos durch Eingabe seiner E-Mail-Adresse prüfen lassen, ob Identitätsdaten von ihm frei im Internet kursieren und missbraucht werden könnten. Die Sicherheitsforscher ermöglichen den Abgleich mit mittlerweile mehr als 10 Milliarden gestohlener und im Internet verfügbarer Identitätsdaten. Dabei liegt der Fokus auf Leaks, bei denen deutsche Nutzer betroffen sind.

Authentifizierung-Methoden

Für Cybersecurity-Experte Marco Föllmer von der EBF GmbH sind Authentifizierung-Methoden, die über Passwörter hinausgehen, ein probates Schutzmittel. Denn einfache Passwortkombinationen, die Nutzer bei verschiedenen Anwendungsdiensten verwenden, sind ein enormes Sicherheitsrisiko für Unternehmen. Doch selbst sehr komplexe Passwörter können ins Visier von Hackern geraten und von ihnen geknackt werden. Als deutlich sicherer gilt die Zwei-Faktor-Authentifizierung (2FA), die bereits in vielen Unternehmen genutzt wird, um Daten abzusichern.

Im Vergleich zur simplen Passworteingabe ist die Zwei-Faktor-Authentifizierung zwar einerseits sicherer, aber andererseits ist sie für Nutzer auch zeitintensiver und aufwändiger. Mitarbeiter empfinden sie daher als wenig nutzerfreundlich. Aus diesem Grund arbeiten immer mehr IT-Experten aktuell an Verfahren, die eine Passworteingabe nicht immer erforderlich machen. Damit dies gelingt, setzen sie auf das „Zero-Trust" Konzept.

Zero Trust – vertraue niemanden

Der Kern des Zero-Trust-Ansatzes lässt sich durch die direkte Übersetzung verstehen: kein Vertrauen. Dabei wird bewusst nicht zwischen internen und externen Quellen unterschieden – jeder Zugriff auf Anwendungen und Unternehmensdaten wird zunächst als nicht vertrauenswürdig eingestuft. Egal, von welchem Gerät, welchem Nutzer oder welcher App: Jeder Zugriff muss explizit autorisiert werden.

Dies ist ein sehr komplexer Ansatz und stellt ein Novum im Vergleich zu bisherigen Handlungsweisen dar. Aber in Zeiten, in denen Qualität und Quantität von Cyberangriffen stetig zunehmen, ist es ein wirkungsvoller Weg, potentielle Einfallstore abzusichern.

Intelligente Richtlinien

Voraussetzung zur Anwendung des Zero-Trust-Prinzips ist es, im Vorfeld Richtlinien zu definieren. Diese legen fest, in welchem Fall ein Nutzer den angeforderten Zugriff ohne zusätzliche Authentifizierungsschritte erhält und in welchem Fall weitere Schritte zur Feststellung der Identität notwendig sind. Dabei existieren verschiedene Authentifizierungsfaktoren, welche zur Bewertung der Zugriffsanfrage abgefragt werden.

VORAUSSETZUNG ZUR ANWENDUNG DES ZERO-TRUST-PRINZIPS IST ES, IM VORFELD RICHTLINIEN ZU DEFINIEREN.

Ulrich Parthier,
Herausgeber it security,
www.it-daily.net

Die verwendeten Geräte spielen dabei eine zentrale Rolle. Handelt es sich um ein von der IT verwaltetes Gerät, so können in der Regel geringere Hürden in Sachen Authentifizierung gelten. Wird das Gerät nicht gemanagt, ist das Misstrauen höher.

Auch die Nutzer selbst werden als Faktor herangezogen: Ist ein Nutzer beispielsweise im Active Directory hinterlegt, genießt er mehr Vertrauen als ein unbekannter Nutzer. Einen weiteren Faktor stellen einzelne Anwendungsdienste und deren Herkunft dar: Stammt eine Anwendung aus dem Firmen-App-Store, dessen Sicherheit von der Unternehmens-IT kontinuierlich geprüft wird? Oder wurde die App aus dem App-Store des Geräteherstellers heruntergeladen?

Bei Letzterem besteht ein erhöhtes Sicherheitsrisiko, weshalb eine zusätzliche Authentifizierung sinnvoll sein kann beziehungsweise notwendig ist. Auch Zertifikate, die an mobile Endgeräte verteilt werden können und eine einzigartige Identität in Form eines Schlüssels ausdrücken, können bei den Richtlinien eine Rolle spielen.

Neuere Ansätze gehen sogar soweit, die Nutzungsgewohnheiten der Mitarbeiter zur Authentifizierung heranzuziehen. Deep Learning macht es möglich, diese genauer kennenzulernen und beispielsweise zu erkennen, wie schnell ein Nutzer tippt oder mit wie viel Druck er auf das Smartphone-Display drückt. Bei ungewöhnlichen Vorgängen kann der Zugriff dann verweigert werden.

Mehr Nutzerfreundlichkeit

Die definierten Richtlinien lassen sich mithilfe eines Unified Endpoint Management Systems (UEM) in die Praxis umsetzen. Sie dienen der Verwaltung von Endgeräten wie Handys und Laptops und machen es möglich, Richtlinien für diese Geräte zu definieren, die dem Zero-Trust-Prinzip folgen. Das UEM überprüft die verschiedenen definierten Faktoren und erkennt, ob sich das Gerät in einer sicheren Situation befindet oder ob es Anomalien gibt. Je nach Ausprägung der verschiedenen Faktoren werden sukzessive stärkere Authentifizierungsschritte eingefordert.

So gelingt es, dass der Arbeitsalltag im Normalfall für den Mitarbeiter deutlich nutzerfreundlicher wird. Denn es ist sogar möglich, dass in Situationen, die das UEM als gänzlich sicher einstuft, gar keine Passworteingabe mehr erforderlich ist. Dies ist zum Beispiel dann der Fall, wenn ein Nutzer, der im Active Directory hinterlegt ist, ein von der IT verwaltetes Gerät benutzt, um auf eine gemanagte App zuzugreifen – und – wichtigste Voraussetzung – wenn dieses Gerät über ein Zertifikat verfügt, das auf sicherem Wege verteilt wurde.

Die konsequente Umsetzung des Zero-Trust-Modells, so Föllmer, bietet Unternehmen die Möglichkeit, für Sicherheit und gleichzeitig hohe Nutzerfreundlichkeit zu sorgen.

Fazit

Unternehmen können so einerseits ihre Daten gegen alle Angriffe – ob von außen oder innen – absichern und andererseits den Mitarbeitern einen effektiven Arbeitsalltag ermöglichen.

Ulrich Parthier

WIE MAN ZERO TRUST IMPLEMENTIERT:

1. **Sensible Daten identifizieren**
2. **Zugang beschränken**
3. **Bedrohungen erkennen**
4. **Eine Baseline verwenden**
5. **Analytik einsetzen**

(Quelle: varonis.com/blog/what-is-zero-trust/)

ZERO TRUST

SICHERE NETZWERKUMGEBUNG IN ZEITEN DES DIGITALEN WANDELS

Unternehmen unterliegen aufgrund der digitalen Transformationen großen Veränderungsprozessen. Dieser Wandel hängt selbst in großem Maße mit den Möglichkeiten der Cloud zusammen, die Grenzen in Unternehmen zwischen intern und extern verschwimmen lässt: Arbeiten von überall und der Zugriff aufs Unternehmensnetz von außerhalb ist zum Standard geworden. Für die IT-Security ist diese Entwicklung eine große Herausforderung, der ein Zero-Trust-Sicherheitskonzept Abhilfe bietet.

Traditionelle Sicherheitsstrategien funktionieren nicht mehr

Der traditionelle Sicherheitsansatz kann diese Probleme nicht lösen. Er besteht aus mehreren Verteidigungslinien („Perimeter Security") und der Prämisse, dass alles, was sich innerhalb der Unternehmensmauern befindet, vertrauenswürdig ist. Doch Studien wie der 2019 Data Breach Investigations Report von Verizon zeigen: Mitarbeiter verursachen intern die größten Schäden. Deren Arbeitsplätze sind dank der WLAN-Omnipräsenz inzwischen überall. Darum gehen die Unternehmensanwendungen auch nach draußen und stehen beispielsweise über Amazon Web Services (AWS), Microsoft Azure oder Google Cloud Platform (GCP) bereit.

Im digitalen Ökosystem eines Unternehmens tummeln sich viele Player und Komponenten:

- Mitarbeiter, die mit dem eigenen Gerät auf Firmeninhalte zugreifen wollen,
- Drittanbieter, die Zugang zu Ressourcen der Firma benötigen,
- neue Anwendungen, in der Cloud,
- neue APIs, auf die von extern über diverse Devices zugegriffen wird.

Diese sich verändernden Ökosysteme treffen auf viele Cyber-Gefahren:

- Malware, Phishing & Datenexfiltration
- Identitätsdiebstahl,
- schwache Single-Faktor-Authentifizierung,
- Ausnutzung von Architektur-Schwachstellen.

Zero Trust-Strategie löst viele Probleme

Für diese Herausforderungen ist die Implementierung einer Zero Trust-Strategie die richtige Antwort. Ihre Devise lautet: Es wird niemandem vertraut, egal ob innerhalb oder außerhalb des Netzwerkes. Zuerst muss der gesamte Traffic rund um die Uhr überwacht und der Zugriff auf jegliche Applikation von einem zentralen Management System explizit erlaubt werden. Im zweiten Schritt wird das klassische Netzwerk-Design basierend auf DMZ in einen „Isolated Services"-Ansatz überführt. Die Applikation ist dann komplett vom Internet isoliert – über einen sogenannten Identity Aware Proxy, der in der Cloud zur Verfügung steht.

Ein cloudbasierter sicherer Applikationszugriff hat viele Vorteile:

- Nur im Verzeichnisdienst autorisierte Personen haben nach der Authentifizierung sicheren Zugriff auf vordefinierte Applikationen,
- Single-Sign-On und Multi-Faktor-Authentifizierung sind Teil der Lösung,
- alle Vorgänge im Unternehmensnetzwerk sind durchgängig protokolliert,
- es ist keine weitere Hardware notwendig,
- der Zugriff auf On-Premise- und Cloud-Applikationen ist sicher.

Angreifer halten sich also nicht mehr unentdeckt im Firmennetzwerk auf. Auch ist die Bereitstellung der Zero Trust-Schutzmechanismen aus der Cloud weit weniger komplex und wartungsintensiv als VPN-Technologie. Und schließlich spart das Unternehmen Kosten, da die Investitionsausgaben (Kapitalaufwand für Sicherheit wie VPN-Hardware und -Software) und die laufenden Betriebskosten für die Security geringer sind.

Elmar Witte | www.akamai.com

VERSTECKTE BEDROHUNGEN AUFSPÜREN

SICHERHEITSRISIKEN SYSTEMATISCH ERKENNEN

Das größte Sicherheitsrisiko für Unternehmen sind Angreifer, die unter dem Radar bleiben und so ungestört ihre Ziele erreichen können. Leider werden böswillige Insider und externe Cyberkriminelle immer cleverer, können oft in Systeme eindringen und Sicherheitstools überwinden, ohne Warnmeldungen auszulösen.

Wie können also Unternehmen diese Aktivitäten im Rauschen der legitimen Anmeldungen erkennen? Die Antwort liegt im Kontext. Es reicht eben nicht aus, die Aktivitäten im gesamten Netzwerk zu überwachen und zu protokollieren, vielmehr müssen die Sicherheitsverantwortlichen in der Lage sein, mehrere Datenquellen zu kombinieren, um auch die subtilen Anzeichen eines heimlichen Angreifers bei der Arbeit zu erkennen.

DER WICHTIGSTE FAKTOR IN DER RISIKOERKENNUNG IST DIE ENTWICKLUNG EINES UMFASSENDEN VERSTÄNDNISSES DER MITARBEITER, PROZESSE UND TECHNOLOGIEN DES UNTERNEHMENS.

Klaus Nemelka, Technical Evangelist, Varonis Systems (Deutschland) GmbH, www.varonis.com/de

Such mich doch!

Der Grund, weshalb es so sehr auf den jeweiligen Kontext ankommt, liegt darin, dass diese fortgeschrittenen Angreifer verschiedene Tools und Taktiken verwenden, um die eingesetzten Sicherheitsmaßnahmen zu umgehen. So nutzen sie für ihre Kommunikation häufig HTTPS und DNS, wodurch sich diese gut verschleiern lässt. Ein durchschnittlicher Benutzer erzeugt pro Tag bis zu 20.000 DNS-Abfragen. Diese enorme Menge an Daten ist kaum zu analysieren, insbesondere wenn die Kommunikation selbst keinen offensichtlich bösartigen Inhalt hat.

Ohne den entsprechenden Kontext, also weitere Anzeichen, die einen Administrator stutzig machen sollten, wäre er sehr lange damit beschäftigt, Protokolle durchzugehen, um so herauszufinden, ob ein Alarm eine echte Bedrohung oder nur ein Fehlalarm ist. Darüber hinaus werden Aktivitäten wie das Einloggen in ein gültiges Gerät während der Geschäftszeiten, die Konzentration auf Daten in Mailboxen und das Extrahieren von nur wenigen Daten auf einmal, wenig Aufmerksamkeit erregen. Auch das Erstellen von Schattenkonten mit mehr Rechten und das Erteilen und Entfernen von Berechtigungen je nach Bedarf sind gute Möglichkeiten für Angreifer, sich unauffällig zu verhalten.

Ich finde Dich!

Wie kommt man nun diesen Akteuren trotzdem auf die Spur? Selbst die erfahrensten und akribischsten Eindringlinge können ihre Präsenz in einem Netzwerk nicht vollständig verdecken. Der wichtigste Faktor bei der Erkennung ist die Entwicklung eines umfassenden Verständnisses der Mitarbeiter, Prozesse und Technologien des Unternehmens.

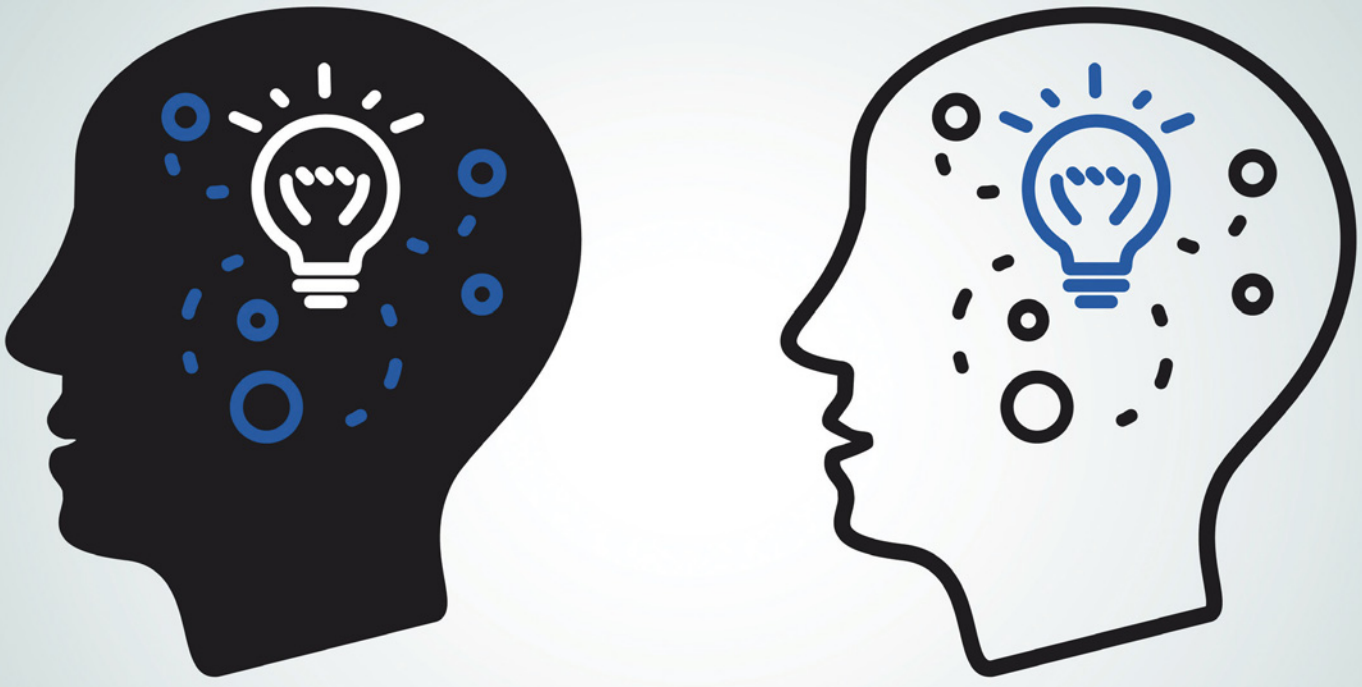
Die wichtigsten Maßnahmen zur Erkennung dieser Bedrohungen sind:

Identifizierung sensibler Daten und Dateizugriffe

Der erste Schritt besteht darin, herauszufinden, wo sich die sensiblen Daten eines Unternehmens überhaupt befinden. Dabei sollten personenbezogene Daten (PII) und andere Daten, die den gesetzlichen Anforderungen unterliegen, priorisiert und Datenverantwortliche und die Konten, auf die sie zugreifen können, festgelegt werden. Um Bedrohungsvektoren zu reduzieren, ist es angeraten, sämtliche nicht mehr aktiv genutzten Daten zu archivieren.

Verwaltung von Benutzerberechtigungen

Sicherheitsverantwortliche sollten über eine umfassende Transparenz über alle Konten verfügen, sowohl von „normalen" Nutzern als auch von Service- und privilegierte Konten – inklusive der Berechtigungen, über die sie verfügen. Vor allem die Überwachung von Berechtigungsänderungen ist bei der Identifizierung von Bedrohungen von großer Bedeutung, da beispielsweise eine Eskalation der Zugriffsrechte auf verdächtiges Verhalten hinweisen kann. Grundsätzlich sollte ein least-privilege-Ansatz durchgesetzt werden. Dadurch wird sicherge-



stellt, dass jeder Mitarbeiter nur auf die Dateien zugreifen kann, die er auch tatsächlich für seine Arbeit benötigt (need-to-know-Prinzip).

Überwachung von Schlüsselsystemen

Es ist wichtig, einen Überblick gerade über die Systeme zu haben, die bei Angreifern besonders beliebt sind und von ihnen entsprechend ausgenutzt werden. Bei Windows Active Directory zum Beispiel sollte das Unternehmen Informationen wie Kontotypen und Servertypen, Berechtigungen, Gruppen, Kollegen und den Unterschied zwischen persönlichen Geräten und öffentlichen Arbeitsplätzen kennen.

Nutzerverhalten kennenlernen

Die Kombination der Benutzeraktivitäten mit bestimmten Geräten hilft, sogar subtile Anzeichen dafür zu erkennen, dass sich ein Angreifer bei verschiedenen Maschinen anmeldet, selbst wenn er nichts offensichtliches Bösartiges tut. Kennt man den Unterschied zwischen der Verwendung öffentlicher und persönlicher Geräte, lassen sich Lärm und Fehlalarme deutlich reduzieren.

Korrelationen machen den Unterschied

Der wichtigste Schritt ist die Korrelation all dieser Daten. Jeder einzelne Punkt ist wichtig, kann aber immer nur einen kleinen Bereich beleuchten. Die Anzeichen eines fortgeschrittenen Angreifers sind jedoch oft zu subtil und können kaum identifiziert werden, wenn einzelne Informationen isoliert betrachtet werden. Nur durch ganzheitliche Sicht wird in diesen Fällen verdächtiges Verhalten erkennbar. In Anbetracht der riesigen Datenmengen, die jeden Tag durch ein Unternehmen fließen, kann dies jedoch nur mit einem automatisierten Ansatz auf der Grundlage von maschinellem Lernen erreicht werden.

Diese umfassende Transparenz über alle Netzwerkaktivitäten gepaart mit der Kenntnis, welches Verhalten „normal" ist, ermöglicht es Unternehmen, Korrelationen herzustellen, die in der Lage sind, auch schwer fassbare Anzeichen bösartiger Aktivitäten zu identifizieren. Wenn ein Benutzer beispielsweise auf ein VPN zugreift und sich dann auf dem Gerät eines anderen Mitarbeiters anmeldet, wird kein Standard-Sicherheitssystem ausgelöst. Aber ein solches Verhalten wäre für einen legitimen Benutzer sehr ungewöhnlich und ist ein klares Zeichen dafür, dass jemand die Zugangsdaten des legitimen Nutzers missbraucht.

Verhaltensanalysen

Mit ausreichendem Datenmaterial können Unternehmen über die Analyse einzelner Benutzer hinausgehen und Peer-Beziehungen in ihre Verhaltensanalyse einbeziehen. Dies ermöglicht es ihnen, einen Benutzer schnell zu erkennen, der im Vergleich zu seinen Kollegen ungewöhnliche Dateiaktivitäten aufweist, was die Reaktionszeiten bei Vorfällen erheblich verkürzt. Sobald Unternehmen diese Zeichen zuverlässig erkennen können, werden selbst die gewieftesten Angreifer nur noch wenige Orte im Netzwerk haben, an denen sie sich verstecken können.

Klaus Nemelka

KÜNSTLICHE INTELLIGENZ

DAS HERZSTÜCK DES NETZWERKS

Unternehmen sehen eine steigende Anzahl mobiler und IoT-Geräte sowie einen Ansturm auf neue Apps in ihrem drahtlosen Netzwerk. Es ist daher an der Zeit für Innovationen, die der IT dabei helfen, die Skalierbarkeit zu erhöhen und diese neuen Anforderungen zu erfüllen. Glücklicherweise entwickeln sich KI und moderne Cloud-Plattformen mit Mikroservices weiter, um diese Anforderungen zu erfüllen. Eine wachsende Anzahl von Unternehmen erkennen außerdem, dass künstliche Intelligenz (KI) eine wichtige Komponente ist und ein lernendes WLAN ermöglicht. Dank KI lässt sich die Effizienz erhöhen und Kosteneinsparungen dank Automatisierung erzielen. Gleichzeitig erhalten Unternehmen detaillierte Einblicke in die User Experience oder Service Level Enforcement (SLE). Es kann auch neue Location-based Services ermöglichen, die Unternehmen und Nutzern einen enormen Mehrwert liefern.

Im Kern des lernenden WAN ist die KI-Engine, die Automatisierungs- und Analysefunktionen bietet. Dazu gehören Wi-Fi-Assurance, Natural Language Processing (NLP)-basierte virtuelle Netzwerk-Assistenten, Asset-Lokalisierung, User Engagement und Standortanalysen.

Es gibt vier wichtige Komponenten für den Aufbau einer KI-Engine für ein WLAN: Daten, Strukturieren & Klassifizieren, Data Science und Erkenntnisse. Hier sind einige Details zu allen vier Elementen.

Daten

Die KI-Engine ist nur so gut wie die Daten, die es aus Netzwerk, Anwendungen, Geräten sowie von den Anwendern erhält. Um eine gute KI-Plattform aufzubauen, benötigt die Engine also Daten – und zwar eine Menge.

Damit dies Realität wird, sind spezielle Access Points notwendig, die die Prä- und Post-Verbindungszustände jedes drahtlosen Geräts erfassen. Sie müssen außerdem sowohl synchrone als auch asynchrone Daten sammeln. Synchrone Daten sind die typischen Daten anderer Systeme, zum Beispiel der Netzwerkstatus. Asynchrone Daten sind ebenfalls kritisch, da sie dem Benutzer Informationen über den Benutzerstatus liefern. Sie sind notwendig, um User Service Levels zu erstellen und Anomalien am Rand zu erkennen. Diese Informationen oder Metadaten werden an die Cloud gesendet, wo die KI-Engine sie strukturiert und klassifiziert.

KI-Primitives

Als nächstes strukturiert die KI-Engine die von den Netzwerk-Elementen empfangenen Metadaten mit einer Reihe von KI-Primitives. Dafür muss sie von Entwicklern mit wireless Netzwerk-Domänen-Wissen programmiert werden. Nur so lassen sich die strukturierten Metadaten für die Analyse durch die Data Science Toolbox klassifizieren – und letztlich Einblicke in das Netzwerk liefern.

Eine Reihe unterschiedlicher KI-Primitives, die als Metriken oder Klassifikatoren strukturiert sind, tracken die End-to-End-Nutzererfahrung für wichtige Bereiche wie Verbindungszeit, Durchsatz, Abdeckung, Kapazität und Roaming. Die Nachverfolgung, wann diese Elemente erfolgreich sind, fehlschlagen oder starten, in welche Richtung sie tendieren und aus welchem Grund, gibt der KI-Engine die notwendige Transparenz, um Service Levels festzulegen. Sie kann diese darüber hinaus entsprechend kontrollieren und durchsetzen.

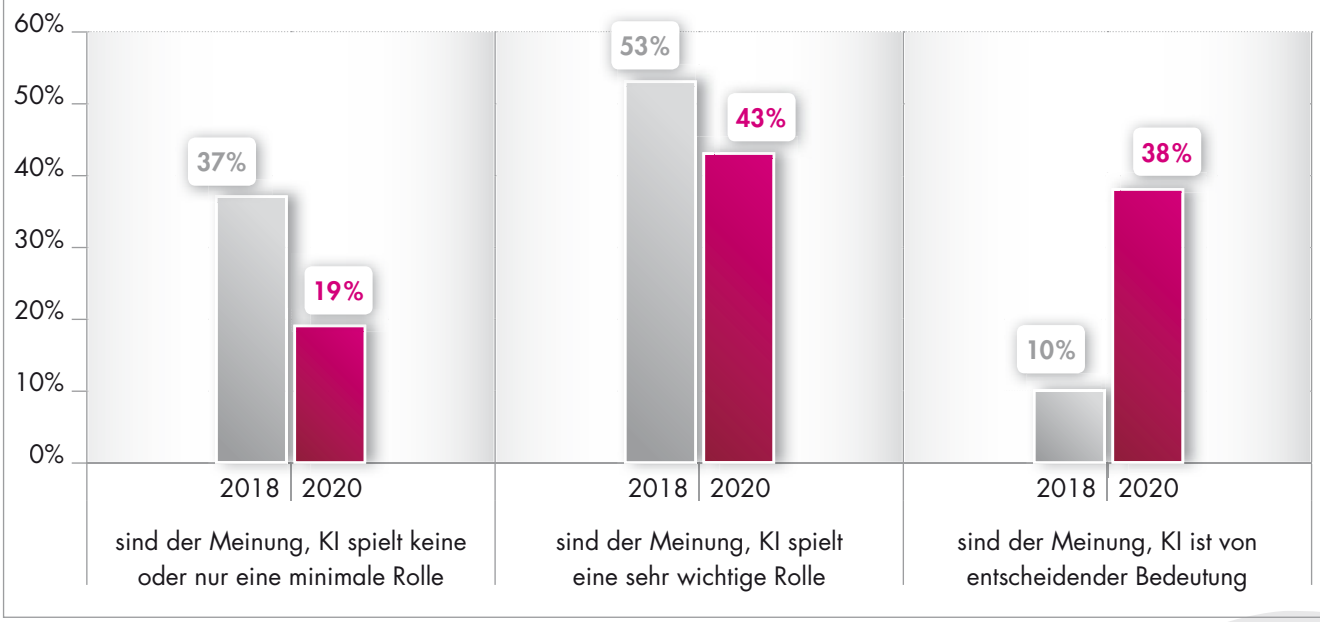
Datenwissenschaften

Sobald die Daten gesammelt, gemessen und klassifiziert wurden, kann die Data Science starten. Hier wird es dann interessant. Der Grund dafür: Es gibt eine Reihe unterschiedlicher Techniken, die sich verwenden lassen. Dazu gehören überwachtes und unbeaufsichtigtes Machine Learning, Data Mining, Deep Learning sowie die gegenseitige Information. Sie werden angewendet, um Funktionen wie Baselining, Anomalie-Erkennung, Ereignis-Korrelation und Vorhersage-Empfehlungen durchzuführen.

KI-ENGINES SIND MITTLERWEILE EIN MUSS FÜR UNTERNEHMEN, DA SIE MIT DER STEIGENDEN ANZAHL NEUER GERÄTE, DINGE UND ANWENDUNGEN IN DER HEUTIGEN VERNETZTEN WELT SCHRITT HALTEN KÖNNEN.

Jeff Aaron, Vice President of Marketing at Mist Systems, a Juniper Company, www.juniper.net

FÜHRUNGSKRÄFTE BERICHTEN, DASS DIE KI FÜR DEN GESCHÄFTSERFOLG IHRER UNTERNEHMEN STRATEGISCH WICHTIGER WERDEN WIRD:



(Quelle: Deloitte's „State of AI in the enterprise" survey 2018, global data)

So werden beispielsweise Zeitreihendaten als Baseline festgelegt und zur Erkennung von Anomalien verwendet. Kombiniert mit einer Ereignis-Korrelation bestimmen sie schnell die Ursache für wireless, kabelgebundene und Geräteprobleme. Durch die Kombination dieser Techniken sind Netzwerkadministratoren in der Lage, die MTTR (Mean Time to Repair)-Probleme zu reduzieren. Sie sparen somit Zeit und senken die Kosten. Gleichzeitig steigt die Zufriedenheit der Nutzer.

Ein gegenseitiger Informationsaustausch wird auch auf Wi-Fi-Service-Level angewendet, um den Erfolg des Netzwerks vorherzusagen. Genauer gesagt: Unstrukturierte Daten werden von der wireless Edge genommen und in domänenspezifische Kennzahlen wie Verbindungszeit, Durchsatz und Roaming umgewandelt. Diese werden auf die SLE-Metriken angewendet. So lässt sich feststellen, welche Netzwerkfunktionen am ehesten zu Erfolg oder Misserfolg führen – und wie umfangreich die Auswirkungen sind.

Darüber hinaus lässt sich unbeaufsichtigtes Machine Learning für eine hochgenaue Lokalisierung im Innenbereich einsetzen. Für Standortlösungen auf der Basis von Empfangssignalstärke-Indikatoren (Received Signal Strength Indicator, RSSI) wird ein Modell benötigt, das RSSI auf Entfernung abbildet. Diese wird oft auch als RF-Pfadverlustmodell bezeichnet. Typischerweise wird dieses Modell durch die manuelle Daten-Erfassung erlernt, dem sogenannten Fingerprinting. Dank KI ist es jedoch möglich, den Wegverlust durch Machine Learning in Echtzeit zu berechnen. Hierbei werden RSSI-Daten von direktionalen BLE-Antennen verwendet. Das Ergebnis ist eine hochpräzise Position, die keine manuelle Kalibrierung oder umfangreiche Standortbestimmungen erfordert.

KI-gesteuerte virtuelle Assistenten

Die letzte der vier Komponenten der KI-Engine ist ein virtueller Assistent, der dem IT-Administrator Einblicke liefert und diese in das Netzwerk selbst einspeist. So lässt sich die Problemlösung automatisieren. Das Ergebnis ist letztlich ein „selbstheilendes Netzwerk".

Ein natürlicher Sprachprozessor ist enorm wichtig, um den Prozess für Administratoren zu vereinfachen, Erkenntnisse aus der KI-Engine zu extrahieren – und zwar ohne die Dashboards oder Befehle des Common Language Interpreters (CLI) durchsuchen zu müssen. Dies ist bei Legacy-Systemen ohne KI der Fall. Dies kann die Produktivität der IT-Teams steigern und gewährleistet gleichzeitig eine bessere Benutzerfreundlichkeit für Mitarbeiter und Kunden.

Drahtlose Netzwerke sind geschäftskritischer denn je, ein Troubleshooting wird jedoch aufgrund der zunehmenden Anzahl unterschiedlicher Geräte, Betriebssysteme und Anwendungen jeden Tag schwieriger und komplexer. KI-Engines sind daher mittlerweile ein Muss für Unternehmen, da sie mit der steigenden Anzahl neuer Geräte, Dinge und Anwendungen in der heutigen vernetzten Welt Schritt halten können.

Jeff Aaron

EINE FRAGE DER GRÖSSE?

WIE TICKT DER MITTELSTAND IN SACHEN IT-SICHERHEIT?

Mit der rapide ansteigenden Digitalisierung in Unternehmen entstehen für die IT-Sicherheit neue Stolpersteine. Während Mitarbeiter sich über neue Technologien oder Konzepte aus den Bereichen Bring your own Device, Internet of Things und Co. freuen, schlagen in den IT-Abteilungen aus Sicherheitssicht die Alarmglocken. Ungesicherte Geräte, das Nutzen öffentlicher W-Lans mit dem eigenen Smartphone oder täuschend echt wirkende E-Mails mit verseuchten Anhängen – die Angriffsvektoren für Cyberattacken sind vielfältig. Wer sich fahrlässig den Gefahren aussetzt, der muss mit schweren finanziellen oder auch imagetechnischen Konsequenzen leben.

Um das zu verhindern, müssen Unternehmen die IT-Sicherheit fest in der Unternehmensstrategie verankern. Nur so kann gewährleistet werden, dass alle an einem Strang ziehen und die IT-Sicherheit den Stellenwert bekommt, den sie dringend benötigt und verdient.

Genießt die IT-Sicherheit den notwendigen Stellenwert? Sind die Mitarbeiter für die Gefahr sensibilisiert worden? Welche technischen und mitarbeiterzentrierten Maßnahmen sind besonders wichtig?

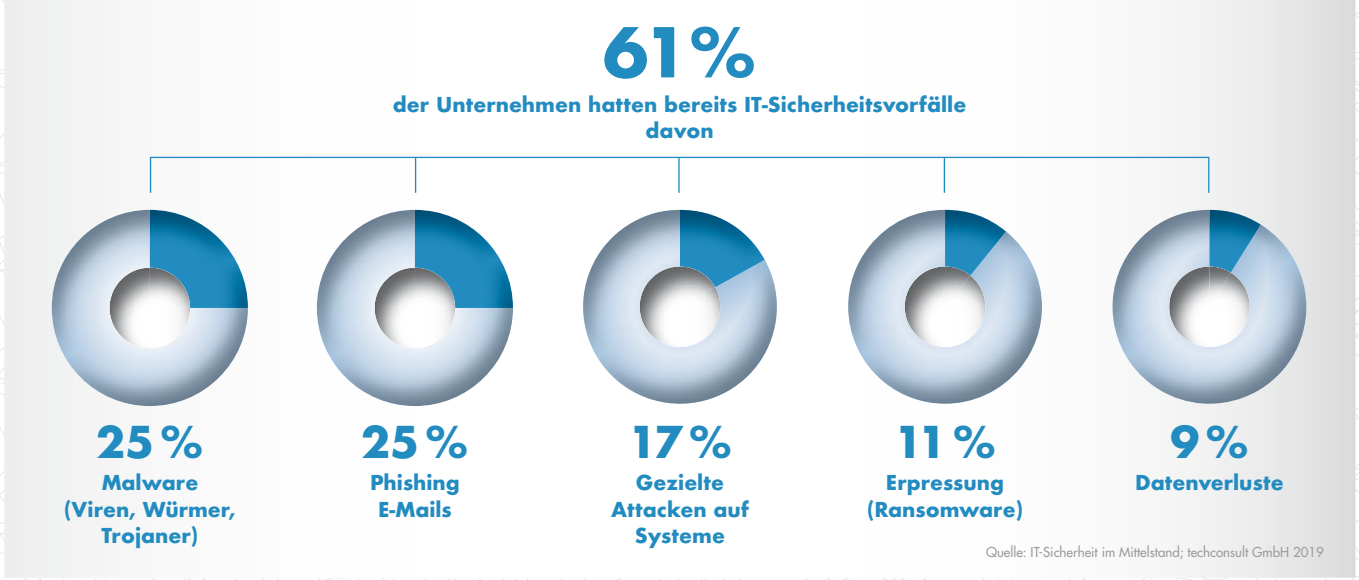
Um diese Fragen zu beantworten, wurden im Rahmen der Studie „IT-Sicherheit im Mittelstand" von DriveLock und techconsult 202 Unternehmen aller Branchen zu ihren IT-Sicherheitsmaßnahmen untersucht.

Knapp die Hälfte der Befragten waren IT-Leiter und CIOs sowie IT-Mitarbeiter, -Administratoren und -Spezialisten. Die zweite Hälfte setzte sich zusammen aus weiteren C-Level-Positionen – CISOs eingeschlossen – Compliance-Spezialisten und Sicherheits- und Datenschutzbeauftragten.

Sicherheit im Mittelstand

Cyberangriffe sind längst als ernstzunehmende Bedrohung im Bewusstsein deutscher Unternehmen angekommen. Doch die Intensität, mit der gegen diese Angriffe vorgegangen wird, unterscheidet sich je nach Branche und Unternehmensgröße. Laut der Studie hat die IT-Sicherheit einen größeren Stellenwert, je größer das Unternehmen ist. Stellt man sich die Frage, wieso mit steigender Unternehmensgröße die Implementation von IT-Sicherheit in die Unternehmensstrategie anwächst, lässt sich dies auch mit der Rollenverteilung in den Unternehmen erklären. In kleinen Unternehmen sind die Geschäftsführung und der IT-Leiter oftmals für die IT-Sicherheit verantwortlich. In größeren Unternehmen

GAB ES IN DEN VERGANGENEN ZWEI JAHREN IT-SICHERHEITSVORFÄLLE IN IHREM UNTERNEHMEN UND WENN JA, UM WELCHE ART VON VORFALL HANDELTE ES SICH?



bewegt sich die Verantwortlichkeit von der Geschäftsführung hin zu einem dedizierten IT-Security-Leiter. Im Gegensatz zum Geschäftsführer oder IT-Leiter kann der IT-Security-Leiter mit deutlich mehr Expertise aufwarten, als es die Generalisten können.

Zuständigkeiten, Stellenwert und Umsetzung

Der IT-Leiter ist in fast allen Unternehmen haupt- oder mitverantwortlich für die IT-Sicherheit (83%). In 64 Prozent der Fälle ist es der IT-Security-Leiter. 27 Prozent der Unternehmen besetzen diese Position nicht einmal. Ähnlich schwach vertreten sind Compliance- und Governance-Verantwortliche. Die Position ist bei mehr als zwei Drittel der Unternehmen nicht vorhanden. Falls doch, haben sie im Vergleich den geringsten Einfluss (40%) auf Prozesse der IT-Sicherheit.

Die Studienergebnisse zum Thema Stellenwert sind leider ebenso wenig überraschend: Je kleiner die Unternehmen, umso seltener ist IT-Sicherheit Teil der Unternehmensstrategie. 50 beziehungsweise 42 Prozent der Unternehmen mit weniger als 50 oder 50-249 Mitarbeitern setzen Security-Maßnahmen proaktiv nur punktuell um, zum Beispiel im Rahmen von Gesetzesvorgaben oder erst nach einem Sicherheitsvorfall. Selbst bei Großunternehmen mit über 500 Mitarbeitern liegt dieser Wert noch bei 32 Prozent. Die verbleibenden 68 Prozent der Unternehmen in dieser Größenordnung sehen IT-Sicherheit als einen zentralen Bestandteil ihrer Unternehmensstrategie. Ein Grund für den hohen Anteil an punktuellen Maßnahmen ist sicherlich, dass beim Großteil der Unternehmen der IT-Leiter neben seinen zahlreichen anderen Pflichten auch für Security zuständig ist. Da ist es wenig erstaunlich, dass Cybersicherheit nur dann Beachtung findet, wenn unbedingt erforderlich wie bei der DSGVO.

In Sachen Umsetzung setzen die Unternehmen größtenteils immer noch auf die Klassiker: Lösungen wie Firewall (67%), Spamfilter (63%) und Antivirus (62%) führen die Liste an. Auch das zeigt, dass Security häufig nebenbei gehandhabt wird. Viele Unternehmen setzen einfach auf diese drei Basics bei der Umsetzung ihrer IT-Sicherheit. Das überrascht nicht, denn diese Lösungen sind bereits seit vielen Jahren etabliert – sowohl in Unternehmen als auch privat. Dahinter folgen Schulungen (57%) und Sensibilisierungskampagnen (50%) für die eigenen Mitarbeiter – noch vor Verschlüsselungstechnologien (ca. 49%).

Bei der tatsächlichen Umsetzung der einzelnen Bereiche existiert jedoch eine Diskrepanz zwischen Wunsch und Wirklichkeit. Eigentlich dürfte es kein Unternehmen geben, das Probleme mit Antivirus, Firewall oder E-Mail-Sicherheit hat. Doch leider sind immer noch 20 Prozent der Unternehmen in diesem Bereich nicht gut aufgestellt. Das heißt, dass ihre eingesetzte Lösung entweder nicht zufriedenstellend funktioniert und Malware trotzdem durchkommt oder aber diese überhaupt nicht vorhanden ist.

Inhouse oder outsourced?

IT-Sicherheit lässt sich in verschiedenen Bereitstellungsformen angehen. Das fängt beim klassischen Inhouse-Betrieb an, über Teilauslagerungen einzelner IT-Security-Bereiche bis hin zum kompletten Outsourcen der gesamten IT-Sicherheit.

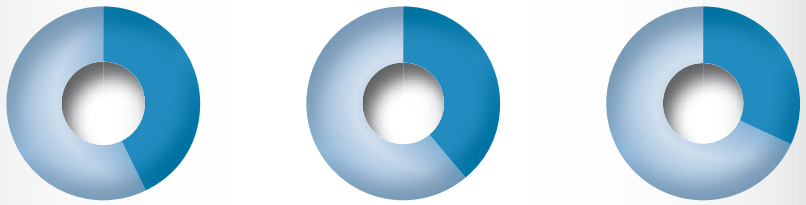
Das Management durch externe Dienstleister ist besonders bei der kleinsten Unternehmensgröße mit 50 Prozent (gesamt 35%) eine der wichtigsten Eigenschaften bei der Wahl von Security-Leistungen. Generell sind externe Security Provider für Unternehmen, die sich nicht selbst um ihre Sicherheitsstrategie kümmern können beziehungsweise wollen, am sinnvollsten. Das ist besonders dann der Fall, wenn es Unternehmen an Ressourcen mangelt wie Security-Fachkräfte oder -Know-how. Das bedeutet auch: Je größer das Unternehmen ist, desto eher wird die IT-Sicherheit im eigenen Haus betrieben.

Fazit

Laut der Studie könnte der Mittelstand durchaus mehr für die IT-Sicherheit tun. Zwar ist sie wichtiger Bestandteil der eigenen Unternehmensstrategie, dennoch hat sie in kleineren Unternehmen deutlich seltener einen Platz in eben dieser.

Martin Mangold | www.drivelock.de

WELCHE AUSWIRKUNGEN DURCH MANGELNDE CYBER-SECURITY-MASSNAHMEN BEFÜRCHTEN SIE?



43 % zu spätes Erkennen von Sicherheitsproblemen

39 % Verstöße gegen die DSGVO

32 % Anstieg unerwarteter Kosten

Quelle: IT-Sicherheit im Mittelstand; techconsult GmbH 2019

Die komplette Studie kann unter folgender URL heruntergeladen werden: **https://bit.ly/2HxMNL6**

DIGITALE IDENTITÄTEN

SO WERDEN DIGITALE IDENTITÄTEN FÜR MENSCHEN UND MASCHINEN DIE

Darrell Long von One Identity weist in seiner Prognose auf die Zusammenhänge zwischen Robotik-Prozessautomatisierung, Cloud, Compliance, Datendiebstahl, Künstliche Intelligenz und das Identity & Access Management hin.

Der Aufstieg der verwundbaren Maschinen

Im Jahr 2020 wird die Robotik-Prozessautomatisierung (RPA) ihren umwälzenden Aufstieg weiter fortsetzen und sich noch stärker in unserem Alltag verankern. Bis Ende 2019 prognostiziert Gartner, dass der Umsatz mit der Robotik-Prozessautomatisierung die 1,3 Milliarden US-Dollar-Marke knacken wird. Für das neue Jahr wird sogar ein noch stärkeres Wachstum erwartet. Allerdings gibt es bei der Integration von RPA ein beherrschendes Problem – das der Sicherheit. Im Zuge der raschen Einführung von RPA spielte Sicherheit nur eine nachgeordnete Rolle, die schwerwiegende Schwachstellen hinterlassen hat. Wie wir es schon bei anderen Innovationen beobachten konnten, rechnen wir im Jahr 2020 mit einem signifikanten Datenschutzverstoß gegen die RPA-Technologie. Denn die Technologie wird die Aufmerksamkeit von Cyberkriminellen zwangsläufig auf sich ziehen. Allein aufgrund der privilegierten Daten, die in RPA-Technologien vorgehalten werden. Leider wird man sich erst um ausreichende Sicherheit bemühen, wenn es zu spät ist, und wenn entsprechende Vorschriften mit der Nutzung von RPA-Technologien verbunden werden.

Sich an der Cloud die Finger verbrennen

Es gibt im Moment eine Art „Goldrausch" bei Unternehmen, ihre Daten in die Cloud zu verschieben. Praktisch jeder will auf den fahrenden Zug aufspringen. Das Problem dabei: viele springen erst und schauen dann genauer hin. Gerade große Unternehmen migrieren in rasantem Tempo in die Cloud, ohne sicherzustellen, dass ihre Daten während der Übertragung ebenso geschützt sind wie an ihrem Bestimmungsort. Das Jahr 2020 wird für etliche Unternehmen von Datenschutzverletzungen und den daraus resultierenden Bußgeldern gekennzeichnet sein. Einfach, weil Firmen versäumt haben, rechtzeitig die notwendigen Schritte einzuleiten. Trotz eines Shared Responsibility Modells und ständigen Schlagzeilen zu Cloud-Sicherheitsschwachstellen, prognostizieren wir, dass viele Unternehmen daran scheitern werden Due Diligence durchzusetzen. Wer Datensicherheit in der Cloud unberücksichtigt lässt, der wird sich an diesem Thema zweifelsohne die Finger verbrennen. In der Folge werden diese Unternehmen zu spät herausfinden, dass Identity Governance und Privileged-Access-Management schon on-premises hätten ordnungsgemäß umgesetzt werden sollen. Um diese Best Practices dann beizubehalten, wenn die Migration in die Cloud ansteht.

Compliance trifft alle Branchen hart

Unternehmen aller Branchen werden mit der Integration proaktiver Datenschutzpraktiken und -richtlinien zu kämpfen haben. Die EU-Datenschutz-Grundverordnung (DSGVO/GDPR) und weitere in Arbeit befindliche Regularien, werden die Unternehmen abstrafen, die im Umgang mit Daten fahrlässig handeln. Firmen müssen ihre Kunden im Falle einer Datenschutzverletzung in Kenntnis setzen. Wenn sich im Zuge dieses Prozesses herausstellt, dass keine angemessenen Datenschutzpraktiken wie Identity Governance and Administration sowie Privileged Access Management umgesetzt wurden, dann ist mit deutlich empfindlicheren Strafen für die Betroffenen zu rechnen. Wir werden vermutlich einen Ansturm der Unternehmen erleben, die nach einer Datenschutzverletzung einen Schritt zurückgehen um die richtigen Sicherheits-Tools und –Methoden ein- und umzusetzen.

Der Markt für gestohlene Daten boomt weiter

Auch im kommenden Jahr werden Daten unter Cyberkriminellen weiterhin als hei-

NÄCHSTEN JAHRE PRÄGEN

ße Ware begehrt sein. Bei dem Versuch, ihre Daten wirksam zu schützen, werden Unternehmen den Ball immer wieder mal verlieren. In unserer datengetriebenen Ökonomie sind Daten mehr wert als Öl, und Hacker sind sich sehr wohl bewusst, welchen Profit sie aus gestohlenen Anmeldedaten zu privilegierten Konten schlagen können. Im neuen Jahr wird sich das besonders auswirken, wenn Unternehmen versäumen

Privileged Account Management (PAM) und Identity Governance and Administration (IGA) korrekt umzusetzen und so die Daten, mit denen sie arbeiten, umfassend zu schützen. Dieses Versagen wird sich unmittelbar auf die Wettbewerbsfähigkeit eines Unternehmens auswirken und Firmen ins Abseits drängen. Im Gegensatz zu sicherheitszentriert arbeitenden Organisationen, die in der Lage sind, ihren Kunden das notwendige Vertrauen zu geben, dass der unternehmerische Fokus auf dem Schutz der Kundendaten liegt.

Künstliche Intelligenz

Künstliche Intelligenz hat jetzt die Gelegenheit von einem Tool, dessen Kapazitäten nicht ausgereizt wurden, und das nicht selten als „Schall und Rauch" bezeichnet wird, zu einem zu werden, das Unternehmen einen echten Mehrwert bietet. Künstliche Intelligenz und Analytik wird die Art und Weise verändern in der Unternehmen Identity Governance and Administration (IGA) implementieren. Das wird ein großer Schritt in die richtige Richtung sein. Hin zu mehr und kontinuierlicher Sicherheit bei der Governance von Zugriffsberechtigungen und damit hin zu einem besseren Schutz des Unternehmens und der vorgehaltenen Daten. Der Grund, warum KI und Analytics in der Vergangenheit nicht so eingesetzt wurden, liegt darin, dass viele Unternehmen einfach nicht wissen wie sie (KI) und Analytics am besten in ihre Sicherheits- und Governance-Programme integrieren. Das wird sich ändern. Im Jahr 2020 sind Unternehmen an einem Punkt angelangt, an dem sie sich in Sachen KI sicherer fühlen und ein besseres Verständnis für den Mehrwert entwickelt haben, den KI für ein Sicherheitsprogramm zu bieten hat. Jetzt ist es an der Zeit, den nächsten Schritt zu tun, um diese Lösungen abzusichern und effektiv zu verwalten.

Darell Long | www.oneidentity.com

IAM CONNECT 2020

Konferenz vom
16. bis 18. März 2020 in Berlin

Treffen Sie One Identity auf der Konferenz IAM CONNECT 2020 und bringen Sie Ihr Know-how über Identity & Access Management und das Internet of Things auf den neuesten Stand.

IAM im industriellen IoT-Umfeld

Mathias Winter, Azure-Experte bei der PI Informatik GmbH, berichtet von der Digitalisierung „alter" industrieller Anlagen und die Herausforderung in diese IoT-Szenarien IAM-Technologien zu etablieren.

IAM für Internet-Dinger (IoT)

Peter Weierich von der IPG GmbH hält einen Workshop über IoT-Projekte und ihre Auswirkungen auf IAM-Prozesse.

IAM-Verantwortliche der Bundesagentur für Arbeit, Deutsche Anlagen-Leasing (DAL), DEVK Versicherungen, Johanniter-Unfall-Hilfe e.V., KfW Bankengruppe, KPT Krankenkasse, Munich Re und Thüringer Aufbaubank berichten über ihre IAM-Projekte.

Konferenz mit Erfahrungsberichten, Speed Demos, Ausstellung, Workshops und Diskussionsrunden

Info und Anmeldung:
www.iamconnect.de

IAM CONNECT 2020

IT & OT IM WANDEL

CYBERBEDROHUNGEN IN DER FERTIGUNGSINDUSTRIE

Über Jahrzehnte hinweg wurden Systeme innerhalb der Informationstechnologie (IT) getrennt von denen der operativen Technologie (OT) in voneinander unabhängigen Netzwerken betrieben. Mit unterschiedlichen Komponenten und unterschiedlichen Zielen.

Während IT-Systeme für Berechnungen verwendet werden, die dazu dienen Informationen zu verarbeiten, hat die operative Technologie eine andere Aufgabe. Mit ihrer Hilfe werden physikalische Prozesse, Umgebungen, Ereignisse und Vorkommnisse in einem Unternehmen überwacht. Allerdings haben die jüngsten Entwicklungen dazu geführt, dass diese zuvor getrennten Umgebungen verschmelzen. Dazu gehören eine zunehmende Automatisierung und Verbesserungen innerhalb von Produktionsanlagen und kritischen Infrastrukturen.

Diese Entwicklung hat allerdings auch unerwünschte Nebenwirkungen. Je mehr die OT über neue intelligente Geräte vernetzt ist, desto mehr sind industrielle Systeme komplett neuen Sicherheitsrisiken ausgesetzt. Drahtlose Geräte sorgen für bequemere Vernetzung und mehr Produktivität, aber sie können auch zur Zielscheibe von Cyberangriffen werden. Cyberkriminelle nutzen die zwischen IT und OT entstandene Sicherheitslücke für sich aus.

Wie schützt man sich?

Doch wie geht der Fertigungssektor mit der wachsenden Zahl von Cyberbedrohungen um und inwieweit bereitet sich die Branche insgesamt angemessen vor? Zumeist haben Industrieunternehmen mit denselben Herausforderungen und Risiken hinsichtlich der benutzten Software zu kämpfen wie jedes andere Unternehmen auch. Jede Software, die Sie kaufen und benutzen birgt Risiken. Wie soll man einschätzen, ob das Risiko akzeptabel ist

SICHERHEIT IST KEIN TECHNOLOGIEPROBLEM, SICHERHEIT IST EIN PROZESSPROBLEM. AUTOMATISIERTE TOOLS HELFEN BEI DER JAGD AUF SOFTWARE-SCHWACHSTELLEN. SIE SIND ALLERDINGS NUTZLOS, WENN SIE NICHT IM RAHMEN EINES ÜBERGREIFENDEN RISIKO-MANAGEMENT-PROZESSES ZUM EINSATZ KOMMEN.

Jonathan Knudsen, Senior Security Strategist, Synopsys Software Integrity Group, www.synopsys.com

oder nicht? Wie soll man Cybersicherheitsrisiken unterschiedlicher Produkte miteinander vergleichen? Historisch betrachtet mussten Industrieunternehmen darauf vertrauen, dass die verwendete Software angemessen sicher war. Das heißt, sich auf Anbieter zu verlassen, die einen Secure Development Life Cycle (SDLC) mittels automatisierter Tools gewährleisten. Ziel dieses Prozesses ist es, so viele Schwachstellen wie möglich zu finden und zu beheben, bevor das Produkt auf den Markt kommt, um die Risiken so gering wie möglich zu halten. In der Fertigungsindustrie kommen aber einige spezielle Herausforderungen dazu. Einerseits überwacht eine Software in einem industriellen Netzwerk meist physische Prozesse. Software-Schwachstellen verursachen unter Umständen physische Schäden. Auf der anderen Seite ist die lange Lebensdauer von industriellen Komponenten und Systemen komplett gegenläufig zu den schnellen und häufigen Update-Zyklen wie sie bei Software üblich sind.

Welche Auswirkungen kann es geben?

Man braucht sich nur die jüngsten Schlagzeilen ansehen, wenn man wissen will, was passiert, wenn es jemandem nicht gelungen ist Cybersicherheit ausreichend zu adressieren. Jedes Unternehmen nutzt Software. Folglich kann auch jedes von ihnen Opfer eines Cyberangriffs werden. Gerade für Industrieunternehmen sind die Folgen erfolgreicher Attacken so vielfältig wie schwerwiegend. Dazu zählen der Diebstahl geistigen Eigentums und sensibler geschäftlicher Informationen ebenso wie physische Schäden an Anlagen und Ausrüstung, Produktionsausfälle und Systeme, die durch Ransomware lahmgelegt werden. Selbst so schwerwiegende Folgen wie Verletzungen und Todesfälle unter der Belegschaft sind nicht auszuschließen.

Gibt es einen Sicherheitspuffer?

Die magische technologische Sicherheitsdecke existiert leider nicht. Wenn man Sicherheitsrisiken effektiv managen will, ist es wie bei vielen anderen Dingen auch. Man muss einiges an Arbeit hineinstecken, und man muss die Art und Weise verändern, in der man bisher vorgegangen ist. Für Industrieunternehmen gilt analog, was für jedes andere Unternehmen auch zutrifft. Die Basis ist eine fundierte und vom Management getragene Sicherheitsinitiative deren Aufgabe es ist die Sicherheitskultur im gesamten Unternehmen zu kommunizieren und zu verankern. Systeme und Netzwerke sollten bei jedem Entwicklungsschritt so konzipiert werden, dass Sicherheit immer Bestandteil der Entwicklung ist. Bei der Beschaffung von Anlagen, Ausrüstung und Software sollte man die potenziellen Sicherheitsrisiken gründlich prüfen, und dazu sollte man etwas von sicheren Softwareentwicklungszyklen verstehen. Nur dann sind Sie in der Lage, den Anbietern prägnante Fragen zu stellen und die Antworten einzuordnen. Man kann noch einen Schritt weiter gehen und eine eigene Risikobewertung erheben. Etwa mithilfe von Software Composition Analysis (SCA) Tools oder Penetrationstests.

Das neue Wundermittel: KI

Es stellt sich die Frage: Inwieweit haben technologische Fortschritte und Automatisierung dazu beigetragen, blinde Flecken im Cyberspace zu finden? Wird die Zukunft durch Automatisierung und KI sicherer?

Nun, Sicherheit ist kein Technologieproblem, Sicherheit ist ein Prozessproblem. Automatisierte Tools helfen bei der Jagd auf Software-Schwachstellen. Sie sind allerdings nutzlos, wenn sie nicht im Rahmen eines übergreifenden Risiko-Management-Prozesses zum Einsatz kommen. Umsichtige Industrieunternehmen werden eigene Assessments anwenden, bevor sie neue Systeme oder Software-Pakete ausbringen. Aber man sollte die Anbieter ermutigen, gründliche und umfassende Sicherheitstests während des gesamten Entwicklungszyklus einer Software durchzuführen. Automatisierte Tools analysieren den Quellcode und die Zusammensetzung der Software, sie bewerten die Sicherheit von Software-Produkten mit Fuzz-Testing, mit interaktiven und mit dynamischen Testmethoden. Zukünftige Neuerungen werden sich in genau dieses Rahmenwerk eines sicheren Entwicklungslebenszyklus einer Software einfügen. Impulse werden vermutlich auch von künstlicher Intelligenz ausgehen.

Jonathan Knudsen

2. Cyber Security Tech Summit Europe 2020
11. März 2020
WCCB Bonn

SECURITY

T · · macht den Unterschied.
Erleben Sie, wie sich „Managed Cyber Defense“ nahtlos in Ihr bestehendes System einfügt: für ein noch wirksameres Entdecken und Abwehren aller Gefahren.
Jetzt unter **0800 33 09333**
oder auf **t-systems.de/security**
oder Live auf dem **2. Cyber Security Tech Summit Europe 2020!**

T · · Systems ·

Let’s power higher performance