itmanagement

DEZEMBER 2021

INKLUSIVE 32 SEITEN

IT SECURITY SPEZIAL

DIGITALE SOUVERÄNITÄT

Das Problembewusstsein schärfen

BÜROKULTUR NEU GEDACHT

Smart und Seamless Offices

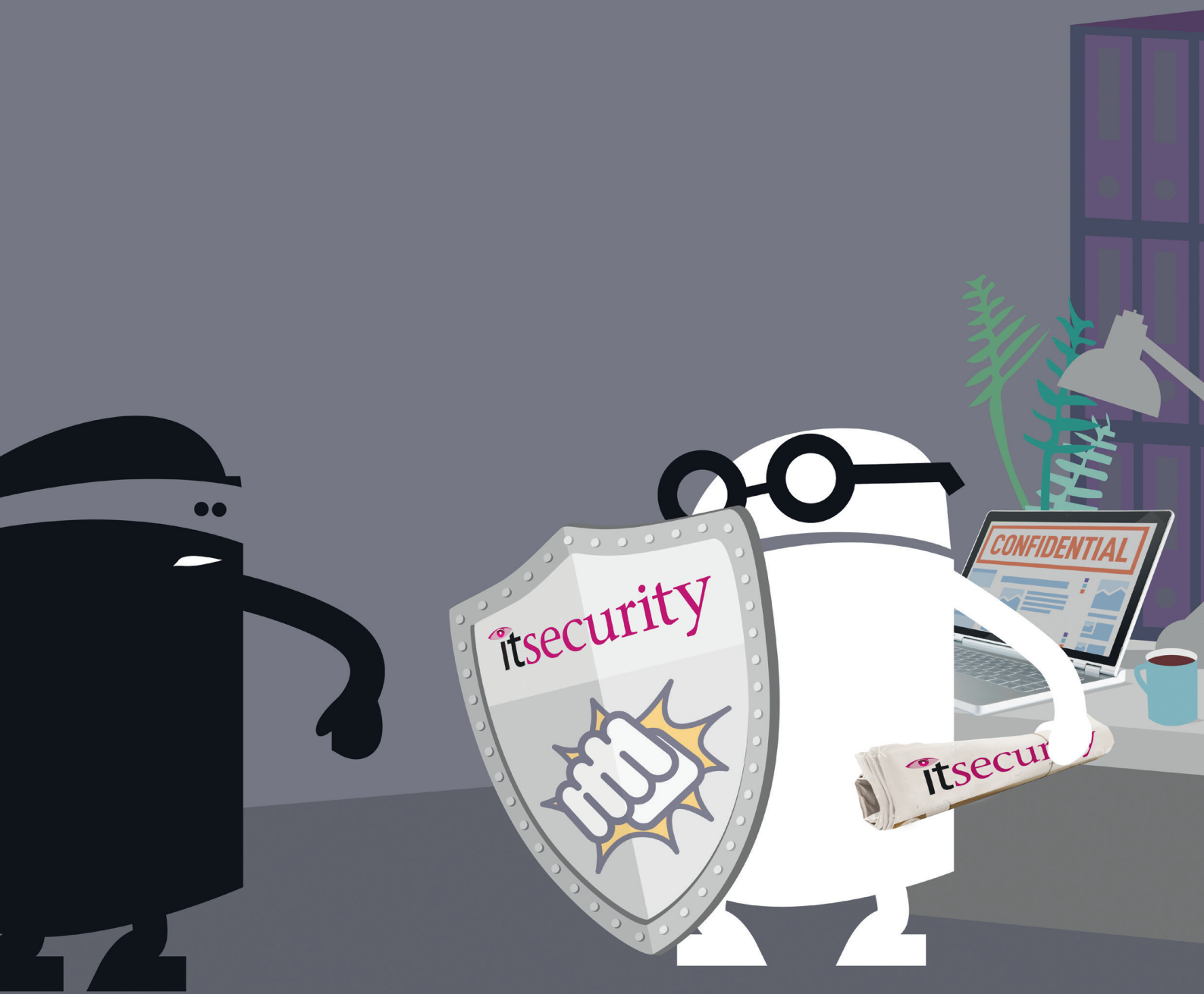
PARTNERSCHAFT MIT ZUKUNFT

FLEXIBLE ARBEITSWELT

Marianne Janik, Microsoft und Peter Arbitter, Telekom

www.it-daily.net

Wer viel weiß, weiß sich zu wehren.



Der nächste Angriff kommt bestimmt.

Gut vorbereitet mit itsecurity

www.it-daily.net

ALLES WIE IMMER?

Das Jahr neigt sich langsam dem Ende zu und was gibt es da Spannenderes, als einen Blick in die Zukunft? Meldungen dazu landen eigentlich täglich in meinem Posteingang und man fühlt sich regelrecht erschlagen, ob der vielen Trends, die im Jahr 2022 auf uns zukommen werden. Um es aber kurz zu machen: Home-Office wird bleiben, aber an der technischen Unterstützung muss gefeilt werden; Cyberattacken werden weiter zunehmen, aber an der Verteidigung muss intensiv gearbeitet werden; Künstliche Intelligenz wird verstärkt eingesetzt werden, aber es gibt nach wie vor Vorbehalte, meistens ethische.

Eigentlich hätte ich genau diesen Text auch 2020 schreiben können, denn gefühlt sind diese Themen identisch zum Vorjahr. Gut, beim Thema New Work/ Home-Office scheint man sich etwas arrangiert zu haben und entwickelt gerade innovative Konzepte für eine intelligentere Büronutzung. In das Thema Cybersecurity kommt auch etwas Bewegung, denn da zeichnet sich ab, dass nun doch mehr Kapital zum Schutz der Unternehmenssoftware in die Hand genommen wird. Tja und künstliche Intelligenz? Die wird vermehrt eingesetzt und keinem fällt es so richtig auf.

Also alles irgendwie beim Alten? Sicher nicht, aber aktuell bin ich noch über keinen wirklich neuen Trend gestolpert. Green IT könnte vielleicht einer werden, ebenso selbstlernende Datensysteme. Was letztendlich draus werden wird, bleibt abzuwarten.

In diesem Sinne, herzlichst

Carina Mitzschke | Redakteurin it management

INHALT

COVERSTORY

8 **Partnerschaft mit Zukunft**
Innovative Veränderungen für eine moderne und flexible Arbeitswelt

IT MANAGEMENT

12 **Hyperkonvergente Infrastrukturen**
Welchen Unternehmen sie helfen können

14 **Digitale Souveränität**
Haben wir noch eine Chance auf digitale Selbstbestimmung?

16 **New Work**
Erfolgreiche Implementierung durch Mitarbeiterzentrierung

20 **Business Analytics**
What-if-Analysen

eBUSINESS

22 **Der Online-Shop ist kein IT-Projekt!**
Dos and don'ts im E-Commerce

24 **E-Commerce**
Besser nicht beim Hosting sparen

25 **Bezahlen mit Daten**
Neue Chance für den E-Commerce

TRENDS 2022

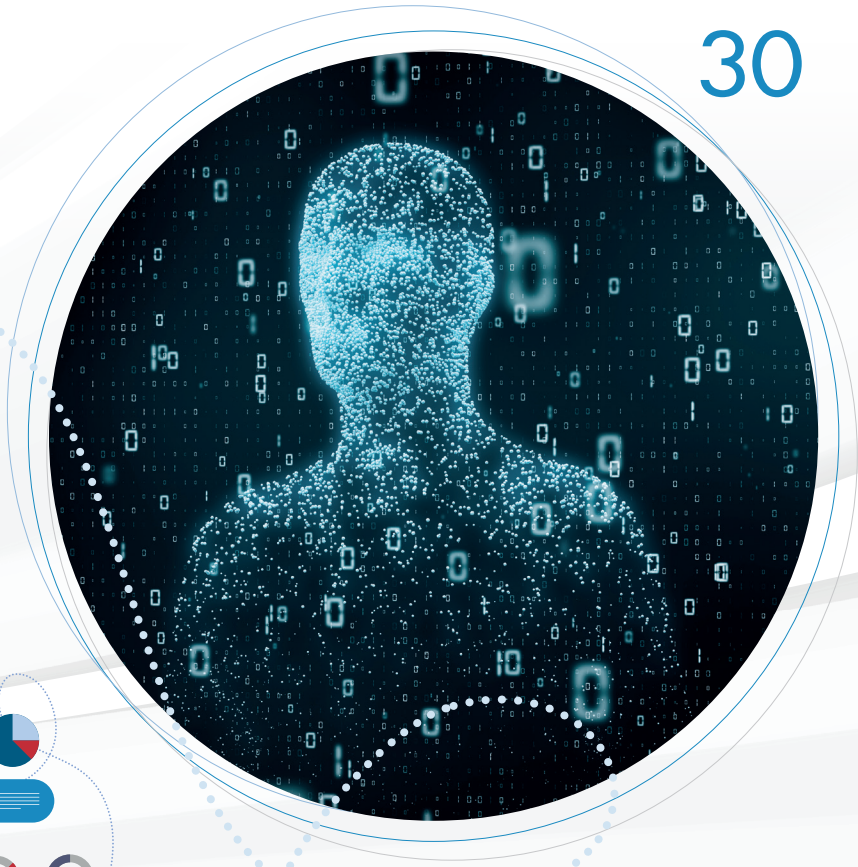
26 **Bürokultur neu gedacht**
Das Büro muss technologisch attraktiver werden

29 **Weniger ist mehr**
Trends in Dokumentenmanagement und Archivierung

30 **KI & Marketing**
Das personalisierte Kundenerlebnis optimieren

32 **Hybride Arbeitsmodelle sind die Zukunft**
Cloudbasierte Kommunikation und UCaaS

8
COVERSTORY



30

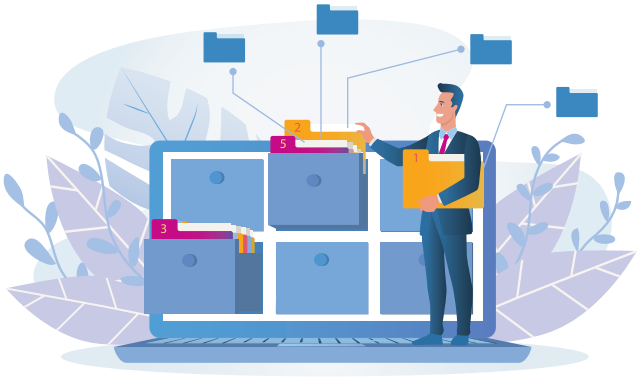
26

Inklusive
32 Seiten

IT SECURITY SPEZIAL

DATABASE AS A SERVICE

AGIL UND KUNDENFREUNDLICH



Software as a Service (SaaS) ist eine Form der Bereitstellung von Anwendungen, die sich sowohl im Consumer-Bereich als auch in Unternehmen immer stärker durchsetzt. Die Vorteile von Database as a Service, als einer spezifischen professionellen SaaS-Anwendung, können unter die beiden Themenfelder technische Vorteile und Kostenaspekte subsumiert werden.

1. **Automatisierung und Management:** DBaaS entlastet die interne IT-Abteilung von einer Fülle von Routineaufgaben. Datenbank-Administratoren benötigen im Schnitt nur noch ein Fünftel des bisherigen Aufwands für Implementierung und Betrieb. Zudem erleichtert DBaaS die Automatisierung von IT-Aufgaben und -Funktionen, beispielsweise in Multi-Cloud-Szenarien oder hybriden Umgebungen.

2. **Flexibilität und Skalierung:** DBaaS ist hochskalierbar. Zusätzliche Datenbankinstanzen sind quasi in Echtzeit verfügbar, wenn sie beispielsweise für Lastspitzen benötigt werden, und können anschließend ebenso rasch wieder heruntergefahren werden. Auch hier werden kaum Admin-Eingriffe benötigt, die Skalierung erfolgt in der Regel automatisch.

3. **Transparente Kostenrechnung:** You pay what you get. Nach diesem Prinzip zahlen Kunden zeitgenau nur für die tatsächliche Nutzung von Datenbankinstanzen und haben so jederzeit 100-prozentige Transparenz über ihre Kosten. Sie spiegeln damit den realen Bedarf und können jederzeit an veränderte betriebliche Belange angepasst werden.

4. **Audit-Sicherheit:** Mit DBaaS sind die Zeiten von Unter- oder Überlizensierungsproblemen vorbei, da die Software-Lizenzen nach Nutzung abgerechnet werden. Damit entfallen auch die nervigen, oft genug teuren Auditierungsverfahren durch den Hersteller.

5. **Kostenvorteile:** Diese Aufwendungen für die Datenbanknutzung werden nicht wie On-premises-Lizenzen als Investitionsgüter (Capex) sondern als Betriebskosten (Opex) abgerechnet, laufen so als operative Ausgaben in die Gewinn- und Verlustrechnung ein und können steuerlich geltend gemacht werden.

www.couchbase.com

BLOCKCHAIN

WARUM SICH CIOS DAFÜR INTERESSIEREN SOLLTEN

Nicht nur durch die Pandemie stehen CIOs unter Druck, innovative Technologien gewinnbringend einzusetzen. Das sind die Hauptgründe, warum sich CIOs mit dem Thema Blockchain und den damit verbundenen Möglichkeiten beschäftigen sollten:

1. Die digitale Infrastruktur wird Blockchain-Fähigkeiten benötigen

2. Mit einer Blockchain-gestützten Daten- und Vertrauensstruktur lassen sich Daten monetarisieren

3. Sie ermöglicht es, mit maschinellen „Kunden" in Kontakt zu treten und Transaktionen durchzuführen

4. Mit Blockchain können Geldbörsen programmiert und Geschäftsmodelle umgestaltet werden

5. Die Dezentralisierung der Blockchain ermöglicht die Entwicklung neuer Modelle für die Verwaltung von Ökosystemen

www.gartner.com

DIE ZUKUNFT DER ARBEIT

SPALTUNG VON FÜHRUNGSKRÄFTEN UND MITARBEITERN?

NTT Ltd, hat die 2021er-Ausgabe seines Global Workplace Report veröffentlicht. Die Studie liefert detaillierte Informationen zu den Bereichen Employee Experience – also den Erfahrungen der Mitarbeiter an ihrem Arbeitsplatz –, vernetzte Digitalisierung sowie Arbeitsplatzgestaltung und bietet damit wichtige Gestaltungsansätze für die Zukunft der Arbeit, auf die sich Unternehmen auf der ganzen Welt nach der Pandemie einstellen müssen.

Die Daten zeigen, dass die meisten Organisationen zwar erkannt haben, welche Maßnahmen sie für die Modernisierung ihrer Arbeitsmodelle in den einzelnen Sektoren priorisieren müssen, viele sind aber noch nicht in der Lage, diese effektiv umzusetzen.

Remote-Arbeit beeinträchtigt die Unternehmensleistung

Die Befragung von weltweit 1.146 leitenden Angestellten sowie 1.400 Mitarbeitern belegt, dass eine Mehrheit der Befragten die während der Pandemie erfolgte Zunahme von Remote-Arbeit kritisch beurteilt. 74 Prozent sehen dadurch die Unternehmensleistung beeinträchtigt und 76 Prozent bezeichnen Homeoffice als Herausforderung für die Angestellten.

Und für 60 Prozent der Personalchefs hat sich das Wohlbefinden der Mitarbeiter im Laufe der Pandemie verschlechtert.

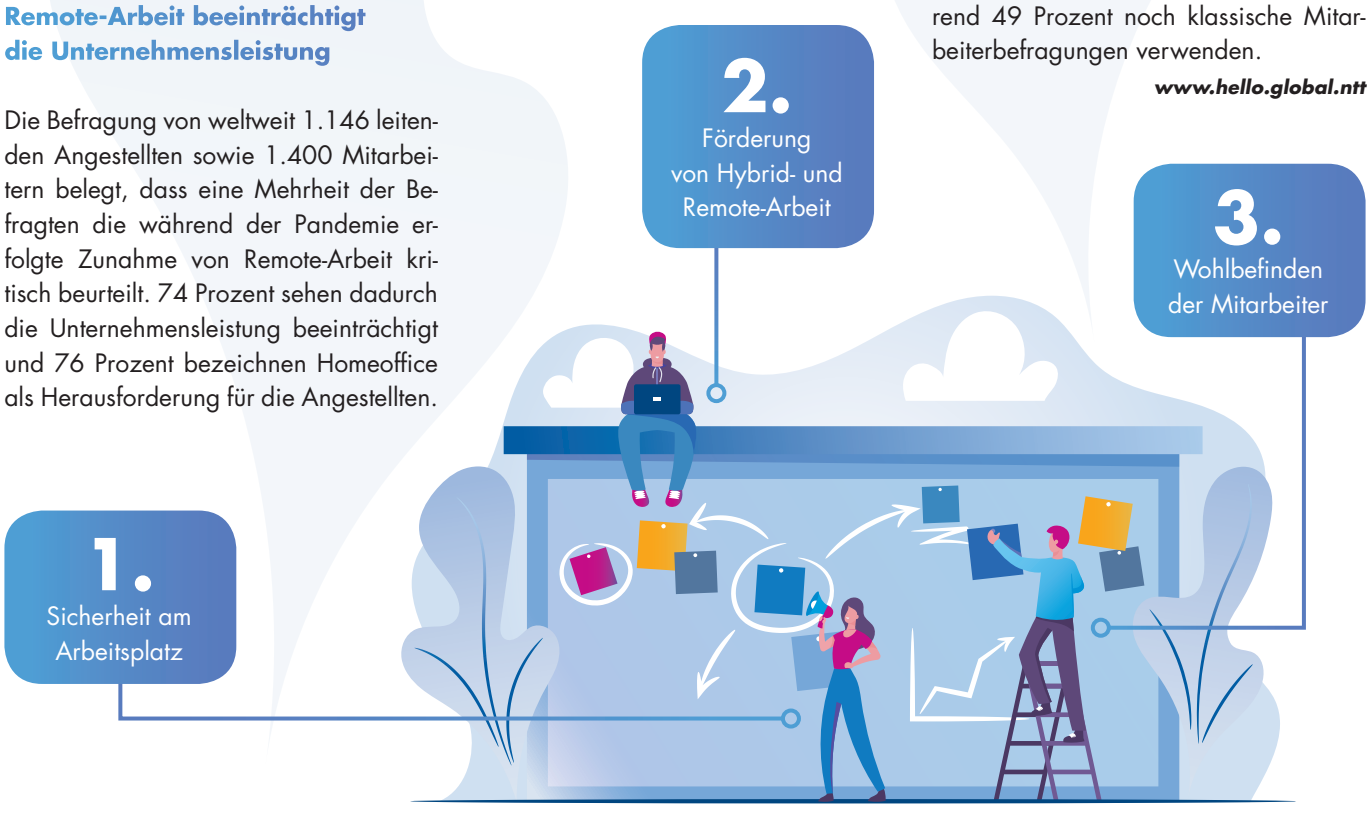
Arbeitsmodelle müssen hybrid, flexibel und sicher sein

Neben der Diskrepanz zwischen Arbeitgebern und Belegschaft bei der Einschätzung der Employee Experience zeigt die Studie auch erhebliche Unterschiede in der Einstellung der Beschäftigten zu ihren persönlichen Arbeitsvorlieben. Demnach bevorzugen Arbeitnehmer, wenn sie die Wahl zwischen Homeoffice, hybrider Arbeit und Arbeit im Büro haben, diese Optionen zu fast gleichmäßigen Teilen. Dieses Ergebnis steht im Widerspruch zu der in der Studie von 73 Prozent der Unternehmen vertretenen Ansicht, dass Mitarbeiter lieber im Homeoffice arbeiten.

Employee Experience als Basis für unternehmerisches Handeln

Die Studie zeigt auch, dass in Unternehmen, die bereits zusammen mit der Belegschaft entwickelte Arbeitsplatzstrategien anwenden, die Zufriedenheit der Mitarbeiter mit der Employee Experience auf das Doppelte ansteigt. Es ist also für Organisationen besonders wichtig, dass sie ihr unternehmerisches Handeln auf Basis gesicherter Einschätzungen der Mitarbeiter ausrichten. Doch davon sind die Unternehmen noch weit entfernt: Daten aus strukturierten Mitarbeiterbefragungen nach der Voice-of-Employee-Methode (VoE) und aus Arbeitsplatzanalysen priorisieren Unternehmen jeweils nur zu etwa 44 Prozent. Und lediglich 37 Prozent der Organisationen nutzen strukturierte VoE-Programme und 37 Prozent Echtzeit-Stimmungsanalysen tatsächlich, während 49 Prozent noch klassische Mitarbeiterbefragungen verwenden.

www.hello.global.ntt



Top-Prioritäten für den Arbeitsplatz

PARTNERSCHAFT MIT ZUKUNFT

INNOVATIVE VERÄNDERUNGEN FÜR EINE MODERNE UND FLEXIBLE ARBEITSWELT

> WIR HABEN GELERNT, DASS DIE AKZEPTANZ FÜR VIRTUELLE ZUSAMMENKÜNFTE UMSO GRÖSSER IST, JE MEHR ZWISCHENMENSCHLICHE INTERAKTION MÖGLICH IST. DESHALB HABEN WIR DAS PROJEKT „MICROSOFT MESH" AUFGESETZT.
>
> Marianne Janik, vorsitzende Geschäftsführerein, Microsoft Deutschland, www.microsoft.com

Die Digitalisierung hat eine Vielzahl von Partnerschaften hervorgebracht – so auch eine Kooperation zwischen Microsoft und der Deutschen Telekom. Die vorsitzende Geschäftsführerin von Microsoft Deutschland, Marianne Janik, und der Leiter des Bereichs Portfolio und Produktmanagement bei der Deutschen Telekom, Peter Arbitter, stellten sich den Fragen von Ulrich Parthier, Herausgeber it management.

Ulrich Parthier: *Digitalisierung und Corona. Wie hat das rückblickend auf die letzten knapp zwei Jahre zusammengepasst?*

Peter Arbitter: Sehr gut! Die Digitalisierung hat es der Wirtschaft ermöglicht, im Zeitraffertempo Home-Office zu etablieren, und für viele Unternehmen waren Digitallösungen die Rettung im Lockdown. Die Frage lautet nun: Wie geht es weiter? Allen ist klar, dass der Digitalisierungsschub der letzten zwei Jahre nicht als Strohfeuer enden darf. Die großen IT-Anbieter sind aufgerufen, neue Angebote für Unternehmen und für deren Kunden zu entwickeln, damit der Digitalisierungsprozess in Deutschland in hohem Tempo weitergeht.

Ulrich Parthier: *Frau Janik, Videokonferenzen waren in der Pandemie das Kommunikationsmittel Nummer 1. Egal ob in Unternehmen, Behörden, Haushalten oder Schulen. Kann man Software wie Microsoft Teams als eine Art digitalen Kitt ansehen, der die Kommunikation und damit den Kontakt am Laufen gehalten hat? Was haben Sie, was sollten wir daraus gelernt haben?*

Marianne Janik: Wir haben vor allem gelernt, dass bei entsprechendem Engagement Dinge möglich sind, die man zuvor für unmöglich gehalten hat. Einige unserer Kunden haben zum Beispiel fast über Nacht ihre Kommunikation auf Microsoft Teams umgestellt. Des Weiteren haben wir gelernt, dass wir als Technologiekonzern eine wichtige Vorbildfunktion für die Wirtschaft haben: Viele Unternehmen wollten von uns wissen, wie man Remote Work am besten umsetzt und wie Mitarbeiterführung ohne Präsenzmeetings gelingen kann. Da wissen wir sehr gut Bescheid; schließlich setzt Microsoft seit 1998 auf Vertrauensarbeitszeit und seit 2014 auf freie Wahl des Arbeitsortes. Ohne Partner wäre es uns aber nicht möglich gewesen, diese Vorbildfunktion zu erfüllen. Nur dank der Zusammenarbeit mit Konzernen wie der Deutschen Telekom können wir der Wirtschaft zeigen, was machbar ist.

Ulrich Parthier: *Partnerschaft ist ein gutes Stichwort. Herr Arbitter, was hat sich in der Digitalisierung für Sie in den letzten eineinhalb Jahren verändert, und wie hat sich das auf die Partnerschaft mit Microsoft ausgewirkt?*

Peter Arbitter: Nun ja, in erster Linie hat sich die Geschwindigkeit des digitalen Wandels erhöht. Die Unternehmen haben die Vorzüge von digitalen Kommunikationstools kennengelernt, und jetzt möchten sie, dass diese Tools möglichst schnell überall zum Einsatz kommen. Was die Partnerschaft zwischen Microsoft und der Deutschen Telekom angeht: Die ist noch fruchtbarer geworden. Wir haben gemeinsam einige Produkte entwickelt, mit denen wir noch besser als bisher auf die Kundenbedürfnisse in der heutigen Arbeitswelt eingehen können.

Ulrich Parthier: *Können Sie Beispiele nennen?*

Marianne Janik: Da ist zum einen die Bündelung von Microsoft Teams mit den Anschlussprodukten der Deutschen Telekom, genannt „Connectivity+". Außerdem haben wir maßgeschneiderte Managed Services rund um das Produktportfolio von Microsoft im Programm, und dann gibt es da noch das Express Route Offering von der Deutschen Telekom, mit dem Kunden einen sehr sicheren Zugriff auf Softwareprodukte von Microsoft haben.

Ulrich Parthier: *Schauen wir doch mal etwas konkreter auf diese Lösungen und auf die enge Kooperation, die angesprochen wurde. Herr Arbitter, Sie bieten als erster deutscher Partner von Microsoft ein neues Voice-Produkt an, dass sich „Operator Connect" nennt. Was steckt dahinter, und wem nützt es?*

> DIE DIGITALISIERUNG ERMÖGLICHTE ES DER WIRTSCHAFT, IM ZEITRAFFERTEMPO HOME-OFFICE ZU ETABLIEREN, UND FÜR VIELE UNTERNEHMEN WAREN DIGITALLÖSUNGEN DIE RETTUNG IM LOCKDOWN.
>
> Peter Arbitter, Leiter Bereich Portfolio- und Produktmanagement, Deutsche Telekom, www.telekom.com

Peter Arbitter: Mit „Operator Connect" bringen wir die Microsoft-Teams-Welt mit der Telefonie der Deutschen Telekom zusammen. Der Kunde erhält ein All-in-one-Kommunikationspaket: eingehende Anrufe, egal ob aus dem Fest- oder aus dem Mobilfunknetz, werden in das Teams-Programm integriert, und auch beim Anrufen aus Teams heraus kann das Mobiltelefon einbezogen werden. Faxgeräte, digitale Alarmanlagen, Aufzugüberwachung lassen sich ebenfalls einbinden. „Operator Connect" liefert also alles aus einer Hand.

Ulrich Parthier: *Frau Janik, das worüber Herr Arbitter gerade gesprochen hat, ist ja nur ein Beispiel für eine moderne, hybride Arbeitswelt. Ganz neu ist jetzt eine Lösung, die ich mal als „Cloud-PC" beschreiben könnte, also einen kompletten Rechner aus der Wolke. Sollte ich jetzt meinen Desktop-Computer oder Laptop einfach in die Schublade stecken oder verschenken?*

Marianne Janik: Nein, denn um ihren Cloud-PC nutzen zu können, brauchen Sie immer ein Endgerät. Das kann allerdings auch das Smartphone sein. Die Innovation bei diesem „Cloud-PC" – den wir „Windows 365" nennen – besteht darin, dass das komplette Betriebssystem samt Anwendungen und Daten nicht mehr auf dem Firmenserver liegt, sondern in der Cloud. Entsprechend ist alles jederzeit und von jedem Ort der Welt aus zugänglich; man braucht dazu nur ein Endgerät und Internetempfang. Angestellte können so auch ohne vorkonfigurierten Firmenlaptop im Homeoffice auf ihren digitalen Arbeitsplatz zugreifen. Viele Kunden, insbesondere kleinere Unternehmen, hatten sich so eine Lösung gewünscht. Im Internet gibt es ein Video dazu, das das System gut erklärt.

Ulrich Parthier: *Ich habe das Video gesehen. Interessant ist, dass es ja erst mal gar nicht so anders aussieht als am eigenen Laptop. Was genau unterscheidet denn Windows 365 von einem klassischen PC oder Laptop?*

Marianne Janik: Für den einzelnen Nutzer im Grunde nichts – er kann seinen Cloud-PC wie ein physisches Gerät nach seinen Bedürfnissen konfigurieren. Rechenleistung, Arbeitsspeicher: Alles lässt sich einstellen, genau wie beim Kauf eines PCs im Einzelhandel. Im Gegensatz zu anderen cloudbasierten Lösungen erfordert Windows 365 nicht einmal besondere Vorkenntnisse. Für IT-Abteilungen unterscheidet Windows 365 sich von physischen PCs dahingehend, dass die Bereitstellung und die Verwaltung deutlich einfacher sind.

Ulrich Parthier: *Herr Arbitter, Sie sind für das Portfoliomanagement der Deutschen Telekom zuständig und immer auf der Suche nach Innovationen. Haben Sie den Cloud-PC schon getestet?*

Peter Arbitter: Natürlich. Die Branche versucht sich ja schon seit Jahrzehnten an Thin-Client-Konzepten, aber bisher gab es da wenig Überzeugendes. Entweder war die zentrale Hardware zu teuer, oder die Clients waren dann doch nicht so „thin", wie es dargestellt wurde. Bei Windows 365 ist das anders. Das System läuft auf Azure und auf allen Formfaktoren, sodass keine teuren Clients nötig sind.

Ulrich Parthier: *Vielleicht noch ein kleiner Blick nach vorne: Was sehen Sie beide beim Blick in die Glaskugel als weitere innovative Veränderungen für eine moderne und flexible Arbeitswelt? Ich fange mal mit Herrn Arbitter an – what's next?*

Peter Arbitter: Wir erwarten deutlich stärkere Rechnerleistungen, die es uns erlauben, noch mehr Realtime-Services anzubieten – wie beispielsweise digitales Simultan-Übersetzen. So etwas gibt es bereits und wird in naher Zukunft breitflächig zur Anwendung kommen.

Ulrich Parthier: *Und wie sieht die Zukunft aus Microsoft-Sicht aus?*

Marianne Janik: Ich hatte ja anfangs schon erwähnt, dass wir in der Pandemie viel gelernt haben. Unter anderem, dass die Akzeptanz für virtuelle Zusammenkünfte umso größer ist, je mehr zwischenmenschliche Interaktion möglich ist. Deshalb haben wir das Projekt „Microsoft Mesh" aufgesetzt. Hierbei handelt es sich um eine Mixed-Reality-Plattform, die Nutzerinnen und Nutzern durch Hologramme das Gefühl gibt, zusammen am selben Ort zu sein. Wir verbinden also die physische und die digitale Welt noch enger miteinander. Die nötige Technologie dazu existiert bereits.

Ulrich Parthier: *Ich danke Ihnen beiden ganz herzlich für dieses Gespräch!*

CONTAINERISIERUNG

VON TECHNOLOGIE PROFITIEREN

Unternehmen sind ständig hin- und hergerissen zwischen technologischen Veränderungen, die neue Geschäftsmöglichkeiten erschließen sollen, und dem Schutz des Unternehmens vor neuen Problemen und Risiken.

In den letzten 20 Jahren hat die Virtualisierung das Server-Computing verändert, indem sie die Ausführung mehrerer separater Betriebssysteme auf einer Hardwareplattform ermöglicht hat. Ein zeitgemäßer Ansatz ist die Containerisierung, die es ermöglicht, mehrere Anwendungen auf einer einzigen Instanz eines Host-Betriebssystems auszuführen.

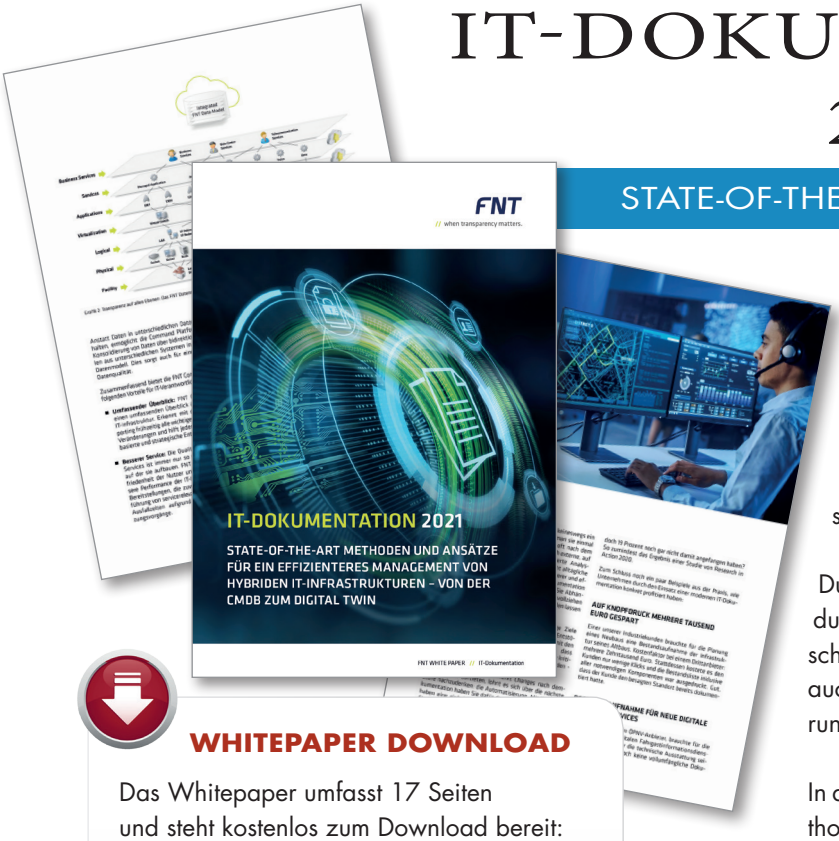
In diesem Whitepaper untersuchen wir die Containerisierung und sehen uns an, wie IT-Experten, Systemarchitekten und Entscheider in Unternehmen von dieser Technologie profitieren.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 11 Seiten und steht kostenlos zum Download bereit:
www.it-daily.net/download

IT-DOKUMENTATION 2021

STATE-OF-THE-ART METHODEN UND ANSÄTZE



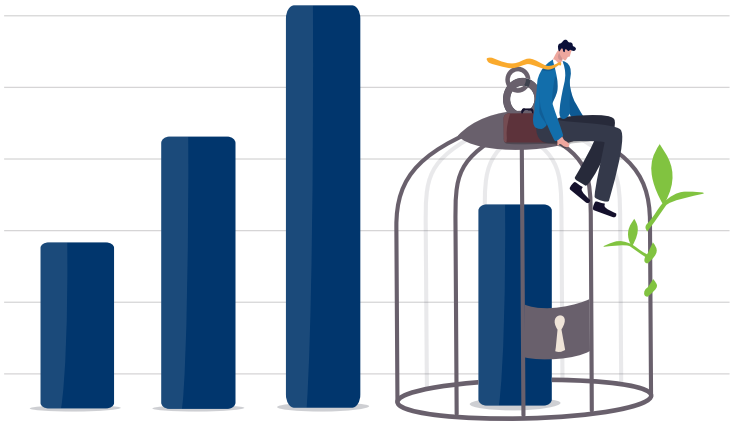
WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 17 Seiten und steht kostenlos zum Download bereit:
www.it-daily.net/download

Die Dokumentation der vorhandenen IT-, Telekommunikations- und Rechenzentrumsinfrastrukturen wird oft als lästiges Übel betrachtet. Dabei bieten moderne Tools eine Vielzahl neue Möglichkeiten, die eigenen Infrastrukturen effizienter zu managen – ohne ausufernden Pflegeaufwand oder ständig veralteter Informationen.

Durch intelligente Automatisierung und Prozesseinbindung schafft man nicht nur die Basis für bessere Entscheidungen und schlankere Abläufe, sondern legt auch den Grundstein für weitergehende Automatisierungsinitiativen in der IT.

In diesem Whitepaper erwarten Sie State-of-the-Art Methoden und Ansätze für ein effizienteres Management von hybriden IT-Infrastrukturen – von der CMDB zum digital Twin.



MICROSOFT-CSP-PROGRAMM

WIE DER SOFTWARE-GIGANT DIE FLEXIBILITÄT ABSCHAFFT

Die Ankündigung drastischer Änderungen bei der Microsoft-Cloud-Lizenzierung erhitzt zurzeit die Gemüter in den IT-Abteilungen. Zum einen erhöht der Hersteller für seine sechs wichtigsten Online-Pläne die Lizenzgebühren. Zum anderen streicht er ab 1. März 2022 die flexible Kündigung innerhalb der Vertragslaufzeit sowie den Preisschutz für Monats-Abos. Björn Orth, CEO des Microsoft Gold Partners VENDOSOFT berichtete in der letzten Ausgabe, wie Unternehmen die Preiserhöhung abfedern können. Wie Firmen mit den weiteren Einschnitten verfahren, darum soll es in diesem Beitrag gehen.

Wenn Björn Orth und sein Team dieser Tage mit ihren CSP-Kunden telefonieren, ernten sie viel Unverständnis. Unternehmen erwarten von ihrem Lizenzberater Antworten, wie mit den Anpassungen der CSP-Programme umzugehen ist. Doch Fakt ist, dass Microsoft zwar fröhlich seine Preiserhöhungen und Lizenzeinschränkungen kommuniziert. Dass diese den meisten Firmenkunden wie Daumenschrauben vorkommen müssen, thematisiert der Hersteller jedoch nicht. Auch kann zum jetzigen Zeitpunkt kein CSP-Provider Empfehlungen für den notwendigen Umstieg aussprechen. Microsoft stellt für die beiden Monate vor Inkrafttreten der Änderungen – also von Januar bis März 2022 – sogenannte Promotion-Aktionen in Aussicht. Wer dann neue Verträge abschließt, soll noch für eine begrenzte Zeit von besseren Konditionen profitieren, beispielsweise einer längeren Preisbindung für seine Monats-Abos. Doch konkret wird Microsoft bei diesem Thema nicht.

Preiserhöhungen

Björn Orth ärgert diese Vorgehensweise. „Wenige Wochen, bevor wir für unsere Kunden entscheiden müssen, welche Lizenzierung die Beste wäre, sind nicht einmal wir als Microsoft Partner ausreichend informiert!“ Für ihn ist unverständlich, wie der Hersteller hier taktiert. „Eine Beratung unserer vielen CSP-Kunden zum jetzigen Zeitpunkt wäre wünschenswert, schon um der Verunsicherung entgegenzuwirken, die sich breitmacht.“ Wenn eine Office 365 E5-Lizenz plötzlich 6,80 Euro mehr kostet (bei Monats-SKUs sogar 15 Euro mehr!), werden Kunden zu Recht nervös. Schnell schlagen die Preiserhöhungen mit einigen Zehntausend Euro in den IT-Budgets zu Buche. Pro Jahr!

Lizenzeinschränkungen

Auf einem ganz anderen Blatt stehen die vertragsrechtlichen Änderungen. Was Microsoft unter dem klangvollen Namen New Commerce Experience (NCE) anpreist, reduziert der Lizenzexperte Orth auf das, was es ist: „Statt flexibler Skalierung des Lizenzbestands gibt es nun starre jährliche Vertragsmodelle ohne Anpassungsmöglichkeit an den eigentlichen Bedarf.“ Ab März 2022 wird eine tagesgenaue Abrechnung monatlicher Lizenzen um 20 Prozent teurer. Damit nicht genug, wird auch die einjährige Preisbindung für Monats-Abos aufgehoben. Erhöht Microsoft zukünftig die Gebühren für Monats-SKUs, gelten sie ab dem Folgemonat. So und ähnlich geht es weiter. Wer fälschlicherweise SKUs einbucht, hat 72 Stunden, um seinen Fehler zu korrigieren. Danach endet die Stornierungsfrist und die Lizenzen sind der Vertragslaufzeit von einem Jahr unterlegen.

Das limitiert den Spielraum für Unternehmen, die ihre Microsoft-Anwendungen in der Cloud haben. Deshalb rät der Lizenzprofi Björn Orth: „Fragen Sie sich, für welche User Sie die Flexibilität der Monats-SKUs benötigen und für welche On-Premises-Lizenzen ausreichen. Wir helfen Ihnen bei der Entscheidung!“

DIE WICHTIGSTEN FAKTEN

zum geänderten Microsoft-CSP-Programm unter:
www.vendosoft.de/csp-aenderungen/

HYPERKONVERGENTE INFRASTRUKTUREN

WELCHEN UNTERNEHMEN SIE HELFEN KÖNNEN UND WORAUF BEI DER AUSWAHL DES RICHTIGEN ANBIETERS ZU ACHTEN IST

ENTSCHEIDEND FÜR DIE EFFEKTIVE NUTZUNG HYPERKONVERGENTER INFRASTRUKTUREN IST DIE PLATTFORM, DIE DIESE VERWALTET.

Xavier Gonzalez, Vice President Corporate Communication, Cyxtera, www.cyxtera.com

Der weiträumige Wechsel ins Home Office und der damit gestiegene Bedarf an IT-Infrastrukturen hat die Kosten für sie in die Höhe schnellen lassen. Für mittelgroße Unternehmen sind die Kosten, die eigene Infrastruktur auszubauen, meist zu hoch. Außerdem mangelt es hier an Flexibilität, weil sie sich nicht an das eigene Geschäft anpassen lässt. Plattformen für Hyperkonvergente Infrastrukturen (HCIs) versprechen die Lösung dieser Herausforderungen. Worauf bei ihnen zu achten ist, klären wir im Folgenden.

Hyperkonvergente Infrastrukturen virtualisieren die gesamte Hardware eines Unternehmens und machen sie so für unterschiedliche Anwendungen skalierbar. Klassische IT-Infrastrukturen bestehen aus den drei Komponenten Storage, Compute und Netzwerk. Will man eine der drei Komponenten erweitern, müssen auch die anderen beiden in den meisten Fällen mitziehen. Insbesondere Storage-Erweiterungen sind hierbei teuer. Plattformen für HCIs können die Kosten hierbei im Rahmen halten und Leistung schnell und skalierbar zur Verfügung stellen.

Die Vorteile von HCIs

HCIs und die Plattformen, die sie verwalten, versprechen hinzuschaltbare Ressourcen innerhalb weniger Mausklicks. Um dies bewerkstelligen zu können, müssen alle Komponenten der IT-Infrastruktur virtualisier- und managebar sein. Ist dies gegeben, kann die Plattform alle Ressourcen zentral aufzeigen und verwalten. Benötigt eine Anwendung beziehungsweise ein Projekt zusätzliche Ressourcen, können diese über die Plattform hinzugefügt werden.

Mittlerweile gibt es unzählige Anbieter von Plattformen, die HCIs für Unternehmen verfügbar machen. Neben der bestehenden Hardware im eigenen Rechenzentrum können Organisationen zudem, je nach Bedarf, auf IaaS-Anbieter zurückgreifen und deren Infrastrukturen in die eigene integrieren.

Sind die unternehmensinternen Infrastrukturen mit HCI-Plattformen kompatibel, können IT-Verantwortliche die Vorteile von HCIs gegenüber klassischen Modellen ausspielen. Dazu zählen:

1 Skalierung per Mausklick

IT-Verantwortliche können bei HCIs die Leistung für Projekte hinzu- und, sobald das Projekt abgeschlossen wurde, wieder abbuchen. Insbesondere das Hinzufügen physischer Infrastrukturen im eigenen Rechenzentrum weist nicht den gleichen Grad an Skalierbarkeit auf, da Einbau und Verbindung mit dem Netzwerk langwieriger sind als sie virtuell per Mausklick hinzuzufügen.

Hinzukommt: Ist das Projekt beendet, hat man mitunter viel Geld für neue Hardware ausgegeben, die nun aber erst einmal nicht mehr benötigt wird, aber trotzdem laufende Kosten verursacht. Bei Plattformen für HCIs können überflüssige Ressourcen einfach abgebucht werden.

2 Schnelligkeit für's Projekt

Projektabteilungen benötigen bei Beginn einer neuen Aufgabe schnellen Zugriff auf IT-Infrastrukturen. Nur so können Unternehmen gewährleisten, wettbewerbsfähig zu bleiben. Zudem sind die Zeitrahmen für solche Projekte oft knapp bemessen, je schneller das Team auf benötigte Ressourcen zugreifen kann, desto schneller kann es mit der Arbeit beginnen. HCIs können innerhalb weniger Stunden bereitstehen, während die Implementierung von Hardware oft Wochen, wenn nicht Monate dauert.

Ist die gesamte unternehmensinterne Infrastruktur Teil einer HCI, lassen sich zudem Hardware-Upgrades leichter vollziehen: In der Plattform wird die auszuwechselnde Komponente zuerst virtuell herausgenommen bevor sie dann physisch entfernt wird.

3 Lizenzoptimierung

Sobald Unternehmen ihre eigenen IT-Infrastrukturen erweitern, kommen zusätzlich zum logistischen und technischen Aufwand auch Lizenzfragen hinzu, die für ihren Betrieb notwendig sind. Eine Erweiterung von Compute-Ressourcen zieht in den meisten Fällen auch zusätzliche Network- und Storage-Erweiterungen mit sich – und somit insgesamt drei Lizenzen.

Bei HCIs hingegen kommt bei einer Erweiterung nur eine Lizenz hinzu. Darüber hinaus müssen Unternehmen Lizenzen für Infrastrukturen nicht im Vorhinein kaufen, sondern können je nach sie nach Bedarf erwerben.

Worauf Entscheider achten müssen

Entscheidend für die effektive Nutzung hyperkonvergenter Infrastrukturen ist die Plattform, die diese verwaltet. HCIs sind zwar herstellerunabhängig, sie benötigen aber eine Plattform für die zentrale Übersicht und Bereitstellung der einzelnen HCI-Komponenten.

IT-Infrastrukturen in Unternehmen sind keine homogenen Gebilde sondern über die Jahre gewachsen. Sie sind in der Regel eine Mischung aus Private-, Public- und On-Premises-Lösungen, die sich mal in unterschiedlichen, mal im selben Rechenzentrum befinden. Eine gute Plattform für das Management von IT-Infrastrukturen sollte all diese Lösungen, zentral managen und verfügbar machen können. Auch bestehende Hardware sollte in sie integrierbar sein, dafür muss sie natürlich vollständig virtualisierbar und somit per Plattform managebar ist.

Die Integration bestehender Infrastrukturen in die HCI-Plattform findet vor Ort statt. Der Plattformbetreiber integriert ein eigenes Patch-Panel in das Rack, das eingebunden werden soll, und ermöglicht so die Kommunikation mit der Plattform. Alle Komponenten sind nun virtualisiert und als Teil der hyperkonvergenten Infrastruktur nutzbar, je nachdem, wo gerade Bedarf besteht.

Für wen kommen HCIs infrage?

Insbesondere der Mittelstand kann bei Projekten mit unterschiedlichen Anforderungen an die IT-Ressourcen von HCI-Modellen profitieren.

Hier kommt mittelständischen Unternehmen insbesondere die Flexibilität der HCIs zugute. Bieten hybride Cloud-Umgebungen aus Private und Public Cloud ein ähnliches Maß an Agilität und Skalierbarkeit, haben sie doch einen höheren Verwaltungsaufwand und sind in vielen Fällen mit größeren Investitionen verbunden.

Gerade der erste Punkt kann schon für mittlere Unternehmen kritisch sein, denn sie verfügen oft nur über kleine IT-Teams und geringe eigene Ressourcen. Eine Plattform, die HCIs verwaltet, kommt diesen entgegen: Das Management bestehender und neu hinzukommender Infrastrukturen lässt sich zentral steuern, dadurch kann sich das IT-Team um wichtigere Dinge als die Implementierung und Wartung von eigenen Servern kümmern. Auch die Nutzung separater Lösungen für das Management von Servern, Speichern und Speichernetzwerken entfällt.

Fazit

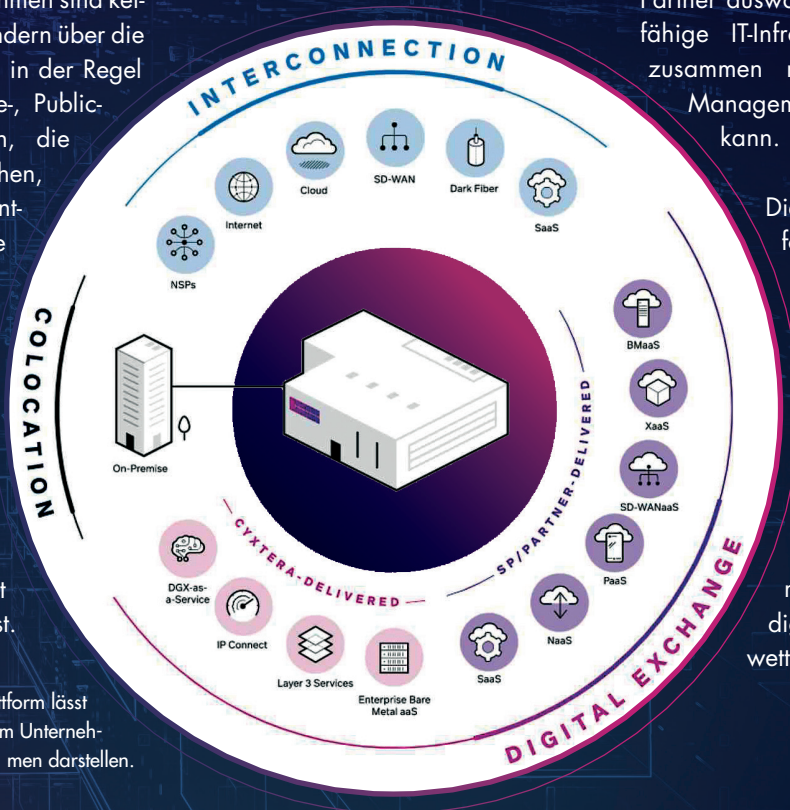
Eigene Infrastrukturen zu virtualisieren und in eine HCI einzubetten, kann insbesondere mittelständischen Unternehmen die Agilität und Skalierbarkeit verschaffen, die sie für ihre Projekte benötigen.

Mit der richtigen Management-Plattform lassen sich zudem, je nach Projektgröße und -anforderungen weitere Cloud-Ressourcen nutzen. Unternehmen müssen sich somit nicht mit der Erweiterung des eigenen Rechenzentrums beschäftigen, sondern können auf das Know-how von IaaS-Anbietern zurückgreifen.

Beispielsweise sollten sie einen Anbieter von Rechenzentrumsdienstleistungen als Partner auswählen, der ihnen leistungsfähige IT-Infrastruktur im HCI-Modell zusammen mit der entsprechenden Management-Plattform bereitstellen kann.

Die softwaredefinierte Plattform von Cyxtera beispielsweise und das hochgradig vernetzte Ökosystem ermöglichen die bedarfsgerechte Bereitstellung von Inhouse- und Partnerlösungen und bieten mittelständischen Unternehmen die Grundlage, um ihre IT-Infrastruktur zu modernisieren und in der digitalen Welt von heute wettbewerbsfähig zu sein.

Xavier Gonzalez



Mit der richtigen Plattform lässt sich die gesamte Infrastruktur im Unternehmen darstellen.

DIGITALE SOUVERÄNITÄT

HABEN WIR NOCH EINE CHANCE AUF DIGITALE SELBSTBESTIMMUNG?

Über Jahre hinweg haben wir uns von der Software und den Services großer US-Hersteller abhängig gemacht. Preisdiktatur und Datenschutzprobleme sind die Folge. Auch Initiativen wie Gaia-X ändern daran wenig. Was können Unternehmen und Behörden tun, um digitale Souveränität zu gewinnen?

Vor Kurzem hat Microsoft eine Preiserhöhung für Office/Microsoft 365 angekündigt. 8 Prozent mehr müssen Kunden ab März 2022 für die Services berappen. Nur M365 E5 und die „F"-SKU-Produkte sind nicht betroffen. Microsoft möchte damit nach eigenen Angaben wirtschaftlich transparenter machen, dass E5 das beste Preis-Leistungs-Verhältnis bietet. Die Erhöhung verringere den Abstand zwischen M365 E3 und E5. Tatsächlich verbirgt sich hinter der Preispolitik nichts anderes als der vehemente Versuch, Kunden in den teuersten Abo-Plan zu drängen. Mancher wird vielleicht darauf reinfallen. Und dann? Kommt die nächste Preiserhöhung müssen alle die Kröte schlucken. Je mehr wir uns abhängig von wenigen großen Herstellern machen, desto stärker können sie die Daumenschrauben andrehen. Wer Microsoft Office einsetzt, kann oder will nicht plötzlich darauf verzichten. Zu viele Geschäftsprozesse und die digitale Zusammenarbeit hängen davon ab. Wie wichtig diese ist, hat die Corona-Krise gezeigt.

Es ist leicht, sich ködern zu lassen

Während des Lockdowns waren Unternehmen und Behörden auf Collaboration-Plattformen und Videokonferenz-Tools angewiesen, um die Geschäftskontinuität aufrechtzuerhalten. Microsoft nutzte dies als Chance, um Kunden für MS Teams anzufixen. Während der akuten Pandemie-Phase stellte der Anbieter seine App kostenlos mit unbegrenzter Besprechungsdauer zur professionellen Nutzung zur Verfügung. Auch viele Schulen wurden geködert, Teams und Office 365 einzusetzen – nicht ohne Kritik. Die Initiative „Digitale Souveräne Schule" konstatierte zum Beispiel, es sei höchst bedenklich, schon Kinder und Jugendliche über ihre gesamte Schulzeit hinweg mit dem immer gleichen digitalen Setting einer einzelnen Firma zu konfrontieren. Und bereits 2019 stellte das Beratungsunternehmen PWC in einer strategischen Marktanalyse im Auftrag des Bundesministeriums des Inneren fest, dass die digitale Souveränität

des Staates durch die starke Abhängigkeit von wenigen Software-Anbietern gefährdet sei. Sie empfahl daher dringend, Abhängigkeiten zu reduzieren. Aber was ist zwischenzeitlich passiert?

Die Cloud verstärkt die Abhängigkeit

Durch den zunehmenden Cloud-Einsatz ist die Abhängigkeit sogar noch größer geworden. Denn während Unternehmen ihre On-Premises-Lizenzen einmal bezahlen und dann unbegrenzt nutzen können, fallen in der Cloud kontinuierlich Gebühren an. Zahlt man sie nicht, stehen die Services nicht mehr zur Verfügung. Die Hersteller können also in gewisser Weise ihre Konditionen diktieren. Kein Wunder, dass viele Anbieter mittlerweile eine rigorose Cloud-Strategie verfolgen. Sie bieten neue Funktionen nur noch in ihren Cloud Services an oder stellen gar keine On-Premises-Versionen mehr bereit. Außerdem versuchen sie, Kunden mit Lock-Angeboten zum Wechsel in die Cloud zu bewegen. Dabei liegt der Teufel oft im Kleingedruckten. So knüpfte Microsoft im Jahr 2020 die vergünstigten Konditionen in seinen Lizenzbestimmungen „From SA" an die Bedingung, dass Kunden mit Software Assurance ihre On-Premises-Lizenzen auch weiterhin halten müssen. Unternehmen und Behörden waren also dazu gezwungen, ihr EU-Recht auf Weiterverkauf gebrauchter Lizenzen abzugeben. Erst nach fortwährender Kritik, unter anderem der Lizenzdirekt, hat Microsoft diese Regelung wieder zurückgenommen.

Datenschutz ist fragwürdig

Zu den finanziellen Knebelbedingungen kommen datenschutzrechtliche Bedenken hinzu, die mit den Cloud Services großer US-amerikanischer Anbieter verbunden sind. Selbst wenn diese ihre Rechenzenten in Europa betreiben, unterliegen sie immer noch dem CLOUD Act. Dieser Erlass, der unter Donald Trump 2018 verabschiedet wurde, verpflichtet amerikanische Unternehmen, Daten an die US-Behörden herauszugeben, unabhängig davon, in welchem Land sie sich befinden. Der CLOUD Act übertrumpft also bei Bedarf die DSGVO. Ein ungutes Gefühl bleibt selbst dann, wenn die US-Anbieter nur noch als Software-Lieferanten fungieren und den Betrieb ihrer Cloud Services europäischen Unternehmen überlassen. Mit einem solchen Angebot versucht Microsoft gerade die Bundesregierung zu ködern. Im Nachbarland Frankreich hat man sich bereits überzeugen lassen und wird künftig Office 365 nutzen – betrieben auf Servern der französischen Konzerne Orange und Capgemini. Aber was, wenn es einmal zu diplomatischen Spannungen zwischen Europa und den USA kommt? Wie unabhängig ist die vermeintlich souveräne Cloud dann noch? Durch Software-Updates könnten Hersteller jederzeit eine Hintertür einbauen, um Daten auszuspionieren. Es dürfte utopisch sein, den Quellcode der Updates vollständig zu kontrollieren.

Gaia-X wird unterwandert

Open Source-Angebote, die ihren Quellcode grundsätzlich offenlegen, scheinen da eine gute Alternative. Die Bemühungen, auf ihrer Basis eigene, europäische Cloud-Infrastrukturen aufzubauen, sind durchaus löblich. Erst vor Kurzem hat das Bundeswirtschaftssystem der Open Source Business Alliance (OSBA) eine Finanzspritze von 15 Millionen Euro zugesichert, um den Cloud Stack für das Projekt Gaia-X aufzubauen. Das war längst überfällig, wie Peter Ganten, Vorstandschef der OSBA, gegenüber der Süddeutschen Zeitung kommentierte: „Die Regierung hat erkannt, dass es hier ein Marktversagen gegeben hat." Zu denken geben sollte jedoch, dass mittlerweile auch die drei großen US-Hyperscaler Amazon, Google und Microsoft Mitglieder der Gaia-X-Allianz sind. Selbst der Big Data-Riese Palantir ist an Bord, obwohl er in der Kritik steht, eng mit Geheimdiensten wie der CIA und der NSA zusammenzuarbeiten.

Das Problembewusstsein schärfen

Dass selbst Initiativen wie Gaia-X bereits unterwandert sind, zeigt, wie wichtig es ist, auch vermeintlich digital souveräne Angebote kritisch zu hinterfragen und das Problembewusstsein zu schärfen. Unternehmen und Behörden sollten sich wieder darauf besinnen, was sie wirklich brauchen. Gerade im Bereich der Anwendersoftware klingen Cloud-Angebote oft verlockend, sind jedoch gar nicht erforderlich, um den tatsächlichen Bedarf zu decken. Denn meist nutzen Mitarbeiter für ihre tägliche Arbeit ohnehin nur einen Bruchteil der enthaltenen Funktionen. Hierfür reichen On-Premises-Versionen in der Regel aus und belassen die Datenhoheit beim Kunden. Auf dem Sekundärmarkt sind sie in Vorgänger- aber auch aktuellen Versionen erheblich günstiger zu erwerben. Mit gebrauchten Software-Lizenzen können Unternehmen und Behörden nicht nur viel Geld sparen, sondern auch ein Stück weit aus den monopolistisch geschlossenen Strukturen der Hersteller ausbrechen. Gleichzeitig ist die Politik gefragt, mehr ernstzunehmende Initiativen zur digitalen Souveränität voranzubringen. Indem Unternehmen und Behörden auf einen gesunden Mix aus gebrauchten Lizenzen und europakonformen Cloud Services setzen, können sie in eine digital selbstbestimmte Zukunft steuern.

Andreas E. Thyen

ES IST ENORM WICHTIG, AUCH VERMEINTLICH DIGITAL SOUVERÄNE ANGEBOTE KRITISCH ZU HINTERFRAGEN UND DAS PROBLEMBEWUSSTSEIN ZU SCHÄRFEN.

Andreas E. Thyen,
Präsident des Verwaltungsrats,
LizenzDirekt AG,
www.lizenzdirekt.com

NEW WORK

ERFOLGREICHE IMPLEMENTIERUNG DURCH MITARBEITERZENTRIERUNG

> UM NEW WORK UMZUSETZEN, HELFEN KLEINE SCHRITTE: DEFINIEREN SIE USE CASES UND PRÜFEN SIE, WELCHE ARBEITSFORMEN IHRE MITARBEITEN BRAUCHEN.
>
> Christian Schmid, Co-Lead Business Area Future Organisation, Campana & Schott, www.campana-schott.com

Im Rahmen von New Work stellen sich Unternehmen auch auf hybride Arbeitsweisen ein. Dazu zählt jedoch mehr als die richtige Technologie: Es geht darum, anhand konkreter Use Cases Anpassungsbedarfe zu evaluieren, damit die Mitarbeitenden optimal von den neuen Arbeitsformen profitieren.

Mit New Work gewinnen verschiedene Aspekte und Themen wie Homeoffice oder neue Collaboration-Tools, aber auch flexible Arbeitszeiten, diverse Teams und flache Hierarchien an Relevanz. Doch was bedeutet dies konkret für Business und IT – und wie erreicht man ein optimales Zusammenspiel der unterschiedlichen Facetten?

In erster Linie ist es wichtig, die Umsetzung im eigenen Unternehmen anhand konkreter Use Cases anzugehen. So kann schneller erkannt werden, wo eine Anpassung von Organisationsprozessen erforderlich ist, dass agile Arbeitsweisen einen immer wichtigeren Stellenwert haben und dass die Befähigung der Mitarbeitenden erfolgskritisch ist.

Dies erfordert neue Denk- und Arbeitsweisen in allen Bereichen, stellt jedoch eine enorme Herausforderung für Führungskräfte dar. Viele Führungskräfte wissen nicht, welche Stellhebel es gibt, damit die Mitarbeitenden und dadurch die gesamte Organisation optimal von New Work profitieren. Hier kann ein Blick in die IT-Abteilung helfen. Häufig wird hier schon seit Jahren remote und agil zusammen gearbeitet. Sie haben ihre Hard- und Software für die Fernarbeit angepasst und auch die Team-Strukturen auf hybride Kollaboration ausgelegt.

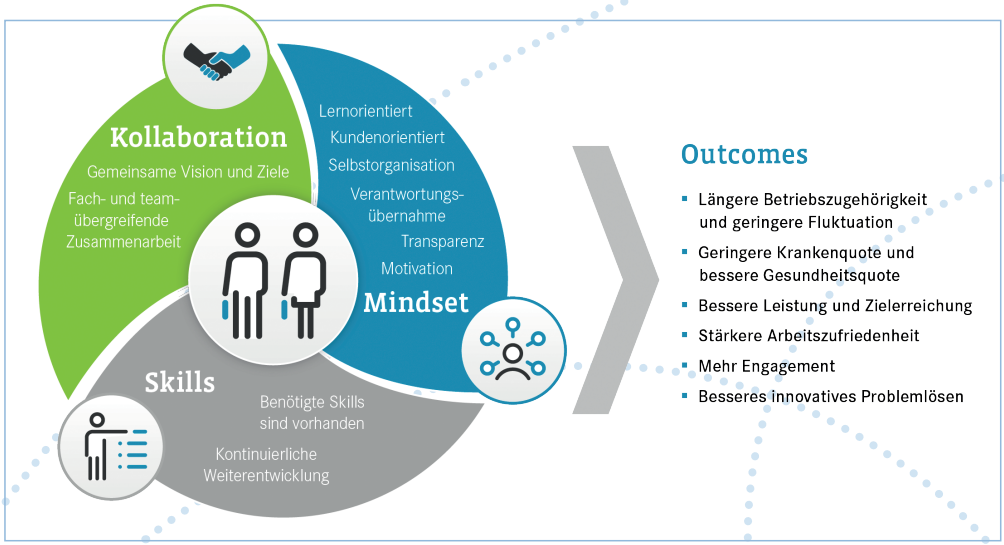
Use Cases definieren und Mitarbeitende befähigen

Hardware-seitig ist es wichtig, dass Unternehmen ihren Mitarbeitenden einen geeigneten digitalen Arbeitsplatz zur Verfügung stellen und auch die Büro-Infrastruktur wie Meeting-Räume passend ausstatten. Um hier schnell erste Erfolge zu erzielen und um hohe Vorabinvestitionen zu vermeiden, muss anhand wesentlicher Use Cases ermittelt werden,

welche Anschaffungen einen konkreten Mehrwert für den täglichen Einsatz bieten.

Bewährt hat sich hierfür die Entwicklung von Personas, das heißt die Beschreibung fiktiver Personen, die einen bestimmten Kreis von Mitarbeitenden anhand ihrer konkreten Bedürfnisse, Fähigkeiten und Ziele repräsentieren. Use Cases beschreiben dann aus Sicht der Persona relevante Arbeitsszenarien und Herausforderungen. Darauf aufbauend werden passende Lösungen entwickelt, die konkreten Nutzen bieten. Neben der technischen Implementierung erhalten die Mitarbeitenden Unterstützung, um diese Lösungen effizient zu nutzen.

Durch diesen Ansatz stehen die Mitarbeitenden im Mittelpunkt der Transformation. Dies führt zu einer erhöhten Mitarbeiterzufriedenheit, einer positiveren Arbeitseinstellung sowie zu einer effizienteren Arbeitsweise.

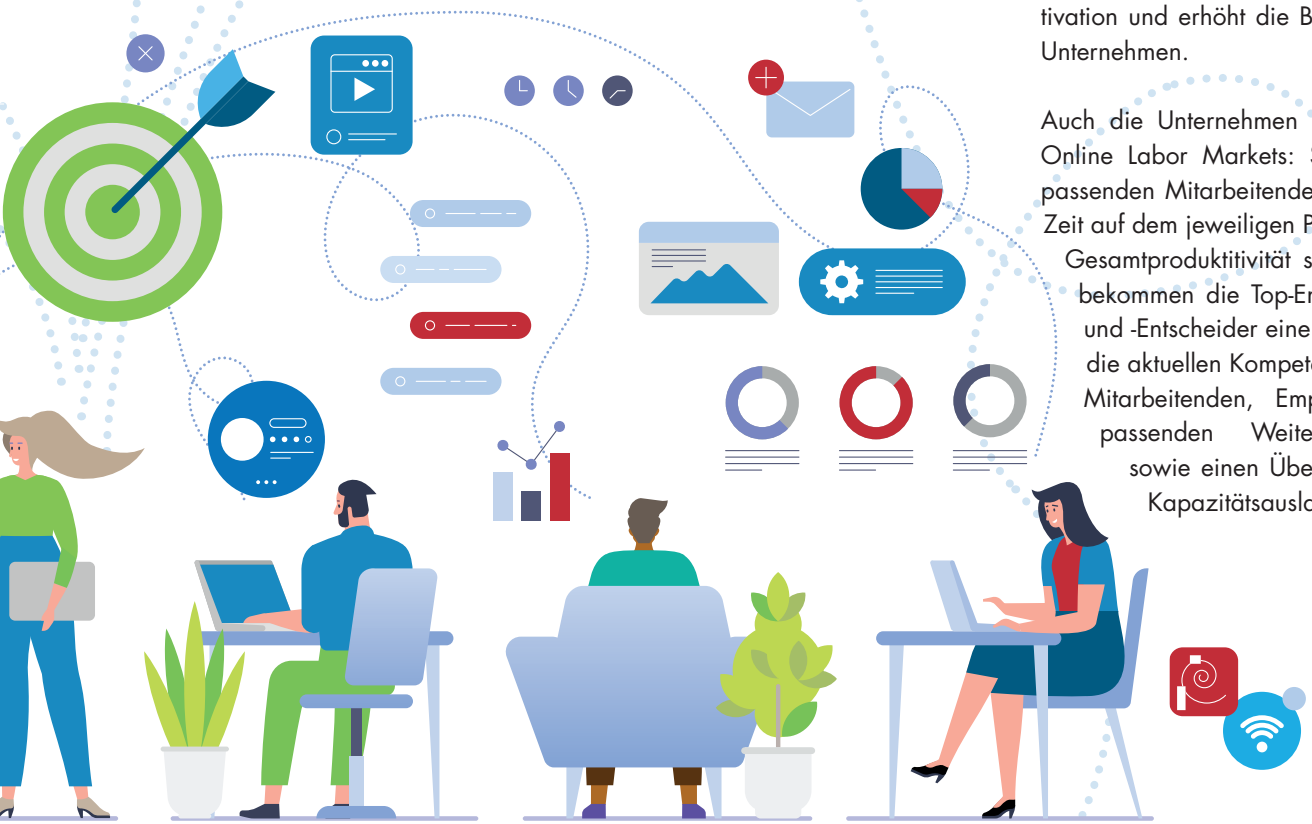


Online Labor Markets für ein starkes Empowerment

Ein weiteres bewährtes Mittel zur Erhöhung von Flexibilität und Motivation sind so genannte Online Labor Markets. Hierüber können sich Mitarbeitende aktiv auf zu ihren Kompetenzen und Interessen passende Projekte bewerben. Online Labor Markets ermöglichen ein Matching von Mitarbeitenden oder Teams mit Projekten oder Aufgaben anhand von Fähigkeiten und Entwicklungspfaden. Zusätzlich lassen sich externe Stakeholder einbinden. Für ein optimales Matching gewinnen KI-gestützte Algorithmen an Bedeutung.

Die Vorteile für Mitarbeitende: Sie werden in Projekten und an Aufgaben empowered, die ihrem Fähigkeits- und Kompetenzprofil entsprechen eigenständig zu arbeiten. Sie können sich zielgerichtet weiterentwickeln und erhalten Einblick in die Themen des Unternehmens. Das verbessert ihre Fähigkeiten, steigert ihre Motivation und erhöht die Bindung an das Unternehmen.

Auch die Unternehmen profitieren von Online Labor Markets: Sie haben die passenden Mitarbeitenden zur richtigen Zeit auf dem jeweiligen Projekt, was die Gesamtproduktivität steigert. Zudem bekommen die Top-Entscheiderinnen und -Entscheider eine Übersicht über die aktuellen Kompetenzprofile ihrer Mitarbeitenden, Empfehlungen zu passenden Weiterentwicklungen sowie einen Überblick über die Kapazitätsauslastung.



NEW WORK BEDEUTET AUCH NEW LEADERSHIP: DAS MANAGEMENT UND TEAMLEITENDE MÜSSEN MITARBEITENDE NOCH MEHR BEFÄHIGEN, EIGENSTÄNDIGE ENTSCHEIDUNGEN ZU TREFFEN UND DINGE AUSZUPROBIEREN.

René Krähling, Managing Consultant, Campana & Schott, www.campana-schott.com

Führungskräfte als Erfolgsfaktor

Aufgrund dieser anstehenden Veränderungen müssen Unternehmen ihre Führungskräfte dazu befähigen, dass diese ihre Mitarbeitenden motivieren, einbinden und ebenfalls befähigen, selbständig Entscheidungen zu treffen – unabhängig davon, ob die Mitarbeitenden im Büro, zu Hause oder mobil arbeiten.

So ist beispielsweise regelmäßig und gezielt nachzufragen, wie es den einzelnen Mitarbeitenden geht: Hat er oder sie Schwierigkeiten beim Erledigen der Aufgaben, mit Kunden oder im Team? Mit dem gebotenen Fingerspitzengefühl müssen diese Punkte im Zuge von Remote Leadership klarer angesprochen werden, da in Videocalls Gesten und Untertöne oft kaum zu erkennen sind. Hierfür sind die Führungskräfte zu sensibilisieren.

Zudem müssen Führungskräfte als Vorbild vorangehen und New Work in der Praxis leben. Dies reicht von einer modernen Führungs- und Fehlerkultur, über das Delegieren von Verantwortung, bis zum Ermitteln und Erhöhen von Motivationsleveln. Dazu gehören neben einer gezielten fachlichen Weiterentwicklung der Mitarbeitenden auch Schulungen im effizienten und produktiven Umgang mit digitalen Tools.

Purpose, Diversität und Nachhaltigkeit: neue Zielsetzungen für Führungskräfte

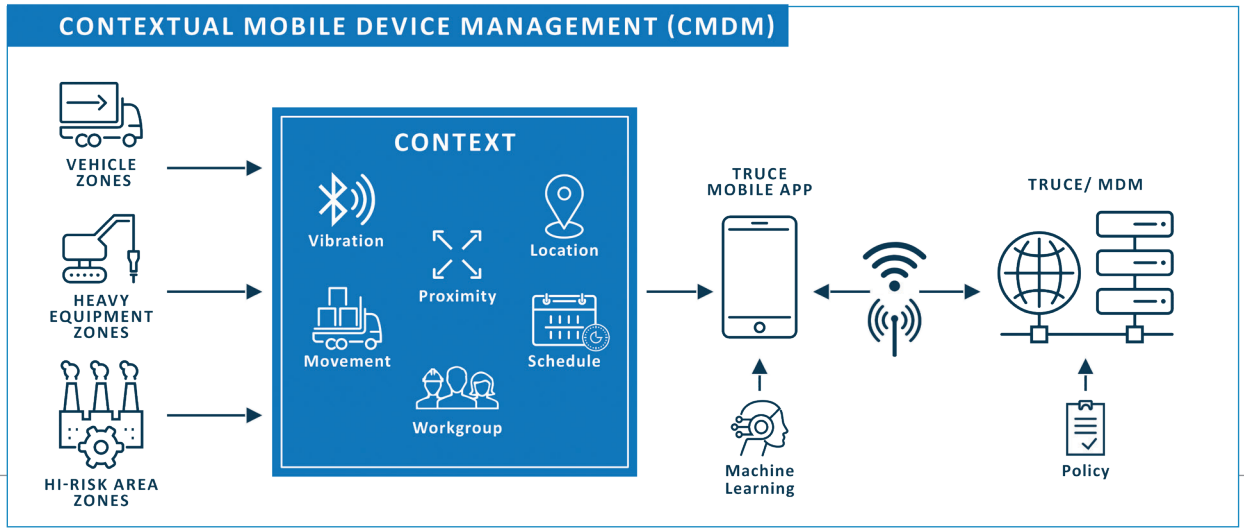
Es wird in Zukunft noch wichtiger, dass Führungskräfte die Mitarbeitenden und deren Entwicklungsperspektiven in den Mittelpunkt stellen. Gemäß dem Future Organization Report 2021 von Campana & Schott und dem Institut für Wirtschaftsinformatik der Universität St.Gallen ist die Motivation der Mitarbeitenden ein zentraler Faktor für den Unternehmenserfolg. Denn Mitarbeitende können nur dann exzellente Leistungen erbringen, wenn sie motiviert und qualifiziert sind sowie die richtigen Rahmenbedingungen für ihre Arbeit haben.

Zu diesen Rahmenbedingungen tragen Purpose, Diversität und Nachhaltigkeit als wesentliche Treiber bei. In der Studie geben 63,9 Prozent der Befragten an, dass ein übergeordneter Purpose bei kritischen Management-Entscheidungen eine Rolle spielen sollte. So agieren Mitarbeitende motivierter, wenn sie in ihrer Arbeit einen Sinn sehen. 87,2 Prozent sagen, dass sie gerne Feedback von Menschen mit unterschiedlichen Perspektiven und Hintergründen bekommen. Diverse Teams sind produktiver, leistungsfähiger und innovativer. Zusätzlich dient Cross-Funktionalität als Grundlage einer exzellenten Organisation und korreliert deutlich mit der Unternehmensleistung. Für 68 Prozent der Mitarbeitenden und Führungskräfte sollten auch die Auswirkungen auf die Umwelt bei kritischen Management-Entscheidungen berücksichtigt werden.

Fazit

Unternehmen, die im Spannungsfeld von New Work erfolgreich sein wollen, können die Erfahrung der IT für relevante Use Cases und die passenden Technologien nutzen. Sie müssen aber auch neue Fähigkeiten aufbauen – nicht nur bei Mitarbeitenden, sondern insbesondere bei Führungskräften. Nur so können sich diese selbst auf die neuen Arbeitsformen einstellen und die Mitarbeitenden auf diesem Weg mitnehmen. Denn nur mit dem engagierten und eigenverantwortlichen Handeln der Mitarbeitenden gelingt die erfolgreiche Integration von New Work in eine leistungsstarke Organisation.

Christian Schmid, René Krähling



MDM PLUS C

WIE NUTZER MOBILER GERÄTE BESSER VOR GEFAHREN DURCH ABLENKUNG GESCHÜTZT WERDEN KÖNNEN

Wir leben und arbeiten in bewegten Zeiten. Mobile Endgeräte sind heute nicht mehr wegzudenken – weder im privaten noch im beruflichen Alltag. Gleich in welcher Branche, Geschäftsprozesse werden digitalisiert, Workflows automatisiert und konsequent auf Smartphones, Tablets, Notebooks und deren Apps verlagert. Denn mobile Lösungen helfen, Arbeitsabläufe zu optimieren – nicht nur in Büros, sondern auch in Arbeitsumgebungen, die ganz ohne Schreibtisch auskommen: in der Fertigung, auf Baustellen, in Lagerhallen und dort, wo schweres Gerät im Einsatz ist, zum Beispiel bei der Steuerung von Produktionsanlagen, Gabelstaplern, landwirtschaftlichen Maschinen oder Gefahrguttransportern.

Der „Arbeitsplatz" ist heute genau da, wo Aufgaben mit beliebigen Endgeräten gelöst werden – egal an welchem Ort und zu welcher Zeit. Das heißt für die IT: „Security First". Viele Dienstleister haben sich deshalb darauf spezialisiert, komplexe Mobile Device Management-Lösungen (MDM) bereitzustellen, die das Thema Sicherheit in den Mittelpunkt stellen und nicht nur vor Datenverlust und Schadsoftware schützen, sondern Mobilgeräte und Applikationen richtlinienkonform verwalten und den Zugriff auf Unternehmensdaten bestens absichern. Doch nur die wenigsten gehen einen Schritt weiter und fügen den Faktor Mensch zusätzlich in ihre Lösungen ein.

CMDM: mobil, sicher, kontextbezogen

Einer davon ist SPIRIT/21. Gemeinsam mit seinen Partnern TRUCE Software und Jamf stellt SPIRIT/21 kontextbezogene Mobility Management-Lösungen speziell für die „deskless workforce" bereit. Dahinter stecken intelligente UEM-Lösungen, die auf traditionellen MDM-Konzepten aufbauen, jedoch zusätzlich eine weitere Sicherheitsebene einfügen. Mit CMDM (Contextual Mobile Device Management) wird es möglich, die Bereitstellung mobiler Anwendungen an die jeweilige Arbeitsumgebung anzupassen – sicher, dynamisch und automatisiert. Das heißt: In Zonen, die eine erhöhte Aufmerksamkeit erfordern, werden nur die Anwendungen zur Verfügung gestellt, die zur Erledigung der jeweiligen Aufgabe tatsächlich benötigt werden. Alle anderen, nicht relevanten Apps und Funktionen werden so lange ausgeblendet, bis der definierte Bereich wieder verlassen wird. Der entscheidende Vorteil: Mitarbeitende werden bei der Nutzung ihrer Mobilgeräte weniger abgelenkt und so besser vor Gefahren, Unfällen und Verletzungen am Arbeitsplatz geschützt.

CMDM erweitert traditionelle MDM-Lösungen um eine zusätzliche Dimension. Ging es bisher vor allem um technische und organisatorische Aspekte, rückt nun die Frage in den Mittelpunkt, wie Teams und Organisationen durch intelligente IT-Lösungen beim Einsatz mobiler Endgeräte situativ geschützt werden können. Neben der Reduzierung von Unfallrisiken bietet CMDM eine Reihe weiterer Vorteile. Zu den wichtigsten zählen: signifikante Einsparungen durch vermiedene Schäden an Fahrzeugen und verringerten Policen bei Versicherungen sowie ein eindrucksvoller Return of Investment. Darüber hinaus können CMDM-Lösungen helfen, betriebliche Abläufe effizienter zu gestalten, und die Einhaltung von Vorschriften und Unternehmensrichtlinien erleichtern.

www.spirit21.com

SPIRIT/21

BUSINESS ANALYTICS

STÄRKERE BETRACHTUNG DER FLEXIBILITÄT VON BUSINESS-ANALYTICS-LÖSUNGEN BEI DEREN AUSWAHL FÜR WHAT-IF-ANALYSEN

Betriebswirtschaftliche Themenstellungen wie die des Controllings, der Finanzplanung oder des Marketings haben für Organisationen eine hohe Bedeutung. In diesen betriebswirtschaftlich orientierten Bereichen dominieren bislang Methoden der Business-Intelligence. Der Schwerpunkt der Business-Intelligence ist im Allgemeinen die Aufbereitung und Darstellung von historischen sowie aktuellen Daten. Die Darstellung kann etwa mittels Dashboards, Berichts- und Abfragewerkzeugen oder OLAP erfolgen.

Der Begriff der Business-Analytics wird seit einigen Jahren diskutiert. Business-Analytics dient dazu, verschiedene Methoden zu nutzen, um unternehmerische Entscheidungen treffen zu können. Eine der Methoden sind What-If-Analysis.

UNTERNEHMEN KÖNNEN MIT DEN GEEIGNETEN TOOLS INSBESONDERE WHAT-IF-ANALYSIS DEUTLICH VEREINFACHEN. WICHTIG SIND EINE FLEXIBLE ANBINDUNG VON QUELLSYSTEMEN SOWIE UNTERSÜTZUNG BEI PLANUNGSSZENARIEN.

Prof. Dr. Henrich Brandes,
Ostfalia Hochschule für angewandte Wissenschaften, www.ostfalia.de

Ausgewählte Problemstellungen

Aufgrund ungeklärter fachlicher Fragen hatten Abteilungen in zahlreichen Organisationen in der Vergangenheit namentlich dieselbe Kennzahl unbewusst unterschiedlich definiert und verschiedenen operativen Systemen entnommen. Dies führe dazu, dass es in einer Organisation voneinander abweichende fachliche Auffassungen hinsichtlich einer Kennzahl gab.

Im Zuge der Einführung von Business-Intelligence-Lösungen war es das Ziel vieler Organisationen, mit einem Data-Warehouse einen Single-Point-of-Truth für Daten zu etablieren, der allgemein anerkannte Kennzahlen bereitstellt. Diese sollten zunächst die Grundlage für Auswertungen und später für Planungen, etwa mit What-If-Analysis, sein. Es zeigt sich häufiger aufgrund von Projektzyklen, dass sich der Ansatz eines Data-Warehouses als einziger Quelle für Analysen und insbesondere für Planungen nicht immer realisieren lässt, wenn Fachbereiche sehr kurzfristige Anforderungen an Kennzahlen definieren.

Als Behelf werden vielfach die erforderlichen Daten aus den Quell-Systemen exportiert, anschließend in eine Tabellenkalkulation importiert und dort vom Fachbereich verwendet.

Die Nutzung von Tabellenkalkulationen erfolgt sicherlich auch vor dem Hintergrund, dass zahlreiche Fachbereichsnutzer die Nutzung eben jener gewohnt sind. Die Hersteller analytischer Informationssysteme haben darauf reagiert und deshalb vielfach Plug-Ins entwickelt. Ein weiteres Argument für den Einsatz einer Tabellenkalkulation ist, dass die Fachbereichsnutzer betriebswirtschaftliche Fragestellungen haben, die sich mit den etablierten Werkzeugen nicht immer ad-hoc beantworten lassen. Dies geht allerdings oftmals mit der Entwicklung komplexer Formeln in einer Tabellenkalkulation einher, wodurch bei geänderten Berichts- oder Planungsanforderungen hohe Aufwände in der Anpassung der Formeln erwachsen, da zum Beispiel Hierarchien und Dimensionen nicht automatisch in Tabellenkalkulationen abgebildet werden.

Außerdem lässt sich in der Praxis beobachten, dass Fachbereichsnutzer insbesondere für What-If-Analysis einzelne Zellen in den Tabellenblättern ändern. Die geänderten Tabellenblätter werden dann vielfach als Tabellenkalkulationsdatei gespeichert und an andere Anwender weitergeleitet, die ihrerseits Änderungen an Dateiinhalten vornehmen. Hierdurch entstehen häufig nicht nachvollziehbare Versionsstände und Inkonsistenzen. Dies steht dem Ziel eines analytischen Informationssystems entgegen, das als Single-Point-of-Truth für Analysen und Planungen dienen soll.

Lösungsansätze

Aufgrund der skizzierten Problemstellungen hinsichtlich einer hohen Flexibilität der Fachbereiche insbesondere für What-If-Analysis, sollten Organisationen bei der Auswahl von Business-Analytics-Produkten zusätzlich zu den „klassischen" Anforderungen und Architekturen neue Wege beschreiten:

So sollten sich durch eine moderne Tech-

nologie mit geringen Aufwänden zusätzlich weitere Datenquellen, etwa mittels Tools wie Olation von PARIS TECHNOLOGIES, integrieren lassen, wodurch neben Auswertungen insbesondere What-If-Analysis auf einer breiteren und vor allem fachlich abgestimmten Datenbasis möglich werden, etwa in einer Tabellenkalkulation mit einem Plug-In wie PowerExcel desselben Herstellers, welches den Datenaustausch mit Olation vollzieht (siehe Bild 1).

Auswertungen und What-If-Analysis setzen oftmals Hierarchien voraus. Ein Beispiel für eine definierte Hierarchie nach Geographie zeigt der Screenshot des Tools Olation (siehe Bild 2). Auf unterster Ebene der Hierarchie sind mehrere Staaten definiert, die auf der nächsthöheren Ebene zu Kontinenten und dann zu einem weiteren übergeordneten Knoten aggregiert werden. Wertausprägungen betriebswirtschaftlicher Kennzahlen kann das Werkzeug dann entsprechend der Hierarchieebene beispielsweise aufsummieren.

Die geographische Hierarchie dient als anschauliches Beispiel, unterliegt aber eher selten Änderungen. Beispiele für häufige Änderungen sind Annahmen über zukünftige Umsätze für potenzielle neue Produkte oder Untersuchungen über eine Zuordnung von vorhandenen oder zukünftigen Produkten zu Produktgruppen oder Hauptproduktgruppen. Aggregationen (Summenbildungen) etwa hinsichtlich der Umsätze sind dann ad-hoc für mehrere Szenarien zu ermitteln. Dies kann in starren Systemen kaum abgebildet werden und ist aufwändig in Tabellenkalkulationen zu realisieren. Besonders nutzenbringend ist es, die Hierarchien und die dazugehörenden Rechenvorschriften, etwa für Summen, in einem sehr flexiblen Werkzeug zu definieren, da Anpassungen je nach Anwendungsfall nicht erforderlich oder Anpassungen mit geringem Aufwand abbildbar sind. Mittels Plug-In können dann in der Tabellenkalkulation in den Datenbeständen OLAP-Operationen (Drill-Down, Slice und ähnliche) inklusive Berechnung der Aggregate erfolgen.

Wie bereits ausgeführt, werden bei What-If-Analysis mehrere Szenarien betrachtet und weiterentwickelt. Anzuraten ist eine Versionierung. Ziel sollte sein, Versionen mit den Werten in den Datenfeldern der Tabellenkalkulation (etwa Umsatz für ein Produkt in einer Verkaufsregion zu einer Zeitperiode) zentral zu speichern und an andere Fachbereichsnutzer weiterzuleiten. Dies unterstützt die Kollaboration auf der Grundlage eines einheitlichen Datenstandes.

Prof. Dr. Henrich Brandes

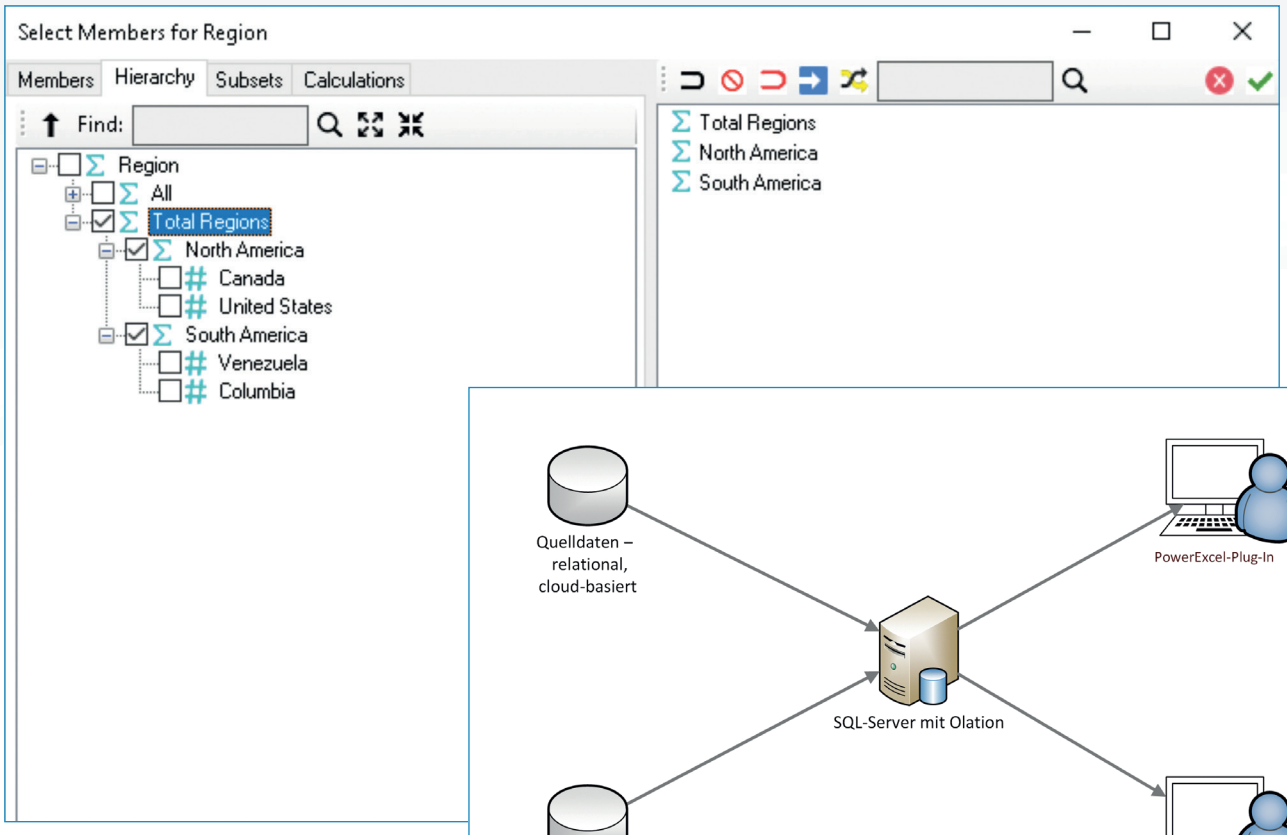


Bild 2:
Screenshot des Tools Olation

Bild 1:
Architekturskizze

DER ONLINESHOP IST KEIN IT-PROJEKT!

DOS AND DON'TS IM E-COMMERCE

Der E-Commerce boomt. Mit einem Plus von fast 15 Prozent wuchs der Onlinehandel in Deutschland im Jahr 2020 erneut zweistellig. Mit einem Bruttoumsatz von über 83 Milliarden Euro wurde ein neuer Rekord erreicht: Der Anteil des E-Commerce am Gesamthandel liegt nun bei über 14 Prozent. Das zeigen Zahlen und Erhebungen der größten Einzelhandelsverbände wie HDE und BEVH. Der E-Commerce wurde in der Pandemie auch wichtigster Wachstumsmotor für den stationären Handel. Daher setzen bestehende Filialisten und Handelsunternehmen auf einen ansprechenden Onlineshop. Viele Händler unterschätzen jedoch die Komplexität von E-Commerce-Projekten.

Wer sich mit dem eigenen E-Commerce-Projekt erfolgreich im Markt etablieren möchte, sollte folgende Fallstricke vermeiden:

1. Fehlendes Ziel des Webshops

Bevor man sich Gedanken macht über Funktionen und technische Spezifikationen des Onlineshops, muss der Händler die zentrale Frage nach dem „Wozu" stellen und beantworten. Welches Ziel möchte ich mit dem Onlineshop erreichen? Sollen neue Zielgruppen gewonnen werden? Ist das Ziel primär den Umsatz zu steigern oder stärker die Marke zu kommunizieren? Erst die Zieldefinition bestimmt, wie der Onlineshop am Ende aussieht und welche Inhalte und Funktionen dieser hat.

2. Fehlendes Verständnis über die Zielgruppen

Ein weiterer Fehler, der uns bei E-Commerce-Projekten auffällt: Marketer und Shop-Verantwortliche vertrauen auf ihr Bauchgefühl, statt empirische Daten zu nutzen, um tatsächliche und potenzielle Zielgruppen zu identifizieren und ihnen ein passendes Angebot im Onlineshop zu unterbreiten. Marketingmanager und Shop-Betreiber sollten mit den Buyer Persona beginnen und darüber Bedürfnisse, Wünsche und Erwartungen der Zielgruppen segmentieren. Erst dann wird der Onlineshop konzipiert und gestaltet.

3. Falsche Priorisierung von Funktionen

Wer statt eines richtigen Warenkorbs alle Energie in eine ausgefallene Augmented Reality Anwendung investiert, hat die Prioritäten falsch gesetzt. Die Basis eines jeden guten Onlineshops ist ein nahtloser Kassen- und Warenkorbprozess. Hier gilt die Devise: Ein Schritt nach dem anderen. Insbesondere bei Plattformen, die nicht regelmäßig überholt werden und daher an neuen technischen Anforderungen angepasst werden müssen, sind diese Basics das wichtigste.

4. Fehlende Optimierung und A/B Tests

Ein häufiger Fehler unterläuft vielen Shop-Betreibern, sobald sie erfolgreich gestartet sind: sie denken nicht daran, ihren Shop permanent zu optimieren, Fehlerquellen auszumerzen und mithilfe von A/B-Tests zu prüfen, welche Varianten und Formate am besten funktionieren und von den Nutzern angenommen werden. Ich empfehle alle drei bis vier Jahre den Onlineshop zu relaunchen und die technische Basis zu prüfen. Tools sollten hinterfragt und möglicherweise ausgetauscht werden.

5. Falsche Technologieauswahl

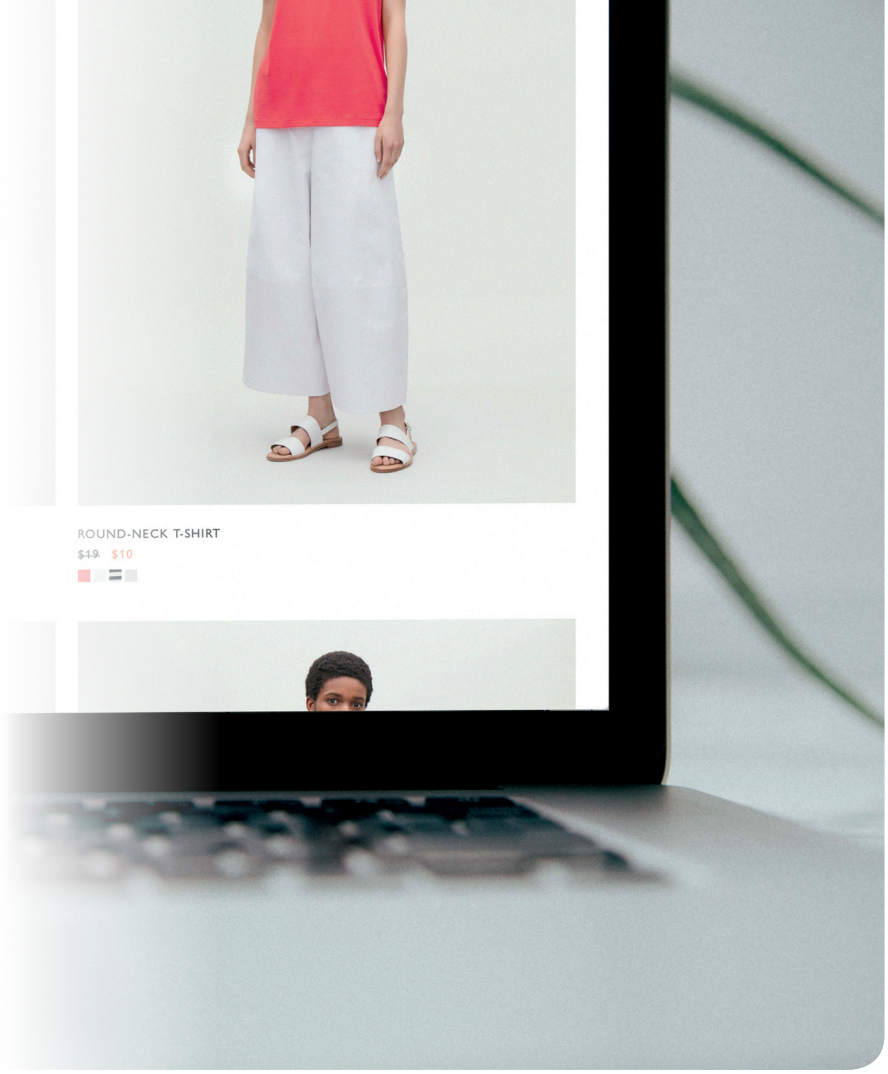
Wer ein E-Commerce-Projekt umsetzen möchte, hat die Qual der Wahl: er kann Tools selbst programmieren, bestehende Komplettlösungen wählen oder Anwendungen von Drittanbietern integrieren. Unsere Projekte und Erfahrungen zeigen, dass die Einbindung von Drittanbietern günstiger und zeitsparender ist und sich bei den meisten Projekten empfiehlt.

Wenn es darum geht, ein E-Commerce-Projekt technisch zu implementieren, bieten sich zwei Ansätze bei der Auswahl

EIN ONLINESHOP IST KEIN REINES IT-PROJEKT: DER KUNDE UND SEINE BEDÜRFNISSE MÜSSEN IM MITTELPUNKT DER PLANUNG UND UMSETZUNG STEHEN.

Artur Wagner, Head of Key Accounts, Y1 Digital AG, www.y1.de

von Software an: „Best of Breed" versus „All in One". Wir empfehlen „Best of Breed", also verschiedene Softwarelösungen wie das Content-Management-System und die Produktdatenbank modular zu integrieren - statt eine Software für alles zu beschaffen („All in One"). „Best of Breed" ist besser geeignet, um den Online-Shop flexibler zu gestalten und so den unterschiedlichen Kundenbedürfnissen zu entsprechen sowie für die Zukunft gerüstet zu sein.



Quelle: Charles Deluvio by unsplash

6. Fehlplanung interner Ressourcen und Verantwortlichkeiten

Ein häufiger Fehler passiert in einer frühen Phase des Projektes, wenn die Verantwortung für den Onlineshop in der IT verortet wird. Der Webshop ist kein IT-Projekt! Hier sehe ich den Ball bei einem dedizierten Shop-Team, das den Onlineshop global verantworten sollte. Selbstverständlich muss die IT frühzeitig eingebunden werden, um das Projekt erfolgreich umzusetzen.

7. Weniger Konzeption, mehr Code

Ein Onlineshop muss sauber programmiert sein. Aber viel wichtiger ist sich vorher Gedanken zu machen und genug Herzblut, Zeit und Know-how in die Konzeption zu stecken. In dieser Phase werden die Nutzer- und Unternehmensbedürfnisse gegeneinander abgewogen. Das ist mit am wichtigsten für einen erfolgreichen Shop-Launch. Erst danach geht es an die technische Umsetzung und die Programmierung.

8. Fehlendes Hinterfragen der Prozesse und des eigenen Businessmodells

Mit dem Wissen wächst der Zweifel, das wusste schon Johann Wolfgang von Goethe. Wer seine E-Commerce-Strategie nicht laufend prüft und hinterfragt, begeht einen Fehler. Ich empfehle jedem, der einen Onlineshop plant und betreibt, sich folgende Fragen zu stellen: Können bestimmte Kategorien im Onlineshop befüllt werden? Kann man den Content erstellen, um den Shop attraktiver zu machen? Ist das eigene Team groß genug, sind genug personelle Ressourcen vorhanden?

Nur wer die eigenen Prozesse hinterfragt und beizeiten sein Businessmodell prüft, kann sich verbessern, neue Chancen erkennen und seine Strategie rechtzeitig anpassen, um am Markt erfolgreich zu bleiben.

9. Einheitsbrei und kein USP

Wer viel Energie in Konzeption steckt, dem passiert dieser Fehler garantiert nicht: Einheitsbrei zu liefern, weil andere das ebenso machen. Stattdessen bietet das erfolgreich umgesetzte E-Commerce-Projekt deutlich erkennbare und leicht verständliche Alleinstellungsmerkmale (USPs). Die Zielgruppen werden in der Kommunikation abgeholt und erkennen im Onlineshop ein Angebot, das ihren Bedürfnissen und Wünschen entspricht.

10. Fehlende Customer Centricity

Gute gemachte E-Commerce-Plattformen stellen den Kunden in den Mittelpunkt. Die User Experience muss von der Startseite über die Produktsuche bis zum Warenkorb und Zahlungsvorgang nahtlos funktionieren und bei jedem Schritt den Ansprüchen des Kunden entsprechen. Die Plattform leitet idealerweise den Kunden intuitiv durch das Angebot. Auch bei der Gestaltung gilt: das Angebot muss dem Kunden und Nutzer gefallen, nicht dem Shop-Betreiber.

11. Beratungsresistenz

E-Commerce-Projekte sind komplex und beschäftigen viele Abteilungen und Menschen. Daher ist es wichtig, sich frühzeitig beraten zu lassen und Meinungen anzunehmen. Der Blick von außen hilft dabei, die häufigsten Fehler zu vermeiden und die Energie lieber in gute Ideen und einen gelungenen Online-Shop zu investieren.

Artur Wagner

E-COMMERCE

BESSER NICHT BEIM HOSTING SPAREN

Der Umsatz durch E-Commerce steigt seit einem Jahrzehnt kontinuierlich. Das Corona-Jahr 2020 hat diese Entwicklung noch einmal deutlich verstärkt. Viele lokale Händler haben sich spätestens letztes Jahr entschieden, entgegen vorherigen Überlegungen doch noch einen Online-Shop zu launchen. Um Umsatzverluste im „Lockdown" zu reduzieren, mussten sich viele Unternehmer möglichst schnell für ein Shopsystem, eine Agentur und ein Hosting-Paket entscheiden – eine ganz schöne Herausforderung.

Denn nicht nur für E-Commerce-Neueinsteiger gibt es dabei einiges zu beachten. Erfahrungsgemäß unterschätzen viele die Rolle des Webhostings im Online-Handel. Oft ist das hauptsächliche Entscheidungskriterium schlicht ein günstiger Preis. Bei der Umsetzung eines Online-Shops findet der Austausch häufig ausschließlich zwischen der umsetzenden Agentur und ihrem Auftraggeber statt. Das Hosting stellt schließlich nur noch die digitale Infrastruktur als Grundlage für den Shop zur Verfügung. Dabei gibt es gute Argumente, den Hoster stärker in solche Projekte miteinzubeziehen.

Als Geschäftsführer des Karlsruher Webhosters qwertiko weiß Yannic Groß um die wichtige Rolle, die Unternehmen wie das seine beim E-Commerce spielen. Im Interview erklärt er, warum es sich lohnt, den Webhoster bei Online-Shop-Projekten schon früh ins Boot zu holen, und weshalb man hier nicht am falschen Ende sparen sollte.

Lisa Ehrentraut: *Herr Groß, welche Rolle kann ein Webhoster in E-Commerce-Projekten spielen?*

Yannic Groß: Viele Menschen denken beim Webhosting nur an die Bereitstellung von Servern. Für erfolgreiche E-Commerce-Projekte ist es aber oft zielführender, das so genannte „Managed Hosting" in Anspruch zu nehmen. Dabei vermietet der Hoster eine betreute Umgebung für das Projekt. Der Dienstleister verwaltet die Hardware einschließlich Betriebssystem und Software. Je nach Angebot ist der Provider verantwortlich für das Einrichten und Konfigurieren von Hard- und Software, für technischen Support, Patch-Management, Systemwartung, Monitoring und Updates.

MAN MUSS DAS RAD JA NICHT NOCH MAL NEU ERFINDEN. EIN GUTES HOSTING IST FÜR EIN ERFOLGREICHES E-COMMERCE-PROJEKT ESSENTIELL UND MAN SOLLTE HIER NICHT AM FALSCHEN ENDE SPAREN.

Yannic Groß,
Geschäftsführer, qwertiko GmbH,
www.qwertiko.de

Lisa Ehrentraut: *Der Webhoster ist mit seiner Infrastruktur dafür verantwortlich, dass ein Online-Shop nach Projektende zuverlässig läuft. Warum also sollte man ihn schon zu Beginn eines Projekts mit einbeziehen? Reicht es nicht, wenn ich als Kunde mit meiner Agentur meinen Shop gestalte und wir dann zum Abschluss einen Hoster suchen?*

Yannic Groß: Unserer Erfahrung nach sind es vor allem die Kosten, die Kunden daran hindern, den Webhoster frühzeitig mit ins Boot zu holen. Seine Rolle scheint klar umrissen und nicht sonderlich individuell für das eigene Projekt, also wird schlicht nach einer günstigen Lösung gesucht. Dabei verkennt man, dass der Hoster auch zu Beginn des Projekts schon wichtigen Input liefern kann und Probleme dadurch schon frühzeitig vermieden werden können. So hat er mit einer technischen Projektübersicht oft einen anderen Blickwinkel als die Agenturen oder der Kunde selbst, er sieht die Software-Seite und wichtige Aspekte für die Programmierung. Auf der anderen Seite kennt er die Stellschrauben des Systems. In neuen E-Commerce-Projekten sollte der Webhoster von Anfang an involviert sein, damit später kein böses Erwachen folgt, weil bestimmte Anforderungen so doch nicht umsetzbar sind. Außerdem: Wenngleich die frühe Einbeziehung des Hosters anfangs höhere Kosten generiert, ist es doch letzten Endes im weiteren Projektverlauf günstiger.

Lisa Ehrentraut: *Kosten sind in der Projektumsetzung ein wichtiges Argument. Warum sollte man ausgerechnet beim Webhosting nicht sparen?*

Yannic Groß: Betrachtet man Online-Shops, wird schnell klar, dass das Hosting hier eine ganz zentrale Rolle spielt. Fast alle Anforderungen an solche E-Commerce-Systeme hängen letztendlich mit einem zuverlässigen Webhosting zusammen. Der Shop soll jederzeit erreichbar sein, also der Server und seine Services immer laufen. Jeder Ausfall ist gleich

ein Umsatz- und dazu noch ein Reputationsverlust. Wenn der Shop einmal genau dann nicht funktioniert, wenn jemand ihn aufruft, hat man den Kunden häufig schon verloren. Darüber hinaus muss so ein System schnell sein. Der erste Seitenaufruf sollte deutlich unter einer Sekunde liegen, ansonsten geht die Absprungrate hoch und das Suchmaschinen-Ranking geht runter. Neben einem ansprechenden Design und einer guten Usability, die von der Programmierung sichergestellt werden, ist es ebenso wichtig, dass die Prozesse im Hintergrund zuverlässig funktionieren, dass Bestellungen im System ankommen bzw. an die externe ERP-Software weitergeleitet werden, dass E-Mails verschickt werden und dass die Suche im Shop konstant läuft. Hier stellt ein „Managed Hosting" sicher, dass alle Prozesse und Systeme gut aufeinander abgestimmt sind und perfekt ineinandergreifen.

? **Lisa Ehrentraut:** *Was bietet „Managed Hosting" für E-Commerce-Projekte, was die eigene IT-Abteilung nicht kann?*

Yannic Groß: Einige Unternehmen planen bei der Einrichtung eines Online-Shops, einfach einen Platz in der Cloud zu mieten und den Betrieb mit eigenen IT-Fachkräften zu übernehmen. Dabei übersehen diese Firmen oft, wie viel Arbeit damit tatsächlich einhergeht. Darüber hinaus lastet viel Verantwortung auf wenigen Schultern – beim „Managed Hosting" gibt es dagegen keinen Urlaub oder Krankheit der zuständigen Kollegen, der Betrieb ist rund um die Uhr an allen Tagen im Jahr sichergestellt. Außerdem ist das Wissen schon vorhanden und die Systeme werden sicher aufgesetzt. Man muss das Rad ja nicht noch mal neu erfinden. Ein gutes Hosting ist daher für ein erfolgreiches E-Commerce-Projekt essentiell und man sollte hier nicht am falschen Ende sparen.

Lisa Ehrentraut | www.bitmi.de

BEZAHLEN MIT DATEN

NEUE CHANCEN FÜR E-COMMERCE

Gerade noch kurz vor Ende seiner Legislaturperiode hat der Deutsche Bundestag das Umsetzungsgesetz zur Digitale Inhalte-Richtlinie der EU (Nr. 2019/770) umgesetzt. Das Gesetzt, das am 01.01.20222 in Kraft tritt, bringt auf den ersten Blick kleine, aber wirkmächtige Gesetzesänderungen für den eCommerce. Denn auf einmal wird aus dem gern freiwillig gegebenen Gut „Daten" eine Möglichkeit, die Inanspruchnahme von Diensten zu bezahlen.

Der Gesetzgeber führt mit den §§ 327 bis 327s BGB einen komplett neuen Untertitel „Vebraucherverträge über digitale Produkte" in das BGB. Dabei fallen zwei Neuregelungen besonders auf: § 312 Abs. 1a und § 327 Abs. 3 BGB. Beide führen einen Kniff ein: stellt eine Verbraucherin für den Erhalt einer Leistung personenbezogene Daten bereit, wird dies der Zahlung eines Entgelts gleichgestellt. Bezahlen mit (personenbezogenen) Daten also. Ausgenommen davon sind allerdings personenbezogene Daten, die der Anbieter zur Leistungserbringung benötigt.

Die Regelungen führen zu mehr Transparenz auf beiden Seiten: Verbraucher erhalten bei der Nutzung „kostenloser" Dienste ein hohes, vertragliches Schutzniveau und die Unternehmen Rechtssicherheit betreffend die Nutzung der Daten. Dies erfordert aber, dass die Verbraucherinnen im Registrierungsprozess über die Verbindung zwischen Daten und Leistung genau aufgeklärt werden. Das Unternehmen muss zudem die Leistung, welche die Verbraucherin im Tausch gegen personenbezogene Daten erhält, genau beschreiben.

AUF EINMAL WIRD AUS DEM FREIWILLIG GEGEBENEN GUT „DATEN" EINE MÖGLICHKEIT, DIENSTE ZU BEZAHLEN.

Christian Koch, Mitglied der BITMi Fachgruppe IT-Sicherheit und Fachanwalt für Informationstechnologierecht bei Kleymann, Karpenstein & Partner mbB www.bitmi.de

Auf der anderen Seite besteht nun auch für Unternehmen Klarheit, dass auch auf „kostenlose" Online-Angebote am Januar 2022 Verbraucherschutzvorschriften Anwendung finden. Allerdings erhält das Unternehmen ein Kündigungsrecht, wenn die Verbraucherinnen ihre Daten nicht mehr zur Verfügung stellen möchten, etwa, weil sie eine erteilte Einwilligung widerrufen. Unternehmen müssen ihre Angebote also nicht kostenlos zur Verfügung stellen.

Die neuen Regelungen werden sicher ein wenig Gewöhnung vor allem auf Anbieterinnenseite benötigen, bringen aber viel Rechtssicherheit für alle Seiten.

Christian Koch | www.bitmi.de

BÜROKULTUR NEU GEDACHT

„WENN CHEFS WOLLEN, DASS IHRE BELEGSCHAFT ZURÜCKKEHRT, MUSS DAS BÜRO TECHNOLOGISCH ATTRAKTIVER GESTALTET WERDEN"

„Hybrid Work ist die Zukunft des Arbeitens" lautet das aktuelle Credo in vielen Unternehmen. Die Pandemie hat die digitale Transformation beschleunigt und eine Rückkehr zu Arbeitsmodellen der Prä-Corona-Zeiten wird nicht mehr möglich sein. Technologien, die ortsunabhängiges Arbeiten ermöglichen, haben die Arbeitswelt bereits verändert – jetzt ist es an der Zeit die Ausstattung der Büroräumlichkeiten ebenfalls anzupassen, da die Sinnhaftigkeit von Büros bereits angezweifelt wird. Das Büro als Arbeitsort sowie die Bürokultur müssen neu definiert und gedacht werden. Perspektivisch haben Unternehmen sonst ein Problem, denn der „War for Talents" ist noch härter geworden – Talenten ist jetzt bewusst, welche Möglichkeiten die Arbeitswelt für sie bereithält. Ein Unternehmen, das technologisch nicht mithalten kann und sich gegen Hybrid Work stemmt, wird schnell qualifizierte Mitarbeiterinnen und Mitarbeiter verlieren und Schwierigkeiten haben, neue Talente an Bord zu holen.

Was Unternehmen jetzt beschäftigt

„Aktuell werden Routinen sowie bestehende Prozesse und Strukturen mehr denn je hinterfragt: Der Chip-Mangel, die Krise in der Supply Chain sowie die mangelhaften IT-Infrastrukturen in Unternehmen, Behörden und an Schulen haben einen wichtigen Denkanstoß gegeben. Die Distributed Workforce stellt Unternehmen vor viele Herausforderungen, doch auch die Rückkehr ins Büro ist eine Challenge für viele Unternehmen, denn es müssen Anreize für diese geschaffen werden. Arbeitnehmer haben verstanden, dass Arbeiten auch anders geht und werden auf ein Stück Flexibilität und Unabhängigkeit nicht verzichten wollen. Wenn Chefs wollen, dass Ihre Belegschaft zurückkehrt, muss das Büro technologisch attraktiver gestaltet werden", erklärt Ingo Wittrock, Marketing Director und New-Work-Experte bei Ricoh Deutschland. Eine Studie von Ricoh zeigt außerdem auf, dass fast die Hälfte der Entscheidungsträger in deutschen Unternehmen glauben, dass die Zusammenarbeit im Büro für den zukünftigen Erfolg des Unternehmens entscheidend ist. Der persönliche Austausch mit Kolleginnen und Kollegen ist für viele Arbeitnehmer ein großer Anreiz um wieder in die Büroräumlichkeiten zurückzukehren, es sollte allerdings nicht der einzige bleiben. Die räumlichen und technologischen Rahmenbedingungen im Büro müssen stimmen, ansonsten lässt sich keine positive Arbeitskultur aufrechterhalten – der Rückzug ins Homeoffice oder sogar die Kündigung sind die Folgen. Führungskräfte müssen lernen, auf Ihre Mitarbeiter zu hören, in den Dialog zu treten und die Büroräumlichkeiten so zu gestalten, dass die Belegschaft gerne zurückkehrt. Technologische Investitionen helfen nicht nur dabei, die Büroflächen sinnvoll zu nutzen und eine barrierefreie Zusammenarbeit zwischen den Beschäftigten im Büro und im Homeoffice zu ermöglichen, sondern können auch einen positiven Beitrag zu einer zukunftsgerichteten Unternehmenskultur leisten.

DAS BÜRO ALS ARBEITSORT SOWIE DIE BÜROKULTUR MÜSSEN NEU DEFINIERT UND GEDACHT WERDEN.

Ingo Wittrock, Marketing Director und New Work Experte, Ricoh Deutschland, www.ricoh.de

Wandel zu Smart und Seamless Offices

Die Chancen stehen gut, dass Unternehmen nicht mehr ihre gesamte Bürofläche benötigen. Da das Konzept Hybrid Work in vielen Unternehmen (in unterschiedlichem Umfang) weiter Bestand hat, ist es oftmals nicht wirtschaftlich, an der gesamten Bürofläche festzuhalten. Es muss jetzt eine Umgebung geschaffen werden, die modern ist und auf die Bedürfnisse der Mitarbeiter zugeschnitten wurde, sodass diese durch einen Arbeitstag im Büro motiviert und inspiriert werden.

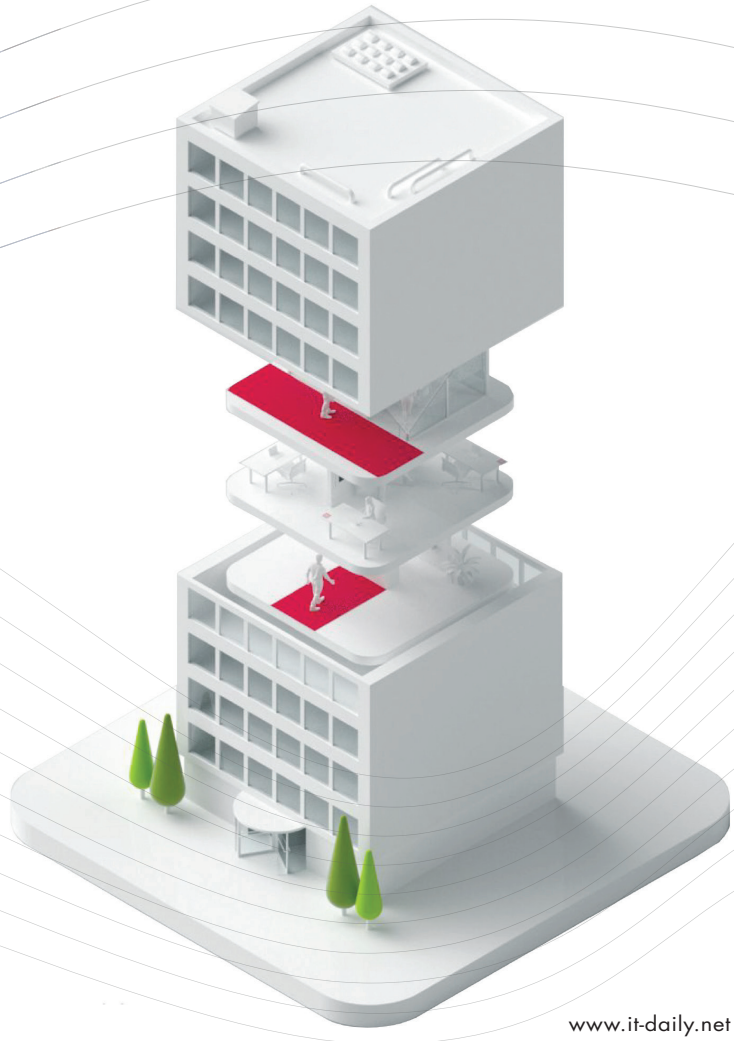
Mit der Verkleinerung der Bürofläche setzen immer mehr Unternehmen mit einer Plattform für Workspace-Management, wie beispielsweise Ricoh Spaces, das Konzept des Desksharings um. Die Desk-Management-App zeigt unter anderem an, welche Räumlichkeiten im Büro bereits besetzt, reserviert oder

noch verfügbar sind. Von Zuhause können die Arbeitnehmerinnen und Arbeitnehmer jederzeit den Status prüfen und sich auf Wunsch einen Arbeitsplatz buchen. Wenn die maximale Auslastung erreicht ist, werden die Benutzer benachrichtigt, sodass überflüssige Fahrten ins Büro verhindert werden können. Es wird außerdem ausgeschlossen, dass sich zu viele Personen in einem Raum oder im Gebäude aufhalten. Zusätzlich ist es für den Admin möglich, einzelne Arbeitsplätze online zu stellen und auch wieder offline zu nehmen. Besprechungsräume können zudem ganz einfach zugewiesen werden, sodass fest geplante Meetings ohne Raumchaos stattfinden. „Flexibel einsetzbare Büroräume und Infrastrukturen sind heutzutage essentiell für Unternehmen. Ricoh Spaces bietet Unternehmen zusätzlich die Möglichkeit unser Smart Locker-System zu integrieren. Nicht nur Post und Pakete, IT-Ausstattung und Ersatzteile können hier kontaktfrei abgeholt werden – die Day Locker für die Belegschaft sind besonders für Desksharing geeignet, da nach einem Arbeitstag im Büro das eigene Arbeitsmaterial hier gelagert werden kann und der zuvor gebuchte Arbeitsplatz wieder für eine Kollegin oder einen Kollegen freigegeben ist. Diese intelligente und sichere Arbeitsumgebung sorgt dafür, dass die Belegschaft ohne Bedenken an ihren Arbeitsplatz zurückkehren kann und Kollegialität und Kreativität wieder im Büro gelebt werden können."

Innovative Technologien

Eine Ricoh Studie zeigt auf, dass 48 Prozent der Angestellten der Ansicht sind, dass Investitionen in KI und Automatisierung die Produktivität einer hybriden Belegschaft steigern würden. Auch wenn besonders kleine und mittlere Unternehmen in diesem Bereich weiterhin nur zögerlich investieren, sind die Chancen und Vorteile, die mit einer Implementierung einhergehen, nicht mehr von der Hand zu weisen. Ein sicheres und cloudbasiertes Dokumenten-Management-Tool, wie beispielsweise DocuWare, erleichtert durch Automatisierung von Workflows und KI-basierte Prozesse, wie die Kopf- und Fußzeilenerkennung der eingepflegten Dokumente, den Arbeitsalltag. DocuWare nimmt sich den größten Herausforderungen des Dokumentenhandlings an: Medienbrüche, Dokumentenintensivität, Informationsmanagement und Dokumentenverwaltung. Außerdem ist der Sicherheitsaspekt sehr wichtig: Besonders in der Buchhaltung, im HR-Bereich oder in der Rechtsabteilung wird mit empfindlichen Daten gearbeitet, zu denen Dritte nicht unbefugt Zugang erlangen dürfen. Mit DocuWare sind diese essenziellen Dokumente digital und zentral für die befugten Mitarbeiter zugänglich, so dass beispielsweise Recruiting- und Buchhaltungsprozesse Compliance- und DSGVO-konform ablaufen und digitale Dokumente revisionssicher im Archiv gespeichert werden können. Die digitalen Freigabeprozesse schaffen einen barrierefreien Arbeitsalltag und somit mehr Zeit für die wesentlichen Aufgaben. Zusätzlich können Mitarbeiterinnen und Mitarbeiter mit einer cloudbasierten Plattform reibungslos zusammenarbeiten – ob im Homeoffice oder im Büro.

Unternehmen müssen heutzutage beides können: Homeoffice und Büroarbeit. Der Mix macht´s – Flexibilität im Hinblick auf ortsunabhängiges Arbeiten ist weiterhin das Gebot der Stunde. Die Interkonnektivität der Systeme und Tools muss dabei gegeben sein, damit zwischen der Arbeit im Büro und im Homeoffice kein Gefälle entsteht. Die Attraktivität eines Arbeitgebers wird sich in nächster Zeit stark über die Technik definieren. Über all dem steht aber, dass die Mitarbeiter wieder zusammengebracht werden und somit eine Unternehmenskultur aufrechterhalten werden kann, die letztendlich auch zum wirtschaftlichen Erfolg eines Unternehmens führt. Eine lebendige Bürokultur motiviert die Beschäftigten und fördert die Kreativität sowie die Kollegialität – auch bis ins Homeoffice.

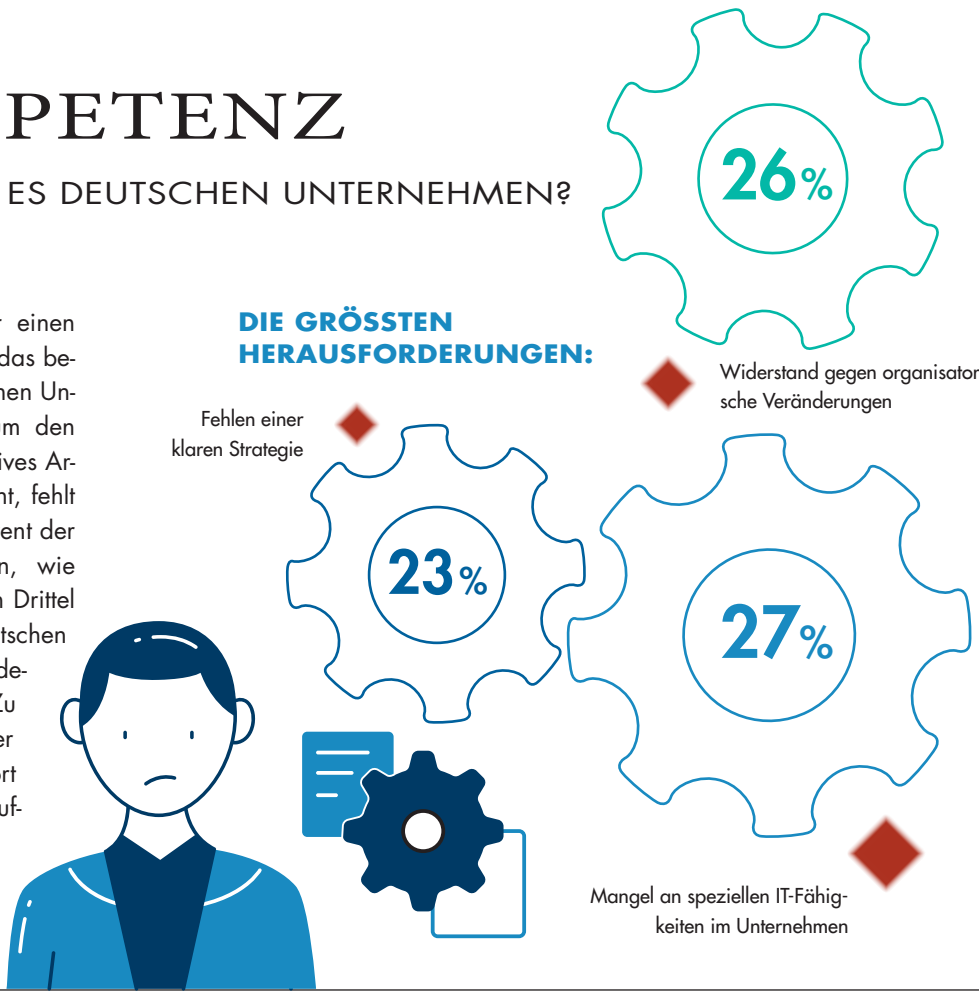


IT-KOMPETENZ

WORAN MANGELT ES DEUTSCHEN UNTERNEHMEN?

Die Corona-Pandemie hat für einen Digitalisierungsschub gesorgt, das bestätigt die Mehrheit der deutschen Unternehmen, aber: Wenn es um den Einsatz neuer Tools für produktives Arbeiten und Kommunikation geht, fehlt es den Mitarbeitern in 43 Prozent der Unternehmen, an Kenntnissen, wie diese Tools zu nutzen sind. Ein Drittel (32 %) der Beschäftigten in deutschen Firmen empfindet die vorhandenen Tools als zu kompliziert. Zu diesem Ergebnis kommt der „People & Technology Report 2022" von Markteffect im Auftrag von Fellowmind.

www.fellowmind.de



STATE OF THE ART

STORAGE@WORK

Storage-Experten haben viele Themen auf ihrem Radar. Ob Virtualisierung, software-defined Storage, Virtualisierung, Hyperkonvergenz, Hyperscaler oder Objektspeicher. Es gibt viele Themen zu bearbeiten. Innovationen und Digitale Transformation tun ihr übriges.

Mit unserem neuen eBook behalten Sie den Überblick, denn es geht nicht nur um den Sinn von Innovationen hinsichtlich der technischen Infrastruktur, sondern auch um Aspekte der IT-Sicherheit und der Wirtschaftlichkeit, Stichwort ROI und TCO, Compliance, DSGVO und die unterschiedlichsten regulatorischen Anforderungen.

Das eBook umfasst 40 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/download

Highlights aus dem eBook:

- **Vorteile von Object Storage**

Wie können Unternehmen angesichts des exponentiell wachsenden Bedarfs an Speicherkapazität die Vorteile von Objektspeicher nutzen, ohne dass die Kosten außer Kontrolle geraten?

- **Daten zur richtigen Zeit am richtigen Ort**

Um Daten adäquat zu speichern, stehen für alle Ansätze HDD und SDD in unterschiedlichsten Ausprägungen zur Verfügung. Unabhängig davon, wo sie genutzt werden, haben diese individuelle Vor- und Nachteile.

- **Sicherheit hat Prio 1**

Häufig wird die Hochverfügbarkeit verwechselt mit Datensicherheit. Zwar bringen Objektspeicher ihre eigenen Sicherheitsmechanismen mit, bei Ransomware-Attacken helfen diese aber nicht.

WENIGER IST MEHR

TRENDS IN DOKUMENTENMANAGEMENT UND ARCHIVIERUNG

Das kommende Jahr steht unter dem Motto „weniger ist mehr". Es geht darum, unnötigen Ballast loszuwerden, das heißt den Daten- und Dokumentenfußabdruck zu reduzieren, Kosten einzusparen und die Standardisierung sowie dokumentenbasierte Prozesse voranzutreiben. Diese vier wichtigen Trends werden demnach das Dokumentenmanagement und die Archivierung 2022 prägen.

1. Nachhaltigkeit heißt „löschen"

In den vergangenen Monaten hat das Thema „Green IT" wieder an Fahrt aufgenommen. Weil die voranschreitende Digitalisierung mit einem steigenden Energie- und Ressourcenverbrauch einhergeht und die Berge an Datenmüll Unmengen an Strom verbrauchen, wird sich hier eine Trendwende vollziehen. Der Grund: Nur wer regelmäßig seine Daten löscht und einen Single Point of Truth (SPoT) für Dokumente schafft, agiert nachhaltig. Auch beim Umstieg auf S/4HANA, den laut SAP Quarterly Statement rund 69 Prozent der SAP-Kunden planen, stehen deshalb Überlegungen zur flexiblen Daten- und Dokumentenverwaltung an. Wer vor der Migration seinen „Keller aufräumt", kann dank intelligenter Archivierung den eigenen Daten- und Dokumentenfußabdruck deutlich reduzieren und Kosten sparen.

2. Mieten statt kaufen: Ein Blick auf flexible betriebswirtschaftliche Modelle kann sich lohnen

Die Zahlen sprechen für sich: Der Umsatz mit Cloud-Computing ist von 8,3 Milliarden Euro in 2019 auf 12,1 Milliarden Euro in 2021 gestiegen. Dieser Trend wird sich weiter fortsetzen. Auch in der Daten- und Dokumentenarchivierung gewinnen cloudfähige Lösungen an Bedeutung. Neben technischen, organisatorischen und steuerlichen Vorteilen, die cloudbasierte Lösungen mit sich bringen können, fällt auch die veränderte Kostenverteilung ins Gewicht, die vor allem für kleine und mittelständische Unternehmen attraktiv ist. Ein Mietmodell kann somit sehr schnell und ohne große Vorfinanzierung zu einer Modernisierung der Dokumentenarchivierung führen.

3. Cloud-Migration gewinnt an Priorität

Aktuell stehen Unternehmen vor besonderen Herausforderungen: Neue Nutzeranforderungen, zunehmender Wettbewerbsdruck und digitale Geschäftsprozesse. Die Migration von bestimmten Anwendungen und Speichersystemen in die Cloud hat für IT-Entscheidungsträger deshalb hohe Priorität. Der Gang von SAP in die Cloud ist nur einer von vielen Indikatoren dazu. Laut aktueller Lünendonk-Studie möchten 87 Prozent der SAP-Kunden das Rollout zu S/4HANA bis 2025 abgeschlossen haben. Ein Großteil davon plant die Nutzung einer Hybrid Cloud – eine Kombination aus On-Premises, Private und Public Cloud – einzusetzen. In diesem Zuge erregt der Schnittstellenstandard CMIS immer mehr Aufmerksamkeit. Mit diesem kann ein „intelligentes Dokument" geschaffen werden, das auf unterschiedlichste Applikationen zugreifen kann. Ein kostenintensives ECM-System wird so nicht mehr benötigt.

4. Prozesse neu denken – RISE mit Dokumenten kann was

RISE with SAP ist in der SAP-Community fast jedem ein Begriff. Der Gedanke von SAP, ein ganzheitliches Konzept zu schaffen, das über die S/4HANA Transformation hinaus geht, ist einer der Trends 2022. Warum? Dokumentenbasierte Prozesse gewinnen weiter an Bedeutung und sollen helfen, die Transparenz und Effizienz entlang der Wertschöpfungskette zu gewährleisten. Historisch gewachsene Dokumentensilos, welche die Effizienz digitaler Geschäftsprozesse beeinträchtigen, sollen endgültig abgelöst werden. Deshalb gilt es, End-to-End-Prozesse einzuführen und manuelle, Papiervorgänge oder Prozesse in Parallelsystemen zu eliminieren.

Benny Schröder | www.kgs-software.com

KI & MARKETING

DAS PERSONALISIERTE KUNDENERLEBNIS OPTIMIEREN

Viele erfolgreiche Unternehmen verwenden bereits KI-gestützte Verfahren im Marketing. Doch noch immer haben einige Marketer Berührungsängste. Das ist unbegründet: Mit der richtigen Herangehensweise gelingt der Einstieg ins KI-gestützte Marketing problemlos.

Ein personalisiertes Kundenerlebnis ist eine Herausforderung, der sich Konsumgüterhersteller schon seit Jahren stellen müssen. Auch im B2B-Umfeld nimmt die Bedeutung dieses Themas zu. Schließlich nutzen B2B-Einkäufer privat Angebote, die mithilfe von Künstlicher Intelligenz ein personalisiertes Erlebnis bieten. Und das gleiche erwarten sie auch im geschäftlichen Bereich.

Künstliche Intelligenz hilft dabei, das personalisierte Kundenerlebnis zu optimieren und bietet Marketingexperten die Möglichkeit, zeitaufwendige, sich wiederholende Aufgaben zu automatisieren. Allein mit manuellen Verfahren werden Unternehmen nicht in der Lage sein, personalisierte Inhalte in großem Umfang anzubieten. Automatisiert und mithilfe trainierter Algorithmen und gut entwickelter Modelle ist dies möglich. KI ist daher ein wesentlicher Bestandteil von Personalisierungsambitionen. Sie schafft im Marketing mehr Zeit für Kreativität und Wertschöpfung.

Viele Unternehmen haben die Vorteile KI-gestützter Methoden bereits erkannt und setzen sie verstärkt ein: Chatbots zum Beispiel vereinfachen das Leben von Kunden und Kundenbetreuern: Letztere müssen wiederkehrende Fragen nicht mehr manuell beantworten und Erstere profitieren von einem unmittelbaren Service, der auch außerhalb der regulären Geschäftszeiten funktioniert.

Marketingabteilungen können mithilfe von KI sich wiederholende Aufgaben automatisieren, zum Beispiel die Erfassung aller Arten von Kundendaten und die genaue Festlegung und Anpassung von Zielgruppen. KI erlaubt auch, datengestützte Entscheidungen zu treffen. Marketingfachleute müssen sich also nicht nur auf ihr Bauchgefühl verlassen.

Trotzdem gilt es, den Einsatz von KI kritisch zu begleiten. Folgende Tipps helfen bei der erfolgreichen Einführung.

Gleichgewicht anstreben

Generell gilt: Wenn Unternehmen sämtliche Prozesse automatisieren, entfällt der menschliche Faktor, aber wenn sie nichts automatisieren, werden sie ineffizient und ineffektiv. Es geht also darum, das richtige Gleichgewicht zwischen Mensch und Technik zu finden.

> KÜNSTLICHE INTELLIGENZ HILFT DABEI, DAS PERSONALISIERTE KUNDENERLEBNIS ZU OPTIMIEREN UND BIETET MARKETINGEXPERTEN DIE MÖGLICHKEIT, ZEITAUFWENDIGE, SICH WIEDERHOLENDE AUFGABEN ZU AUTOMATISIEREN.
>
> Maren Horn, Client Service Director, Macaw, www.macaw.net

KI kann beispielsweise die Inhalte für die Suchmaschinenoptimierung generieren oder regelmäßige Marketingberichte erstellen. Dadurch haben Mitarbeiterinnen und Mitarbeiter mehr Zeit, innovative Marketingkampagnen aufzusetzen.

Am Beispiel Chatbots zeigt sich, dass die Nutzung von KI keine Einbahnstraße ist. In manchen Fällen möchten Kunden lieber mit einem echten Menschen sprechen, – also mit jemandem, der wirklich zuhört und ihnen persönlich sagt, was sie tun sollen.

Für die Nutzung von KI-gestützten Verfahren im Marketing gilt daher das Motto: „Digitalisieren, wo möglich, aber menschlicher Umgang, wo erwünscht".

Verwendungszweck von Daten definieren

KI erlaubt eine einfache Erfassung von Nutzer- und Kundendaten. Damit Unternehmen aber nicht sinnlos Daten erfassen, benötigen sie eine Datenstrategie: Welche Erkenntnisse sollen aus den Daten gezogen werden? Soll herausgefunden werden, an welchem Punkt der Customer Journey der Kunde abbricht? Oder ist von Interesse, wie Kunden auf die Website kommen? Welche Daten werden benötigt, um diese Informationen extrahieren zu können?

Eine Datenstrategie sorgt also dafür, dass Unternehmen aus Daten sinnvolle Schlüsse ziehen können mit dem Ziel, Kunden ein personalisiertes Erlebnis zu bieten: kein generischer Content-Push mehr, sondern Ansprache des Kunden mit genau den richtigen Inhalten, zum richtigen Zeitpunkt und über den richtigen Kanal.

KI und Marketing – einfach umsetzen

Marketer nutzen bereits täglich Künstliche Intelligenz – in vielen Fällen, ohne sich dessen bewusst zu sein. Ganz zu schweigen von all den KI-Anwendungen, die – teils auch unbewusst – im privaten Umfeld zum Einsatz kommen: die Serien- und Filmvorschläge von Netflix oder die Discover Weekly Playlist von Spotify.

All diese Angebote werden auf der Grundlage des Nutzerverhaltens zusammengestellt, um das Anwenderprofil zu verfeinern und damit ein personalisiertes Kundenerlebnis zu ermöglichen.

Viele Marketing-Tools und -Anwendungen bieten inzwischen leistungsfähige KI-Funktionen: ein idealer Weg, um mit Künstlicher Intelligenz auf leicht zugängliche Weise zu beginnen.

Maren Horn

KI-TECHNIKEN

Künstliche Intelligenz ist ein Teilgebiet der Informatik, aber als Begriff nicht einheitlich definiert. Der BITKOM bezeichnet KI als eine Eigenschaft eines IT-Systems, „menschenähnliche", intelligente Verhaltensweisen zu zeigen. Für das Marketing spielen dabei vor allem die Teilgebiete Machine Learning, Deep Learning und Natural Language Processing (NLP) eine wesentliche Rolle. Sie werden zur Automatisierung von Prozessen, zur Datenanalyse und zur Kommunikation verwendet.

Machine Learning: Wie Menschen aus Erfahrungen Entscheidungen ableiten, versucht Machine Learning mithilfe von Algorithmen Wissen aus Daten zu generieren. Dazu zählt beispielsweise die Erkennung von Mustern.

Deep Learning ist ein Teilgebiet von Machine Learning, das künstliche neuronale Netze, – das sind Algorithmen, die der Funktionsweise des menschlichen Gehirns nachempfunden sind, – verwendet.

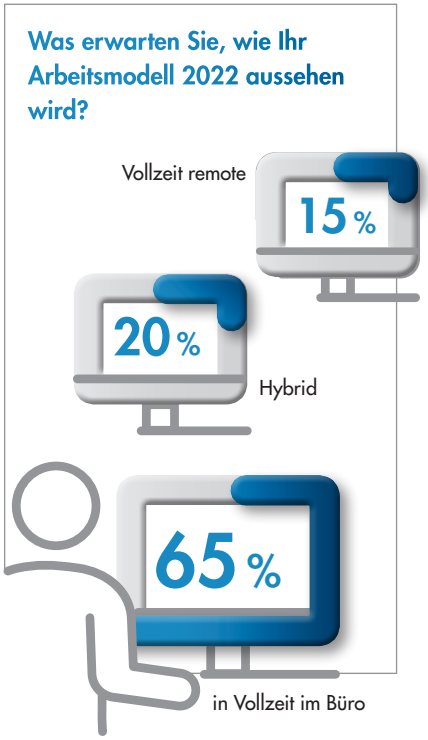
Natural Language Processing (NLP) bezeichnet die Fähigkeit einer Anwendung, menschliche Sprache mit Hilfe von Deep Learning zu erkennen und zu verarbeiten.

HYBRIDE ARBEITSMODELLE

CLOUDBASIERTE KOMMUNIKATION UND UNIFIED COMMUNICATIONS AS A SERVICE

Remote? Hybrid? Im Büro vor Ort? Die Diskussion über neue Arbeitsmodelle ist spätestens seit der Coronapandemie in der breiten Bevölkerung entfacht. Die Pandemie hat Homeoffice von heute auf morgen notwendig gemacht. Unternehmen mussten ihre Mitarbeitenden mit allen erforderlichen Instrumenten ausstatten, um eine produktive Arbeit von zu Hause aus möglich zu machen. Und sie haben dabei gelernt, dass Remote Work die Qualität der Arbeit nicht schmälert, sondern sogar verbessern und zu einer besseren Work-Life-Balance führen kann.

Mit Zunahme der Impfquote sind viele Unternehmen nun teilweise ins Büro zurückgekehrt – und stehen damit vor einer neuen Herausforderung: Ging es 2020 vor allem darum, möglichst schnell komplette Fernarbeit zu ermöglichen, sind nun vor allem hybride Arbeitsmodelle gefragt. Es geht nicht mehr um ein Entweder-oder zwischen Büro und Heimarbeit. Vielmehr wollen Mitarbeitende nun flexibel zwischen Büro, zu Hause und anderen Arbeitsplätzen wechseln. Es geht um multimodales Arbeiten – über verschiedene Geräte und Standorte hinweg. Möglich wird dies nur über cloudbasierte Kommunikation. Entscheidend ist, dass Unternehmen die während Corona eingeführten Kommunikationssysteme nun konsolidieren und ganzheitlich darüber nachdenken, wie sie Collaboration-Tools optimieren können, um Teams auch in hybriden Arbeitsmodellen miteinander zu verbinden und eine nahtlose Interaktion zu ermöglichen. Unified Communications as a Service (UCaaS) ist die Antwort, um diesen Herausforderungen möglichst effizient zu begegnen.



UCaaS: Messaging, Video und Phone

Bei Unified Communications as a Service handelt es sich um ein cloudbasiertes Bereitstellungsmodell, das verschiedene Kommunikations- und Kollaborationsanwendungen zentral auf einer Plattform vereint. Dazu zählen Funktionen wie Messaging, Videokonferenzen und Cloud-Telefonie. Über eine offene API-Struktur können Unternehmen Kommunikationsfunktionen zudem in Geschäftsanwendungen von Drittanbietern, die sie täglich verwenden, integrieren. Dies führt zu einer All-in-one-Lösung, die für Unternehmen kostengünstiger als herkömmliche Vor-Ort-Telefonanlagen ist und zudem mit Skalierbarkeit punktet. Wächst ein Unternehmen, ist es über die Plattform einfach, weitere Benutzer oder auch Standorte hinzuzufügen. Darüber hinaus trägt UCaaS zur Optimierung von Effizienz und Produktivität im Betrieb bei.

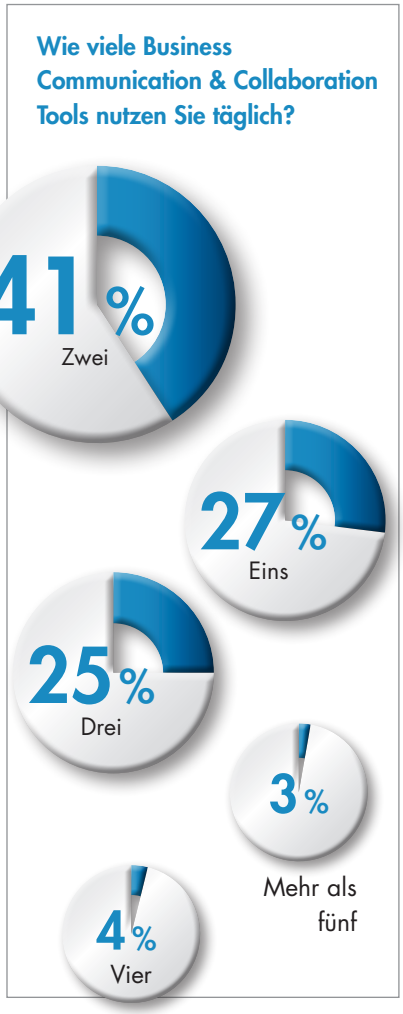
DER TREND GEHT HIN ZU UNIFIED COMMUNICATIONS AS A SERVICE. CLOUDBASIERTE KOMMUNIKATION ERMÖGLICHT ES MITARBEITENDEN, IN HYBRIDEN ARBEITSMODELLEN PRODUKTIV ZUSAMMENZUARBEITEN, UND ZWAR ÜBER VERSCHIEDENE STANDORTE UND GERÄTE HINWEG

Marco Meier, Regional Vice President Sales DACH, RingCentral, https://www.ringcentral.com/de/de

Den Trend hin zu Cloud-Kommunikations- und Kollaborationslösungen bestätigt auch eine aktuelle Studie, die Ipsos im Auftrag von RingCentral vom 25. bis 31. August 2021 unter 1.000 deutschen Arbeitnehmern durchgeführt hat: 60 Prozent der Arbeitnehmer gaben an, dass sie aufgrund von COVID-19 heute stärker auf Kollaborationstools angewiesen sind. Knapp die Hälfte (46 Prozent) geht zudem davon aus, dass Kollaborationstools die Kommunikation während der Pandemie verbessert haben. Die meisten (73 Prozent) nutzen dabei täglich mehr als ein Tool. Mehr als ein Drittel (35 Prozent) der Angestellten gehen zudem davon aus, dass sie sich im nächsten Jahr weiterhin in hybriden Arbeitsmodellen oder Remote Work befinden werden. 72 Prozent glauben, dass die Freiheit, von über-

SIND DIE ZUKUNFT

(UCAAS) MACHEN HYBRIDE ZUSAMMENARBEIT MÖGLICH



all aus zu arbeiten, künftig die Norm in allen Branchen darstellen wird.

New Work:
Vier Trends sind entscheidend

Der Wechsel hin zu hybriden Arbeitsmodellen wird 2022 insbesondere vier Trends mit sich bringen.

Erstens: Die Gleichberechtigung der Mitarbeitenden. Unabhängig davon, wo Mitarbeitende arbeiten – alle müssen den gleichen Zugang zu digitalen Technologien haben. Kommunikations- und Kollaborationstools müssen die gleichen Bedingungen für Teammitglieder an verschiedenen Standorten und Geräten schaffen. Jemand, der von zu Hause aus arbeitet, muss genauso am Unternehmensalltag partizipieren können wie jemand im Büro. Dafür müssen, zum Beispiel über Videokonferenzsysteme wie RingCentral Rooms, auch hybride Konferenzen möglich gemacht werden – sprich Konferenzen, an denen sowohl Mitarbeitende in Konferenzräumen vor Ort als auch Mitarbeitende, die remote arbeiten, teilnehmen können.

Zweitens: Kommunikations-APIs. Mithilfe einer UCaaS-Plattform und einer offenen API-Struktur (Application Programming Interface) können Unternehmen Tools für die Unternehmens- und Kundenkommunikation sowie Zusammenarbeit entwickeln, die ihren individuellen Bedürfnissen entsprechen. Verschiedene Kommunikationsfunktionen können damit auf einfache Weise zusammengesetzt werden.

Drittens: Künstliche Intelligenz (KI). Unternehmen werden weiterhin auf KI setzen, um Geschäftsabläufe zu rationalisieren und gleichzeitig zwischenmenschliche Beziehungen zu fördern. KI kann beispielsweise dabei unterstützen, bestimmte Prozesse im Call Center zu automatisieren oder die Komplexität von bestimmten Kundenanfragen zu reduzieren. Auf diese Weise können sich Call-Center-Agenten voll und ganz auf die Beantwortung der Kundenprobleme konzentrieren. Darüber hinaus kann KI dabei helfen, die Zusammenarbeit von Teams in Videomeetings zu verbessern.

Für seine UCaaS-Plattform RingCentral MVP führt der Anbieter beispielsweise im ersten Quartal 2022 neue, KI-gestützte Funktionen ein: Live-Transkriptionen ganzer Meeting-Gespräche helfen Mitarbeitenden, die zu spät kommen, einfach auf den neuesten Stand zu kommen. Meeting-Zusammenfassungen bieten eine automatisch generierte Kurzresümee von Videokonferenzen, um Meeting-Müdigkeit entgegenzuwirken und Mitarbeitenden bei gleichzeitig stattfindenden Konferenzen eine Hilfestellung zu bieten.

Viertens: Datenschutz. Gerade im deutschen Markt ist Datenschutz in der Cloud das A und O. Entscheidend ist hier die Auswahl eines Cloud-Anbieters, der die notwendige Transparenz und Beratung bietet und über eine entsprechend offizielle Zertifizierung verfügt, um das Unternehmen schützen zu können. Bei RingCentral sorgt zum Beispiel ein eigens in Frankfurt am Main eröffnetes Rechenzentrum für Datensicherheit in Deutschland und hilft dabei, europäische Gesetze und Richtlinien einzuhalten.

Als Antwort auf das Schrems II-Urteil des Europäischen Gerichtshofs und die Veröffentlichung neuer Standardvertragsklauseln der Europäischen Kommission für Übermittlungen personenbezogener Daten aus dem Europäischen Wirtschaftsraum (EWR) in ein Drittland im Juni 2021 hat das Unternehmen zudem eine Überprüfung seiner Datenübermittlungen in Länder außerhalb des EWR durchgeführt. In einem neu eingerichteten Trust Center können Kunden nun auf alle Informationen rund um dieses Thema zugreifen. Sie finden hier beispielsweise die Vereinbarung zur Übermittlung von Kundendaten auf Basis der Standardvertragsklauseln sowie weitere Informationen über Datenschutz- und Sicherheitsprogramme, Compliance-Zertifizierungen sowie den Transparenzbericht und die Risikobewertung für den Transfer persönlicher Daten.

Unternehmen können sich mithilfe von UCaaS für hybride Arbeitsmodelle rüsten und ihren Mitarbeitenden passende, sichere Tools an die Hand geben, um stets miteinander verbunden und produktiv zu bleiben.

Marco Meier

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
01. MÄRZ 2022

GREEN COMPUTING — Optimierung gesucht
SAP PARTNERLÖSUNGEN — Anwendungen für alle
KÜNSTLICHE INTELLIGENZ — Bereit für die Zukunft?

DIE AUSGABE 01/02 2022
VON IT MANAGEMENT
ERSCHEINT AM 31. JANUAR 2022.

INSERENTENVERZEICHNIS

it management

it verlag GmbH	U2, U3, U4
noris network AG	3
Vendosoft GmbH (Advertorial)	11
Spirit/21 GmbH (Advertorial)	19

it security

it verlag GmbH	U2, 9, U4
Varonis Systems (Advertorial)	15

WIR WOLLEN IHR FEEDBACK

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

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Carina Mitzschke, Silvia Parthier (-26)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Prof. Dr. Henrich Brandes, Xavier Gonzalez, Maren Horn, Christian Koch, René Krähling, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Christian Schmid, Benny Schröder, Andreas E. Thyen, Artur Wagner, Ingo Wittrock

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 Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche 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. 29. Preisliste gültig ab 1. Oktober 2021.

Mediaberatung & Content Marketing-Lösungen
it management | it security | it daily.net:
Kerstin Fraenzke, Telefon: 08104-6494-19, E-Mail: berthmann@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94, Mobil: 0172-5994 391
E-Mail: reetz@it-verlag.de

Online Campaign Manager:
Vicky Miridakis, Telefon: 08104-6494-2, 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.

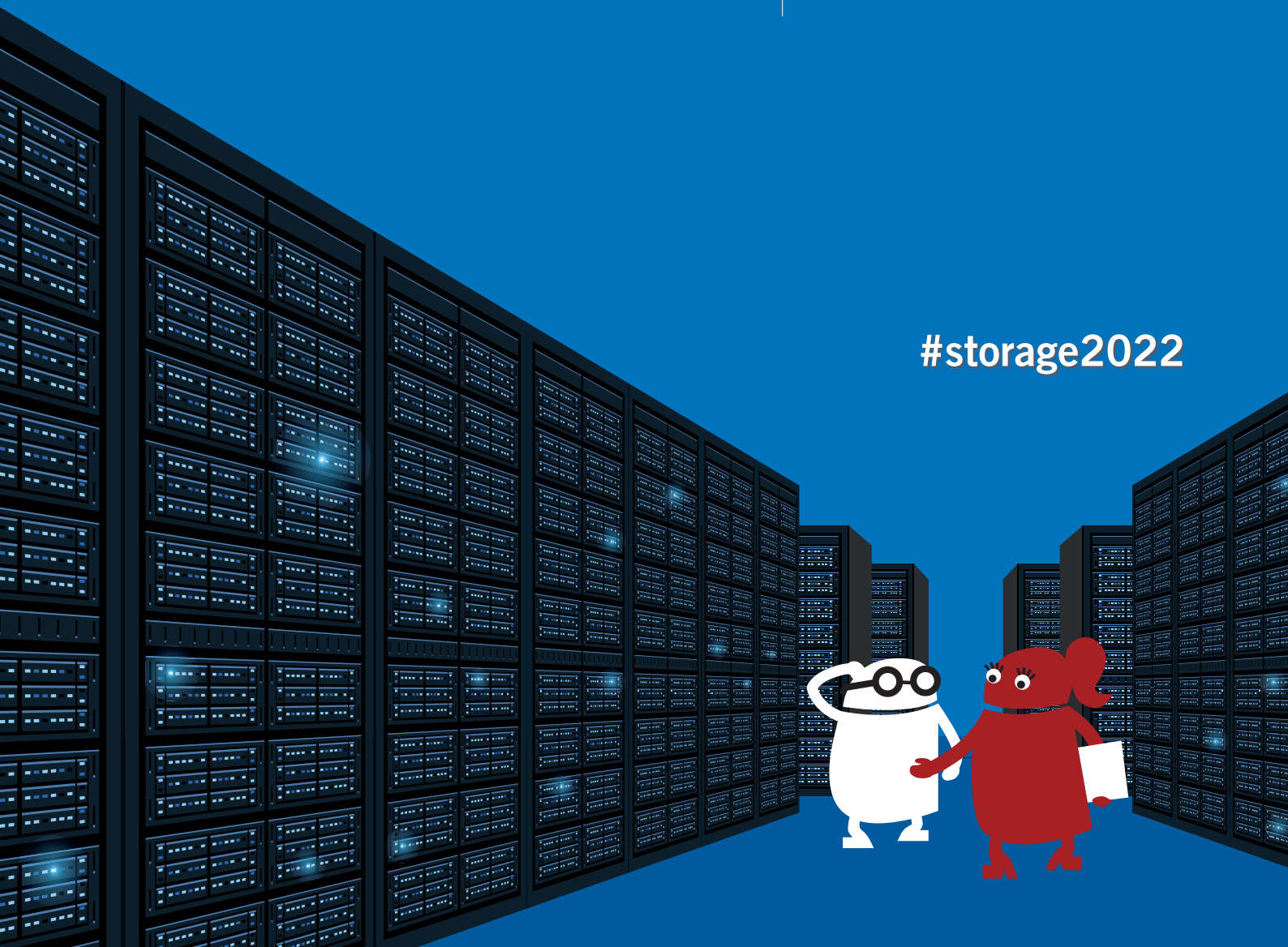
Abonnementservice:
Eva Neff, Telefon: 08104-6494 -15,E-Mail: neff@it-verlag.de
Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugs zeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht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

SAVE THE DATE!

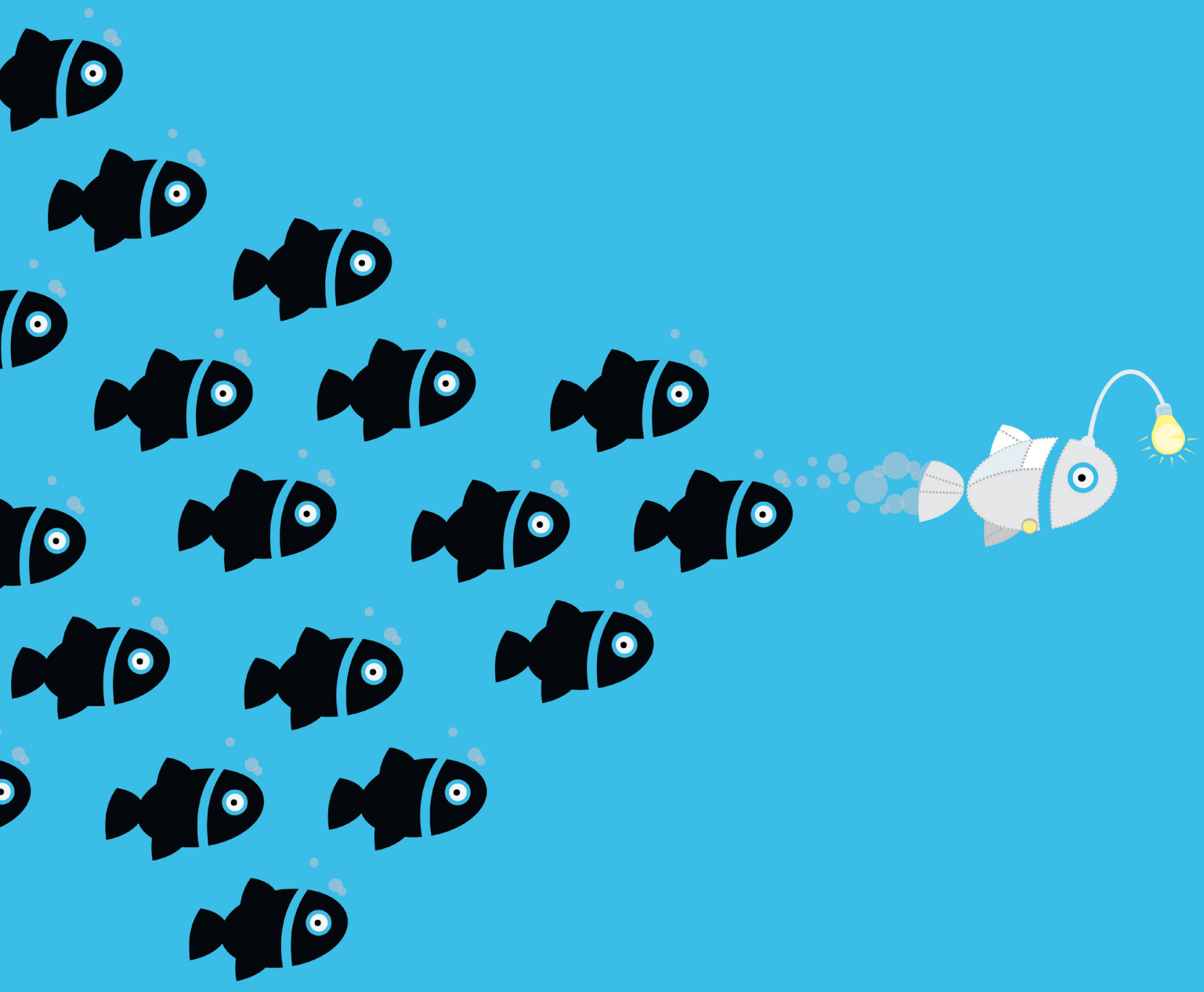
Data Protection im Fokus

2. Februar 2022 | Digitalevent

#storage2022



Thought Leadership



itsecurity
DEZEMBER 2021

DAS SPEZIAL

KATZ-UND-MAUS-SPIEL

SECURITY & CYBERCRIME

Sven Janssen, Sophos Technology GmbH

NATIVE SECURITY

Microsoft Security managen

AUTHENTIFIZIERUNG

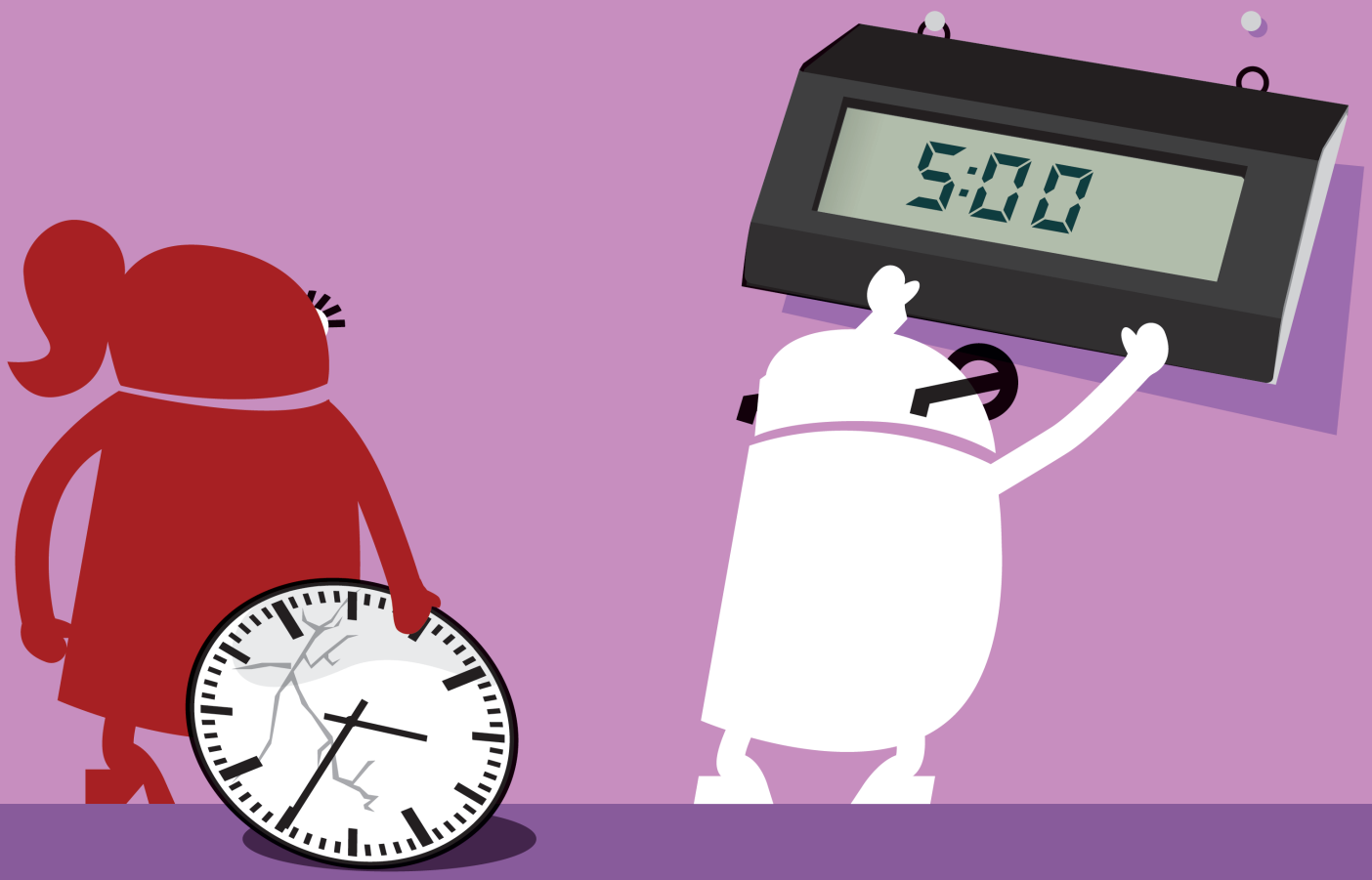
Passwortlos mit Passwort

ZERO TRUST

Mehr als nur blockieren

www.it-daily.net

Digitalisierung leicht gemacht!



Expertenwissen für

IT-Strategien & Innovationen

itmanagement

www.it-daily.net

INHALT

COVERSTORY

4 **Security und Cyberkriminalität**
Katz-und-Maus-Spiel

7 **Adaptive Cybersecurity**
Ein Sicherheits-Ökosystem, dass sich der Gefahrenlage anpasst

IT SECURITY

10 **Native Security**
Microsoft Security Funktionen besser managen

12 **Security Awareness**
Das Sicherheitsbewusstsein im Unternehmen verbessern

16 **Passwortlos mit Passwort**
So geht Marketing heute

18 **Zero Trust**
Mehr als nur blockieren

19 **Schutz des IT-Netzwerks**
Kein „Black Out" mit macmon ZTNA

20 **Instant Messenger sicher einsetzen**
Studie, Checkliste und Praxisleitfaden

21 **Cloud Workloads**
Eine umfassende Plattformsicherheit wird benötigt

22 **Flexibel und skalierbar**
Systemhäuser setzen auf Security as as Service

23 **SAP-Systeme schützen**
Bestmöglich auf Nummer sicher gehen

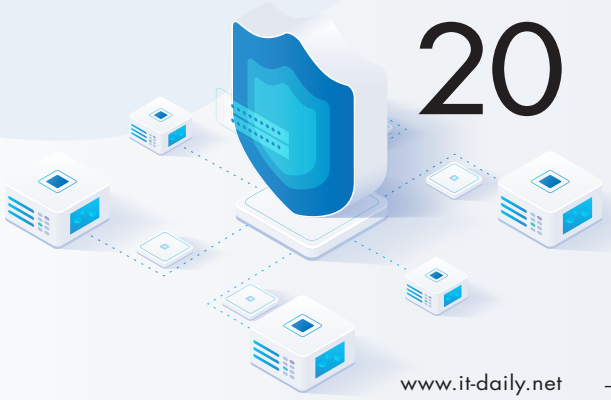
24 **Extended Detection & Response**
Mehr als nur Endpunktschutz

25 **Im Visier von Cyberkriminellen**
E-Mail-Verschlüsselung und digitale Signaturen

26 **Cyber-Versicherungen**
Essenzielle Absicherung trotz steigender Prämien

28 **IT Security Award 2021**
Gewinner im Rahmen der „IT-SA 2021" ausgezeichnet

4 COVERSTORY



SECURITY UND CYBERKRIMINALITÄT

KATZ-UND-MAUS-SPIEL: WER IST DIE KATZE UND WER DIE MAUS?

Wie steht es im Moment um die Cyber-Gefahrenlage und welche Möglichkeiten bestehen, sich vor modernen Angriffen und den nicht unerheblichen Auswirkungen mit Schutzlösungen und Security-Services abzusichern? Darüber sprach it-security-Herausgeber Ulrich Parthier mit Sven Janssen, Director Channel Sales DACH bei Sophos.

Ulrich Parthier: *Herr Janssen, Security ist für Unternehmen nichts Neues und wir wissen alle, dass sich die Entwicklungen sowohl auf der Schutzseite als auch auf der Seite der Angreifer schnell weiterentwickeln. Wo genau stehen wir heute?*

Sven Janssen: Neben vielen verschiedenen Angriffsarten von Cyberkriminellen ist und bleibt Ransomware die größte Gefahr für die Masse der Unternehmen und vor allem die mit der größten Tragweite. Ein weiterer Trend ist der Diebstahl von sensiblen Daten, welche die Kriminellen entweder verkaufen oder veröffentlichen, was je nach Datenart und Inhalt noch schlimmer für Unternehmen sein kann.

Insgesamt kann man sagen, dass sich die Gefahrenlage nicht wesentlich verbessert, aber deutlich verändert hat. Cyberkriminelle nutzen unglaublich hochentwickelte Technologien für ihre Angriffe und setzen vermehrt auf menschlich gesteuerte Angriffe, welche ihre Chancen im Vergleich zu den traditionellen, automatisierten Attacken deutlich erhöht.

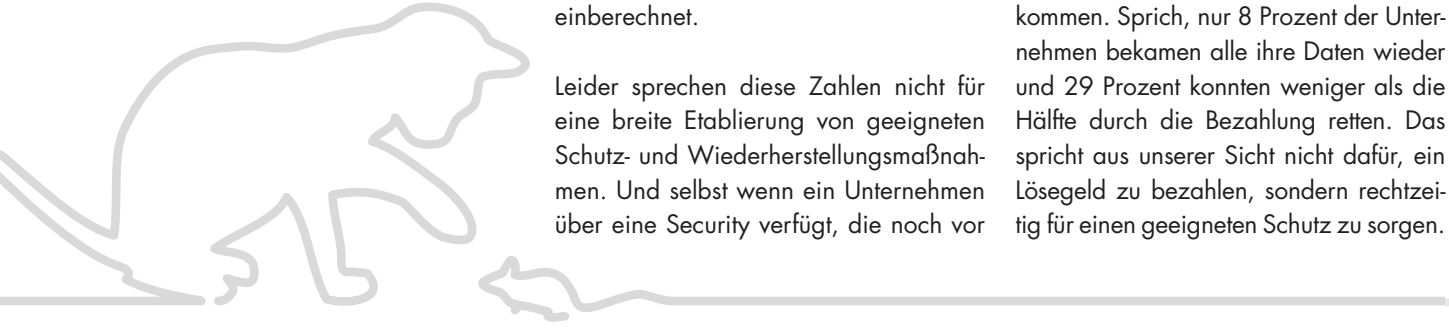
Ulrich Parthier: *Weiß man, wie viele Unternehmen angegriffen wurden und tatsächlich das geforderte Lösegeld bezahlen? Oder haben viele mit geeigneten Sicherungsmaßnahmen entsprechend vorgebeugt?*

Sven Janssen: Man muss leider mit einer großen Dunkelziffer rechnen, denn nicht jedes Unternehmen meldet einen Angriff oder gar die Zahlung von Lösegeld. Aus unseren jüngsten Studien wissen wir aber, dass rund 46 Prozent der deutschen Organisationen mit Ransomware attackiert werden. Nicht nur angegriffen, sondern Opfer einer Datenverschlüsselung sind davon zirka 54 Prozent. Zwar sinken die Zahlen leicht im Vergleich zu den Vorjahren, allerdings haben sich die Lösegeldforderungen drastisch erhöht. In Deutschland reden wir von durchschnittlich 115.000 Euro allein für das Lösegeld. Die Kosten für die Wiederherstellung – sofern diese überhaupt und trotz Zahlung möglich ist – sind noch nicht einberechnet.

Leider sprechen diese Zahlen nicht für eine breite Etablierung von geeigneten Schutz- und Wiederherstellungsmaßnahmen. Und selbst wenn ein Unternehmen über eine Security verfügt, die noch vor einem Jahr einen guten Schutz bot, kann diese nur wenig gegen die zuvor erwähnten menschlich gesteuerten Attacken ausrichten. Hier können nur integrierte Security-Ökosysteme helfen, welch ebenfalls menschlich gesteuerte Abwehr einschließen.

Ulrich Parthier: *Das bedeutet, ein Großteil dieser Unternehmen hat das Lösegeld bezahlt?*

Sven Janssen: Abgesehen von der zuvor erwähnten Dunkelziffer ist anzunehmen, dass enorm große Mengen an Lösegeld fließen. Andernfalls würde sich der riesige und kostspielige Aufwand für die Cyberkriminellen nicht lohnen. Allerdings ist das Lösegeld nur ein Teil der Kosten, die auf ein Unternehmen im Falle einer Datenverschlüsselung zukommen. Wir wissen, dass sich die Durchschnittskosten allein für die Wiederherstellung nach einem Ransomware-Angriff in nur einem Jahr mehr als verdoppelt haben, in Deutschland von rund 390.000 Euro zu 970.000 Euro in 2021. Vielleicht noch tragischer ist das Ergebnis nach der Lösegeldzahlung, denn diese ist keinerlei Garantie für die Wiederherstellung der Daten. 92 Prozent der Unternehmen haben ihre Daten nach der Lösegeldzahlung nicht komplett zurückbekommen. Sprich, nur 8 Prozent der Unternehmen bekamen alle ihre Daten wieder und 29 Prozent konnten weniger als die Hälfte durch die Bezahlung retten. Das spricht aus unserer Sicht nicht dafür, ein Lösegeld zu bezahlen, sondern rechtzeitig für einen geeigneten Schutz zu sorgen.



Ulrich Parthier: *Wie schaffen es Cyberkriminelle in Zeiten hoher Datensicherheit immer mehr zu erbeuten und zu verschlüsseln?*

Sven Janssen: Zu dieser Frage gibt es gleich mehrere Antworten. Bei den prominenten Angriffen, von denen man gelegentlich in der Öffentlichkeit Kenntnis erhält, greifen Cyberkriminelle nicht ausschließlich auf automatisierte Angriffstechnologien zurück, sondern steuern die Attacke zu einem großen Teil händisch, mit enormem Fachwissen und oft über Monate hinweg.

Aber auch bei den rein automatisierten Angriffsvarianten kommen mittlerweile sehr komplexe und raffinierte Technologien zum Einsatz. Diese sind nicht selten erfolgreich, Sicherheitslösungen auszutricksen.

Eine weitere Antwort auf Ihre Frage bezieht sich auf das Security-Konzept und die Lösungen, die Unternehmen einsetzen und die allzu oft nicht auf dem neuesten Stand der Schutzmöglichkeiten sind. Hier haben Kriminelle leichtes Spiel und nutzen jede Lücke, die sich ihnen bietet.

Last but not least darf man menschliches Verhalten und Fehler der Computeranwender nicht unterschätzen. Phishing-Attacken beispielsweise erreichen erstaunlich oft ihr Ziel. Schulungen und Phishing-Simulationsprogramme, die das korrekte Verhalten immer wieder trainieren, tragen sinnvoll zu mehr Sicherheit bei.

Ulrich Parthier: *Und hier kommen Security-Lösungen und Technologien mit künstlicher Intelligenz ins Spiel?*

Sven Janssen: KI ist tatsächlich eine Möglichkeit, Angreifer aufgrund verhaltensbasierter Auffälligkeiten zu entdecken und unschädlich zu machen. Allerdings reicht KI für komplexe und menschlich gesteuerte Attacken heute nicht mehr aus. Nur ein Schutz, der den Möglichkeiten der Angreifer ebenbürtig oder sogar voraus ist, kann die komplexen Attacken aufspüren und verhindern. Hierfür benötigt man eine Kombination von Schutzlösungen im Netzwerk, an den Endpoints, für die Cloud und für viele andere Stellen mehr, die intelligent miteinander verknüpft sind, untereinander kommunizieren und auf eine riesige Wissensbasis zurückgreifen. Diese Lösungen werden zusätzlich mit menschlicher Expertise, Forensik und Monitoring nahtlos verknüpft. Experten scannen das Netzwerk kontinuierlich und decken dabei die Gefahrenbereiche ab, die bis heute auf Grundlage von KI-basiertem Schutz und Ähnlichem noch nicht realisierbar sind. Wir nennen dieses Gesamtkonstrukt ein Adaptive Cybersecurity Ecosystem.

Ulrich Parthier: *Wie genau funktioniert Ihr Adaptive Cybersecurity Ecosystem?*

Sven Janssen: Das Sophos Adaptive Cybersecurity Ecosystem basiert auf den gesammelten Bedrohungsdaten der SophosLabs, der Künstlichen Intelligenz (KI) und von unseren Sophos Security Opera-

> INSGESAMT KANN MAN SAGEN, DASS SICH DIE GEFAHRENLAGE NICHT WESENTLICH VERBESSERT, ABER DEUTLICH VERÄNDERT HAT.
>
> Sven Janssen, Director Channel Sales DACH, Sophos Technology GmbH, www.sophos.com

DIE FÜNF GRUNDPFEILER EINES ANPASSUNGSFÄHIGEN CYBERSECURITY-ÖKOSYSTEMS

tions, bestehend aus menschlichen Analysten, die über das Sophos Managed Threat Response-Programm in Tausenden von Kundenumgebungen eingebunden sind. In einem zentralen und riesigen Data Lake fließen alle Informationen aus allen Lösungen und Threat Intelligence-Quellen zusammen. Damit sind Echtzeit-Analysen und das Aufspüren verdächtiger Signale möglich, um Attacken zu entdecken und zu verhindern.

Parallel dazu können Kunden, Partnern und Entwickler, Tools und Lösungen mit Hilfe unserer offenen APIs entwickeln und mit dem Eco-System interagieren.

Die fünf Grundpfeiler – Threat Intelligence, Next-Gen-Technologien, Data Lake, APIs und zentrale Verwaltung – bilden ein anpassungsfähiges Cybersecurity-Ökosystem, das ständig dazulernt und sich verbessert. Dieses Ökosystem ist sehr umfassend und leistungsfähig und Unternehmen können je nach Bedarf aus vielen einzelnen Elementen individuell wählen. Viele Kunden beginnen mit dem Sophos Endpoint-Schutz oder einer Firewall und erweitern ihr System entsprechend ihren Anforderungen.

? **Ulrich Parthier:** *Das klingt nach weiterhin guten Geschäftsaussichten für Sophos.*

Sven Janssen: Durch gute Geschäfte können wir uns unsere Labs und vor allem auch die rasante Weiterentwicklung von Sicherheitssystemen leisten, die mit den Machenschaften der Cyberkriminellen Schritt halten können. Mindestens so wichtig ist aber auch die enge Zusammenarbeit mit unseren Channel-Partnern, die das wichtigste Standbein unserer Vertriebsstrategie darstellen. Wir bieten unseren Channel-Partnern ein sehr umfangreiches Sicherheits-Ökosystem, welches sie in ihre eigenen Servicemodelle perfekt integrieren können. Besonders wichtig ist es, die Bedürfnisse der Kunden, von kleinen über mittelständische bis hin zu großen Unternehmen über unsere Partner erfüllen zu können. Und genau da kommt unser integriertes Ecosystem zum Tragen. Der Kunde muss im Grunde nur wissen, dass es da ist und funktioniert. Er muss es aber nicht zwingend selbst beherrschen. Dafür sind unsere Partner hochausgebildete und zertifizierte Experten, die Unternehmen mit begrenztem IT-Stab bei Bedarf mit Services unterstützen können. Hier sehen wir übrigens seit zwei Jahren einen starken Trend. Weltweit beobachten wir im Managed Service-Bereich einen Zuwachs von 67 Prozent allein im letzten Geschäftsjahr.

? **Ulrich Parthier:** *Wie ist Ihre Einschätzung, wo werden wir in 3 bis 5 Jahren mit der Security stehen?*

Sven Janssen: Der Blick in die Vergangenheit und ein vorsichtiger Blick in die Glaskugel sagen uns, 100-prozentige Sicherheit wird es nie geben. Nach heutigem Kenntnisstand ist es leider nur eine Frage der Zeit, bis ein Unternehmen Opfer einer Attacke wird. Allerdings sind wir heute mit den Möglichkeiten der Security weitaus besser aufgestellt als jemals zuvor und wir sind mindestens auf Augenhöhe mit den Entwicklungen der Cyberkriminellen.

Die Einschätzung unserer Labs und auch von mir ist, dass die Komplexität der Angriffe weiter steigt und daher wird auch die Abwehr an zusätzlicher Komplexität gewinnen. Wichtig dabei ist, dass wir bei all unseren Bemühungen für mehr Schutz den Kunden nie außer Acht lassen. Bei allem gebotenen Geschäftssinn geht es nicht um den Selbstzweck von Security-Firmen. Es gilt Unternehmen zu schützen und diese müssen auf die Reise mitgenommen werden – ebenso wie unsere Partner. Hilfreich ist hierbei sicherlich unser Engagement beim offenen Austausch von Forschungsergebnissen und Entwicklungen, die wir der gesamten Branche frei zur Verfügung stellen und damit den Wissenstransfer und Fortschritt fördern.

! **Ulrich Parthier:** *Herr Janssen, wir danken für die spannenden Ein- und Ausblicke in die Security für Unternehmen.*

THANK YOU

ADAPTIVE CYBERSECURITY

EIN SICHERHEITS-ÖKOSYSTEM, DASS SICH DER GEFAHRENLAGE ANPASST

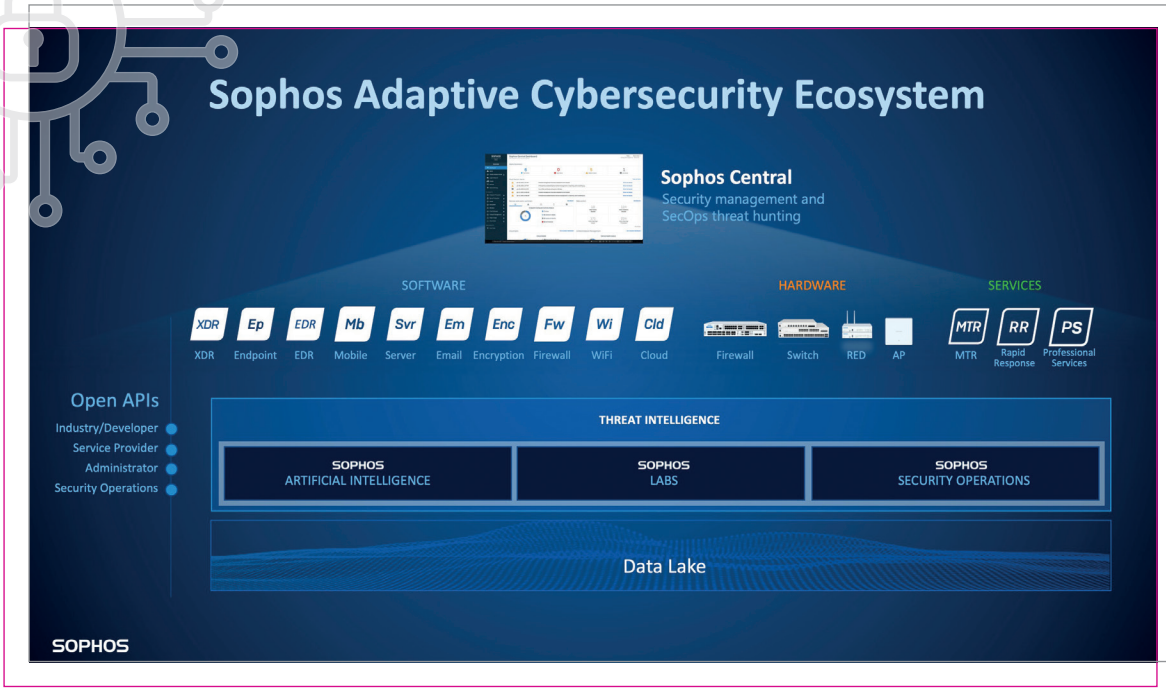
Unternehmen und Organisationen sind kontinuierlich gefordert, den Schutz in ihrem Netzwerk und an ihren Endpoints sicherzustellen. Die Herausforderung dabei ist, dass Cyberkriminelle eine enorme Geschwindigkeit bei der Entwicklung von neuen und gefährlichen Tools für ihre Angriffe an den Tag legen und dass der Schutz gegen die kriminellen Machenschaften damit mindestens Schritt halten muss.

Ein kleiner Exkurs in die „State of Ransomware Studie" von Sophos zeigt die Gefahrenlage: Durchschnittlich sind 46 Prozent der deutschen Unternehmen Ransomware-Angriffen ausgesetzt und 54 Prozent davon haben mit den Folgen zu kämpfen. Der weltweite ermittelte Lösegelddurchschnitt beträgt 14.000 Euro. Rund 32 Prozent der Unternehmen bezahlen das Lösegeld, doch davon erhalten nur acht Prozent ihre Daten vollständig zurück. Wohlgemerkt sind dies nur Erkenntnisse zu Ransomware, die zwar zu den wichtigsten Themen der Security gehört, längst aber nicht die einzige Gefahr darstellt.

„Wir können uns nicht ständig um neue Security kümmern ..."

Die Herausforderung, vor die die Wirtschaft durch die hochbeweglichen und technisch versierten Cyberkriminellen gestellt wird, ist die Notwendigkeit als Unternehmen im Grunde kontinuierlich neue Technologien zum Schutz implementieren und administrieren zu müssen, um sich gegen die immer raffinierten Attacken zu schützen. Künstliche Intelligenz (KI), Endpoind Detection and Response (EDR), Extended Detection & Response (XDR), Secure Access Service Edge (SASE), Security Orchestration, Automation and Response (SOAR), Professional Service Automation (PSA), Remote Monitoring and Management (RMM) oder Zero Trust (ZT) sind nur einige Technologien und Konzepte, die als wichtige Komponenten zur Abwehr modern durchgeführter Attacken gelten.

Vielleicht können Konzerne mit großen und erfahrenen Security-Teams all diese Neuerungen beurteilen, bewerten und mit der vorhandenen Manpower umsetzen. Kleinere und mittelständische Unternehmen jedoch haben hier oft das Nachsehen. Sie werden von der Fülle der neuen Angriffstaktiken oftmals überrollt und sind durch die entsprechenden Sicherheits-Tools mitunter überfordert. Das macht sie zu einem lukrativen Ziel für die Angreifer. Doch es existieren auch für diese Unternehmen Möglichkeiten, alle modernen Sicherheits-Tools einzusetzen. Die Lösung ist ein zentrales Sicherheits-



konzept, in das man diese integriert: ein so genanntes Adaptive Cybersecurity Ecosystem. Mit einer überschaubaren Mannschaft oder in Zusammenarbeit mit spezialisierten IT-Partnern bietet dieses Ökosystem auch kleineren und mittelständischen Unternehmen einen kompletten State-of-the-Art-Schutz – nur eben unkompliziert und vergleichsweise leicht im Handling.

Umfassende Sicherheit

Auf der ständigen Suche nach Möglichkeiten zur Verbesserung von Produktivität und Effizienz haben Unternehmen einen hohen Grad an Digitalisierung geschaffen. Beispielsweise die Migration von Daten und Anwendungen in die Cloud – nicht zuletzt begünstigt durch das dezentrale, mobile Arbeiten seit der Pandemie – hat viele Vorteile mit sich gebracht, darunter niedrigere Betriebskosten sowie eine verbesserte Performance und Skalierbarkeit. Doch je komplexer ein System ist, desto schwieriger wird es, alle Gefahrenbereiche zu identifizieren und in die Sicherheitsstrategie zu integrieren. Intelligente, anpassungsfähige Angreifende haben es genau auf diese Systeme abgesehen.

Mit einem Adaptive Cybersecurity Ecosystem wie es Sophos anbietet, sind Unternehmen umfassend geschützt und vor allem den Cyberkriminellen den entscheidenden Schritt voraus. Und: das Unternehmen, muss dafür keinen Spezialistenstab aufbauen.

Das Ökosystem umfasst Automatisierung und die Kompetenz menschlicher Spezialisten, um den Angreifern zuvorzukommen, indem es kontinuierlich lernt. Es basiert auf den gesammelten Bedrohungsdaten der SophosLabs, Sophos Security Operations (menschliche Analysten, die in Tausenden von Kundenumgebungen eingebunden sind) und der Künstlichen Intelligenz (KI). Ein einziger, integrierter Data Lake (großer und ständig wachsender Informations-Pool über Technologien, Taktiken und Verhaltensweisen der Angreifer) fasst Informationen aus allen Lösungen und Threat Intelligence-Quellen zusammen. Echtzeit-Analysen ermöglichen es Verteidigern, Einbrüche zu verhindern, indem sie verdächtigen Signale finden.

DAS ADAPTIVE CYBERSECURITY ÖKOSYSTEM UMFASST DIE AUTOMATISIERUNG UND DIE KOMPETENZ MENSCHLICHER SPEZIALISTEN, UM DEN ANGREIFERN ZUVORZUKOMMEN, INDEM ES KONTINUIERLICH LERNT.

Michael Veit, Sicherheitsexperte, Sophos Technology GmbH, www.sophos.com

Soweit zur Integration aller denkbaren Schutzmechanismen und Tools in einem Ökosystem. Das entscheidende für viele Unternehmen ist allerdings, dass innerhalb einer solchen Methode nicht einzelne Komponenten eingerichtet und verwaltet werden müssen, sondern alles über eine zentrale Oberfläche vergleichsweise leicht administriert werden kann – und zwar intern vom eigenen IT-Team oder vom vertrauten externen Dienstleister als Managed Service. Hiermit bietet sich für viele Unternehmen eine Grundlage, um ihre Security zu stärken und den heutigen Gefahren Stand zu halten.

Die menschlichen Bedrohungsjagd

Die Erkenntnisse zeigen, dass es mit einer rein automatisierten Bedrohungsjagd, -abwehr und -prävention leider nicht mehr getan ist. Angreifer führen ihre Attacken oft über Wochen und Monate hinaus durch, um die Sicherheitsmechanismen in Unternehmen geschickt zu umgehen. Wird eine Attacke erkannt, wurden die Vorbereitungen dafür meist schon vor geraumer Zeit unbemerkt durchgeführt. Dies trifft insbesondere zu, wenn die Cyberkriminellen ihre Angriffe teils manuell mit menschlicher Expertise steuern und durchführen. Genau an diesem Punkt treffen automatisierte Sicherheitsmechanismen an ihre Grenzen und es werden menschliche Experten benötigt, um den Gangstern rechtzeitig auf die Schliche zu kommen.

Ein Sicherheitsteam, das diese Disziplin vollständig beherrscht, werden sich nur wenige Unternehmen leisten können. Jedoch existiert die Möglichkeit, sich diese Dienste von ausgewiesenen Experten einzukaufen. Die konkreten Aufgaben dieser Teams sind das Aufspüren komplexer Bedrohungen und Vorfälle und die Bestimmung von Ausmaß und Schwere von Bedrohungen. Sie ergreifen Maßnahmen, um die Bedrohung nicht nur an der auffälligen Stelle, sondern im gesamten Firmennetz zu eliminieren. Schließlich geben sie konkrete Ratschläge, um die Ursache wiederholt auftretender Vorfälle zu bekämpfen.

Eine solche Expertise ist besonders erfolgreich, wenn sie in das Gesamtkonzept für die Sicherheit im Unternehmen eingebunden wird. Selbstverständlich können die Experten, beispielsweise von Sophos mit dem Managed Threat Response Service (MTR), zusätzlich zu jeglicher Security-Lösung hinzugezogen werden. Die geballte Schlagkraft kann das Team aber dann ausspielen, wenn es innerhalb des Adaptive Cybersecurity Ecosystems angesiedelt ist und auf alle integrierten Informationen, Warnungen und Erkenntnisse Zugriff hat. Auf diese Weise ist leistungsstarke Security mit Machine Learning und Künstlicher Intelligenz mit menschlicher Expertise zu einem schlagkräftigen Ökosystem vereint.

Michael Veit

SAVE THE DATE!

CYBERSECURITY

DIE GEFAHR AUS DEM OFF

Digitalevent

8. Februar 2022

#cybersec2022

NATIVE SECURITY

MICROSOFT SECURITY FUNKTIONEN BESSER MANAGEN

Betriebssystem-Anbieter wie Microsoft haben ihre integrierten Sicherheitsfunktionen für Endgeräte in den letzten Jahren deutlich erweitert und professionalisiert. Analysten sprechen hier von „nativer Sicherheit" oder „Native OS-Security". Unter diese Begriffe fallen dann beispielsweise Funktionalitäten zur Datensicherheit und -verschlüsselung, Authentifizierung, Antiviren- und Zero-Day-Exploit-Schutz, Firewall Management und sicheren Konfiguration. Diese Funktionen sind in das Betriebssystem integriert und stehen Lizenznehmern der Betriebssysteme „nativ" zur Verfügung.

Tools wie der Microsoft Defender Antivirenschutz oder die BitLocker Festplattenverschlüsselung können mittlerweile mit Lösungen von Drittanbietern konkurrieren und diese sogar weitestgehend ersetzen.

Warum also sollten IT-Administratoren trotzdem Speziallösungen von Drittanbietern in Erwägung ziehen?

Zum einen gelten native Lösungen in Punkto Handhabung, Einrichtung und Verteilung unternehmensweiter Sicherheitsprofile in größeren Organisationen bei IT-Managern nicht als komfortabel zu verwalten. Zum anderen: Native Lösungen generieren zwar viele nützliche Daten und Protokolldateien, bieten aber nicht die Möglichkeit, diese wertschöpfend weiter zu verarbeiten, um beispielweise anomales Verhalten auf den Endpunkten zu identifizieren. So bieten native Lösungen wichtige, grundlegende Schutzfunktionen, die für einen umfassenden Schutz aber unbedingt komplettiert werden müssen und mehr Komfort in der Handhabung benötigen: Dies alles mit dem Ziel, maximale Sicherheit zu schaffen.

Unter der Devise „IT Security made easy" hat sich der Endpoint Security Spezialist DriveLock zum Ziel gesetzt, mehr aus den nativen Security-Tools herauszuholen.

Zentrale und aufwandsreduzierende Konfiguration

Alle Native Security Management-Module von DriveLock, die auf Microsoft Einzellösungen aufbauen, haben gemeinsam, dass sie in einer zentralen Management-Konsole konfiguriert werden. So wird die ohnehin komplexe Konfiguration vereinfacht und der Aufwand minimiert, da Administratoren nicht an unterschiedlichen Stellen Einstellungen vornehmen müssen.

Zentrale Übersichten und ganzheitliche Schutzniveaus

Auch die Übersichten, Dashboards und konfigurierbaren Reports für Analysen und für das Monitoring sind zentral in einer Überwachungskonsole abgebildet. Mit einer Drittanbieter-Lösung können Sie die aktuellen Sicherheitsniveaus über alle Schutzmaßnahmen (Verschlüsselung, Antivirenschutz, Applikationskontrolle) hinweg ganzheitlich darstellen. Damit erhalten Sie eine vollständige Compliance-Übersicht aus allen Daten und erfüllen gesetzliche Nachweispflichten.

Zentrales Management von Sicherheitsprofilen

Große Unternehmen mit Tausenden von Arbeitsplätzen müssen einer Vielfalt von unterschiedlichen Berechtigungen und Profilen für die Softwarenutzung ihrer Mitarbeitenden gerecht werden. Eine Speziallösung erlaubt das Einrichten zentraler Sicherheitsrichtlinien und deren Verteilung im Unternehmen. Das reduziert Aufwand. Mit DriveLock beispielsweise werden Ihre Sicherheitsprofile unternehmensweit verteilt und sofort eingerichtet.

Reduktion der Anzahl von Agenten

Jede Endpoint Security Lösung benötigt normalerweise einen Agenten auf dem Endpoint, der für die Überwachung zuständig ist. Mit Drivelock benötigen Sie nur einen einzigen Agenten auf dem Endpoint. Das spart Ressourcen und vermeidet Inkompatibilitäten.

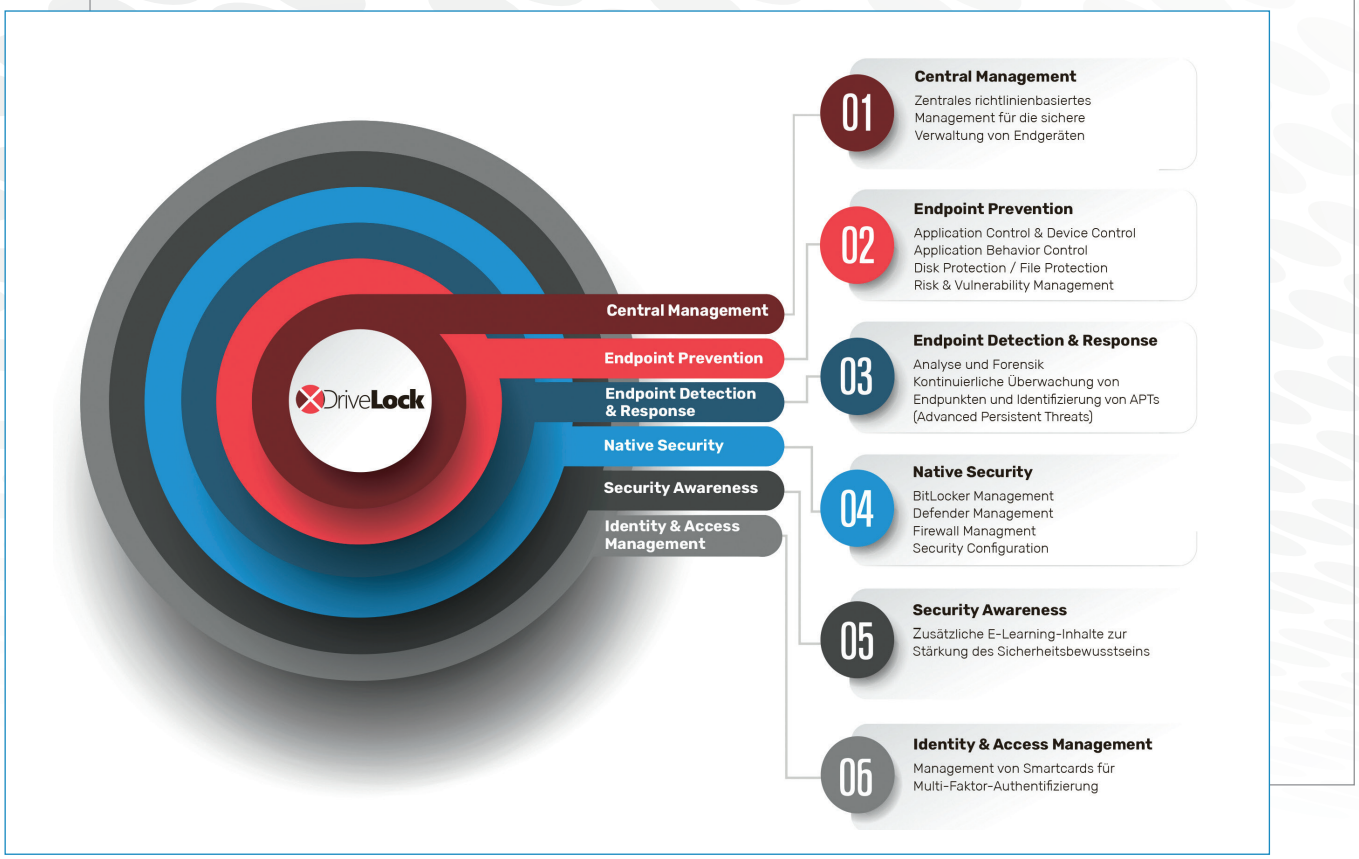
Der Anbieter kann die vom Betriebssystem gesammelten Ereignisdaten zur Verhaltensanalyse in seine Produkte integrieren, und reichert deren Ergebnisse an. Ein EDR-Tool (Endpoint Detection & Response) kann so das Verhalten auf den Endpunkten noch besser analysieren und Anomalien feststellen. Scan-Ergebnisse des Defender Antivirus können für weiterführende Produkte wie Applikationskontrolle genutzt werden, oder der Scanner untersucht bei Anschluss externer Geräte deren Inhalte.

Die Lösung optimiert aber nicht nur das Management der nativen Security Lösungen, sondern ergänzt sie auch um wichtige Funktionen:

1. BitLocker Management

Microsofts Festplattenverschlüsselung BitLocker ist mit steigenden regulatorischen Anforderungen im Unternehmen zusehends nicht komfortabel handhabbar und für strenge Sicherheitsvorschriften, zum Beispiel 2-Faktor-Authenfizierung, nicht ausreichend genug.

DriveLock BitLocker Management ermöglicht eine zentrale – auch vom Active Directory (AD) unabhängige – Konfiguration.



Der Anbieter erweitert die Identifikation des Users für den Zugriff auf verschlüsselte Festplatten um eine leistungsfähigere Pre-Boot-Authentifizierung: DriveLock PBA für BitLocker. Sie ermöglicht nicht nur den sicheren, vertrauenswürdigen Start des Rechners (Secure Boot), sondern ergänzt den limitierten Funktionsumfang der BitLocker eigenen PBA. Sie unterstützt Zwei-Faktor-Authentifizierungsmethoden über Smartcards und Tokens und ermöglicht Single-Sign-On an Windows. Bei verlorenen Zugangsdaten bietet sie eine Self-Service-Notfallanmeldung. Zudem ist im Notfall ein sicheres One-Time Recovery mit automatischem Schlüsseltausch möglich.

2. Local Firewall Management

Im Rahmen des Firewall Managements regeln Sie mit DriveLock-Richtlinien sehr einfach die ein- und ausgehenden Verbindungen. Sie können die Microsoft Firewall-Regeln im laufenden Betrieb um zusätzliche Kriterien wie Zeit, Netzwerkverbindung, Computer oder sogar Benutzer erweitern. In Anhängigkeit davon, ob Sie im Unternehmens-LAN oder von Zuhause arbeiten, können Sie Port-Freigaben automatisch aktivieren bzw. deaktivieren.

3. Defender Antivirus Management

Antivirenprogramme sind wichtig, aber nur EIN Baustein in einer ganzheitlichen Sicherheitslösung. DriveLock ermöglicht nicht nur die Verwaltung von Microsoft Defender Antivirus an zentraler Stelle, sondern die Weiterverarbeitung der Scanergebnisse durch Module wie Applikationskontrolle oder EDR. Der Virenscanner wird auch beim Verbinden von externen Laufwerken gestartet. Diese werden erst freigeschaltet, wenn keine Schadsoftware festgestellt wurde.

Für die Konfiguration mit DriveLock sind keine Microsoft Management-Lösungen wie Intune oder SCCM notwendig. Auch das Verwalten einzelner Gruppenrichtlinien entfällt.

4. Lokale Benutzer und Gruppen

Ziel dieser Funktionalität ist der Schutz vor „Privilege Escalation" Angriffen, in denen versucht wird, auf administrative Konten zuzugreifen oder sich diese anzueignen. Lassen Sie den Anbieter Ihre lokalen Benutzer und Gruppen verwalten, um die Sicherheit zu erhöhen, ohne die Produktivität der Endbenutzer auf den Endgeräten zu beeinträchtigen. Jedes lokale Konto auf einzelnen Rechnern kann angelegt, aktualisiert oder gelöscht werden. Zufällige Passwort-Vergaben sind ebenfalls möglich. Regeln können so angepasst werden, dass sich die Einstellungen automatisch ändern, wenn ein Benutzer vom Home Office ins Firmennetzwerk wechselt und umgekehrt. Der DriveLock Agent speichert jedes Passwort sicher verschlüsselt, so dass ein Arbeiten mit einer „run as" Kommandozeile weiterhin möglich ist. Bestehende Mitglieder bleiben erhalten, auch wenn sich Gruppennamen ändern.

Verleihen Sie Ihren Microsoft Security Tools den richtigen Schub. So schaffen Sie eine effektivere Sicherheit für unsere Anwender, als es mit nativen Funktionen allein möglich wäre.

Andreas Fuchs | www.drivelock.de

SECURITY AWARENESS

5 SCHRITTE, WIE SIE DAS SICHERHEITSBEWUSSTSEIN IM UNTERNEHMEN LANGFRISTIG VERBESSERN

Das Sicherheitsbewusstsein im Unternehmen und bei Angestellten zu schärfen und vor allem aufrecht zu erhalten, ist eine regelmäßige Aufgabe. Ähnlich wie das Prinzip des lebenslangen Lernens gibt es hierbei keinen Endpunkt, den man erreichen kann und an welchem man sich nie wieder Gedanken machen muss. Bedrohungen und Risiken im IT-Umfeld sind in den meisten Fällen dynamisch. Sie verändern sich und entwickeln sich weiter.

UM DAS SICHERHEITSBEWUSSTSEIN BEI NUTZERN IM UNTERNEHMEN SO HOCH WIE MÖGLICH ZU HALTEN, BEDARF ES EINER OFFENEN, KONSTRUKTIVEN UND REGELMÄSSIGEN KOMMUNIKATION ZU MÖGLICHEN GEFAHREN.

Ari Albertini, Revenue Flow Manager, Mitglied der Geschäftsleitung, FTAPI Software GmbH, www.ftapi.com

Entscheidend für eine erfolgreiche Security Awareness in Unternehmen ist daher eine Kombination aus technischen, erzieherischen und kulturellen Maßnahmen. Je besser diese ineinandergreifen, desto geringer ist die Chance von Sicherheitsvorfällen, Hacks oder Leaks.

1. Fehler passieren – immer

Am Anfang eine nachhaltigen Security-Awareness-Strategie steht die wichtige Erkenntnis, dass Fehler in der ein oder anderen Form immer passieren. Das soll keine Entschuldigung sein, sich nicht anzustrengen, sondern dient dem Verständnis, dass es immer Verbesserungsmöglichkeiten gibt und dass es oft auch Fehler braucht, um Dinge zu erkennen. Oder wie in diesem Fall, sie sicherer zu gestalten. Es geht bei der IT-Sicherheit im Prinzip um konstante Risikominimierung. Das mag für viele hart und ernüchternd sein, bietet aber die Grundlage für alles Weitere.

Das bedeutet, dass es nicht nur wichtig ist, Fehler zu vermeiden, sondern aus ihnen die richtigen Schlüsse zu ziehen. Aber wo fängt der Fehler an?

2. Die Fehlerkette endet zwar meist bei Angestellten – sie beginnt aber oftmals woanders

Wenn man sich IT-Sicherheitsvorfälle ansieht und sich fragt „Wie konnte das denn passieren?“, tendiert man schnell dazu, eine einzelne Person verantwortlich zu machen. Herr Müller zum Beispiel hat einen Link geöffnet und so einem Virus Tür und Tor geöffnet. Fehler sind in den meisten Fällen keine Einzelhandlungen mit böser Absicht - dann wären Sie genaugenommen auch kein Fehler sondern kriminelle Akte und Sabotage. Das sogenannte „menschliche Versagen“ steht oft am Ende einer Fehlerkette, nicht am Anfang. Ein Fehler muss organisatorisch möglich sein, um gemacht werden zu können. Das klingt sehr theoretisch, ist aber durchaus praktisch zu verstehen.

Unternehmen sind Organisationen, in denen bestimmte Regeln herrschen. Mitglieder einer Organisation bewegen sich innerhalb dieses Sets an Regeln und wenden sie in der täglichen Arbeit so gut es geht an. Wenn ich den Mitgliedern einer Organisation aber nicht die richtigen Werkzeuge oder die passenden Anweisungen oder auch Freiheiten mitgebe, um die von mir aufgestellten Regeln zu befolgen, dann kann ich schwer erwarten, dass alles rund läuft. Wenn ich dann noch eine Kultur schaffe und aufrechterhalte, in welcher der offene Umgang mit Fehler bestraft wird, komme ich in einen Teufelskreis. Dann werden Fehler verheimlicht, ziehen verheerende Kreise und können nicht für die Zukunft genutzt werden können.

Wie gesagt, lassen sich Fehler nie ganz vermeiden. Allerdings lassen sich viele Fehlerketten frühzeitig unterbrechen und

Bild: FTAPI Software GmbH

ihre Auswirkungen abmildern oder sogar verhindern - mit den richtigen Maßnahmen, Programmen und Trainings.

3. Jeden Fehler offen analysieren und daraus lernen

Anstatt die Frage zu stellen „Wer ist schuld?" lautet die wichtigere Frage „Wie können wir verhindern, dass es sich wiederholt?" Ein Ansatz hierfür mit Blick auf IT-Sicherheit wäre auch: Ein Fehler bedeutet, dass die Abläufe nicht gut genug waren, um diesen zu verhindern. Die `Schuld` ist eher im System zu suchen.

Es muss innerhalb einer Organisation die Möglichkeit geben, Fehler frühzeitig zugeben zu können ohne, dass gleich drakonische Maßnahmen verhängt werden. Je früher auf etwas hingewiesen werden kann, desto größer ist die Wahrscheinlichkeit, dass man erfolgreiche Gegenmaßnahmen ergreift und es in Zukunft verhindert. Haben Angestellte hingegen Angst, auf etwas hinzuweisen, geht die Fehlerkette weiter.

Unternehmen müssen dafür genau wissen, an welchen Stellen besonders kritische und sensible Daten verwendet werden. Dieser Bestandsaufnahme folgt dann die Erarbeitung einer IT-Sicherheitsrichtlinie, in der man etwa festlegt, welche Datentypen und welche Programme verwendet werden müssen, welche Programme benutzt werden dürfen, wie der Austausch mit extern geregelt ist und was im Falle eines Notfalls zu tun ist.

Die Gesamtverantwortung dafür kann nicht komplett delegiert werden. Denn sie bleibt beim obersten Führungspersonal, welches das Vorhaben initiieren, steuern und auch kontrollieren muss. Auch muss es notwendige Ressource bereitstellen.

Jedem bedeutenden Fehler muss ein Learning folgen und dieses muss auch kommuniziert und thematisiert werden.

4. Schulungen und Best Practices regelmäßig thematisieren

Alle Angestellten, die mit kritischen Daten und entsprechenden Programmen arbeiten, sollten in regelmäßigen Abständen an Sicherheitsschulungen teilnehmen.

Die Nutzungsweise neuer Software muss entsprechend beigebracht werden. Wenn man eine sichere Lösung falsch benutzt, ist das kontraproduktiv. Unsere Erfahrung etwa im sicheren Datentransfer zeigt, dass die Nutzungsrate beim Kunden sehr hoch ist, wenn die Lösung leicht zu verstehen ist und wenn sich für die Nutzer möglichst wenig ändert.

Und wenn in der Öffentlichkeit über größere Sicherheitslecks bei Firmen oder Behörden berichtet wird, sollte man das im Blick behalten und entsprechend intern thematisieren. Das kann etwa in einem Webinar passieren. Oder es ist mal eine gemeinsame Mittagspause mit kurzer Präsentation. Dort kann etwa eine Datenschutzbeauftragte Learnings aus aktuellen Beispielen im Unternehmenskontext erläutern.

Viele Firmen schicken Ihre neuen Angestellten in Onboarding-Programme. Bei diesen geht es meistens um Angelegen-

heiten mit der Personalabteilung oder der Einrichtung der IT. Schulungen für Datensicherheit sind hier eine ideale Ergänzung.

5. Automatisierte Sicherheit bei Systemen und Programmen als zusätzliche Sicherheitsstufe

Grundsätzlich sollte es für Nutzer so einfach wie möglich sein, IT-Sicherheitsvorkehrungen zu befolgen. Die Nutzer müssen verstehen, dass Sicherheitsbewusstsein nicht nach dem Login endet. Sie müssen dazu abgeholt werden, welche Programme sie nutzen und nicht nutzen dürfen. Man denke hier etwa an scheinbar kostenlose und browserbasierte Filesharing-Portale, die oftmals aus datenschutzrechtlicher Sicht ein Albtraum sind. Hier kann eine entsprechend aufgestellte IT ebenfalls mit Blocklisten einiges verhindern, aber sie sollte nicht auf sich allein gestellt sein.

Gleiches gilt allerdings auch für etwaige Administrations-Einstellungen. Ähnlich wie bei Passwortrichtlinien oder erwähnten Blocklisten bieten einige Lösungen Konfigurationen, die eine bestimmte ungewollte Art der Softwarenutzung automatisch unterbinden. Beispielsweise lässt sich einstellen, dass E-Mails mit Anhängen bestimmter Dateiformate oder

-größen erst gar nicht verschickt werden können. Unternehmen sollten sich aber nicht nur auf die Technik verlassen. Jede technische Maßnahme wird umso effektiver, je sicherheitsbewusster die Angestellten sind.

Um das Sicherheitsbewusstsein bei Nutzern im Unternehmen so hoch wie möglich zu halten, bedarf es einer offenen, konstruktiven und regelmäßigen Kommunikation zu möglichen Gefahren sowie Schulungen zur richtigen Anwendung von Programmen abgerundet von technischen Einstellungen, die versehentliche Fehler systembedingt gar nicht erst zulassen.

Ari Albertini

DATEN SCHÜTZEN

DER RANSOMWARE ENDLICH HERR WERDEN

Die Ransomware-Welle reißt einfach nicht ab. Mittlerweile lesen sich die Opfer wie ein Who-is-Who der internationalen Wirtschaft. Aber auch in Deutschland kommt es immer wieder zu erfolgreichen Attacken mit verheerenden Folgen, wie zuletzt etwa bei MediaMarkt/Saturn, wo infolge des Angriffs unter anderem die Kassensysteme ausgefallen sind, bei der Funke Mediengruppe, welche wochenlang nur einen Notbetrieb aufrechterhalten konnte, beim Automobilzulieferer Eberspächer, der erst nach zwei Wochen seine Produktion wieder hochfahren konnte, oder beim Medizin-Dienstleister Mediatixx mit Auswirkungen auf Tausende Arztpraxen.

Die Taktiken ändern sich, der Schaden bleibt

Zum andauernden „Erfolg" der Ransomware trägt sicherlich auch bei, dass die Cyberkriminellen ihre Taktiken und Techniken laufend anpassen. Früher folgten Ransomware-Angriffe meist dem Gießkannen-Prinzip. Heute dringen Angreifer gezielt und sehr subtil in Unternehmen ein, um an wertvolle, sensible Informationen zu gelangen. Sie gehen unauffällig vor, indem sie – oftmals durch Phishing gewonnene – Anmeldedaten autorisierter Benutzer verwenden, um nach wichtigen Informationen zu suchen. Oder sie nutzen sie, um innerhalb des Netzwerks mehr Rechte zu erhalten, bevor sie Daten stehlen, verschlüsseln und ein Lösegeld fordern. Hinzu kommt das Geschäftsmodell der Ransomware-as-a-Service, das wesentlich zur massenhaften Ausbreitung beigetragen hat.

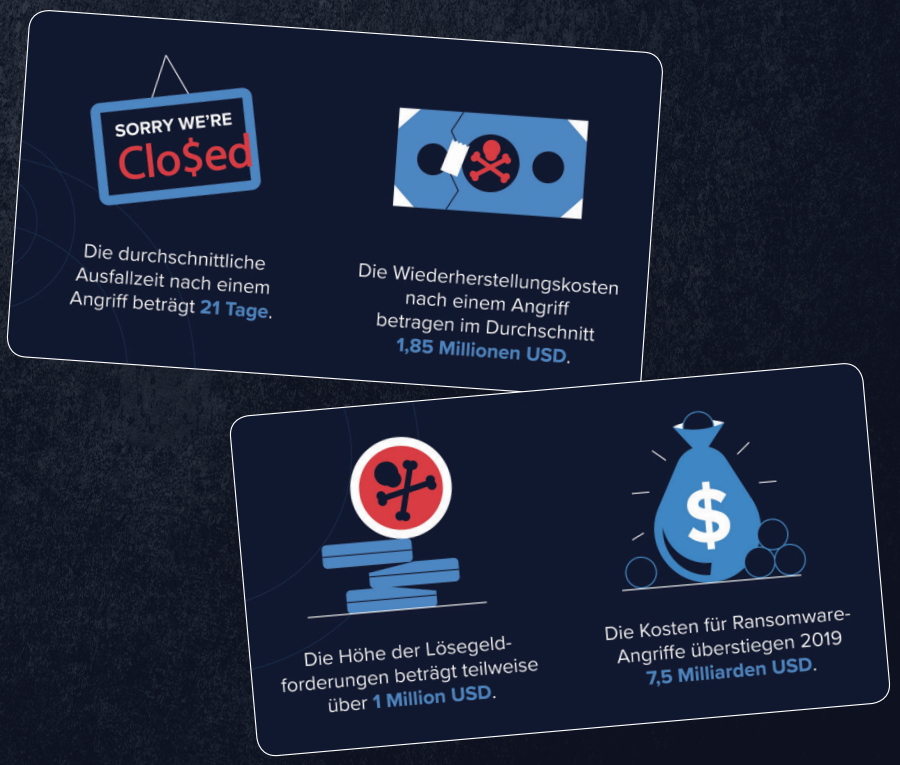
Dabei zeigt die Ransomware sehr gut die generelle Problematik der Datensicherheit: Daten müssen dort geschützt werden, wo sie sind. Man muss in der Lage sein, bei abnormalem Verhalten Alarm zu schlagen und vollständig zu verstehen, was passiert ist. So kann man der Ursache auf den Grund gehen, eine effektive Forensik durchführen und sehr schnell zu einer Lösung kommen. Dabei ist es von größter Wichtigkeit, alle Plattformen einzubeziehen und einen Kontext herzustellen, um präzise erkennen zu können, was passiert und aus welcher Richtung ein Angriff erfolgt.

Explosionsradius reduzieren

Angreifer werden es immer hinter den Perimeter, also hinter die traditionell stark gesicherten Grenzen der Unternehmens-Infrastruktur, und in die Systeme schaffen. Entsprechend sollten Sicherheitsverantwortliche ihr Augenmerk darauf richten, wie sie mit diesem unvermeidlichen Feind im Inneren umgehen. In erster Linie bedeutet dies, den Schaden zu reduzieren, den ein Eindringling anrichten kann. Hierbei spielen Zugriffsrechte eine entscheidende Rolle. Untersuchungen zeigen immer wieder, dass ein Mitarbeiter im Durchschnitt Zugriff auf mehrere Millionen Dateien hat. Wird ein solches Konto etwa durch Phishing korrumpiert, hat auch der Angreifer Zugriff auf Millionen Dateien. Diesen enormen Explosionsradius gilt es gemäß dem Least-Privilege-Ansatz auf ein Minimum zu reduzieren. Dadurch ist die Gefahr natürlich nicht vollständig gebannt, das Risiko und das Ausmaß jedoch schon deutlich reduziert. Kommt dann noch die intelligente Analyse des Nutzerverhaltens hinzu, die auffälliges Verhalten wie das reihenweise Öffnen, Kopieren oder Verschlüsseln von Daten erkennt, lassen sich Angriffe nahezu aller Art frühzeitig erkennen und automatisiert stoppen.

Im Grunde lässt sich Datensicherheit auf drei einfache Fragen reduzieren: Wissen wir, wo unsere wichtigen Daten gespeichert sind? Haben nur die richtigen Personen Zugang zu den Daten? Und ist gewährleistet, dass die Daten korrekt verwendet werden? Kann man alle drei mit „Ja" beantworten, sind die Daten sicher. Ist die Antwort auf nur eine der Fragen ein „Nein", sind die Daten nicht sicher. Dies gilt für Ransomware-Attacken gleichermaßen wie für Insider-Bedrohungen und Datendiebstähle.

Michael Scheffler, www.varonis.com/de



PASSWORTLOS MIT PASSWORT

SO GEHT MARKETING HEUTE

Passwortbasierte Anmeldeprozesse am PC sind weder sicher noch komfortabel. Viele Sicherheitsanbieter propagieren deshalb passwortlose Lösungen – die in aller Regel leere Marketingversprechen sind, da im Backend weiterhin Kennwörter gespeichert werden. Eine echte Passwortlosigkeit bieten Lösungen, die auf einem Public-Key-Verschlüsselungsverfahren basieren.

Beim Rechner-Login werden traditionell Passwörter verwendet, die allerdings nur eine minimale Sicherheit gewährleisten. So sind auch 80 Prozent aller Sicherheitsvorfälle auf gestohlene, ausgespähte oder zu schwache Passwörter zurückzuführen. Unternehmen denken deshalb über Alternativen nach, vor allem über Lösungen, die eine hochsichere und anwenderfreundliche passwortlose Anmeldung versprechen.

WENN EIN UNTERNEHMEN NICHT LEICHTGLÄUBIG DEM MARKETINGVERSPRECHEN DER PASSWORTLOSEN AUTHENTIFIZIERUNGSLÖSUNG VERTRAUEN MÖCHTE, SOLLTE ES IMMER GENAU PRÜFEN, OB ES NUR UM EINE ANWENDERORIENTIERTE ODER UM EINE ECHTE PASSWORTLOSIGKEIT GEHT.

Jochen Koehler,
Leiter der Region Zentraleuropa, HYPR,
www.hypr.com

Dabei ist allerdings Vorsicht geboten. Nicht alles, was als passwortlos angeboten wird, kommt auch wirklich ohne Passwort aus. Ein Beispiel dafür sind One-Time-Password (OTP)-Token, die bei Smartphone-Apps im Online-Banking genutzt werden. Sogenannte Authenticator-Programme vereinfachen den Anmeldeprozess, indem der Nutzer lediglich dazu aufgefordert wird, eine Push-Anfrage auf seinem Smartphone zu bestätigen. Dass sich auch dahinter eine passwortbasierte Anmeldung verbirgt, die vor Angreifern nur bedingt schützen kann, ist oftmals nicht bekannt. Im Backend existieren weiterhin Passwörter als „Shared Secrets", also Credentials, die etwa in einer Datenbank gespeichert sind. Solche Verzeichnisse sind aus Sicherheitsgründen immer problematisch, da ein Zugriff Hackern vielfältige Angriffsszenarien eröffnet.

Echte Passwortlosigkeit braucht kein Passwort

Bei der Einführung einer passwortlosen Lösung sollten Unternehmen somit darauf achten, dass sie eine echte passwortlose PC-Anmeldung und Authentifizierung bietet, also auch im Backend keine Kennwörter oder PINs vorhanden sind. Ein solche Lösung ersetzt Passwörter durch sichere kryptografische, asymmetrische Schlüsselpaare. Damit sind Hackerangriffe auch nur auf einzelne Personen und Geräte denkbar, nicht aber auf eine Datenbank mit zahlreichen Anmeldeinformationen.

Lösungen für die passwortlose Anmeldung, die Kennwörter durch sichere kryptografische, asymmetrische Schlüsselpaare ersetzt, sind bereits seit Längerem verfügbar. So ist mittels Smartcards und Public-Key-Kryptografie eine hochsichere Authentifizierung an PC-Systemen möglich. Dieses Verfahren wird allerdings kaum genutzt, da es den Einsatz spezifischer Endgeräte mit adäquaten Kartenlesern voraussetzt. Inzwischen gibt es dazu aber sichere und komfortable Alternativen, etwa die Nutzung von Smartphones als Smartcards. Voraussetzung ist lediglich, dass der von der FIDO (Fast IDentity Online)-Allianz definierte offene Industriestandard für die Zwei-Faktor-Authentifizierung unterstützt wird. Die Multi-Faktor-Authentifizierung (MFA) ist ein zentrales Kriterium, um eine höchstmögliche Sicherheit zu erzielen.

Das Smartphone wird zur Smartcard

Wird eine solche Smartphone-basierte Authentifizierungslösung bereits bei der Anmeldung am Desktop genutzt, ist ein Schutz vor potenziellen Angriffen zum frühestmöglichen Zeitpunkt gewährleistet. Die Unterstützung offener Standards wie FIDO oder von Protokollen wie Radius bietet darüber hinaus einen weiteren Vorteil: Ein Anwender kann dann zusätzlich erforderliche Authentifizierungen im Netzwerk ebenfalls gänzlich passwortlos durchführen, etwa bei der Nutzung von VPNs (Virtual Private Networks), SSO (Single Sign-On)-Verfahren und Remo-

te-Desktop-Verbindungen oder in VDI (Virtual Desktop Infrastructure)-Umgebungen.

In einer echten passwortlosen Architektur wird die Verwendung von Shared Secrets wie Passwörtern, PINs, SMS-Codes oder OTPs durch eine Public-Key-Kryptografie ersetzt. Die zur Authentifizierung erforderlichen Schlüsselpaare werden für jeden Anwendungsfall individuell generiert. Dabei verbleiben die privaten Schlüssel jederzeit auf dem mobilen Gerät des jeweiligen Benutzers. Sie sind sicher gespeichert auf der Hardwareebene, das heißt in der TrustZone – bei Apple iOS in der Secure Enclave und bei Android im Trusted Execution Environment. Die öffentlichen Schlüssel werden in einer solchen Lösungsumgebung auf einem passwortlosen Authentifizierungsserver abgelegt.

Interoperabilität ist unverzichtbar

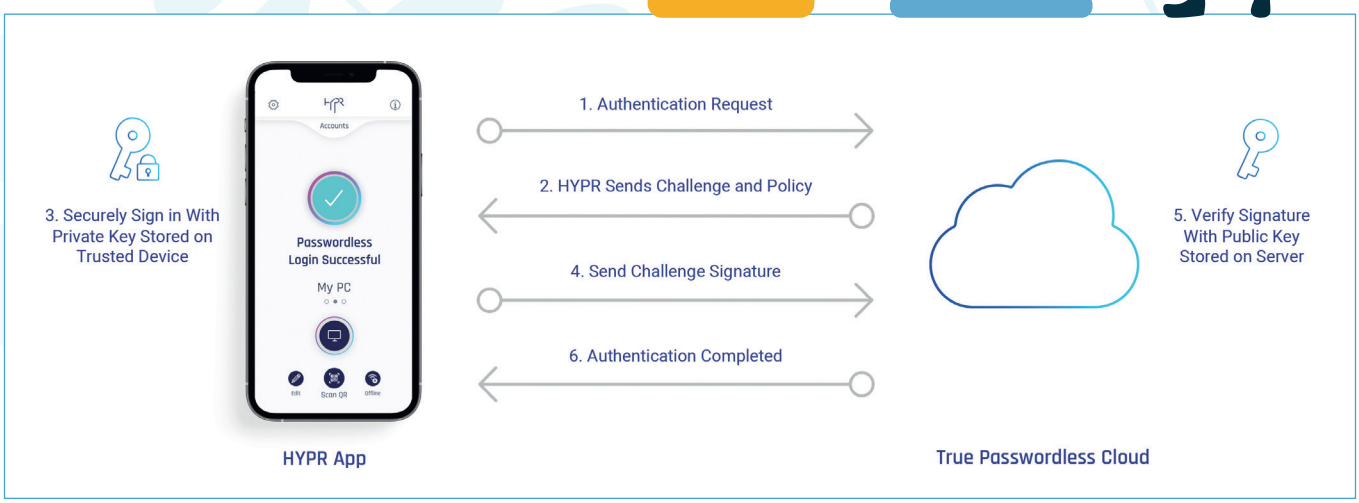
Wichtig ist, dass bei der Einführung einer passwortlosen Lösungsarchitektur kein Silosystem entsteht. Das heißt, eine passwortlose MFA-Lösung muss sich auch flexibel und nahtlos in bestehende Systeme wie Identity-Access-Management-Lösungen oder Cloud-Dienste einbinden lassen. Darüber hinaus sollte auch eine Kompatibilität zu anderen echten passwortlosen Techniken gegeben sein. Beispiele dafür sind Security-Token wie Smartcards und FIDO-Sticks.

Eine echte passwortlose MFA bietet unter anderem folgende Vorteile:

- Entlastung des IT-Helpdesks, der einen hohen Aufwand bei vergessenen Kennwörtern, System-Lockouts oder fehlgeschlagenen Änderungsprozeduren hat
- Vermeidung von Phishing- und Credential-Stuffing-Attacken
- Steigerung der Mitarbeiterproduktivität durch die Beseitigung der zeitaufwendigen Passwortprozeduren und Multi-Faktor-Anmeldeprozesse für unterschiedliche Cloud-Dienste
- Investitionsschutz, da vorhandene Lösungen wie Identitätsplattformen weiterverwendet werden können.

Wenn ein Unternehmen nicht leichtgläubig dem Marketingversprechen der passwortlosen Authentifizierungslösung vertrauen möchte, sollte es immer genau prüfen, ob es nur um eine anwenderorientierte oder um eine echte Passwortlosigkeit geht. Letztere ist nur dann wirklich gegeben, wenn nicht nur der Nutzer ohne Passwörter agieren kann, sondern wenn auch im Backend keine Kennwörter vorhanden sind, also mit gespeicherten Credentials etwa in einer Datenbank. Ausschließlich eine gänzlich passwortlose MFA bietet eine höchstmögliche Sicherheit.

Jochen Koehler



Die Lösung HYPR True Passwordless MFA vereinfacht den Anmeldeprozess am PC. Der Prozess vom Login bis zur Zugriffsgewährung im Überblick. (Quelle: HYPR)

ZERO TRUST

MEHR ALS NUR BLOCKIEREN

Zero Trust ist derzeit eines der beliebtesten Schlagworte in der Cybersecurity und wird entsprechend häufig und ungenau verwendet. Gemeinsam haben alle Ansätze, dass der Grundsatz von Zero Trust darin besteht, von „Vertrauen, aber überprüfen" zu „Überprüfen und dann vertrauen" überzugehen. Gleichwohl ist diese Formulierung gerade in nicht statischen Umgebungen problematisch: „Überprüfen und dann vertrauen" geht davon aus, dass man, sobald man sich vergewissert hat, einsatzbereit ist. Und wenn das nicht der Fall ist, ist eine permanente Sperrung gerechtfertigt. Die erste Option hinterlässt eine erhebliche Lücke in der Verteidigung eines Unternehmens, und die zweite Option beeinträchtigt die Produktivität des Unternehmens.

Kontinuierliche Anpassung des Vertrauens

In einer Cloud-first-Umgebung ohne Perimeter wird jedoch eine kontinuierliche Anpassung benötigt. Die eindeutige Formulierung „Null" (Zero) ist in einer solch nuancierten Umgebung ungeeignet. Der Kontext ist entscheidend, und die Beurteilung des Vertrauens erfordert Einblicke, um den Grad der Erlaubnis effektiv zu bestimmen. Dies ist im Rahmen einer SASE-Umgebung möglich. Hier ist Zero Trust im Grunde „kontinuierliches adaptives Vertrauen" über Benutzer, Geräte, Netzwerke, Anwendungen und Daten hinweg. Die Fülle an kontextbezogenen Einblicken, die innerhalb einer SASE-Plattform zur Verfügung stehen, macht es überflüssig, implizites Vertrauen zu gewähren oder Genehmigungsentscheidungen auf einzelne Informationen (etwa eine IP-Adresse) zu stützen. Stattdessen können Entscheidungen auf der Grundlage eines maßgeschneiderten Satzes ständig neu bewerteter Parameter getroffen werden, die aus mehreren miteinander verflochtenen Kontextelementen bestehen (zum Beispiel: Benutzeridentität + Geräteidentifikation + Zeit + Geolokalisierung + Geschäftsrolle + Datentyp). Und da bei SASE die Sicherheitsrichtlinien den Daten und nicht dem Benutzer oder dem Gerät folgen, bestimmt die Ressource selbst den angemessenen Grad des Vertrauens – und zwar nur für eine bestimmte Interaktion, die jedes Mal neu bewertet wird, wenn sich ein Parameter ändert.

DIE FÜLLE AN KONTEXTBEZOGENEN EINBLICKEN, DIE INNERHALB EINER SASE-PLATTFORM ZUR VERFÜGUNG STEHEN, MACHT ES ÜBERFLÜSSIG, IMPLIZITES VERTRAUEN ZU GEWÄHREN ODER GENEHMIGUNGSENTSCHEIDUNGEN AUF EINZELNE INFORMATIONEN ZU STÜTZEN.

Neil Thacker, CISO EMEA/LATAM, Netskope, www.netskope.com

Die Bewertung des Vertrauens zu Beginn einer Interaktion allein ist dementsprechend nicht ausreichend. Diese Vertrauensbewertung sollte während der gesamten Interaktion stattfinden. Dabei muss der Kontext kontinuierlich bewertet werden, da Änderungen des Kontexts zu einer Anpassung (Erhöhung oder Verringerung) des angemessenen Vertrauensniveaus führen können, was wiederum die Art des gewährten Zugriffs auf die Ressource verändern sollte.

Das Gleichgewicht wahren

Die Vorteile eines kontinuierlichen adaptiven Vertrauenskonzepts sind vielfältig, aber drei davon stechen bei der Ausarbeitung eines Business Case besonders hervor:

1. Mehr Möglichkeiten, ein gewisses Maß an Zugang zu gewähren, um die Mehrheit der Sicherheitsentscheidungen von „Nein" auf „Ja, mit Bedingungen" umzulenken

2. Unangemessener Zugriff wird eingeschränkt, wodurch der Explosionsradius gefährdeter Konten verringert wird

3. Verbesserte und ständige Transparenz in Bezug auf sensible Datentypen, Standorte und Bewegungen

Zur Aufgabe von Sicherheitsteams gehört nicht nur das Einschränken und Sperren, sondern auch das Gewähren von Zugang. Kontinuierliches adaptives Vertrauen nutzt Erkenntnisse, um dynamische Berechtigungen zu erteilen und zu entziehen. Auf diese Weise können Unternehmen ihre Produktivität maximieren, ohne sich unnötigen Risiken auszusetzen.

Neil Thacker

SCHUTZ DES IT-NETZWERKS

KEIN „BLACK OUT“ MIT MACMON ZTNA

„An einem kalten Februartag brechen in Europa alle Stromnetze zusammen. Der totale Blackout. Ein Hackerangriff? … In seinem Roman „Black Out“ skizziert Marc Elsberg die Folgen einer Manipulation von Endgeräten im Stromnetz, ganz Europa ist ohne Energieversorgung. Unrealistisch?!? Leider nicht: Medien berichteten im Juli 2021: Fast die komplette deutsche Wirtschaft ist von Cyber-Attacken betroffen. Der Schaden erreichte zuletzt die jährliche Summe von 223 Milliarden Euro.

New Work – neue Vulnerabilität

Begünstigt wurde die Entwicklung durch die Digitalisierung von Handel und Wirtschaft und den Anstieg von flexibler Arbeit, jederzeit und von überall. Zur notwendigen technischen Ausstattung gehören Laptop, Smartphone, Drucker, Videokonferenztools, branchenabhängige Endgeräte und eine leistungsfähige Netzwerkverbindung für einen sicheren Zugang zum Datennetz via VPN. Verschiedenste Dienste, auf die Mitarbeiter zugreifen müssen, werden sukzessive in die Cloud verlagert. Der Schutz des IT-Netzwerks ist durch die Hybridisierung in den Mittelpunkt der IT-Security gerückt.

Zuverlässige Sicherheit

Das Berliner Software-Unternehmen macmon secure trägt schon seit 2003 dem Zero Trust Network Access (ZTNA)-Ansatz Rechnung, indem nur definierten Geräten individueller Zugang zum Netzwerk erlaubt wird. Mit macmon Secure Defined Perimeter (SDP) wird der Schutz nun auch auf sämtliche Cloud-Dienste ausgedehnt, denn Alles, was vom Cyberspace abhängt, ist potenziell gefährdet: persönliche Daten, Unternehmensdaten, Kundendaten, geistiges Eigentum oder wichtige Infrastruktur. Der Ansatz fußt auf der Philosophie, weder einem Gerät noch einem Benutzer einen Vertrauensvorschuss zu geben, bevor keine sichere Authentifizierung stattgefunden hat. So kann der Netzwerkzugang individuell gesichert und vor allem auf das nötigste beschränkt werden, was die Angriffsfläche maßgeblich reduziert.

Sabine Kuch | www.macmon.eu

IDENTITY ACCESS MANAGEMENT

NEUE PROBLEME, DIE ES ZU LÖSEN GILT

Das Einsatzspektrum von IAM-Systemen dehnt sich beständig aus. Dabei sind neben der technischen Umsetzung, der organisatorische Wandel und die Ausrichtung des IAM-Teams wichtige Erfolgsfaktoren, um von den Benefits einer dezentralen IAM-Struktur zu profitieren.

Highlighs aus dem eBook

Synthetic Identities

Bei diesem neuen Begriff handelt es sich um eine Art von Betrug, bei dem echte und gefälschte Informationen kombiniert werden, um eine neue Identität zu erschaffen. Diese Informationen werden dann verwendet, um betrügerische Konten zu eröffnen und Einkäufe zu tätigen.

Agiles IAM

Um die Anforderungen agiler Lösungen für Endbenutzer und deren Interaktionswünsche umzusetzen, bieten IAM-Tools verschiedene Lösungsansätze. Der erfolgversprechendste Lösungsansatz zeigt sich in der Einführung und Bereitstellung eines IAM Development Kits.

Identitätsbasierte Angriffe

Um identitätsbasierten Bedrohungsvektoren zu begegnen und Erkennungs- und Präventionslücken zu schließen, sollte der Sicherheitsansatz für einen ganzheitlichen Schutz von Identitäten auf drei Grundsäulen aufbauen.

Das eBook umfasst 32 Seiten und steht kostenlos zum Download bereit:
www.it-daily.net/download

INSTANT MESSENGER SICHER EINSETZEN

STUDIE, CHECKLISTE UND PRAXISLEITFADEN

Chat-Apps auf dem Smartphone gehören zu den beliebtesten Tools für die private Kommunikation. Auch in Unternehmen werden Instant Messenger immer häufiger für den schnellen Informationsaustausch zwischen Kollegen oder mit Kunden eingesetzt. Doch hier lauern juristische Fallstricke – besonders im Hinblick auf den Datenschutz und den Schutz von Geschäftsgeheimnissen. Eine Studie des FZI Forschungszentrums Informatik in Karlsruhe analysiert die komplexe Rechtslage und liefert eine 11-Punkte-Checkliste sowie einen Praxisleitfaden mit.

„In unserer Studie haben wir die Rechtslage für einen Einsatz von Messenger-Diensten im Unternehmen aufgezeigt mit dem Ziel, Klarheit über diesen komplexen Bereich zu schaffen und die rechtlichen Pflichten auch mit vereinfachten Checklisten aufzubereiten", sagt die Leiterin der Studie, Dr. Manuela Wagner.

Datenschutzrechtlich äußerst bedenklich sei etwa die automatische Übermittlung der Kontaktverzeichnisse von Endgeräten an die Anbieter von Messengerdiensten. Ebenfalls raten die Experten von Angeboten ab, die einen Datentransfer in ein Drittland außerhalb der EU und des Europäischen Wirtschaftsraums vorsehen, für das kein so genannter Angemessenheitsbeschluss der EU-Kommission vorliegt.

Mit dem Wegfall des „Privacy Shield"-Abkommens zwischen der EU und den USA im Jahr 2020 sei das Weiterleiten von Daten in die Vereinigten Staaten problematisch geworden. „Durch den CLOUD-Act gilt dies selbst für innerhalb der EU gespeicherte Daten US-amerikanischer Unternehmen, weil auf Verlangen von US-Behörden auch außerhalb der USA gespeicherte Daten herausgegeben werden müssen", schreiben die Studienautoren.

Strafen in Millionenhöhe drohen

Unternehmen, Verbände oder Behörden riskieren hohe Sanktionen, wenn sie bei der internen oder externen Kommunikation die Datenschutzvorgaben verletzen. So sieht die Datenschutz-Grundverordnung (DSGVO) bei bestimmten Verstößen Geldbußen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Vorjahresumsatzes vor.

Hinzu kommt, dass Geschäftsgeheimnisse nach neuer Rechtslage (Gesetz zum Schutz von Geschäftsgeheimnissen – GeschGehG) nur dann rechtlichen Schutz genießen, wenn die geheimen Informationen mit angemessenen Maßnahmen geschützt werden. Es liegt also im Interesse der Unternehmen, bei der Nutzung von Messenger-Lösungen auch den Schutz von Geschäftsgeheimnissen zu bedenken.

Vorsicht bei Apps für den Privatgebrauch

„Aus unserer Arbeit lässt sich unter anderem das Fazit ziehen, dass zahlreiche, gerade für den privaten Gebrauch entwickelte Instant Messenger den im Unternehmenskontext relevanten rechtlichen Anforderungen an Daten- und Geschäftsgeheimnisschutz in der Europäischen Union kaum oder gar nicht genügen", betont Studienleiterin Manuela Wagner.

Die Studie wurde vom Schweizer Messenger Threema in Auftrag gegeben, wobei die Verantwortung über die Inhalte allein beim FZI lag. Das Unternehmen bietet mit Threema Work eine Lösung an, die alle rechtlichen und technischen Anforderungen an den Daten- und Geheimnisschutz vollumfänglich erfüllt. Zudem bietet die Lösung Möglichkeiten der Administration und weitere Business-Funktionen, die für den professionellen Einsatz in der Unternehmenskommunikation unerlässlich sind.

www.threema.ch

STUDIE & LEITFADEN

Die Studie „Daten- und Geheimnisschutz bei der Kommunikation im Unternehmenskontext" einschließlich einer 11-Punkte Checkliste sowie einem 17-seitigen Leitfaden für Praktiker kann hier kostenfrei abgerufen werden:

https://three.ma/rechtsstudie

CLOUD WORKLOADS

EINE UMFASSENDE PLATTFORMSICHERHEIT WIRD BENÖTIGT

CLOUD WORKLOADS SIND DERZEIT OFT DAS SCHWÄCHSTE GLIED IN DER ABWEHRKETTE VON UNTERNEHMEN. DIESE ZU VERBESSERN, WIRD IN DEN KOMMENDEN MONATEN EINE ENTSCHEIDENDE AUFGABE FÜR DIE UNTERNEHMENSSICHERHEIT.

Jörg von der Heydt,
Reginal Director DACH, Bitdefender,
www.bitdefender.de

Der Trend, Applikationen, Prozesse und Informationen in die verschiedensten Cloudumgebungen zu verlagern, wird stärker. Daraus ergeben sich neue Maßstäbe für die IT-Sicherheit der Cloud Workloads. Nur Plattformen können die Sicherheit in der Wolke handhabbar machen.

Cloudbasierte Applikationen, Services oder Funktionen beruhen auf mehreren Cloud Workloads als plattformunabhängige Services oder ausführbarer Code, die auf verschiedenen Systemen laufen. Diese Cloud Workloads erfüllen einzelne Aufgaben und laufen separat voneinander in verschiedenen Cloud-Computing-Modellen - losgelöst von der zugrunde liegenden Plattform oder Hardware. Sind sie unterbrochen, kommen Geschäftsprozesse zum Erliegen. Greift ein Unberechtigter auf sie zu, kann er wertvolle Informationen entwenden.

Neue Ziele, bekannte Vorgehensweisen

Jede Information und jeder Prozess, den Unternehmen in die Cloud auslagern, macht eine Cloudstruktur für Angreifer zum immer lohnenderen Ziel. Die Urheber komplexerer Attacken müssen unter Umständen nur ein einziges Cloud Workload Element kompromittieren, um den maximalen Erfolg zu erzielen. Da kann es nicht verwundern, dass versierte Hacker alle grundlegenden Angriffsmechanismen von Endgeräten auf Cloud Workloads übertragen – wie etwa Phishing, DDoS, APTs, Datenexfiltration oder Ransomware.

Hierfür nutzen sie die besonderen Risiken einer Cloud-Infrastruktur aus. Cloud Workloads und die dazugehörigen Cloud-Infrastrukturen erhöhen signifikant die Angriffsoberfläche – etwa durch unzureichend gesicherte APIs oder Benutzeroberflächen. Die Cloud verspricht, neue Strukturen schnell und flexibel einzurichten, doch gerade hier passieren Fehler. Und nicht selten verlassen sich IT-Teams und Unternehmen auf den Cloud-Anbieter, wenn es um Sicherheit geht. Dieser steht aber nur für den Erhalt von Strukturen ein, nicht aber für Daten.

Plattform-Rezepte für Cloud Workload Security

Traditionelle Cybersecurity-Ansätze greifen bei Arbeitslasten in der Cloud zu kurz. Zu groß und amorph ist die neu geschaffene Angriffsfläche, die es zu überwachen gilt. Es ist unmöglich, manuell jeder Workload einen Cybersecurity-Agenten zuzuweisen. Häufig mangelt es herkömmlichen Sicherheitslösungen daher schon an der Sichtbarkeit der zu schützenden Systeme. Cloud Workload Security benötigt aber genau diese Transparenz.

Zu bewährten Praktiken für die Sicherheit gehört ein Zero-Trust-Ansatz. Diese Technologie kontrolliert jeden ein- und ausgehenden Datenverkehr, um zwischen legitimen und illegitimen Anfragen zu unterscheiden. Das heißt, jede Workload muss beweisen, dass sie legitim ist, um dann auch nur die Zugriffsrechte zu bekommen, die sie unbedingt braucht.

Weil durch neu hinzugefügte Cloud-Dienste schnell heterogene Strukturen entstehen, greifen Einzellösungen zu kurz. Nur umfassende Security-Plattformen vereinen die notwendigen Technologien und Methoden für Workloads aller Art und machen deren Sicherheit durch eine zentrale Managementkonsole handhabbar.

Fazit

Cloud Workloads sind derzeit oft das schwächste Glied in der Abwehrkette von Unternehmen. Diese zu verbessern, wird in den kommenden Monaten eine entscheidende Aufgabe für die Unternehmenssicherheit. Sicherheitsplattformen, die Cloud Workloads berücksichtigen, bieten den IT-Verantwortlichen einen konsolidierten Überblick über sämtliche Ressourcen und Gefahren – ob On-Premises oder in der Cloud.

Jörg von der Heydt

FLEXIBEL UND SKALIERBAR

SYSTEMHÄUSER SETZEN AUF SECURITY AS A SERVICE

IMMER MEHR SYSTEMHÄUSER UND IT-VERANTWORTLICHE STEIGEN UM AUF SECURITY AS A SERVICE.

Dariush Ansari, Geschäftsführer, Network Box Deutschland GmbH, www.network-box.eu

Nie war eine effektive IT-Security wichtiger für eine wachsende Geschäftsentwicklung. Und nie waren die Sicherheitsrisiken schwieriger zu kontrollieren als heute.

Fast die komplette deutsche Wirtschaft ist laut Studien von Cyberattacken betroffen. Der Schaden erreichte im letzten Jahr den Rekordwert von 223 Milliarden Euro. Social Engineering, Ransomware, DDoS, Phishing - die Angriffe werden immer komplexer und die Abwehr dadurch immer aufwändiger. „Immer mehr Systemhäuser und IT-Verantwortliche steigen um auf Security as a Service" so Dariush Ansari, Geschäftsführer des MSSP und Systemhauspartner Network Box Deutschland GmbH. Vier gute Gründe dafür seien die planbaren Kosten dank monatlich kündbarer Miete; mehr Flexibilität und Skalierbarkeit, um schnell und unkompliziert auf neue Anforderungen und Sicherheitslücken zu reagieren und eine höhere Ausfallsicherheit durch automatisierte Updates, Disaster Recovery und Backups. „Doch der wahrscheinlich wichtigste Grund ist das Security-Know-how trotz Fachkräftemangel", so Ansari. „Als Managed Security Service Provider entlasten wir unsere Systemhauspartner, indem wir im Hintergrund den Bereich IT-Sicherheit eigenverantwortlich und zuverlässig übernehmen." Der IT-Sicherheitsspezialist aus Köln unterstützt Systemhäuser bei der Betreuung ihrer Endkunden mit Managed UTM-Lösungen, Security Awareness Trainings und ganzheitlichen IT-Sicherheitskonzepten für jede Unternehmensgröße.

BIOMETRIE

SICHERE AUTHENTIFIZIERUNG?

Mit zunehmender Digitalisierung und damit einhergehenden Cybersecurity-Risiken ist auch die Verwendung biometrischer Methoden gestiegen. 68 Prozent der Deutschen halten biometrische Authentifizierung für Smartphone, Notebook und Ähnlichem für sicherer, dennoch bevorzugen 59 Prozent weiterhin Passwörter. Denn Sicherheit ist für die Nutzer nicht alles, es gibt auch Bedenken, so eine aktuelle Online-Studie von Software Advice.

www.softwareadvice.de

BEDENKEN BEI DER VERWENDUNG BIOMETRISCHER TECHNOLOGIEN

SAP-SYSTEME SCHÜTZEN

BESTMÖGLICH AUF NUMMER SICHER GEHEN

Cyber Security ist eine Frage der Abwägung. Hundertprozentige Sicherheit gibt es nicht – egal, wie viel Budget Unternehmen investieren. Wesentlich ist, die relevantesten Prozesse und Systeme bestmöglich gegen Cyber-Attacken zu schützen, um das eigene Geschäft sicher betreiben zu können. Dabei landen Unternehmen schnell bei ihrem SAP-System. Es ist besonders schützenswert, weil es oft den IT-seitigen Kern der Produktion bildet. Dementsprechend ist es eine sehr gute Idee, in Sachen Cyber Security beim SAP-System anzusetzen.

Doch welche Komponenten, Daten oder Prozesse im SAP-Ökosystem bilden einen geeigneten Ausgangspunkt? Eine heikle Frage, denn viele Unternehmen wissen gar nicht, welche Prozesse es überhaupt gibt und wie sie softwareseitig abgebildet und gestützt sind. Eine derartige Schatten-IT wird im Hinblick auf Cyber Security schnell zu einem großen Problem. Darum sind Firmen gefordert, sich zunächst mit ihrer SAP-Systemlandschaft und vor allem deren Nutzung und Bezug zu den Geschäftsprozessen auseinanderzusetzen, bevor sie Security-Ziele definieren und Software anschaffen. Letztendlich müssen die Geschäftsprozesse geschützt werden und nicht die Systeme an sich.

Intranet-, Internet- oder API-Security?

Dabei ist es ratsam, sich drei Szenarien zu widmen: Intranet-Security, Internet-Security und API-Security. Im ersten Fall stehen die eigenen SAP-Anwender im Fokus. Firmen müssen in Erfahrung bringen, wer überhaupt mit dem ERP-System arbeitet und welche nutzerspezifischen Privilegien zum Beispiel bei Administratoren und Finance-Experten bestehen. Nur so können sie deren Rechte und Devices gezielt schützen, etwa mit Multi-Faktor-Authentifizierung. Solche Maßnahmen sind machbar, weil hier konkrete Einflussmöglichkeiten sowohl auf die Nutzer als auch auf die Geräte bestehen. Anders sieht das bei der Internet-Security aus. Hier geht es darum, Zugriffe aus dem Internet auf Applikations-Ebene abzusichern, da kein Einfluss auf Nutzer oder Geräte besteht. Somit muss etwa eine webbasierte SAP Fiori Anwendung auf Anwendungsebene gesichert werden. Der dritte Bereich umfasst die Sicherheit von Schnittstellen, über die Unternehmen zum Beispiel ihren Partnern Daten bereitstellen oder Bestellungen erhalten.

Das SAP-System schützen

Erst nach dieser strategisch-theoretischen Vorarbeit ist es zweckmäßig, sich mit konkreten Maßnahmen und Tools auseinanderzusetzen. Sinnvoll ist eine modulare Lösung, die verschiedene Komponenten integriert. Bewährt hat sich zum Beispiel eine kombinierte Security-Plattform auf Basis der Azure Cloud und Azure Sentinel. So können Firmen ihr SIEM individuell skalieren und die Reaktionen auf Alerts teilweise automatisieren (SOAR). Unverzichtbar sind auch qualifizierte Mitarbeiter. Zum einen braucht es Ingenieure, welche die technischen Komponenten zusammenführen, sie weiterentwickeln und so Detection wie auch Response optimieren – mit dem Ziel, unerlaubte Zugriffe über diverse Endpoints, aus dem Internet oder über das Netzwerk zu erkennen und Alarme automatisiert auszulösen. Zum anderen sind Analysten erforderlich, die die Alerts auswerten und bei tatsächlichen Cyber-Attacken adäquate Maßnahmen ergreifen: Nutzerkonten sperren, Systeme vom Netzwerk trennen, Buchungen stoppen, einen Notfallplan aktivieren. Damit haben Unternehmen die ersten richtigen Schritte getan, um ihr SAP-System und damit ihre Produktion gegen Hacker-Angriffe zu schützen und ihr Business weiter betreiben zu können. Abgeschlossen ist das Thema Sicherheit aber natürlich nie – ebenso wenig wie die kontinuierliche Optimierung anderer kritischer Geschäftsprozesse.

Andreas Nolte

HUNDERTPROZENTIGE SICHERHEIT GIBT ES NICHT – EGAL, WIE VIEL BUDGET UNTERNEHMEN INVESTIEREN.

Andreas Nolte, Head of Cyber Security, Arvato Systems, www.arvato-systems.de

EXTENDED DETECTION & RESPONSE

MEHR ALS NUR ENDPUNKTSCHUTZ

Wenn es um den Schutz von Unternehmensnetzwerken geht, ist der Endpunkt der erste und wichtigste Ausgangspunkt, den es zu sichern gilt. Früher wurde dies mit einer Technologie namens EDR (Endpoint Detection & Response) erreicht – doch heute gibt es einen neuen Standard: XDR (Extended Detection & Response). Der XDR-Ansatz von SentinelOne heißt Singularity und beruht auf der einzigartigen Art und Weise, wie die Plattform den traditionellen EDR-Ansatz neu definiert.

Herausforderungen wie die Normalisierung, Kontextualisierung und Korrelation von Daten sind nicht neu. Ebenso wenig wie die Notwendigkeit, den Grad der Automatisierung zu maximieren und starken Schutz über alle IT-Oberflächen hinweg aufrechtzuerhalten. Die bis dato etablierten EDR-Grundlagen sind von entscheidender Bedeutung, doch sie müssen mit neuen Innovationen und einer Umsetzung in exponentiell größerem Maßstab kombiniert werden.

Weiterentwicklung etablierter Technologien

XDR liegt im Spannungsfeld zwischen Evolution und Revolution. Diese Art von Sicherheitslösung ist mehr als nur ein Sammelsurium von bestehenden Fähigkeiten; um den modernen Bedrohungen des Cyberraums begegnen zu können, bedarf es einer organischen Weiterentwicklung von EDR. Die Fülle an verwundbaren Oberflächen heutiger Unternehmensnetzwerke und die schiere Menge an Daten dienen als Katalysator für schnelle Weiterentwicklungen etablierter Sicherheitstechnologien.

Die neuen Technologie-Initiativen in der Sicherheitsbranche, zusammen mit den oben erwähnten EDR-Grundlagen, prägen den Begriff XDR – eine neue Art von Lösung, die autonom und in Maschinengeschwindigkeit alle Endpunkte, IoT-Geräte, Server, Cloud-Workloads und weitere Assets schützt.

de.sentinelone.com/

CYBERSECURITY

NEUE DENKANSÄTZE SIND GEFRAGT

Das Editorial beschäftigt sich mit dem Thema KI. Es interessiert und fasziniert die IT-Welt derzeit extrem. Allerdings ist es auch ein Hypebegriff. Zeit, um die Fakten einmal geradezurücken.

Highlights aus dem eBook:

Attack Surface Management-Plattformen

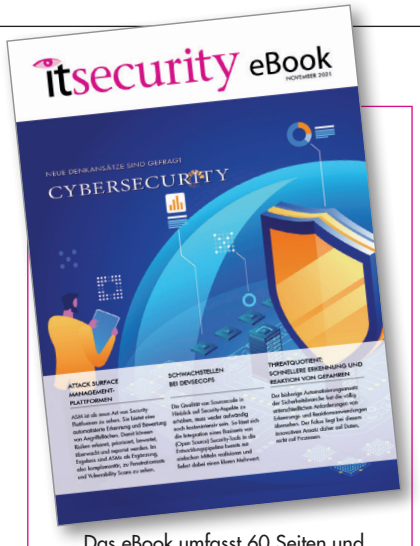
ASM ist als neue Art von Security-Plattformen zu sehen. Sie bietet eine automatisierte Erkennung und Bewertung von Angriffsflächen. Damit können Risiken erkannt, priorisiert, bewertet, überwacht und reportet werden.

Schwachstellen bei DevSecOps

Die Qualität von Sourcecode in Hinblick auf Security-Aspekte zu erhöhen, muss weder aufwändig noch kostenintensiv sein. So lässt sich die Integration eines Basissets von Security-Tools in die Entwicklungspipeline bereits mit einfach Mitteln realisieren und liefert dabei einen klaren Mehrwert.

Threat Quotient

Der bisherige Automatisierungsansatz der Sicherheitsbranche hat die völlig unterschiedlichen Anforderungen von Erkennungs- und Reaktionsanwendungen übersehen. Der Fokus liegt bei diesem innovativen Ansatz daher auf Daten, nicht auf Prozessen.



Das eBook umfasst 60 Seiten und steht kostenlos zum Download bereit:
www.it-daily.net/download

IM VISIER VON CYBERKRIMINELLEN

E-MAIL-VERSCHLÜSSELUNG UND DIGITALE SIGNATUREN

Die Bedeutung der digitalen Kommunikation ist heute größer denn je. So werden immer mehr Meetings per Videokonferenz durchgeführt; viele Mitarbeiter arbeiten statt im Büro im Homeoffice. Dies hat auch Auswirkungen auf den Versand von Dateien. Hierbei setzen viele Unternehmen auf das Business-Kommunikationsmittel Nummer Eins: die E-Mail. Doch nicht nur unter den Nutzern ist dieses Mittel äußerst beliebt. Die elektronischen Nachrichten sind auch im Visier von Cyberkriminellen. Daher ist ein Schutz vor Cyberangriffen unerlässlich.

Ransomware, Phishing, Spear-Phishing, Social Engineering – Cyberangriffe auf E-Mails nehmen immer weiter zu und werden immer professioneller. Die bekanntesten Angriffsmethoden sind Phishing- und Ransomware-Attacken. Beim Phishing verschicken Kriminelle trügerisch echt aussehende Mails und fordern den Nutzer darin auf, sich etwa auf nachgebauten Seiten mit den persönlichen Kontodaten anzumelden. Auf diesem Wege gelangen Hacker an sensibelste Daten, mit denen sie großen Schaden anrichten können. Ebenfalls hohen Schäden können auch durch Ransomware-Attacken verursacht werden. Dabei versenden Kriminelle eine Schadsoftware, die sich dann automatisch im Unternehmensnetzwerk installiert und Systeme teilweise verschlüsselt oder komplett lahmlegt.

Quelle: @OOCMEN istockphoto.com

Zu den ausgeklügelteren Methoden zählen Spear-Phishing – ein zielgerichteterer Phishing-Angriff auf Hunderte von Empfängern – und Social-Engineering, also Mails, in denen Nutzer gezielt beeinflusst werden, bestimmte Aktionen auszuführen.

Doch unabhängig, um welche Art von Cyberangriff es sich handelt, lassen sich diese durch E-Mail-Verschlüsselung und digitale Signaturen schon leicht vermeiden.

E-Mail-Sicherheit erhöhen

Anders als viele denken, ist die Einrichtung einer E-Mail-Verschlüsselung einfach umsetzbar und mit wenig Aufwand sowie Kosten verbunden. Technologien wie S/MIME- Verschlüsselung gewährleisten, dass Daten auf dem gesamten Weg vom Absender bis zum Empfänger zu keinem Zeitpunkt unverschlüsselt sind und durch Unbefugte mitgelesen werden können. Moderne Systeme erlauben darüber hinaus eine Spontan-Verschlüsselung, wenn der Empfänger über kein eigenes Schlüsselmaterial verfügt.

Um gar nicht erst auf Phishing-Angriffe hereinzufallen, eignen sich digitale Signaturen, die den Absender von E-Mails eindeutig identifizieren. Ist eine E-Mail mit einer solchen Signatur versehen, schafft dies Authentizität sowie Integrität der E-Mail. Bei ungebrochener Signatur kann sich der Empfänger sicher sein, dass die Nachricht vom angegebenen Absender stammt, unverändert ist und somit vertrauenswürdig.

> ANDERS ALS VIELE DENKEN, IST DIE EINRICHTUNG EINER E-MAIL-VERSCHLÜSSELUNG EINFACH UMSETZBAR UND MIT WENIG AUFWAND SOWIE KOSTEN VERBUNDEN.
>
> Günter Esch, Geschäftsführer SEPPmail – Deutschland GmbH, www.seppmail.de

Für den Erhalt einer digitalen Signatur ist ein offiziell prüfbares Zertifikat notwendig. Dieses wird von Zertifizierungsstellen vergeben und muss bei diesen beantragt werden. Die sogenannten Certificated Authorities (CAs) bestätigen dann, dass das Zertifikat als persönlicher, öffentlicher Schlüssel zu einer bestimmten E-Mail-Adresse gehört. Dieser administrative Prozess, der Managed Public Key Infrastructure (MPKI)-Prozess, wird inzwischen von einigen professionellen Lösungen automatisch übernommen. In diesem Fall erhalten Nutzer ihre Signatur mit der ersten ausgehenden Mail.

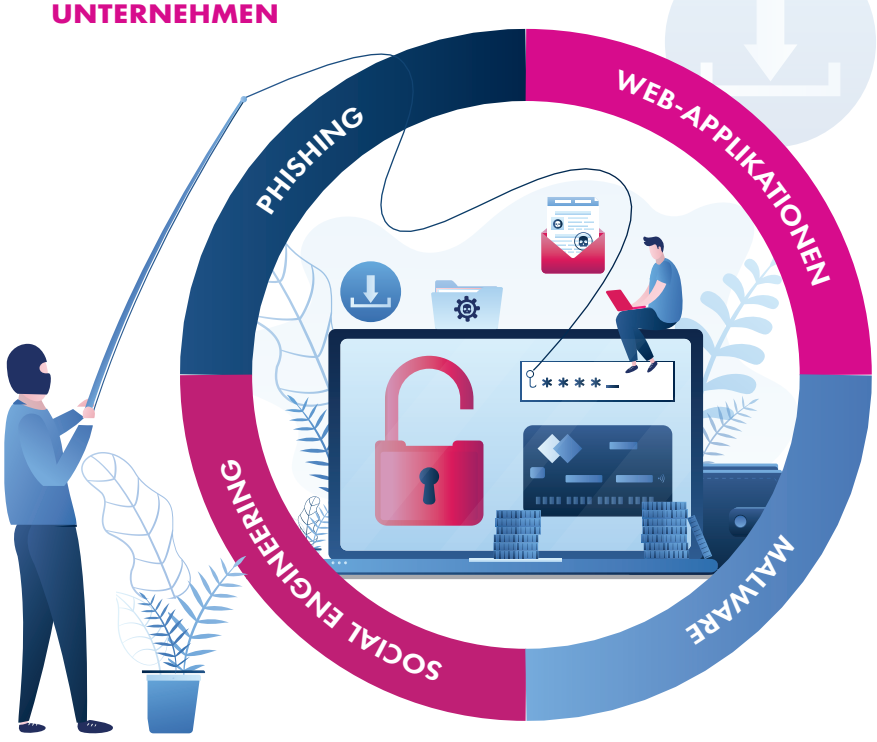
Günter Esch

CYBER-VERSICHERUNGEN

ESSENZIELLE ABSICHERUNG TROTZ STEIGENDER PRÄMIEN

Der Anstieg der Durchdringung von Cyber-Versicherungen bei Gewerbekunden nahm zuletzt rasant an Fahrt auf. Die Entwicklung der Schadenszahlen zeigt, wie wichtig eine Absicherung gegen Hackerangriffe für mittelständische Unternehmen oder auch – wie zuletzt – die öffentliche Verwaltung ist. Abgedeckt sind zunächst Vermögensschäden, die dem Unternehmen selbst durch eine Cyber-Attacke entstehen. Neben dem Ertragsausfall sind dies nötige Aufwendungen, um nach einem Angriff wieder zum normalen Geschäftsbetrieb zurückzukehren und beschädigte IT-Systeme und Daten wiederherzustellen. Auch die Haftpflicht im Falle der Weitergabe eines Virus oder bei Datenschutzverletzungen sind Bestandteile der Cyber-Versicherung. Wie schon im Jahr 2020 ziehen die jüngsten Cyber-Angriffe und die dadurch entstandenen Kosten für die Versicherer künftig höhere Prämien nach sich.

DIE HÄUFIGSTEN CYBER-ATTACKEN AUF DEUTSCHE UNTERNEHMEN



„Die aktuelle Lage zeigt wie sehr sich Cyber-Versicherungen lohnen und in der Cyber-Krise einen echten Mehrwert für die Unternehmen bieten. Die finanziellen Risiken einer Cyber-Attacke werden immer noch unterschätzt. Die nächste Welle von Hacker-Angriffen kommt ganz bestimmt und wird zeigen, wie gut Unternehmen, Verwaltungen oder Krankenhäuser aus den aktuellen Vorfällen gelernt haben und selbst auf so eine Krise vorbereitet sind“, fasst Ole Sieverding, Geschäftsführer von CyberDirekt mit Sitz in Berlin, zusammen.

Die Cyber-Angriffe kommen

Deutsche Unternehmen stehen nach wie vor im Fokus von Cyber-Kriminellen. Beispiele dafür gibt es genug: die Attacke auf ein Unternehmen aus dem Lebensmittel-Einzelhandel, der Angriff auf einen bekannten E-Commerce Shop oder das Online-Banking einer gesamten Bankengruppe. All das zeigt, dass nicht nur Unternehmen, sondern zunehmend auch die Endverbraucher und Kunden in der Folge dieser Attacken betroffen sind. Cyber-Angriffe auf die deutsche Wirtschaft werden immer spezialisierter und für die betroffenen Firmen in den meisten Fällen teurer. Der Schadenaufwand weist teilweise extrem hohe Summen auf, gesamtwirtschaftlich ebenso wie für die betroffenen Unternehmen. Dies geht Schadensstatistiken aller in diesem Bereich tätigen Versicherer hervor.

DIE CYBER-VERSICHERUNG BLEIBT ESSENZIELL UND IST DAMIT NACH WIE VOR EIN WICHTIGER BESTANDTEIL DES RISIKOMANAGEMENTS SEIN.

Hanno Pingsmann, Geschäftsführer, CyberDirekt, www.cyberdirekt.de

Professionalisierungsgrad erhöht

Es lässt sich beobachten, dass nun verstärkt eine Professionalisierung bei den Cyber-Kriminellen einsetzt, und lukrative Ziele in vielfältigen Branchen attackiert werden. Von Behörden, Hochschulen, Kliniken und Arztpraxen über DAX-Unternehmen und Konzerne bis hin zum Einzelhandel und Mittelstand – jede Institution kann und wird von Cyber-Kriminellen ins Visier genommen. Insbesondere für kleine Unternehmen ist das Risiko groß, denn schnell kann ein Cyber-Angriff die wirtschaftliche Existenz gefährden. Häufig fehlt gerade bei KMUs das Risikobewusstsein für die abstrakte Gefahrenlage. Meist werden erst nach einem Angriff im engeren Umfeld Vorsichtsmaßnahmen oder Absicherungen in Betracht gezogen.

Die Prämien steigen

Der Schadenaufwand der Cyber-Versicherer hat im Jahr 2020 ein Niveau erreicht, das kaum noch durch die eingenommenen Versicherungsprämien zu finanzieren ist. Seit 2018 sind Schadenhäufigkeit und -höhe bei Cyber-Attacken um bis zu 300 Prozent gestiegen. Die Zahlen für das Jahr 2021 dürften diesen Trend fortsetzen und sogar steigern. Größere Sicherheitslücken und ihre Auswirkungen - wie beispielsweise bei den Microsoft Exchange-Servern aus März und April 2021 - sind darin noch gar nicht berücksichtigt. Die Folge: Prämien für Cyber-Versicherungen erhöhen sich stark. Ein Versicherer sieht sich beispielsweise gezwungen, seinen Bestandskunden Prämienaufschläge von über 50 Prozent aufzuerlegen. Gleichzeitig steigt die Nachfrage, denn das Thema wird immer präsenter. Doch unterm Strich ist und bleibt die Cyber-Versicherung essenziell und ist damit nach wie vor neben Mitarbeitersensibilisierung und technischen Aufrüstungen ein wichtiger Bestandteil des Risikomanagements.

Hanno Pingsmann

CYBER-BEDROHUNGEN

DER EINFLUSS VON COVID-19

McAfee Enterprise & FireEye stellen die aktuelle Studie „Cybercrime in a Pandemic World" vor, die den dringenden Bedarf an optimierten Cyber-Sicherheitsarchitekturen vor Augen führt. Die Ergebnisse zeigten, dass 81 Prozent der Unternehmen weltweit während der Pandemie vermehrt mit Cyber-Bedrohungen konfrontiert waren, wobei 56 Prozent Downtime aufgrund von Cyber-Vorfällen erlebten. 79 Prozent dieser Vorfälle fielen in Spitzenzeiten. Das herannahende Weihnachtsgeschäft sowie die damit verbundenen Erwartungen der Verbraucher setzen Unternehmen, Angestellt und Lieferketten unter Druck und machen sie verwundbar für Cyber-Angriffe.

Auch in Deutschland erlebten mehr als die Hälfte der Befragten (65 %) in ihrer Branche eine Zunahme der Cyber-Bedrohungen seit Beginn der Corona-Pandemie. Hierbei hatten 42 Prozent der deutschen Unternehmen mit Downtime durch Cyber-Risiken zu kämpfen, drei Viertel davon zu Spitzenzeiten. Darüber hinaus zeigt die Studie, dass mit 50 Prozent Zustimmung Phishing hierzulande als größte Bedrohung gilt.

Die Studie zeigt auch: Während IT-Fachleute erkannt haben, dass sich die Cyber-Bedrohungslage verschärft hat, räumten Unternehmen diesem Thema während der Pandemie nicht ausreichend Priorität ein. Die Zahlen zeigen aber, dass dies notwendig wäre:

60 PROZENT der Unternehmen verzeichneten eine Zunahme der Online-Aktivitäten

33 PROZENT mussten ihre Technologie- und Sicherheitsbudgets kürzen

56 PROZENT Prozent hatten aufgrund eines Cyber-Problems mit Ausfallzeiten zu kämpfen

www.mcafee.com

IT SECURITY AWARD 2021

GEWINNER IM RAHMEN DER „IT-SA 2021“ AUSGEZEICHNET

Nachdem die it-sa im vergangenen Jahr coronabedingt ausgefallen ist, war sie in diesem Jahr wieder Plattform für die Verleihung der it security Awards. Die diesjährigen Preisträger sind QuantiCor Security, Digital Shadows, Saviynt und Netskope.

Management Security

QuantiCor Security – Quantum-safe Encryption Gateway

Bei dieser Lösung handelt es sich um eine Verschlüsselung der neuen Generation. Viele Verschlüsselungslösungen erfordern einen hohen Verwaltungsaufwand, ohne einen ausreichenden Mehrwert zu bieten. Mit QuantiCors Quantum-safe Encryption Gateway werden Kosten eingespart und die Verschlüsselung vereinfacht. Die automatisierte Verschlüsselungslösung reduziert die Komplexität der Administration und der täglichen Schlüsselverwaltung.

Im Vergleich zu anderen Verschlüsselungslösungen benötigt dieser Service nur die E-Mail-Adresse des Empfängers, um Encryption Keys zu erstellen – die IT-Abteilung muss sich um nichts kümmern. Diese quantensichere Verschlüsselungsmethode entlastet das IT-Personal von der täglichen Aufgabe des Ausstellens und Entziehens von Schlüsseln. Die gehostete Schlüsselverwaltung stellt sicher, dass Verschlüsselungsschlüssel rund um die Uhr verfügbar sind und ermöglicht die Wiederherstellung von Passwörtern und Schlüsseln ohne Eingreifen der IT-Abteilung.

Um ein Höchstmaß an Schutz zu ermöglichen und die Kommunikation, Daten und Dokumente langfristig zu sichern, werden die neuesten, leistungsfähigsten Verschlüsselungs- und Authentifizierungsverfahren eingesetzt. Auf diese Weise bietet QuantiCor sogar vor mächtigen Quantencomputer-Angriffen und fortschrittlichen Algorithmen Schutz.

Vorteil für die Anwender

Kostenreduktion, Aufwandssenkung, höchste Sicherheit durch Einsatz der neuesten, leistungsfähigsten Verschlüsselungs- und Authentifizierungsverfahren, bietet auch Schutz vor Quantencomputer-Angriffen und fortschrittlichen Algorithmen.

Web/Internet Security

Digital Shadows – Monitoring-Tool SearchLight

Digital Shadows ist Anbieter für Digital Risk Protection (DPR) und unterstützt Unternehmen, digitale Risiken zu erkennen, zu verstehen und zu entschärfen. Dazu überwachen sie rund um die Uhr das Open, Deep und Dark Web und spüren kompromittierte Daten (Logins), Bedrohungen durch Cyberkriminelle (Ransomware) sowie Markenmissbrauch (Domain Spoofing) auf – für kundenspezifische und relevante Cyber Threat Intelligence (CTI).

Das Monitoring-Tool SearchLight ermittelt fortlaufend externe digitale Bedrohungen. Dabei kombiniert die Lösung skalierbare Datenanalytik mit dem Know-how von Threat-Intelligence-Analysten. SearchLight arbeitet in vier Schritten, wobei Kunden in jeder Phase von Sicherheitsspezialisten und Customer Success Managern unterstützt werden.

1. Konfigurieren

Im ersten Schritt werden gemeinsame Assets definiert, die es zu schützen gilt. Das Monitoring passt sich dabei an individuelle Anforderungen des Kunden an. Das Ergebnis sind Alerts mit hoher Relevanz und echtem Mehrwert. SearchLight arbeitet iterativ. Der Katalog an Assets wird kontinuierlich angepasst und aktualisiert.

2. Sammeln

SearchLight durchsucht das Open, Deep und Dark Web kontinuierlich nach exponierten Assets. Zu den Quellen zählen unter anderem Code- und File-Sharing-Sites, kriminelle Foren, Chat-Kanäle, Social Media und Suchmaschinen. Teams für den Bereich „Collections und Closed Sources“ erweitern diese Quellen ständig.

3. Analysieren

Dank smarter Filter lässt sich die Flut an Threat-Alerts kanalisieren und auf Vorfälle reduzieren, die für den Kunden tatsächlich eine Gefahr darstellen. Die detaillierten Security Advisories fassen die wichtigsten Infos kompakt zusammen

IT SECURITY AWARD 2022

Die Bewerbungsunterlagen für den it security Award 2022 finden Sie ab April unter der folgenden URL:

www.it-daily.net/award

– zu Akteuren, ihren Taktiken, Techniken und Prozeduren (TTPs) sowie bisherigen Vorfällen. Dieser umfangreiche Kontext spart Zeit bei der Triage.

4. Eindämmen

Jeder Alert empfiehlt Gegenmaßnahmen und ermöglicht es, Takedown-Verfahren einzuleiten. Die sofortige Integration in Enforcement- und Automatisierungsplattformen ermöglicht es Sicherheitsteams, schnell und gezielt weitere Maßnahmen zur Risikominimierung zu treffen.

Und das sind die Alleinstellungsmerkmale:

- Umfassende Abdeckung von Quellen im Open, Deep und Dark Web (nicht nur Social Media)
- Maßgeschneiderte, relevante Threat Intelligence: Filtert 95 Prozent irrelevanter Informationen aus

Vorteil für die Anwender

Ein effizientes Ressourcen-Management ohne versteckte Kosten (Lowest-Total-Cost-of-Ownership). Die Cyber Threat Intelligence (CTI) passt sich Kundenanforderungen individuell an und ist beliebig skalierbar.

Identity & Access Management

Saviynt – Zero Trust Identity

Saviynt ist ein Anbieter von Identity Governance und Administration (IGA) sowie Cloud-Sicherheitslösungen. Mit Saviynt können Unternehmen Anwendungen, Daten und Infrastruktur auf einer einzigen Plattform für die Cloud und Unternehmen sichern. Das Unternehmen bietet IGA-Lösungen der nächsten Generation durch die Integration fortschrittlicher Risikoanalysen mit differenzierter Rechteverwaltung. Ferner bietet es integrierte Unterstützung für kontinuierliches Compliance-Management, Segregation of Duties (SOD)-Analyse und -Wiederherstellung, Zugriffsrechte und Rollenkontrolle.

Version 3.0 ist die wohl innovativste und richtungsweisendste Identity-Governance- und Administrations-Lösung. Mit nur einer service-basierten Identitäts- und Security-Governance-Plattform unterstützt es Unternehmen bei der Sicherung kritischer Anwendungen, Daten und Infrastrukturen wie Microsoft Office 365, Microsoft Azure, Microsoft Dynamics GP, AWS, Salesforce, Workday, SAP, Oracle Cloud ERP/EBS, Epic, Cerner und mehr. Die Vision von Saviynt ist es, das Identitätsmanagement, das Anwendungs-GRC (Governance, Risk & Compliance) und die identitätsorientierte Cloud-Sicherheit (CASB) sowie privilegiertes Zugriffsmanagement (Cloud PAM) in einer Oberfläche zu verwalten. Es definiert Identität als neuen Perimeter, indem daten-, verhaltens- und nutzungsbasierte Identitätsanalysen, die sich über Multi-Cloud- und Hybridumgebungen erstrecken, tief integriert werden. Mit einer umfassenden Bibliothek mit mehr als 1.500 kontinuierlich gepflegten Compliance-Einstellungen, Risiko-Signaturen und Funktionstrennungen etabliert Saviynt eine gänzlich neue Grundlage für die Datensicherheit. Somit hilft der Anbieter Unternehmen schon heute, schrittweise oder vollständig auf zukunftssichere Cloud Infrastrukturen zu migrieren ohne die Aspekte von Enterprise-Access-Governance aus den Augen zu verlieren.

Cloud Security

Netskope – Cloud & Web Security Platform

Der Anteil der über die Cloud verbreiteten Malware nimmt laut Cloud & Threat Report (Juli 2021) weiter zu und hat mit 68 Prozent ein Allzeithoch erreicht. Dabei machen Cloud-Speicher-Apps fast 67 Prozent der über die Cloud verbreiteten Malware aus. Effektive Cloud-Sicherheit kann nur aus der Cloud kommen und muss CASB, SWH und ZTNA vereinen, um so zukunftssicher zu sein und die Einführung von SASE zu ermöglichen.

Die Schatten-IT ist ein weiteres Problem in Unternehmen. 97 Prozent der im Unternehmen genutzten Cloud-Apps sind Schatten-IT, also nicht verwaltet und von Mitarbeitern eigenständig eingesetzt – mit den damit verbundenen Sicherheitsrisiken. Hinzu kommt eine mangelnde Transparenz der Cloud-Aktivitäten: Sensible Daten werden immer häufiger in persönlichen Apps gespeichert. Dabei lädt der durchschnittliche Unternehmensnutzer jeden Monat 20 Dateien von diesen verwalteten Geräten auf persönliche Apps hoch. Insbesondere ausscheidende Mitarbeiter versuchen, erhebliche Mengen an Unternehmensdaten zu exfiltrieren, bevor sie das Unternehmen verlassen. Sie laden in den letzten 30 Tagen ihres Arbeitsverhältnisses dreimal so viele Daten wie üblich auf persönliche Apps hoch. 15 Prozent dieser Daten stammen entweder vom Unternehmenskonto oder verstoßen direkt gegen eine Datenrichtlinie des Arbeitgebers.

Eine sichere Cloud-Adaption kann nur durch SASE erfolgen. SASE steht für Secure Access Service Edge und genau dort ist Netskope zuhause. Wichtig ist das richtige Gleichgewicht zwischen Schutz und Geschwindigkeit, welches Anwender benötigen, um ihre Geschäftsabläufe zu beschleunigen und ihre digitale Transformation sicher voranzutreiben. Unternehmen profitieren so von den Vorteilen der Cloud bei gleichzeitiger Verbesserung des Sicherheitsniveaus durch die Umsetzung des SASE-Ansatzes.

Das Sicherheitsnetzwerk NewEdge bietet durch seine starke Vernetzung den Anwendern ein Nutzererlebnis mit geringsten Latenzen, bei dem gleichzeitig die höchste Sicherheit gewährleistet wird. Damit unterscheidet sich die Nutzung einer Cloud-Anwendung nicht von lokal betriebenen Lösungen.

Vorteil für die Anwender

Die aktuellen Problemstellungen zeigen, dass Unternehmen die Sicherheit angesichts der tatsächlichen Nutzung von Cloud-Anwendungen überdenken müssen. Sie sollten auf eine Sicherheitsarchitektur setzen, die Kontext für Apps. Cloud-Dienste sowie Web-Benutzeraktivitäten bietet und die Zero-Trust-Kontrollen anwendet, um Daten zu schützen, wo und wie auch immer auf sie zugegriffen wird.

Über die it security Awards 2021 freuen sich (von links nach rechts): Frank Schmäring, Sr. Solutions Engineer, Saviynt, Robert Blank, Regional Sales Manager DACH, Digital Shadows, Kristina Vervoort, Regional Sales Director DACH, Netskope, Rachid El Bansarkhani, CEO, QuantiCor Security und Ulrich Parthier, Herausgeber it security. (Quelle: www.it-daily.net)

DATEN EFFIZIENT SCHÜTZEN

DIE 5 HÄUFIGSTEN RISIKEN

Meldungen von Unternehmen, die von Datenschutzverletzungen und Daten-Leaks betroffen sind, haben in letzter Zeit stark zugenommen. Im Durchschnitt kosten diese Verletzungen deutsche Unternehmen stolze 4,11 Millionen Euro – damit liegt Deutschland auf Platz vier der teuersten Märkte.

Die häufigsten Datenschutzverletzungen

1. Hackerangriff

Dabei wird ein Unternehmen von außen mithilfe von Schadsoftware, Trojanern oder Malware angegriffen. Einfallstore sind häufig Sicherheitslücken oder Fehlkonfigurationen des Firmennetzwerks.

2. Unerlaubte Weitergabe von Daten

Die Gefahr besteht, wenn sensible Daten unerlaubt weitergegeben werden, zum Beispiel über einen Messenger-Dienst – egal ob absichtlich oder versehentlich.

3. Datendiebstahl

Der digitale Datendiebstahl durch Cyberattacken oder Phishing führt in diesem Bereich das Feld an. Aber auch der physische Datendiebstahl wie das Entwenden eines USB-Sticks oder einer Festplatte spielt nach wie vor eine Rolle.

4. E-Mail- oder Post-Fehlversand

Werden personenbezogene Daten per E-Mail oder auf dem Postweg an eine nicht autorisierte Person geschickt, liegt schnell eine Datenschutzverletzung vor. In den seltensten Fällen kann nachvollzogen werden, was mit den Daten passiert ist.

5. Offener Mailverteiler

Wenn eine E-Mail mehreren Personen zugestellt werden soll, darf normalerweise nicht bekannt sein, wer die Nachricht noch erhalten hat. Ist dieses aber ersichtlich, ist der Datenschutz nicht ausreichend gewährleistet.

Wie kann man sich schützen

Durchdachte Softwarelösungen bieten dank vorgefertigter und intuitiver Workflows einen einfachen Weg, um Datenschutz in Unternehmen übersichtlich zu managen. Darüber hinaus helfen Mitarbeiterschulungen und -Sensibilisierungen, strukturierte und transparente Prozesse im Unternehmen sowie eine klare Aufgaben- und Kompetenzverteilung, das Risiko von Datenschutzverletzungen zu minimieren.

www.datenschutzexperte.de

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Ari Albertini, Günter Esch, Andreas Fuchs, Jochen Koehler, Sabine Kuch, Carina Mitzschke, Andreas Nolte, Silvia Parthier, Ulrich Parthier, Hanno Pingsmann, Michael Scheffler, Neil Thacker, Michael Veit, Jörg von der Heydt

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

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

Manuskripteinsendungen:
Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in 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 Veröffentlichungen 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. 29, gültig ab 1. Oktober 2021.

Mediaberatung & Content Marketing-Lösungen it management | it security | it daily.net:
Kerstin Fraenzke
Telefon: 08104-6494-19
E-Mail: fraenzke@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 Beträge

Immer gut informiert!

Tägliche News für die Enterprise IT

finden Sie auf **www.it-daily.net**

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