itmanagement

OKTOBER 2020

INKLUSIVE 48 SEITEN
IT SECURITY

SAP SPEZIAL

Umdenken erforderlich

PROJEKT-MANAGEMENT

Die richtigen Tools

AFI

On-Premises, SaaS oder Outsourcing **ab Seite 16**

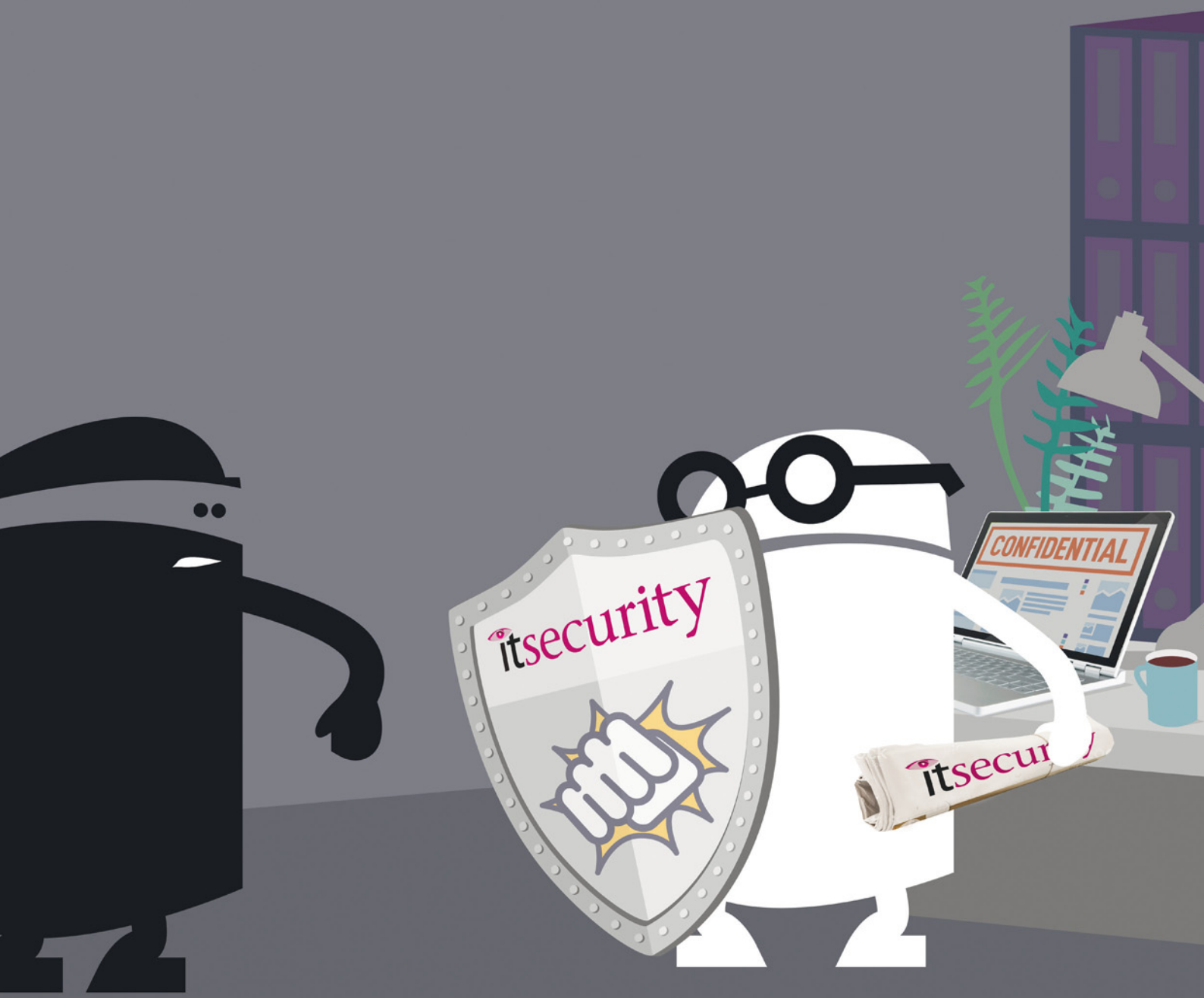
S/4HANA

SICHERE TRANSFORMATION

Ralf Kempf, SAST SOLUTIONS

www.it-daily.net

Wer viel weiß, weiß sich zu wehren.



Der nächste Angriff kommt bestimmt.

Gut vorbereitet mit itsecurity

www.it-daily.net

MOST WANTED

Der Mangel an IT-Experten wird immer größer! Ein riesiges Problem für die Branche – und das nicht erst seit gestern.

Die Digitalisierung schreitet, mehr oder weniger, voran, das IoT wächst kontinuierlich und damit einhergehende Sicherheitsfragen ebenso. Allein während des Lockdowns nahmen Cyberangriffe auf Infrastrukturen eklatant zu. Innerhalb eines Jahres stiegen beispielsweise Ransomeware-Angriffe auf Krankenhäuser um 73 Prozent! (https://bit.ly/3hXytLE) Mit Threat Intelligence, Firewalls, Sandboxing etc. kommt man da nicht wirklich weiter. Was fehlt, sind die Fachleute, die Experten, die Zusammenhänge erkennen und die passende oder am besten geeignetste Lösung für Unternehmen implementieren können. Doch hier scheitert es bereits.

Woran das liegt? Ein erster Impuls meinerseits: am Föderalismus in Deutschland! Natürlich liegt hier nicht die Wurzel des Problems, aber vielleicht ein Teil davon. Einheitliche Schulsysteme wären schon mal ein Anfang und würde man dann noch beizeiten – weiterführende Schulen – mit den Grundlagen des Internets, der Programmierung, Basics wie Word, Powerpoint anfangen, würden vielleicht Arbeitnehmer heranwachsen, die zu Experten werden könnten. Denn, dass die „Jugend von heute" technikaffin ist, kann man nicht leugnen, aber vielleicht muss man sie einfach in die richtige Richtung schubsen, beziehungsweise Starthilfe geben. Einsatzgebiete und Anwendungen gibt es auf jeden Fall genug, wie Sie in dieser Ausgabe nachlesen können.

Viel Spaß beim Weiterbilden

Carina Mitzschke | Redakteurin it management

10
COVERSTORY

16

INHALT

20

COVERSTORY

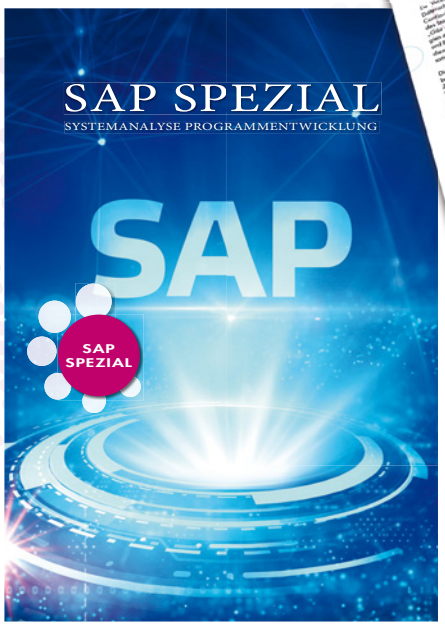
SAP SPEZIAL

IT MANAGEMENT

26

AP

18



14

Inklusive 48 Seiten

IT SECURITY SPEZIAL

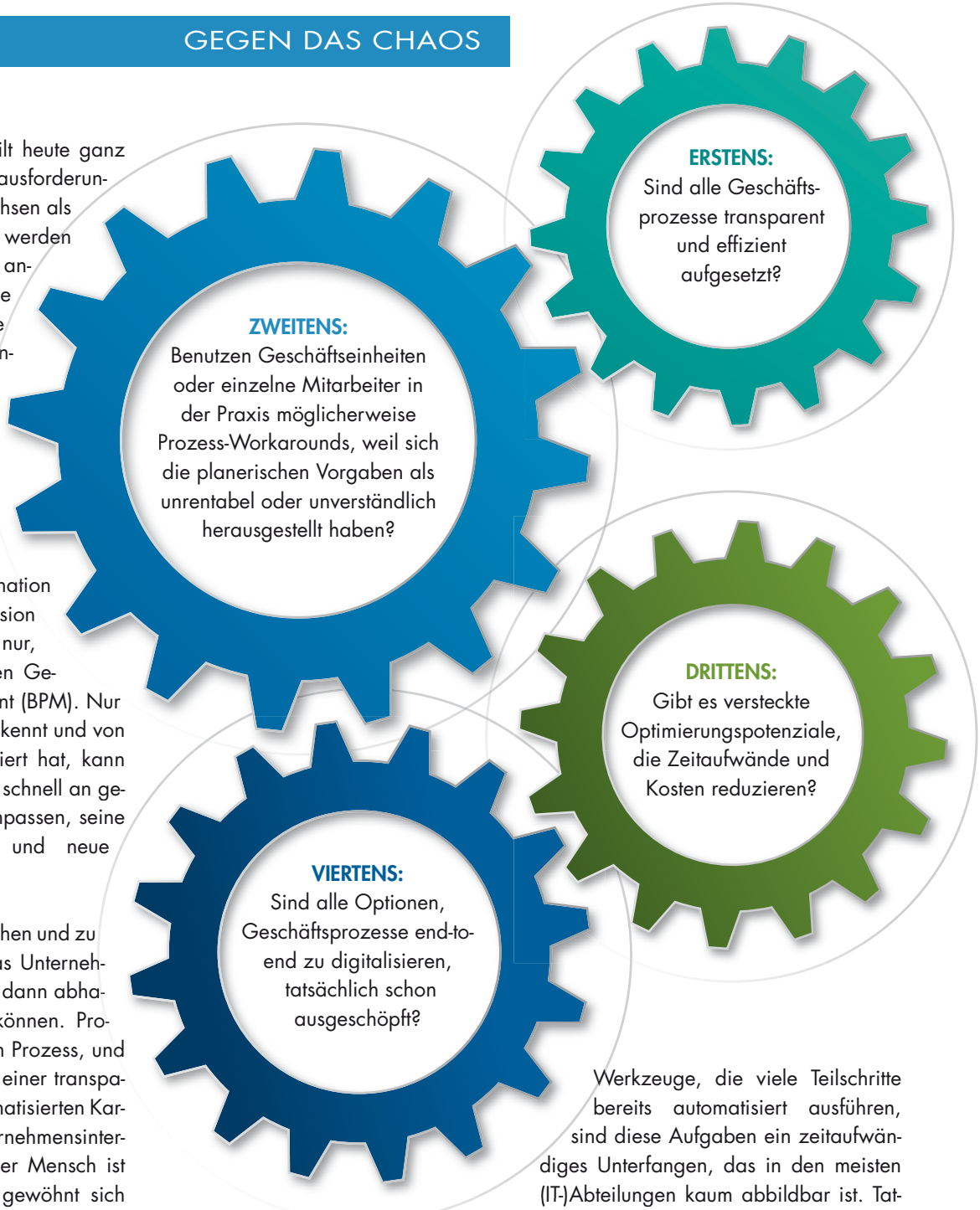
SAUBERE GESCHÄFTSPROZESSE

GEGEN DAS CHAOS

Was früher schon galt, gilt heute ganz besonders, denn die Herausforderungen sind eher noch gewachsen als gesunken. Einige Märkte werden sich komplett neu erfinden, andere zumindest teilweise verändern. Das, was alle Unternehmen heute gemeinsam haben, ist die Notwendigkeit zur Transformation, eine flexible Anpassung an neue Kundenbedürfnisse und neue Marktbedingungen.

Deshalb ist eine Kombination aus Flexibilität und Präzision besonders wichtig, nicht nur, aber vor allem im eigenen Geschäftsprozess-Management (BPM). Nur wer seine Prozesse genau kennt und von Anfang bis Ende digitalisiert hat, kann sich flexibel und vor allem schnell an geänderte Anforderungen anpassen, seine Kunden zufriedenstellen und neue Märkte erobern.

Prozess-Exzellenz zu erreichen und zu halten, ist kein Projekt, das Unternehmen einmal erledigen und dann abhaken und ad acta legen können. Prozess-Exzellenz ist selbst ein Prozess, und der erste Schritt besteht in einer transparenten und möglichst automatisierten Kartographierung ihrer unternehmensinternen Prozess-Landschaft. Der Mensch ist ein Gewohnheitstier und gewöhnt sich auch an umständliche, chaotische Arbeitsweisen. Nur leider führen umständliche Prozessverläufe nicht zielführend und auf möglichst kurzem Weg zum Erfolg. Unternehmen sollten sich deshalb vier entscheidende Fragen stellen:



Process Mining ist nur der erste Schritt, darauf folgen Prozess-Optimierung, die Umsetzung in ausführbaren Workflow und ein kontinuierlicher Praxis-Check, also die schnelle Anpassung an neue Herausforderungen. Ohne leistungsstarke Werkzeuge, die viele Teilschritte bereits automatisiert ausführen, sind diese Aufgaben ein zeitaufwändiges Unterfangen, das in den meisten (IT-)Abteilungen kaum abbildbar ist. Tatsächlich sind praxiserprobte Werkzeuge essenziell, damit Unternehmen Prozess-Exzellenz erreichen, sich vom Wettbewerb deutlich absetzen können und erfolgreich am Markt wirtschaften.

www.signavio.com/de

NEUE STUDIE

VERALTETE DRUCKINFRASTRUKTUREN

Lexmark hat kürzlich die Marktforscher von IDC mit der Durchführung einer weltweiten Untersuchung beauftragt, die während der ersten Phase der Corona-Pandemie im Frühjahr 2020 durchgeführt wurde. Sie zeigt, dass vier von fünf (79 Prozent) der befragten Unternehmen im Rahmen ihrer Digitalisierungsinitiativen in eine Cloud-Infrastruktur investieren. 57 Prozent geben allerdings an, dass sich eine zu alte Druckinfrastruktur negativ auf ihre Cloud-Migrationsstrategie auswirkt.

Auch wenn das Druckvolumen insgesamt zurückgegangen ist, da einige Unternehmen bereits einen „Digital First"-Ansatz beim Dokumentenmanagement verfolgen, erfordert laut Studie etwas mehr als die Hälfte aller grundlegenden Workflow-Prozesse immer noch eine erhebliche Zahl an Ausdrucken. Unternehmen müssen daher für die absehbare Zukunft die Möglichkeit zum Drucken als wesentliche IT-Dienstleistung bereitstellen.

Die Verwaltung der IT-Infrastruktur stellt insgesamt nach wie vor eine Herausforderung dar. Die Mehrheit der befragten Unternehmen äußerte in diesem Zusammenhang sehr ähnliche Probleme, auch in Bezug auf die klassischen Druckprozesse.

WAS UNTERNEHMEN BEMÄNGELN

81 %
Gewährleistung der Sicherheit von Druckinfrastruktur und -geräten

81 %
Die mit der Verwaltung von Druckern und Druckservern verbundene IT-Belastung

80 %
Bestandsverwaltung bei gleichzeitig mangelnder Transparenz der Ausgaben

79 %
Veraltete Technologie sowie Schwierigkeiten bei der Aktualisierung oder dem Austausch von Bestands-Druckhardware

www.lexmark.com

KOMMUNIKATIONSTIPPS

ARBEIT AN VERTEILTEN STANDORTEN

Die zunehmende Arbeit im Home-Office bietet eine Vielzahl an Möglichkeiten, aber auch an Risiken. Laut Umfrage unter 500 Büroarbeitern glaubt die große Mehrheit der Befragten (83 Prozent), dass die Corona-Krise einen neuen Unternehmenstrend hin zu mehr Digitalisierung und Home-Office eröffnet hat. Die klare Mehrheit (61 Prozent) spricht sich ebenso für ein Gesetz aus, das ein Recht auf Home-Office etabliert, wie es derzeit in Deutschland diskutiert wird.

Um die Mitarbeiterkommunikation im Home-Office am Laufen zu halten, sollten die Kommunikations-Tools sorgfältig ausgewählt werden. Im Büro kommunizieren die Mitarbeiter in großen informellen Brainstorming-Runden, in kleineren Projekt-Gruppen oder sie haben vertrauliche Gespräche zu zweit. Diese unterschiedlichen Kommunikationsformen sollten ebenso abgedeckt werden können, wenn die Mitarbeiter nicht persönlich zusammensitzen.

Die OTRS AG hat Tipps zusammengestellt, um die Arbeit auch im Home-Office im Fluss zu halten:

1. **Lösung für Videokonferenzen:** Für den Kommunikationsfluss ist es wichtig, während einer Besprechung auch die Mimik einer Person beobachten zu können. Dafür eignet sich ein Tool wie GoToMeeting, das alle Teammitglieder gleichzeitig einschalten können, um eine effiziente Gruppendiskussion zu führen.

2. **Lösung zum spontanen Chat:** Der Austausch, der in einer spontanen Kaffeepause stattfindet, kann manchmal zu hervorragenden Ideen führen. Deswegen ist es essentiell, auch die spontane Chat-Funktion zwischen Kollegen mit entsprechenden Lösungen wie zum Beispiel Rocket-Chat zu fördern.

3. **Brainstorming-Optionen:** Auch virtuell können Ideen mit farbigen Post-It´s festgehalten werden, so dass es zu weiteren kreativen Interaktionen kommt. Wie wäre es mit Miro?

4. **Online-Webinare:** Weiterbildung ist ein wichtiger Motivator für Mitarbeiter. Auch wenn die Fortbildung nicht physisch stattfinden kann, gibt es immer noch viele Möglichkeiten, sich weiterzuentwickeln: Webinare (oftmals auch kostenlos über LinkedIn) bieten sich an sowie interne Trainingsmöglichkeiten per Videokonferenz oder Online Podcasts.

www.otrs.com

DATA TRAVELER
DIE OPTIMALE WAHL

Kingston Digital kündigt die Verfügbarkeit einer 128 GB-Version des verschlüsselten DataTraveler2000-USB-Sticks an. Der DT2000 ist zertifiziert für FIPS 140-2 Level 3, bietet eine AES-256-Bit-Hardware-Verschlüsselung auf Militär-Standard und verfügt über eine alphanumerische Tastatur, die den Nutzern das Sperren des Sticks über eine Wort- oder Zahlenkombination ermöglicht.

www.kingston.com

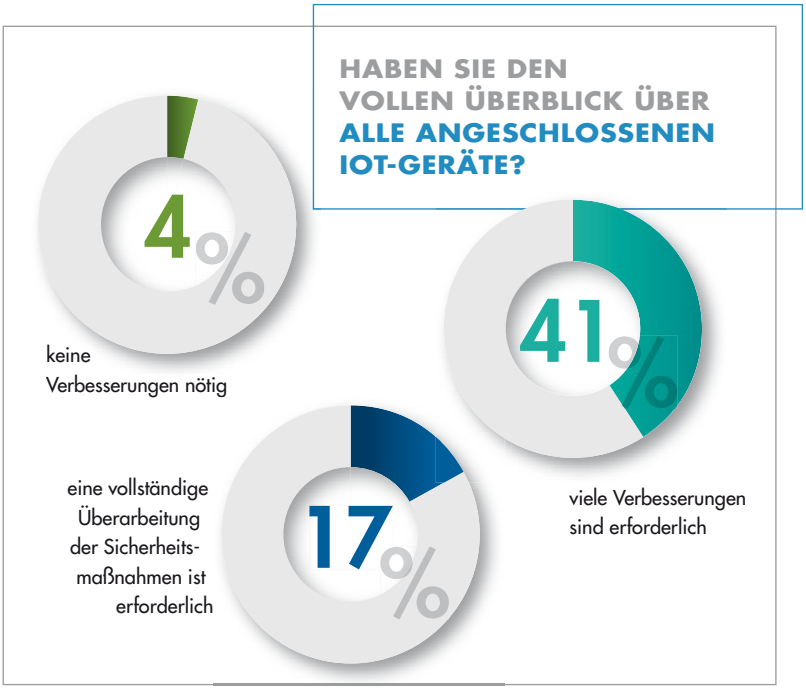
INTERNET OF THINGS

CHANCE UND RISIKO

Das Internet der Dinge ist für viele Unternehmen in Deutschland sowohl Chance als auch Risiko, so das Ergebnis einer aktuellen Studie um Auftrag von Palo Alto Networks. Einerseits ermöglicht ein hoher Vernetzungsgrad eine Effizienzsteigerung, zunehmende Automatisierung, bessere Datennutzung und neue Geschäftsmodelle. Gleichzeitig aber stellt die wachsende Popularität des IoT für Unternehmen und ihre IT-Abteilungen eine wachsende Herausforderung für die Daten und IT-Sicherheit dar.

Da Unternehmen nur das verwalten und schützen können, was sie sehen, sollte sie sich dringend einen vollständigen Überblick über die genaue Anzahl der an die Netzwerke angeschlossenen IoT-Geräte verschaffen.

www.paloaltonetworks.com



SICHERE TRANSFORMATION

STRATEGIE, UMSETZUNG, SICHERHEITSÜBERWACHUNG IN ECHTZEIT – ALLES AUS EINER HAND

Ralf Kempf, CTO SAST SOLUTIONS bei der akquinet AG hat mit seinem Team bereits viele Unternehmen bei der sicheren Migration auf SAP S/4HANA begleitet. Über Erfolgsrezepte äußert er sich im Gespräch mit Ulrich Parthier, Herausgeber it management.

Ulrich Parthier: *Die Digitale Transformation beschäftigt heute jedes Unternehmen. Da stellt sich zu allererst die Frage „Warum SAP S/4HANA"?*

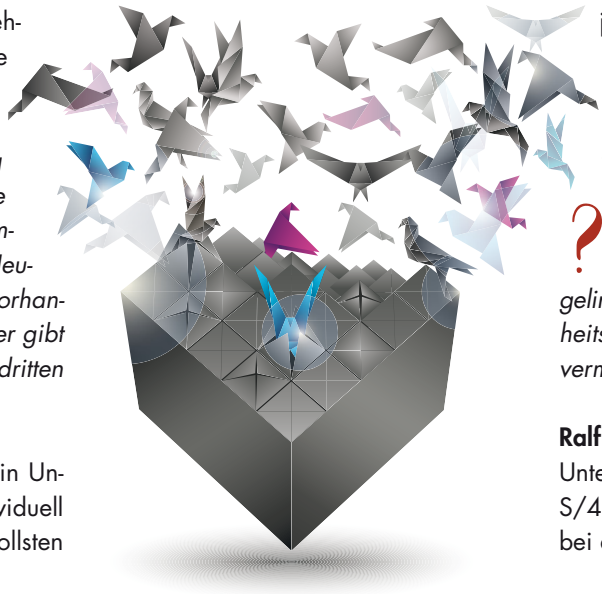
Ralf Kempf: Für diese Entscheidung gibt es eine Vielzahl von Gründen, wie den Zugriff auf Geschäftszahlen in Echtzeit, die Automatisierung von Prozessen oder eine bessere Unterstützung neuer Geschäftsmodelle. Wenn man künftig wirtschaftlich agil auf neue Anforderungen an die IT reagieren und wettbewerbsfähig bleiben möchte, wird man an S/4HANA nicht mehr lange vorbeikommen. Nicht ganz außer Acht zu lassen ist natürlich auch die Einstellung des Supports für derzeitige ERP-Systeme durch die SAP – auch wenn die Deadline 2027 beziehungsweise 2030 für viele Unternehmen gefühlt noch in weiterer Ferne liegt.

Ulrich Parthier: *Beim Umstieg auf SAP S/4HANA lautet die Gretchenfrage: Wie gelingt der Umstieg? Wähle ich eine komplette Neueinführung oder kann ich meine vorhandenen Prozesse übernehmen? Oder gibt es eventuell auch noch einen dritten Weg?*

Ralf Kempf: Welcher Ansatz für ein Unternehmen der ideale ist, muss individuell betrachtet werden. Ist es am sinnvollsten alte „Prozesszöpfe" endlich einmal abzuschneiden und im Rahmen eines Greenfield-Ansatzes ganz neu aufzusetzen? Oder ist die vorrangige Herausforderung die Aufwände so gering wie möglich zu halten und man entscheidet sich für einen Brownfield-Ansatz. Und natürlich gibt es auch einen Mittelweg, den Selective Data-Ansatz, der die Möglichkeit bietet, gute Prozesse zu überführen und veraltete Prozesse neu abzubilden.

Eines eint alle Ansätze: Es gilt eine Reihe grundlegender Entscheidungen bereits vor Einführung von SAP S/4HANA zu treffen. Wir erleben leider viel zu oft, dass Verantwortlichen zu Projektbeginn nicht wirklich bewusst ist, welche Herausforderungen insgesamt vor ihnen liegen und das kostet später nicht nur Zeit, sondern verursacht häufig auch erhebliche Extrakosten.

Ulrich Parthier: *Thema Experten-Stau. Wo sehen Sie die Gefahren?*



Ralf Kempf: Laut DSAG-Investitionsreport 2020 werden bis Ende 2021 erst rund 20 Prozent aller Unternehmen auf das neue System migriert sein. Weitere 40 Prozent planen im Rahmen ihrer S/4HANA-Strategie einen technischen Releasewechsel bis Ende 2023. Es ist somit mit einer wahren Projektlawine bereits ab 2022 und einer hohen Nachfrage an spezialisierten Dienstleistern zu rechnen. Während ein großer Teil der Unternehmen bereits mitten in der Migration steckt, plant ein ebenso großer Teil genau dann mit der Umsetzung zu beginnen.

Dazu kommt noch die Verlängerung der Support-Deadline für SAP ERP-Systeme. Dies bedeutet nicht, dass Unternehmen, die S/4HANA noch nicht im Einsatz haben, sich jetzt Zeit lassen können, denn es droht ein vorhersehbarer Experten-Engpass. Ein derart großes Projekt wie eine Migration auf S/4HANA erfordert immer mehr Workload, als man am Anfang einplant. Unternehmen und Verantwortliche sollten sich daher mit den internen Ressourcen auf das Kernprojekt der Umstellung konzentrieren und für das Spezialthema wie die Absicherung der neuen Systeme auf externe Experten setzen, die das interne Team entlasten.

Ulrich Parthier: *Ein Damoklesschwert ist das Thema SAP-Sicherheit. Wie gelingt es, mit einer guten Strategie Sicherheits-Schwachstellen in S/4HANA zu vermeiden?*

Ralf Kempf: Fakt ist, fast ein Drittel der Unternehmen, die eine Migration auf S/4HANA planen, vernachlässigen hierbei die Absicherung der neuen Systeme.

AUF S/4HANA

> ACHTEN SIE DARAUF, IHRE SICHERHEITSMÄNGEL NICHT MIT NACH S/4HANA ZU ÜBERNEHMEN, WIE BEISPIELSWEISE CODING, DAS LÄNGST SCHON NICHT MEHR VERWENDET WIRD. DAS ÖFFNET BELIEBTE HINTERTÜREN FÜR CYBER-KRIMINELLE UND ES ENTSTEHEN FOLGEKOSTEN IN MILLIONENHÖHE.
>
> Ralf Kempf, CTO SAST SOLUTIONS, akquinet AG, www.akquinet.com

EINE MIGRATION OHNE INTENSIVE PLANUNG UND BERÜCKSICHTIGUNG DER BEREICHE CYBER SECURITY & AUTHORIZATION MANAGEMENT FÜHRT ZU EINER VIELZAHL NEUER SICHERHEITSRISIKEN UND VERMEIDBAREN FOLGEAKTIVITÄTEN. SETZEN SIE DAHER VON ANFANG AN AUF EINE GANZHEITLICHE S/4HANA-STRATEGIE UND BINDEN SIE ERFAHRENE EXPERTEN EIN.

Doch die Nicht-Beachtung der Sicherheitsaspekte kann zu erheblichen wirtschaftlichen Schäden führen. Dabei bietet ein Migrationsprojekt auch die Chance, mit einer sauber aufgesetzten und ganzheitlichen geplanten Security & Compliance-Strategie die Absicherung der IT-Systeme auf ein neues Level zu heben. Daher sollte das oberste Credo sein, diese Herausforderung auch als Chance zu verstehen: um die Sicherheit in SAP-Systemen zu verbessern, Rollenkonzepte effizienter zu gestalten und das neue System mit all seinen Vorteilen nutzen zu können.

Ulrich Parthier: *Wie lautet ihre Empfehlung?*

Ralf Kempf: Bei einer Konvertierung auf SAP S/4HANA ist es entscheidend, von vorneherein eine belastbare und konsistente Grundsicherheit in die Migrationsstrategie einzubeziehen. So vermeiden Sie nicht nur typische Stolperfallen beim Plattformwechsel an sich, sondern auch die zu späte Überführung Ihrer SAP-Berechtigungen und profitieren dadurch in dreifacher Hinsicht.

1. **Die Zeitersparnis:** Sie fassen das Projekt nur einmal an und das dafür vollumfänglich. Dadurch verkürzen Sie den Migrationszeitraum insgesamt und können früher starten alle Vorteile des neuen Systems zu nutzen.

2. **Schonung der internen Ressourcen:** Holen Sie sich frühzeitig die richtigen Berater und Software-Lösungen an Bord, auch beim Thema SAP Sicherheit und Compliance. Das stellt sicher, dass Ihr Tagesgeschäft parallel ungestört weiterläuft. Mit der richtigen Software, wie der SAST SUITE, profitieren Unternehmen zum einen bei der vollumfänglichen Grundabsicherung der neuen Systeme. Zusätzlichen unterstützt die SAST SUITE bei der sicheren Überführung aus den Altsystemen und man gewinnt für die Zeit nach der Migration durch die Automatisierung von Abläufen und ein kontinuierliches Echtzeit-Monitoring.

3. **Finanzielle Ersparnisse:** Die Umstellung auf ein neues System ist bereits ein teures Unterfangen. Doch werden die Themen Sicherheit und Compliance erst nach einer Migration angefasst, wird es ungemein teurer. Dann muss nicht nur die neue Plattform selbst abgesichert werden, hinzu kommt die Bereinigung der unnötig migrierten Altlasten. Ganz zu schweigen von dem wirtschaftlichen Schaden, der einem Unternehmen droht, wenn es aufgrund von migrierten Sicherheitslücken zu Datendiebstählen kommt.

Je eher Unternehmen mit einer ganzheitlichen Migrations-Strategie starten, desto besser sind die neuen S/4HANA-Systeme gegen Bedrohungen von innen und auch außen abgeschirmt.

Ulrich Parthier: *Welche weiteren Fehler werden aus ihrer Erfahrung bei der Migration auf S/4HANA gemacht?*

Ralf Kempf: Ein häufiger Irrglaube ist, dass Fiori – also die Benutzeroberfläche mit SAP Apps – eine Lösung für nahezu alles ist und so heißt es in vielen Migrationsprojekten „Fiori first!". Doch seitens der SAP ist Fiori noch nicht durchgängig und es sind noch lange nicht alle Prozesse abgedeckt. Daher ist unsere Empfehlung, Fiori nur da einzusetzen, wo es einen echten Mehrwert bietet und Dinge vereinfacht.

Ein zweiter Tipp, damit Unternehmen auch von den vielen Vorteilen der neuen Technologie profitieren können: Planen Sie mehr Zeit ein. Den Fachbereichen fehlen häufig das erforderliche Prozess-Knowhow und das Wissen, wie sie künftig in S/4HANA arbeiten wollen. Geschäftsprozesse bereichsübergreifend sinnvoll zu optimierten geht eben nicht mal kurz neben dem Tagesgeschäft.

Ein dritter Fehler, dem wir leider öfter begegnen, sind die schon angesprochenen Altlasten, die teils quasi „aus Versehen" ins neue System übernommen wurden – ich denke hier gerade ganz konkret an Coding. Anstatt zunächst zu analysieren, was wirklich noch gebraucht wird, wird alles 1:1 kopiert. Die Folge: Es werden auch alle Sicherheitsmängel mit übernommen, ebenso wie Coding, das längst nicht mehr verwendet wird und dann beliebte Hintertüren für Cyberkriminelle bietet. Dadurch entstehen Folgekosten in Millionenhöhe.

Alles Stolperfallen, die mit einer guten und von Anfang an ganzheitlichen S/4HANA-Sicherheitsstrategie absolut vermeidbar sind.

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

Folge uns auf Social Media:

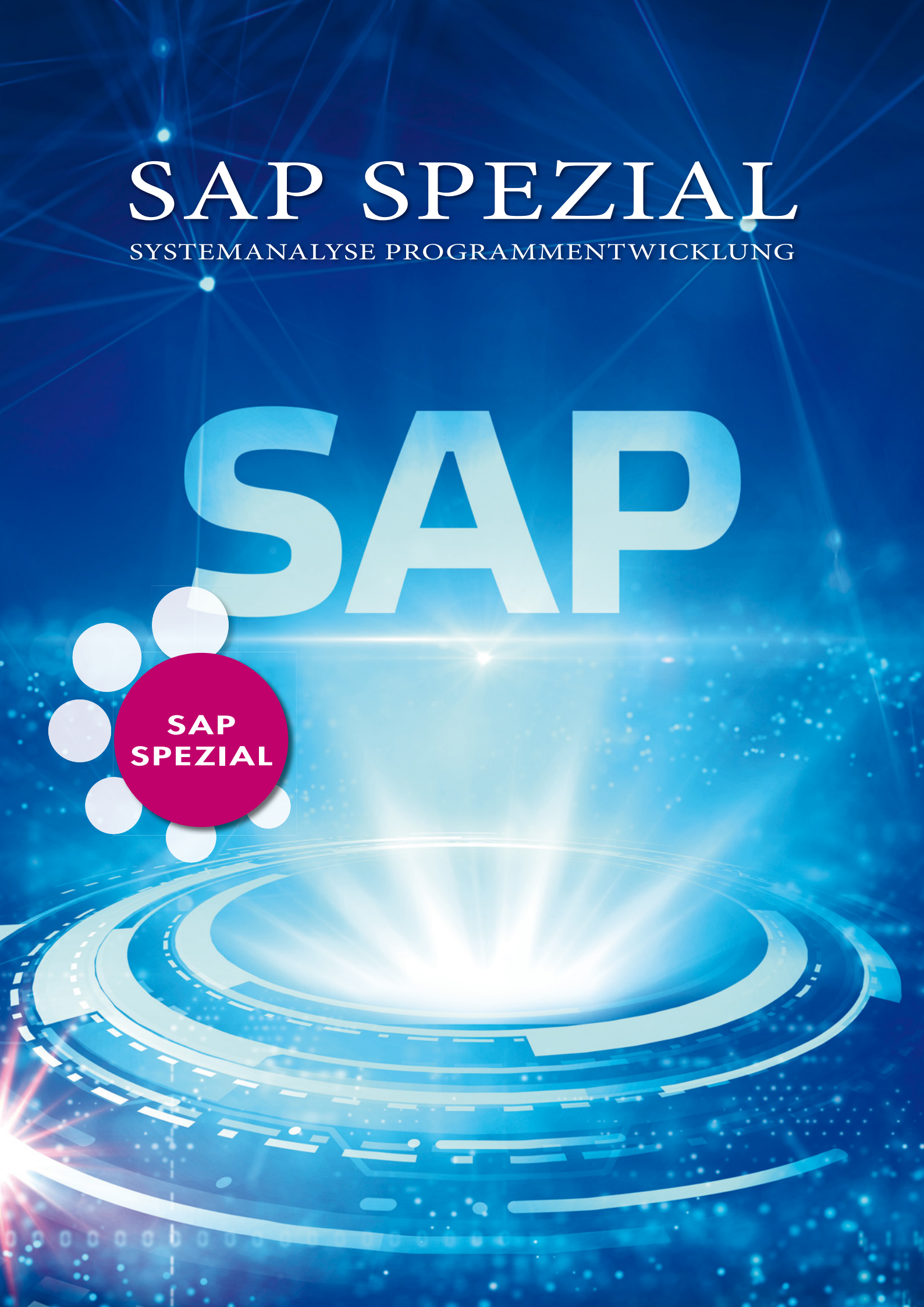
Suchen: IT-Profis.
Bieten: Deutschland.

Jetzt beim ITZBund bewerben und unsere Zukunft digital gestalten.
Digital-für-Deutschland.de

Informations
Technik
Zentrum Bund

SAP SPEZIAL

SYSTEMANALYSE PROGRAMMENTWICKLUNG



SAP, THE AGILE WAY

PRAXISBEWÄHRTE TIPPS FÜR DIE FÜHRUNG WELTWEIT VERTEILTER SAP-TEAMS

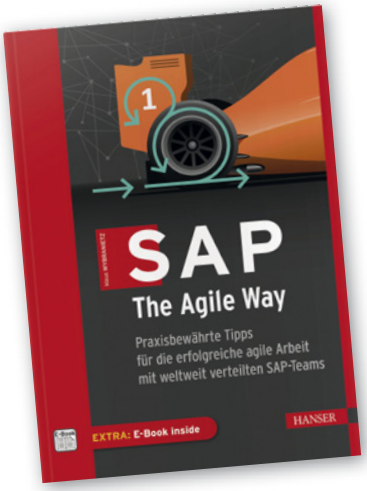
„Ja, Scrum ist toll, aber mit SAP funktioniert das nicht!" Klaus Wybranietz beweist seit Jahren das Gegenteil: Scrum und SAP können auf einen Nenner gebracht werden, und das sogar sehr erfolgreich. Denn in seinen Projekten für internationale Großkonzerne hat Klaus Wybranietz immer wieder die Erfahrung gemacht: Selbst weltweit verteilte SAP-Teams könne mit Scrum das Dreifache in der halben Zeit erreichen.

In diesem Buch erklärt der Autor die Entwicklungsstufen, über die er SAP-Teams aus dem klassischen Wasserfalldenken heraus und stattdessen hinein in die agile Performance führt.

Agile SAP-Teams aufbauen:
Wie Teambuilding im SAP-Umfeld klappt und selbst eigenbrötlerische SAP-Superstars teamfähig werden

Agile SAP-Teams weiterentwicklen:
Kompetenzen gezielt aufbauen und ein abgestimmtes Regelwerk ausarbeiten – bewährte Praktiken für fortgeschrittene agile SAP-Teams

Remote-Arbeiten mit weltweit verteilten agilen SAP-Teams:
Tipps für die effektive Zusammenarbeit auf Distanz – nicht erst durch Covid-19 gesammelt, sondern seit 20 Jahren erprobt



Echte Werte schaffen durch Value Stream Management:
Mit dem Flusskonzept und den Metriken von Kanban agile SAP-Teams schneller und wertschöpfender machen.

SAP, The Agile Way
Klaus Wybranietz,
Carls Hanser Verlag,
2020

ON-PREMISES, SAAS ODER OUTSOURCING

HABEN WIR EINE WAHL? ODER SIND WIR NICHT LÄNGST GETRIEBENE?

Das Outsourcing von Dienstleistungen sowie Software boomt und die Vorteile liegen auf der Hand: Kostenersparnis, Qualitätsverbesserung und die Konzentration auf eigene Kernkompetenzen. Haben Unternehmen heute dann überhaupt noch eine Wahl?

Die Zeiten, in denen Entscheidungswege für IT-Systeme mehrere Jahre in Anspruch nehmen konnten, sind vorbei. Immer wieder gibt es Treiber von außen, die eine schnelle Reaktion beziehungsweise Veränderung provozieren – daher sprechen umso mehr Gründe dafür, Veränderungen im eigenen Unternehmen strategisch auszurichten.

Business Process Outsourcing (BPO)

Was verbirgt sich eigentlich hinter einem „ausgelagerten Betriebsprozess"?

Modelle für Shared Services, Zeitarbeit und „Outsourcing" sind nichts Neues. Es gibt sie bereits seit mehr als 20 Jahren. Sie sind entsprechend dokumentiert, beschrieben und wissenschaftlich beleuchtet. Neu, im Vergleich zu damals, ist die Tiefe der Prozessintegration in die IT-Landschaft und die damit verbundene Abhängigkeit, diese auch im ERP-System abzubilden.

Heute durchlaufen beispielsweise eingehende Rechnungen das Unternehmen nicht mehr in Papierform, sondern werden digitalisiert und zumindest per E-Mail weitergereicht. Im nächsten Schritt landen sie in einem IT-System, das digitale Aufbewahrungssysteme, Workflowtechnologie sowie Buchhaltungssysteme vereint. Bearbeitungsabläufe, Ablage- sowie Suchprozesse werden dadurch optimiert und die Durchlaufzeiten verkürzt. Gleichzeitig erhöht sich der betriebliche IT-Aufwand: Immer mehr Systeme müssen technisch betreut und fachlich gewartet werden. Eine IT-Landschaft ohne Fehl und Tadel wird ein Traum bleiben. Das äußert sich in abgeschlossenen Service- und Wartungsverträgen genauso wie in notwendigen Schulungen für das IT-Personal.

Der BPO-Effekt

Drei Effekte stellen sich idealerweise ein, wenn Teil- oder Gesamtprozesse ausgelagert werden:

- Neuer Raum für wertschöpfende Kernkompetenzen, und zwar abteilungsübergreifend: Anstatt Papierbelege abzulegen und wieder zu suchen, kümmern sich die Buchhaltungskräfte um das Forderungsmanagement des Unternehmens. IT-Ressourcen stehen etwa für produktionssteuernde Projekte zur Verfügung.

Am Beispiel eingehender Rechnungen gilt das für eine Vielzahl von Unternehmen, wenn sie nicht gerade Dienstleister im Buchhaltungsbereich sind und ihr Geschäftsmodell genau auf diesen Tätigkeiten basiert.

> WAS MOTIVIERT UNTERNEHMEN, SOFTWARE NICHT MEHR IM EIGENEN HAUS ZU BETREIBEN, SONDERN ALS SERVICELEISTUNG ZU BEZIEHEN? IM KERN GIBT ES DREI WESENTLICHE ANFORDERUNGEN AN DEN BETRIEB VON IT-SYSTEMEN: VERFÜGBARKEIT, FUNKTIONALITÄT UND PERFORMANCE.
>
> Sven Schal, Geschäftsführer AFI Solutions GmbH, www.afi-solutions.com

➤ Prozesse sind trotz Veränderungen stabiler und verlässlicher abgebildet. Rechtsvorgaben ändern sich permanent, wie beispielsweise das Steuerrecht oder die Datenschutzbestimmungen: Hier kann sich das Unternehmen entspannt zurücklehnen, denn der Dienstleister ist aufgefordert, die Prozessqualität sicherzustellen.

➤ Prozesse auszulagern, ergibt vor allem dann Sinn, wenn am Ende des Tages auch Kosten eingespart werden. Dies im Vorfeld zu ermitteln, ist nicht immer ganz trivial: Kostenstellen müssen sauber getrennt, indirekte Effekte bewertet und in eine Kostenbetrachtung eingebracht werden. Außerdem spielt die zu erwartende Laufzeit eines BPO-Vertrages eine erhebliche Rolle, damit sich Anfangsaufwendungen nach einer gewissen Zeit auch wirklich rechnen.

Generell sollte das Auslagern von Teilprozessen nicht defizitär als Verlust betrachtet werden, sondern als Chance, sich auf seine Kernkompetenzen zu fokussieren – sowohl vom Projektteam als auch von den betroffenen Fachabteilungen.

Software as a Service (SaaS)

Was motiviert Unternehmen, Software nicht mehr im eigenen Haus zu betreiben, sondern als Serviceleistung zu beziehen? Im Kern gibt es drei wesentliche Anforderungen an den Betrieb von IT-Systemen:

➤ **Verfügbarkeit**

➤ **Funktionalität**

➤ **Performance**

Verfügbarkeit: Vernünftige Cloud-Services schaffen es im Mittelstand zumindest rechnerisch, eine bessere Verfügbarkeit ihrer Services gegenüber einer On-Premises-Installation zu gewährleisten. Die Systeme sind in ihrer Kernfunktion redundant ausgelegt und geplante Wartungsarbeiten bedeuten keinen Service-Ausfall.

Funktionalität: Neue Funktionalitäten lassen sich in einer Cloud-Umgebung einfacher und schneller zur Verfügung stellen als in einer On-Premises-Installation. Und das Beste: Unternehmen müssen sich nicht selbst darum kümmern. Die aktuelle Funktionalität ist sofort für den Anwender nutzbar. Ähnliches ist bei der Cloud-Strategie der SAP zu beobachten: Gewisse Funktionalitäten von Cloud-Services werden zukünftig nicht mehr On-Premises zur Verfügung gestellt.

Anwendungen und Services, die zum Beispiel Künstliche Intelligenz (KI) einsetzen, würden On-Premises die Kosten sprengen. Sehr wohl lohnt ihr Einsatz aber in Umgebungen, die eine entsprechende Rechenleistung zur Verfügung stellen müssen. Siri, Alexa, Cortana, SAP Co-Pilot oder andere Spracherkennungssysteme sind bei aller Ausbaufähigkeit Technologien, die vor allem cloudbasiert angeboten werden.

Performance: Insbesondere das Dialogverhalten von Anwendungen ist ein entscheidender Faktor für die Anwenderakzeptanz cloudbasierter Services. Trotz ständig steigender Datenraten und sinkender Latenz von Internetleitungen bleibt das in vielen Fällen eine echte Herausforderung. Nicht alle Anbieter haben ihre Services so umgestellt, dass die User-Experience entsprechend positiv ausfällt. Die andere Seite von Performance ist die Rechenleistung, die abgerufen werden kann. Hier wiederum ist ein Cloud-Anbieter im Vorteil, da im Zweifel deutlich dynamischer und umfangreicher Leistung einfach dazugeschaltet werden kann. Performance ist also kein Hinderungsgrund mehr für den Einsatz cloudbasierter Lösungen.

SaaS und mobiles Arbeiten

Der Hauptgrund für die Einführung von SaaS-Lösungen ist der Wunsch nach mobilem Arbeiten. Dies gilt für Anwendungen im Human-Resources-Bereich gleichermaßen wie für Lösungen im Customer-Relationship-Management-Umfeld.

Bei On-Premises-Anwendungen verhindern oft die bestehende IT-Infrastruktur sowie die eingesetzte Softwareversion den mobilen Zugriff. Hier gibt es dann zwei Handlungsstränge, um die mobile Anwendung zu ermöglichen: Ein Upgrade-Projekt verbunden mit Anpassungen der IT-Infrastruktur oder der Wechsel zu einem SaaS-Konzept, mit der Aussicht, beide Themen nachhaltig zu erledigen.

Natürlich spielen auch initiale und laufende Kosten eine Rolle genauso wie die Tatsache, dass sich auch ein Umstieg auf eine SaaS-Lösung nicht ohne Projektaufwand realisieren lässt. Hierbei ist jedoch zu beobachten, dass externe Beratungsaufwände niedriger ausfallen als sie das in der Vergangenheit bei On-Premises-Installationen getan haben.

Ob Unternehmen jetzt die Wahl haben und wie der Einsatz von SaaS und BPO in der Praxis aussehen kann, erfahren Sie im zweiten Teil des Artikels „On-Premises, SaaS oder Outsourcing: Haben wir eine Wahl? Oder sind wir nicht längst Getriebene?“, der in der kommenden Ausgabe der it-management am 30. Oktober 2020 erscheinen wird.

Sven Schal

UMDENKEN ERFORDERLICH

S/4HANA PROJEKTE KÖNNEN AUCH REMOTE ERFOLGREICH SEIN

Bildquelle: valantic

SAP S/4HANA-PROJEKTE KÖNNEN AUCH REMOTE ERFOLGREICH SEIN.

Thomas Latajka, Geschäftsführer, valantic ERP Services, www.valantic.com

Die Corona-Krise stellt Unternehmen weltweit vor große Herausforderungen und hat zugleich bereits die Weichen für einen schnelleren Digitalisierungsfortschritt gestellt. Auch in der Projektzusammenarbeit zwischen SAP-Anwender- und Beratungsunternehmen, etwa bei SAP S/4HANA-Implementierungen, erfordert die Krise ein Umdenken und neue Herangehensweisen. Darüber und wie SAP Gold Partner valantic Kunden durch den Prozess der Neuausrichtung mit S/4HANA führt sprach Ulrich Parthier, Herausgeber it management, mit Thomas Latajka, Geschäftsführer bei valantic ERP Services.

Ulrich Parthier: *Aus welchen Branchen stammen Ihre Kunden und mit welchen Herausforderungen haben sie derzeit zu kämpfen?*

Thomas Latajka: Innerhalb unserer SAP S/4HANA-Implementierungsprojekte kommen viele unserer Kunden beispielsweise aus der Nahrungsmittel- und Getränkeindustrie. Für sie ist es wichtig, dass auch während der Krise die komplette Lieferkette, Vertrieb und Logistik zuverlässig funktionieren, damit die Produktion reibungslos weiterlaufen kann und ihre Produkte die Verbraucher erreichen, ohne dass irgendwo größere Lieferengpässe entstehen. Zum anderen sollen laufende Digitalisierungsprojekte, wie zum Beispiel S/4HANA-Implementierungen, möglichst im Plan bleiben und sich trotz weniger Präsenz beim Kunden nicht unnötig verzögern und damit verteuern.

Weitere Themen sind unsere Kunden derzeit beispielsweise die aktuelle temporäre Mehrwertsteuersenkung durch das Corona-Konjunkturpaket der Bundesregierung, die zeitnah in den SAP-Systemen abzubilden war, die Automatisierung kritischer ERP-Prozesse, der Aufbau neuer Vertriebsstrukturen in Form von Online-Plattformen, die Digitalisierung und Neustrukturierung der Supply Chain und vieles mehr.

Ulrich Parthier: *Was hat sich für Sie als SAP-Beratungs- und Digitalisierungsunternehmen in der Corona-Zeit verändert? Gab es Auswirkungen auf die Zusammenarbeit mit Ihren Kunden?*

Thomas Latajka: Zunächst muss man natürlich sagen, dass sich Anfang dieses Jahres, als von den ersten Corona-Fällen berichtet wurde, sicher niemand hätte vorstellen können, was da wirklich mit welcher Wucht auf uns zurollt und welche Auswirkungen diese Pandemie weltweit haben würde. Der Shutdown, Kontaktbeschränkungen und der zeitweilige absolute Stillstand ganzer Industrien und die existenzielle Not vieler Kleinunternehmer sind in der jüngeren Geschichte ja bisher ohne Beispiel.

Als Digitalisierungsunternehmen gab und gibt es aber nach wie vor genügend für uns zu tun, da sich viele unserer Kunden aktuell mitten in Transformationsprojekten befinden. Wie viele andere Unternehmen mussten auch wir einige Präsenzveranstaltungen, darunter unser großer Digitalkongress visiondays, absagen. Dafür haben wir mit dem Customer Focus Day SAP eine neue Online-Plattform für den Austausch von SAP Kunden und Expert*innen geschaffen. Auch auf Seiten unserer Kunden wurden Präsenzmeetings zunächst ausgesetzt. Es entwickelte sich dann aber schnell eine neue Form der Projektzusammenarbeit auf Distanz.

Ulrich Parthier: *Was meinen Sie damit genau?*

Thomas Latajka: Wir mussten teilweise mehrtägig geplante Workshops mit Kunden adhoc virtuell stattfinden lassen. Das war nicht ganz so einfach, denn es stellte

sich schnell heraus, dass es bei weitem nicht ausreicht, Inhalte, die für Präsenzveranstaltungen gedacht sind, 1:1 in Präsentationen zu transkribieren. Man muss viele weitere Faktoren berücksichtigen. Etwa, dass bei Online-Meetings oder Videokonferenzen die digitale Aufnahmekapazität von Menschen Grenzen hat und man sie nicht zu lang ansetzen darf. Ebenso, dass man ausreichend Pausen einbauen muss und für genügend Interaktion sorgt, damit das Auditorium nicht nach kurzer Zeit „wegdämmert". Da gab es für uns als Berater viele Learnings. Aber letztendlich haben wir von einer hohen Lernkurve sehr profitiert und erfahren, dass unsere Kunden gerade in der jetzigen Zeit sehr positiv auf unsere virtuellen Konzepte für Workshops reagieren. Fehlende Workshops können Projekte von einem Tag auf den nächsten komplett stoppen und für alle Seiten immensen wirtschaftlichen Schaden verursachen. Wir haben gemeinsam mit unseren Kunden sogar komplexe SAP-Großprojekte komplett remote, in virtueller Zusammenarbeit, gestartet. Eine neue und sehr gute Erfahrung.

? **Ulrich Parthier:** *Wie schätzen Sie die Priorisierung von IT-Projekten bei SAP-Anwenderunternehmen ein? Hat sich die Lage hier verändert durch die Krise?*

Thomas Latajka: Einerseits sehen wir, dass es Branchen gibt, die SAP-Projekte gestoppt, eingefroren, Budgets massiv gekürzt oder verschoben haben. Die meisten unserer laufenden Projekte konnten wir glücklicherweise fortsetzen, wie geplant. Für unsere Kunden spielt angesichts der Krise allerdings das Thema finanzielle Absicherung eine viel wichtigere Rolle. Das heißt, die zuverlässige Kalkulierbarkeit und Planbarkeit von Projekten bekam einen höheren Stellenwert. Wir haben speziell für S/4HANA Projekte die Project Simplification für ein agiles Projektmanagement in überschaubaren Teilschritten entwickelt. Hier können Kunde und Beratungsteam den Projektfortschritt jederzeit transparent monitoren und möglichen Schwankungen frühzeitig und gezielt entgegensteuern.

? **Ulrich Parthier:** *Wie führen Sie Kunden durch den Prozess der Neuausrichtung mit SAP S/4HANA?*

Thomas Latajka: Wir setzen speziell bei S/4HANA Projekten eine von zwei alternativen agilen Projektvorgehensweisen ein, die Project Simplification oder die Continuous Discovery & Delivery. Bei der Project Simplification werden vor der Umsetzung alle Prozesse im Unternehmen genau analysiert und es werden Arbeitspakete erstellt. Vorteile der Project Simplification sind unter anderem eine exaktere Planung der Laufzeit, ein genaueres Forecasting des Projektbudgets und eine bessere Ressourcenverteilung durch die insgesamt längere Projektlaufzeit. Auch lässt sich mithilfe der Project Simplification die Komplexität eines solchen Projekts verringern. Bei der anderen Vorgehensweise, der Continuous Discovery & Delivery, werden Einzelprozesse analysiert und designt und dann dazu die entsprechenden Arbeitspakete erstellt und kontinuierlich umgesetzt. Vorteile sind hier eine potenziell höhere Akzeptanz bei Projektmitarbeitern, die kontinuierlich direkt eingebunden werden und eine kürzere Projektlaufzeit, da ansonsten getrennte Projektphasen hier parallel ablaufen. Nachteil ist allerdings ein deutlich anspruchsvolleres und komplexeres Projektcontrolling. Das Projekt wird „leitungsintensiver", wenn man so will.

? **Ulrich Parthier:** *Welche Rolle spielt das Projektteam und seine Zusammensetzung?*

Thomas Latajka: Eine sehr wichtige Rolle. Insgesamt haben wir festgestellt, dass große Digitalisierungsprojekte nicht mehr IT-getrieben sein dürfen, um erfolgreich zu sein. Im Gegenteil müssen die Fachabteilungen mit ihrem Expertenwissen der Prozesse wieder in den Vordergrund rücken. Wir arbeiten aus diesem Grund innerhalb unserer S/4HANA-Großprojekte mit einer ganz bestimmten Projektstruktur in Form einer Projektpyramide, bestehend aus Lenkungskreis, Projektleitung und Projektteam, in dem die Verantwortlichkeiten genau definiert sind. So sind kurze Wege und ein bestmöglicher Austausch gewährleistet.

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

ZUKUNFT MIT WEITSICHT

DSAG: VIRTUELLES ALTERNATIVANGEBOT

Nach der Absage des regulären DSAG-Jahreskongresses, sprach Carina Mitzschke, Redakteurin it management, mit Marco Lenck, Vorstandsvorsitzender DSAG, über eine alternative Veranstaltung und welche Erwartungen die DSAG und die Kunden an die SAP haben.

Carina Mitzschke: *Die Absage des DSAG-Jahreskongresses in Leipzig aufgrund der Covid-19-Situation kommt nicht überraschend. Sie werden die Veranstaltung nicht ähnlich digital durchführen wie die SAPPHIRE NOW. Welche Gründe sprechen dagegen und gibt es alternative Ideen?*

Marco Lenck: Der direkte Austausch vor Ort und das persönliche Netzwerken sind Werte der DSAG und machen den DSAG-Jahreskongress zu etwas Besonderem. Deshalb ist es uns wichtig, dass wir auch mit einem virtuellen Alternativangebot den bewährten Mehrwert aus authentischen Berichten der DSAG-Mitglieder, einem Austausch auf Augenhöhe und einem hohen Informationsgehalt bieten. Aktuell erarbeiten wir daher für dieselbe Kalenderwoche des ursprünglich geplanten Kongresses für 2020 ein neues Format. Wir werden unter dem Namen „DSAGLIVE – Unser Event 2020" eine Alternative anbieten. Sie wird den Leitgedanken des vorgesehenen Jahreskongress-Mottos „Zukunft mit Weitsicht! Nachhaltig gewinnt." aufgreifen. Denn: Nachhaltiges Krisenmanagement in Zeiten von Corona und vorausschauende Digitalisierung bleiben weiterhin relevante Themen für Anwenderunternehmen.

Carina Mitzschke: *Welche dringenden Fragen, Probleme in Bezug auf die aktuelle Situation werden gegenwärtig innerhalb der DSAG-Gruppe am häufigsten diskutiert?*

Marco Lenck: Die Corona-Krise hat die Bedarfe vieler Unternehmen bei der Digitalisierung aufgezeigt. Obwohl die Unternehmen rein technologisch bereits einen hohen Digitalisierungsgrad erreicht haben, wurde teilweise deutlich, wie unflexibel sie bei der Anpassung der Prozesse sind, zum Beispiel wenn es um Zahlungsverfolgung, Lieferströme oder die Anpassung der Produktion an die neuen Bedingungen geht.

Carina Mitzschke: *Nun hat Christian Klein, CEO SAP, seine Vision der kommenden Jahre auf der SAPPHIRE NOW vorgestellt: Kernthemen sind Resilienz, Profitabilität und Nachhaltigkeit. Kam dies überraschend oder haben Sie mit so einer Ausrichtung gerechnet?*

Marco Lenck: Diese Ausrichtung kam für uns nicht überraschend, da sich unter den Schlagworten Resilienz, Profitabilität und Nachhaltigkeit die Themen einordnen lassen, die wir seitens der DSAG schon mehrfach positioniert haben: Integration, Harmonisierung der Datenmodelle und Business-Objekte sowie die Schaffung digitalen Mehrwerts. Christian Klein ist auf all diese Punkte eingegangen. Das ist ein aus DSAG-Sicht gutes Zeichen, dass SAP erkannt hat, wie wichtig die Harmonisierung ist und mit Hochdruck an der Abarbeitung ihrer Roadmap arbeitet.

Aus technologischer Sicht fordert die DSAG schon seit Längerem die Harmonisierung der SAP-Lösungen hinsichtlich User-Interface/User-Experience sowie Erweiterungs- und Betriebskonzepten. Gleichzeitig hat SAP verstanden, dass die Integrationsfähigkeit von Software in einer stark vernetzten Welt ein Schlüsselfaktor für Unternehmen ist. Damit meine ich die Integration sämtlicher Produkte und Services von SAP am Markt – von Finance, entlang der Value Chain bis zu allen Facetten der Digitalisierung. Und auch die flexible Anpassung der Lieferketten durch digitale Plattformen ist etwas, wonach Unternehmen streben, und wo SAP ihnen als starker Partner zur Seite stehen kann und muss.

Carina Mitzschke: *Nach wie vor setzt SAP das Thema digitale Transformation und somit das intelligente Unternehmen besonders in den Fokus. Dazu kommen die Einbindung von mehr KI und der Ausbau der Customer Experience. Bereits im letzten Jahr haben Sie betont, dass sich die DSAG*

KUNDEN SIND DANN ERFOLGREICH UND ZUFRIEDEN, WENN SIE IHRE GESCHÄFTSPROZESSE UND -MODELLE MIT SAP-LÖSUNGEN EINFACH, UMFASSEND UND LANGLEBIG ABBILDEN KÖNNEN.

Marco Lenck, DSAG-Vorstandsvorsitzender, www.dsag.de

hier einfache und schnell einsetzbare Lösungen für mehr Innovationen seitens SAP wünscht. Erwarten Sie, dass sich hier jetzt nach der SAPPHIRE NOW etwas tut?

Marco Lenck: Wir erwarten klare, praktikable Lösungen zu den oben genannten Themen, die schnell, einfach und durchaus auch kurzfristig einsetzbar sind. Immerhin sprechen wir bald ein Jahr über Integration, Harmonisierung und digitalen Mehrwert. Jetzt erwarten wir, dass SAP liefert. Wir gehen davon aus, dass erste Lösungen auf der DSAGLIVE vorgestellt werden.

? **Carina Mitzschke:** *Klein argumentierte während seiner Keynote, dass innovative Unternehmen die Covid-19-Krise besser überstehen werden. Dennoch tut sich SAP schwer, Freiräume für Unternehmen zu schaffen, um eben jene Innovationen zuzulassen. Erwarten Sie hier eine Veränderung beziehungsweise wie sollte hier eine Unterstützung seitens SAP aussehen?*

Marco Lenck: Damit Kunden Innovationen schaffen können, brauchen sie passende Lösungen. SAP muss also bezogen auf die Anwenderunternehmen erkennen, welche Lösungen für diese wirklich wichtig sind und wie solche Lösungen gebaut werden. Und hier kommt es wieder darauf an, dass SAP ihre Hausaufgaben hinsichtlich der zuvor erläuterten Themen macht. Aus DSAG-Sicht muss SAP dazu auch weiter intern an ihrer Strategie arbeiten, um Kunden die benötigten Lösungen bereitzustellen.

Bezogen auf SAP selbst muss sich der Software-Hersteller wie jedes andere Unternehmen auch, der aktuellen Situation stellen. Aus Anwendersicht wäre wünschenswert, dass das Unternehmen sein Profil weiter schärft und schneller Proof-of-Concepts bereitstellt, damit Unternehmen und Partner schnellstmöglich ihre Entscheidungsprozesse anstoßen können, um eben genannte Innovationen zu realisieren.

? **Carina Mitzschke:** *Klein schloss seine Keynote mit der Aussage, dass SAP immer am besten ist, wenn es auf die Kunden hört. Stimmen Sie dem zu?*

Marco Lenck: Ja, dem stimme ich uneingeschränkt zu. Die Kunden sind das Kapital von SAP, der Wettbewerbsvorteil. Das hat sich in der Vergangenheit immer wieder bestätigt. Daher begrüßen wir auch, dass SAP sich mit ihren Strategien und Lösungen an den Digitalisierungsvorhaben der Kunden ausrichtet. Kunden sind dann erfolgreich und zufrieden, wenn sie ihre Geschäftsprozesse und -modelle mit SAP-Lösungen einfach, umfassend und langlebig abbilden können. Daher ist aus DSAG-Sicht klar, dass sich SAP mit dem Best-of-Suite-Ansatz dauerhaft Wettbewerbsvorteile sichern und auch nachhaltig eine starke Marktposition einnehmen kann.

! **Carina Mitzschke:** *Herr Lenck, wir danken für dieses Gespräch.*

VOM DATEN-FRIEDHOF ZUM INFORMATIONS-MANAGEMENT

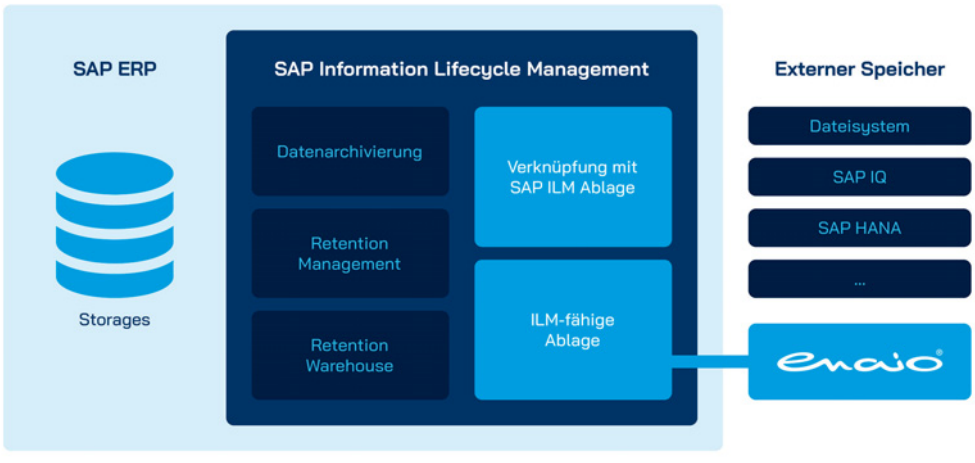
VOR SAP-MIGRATION: DATENBANKEN ENTLASTEN OHNE ARCHIVIERUNGSCHAOS

Ist das wichtig – oder kann das weg? Diese Frage stellen sich nicht nur Projektmanager, Hausjuristen und IT-Verantwortliche immer häufiger: Spätestens seit Einführung der DSGVO ist das Bewusstsein für die Notwendigkeit eines Lebenszyklus-Managements von Informationen (ILM) mit fristgerechter Löschung von Daten und Dokumenten gewachsen. Auch die Kosten für allzu mächtige Datenbanken oder eine anstehende Migration auf S/4HANA können aktuell den Druck erhöhen, eine konsequente und systematische Archivierung voranzutreiben. Diese sollte allerdings nicht auf Kosten von Transparenz, Benutzerfreundlichkeit und Informationsfluss gehen.

Mit der Datenschutzgrundverordnung kam die große Betriebsamkeit: Jedes Unternehmen, das sensible oder personenbezogene Daten verarbeitet und speichert, musste sich zunächst einen Überblick verschaffen, welche Daten zu welchem Zweck eigentlich an welchen Stellen gehortet werden. Und dann, wie lange deren Speicherung überhaupt notwendig oder zulässig ist. Denn jedes Dokument und jede Art von Datensatz unterliegt eigenen Lösch- und Aufbewahrungsfristen: Steuerlich relevante Belege etwa müssen mindestens zehn Jahre verfügbar sein, Bewerberunterlagen hingegen nach Abschluss einer Stellenausschreibung umgehend gelöscht werden. Bei einem stetig wachsenden Informationsaufkommen – die Menge der weltweit produzierten Daten verdoppelt sich im Schnitt alle zwei Jahre – ist ein rechtskonformes und professionelles Management der Speicherung ohne Software-Unterstützung schlicht illusorisch. Die teils drastischen Sanktionen bei Datenschutzverstößen wurden so zum wichtigen Treiber für einen differenzierteren Umgang mit der Datenspeicherung.

Umstieg mit leichtem Gepäck

Auch überquellende Datenbanken sind ein guter Grund, sich mit ILM und Archivierung zu beschäftigen: Je voller die Server, desto behäbiger das System und desto höher die laufenden Kosten. Steht dann noch ein Upgrade auf eine neue Software-Version oder gar der Wechsel einer Anwendung ins Haus, wächst die Bereitschaft, nicht unbedingt benötigte Informationen in ein Data Warehouse auszulagern oder zumindest fristgerecht zu löschen. Das ermöglicht mitunter eine deutlich schlankere Umsetzung mit kleinerem Budget.



So weit, so einfach. Die Praxis ist es allerdings oft nicht: Denn Unternehmenswissen liegt in der Regel in einer Vielzahl an Dateiformaten und in ganz unterschiedlichen Anwendungen vor – vom E-Mail-Programm bis zur Warenwirtschaft von SAP. Werden diese dann in verschiedene Archive verschoben und muss danach ein älterer Geschäftsvorfall oder

ÜBERQUELLENDE DATENBANKEN SIND EIN GUTER GRUND, SICH MIT ILM UND ARCHIVIERUNG ZU BESCHÄFTIGEN: JE VOLLER DIE SERVER, DESTO BEHÄBIGER DAS SYSTEM UND DESTO HÖHER DIE LAUFENDEN KOSTEN.

Dr. Olaf Holst, Chief Technology Evangelist, Optimal Systems, www.optimal-systems.de

ein Projektdetail recherchiert werden, entsteht der einmal eingesparte Aufwand nicht selten an anderer Stelle: bei der aufwändigen Suche.

Leichter finden – auch im Archiv

Hagen Mrowetz, SAP-Experte bei Optimal Systems, hat etwas gegen das mühsame Durchforsten von Archiven: Die Logik einer umfassenden und flexiblen Enterprise Content Management (ECM) Lösung, die dank einer Vielzahl an Schnittstellen als zentrale, abteilungsübergreifende Informationsplattform fungieren kann. „enaio sorgt im Grundsatz dafür, dass das Unternehmenswissen – unabhängig von Dateiformat und der Anwendung, in der es erzeugt oder bearbeitet wird – durchgängig verfügbar ist, ohne Bereichsgrenzen." Hierzu legt enaio alle Daten und Dokumente in einer digitalen Aktenstruktur ab. So finden Nutzer entsprechend ihrer Zugriffsrechte sämtliche zu einem Projekt gehörenden Informationen: Pläne, Beschreibungen, Bilder, Videos, Belege, Lieferantendaten oder E-Mails können gebündelt angezeigt und aufgerufen werden, anstatt mehrere Suchläufe in verschiedenen Anwendungen zu starten. Die gleiche Funktionalität bietet die ECM-Lösung auch nach der Archivierung.

Diese erfolgt ebenfalls denkbar einfach: Dank der Flexibilität der ECM-Lösung ist diese offen für verschiedenste Drittanwendungen, von Microsoft Office bis hin zu den gängigen ERP-Systemen. Im Fall von SAP nutzt enaio nutzt die zertifizierte Archivschnittstelle ArchiveLink, um relevante Daten in ein Archiv auszulagern und zugleich innerhalb der Aktenstruktur des ECM-Systems verfügbar zu halten. Werden in enaio archivierte Informationen zu einem späteren Zeitpunkt wieder in SAP gebraucht, stellt die ECM-Lösung diese in der gewohnten Ansicht zur Verfügung – ohne damit die Datenbank zu belasten. Außerdem kann ein SAP-Anwender aus einem Datensatz direkt in die dazugehörige enaio Vorgangsakte springen und umgekehrt. Das spart viel Zeit und erhöht die Auskunftsfähigkeit, betont Hagen Mrowetz: „SAP-Nutzer können dank enaio mit wenigen Klicks der gesamten Vorgang aufrufen, ohne durch verschiedene Menübäume navigieren oder zusätzlich andere Anwendungen starten zu müssen."

Selektives Gedächtnis

Die in SAP ILM vorgegebenen Regeln für Aufbewahrung und Löschung behalten dabei ihre volle Gültigkeit. Werden sie in enaio archiviert, sind die Informationen nicht nur dauerhaft und sicher gespeichert, sondern werden – entsprechend der in SAP ILM hinterlegten Löschfristen – auch vollständig aus allen Systemen getilgt. Auf die Umsetzung eines sogenannten Legal Hold ist ebenfalls Verlass: Informationen, deren Löschung zwar ansteht, die aber beispielsweise wegen eines schwebenden juristischen Verfahrens noch aufbewahrt werden müssen, können in SAP ILM einen entsprechenden Vermerk erhalten. Er setzt die automatische Löschung nach Fristen außer Kraft und überlässt die Entscheidung dem fachlichen Nutzer, wie lange die Daten noch verfügbar bleiben müssen. enaio sorgt in jedem Fall dafür, dass die betreffenden Informationen entsprechend dem jeweils aktuellen Stand im Lebenszyklus-Management behandelt werden. Das hält Datenbanken und Betriebskosten schlank und reduziert rechtliche Risiken in Bezug auf die Einhaltung der DSGVO.

Dr. Olaf Holst

DOKUMENTE RICHTIG ARCHIVIEREN

Der Gesetzgeber erlaubt inzwischen die Aufbewahrung der meisten Dokumente in elektronischer Form. Ein Dokumentenmanagementsystem (ECM) wie enaio übernimmt deren digitale Erfassung, strukturierte Ablage und das Lebenszyklus-Management. Dazu gehört auch die Übergabe älterer Daten an eine Archivlösung und die regelbasierte Löschung nach Ablauf der gesetzlichen Aufbewahrungsfristen.

Eine Aufbewahrungsfrist von zehn Jahren gilt für

- Buchungsbelege (Rechnungen, Kontoauszüge, Quittungen, Schecks, Lohn- und Gehaltsabrechnungen, Steuerbescheide, Lieferscheine)
- Jahresabschlüsse
- Handelsbücher
- Eröffnungsbilanzen
- Konzernabschlüsse
- Inventare
- Lageberichte

Eine sechsjährige Aufbewahrungsfrist ist für folgende Dokumente vorgesehen:

- Handels- und Geschäftsbriefe
- Korrespondenz
- Bankbürgschaften
- Zollbelege
- Betriebsprüfungsberichte
- Darlehensunterlagen

Persönliche Daten, etwa die Gästeangaben beim Corona-bedingten Check-In in ein Restaurant, müssen nach vier Wochen gelöscht sein, Bewerberunterlagen dürfen sechs Monate aufbewahrt werden. Unternehmen sind durch die DSGVO angehalten, eigene Löschungskonzepte zu entwickeln und dokumentiert umzusetzen.

BIG DATA UND ANALYTICS

KI UND ML AUF DEM VORMARSCH

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

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

Dieses eBook weist den Weg in die Zukunft von Big Data und Analytics. Deep Data Analytics, Künstliche Intelligenz, Machine Learning und Natural Language Processing heißen die Gefährten.

Highlights aus dem eBook

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

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

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

SOFTWARE QUALITY & TESTING

NEUE ARBEITSGEBIETE FÜR FEHLERFREIEN CODE

Das eBook „Software Quality & Testing" ist deutschsprachig, 52 Seiten lang und das PDF ca. 8 MB groß. Es steht unter diesem Link kostenlos zum Download bereit:
www.it-daily.net/download

Automatisiertes Testen ist heutzutage kein Hexenwerk mehr. Jedes gute Unternehmen entwickelt Software mit automatisierten Unit-Tests und Integrationstests. Es ist klar, dass neue Programmiersprachen und Verfahren die tägliche Arbeit erleichtern. Egal ob DevOps, Low-Code, das Stichwort heißt Evolution.

Highlights aus dem eBook

• Potential- & Prozessanalyse
Wenn Effizienz, Effektivität und Qualität in den Prozessen verbessert oder Methoden, Tools oder Techniken auf den neuesten Stand gebracht werden sollen, dann nur mit Hilfe einer Potenzialanalyse mit Umsetzungs-Roadmap.

• Open Source Risikoanalyse
Veralteter Code, überholte Versionen, fehlende Patches, das ist bei Open Source Normalität. Es gibt einen besorgniserregenden Rückstand bei der Nutzung der neuesten Version von Open-Source-Komponenten.

• Schlüsselwortbasiertes Testen
Wir zeigen, wie ein automatisiertes Umfeld aufgebaut werden kann, so dass manuell arbeitende Tester schon nach einer kurzen Einarbeitung automatisierte Testfälle schreiben und auch verwalten können.

DFC & dikomm

GRÖSSTE DOPPEL-VERANSTALTUNG ZUM THEMA DIGITALISIERUNG IN MITTELSTAND UND VERWALTUNG AM 05.11.2020

Anfang November findet in der Messe Essen Halle 3 wieder der Digital Futurecongress (DFC) und die dikomm – Zukunft digitale Kommune zusammen in einer Location statt. Der Parallel-Event richtet sich an mittelständische Entscheider und Geschäftsführer sowie kommunale IT-Verantwortliche, Bürgermeister und andere Datentechnologie-Interessierte.

Beide Formate bieten als umfangreiche, kombinierte Netzwerk-Veranstaltung auf einer Ebene Raum für zwei Ausstellungen mit etwa 100 spezialisierten Anbietern sowie viele entsprechende Redebeiträge, Workshops und Matchmaking-Möglichkeiten. Besucher können in einem kompakten Rahmen aktuelle Lösungen zum Thema effektive Datentransformation für KMU oder konstruktive Umsetzungsmöglichkeiten bei der digitalen Verwaltung städtischer Einrichtungen im persönlichen Dialog kennenlernen und sich bei entsprechenden Vorträgen, Key Note Speakern, Best Practice-Vorstellungen über prozessrelevante (Optimierungs-)Trends informieren.

Daneben ist es möglich, in Gesprächen mit Experten oder Kollegen eingehend und detailliert neue Impulse im digitalen Kontext zu erhalten beziehungsweise wertvolle, praktische Erfahrungswerte, Tipps oder Empfehlungen mitzunehmen oder weiterzugeben.

dikomm zukunft digitale kommune | DIGITAL FUTURECongress

Weitere Infos unter https://essen.digital-futurecongress.de und https://www.dikomm.de

ÄNDERUNG DER LIZENZBESTIMMUNGEN „FROM SA“

WELCHE SOFTWARE DARF NOCH GEBRAUCHT VERÄUSSERT WERDEN?

Im Mai 2020 verkündete Microsoft Änderungen seiner Lizenzbestimmungen für sogenannte “from SA”-Verträge. Seither sind Unternehmen verunsichert, welche ihrer käuflich erworbenen Microsoft-Lizenzen sie noch veräußern können und welche nicht. Sebastian Ruml, Lizenzstratege und Chefeinkäufer beim Gebrauchtsoftware-Händler VENDOSOFT, erklärt, was es mit den Einschränkungen auf sich hat und wen sie betreffen.

Die Glöckle Group, ein mittelständisches Unternehmen aus dem Schwäbischen, migrierte 2019 in die Cloud. In diesem Zuge veräußerte das Unternehmen etwa 250 Microsoft-Lizenzen an die VENDOSOFT GmbH. Darunter Office 2019, verschiedene Server aus SA-Verträgen sowie deren Zugriffslizenzen. Rund 100.000 Euro erwirtschaftete Glöckle mit dem Verkauf. Der Ertrag wurde zu 100 Prozent in das Cloud-Projekt reinvestiert. VENDOSOFT führte die erworbenen Lizenzen dem Zweitmarkt für Software zu.

Nach diesem Prinzip entsteht ein Kreislauf, von dem alle Beteiligten profitieren: Glöckle konnte einen Großteil seiner Migrationskosten mit den fortan nicht mehr benötigten Software-Assets decken. VENDOSOFT wiederum ermöglicht Unternehmen auf diese Weise den Erwerb neuwertiger Gebrauchtsoftware zu einem Bruchteil ihres Neupreises. Dem scheint Microsoft mit der Änderung seiner AGBs einen Riegel vorschieben zu wollen. Das ist grundsätzlich verständlich – auch wenn der Gebrauchthandel den Software-Giganten wirtschaftlich kaum tangieren dürfte. Ob die AGB-Änderungen rechtlich einwandfrei sind, wird derzeit auf verschiedenen Ebenen geprüft. Das kann und wird sich hinziehen. In der Zwischenzeit herrscht eine gewisse Verunsicherung auf Seiten der Verkäufer – also jener Unternehmen, die ihre gebrauchte Software veräußern wollen.

WIR PRÜFEN FÜR UNTERNEHMEN KOSTENLOS UND INDIVIDUELL, OB ES SICH NICHT VIELMEHR LOHNT, IHRE ALTLIZENZEN AN UNS ZU VERKAUFEN UND DIE MICROSOFT CLOUD OHNE „FROM SA“ ZU BEZIEHEN.

Sebastian Ruml,
Lizenzstratege und Chefeinkäufer,
VENDOSOFT GmbH, www.vendosoft.de

Welche Lizenzen sind von den Änderungen betroffen?

Um Firmen weiterhin die Chance zu bieten, IT-Bestände zu rekapitalisieren und zugleich ihr Software Asset Management zu verschlanken, klärt der Microsoft Gold Partner VENDOSOFT kostenlos darüber auf, welche Lizenzen und welche Vertragsformen überhaupt den neuen Bestimmungen unterliegen. Denn die Regelungen gelten nicht pauschal für alle Software-Assurance-Verträge von Microsoft.

„Bei den Lizenzen sind es alle in einem Unternehmen eingesetzten On-Premises-Produkte, die Cloud-fähig sind“, so Sebastian Ruml. Dazu zählen:

- Microsoft Office, Project und Visio
- das Betriebssystem Windows 10
- Exchange, Skype for Business und SharePoint Server (hingegen nicht: Windows Server, SQL Server, System Center Server
- die Client Access Licenses (CAL) zu oben genannten Servern

Wohlgemerkt: Alle vor Mai 2020 von einem Unternehmen erworbenen Lizenzen können und dürfen bedenkenfrei veräußert werden! Nur für Neukunden beziehungsweise mit der nächsten Vertragsanpassung tritt die Beschränkung in Kraft. „Und auch dann hat jedes Unternehmen

die Wahl, ob es sich darauf einlässt", ergänzt Sebastian Ruml. Was es damit auf sich hat, beschreibt der Absatz „Ist die Änderung in den Microsoft- Produktbestimmungen alternativlos?".

Welche Verträge sind von den Änderungen betroffen?

Kommen wir zu den Vertragsformen. Da kursierten zunächst widersprüchliche Aussagen. Bestätigt scheint, dass die Vertragsanpassungen nur für Microsoft Enterprise Agreements greifen. Damit sind MPSA, select-Verträge und auch open-value- und open-license-Verträge laut Ruml ausgenommen. „Ohnehin ausgenommen sind reine Subscription-Vereinbarungen und solche, in denen kein Produkt mehr unter SA steht."

Microsoft verwehrt damit ausgerechnet „den Großen", ihre einmal gekaufte – und damit rechtlich als Eigentum anzusehende – Software wiederzuverkaufen. Ein Unding, wenn man bedenkt, dass es in Konzernen mit 2000 Lizenzen und mehr Teil der Finanzierungsstrategie ist, ihr in IT-Assets gebundenes Kapital zu einem Zeitpunkt X wieder in aktives Budget zu wandeln.

Ist die Änderung in den Microsoft-Produktbestimmungen alternativlos?

Das führt zu der Frage, ob es Kunden einfach so hinnehmen müssen, dass das Bestehen einer aktiven (oder erneuerten) Software Assurance zu einer Lizenz im Zeitpunkt des Umstiegs auf die Cloud nicht mehr genügen soll? Nach dem Willen von Microsoft müssen diese „qualifizierenden Lizenzen" fortan während der gesamten Dauer eines Abonnements behalten werden. Das bedeutet: On-Premises-Software aus Enterprise Agreements kann nicht veräußert werden.

Unternehmen sollten jedoch wissen, dass es sich lediglich um einen vermeintlichen Kaufanreiz von Microsoft handelt, um Kunden den Wechsel auf Abo- beziehungsweise Cloud-Modelle schmackhaft zu machen. Eine Art Rabattierung, die gar nicht mal schlecht klingt, de facto aber eine Beschränkung der Kundenrechte ist. Und die nicht zwangsläufig die günstigste Alternative darstellt.

Dazu Sebastian Ruml: „Wir prüfen für Unternehmen kostenlos und individuell, ob es sich nicht vielmehr lohnt, ihre Altlizenzen an uns zu verkaufen und die Microsoft Cloud ohne „From SA" zu beziehen." In 8 von 10 Fällen, die VENDOSOFT derzeit vorliegen, ist dieses Vorgehen für das jeweilige Unternehmen wirtschaftlich sinnvoller.

Große Verkaufswelle erwartet

Wie eingangs erwähnt, betrifft die Änderung der Produktbestimmungen neue SA-Verträge beziehungsweise wird sie bei bestehenden Lizenzen mit der nächsten Vertragsanpassung wirksam. Einkäufer Sebastian Ruml spürt bereits die Auswirkungen. „Wir erhalten derzeit so viele Ankaufsanfragen wie noch nie!" Denn viele IT-Chefs und CFOs empfinden die neueste Microsoft-Aktion als unterschwelligen Angriff auf das geltende Recht an ihrem Eigentum – und informieren sich, wie sie dem begegnen können. Ein Verkauf der vorhandenen Software aus SA-Verträgen zum jetzigen Zeitpunkt ist eine ebenso kluge wie lukrative Möglichkeit. VENDOSOFT unterstützt dabei im gesamten Prozess – von der Prüfung der zu veräußernden Lizenzen bis hin zur Deinstallation und Rechteübertagung unter Einhaltung des geltenden Rechts.

Angelika Mühleck

Wer wie die schwäbische Glöckle Group einen Großteil seiner Cloud-Kosten durch den Verkauf gebrauchter Microsoft-Lizenzen refinanzieren will, findet hier Auskunft – und eine CaseStudy zum Thema:

www.vendosoft.de/gebrauchte-software-verkaufen/

KI IM STAMMDATENMANAGEMENT

VIELE ANWENDUNGSFELDER, GUTE DATEN UNERLÄSSLICH

KÜNSTLICHE INTELLIGENZ HAT AUCH IM STAMMDATEN-MANAGEMENT EINZUG GEHALTEN. IHR WEITERER ERFOLG WIRD DAVON ABHÄNGEN, OB ES GELINGT, DIE DATENQUALITÄT ZU SICHERN UND DIFFERENZIERTE, AUSSAGEKRÄFTIGE DATEN ZU GENERIEREN.

Monika Pürsing, Geschäftsführerin, zetVisions GmbH, www.zetVisions.de

Für die Suche nach „artificial intelligence" liefert die Suchmaschine Google - selbst ein Paradebeispiel für die Anwendung künstlicher Intelligenz - über 150 Millionen Ergebnisse in 0,56 Sekunden. Für „machine learning", ein Teilgebiet der künstlichen Intelligenz (KI), liefert der Algorithmus 116 Millionen Ergebnisse. Beeindruckende Zahlen, die zeigen, wie sehr künstliche Intelligenz und maschinelles Lernen diskutiert wurden und werden. Für KI gibt es eine ganze Reihe von Anwendungsgebieten, wie etwa Expertensysteme (Beispiel Watson), Gesichts- und Spracherkennung, Predictive Analytics und Robotik. KI lässt sich natürlich auch für das Management von Stammdaten wirkungsvoll einsetzen.

Stammdaten sind die Voraussetzung, um Daten überhaupt nutzen zu können. Ohne Stammdaten fehlt es an Definitionen und Kontext, ohne Stammdaten fehlt die Möglichkeit, Daten zu verstehen, verknüpfen zu können, zu interpretieren und richtig zu verwenden. Der Haken ist – wie so oft – die Qualität der Daten. Man kann das auf eine ganz einfache Formel bringen: Gute Daten verbessern die künstliche Intelligenz. Das Gegenteil trifft leider auch zu. „Schlechte Datenqualität ist Feind Nummer eins für den weit verbreiteten, profitablen Einsatz des maschinellen Lernens", schrieb Thomas C. Redman, der „Data-Doc", vor zwei Jahren im Harvard Business Review. Während die bissige Beobachtung ‚garbage-in, garbage-out' die Analytik und Entscheidungsfindung seit Generationen geplagt habe, enthalte sie für das maschinelle Lernen eine besondere Warnung. Die Qualitätsanforderungen an das maschinelle Lernen seien hoch, und schlechte Daten könnten ihm zweimal den Kopf verdrehen – erstens die historischen Daten, die zum Training des Vorhersagemodells verwendet werden, und zweitens die neuen Daten, die von diesem Modell für zukünftige Entscheidungen verwendet werden.

Daten als immaterieller Unternehmenswert

Es ist das alte Lied von der Datenqualität. „The Machine Learning Race Is Really a Data Race", lautete Ende 2018 die Überschrift eines Beitrags im Sloan Management Review. Daten werden zu einem Unterscheidungsmerkmal, weil viele Unternehmen nicht über die benötigten Daten verfügen. Die wertvollen, nützlichen Daten, die sie in die Lage versetzen, beispielsweise im Finanzbereich nicht nur materielle Vermögenswerte, sondern vor allem immaterielle Vermögenswerte zu messen. Dass Daten zu diesen immateriellen Unternehmenswerten gehören, diese Sichtweise ist noch nicht sehr weit verbreitet. Christine Legner und Martin Fadler vom Competence Center Corporate Data Quality in St. Gallen bemängeln: „Trotz der zunehmenden Relevanz von Daten im Kontext der Digitalisierung wird bisher in nur wenigen Unternehmen dem Management der Daten die gleiche Aufmerksamkeit zuteil, wie anderen Unternehmenswerten." In ihrer Studie „Managing Data as an Asset with the Help of Artificial Intelligence" (2019) kommen Legner und Fadler zu der Einsicht, in traditionellen Unternehmen seien Daten eine wichtige, aber vor allem unterstützende Ressource in Geschäfts- und Entscheidungsprozessen; in einer zunehmend digitalisierten Welt würden sie zu einem Wert an sich, weil sie die unabdingbare Voraussetzung für digitale Geschäftsmodelle und Strategien seien.

Die gute Nachricht sei, so Legner und Fadler, dass durch substanzielle Fortschritte künstliche Intelligenz und maschinelles Lernen – was das Lernen aus Daten und die Automatisierung sich wiederholender Aufgaben betreffe – Unternehmen bei ihren Datenmanagement-Aktivitäten unterstützen könnten. Ihre Studie zeige, dass maschinelles Lernen in allen Phasen des Datenlebenszyklus angewendet werden könne, um Folgendes zu erreichen:

- Datenbestände auf effiziente, benutzerfreundliche Weise zu erstellen und anzureichern;
- Aufrechterhaltung qualitativ hochwertiger Daten durch Unterstützung aktiver und reaktiver Datenpflege sowie zur Datenvereinheitlichung;

- Management des Datenlebenszyklus, insbesondere bei sensiblen Daten und bei der Ausmusterung von Daten;

- Steigerung der Nutzung von Daten durch Verbesserung der Datenentdeckung durch Nutzer, insbesondere durch Data Scientists.

Datenlebenszyklusphasen

Für jede dieser Datenlebenszyklusphasen haben Legner und Fadler Anwendungsszenarien für maschinelles Lernen identifiziert.

Die Phase der Datenerstellung und -erfassung komme es zu Schreibfehlern, falschen oder ungültigen Dateneinträgen, leeren Feldern und manuellem Aufwand. Hier unterstütze maschinelles Lernen die Datenerstellung, zum Beispiel durch automatisches Ausfüllen von Werten in Formularen und automatisches Extrahieren von Daten, sowie die Datenanreicherung.

Die Problemfelder in der Phase der Datenvereinheitlichung und -pflege lägen etwa in der Datenintegration über mehrere Systeme hinweg (was zu Inkonsistenzen führe), in der Korrektur von Datenfehlern und in der Definition von Geschäftsregeln. Maschinelles Lernen unterstütze zum einen die Datenpflege aktiv durch Geschäftsregeln und reaktiv durch Datenkorrektur, zum anderen die Datenvereinheitlichung durch Abgleich und Eliminierung von Datendubletten.

In der dritten Phase stehen der Datenschutz und die Ausmusterung von Daten im Zentrum. Als problematisch erweise sich dabei die mangelnde Transparenz, wo Informationen gespeichert werden, die sich auf eine identifizierbare Person beziehen (personally identifiable information, PII), und damit verbunden die Einhaltung von Datenschutzbestimmungen. Künstliche Intelligenz und maschinelles Lernen unterstützten den Datenschutz – beispielweise durch die Identifizierung sensibler Daten und die Aufdeckung betrügerischen Verhaltens – und das „Data Retirement", wenn Daten ihr „Lebensende" erreicht haben.

Die Phase der Datenentdeckung und -nutzung sei gekennzeichnet durch Probleme beim Auffinden und bei der Bereinigung relevanter Daten sowie bei der Identifizierung von Datenbeziehungen. Hier könnten künstliche Intelligenz und maschinelles Lernen die Datenermittlung beispielsweise durch Empfehlungen und die Verknüpfung von Datensätzen unterstützen.

Fazit

Legner und Fadler kommen unter dem Strich zu dem Fazit, maschinelles Lernen habe das Potenzial, die Datenmanagementpraktiken erheblich zu verbessern und die Datenqualität zu steigern. Ein gutes Beispiel dafür liefere Bosch. Dort sei es gelungen, den aufwändigen Prozess der manuellen Zuweisung von Zolltarifnummern zu einem Produkt – im Außenhandel muss jedes Unternehmen seine Produkte als Voraussetzung für Export-/Importprozesse entsprechend klassifizieren – durch eine Lösung zu ersetzen, die mit Hilfe überwachter Machine Learning-Algorithmen eine automatisierte Zuweisung von Warencodes mit hoher Genauigkeit (90 Prozent) ermöglicht.

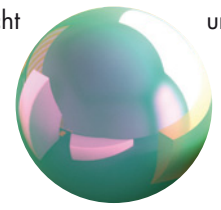
Monika Pürsing

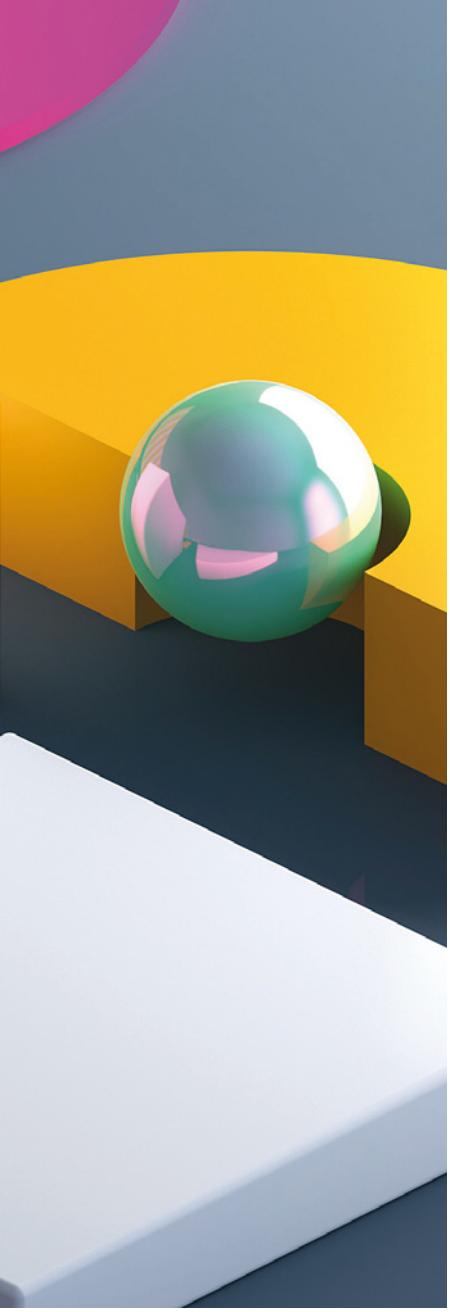
AUTOMATION IN DER FINANZABTEILUNG

GRUNDLAGE, UM BESONDERE ZEITEN UND AUDITS ERFOLGREICH ZU MEISTERN

Kaum war das erste Quartal 2020 zu Ende, sahen sich nahezu alle Unternehmen und insbesondere CFOs einer bisher noch nie dagewesenen Herausforderung gegenüber: Plötzlich und völlig unerwartet mussten sowohl die laufende Buchhaltung als auch die Abschlüsse remote erledigt werden. Das gesamte Finanzteam inklusive aller, die aus den Abteilungen Daten und Informationen an die Finanzabteilung übergeben mussten, befanden sich im Home-Office. COVID-19 hatte zugeschlagen. Ein Großteil der lokalen und weltweiten Wirtschaft musste sich sehr schnell bewegen, um auf anderen Wegen zumindest einen Teil des Geschäftsbetriebs aufrecht zu erhalten. Allen voran die Buchhaltung, da diese trotz des Virus an die Termine ihrer Abschlüsse gebunden war. Dank der flexiblen IT konnten viele Unternehmen entscheidende Aufgaben ins Home-Office verlagern. Dies gelang insbesondere dann, wenn die Systeme flexibel genug und die Prozesse im Unternehmen weitgehend digitalisiert waren. Unternehmen, die bisher maßgeblich auf manuelle Prozesse gesetzt hatten, traf COVID-19 ungleich schwerer, denn diese ließen sich nicht so einfach ins Home-Office transferieren. Gut für diejenigen, die in der Buchhaltung bereits seit längerer Zeit auf die digitale Automatisierung setzen.

Doch für die Finanzabteilungen bestand die Herausforderung nicht nur darin, das Tagesgeschäft fristgerecht zu erledigen. Mit dem weitgehenden Stillstand der Wirtschaft galt es auch, Prognosen und Zukunftsszenarien zu entwickeln, die im Wesentlichen auf den veränderten Marktbedingungen und den antizipierten Entwicklungen und Zahlen beruhen. Dafür ist in traditionell organisierten Finanzabteilungen mit vielen manuellen Buchungen und Abgleichen immer auch der persönliche Austausch mit anderen Mitarbeitern nötig. Ist dieser Austausch jedoch eingeschränkt, wie jüngst während der pandemiebedingten Heimarbeit, verlangsamen sich die Abschlussprozesse dramatisch. Zudem ist das Risiko ungleich höher da, nicht alle Daten umgehend zur Verfügung stehen und über nicht gesicherte elektronische Kommunikationswege sogar in falsche Hände geraten können – beispielsweise die für manuelle Prozesse benötigten





Excel-Tabellen mit Daten, die nicht automatisiert im System verbucht und abgeglichen sind. Hinzu kommen unsichere Datenübertragungswege oder Kollaborationsplattformen, die nicht den Compliance-Standards entsprechen. Doch der kritischste Punkt ist eine stark verzögerte und potenziell ungenaue Buchhaltung – von zuverlässigen Prognosen ganz zu schweigen.

Automation hilft nicht nur jetzt

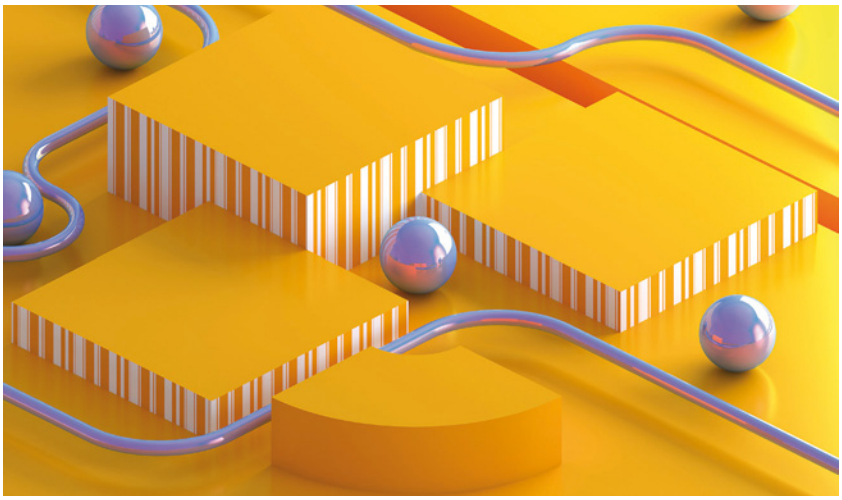
Die Automation auch in der Finanzabteilung hilft generell, Buchungen und Kontenabgleiche wesentlich schneller, transparent, zuverlässiger und sicherer zu gestalten, da manuelle Prozesse weitgehend entfallen. Für Unternehmen, die bereits vor der Pandemie in moderne Softwarelösungen für die Buchhaltung investiert haben, zahlen sich diese nun deutlich aus. Beim automatisierten oder auch virtuellen Monatsabschluss geht es darum, die für den Finanzabschluss relevanten Informationen aus den unterschiedlichen ERP-Systemen in einen automatisierten Abschlussprozess zu übergeben. Das übergeordnete Ziel ist es, möglichst alle manuellen Arbeiten zu eliminieren. Die Vorteile liegen klar auf der Hand: Durch die Automatisierung der Prozesse werden Fehler drastisch reduziert und es wird viel Zeit gespart. Akkurate Finanzergebnisse bieten dem Unternehmen zudem eine valide Grundlage für geschäftliche Entscheidungen, insbesondere in der Krisenzeit. Der Abruf der Informationen erfolgt automatisiert und digital. Außerdem ist es hilfreich, wenn der virtuelle Monatsabschluss im Idealfall Cloud-basiert ist. Die Cloud schafft die Möglichkeit ortsunabhängig und damit auch in Home-Offices zu arbeiten.

Sicherheit für Audits

Für Unternehmen, insbesondere für solche, die ihre Ergebnisse nicht nur vor der Bafin, sondern auch an der Börse präsentieren müssen, sind akkurate Zahlen das A und O. Nachträgliche Korrekturen kommen weder bei den Behörden noch bei Anlegern gut an. Und auch institutionelle Anleger schrecken vor Investitionen in Unternehmen mit einer zweifelhaften Berichtshistorie eher zurück. Es gilt also korrekte Ergebnisse zu den gegebenen Deadlines abzuliefern. Doch dies scheint nicht immer einfach zu sein. Eine Studie aus dem Jahr 2019 bestätigt diese Vermutung: Während 71 Prozent der Befragten aus dem C-Level angaben, der Genauigkeit ihrer Finanzdaten vollends zu vertrauen, waren davon nur 38 Prozent der Finanzexperten überzeugt. Die Studie legt den Schluss nahe, dass CEOs ihre geschäftlichen Entscheidungen auf Basis von Zahlen treffen, denen sie vertrauen, wohingegen die Personen, die diese Statements und Reportings vorbereiten, diesen nicht vertrauen. Das ist keine gute Basis, denn dies indiziert ein unnötig hohes Risiko für viele Unternehmen und birgt gravierenden Auswirkungen bei penibel durchgeführten Audits.

Alternativ ist ein automatisierter Abschluss die beste Voraussetzung für eine einfache, schnelle und gründliche Überprüfung der Finanzen. Prüfer erhalten vollständige Transparenz über den Dokumentenfluss. Alle nötigen Einblicke in die Bücher sind vorhanden und transparent nachvollziehbar. Da viele Auditoren darüber hinaus auf Remote-Audits umstellen, werden Unternehmen mit automatisierten Abschlussprozessen die Prüfung schneller, effizienter und vor allem ohne Probleme abschließen – zum Wohl des Unternehmens, der Prüfer und Behörden sowie der Investoren.

Robert Kathmann
www.blackline.com/de



ERFOLGREICHES PROJEKT

MIT DEN RICHTIGEN TOOLS ZUM ZIEL

Projektmanagement soll die Arbeit erleichtern, den täglichen Stress reduzieren und alle, die zusammen im Projekt arbeiten, erfolgreicher machen. Doch um dieses Ideal in der Praxis umzusetzen, muss die Unterstützung durch die Tools stimmen.

In vielen Unternehmen gilt das Thema Projekte als rotes Tuch: Zeit, Geld und Energie werden verschwendet und am Ende sind die Resultate oft äußerst dürftig. Vermeiden lässt sich das in den meisten Fällen durch klare Zielvorgaben, methodisches Projektmanagement und die richtige Software, die bei der Planung, Umsetzung und Kontrolle hilft.

> MIT DEN RICHTIGEN PROJEKTMANAGEMENT-TOOLS SIND FÜHRUNGSEBENE, PROJEKTLEITUNG, TEAMS UND MITARBEITER JEDERZEIT AUF EINER GEMEINSAMEN UND TRANSPARENTEN INFORMATIONSEBENE.
>
> Andrea Wörrlein, Verwaltungsrätin bei der VNC AG (Schweiz), Geschäftsführerin bei der VNC GmbH (Deutschland), https://vnclagoon.com

Die Funktionalität von Projektmanagement-Tools geht mittlerweile über reine Projektplanungsfunktionen weit hinaus. Die Profilierung und Differenzierung geschieht über Funktionen wie integriertes Aufgaben- und Ticketmanagement, Terminplanung, Fortschrittsüberwachung, Zeitverfolgung, Gantt-Charts oder Wikis. Und der Zugang zu den Projektmanagement-Tools kann oft wahlfrei über Apps oder über einen beliebigen Browser erfolgen.

Time is money – time is quality

Ein wichtiger Punkt, auf den Gesundheitsinstitute verstärkt hinweisen, ist die hohe Stressbelastung vieler Beschäftigter. So rät etwa das Institut für Betriebliche Gesundheitsberatung (IFBG) zur Einführung und Nutzung von Workload- oder Auslastungsbarometern, um stressbedingten Symptomen wie beispielsweise Konzentrationsproblemen vorzubeugen. Ein solches Barometer ist idealerweise Teil des Projektmanagement-Stacks. Voraussetzung dafür ist die durchgängige Transparenz durch Timesheets, die auch die Informationen für Reporting und Controlling liefern. Je granularer sie erfasst werden, desto feiner können die Beiträge und Aufwände der Mitarbeiter zum Projekt und etwaige Überlastungen erkannt werden.

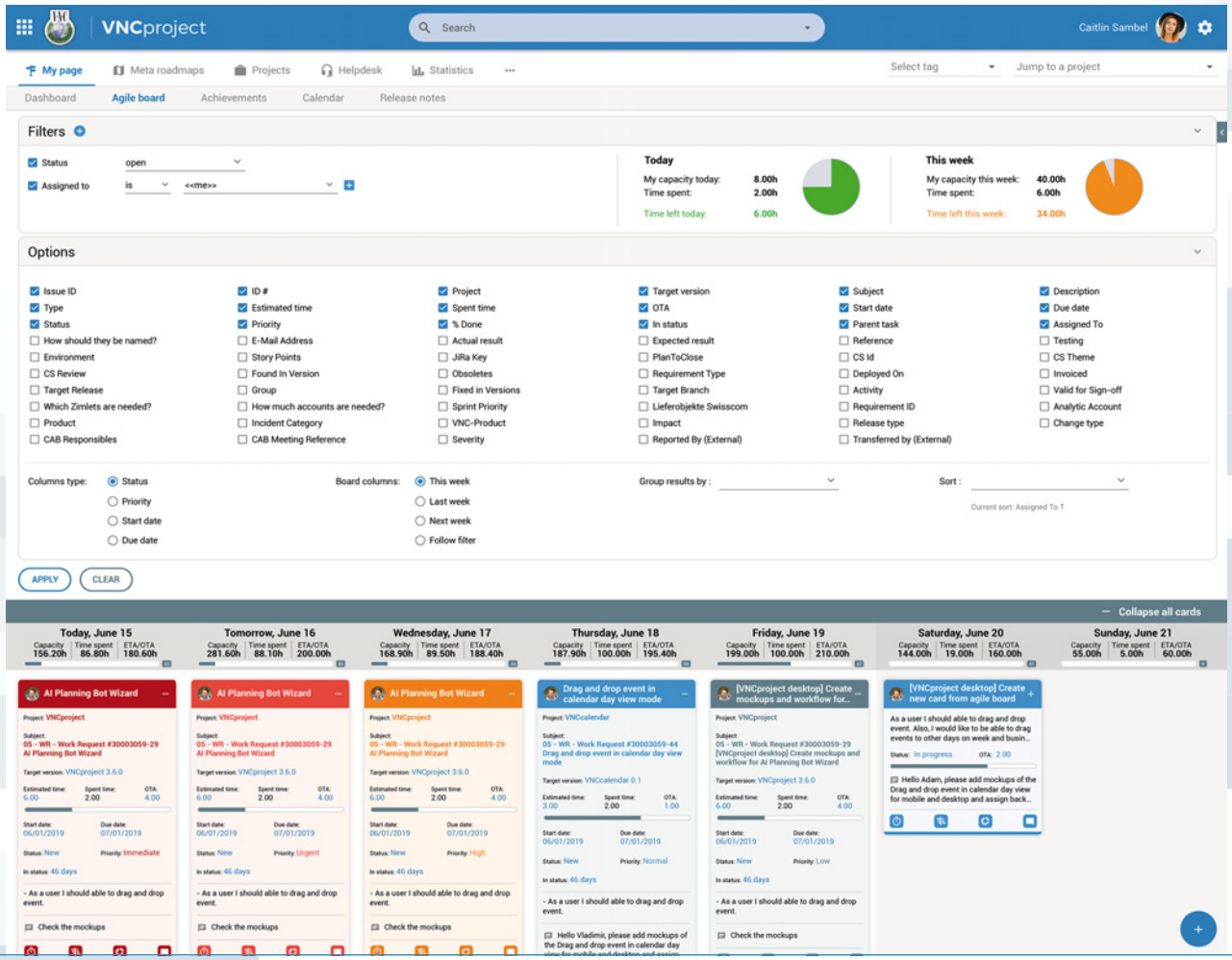
Die Akzeptanz für diese „digitalen Stechuhren" ist allerdings häufig sehr gering. Grund dafür ist aber meist nicht generelle Ablehnung, sondern die unnötig komplizierte und damit zeitintensive Bedienung. Gute Tools benötigen dafür nur zwei Klicks. Im Kontext des Projektmanagements ermöglichen Timesheets die Erfassung des individuellen Projektinputs durch Teams und einzelne Mitarbeiter – und dienen damit auch der gerechten Beurteilung der individuellen Arbeitsleistung. Ein Punkt, den Mitarbeiter normalerweise sehr schätzen. Ein gutes Timesheet geht dabei über die reine Zeiterfassung weit hinaus und erfasst auch die Arbeitsleistung von Teams und Mitarbeitern in Relation zu Aufgaben, Tickets, Projekten oder Produktversionen.

Meta Roadmap Planning (MRP)

Noch einen Schritt weiter geht das Meta Roadmap Planning (MRP). Es kommt, ähnlich wie die agile Entwicklungsmethode Scrum, ursprünglich aus der Software-Entwicklung. Dort werden in einer Roadmap sämtliche Ziele und Entwicklungsschritte, wie etwa Prioritäten, Zeithorizonte, Team-Mitarbeiter und Verantwortlichkeiten, festgehalten und ständig aktualisiert. Dabei sind Meta-Tasks als Entwicklungseinheiten definiert, denen die entsprechenden Tickets zugeordnet werden. Dadurch ist es möglich, wie aus der Vogelperspektive einen Metablick auf den aktuellen Stand des Projekts zu bekommen. Ein Drill-down zeigt alle zugeordneten Tickets und deren Status. So kann man beispielsweise einen der kritischsten Projektaspekte im Griff behalten: die Zeit – diesmal nicht bezogen auf einzelne Mitarbeiter, sondern auf das Projekt und dessen Teilaufgaben insgesamt. Ein Projektmanager kann so jederzeit Richtmarken wie die geplante Zeit (Time planned, ETA) oder die verbleibenden Zeit (Time left to finish, OTA) für ein bestimmtes Ticket oder einen Meta-Task kontrollieren.

MRP versorgt so sowohl die Führungskräfte und Projektmanager als auch jeden einzelnen Projektmitarbeiter mit detaillierten Informationen über den Projektverlauf und eventuelle kritische Abweichungen vom geplanten Weg, wie etwa Zeitüberschreitungen, wiederkehrende Fehler oder geänderte Anforderungen. Roadmaps, Prio-

MANAGEMENT



Das Ticketsystem gestattet jederzeitigen Einblick in den Projektverlauf. (Quelle: VNC)

ritäten, Deadlines, Tickets und Budgets sind jederzeit transparent und können mit den Zielvorgaben abgeglichen werden. So haben alle mit dem Projekt befassten Mitarbeiter jederzeit Zugriff auf alle projektrelevanten Informationen, können in jeder Projektphase den Soll- mit dem Ist-Zustand abgleichen und gegebenenfalls rasch auf Abweichungen reagieren.

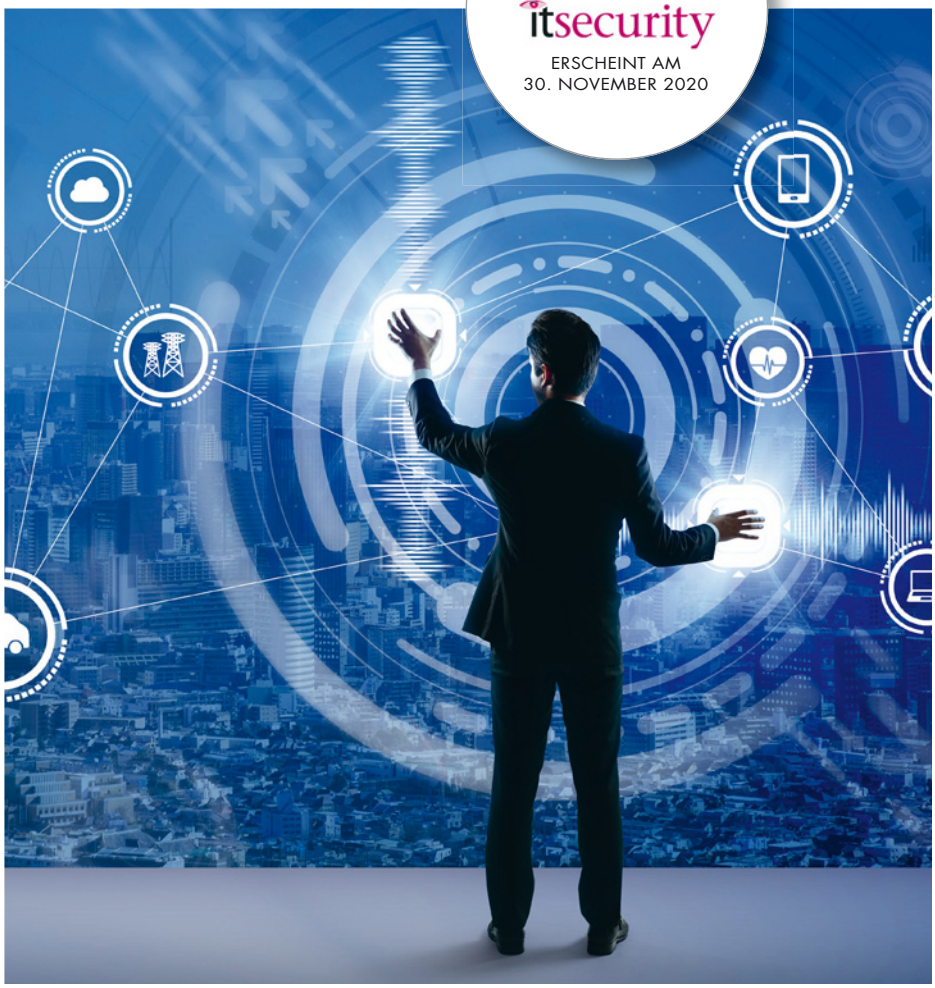
Agile Projektsteuerung

Um nach all diesen für den erfolgreichen Projektverlauf so wichtigen Informationen nicht lange suchen zu müssen, ist die übersichtliche Darstellung ein wichtiges Qualitätskriterium eines Projektmanagement-Tools. Agile Boards ermöglichen diese Echtzeittransparenz und vereinfachen gleichzeitig das Management der verschiedenen Workloads. Dazu zählen etwa die übersichtliche Darstellung aller für einen Tag geplanten Tasks für jeden Mitarbeiter, deren Relevanz und die dafür angesetzte Zeit. Sämtliche Tickets, Tasks und Zeitschienen sind im Board editierbar. So können beispielsweise aufgrund dieser Transparenz sichtbar und notwendig gewordene Veränderungen direkt dort vorgenommen werden, etwa die Zuweisung von Tickets zu bestimmten Tasks oder die Priorisierung von Meta-Tasks.

Mit den richtigen Projektmanagement-Tools sind Führungsebene, Projektleitung, Teams und Mitarbeiter jederzeit auf einer gemeinsamen und transparenten Informationsebene. Alle Aspekte des Projekts sind für jedermann sichtbar, nachvollziehbar und bei Bedarf veränderbar. Diese Software-Unterstützung ist die Basis für einen erfolgreichen Projektverlauf und -abschluss. Die Erfahrungen aus der Software-Entwicklung haben aus Projektmanagement-Tools mächtige Steuerungsinstrumente gemacht. Ihr Einsatz erhöht die Chance, Projekte erfolgreich an das gewünschte Ziel zu bringen.

Andrea Wörrlein

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
30. NOVEMBER 2020



DIGITALER WANDEL

Optimistisch in die Zukunft

ZUKUNFT RPA?

Schluss mit den Mythen

CLOUD COMPUTING

Automatisierter Datenaustausch

DIE AUSGABE 11/2020 VON IT MANAGEMENT ERSCHEINT AM 30. OKTOBER 2020.

INSERENTENVERZEICHNIS

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Dr. Olaf Holst, Robert Kathmann, Carina Mitzschke, Angelika Mühleck, Silvia Parthier, Ulrich Parthier, Monika Pürsing, Sven Schal, Andrea Wörrlein

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 27.
Preisliste gültig ab 1. Oktober 2019.

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

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

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

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

Erscheinungsweise:
10x pro Jahr

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

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

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

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

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

q.beyond
expect the next

Digitalisierung beyond konventionell

Aus QSC wird q.beyond: Wir denken Digitalisierung neu. Mit pragmatischen Komplettlösungen aus clever vernetzten Bausteinen rund um die Themen Cloud, SAP und IoT. Innovativ, branchenspezifisch, passgenau. Von Mittelstand zu Mittelstand. **Expect the next!**

qbeyond.de

itsecurity
OKTOBER 2020

DAS SPEZIAL

RECHENZENTREN UND MANAGED SERVICES

EINE ERFOLGSGESCHICHTE

Ingo Kraupa, noris network AG

SICHERHEITSRISIKEN

Cloud-Native
Architekturen

DATENSCHUTZ

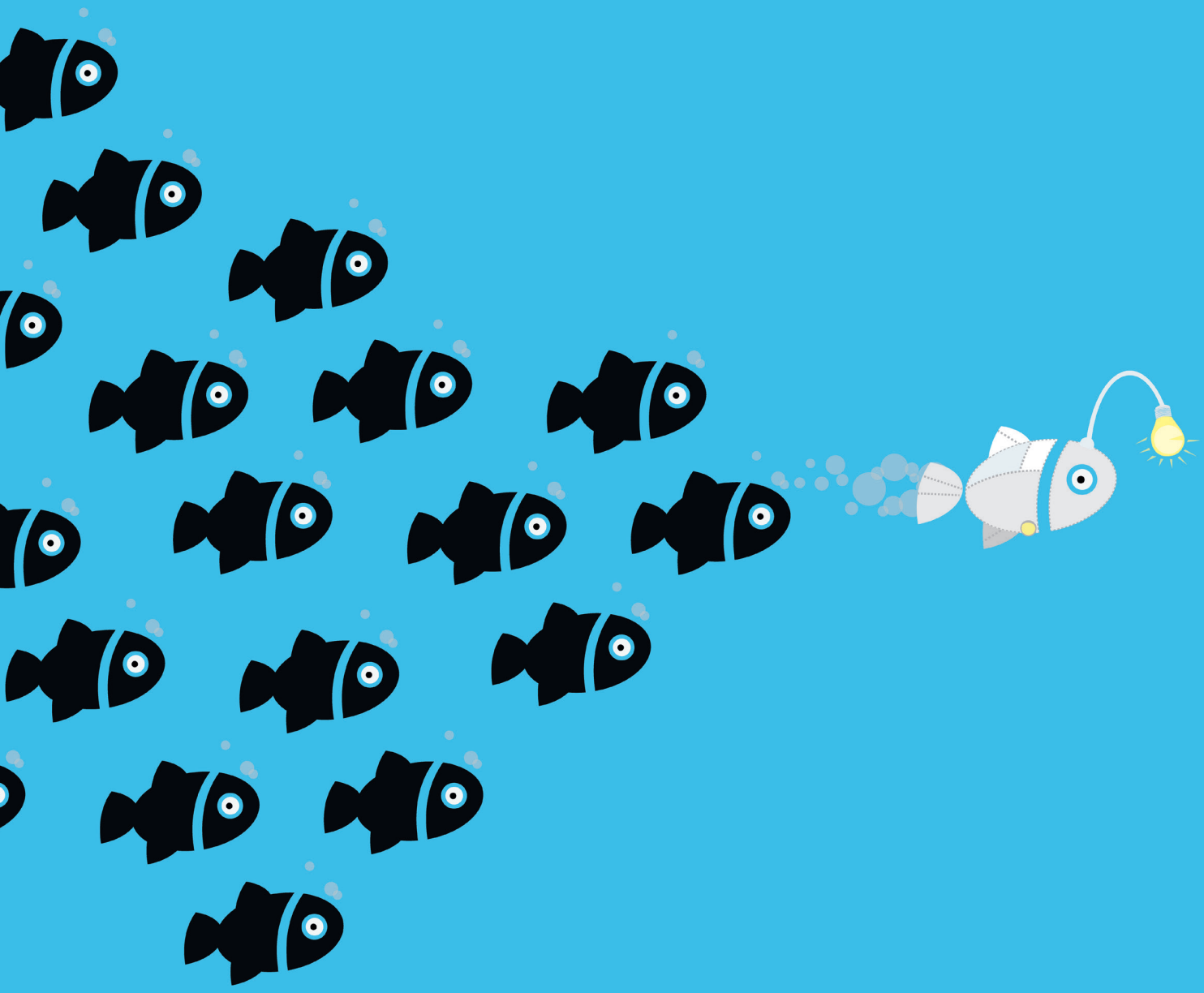
Beziehungsstatus:
kompliziert?

INSELLÖSUNGEN

Security
ganzheitlich denken

www.it-daily.net

Thought Leadership



KÜNSTLICHE INTELLIGENZ
THOUGHT LEADERSHIP

26

INHALT

4

COVERSTORY

COVERSTORY

IT SECURITY

RECHENZENTREN UND MANAGED SERVICES

NORIS NETWORK – EINE ERFOLGSGESCHICHTE

> MIT DEM NEUBAU IN NÜRNBERG SIND WIR IN DAS TOP-SEGMENT AUFGESTIEGEN.
>
> Ingo Kraupa. Vorstandsmitglied, noris network AG, www.noris.de

In wenigen Jahren zu einem der technologisch führenden Anbieter von Rechenzentren und Managed Services in Deutschland – die noris network AG ist eine Erfolgsgeschichte. Aber wie wollen sich die Nürnberger in Zeiten von Pandemie, Cloud-Trends und wachsendem Wettbewerbsdruck der großen Anbieter mittelfristig behaupten? Ulrich Parthier, Herausgeber it security, sprach mit Ingo Kraupa, Vorstandsmitglied der noris network AG.

Ulrich Parthier: *Herr Kraupa, die Entwicklung ihres Unternehmens ist beeindruckend. Dennoch: Drohen nicht auch bei den IT-Dienstleistern die mittelgroßen zwischen den kleinen/billigen und großen/internationalen zerrieben zu werden?*

Ingo Kraupa: Gerade in den letzten Jahren haben wir durch kluge Entscheidungen und eine klare Strategie große Erfolge erzielt. Wir haben heute eine gute Größe, bei der wir zeitgleich viele spannende Projekte stemmen, dabei aber noch nahe am Kunden und an der Technik sein können. Unser Geschäftsmodell funktioniert in der jetzigen Form wirklich sehr gut.

Ulrich Parthier: *Sie haben in kurzer Frist neue Rechenzentren in Nürnberg, München und Hof eingerichtet. In Nürnberg und München werden aktuell weitere modernste IT-Flächen aufgebaut. Ist die Nachfrage so hoch – auch nach der Pandemie?*

Ingo Kraupa: Bedarf und Nachfrage für RZ-Flächen sind in Deutschland ungebrochen stark. Wir planen, weitere Rechenzentren zu bauen und zu betreiben. Wir brauchen diese Ressourcen, um handlungsfähig zu bleiben. Gleichzeitig lösen wir mit den Anbauten das Leistungsversprechen an Kunden ein, die am Standort expandieren wollen. Den Bau modernster Rechenzentren beherrschen wir sehr gut. Wir haben jüngst vor Equinix und Interxion den Service Provider Award für den besten Rechenzentrumsanbieter XXL Deutschlands gewonnen.

Ulrich Parthier: *Macht ein RZ in der Nähe von Frankfurt nicht auch Sinn für Sie?*

Ingo Kraupa: Wir sind Anbieter von Premium-Rechenzentren. Mit der Fertigstellung unseres zweiten Bauabschnittes in Nürnberg sind wir in das Topsegment vorgestoßen und betreiben ein nach TÜV TSI Level 4 zertifiziertes Colocation-Rechenzentrum – meines Wissens einzigartig in Deutschland. Parallel haben wir den Standort in München um 5 000 m² erweitert. Die Standorte sind mit Ultra-Low-Latency-Technologie mehrfach redundant vernetzt und ermöglichen moder-

ne Dual-Site-Konzepte. Kunden aus der Finanzbranche genießen damit eine Verfügbarkeit, die sie aktuell in Frankfurt nicht adäquat erreichen könnten.

Ulrich Parthier: *Wie bewerten Sie die Corona-Krise? Zählen Sie sich zu den Gewinnern?*

Ingo Kraupa: Bei dieser Krise von Gewinnern zu sprechen, ist für mich nicht adäquat. Wir konnten aber die Verluste durch erforderliche Einsparungen unserer Kunden mit Neugeschäften ausgleichen. Resilienz ist in der Pandemie für Unternehmen zu einem wichtigen Entscheidungsfaktor bei der Auswahl von IT-Partnern und bei Investitionsentscheidungen geworden. Zudem erwarten wir in Deutschland einen Digitalisierungsschub. Beides wird uns mittelfristig entgegenkommen. Generell ist unser Business eher stabil und weniger stark Schwankungen unterworfen. Insofern können wir das volle Ausmaß der Krise wohl erst in ein bis zwei Jahren beurteilen.

Ulrich Parthier: *Welche Märkte sind besonders attraktiv für Sie?*

Ingo Kraupa: Wir adressieren Kunden, denen Sicherheit, Verfügbarkeit und Zertifizierungen wichtig sind. Da finden wir Bedarf in sehr vielen Branchen. Zielgruppengerechte Lösungen haben wir für den Finanzsektor, den öffentlichen Bereich, Automotive und Software.

Ulrich Parthier: *Bieten Sie Services, die andere nicht bieten?*

Ingo Kraupa: Mir fällt kein einzelner Service ein, den wir exklusiv anbieten. Wenn ein Kunde aber eine Vielzahl von Services benötigt, die alle miteinander harmonieren und zertifiziert sein sollen, dann schrumpft die Zahl der Anbieter, die diese Themen glaubhaft vereinen, massiv. Ausschlaggebend ist oft, dass wir diesen berühmten einen wichtigen Schritt mehr für die Kunden gehen, den vor allem große Wettbewerber nicht gehen wollen.

Ulrich Parthier: *Die Verteilung Ihrer RZ-Kapazitäten auf mehrere Standorte entspricht der Forderung nach Georedundanz. Wie wichtig ist das in der Praxis?*

Ingo Kraupa: Für viele Kunden ist Business Continuity ein ernstes Thema. Wir sind einer der wenigen Anbieter, die vom Betrieb der eigenen Rechenzentren über den Betrieb der Cloud-Plattformen, dem eigenen Netzwerk bis hin zum Applikationsbetrieb die volle Wertschöpfungskette eines IT-Services abbilden können. Gerade Kunden aus dem Bankenumfeld schätzen das. Für sie bedeutet jede Weiterverlagerung zusätzliches Risiko und hohen Aufwand. Georedundanz ist hier ein Erfordernis aus dem Risikomanagement. Die bisherigen Latenz- und Reichweitenproblematiken lösen wir mit neuen Konzepten adaptiv und verringern damit Risiken.

Ulrich Parthier: *Ist IT nicht eine horizontale, branchenübergreifende Technologie? Warum arbeiten Sie mit einer Vertikalisierungsstrategie?*

Ingo Kraupa: Ja, ein Rechenzentrum für die Automobilindustrie schaut nicht grundsätzlich anders aus als eines für den öffentlichen Sektor. Aber während die einen Wert auf eine BSI-Zertifizierung legen, ist für die anderen TISAX wichtig. Im Bereich der Applikationen unterscheiden sich die Anforderungen gewaltig. Und es ist natürlich wichtig, die Sprache des Kunden zu sprechen und seine Anforderungen zu verstehen.

Ulrich Parthier: *Sie bieten – ungewöhnlich für einen Colocation-Anbieter – eigene Cloud-Infrastrukturen. Welche Kunden adressiert dieses Angebot?*

Ingo Kraupa: Unsere Kunden haben meist Private Clouds oder hybride Ansätze. Dabei wollen sie „atmen" können und eine gewisse Flexibilität haben – diese muss aber nicht so extrem wie beim Hyperscaler sein. Wichtiger sind die Themen Sicherheit und Verfügbarkeit. Extreme Dynamik sehen wir bei den Plattform-Services. War das anfänglich ein Thema für Experten, ist die Nachfrage im letzten Jahr regelrecht explodiert. Viele Kunden beschäftigen sich intensiv mit diesem Thema und genießen die Vorteile von Containern und deren Orchestrierung.

Ulrich Parthier: *noris network wird bei Public Cloud Service nicht die Funktionalitäten der Hyperscaler anbieten können. Was ist mit Kunden, die Hyperscaler Services nutzen wollen?*

Ingo Kraupa: Als Mittelständler geht es uns immer um langfristige, nachhaltige Kundenbeziehungen. Wenn ein Kunde beim Hyperscaler besser aufgehoben ist, dann bringen wir ihn dort hin. Wir haben direkte Partnerschaften und Anbindungen zu den wichtigsten Hyperscalern und zu großen europäischen Hostern wie OVH.

Ulrich Parthier: *Kleine und mittlere Unternehmen gelten als agiler und kundennäher. Hand aufs Herz: Sind Sie selbst noch bei Kunden?*

Ingo Kraupa: Ja, unsere Kunden kennen mich. Ich rede viel mit ihnen, um herauszuhören, in welche Richtung sie denken und unsere Strategien dagegen zu verproben. Ich bin Verbindungsglied, wenn es darum geht, Anforderungen einzelner Kunden in einen Standard zu überführen oder bis dato unterschiedlich gehandhabte Praktiken zu vereinheitlichen, um eine möglichst gute Lösung für den Kunden zu erreichen. Ich verstehe mich da ganz als Dienstleister.

Ulrich Parthier: *Herr Kraupa, wir danken für dieses Gespräch.*

Der jüngste Colocation-Erweiterungsbau in Nürnberg ist TÜV-TSI-Level-4-zertifiziert.

MIT VERTIKALISIERUNG ZUM ERFOLG

EINEN WICHTIGEN SCHRITT MEHR FÜR DIE KUNDEN GEHEN

Der Wettbewerbsdruck auf die Anbieter von Colocation-Flächen und Managed Services steigt weiter. Und in der Cloud-Welt der Zukunft scheint Größe der allein bestimmende Faktor zu werden. Mittelgroße Anbieter sind gefordert, neue Geschäftsmodelle zu entwickeln. Eine mögliche Antwort: Technologie und Vertikalisierung.

Für viele ist das Rennen längst entschieden: Die IT wandert in die Cloud und hier setzen sich ein paar wenige, sehr große Anbieter wie Amazon, Google, Microsoft durch. Die Triebfedern hinter dieser Konzentration: Preisvorteile durch Skaleneffekte in weltumspannenden IT-Infrastrukturen, das Setzen von technologischen Quasistandards und extrem kostengünstige, weil gleichartige Angebote an die Kunden. Was aus der Vogelperspektive schlüssig erscheint, weicht bei näherem Hinsehen einer differenzierteren Sichtweise. Die Anbieterszene im Bereich Colocation, Managed Services und selbst bei Cloud-Lösungen ist weiterhin vielfältig. Ein Grund: Mittelgroße Anbieter zeigen sich einfallsreich, schärfen ihre Leistungen, stimmen diese besser und individueller auf Kunden ab und bieten vielen Kunden so weiterhin die attraktiveren Angebote.

Vorteile kleinerer Anbieter nutzen

Dabei können kleinere Anbieter auf einige klare Vorteile gegenüber den Branchenriesen setzen. So ist die Betreuung meist persönlicher, sie zeigen sich flexibler und sind mit ihren Standorten auch manchmal einfach näher dran am Kunden. Allerdings: Individualisierung kostet Zeit und Geld, behindert Skalierung und Wachstum. Daher gilt es für mittelgroße Anbieter, einen Mittelweg zwischen kostentreibender Individualisierung und den kostengünstigen Standardangeboten der ganz großen Anbieter zu finden. Einen Ausweg bietet die Vertikalisierung.

„Die Anforderungen der Unternehmen sind deutlich differenzierter und vielfältiger, als es der Ruf der IT als horizontale Technologie uns manchmal glauben lässt. Branchen und Unternehmen setzen bei

ihren Anforderungen sehr unterschiedliche Schwerpunkte, die Reifegrade unterscheiden sich und spätestens bei den Applikationen gibt es riesige Unterschiede. Wir fahren aktuell eine Vertikalisierungsstrategie, fokussieren auf Branchen mit speziellen Ansprüchen an Sicherheit, Technologie und Service. So können wir Banken und Versicherungen, öffentlichen Einrichtungen, Softwareanbietern und der Automobilindustrie sehr attraktive Angebote machen und zeigen, dass wir ihre Sprache sprechen", bringt es Ingo Kraupa, Mitgründer und Vorstandsmitglied der noris network AG auf den Punkt. Der Nürnberger Dienstleister kann mit TISAX, PCI-DSS oder dem ISO 27001-Zertifikat auf der Basis von IT-Grundschutz einige branchenspezifische Zertifizierungen und viel Erfahrung mit der proaktiven, praktischen Unterstützung bei Audits bieten. Bei größeren Anbietern suchen Kunden das meist vergeblich. Gleichzeitig stellt diese Unterstützung einen großen praktischen Nutzen dar. Schon weil ein missratener Audit in Branchen wie Banken und Finanzen oder bei öffentlichen Einrichtungen ein Anlass für Eskalationen ist, den die IT-Verantwortlichen unbedingt vermeiden wollen.

Natürlich ist diese Strategie nicht ohne Kosten und Risiken. So investieren die Nürnberger massiv in neue RZ-Technologien und -Flächen, um auch künftig den hohen, weiterwachsenden Sicherheits- und Verfügbarkeitsanforderungen ihrer Kunden entsprechen zu können. Der jüngste Colocation-Erweiterungsbau in Nürnberg ist TÜV-TSI-Level-4-zertifiziert und die RZ-Standorte in München und Nürnberg sind durch Ultra-Low-Latency-Technologie mehrfach redundant vernetzt. Der Hintergrund: Viele der Kunden sind schon von den Aufsichtsbehörden gezwungen, ausgefeilte Business-Continuity-Strategien und moderne Dual-Site-Konzepte umzusetzen. Wer hier mitspielen will, muss entsprechend investieren.

Technologisch mithalten

Ein weiterer Bereich, in dem der Dienstleister mit hoher Flexibilität punktet, ist die Cloud-Transformation. Technische und wirtschaftliche Zwänge führen dazu, dass oft nur Teilbereiche von Anwendungen in die Cloud umgezogen werden können. Diese Anwendungen arbeiten oft noch mit Daten aus Legacy-Systemen. Diese müssen dann aus Latenzüberlegungen in unmittelbarer Nähe zur Cloud-Infrastruktur betrieben werden. Anders als die internationalen Cloud-Anbieter bietet noris network hierfür hybride Architekturen, also das Nebeneinander von Cloud- und klassischen Infrastrukturen. „Es gibt kleine Unternehmen oder Start-ups, die direkt in die Cloud springen. Aber für die meisten gewachsenen Unternehmen ist der Weg in die Cloud eher ein jahrelanger Marathon als ein kurzer Sprint. Hier bieten wir uns als Migrationspartner an, der die sich wandelnden Anforderungen auf diesem Weg flexibel abbilden kann und zugleich das Know-how – auch im Bereich Compliance-konformer Datensicherheit – für diese Migration vertiefen kann", so Ingo Kraupa.

Und Ingo Kraupa lüftet ein weiteres Geheimnis. „Es fällt mittelgroßen Unternehmen schwer und ist ein relevanter Kostenblock, aber um technologisch vorn bleiben zu können, muss man sich an Diskussionen und Entwicklungen zur künftigen IT aktiv beteiligen." So arbeiten Spezialisten der noris network AG bei der 5GAA mit, die als Vereinigung die 5G-Technologie für Vehicle-to-X-Kommunikation (V2X) standardisieren und nutzbar machen will. Das Kalkül des Dienstleisters: Wenn künftig Fahrzeuge mit Fahrzeugen, Fußgängern und Infrastruktur kommunizieren, um die Sicherheit beim (autonomen) Fahren zu erhöhen, wird dies hohe Anforderungen an Datenkommunikation, -speicherung und -sicherheit stellen – und neue Geschäftsfelder öffnen. Gleiches gilt für die Beteiligung an GAIA-X. Die europäische Cloud-Initiative könnte mittelfristig für Bewegung im internationalen Cloud-Markt sorgen und die Datensicherheitsbedenken vieler Unternehmen an den heutigen Strukturen aufnehmen. „Innovation in der IT ist für uns eine Leidenschaft. Das Ende der Entwicklung ist hier noch lange nicht erreicht, Themen wie Datenhaltung und -sicherheit sind noch nicht fertig gelöst. Die Zeit ist reif, dass wir Provider in Europa hier an einem Strang arbeiten."

Die Beispiele zeigen, dass es weiterhin gute Differenzierungsmöglichkeiten für kleine und mittelgroße IT-Dienstleister gibt. Und das ist gut für Kunden und Wettbewerb. Auch weil, wie es Ingo Kraupa formuliert, kleinere IT-Dienstleister „diesen berühmten einen wichtigen Schritt mehr für die Kunden gehen, den vor allem große Wettbewerber nicht gehen wollen."

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

SCHWACHSTELLE BENUTZERKONTO

DAS A UND O BEI DER ERMITTLUNG FEHLERHAFTER BERECHTIGUNGEN IN MICROSOFT-UMGEBUNGEN? EINE KONTINUIERLICHE ÜBERPRÜFUNG!

Wie aus dem Studienbericht 2020 zum Thema „Spionage, Sabotage und Datendiebstahl" der Bitkom hervorgeht, gaben 74 Prozent der befragten Unternehmen an, dass Cyberattacken zugenommen haben. 82 Prozent gehen außerdem davon aus, dass sich die Sicherheitslage künftig noch weiter verschärfen wird. Angesichts dessen ist es wichtig, Sicherheitsmaßnahmen zu ergreifen, um typische Einfallstore zu schließen. Dazu gehören unter anderem veraltete Mitarbeiterkonten, über die sich Kriminelle Zugang zu IT-Systemen verschaffen und sensible Informationen abgreifen können. Mit der in drei Varianten erhältlichen Lösung daccord von G+H Systems lassen sich solche Schwachstellen beheben. Eine von ihnen: die Microsoft Edition zur Analyse und Überwachung der Richtlinien und Benutzerkonstellationen im Active Directory (AD) und im NTFS-Filesystem.

Die manuelle Analyse von AD-Objekten und Fileserverstrukturen ist zeitaufwendig und birgt ein hohes Fehlerpotenzial. So ist es schnell passiert, dass Missstände wie Überberechtigungen oder aktive Benutzerkonten ehemaliger Mitarbeiter unentdeckt bleiben. Damit zu keinem Zeitpunkt der Überblick verloren geht, wer worauf Zugriff hat, ist eine softwarebasierte Auswertung der Berechtigungen nötig. Die daccord Microsoft Edition lässt sich einfach installieren sowie konfigurieren, erfasst die Zugriffsberechtigungen der einzelnen Benutzer und Gruppen innerhalb der firmeninternen Microsoft-Infrastruktur.

Die Top-Features

Verwaiste Konten aufdecken, indem Personendaten integriert werden und ein Bezug zu den natürlichen Personen hergestellt wird.

- Personalstammdaten lassen sich während oder nach der Konfiguration als CSV-Datei hochladen.
- Um die Daten aktuell zu halten, ist es möglich, den Zeitplan des zyklischen Datenimports zu bestimmen, der aus dem Personalsystem bereitgestellt wird.

Jederzeit den Überblick behalten durch eine beständige Überprüfung der Konstellationen.

- Es erfolgt kein einmaliger, sondern ein dauerhafter Check des Datenbestandes. Dies ist essenziell, um Schwachstellen zu vermeiden.

Kontenursprung feststellen und Veränderungen dokumentieren mittels Historienfunktion:

- Anstelle einer Momentaufnahme werden anhand konfigurierter Zeitpläne alle Läufe historisch festgehalten, sodass man jederzeit einen Einblick in die Veränderungen bekommt.

Vollautomatisierte Kontrolle dank vorgefertigter Richtlinienpakete:

- Die mitgelieferten Richtlinien erlauben die Überprüfung der Umgebung auf Konformität zu Microsoft-Empfehlungen oder rechtlichen Anforderungen.
- Jede Richtlinie ist ein- und ausschaltbar und beinhaltet Korrekturempfehlungen.
- Es lassen sich Risikolevel definieren, ab denen ein Wert als kritisch angezeigt wird.
- Liegen unternehmenseigene Richtlinien vor, kann ein individuelles Richtlinienpaket erstellt werden.

Schnellübersicht durch umfangreiches Dashboard:

- Auf dem integrierten Dashboard erhält man eine anschauliche Übersicht über alle Systeme und Daten.
- Ungereimtheiten im Daten- oder Personenbereich sowie Abweichungen zu den Richtlinien fallen unmittelbar auf.

Sebastian Spethmann
www.daccord.de/microsoft

E-MAIL-VERSCHLÜSSELUNG?

BEWUSSTSEIN FÜR DATENSCHUTZ STÄRKEN

Vor mehr als zwei Jahren ist die Datenschutz-Grundverordnung (DSGVO) in Kraft getreten. Sie schreibt die Verschlüsselung personenbezogener Inhalte in E-Mails eindeutig vor. Dennoch verzichten viele Unternehmen auf eine Secure E-Mail-Lösung, da ihnen der Aufwand vermeintlich zu hoch ist. Dabei existieren zuverlässige Lösungen, die es erlauben, spontan und sicher mit jedermann zu kommunizieren, ohne Dokumente erst ausdrucken, kuvertieren und zur Post bringen zu müssen. Woran liegt es also, dass sich die E-Mail-Verschlüsselung noch nicht richtig durchgesetzt hat? Und was genau sollte eine moderne Lösung zur Absicherung des E-Mail-Verkehrs mitbringen? Diese und weitere Fragen beantwortet Ihnen Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH, im Interview mit itsecurity-Publisher Ulrich Parthier.

Ulrich Parthier: *Wie schätzen Sie den bisherigen Umsetzungsgrad der E-Mail-Verschlüsselung ein?*

Günter Esch: An dieser Stelle möchte ich auf eine deutschlandweite TeleTrust-Umfrage zur IT-Sicherheit im Home-Office verweisen, die ergeben hat, dass 41 Prozent der Befragten Maßnahmen zur E-Mail-Sicherheit getroffen haben. Die restlichen 59 Prozent haben somit keine Verschlüsselungslösung genutzt. Folglich hat sich die E-Mail-Verschlüsselung noch nicht richtig etabliert. Als die DSGVO wirksam wurde, gab es zunächst viel Bewegung und einen starken Aktivismus, der sich jedoch nicht bis heute fortgesetzt hat. Es entscheiden sich zwar weiterhin Unternehmen für einen sicheren E-Mail-Versand, doch der Hype, endlich etwas zu tun, ist abgeflacht. Dies lässt sich mit der aktuellen COVID-19-Situation vergleichen. Corona kam, es folgte der Lockdown, und die meisten Menschen haben sich an die Hygiene- und Abstandsregeln sowie die Kontakteinschränkungen gehalten, denn das Bewusstsein war da: Es gibt einen gefährlichen Virus. Nachdem nun einige Monate vergangen sind, werden viele wieder leichtsinnig, und das Virus rückt in den Hintergrund, obwohl es nicht weg ist. Eine ähnliche Entwicklung ist auch beim Thema E-Mail-Sicherheit zu beobachten – und das trotz zunehmender Cyberattacken.

Ulrich Parthier: *Woran liegt es, dass noch immer zahlreiche Unternehmen keine Lösung zur Verschlüsselung von E-Mails verwenden?*

Günter Esch: Für alle Nutzer wäre es komfortabel, wenn die Verschlüsselung im Hintergrund erfolgt, ohne dass der gewohnte Arbeitsprozess unterbrochen wird. Doch die dafür benötigten Verschlüsselungsverfahren sind in der Praxis leider noch nicht genug verbreitet. Um also auch mit denjenigen Empfängern geschützt zu kommunizieren, die selbst kein Schlüsselmaterial besitzen, greift man auf die sogenannte Spontanverschlüsselung zurück. Zur E-Mail-Entschlüsselung ist die Eingabe eines Passwortes notwendig, was manche davon abhält, eine Sicherheitslösung einzuführen. In meinen Augen sollte dieser Prozess jedoch kein Problem darstellen, da er dem optimalen Schutz digital verschickter Daten dient. Bei der Anmeldung in anderen Applikationen, zum Beispiel einer Banking-App, tippen wir schließlich auch wie selbstverständlich aus Sicherheitsgründen ein Passwort ein. Warum dann nicht auch beim Öffnen

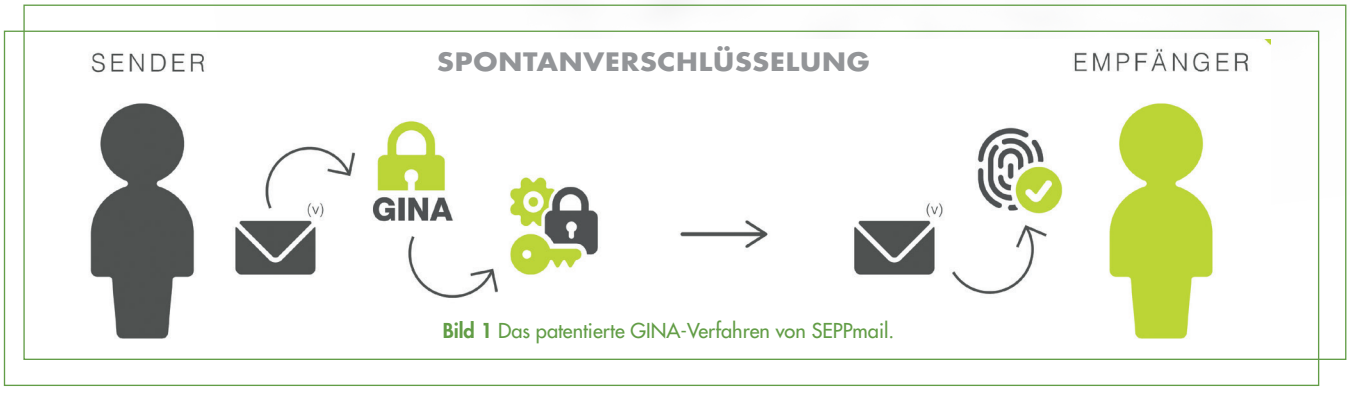


Bild 1 Das patentierte GINA-Verfahren von SEPPmail.

ICH GEHE DAVON AUS, DASS SICH DIE SENSIBILITÄT IN PUNCTO E-MAIL-SICHERHEIT WEITERHIN VERSTÄRKEN WIRD. DENN DIE KRIMINELLE ENERGIE GEHT GENAUSO WENIG WEG WIE DIE BEDROHUNG DURCH VIREN WIE COVID-19.

Günter Esch, Geschäftsführer, SEPPmail – Deutschland GmbH, www.seppmail.de

vertraulicher Mails? Hier gilt es, ein neues Bewusstsein zu entwickeln.

Ulrich Parthier: *Welchen Vorteil hat es, vertrauliche Dokumente verschlüsselt via E-Mail auszutauschen?*

Günter Esch: Natürlich zuallererst, dass die übermittelten Daten nicht von unautorisierten Instanzen abgefangen und mitgelesen werden können. Zudem lassen sich so die Richtlinien der DSGVO einhalten. Zusätzlich profitieren die Nutzer davon, dass die digitale Informationsübertragung deutlich schneller erfolgt als der postalische Versand. Wenn es beispielsweise Dokumente wie Untersuchungsergebnisse zu übermitteln gilt, die wichtig für den weiteren Behandlungsverlauf sind, sollten sie zeitnah den Empfänger erreichen. Außerdem steigern sich das Image und die Vertrauensbasis zu Kunden oder Partnern eines Unternehmens deutlich, wenn eine Verschlüsselungslösung genutzt wird.

Ulrich Parthier: *Was zeichnet eine gute E-Mail-Verschlüsselungslösung aus?*

Günter Esch: Eine geeignete Secure E-Mail-Lösung unterstützt alle gängigen Verschlüsselungsverfahren wie S/MIME, OpenPGP, TLS und Domainverschlüsselung. Um auch die Spontanverschlüsselung abdecken zu können, sollten die dazu erforderlichen Technologien implementiert sein. Essenziell ist es, dass die E-Mails komplett ausgeliefert und nicht auf der Appliance zum Download zurückgehalten werden. Darüber hinaus sollten weder eine zusätzliche Softwareinstallation noch ein PDF-Reader notwendig sein, um die E-Mail zu lesen. Damit der Empfänger unmittelbar antworten kann, eignet sich die Einbindung einer Antwortfunktion, über die sich auch eigene Attachments verschlüsselt zurückschicken lassen.

Ulrich Parthier: *Wie läuft dieses Verfahren zur Spontanverschlüsselung ab?*

Günter Esch: Im Falle unseres Verfahrens ist auf der Appliance ein standardisiertes Rule-Set etabliert, das sich auf die Anforderungen des Unternehmens anpassen lässt. Bei dem Standardset markiert der Sender die E-Mail zunächst als vertraulich. Kommt die Meldung auf der Appliance an, prüft diese, ob bereits ein Verschlüsselungsverfahren vorhanden ist. Schlägt keiner der Standardtechnologien an, findet das Verfahren der Spontanverschlüsselung Anwendung. Die E-Mail wird dabei samt Anhängen verschlüsselt und mit einer Trägermail ausgeliefert. Der verschlüsselte Anhang lässt sich durch Eingabe eines Passwortes auf jedem internetfähigen Gerät mit Browser öffnen, um die Nachricht zu entschlüsseln. Dafür stehen verschiedene Passwort-Optionen zur Verfügung.

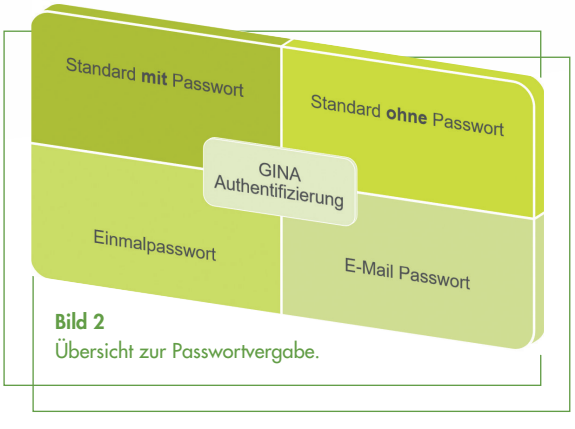


Bild 2
Übersicht zur Passwortvergabe.

Die Appliance kann etwa ein Initialpasswort für den Sender erstellen, das der Empfänger über einen zweiten Übertragungsweg erhält. Alternativ gibt es die Möglichkeit eines Einmalpasswortes, für das lediglich die Mail-Adresse und die Handynummer des Empfängers benötigt werden. Daraufhin lässt sich jede E-Mail des Absenders verschlüsseln, und der Empfänger erhält ein einmalig gültiges Kennwort zur Entschlüsselung per SMS. Sollten vertrauliche E-Mails nur selten mit einem Empfänger ausgetauscht werden, besteht zudem die Option des E-Mail-Passworts, das einer spezifischen Mail zugeordnet ist und ohne Registrierung funktioniert. Empfänger, die häufiger verschlüsselte Mails bekommen, können sich beim Versender registrieren und im Anschluss entweder mit oder ohne Login sichere E-Mails empfangen.

Ulrich Parthier: *Glauben Sie, dass sich die E-Mail-Verschlüsselung zukünftig noch weiter bei den Unternehmen verbreiten wird?*

Günter Esch: Sicherlich nicht so schnell, wie es in Hinblick auf die Vorgaben der DSGVO und der Abwehr vor Cyberkriminellen sein sollte. Ich gehe allerdings davon aus, dass sich die Sensibilität in puncto E-Mail-Sicherheit weiterhin verstärken wird. Denn die kriminelle Energie geht genauso wenig weg wie die Bedrohung durch Viren wie COVID-19.

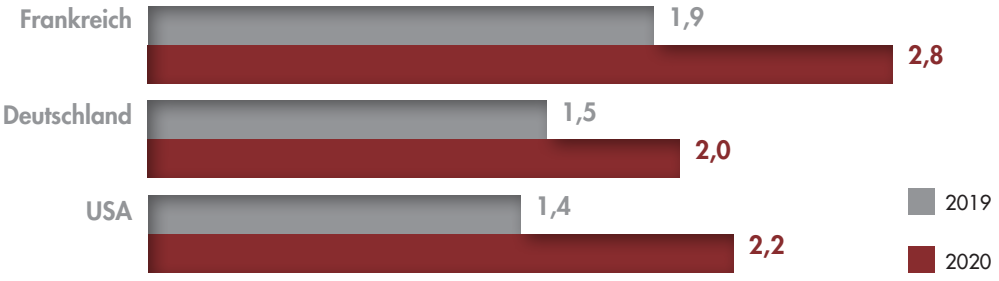
Ulrich Parthier: *Herr Esch, wir danken für das Gespräch.*

CYBER-SICHERHEIT

KOSTENEXPLOSION UND GESTIEGENES RISIKOBEWUSSTSEIN

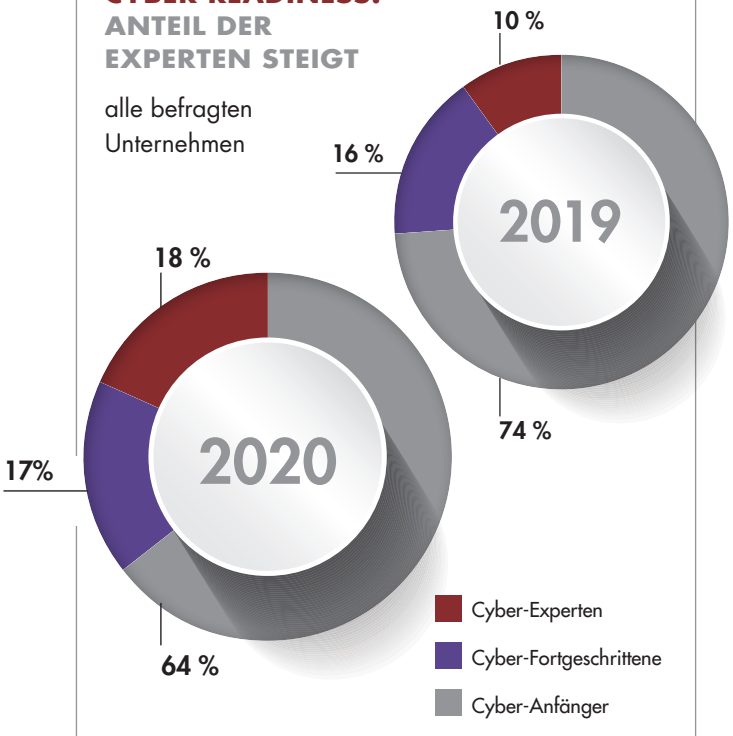
UNTERNEHMEN GEBEN IMMER MEHR GELD AUS, UM SICH VOR CYBER-ATTACKEN ZU SCHÜTZEN

Gesamtausgaben der Unternehmen für Cyber-Sicherheit in Mio.Euro.



CYBER READINESS: ANTEIL DER EXPERTEN STEIGT

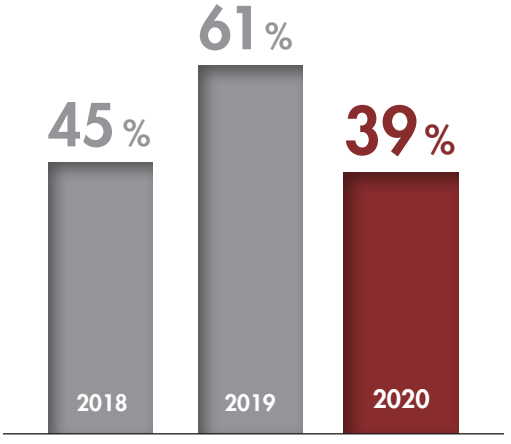
alle befragten Unternehmen



Hierzulande zählt nach wie vor die deutliche Mehrheit (66 %) der befragten Unternehmen zu den sogenannten Cyber-Anfängern, die nicht ausreichend auf Cyber-Risiken vorbereitet sind. 2019 waren es 70 Prozent.

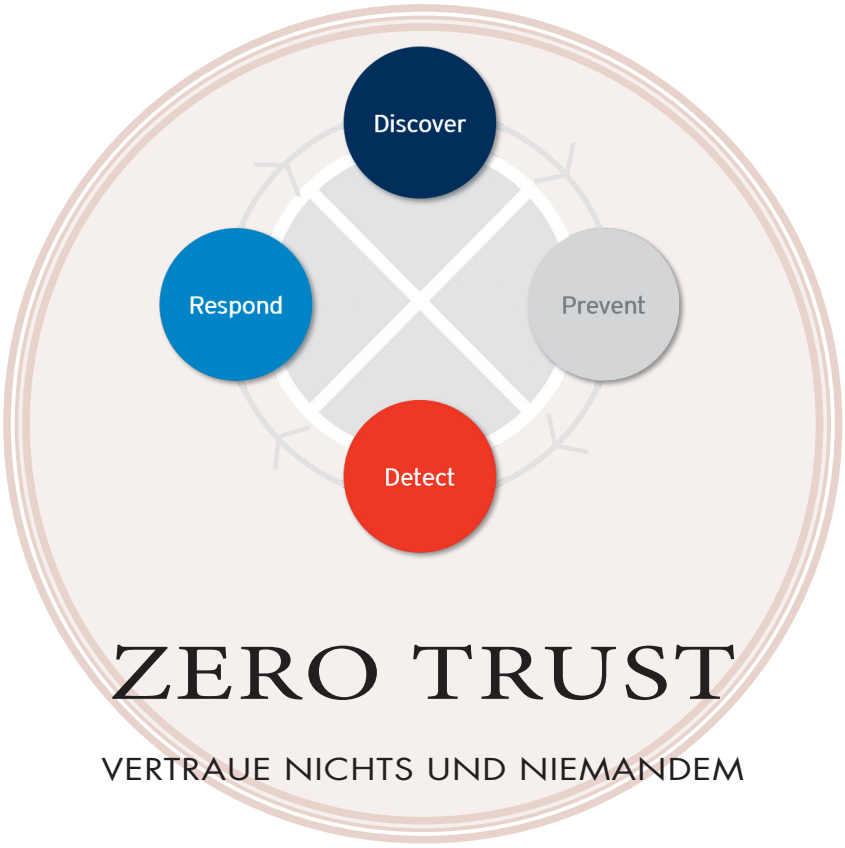
ANZAHL DER ERFOLGREICHEN CYBER-ANGRIFFE NIMMT ERSTMALS DEUTLICH AB

Anteil der internationalen Unternehmen, die angeben, im letzten Jahr Opfer mindestens eines Cyber-Angriffs geworden zu sein



In Deutschland waren es 2020 noch 41 Prozent der befragten Unternehmen, im Vorjahr waren es 61 Prozent.

www.hiscox.de/cyber-readiness-report-2020



ZERO TRUST

VERTRAUE NICHTS UND NIEMANDEM

Wir leben in digitalen Zeiten und produzieren große Mengen an Daten, die digital gespeichert werden. Diese Daten sind wertvolles Gut – sie können gestohlen und missbraucht werden, Unternehmen machen sich erpressbar. Professionelle profitorientierte Hacker nutzen immer raffiniertere Techniken. Die Zahl der Schadsoftware-Varianten steigt seit Jahren stetig. Gefälschte Emails, Phishing, Spionage oder leichtsinniges Verhalten der Mitarbeiter gehören heute zu den größten Sicherheitsrisiken für Unternehmen.

Herkömmliche Sicherheitskonzepte verorten den „Feind" dabei außerhalb des Unternehmensnetzwerks: War das Unternehmen nach außen geschützt, so galt es als sicher. In heutigen vernetzten digitalen Strukturen mit vielen Endgeräten, verteilten Daten und standortunabhängigem Arbeiten fallen diese klaren Grenzen weg. Eine Firma ist heute jederzeit und überall verwundbar.

Never trust – always verify

Diese Tatsache erfordert ein neues Sicherheitsdenken nach der Maxime „Never trust – always verify" – oder in anderen Worten „Zero Trust": Vertraue nichts und niemandem. Zero Trust bedeutet, jeder Anwendung, jedem Zugriff, jedem Dienst, jedem Gerät zu misstrauen und diese stets zu überprüfen. Jeglicher Datenverkehr wird überprüft, alle Benutzer oder Dienste müssen sich authentifizieren.

Welche Lösungsbausteine muss ein IT-Sicherheitskonzept enthalten, das diesem Prinzip gerecht wird? Eine erste Orientierung für den Aufbau einer ganzheitlichen IT-Sicherheit bietet das Phasenmodell mit den Schritten Discover – Prevent – Detect und Respond.

In der Phase **Discover** verschaffen Sie sich einen Eindruck vom aktuellen Sicherheitszustand Ihres Unternehmens. Gibt es Schwachstellen in Form veralteter Software, fehlender Patches? Hierbei helfen Schwachstellen-Scanner. Gibt es Richtlinien bzgl. der Nutzung von eigenen Endgeräten (ByoD) oder der Verwendbarkeit von USB-Sticks?

In der **Prävention** nutzen Sie alle Möglichkeiten, Angriffe abzuwehren oder den Datendiebstahl wertlos zu machen. IT-Grundschutz oder Branchenempfehlungen für KRITIS-Unternehmen empfehlen hier unter anderem Maßnahmen wie Datenverschlüsselung, Applikationskontrolle zum Schutz vor Schadsoftware und Kontrolle des Datenflusses auf Wechseldatenträger. Auch der Faktor Mensch spielt hier eine wichtige Rolle. Sicherheitskampagnen, Schulungen und Sensibilisierung für Sicherheitsrisiken sind kritische Präventionsmaßnahmen, die das Risiko für Angriffe und Datenverlust signifikant reduzieren.

In der Phase **Detect** helfen Werkzeuge, die ein anomales Verhalten auf den Endpunkten signalisieren und Forensiker mit Daten bzw. Anomalien auf definierten Events unterstützen, beim Aufspüren von Bedrohungen, die sich bereits im System befinden.

Die Reaktion (**Respond**) auf Bedrohungen kann sowohl manuell als auch automatisch erfolgen, u.a. durch Quarantäne oder das Beenden von Prozessen. Auch hier unterstützen Systeme, bei denen sogenannte Security Alerts vordefinierte Reaktionen triggern.

IT-Security auf Knopfdruck

Eine ganzheitliche Zero Trust Strategie benötigt eine integrierte Plattform, die die oben genannten Bausteine integriert und so Schadsoftware, Cyberangriffe und Datenverlust wirkungsvoll verhindert und bekämpft. Eine so umfangreiche Lösung muss nicht zwangsläufig von der hauseigenen IT installiert, betrieben und gewartet werden – gerade, wenn es bei kleineren Unternehmen an IT-Fachpersonal oder Budget mangelt. DriveLock als cloudbasierter Endpoint Protection-Anbieter verfügt über eine solche Zero Trust Plattform, die schnell und kostengünstig aus der Cloud zur Verfügung steht – quasi IT-Security auf Knopfdruck.

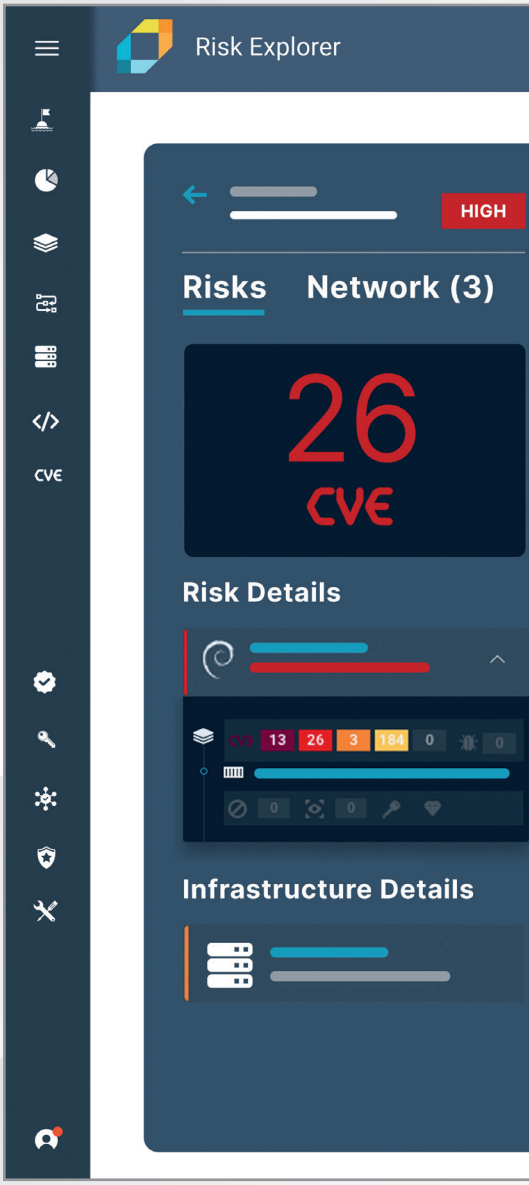
Andreas Fuchs

www.drivelock.com

DriveLock

CLOUD-NATIVE ARCHITEKTUREN

UMGANG MIT NEUEN SICHERHEITSRISIKEN



Container-basierte und serverlose cloud-native Architekturen stellen die bedeutendsten Computing-Fortschritte für die Bereitstellung von Anwendungen in Unternehmen dar, seit VMware 1999 sein erstes Produkt, Workstation 1.0, vorgestellt hat. Obwohl diese Technologien bei Flexibilität, Kosteneinsparungen und Skalierbarkeit eine Reihe von Vorteilen bieten, sind sie auch mit neuartigen sicherheitstechnischen Herausforderungen verbunden, die es bei der Migration von Anwendungen vom Rechenzentrum in die Cloud zu berücksichtigen gilt. Bei sachgemäßer Umstellung kann für diese neuen Entwicklungs- und Bereitstellungsumgebungen ein noch nie dagewesenes Sicherheitsniveau erreicht werden. CISO sollte sich jedoch darüber im Klaren sein, welchen Einfluss diese modernen Technologien auf den Sicherheits- und Compliance-Status seiner Organisationen haben, wenn das Unternehmen sie in der Produktion einführt, und seine Erwartungen im Vergleich zu den vorhandenen Tools und Methoden neu justieren.

DIE DEVOPS-BEWEGUNG SETZT GANZ AUF GESCHWINDIGKEIT UND GIBT ENTWICKLERN DAS RÜSTZEUG AN DIE HAND, ANWENDUNGEN SCHNELLER DENN JE ZU ENTWICKELN UND BEREITZUSTELLEN, OFTMALS AUF GRUNDLAGE AUTOMATISIERTER PROZESSE.

Arne Jacobsen,
Director Sales EMEA, Aqua Security,
www.aquasec.com

Früher hatten Sicherheitsabteilungen die Möglichkeit, auch noch kurz vor der Umstellung von Anwendungen auf die Live-Produktionssysteme prüfend und beratend einzugreifen. Noch kurz vor einem Release wurden die erforderlichen Änderungen vorgenommen, häufig unter Inkaufnahme erheblicher Verzögerungen, um den bestehenden Anforderungen an Betrieb, Sicherheit und Compliance gerecht zu werden. Das war einmal. Die DevOps-Bewegung setzt ganz auf Geschwindigkeit und gibt Entwicklern das Rüstzeug an die Hand, Anwendungen schneller denn je zu entwickeln und bereitzustellen, oftmals auf Grundlage automatisierter Prozesse. Die IT-Sicherheit kann diesen Fortschritt nicht aufhalten und wird auf der Strecke bleiben, wenn sie versucht, ihn zu bremsen. CISOs sollte sich vorrangig mit der Entwicklung und Umsetzung einer Strategie beschäftigen, die einen proaktiven Umgang mit cloud-nativen Sicherheitsanforderungen ermöglicht.

Veränderliche Rahmenbedingungen

Bei den Gesprächen mit unseren Kunden wird eine Herausforderung immer wieder genannt: wie fließend und dynamisch die Rahmenbedingungen mittlerweile sind. Hieraus ergibt sich ein neuartiges Sicherheitsparadigma: Unternehmen müssen in der Lage sein, ihre cloud-nativen Anwendungen schon ganz früh während ihrer Entwicklung bis hin zur Bereitstellung in der Produktion, über Multi-Cloud-Umgebungen hinweg und trotz eines sich ständig ändernden Technologie-Stacks zu schützen und zu sichern.

Portworx, ein Unternehmen, das sich auf Container-Speicherung und Datenma-

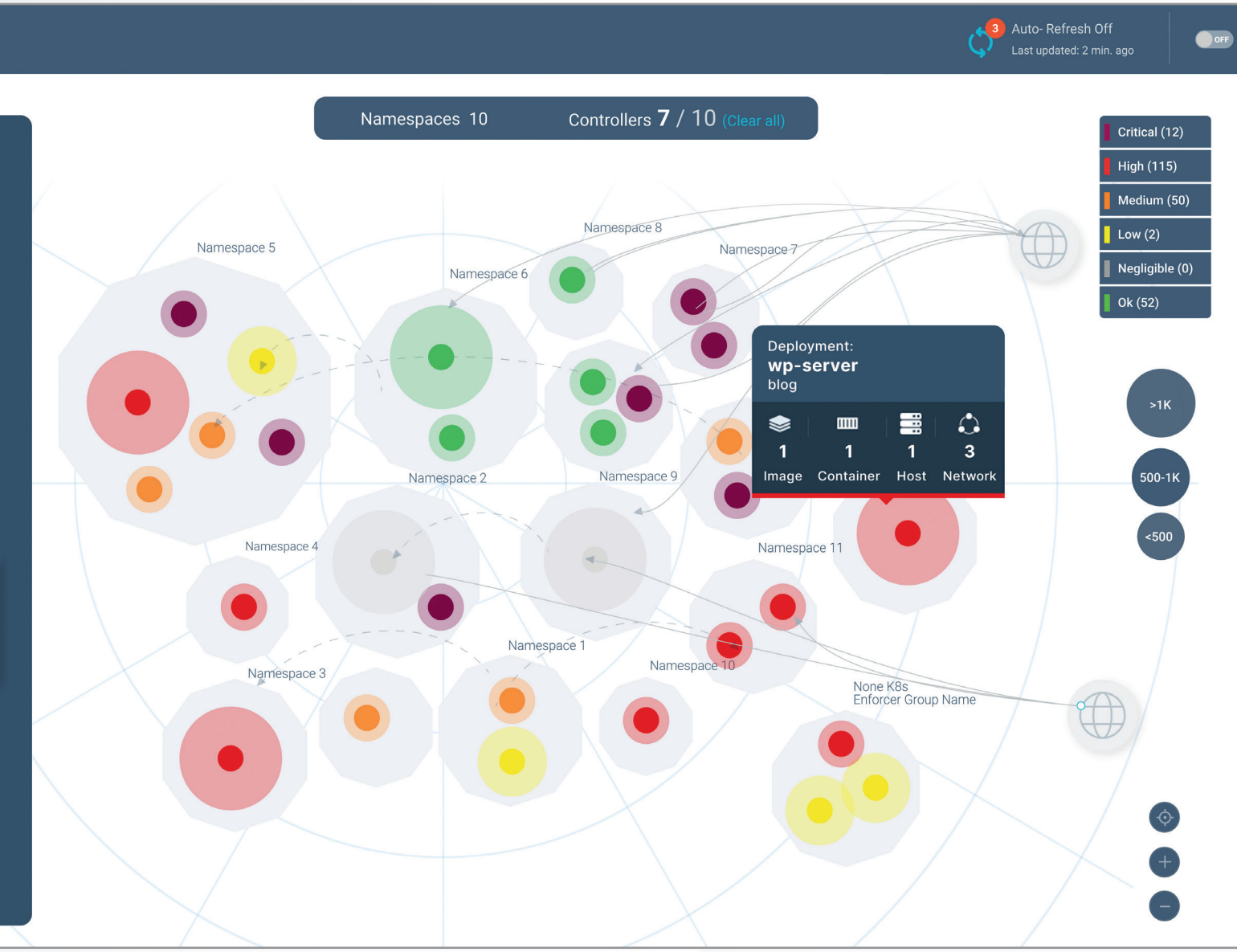


Bild 1: Aqua Risk Explorer – Kubernetes-natives Visualisierungs- und Priorisierungstool.

nagement spezialisiert hat, führt seit 2016 jedes Jahr einen Container Adoption Survey aus. Die 2019er Umfrage, die zusammen mit Aqua durchgeführt wurde, „zeichnet ein Bild von unvermindertem Wachstum im Bereich der Containerisierung, gaben doch mittlerweile 87 Prozent der Befragten an, dass sie mit Container-Technologien arbeiten, im Vergleich zu nur 55 Prozent im Jahr 2017. Von denen, die Anwendungen in Containern nutzen, setzen diese 90 Prozent in der Produktion ein, im Vergleich zu 84 Prozent 2018 und 67 Prozent im Jahr 2017."

Während die Portworx-Umfrage 2017 die persistente Speicherung noch als wichtigsten Hemmschuh für die Einführung von Container-Technologien ausmachte, schaffte es dieser Aspekt im letzten Jahr nicht unter die Top 3. 2019 wurden als die drei wichtigsten Herausforderungen die Datensicherheit, das Schwachstellen-Management und der Laufzeitschutz genannt.

Sicherheit in der DevOps-Welt

Doch selbst in diesem sich rasch wandelnden Sicherheitsumfeld setzen viele Unternehmen weiterhin auf herkömmliche Sicherheitstools, die häufig nicht mit der Geschwindigkeit, der Größe und der dynamischen Netzwerkumgebung von Containern Schritt halten können. Das Aufkommen neuartiger serverloser Funktionen verschärft das Problem zusätzlich, weil diese die Infrastruktur noch weiter abstrahieren, um eine einfache Ausführungsumgebung für Anwendungen und Microservices bieten zu können. Cyberkriminelle sind darauf aus, Schwachstellen im serverlosen Funktionscode auszunutzen oder machen sich schlecht konfigurierte Berechtigungen für Cloud-Infrastrukturen zu Nutze, um sich Zugang zu

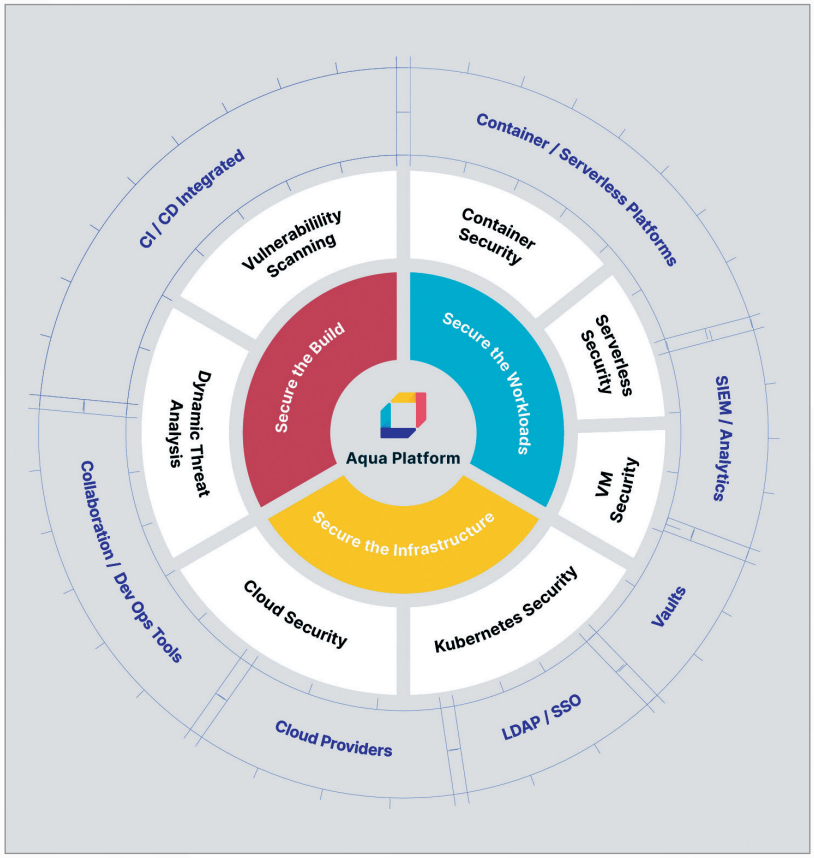


Bild 2: Aqua Security – Die umfassende Plattform für native Sicherheit in der Cloud.

Services oder Netzwerken mit sensiblen Informationen zu verschaffen.

Die steigende Abhängigkeit von Open-Source-Anwendungen stellt eine weitere mögliche Sicherheitsschwachstelle dar. Programmcode wird nie ganz neu geschrieben, jeder bedient sich mittlerweile bei Komponenten auf GitHub oder anderen Open-Source-Projekten oder nutzt vorhandenen Code in Repositorys innerhalb oder außerhalb seines Unternehmens, möglicherweise ohne sich der Schwachstellen in der Codebasis bewusst zu sein.

Denn in einer von DevOps dominierten Welt ist Geschwindigkeit das oberste Gebot. Die Produktivität steigt, aber mit ihr auch das Sicherheitsrisiko. Gestern noch wurde der Code an die Zielarchitektur angepasst, bevor er auf der von der IT vorgegebenen Standardbetriebsplattform in Produktion ging. Heutzutage stellen Unternehmen ihre in Containern entwickelten Anwendungen aus Gründen der Geschwindigkeit direkt in der Produktion bereit, verwalten sie mithilfe von Kubernetes und lassen sie irgendwo in der Cloud ausführen (gegebenenfalls immer noch am Standort, häufig jedoch über einen Public-Cloud-Service). Dieses Modell verlangt Entwicklern und dem operativen Team ein gesteigertes Sicherheitsbewusstsein ab, wobei die Sicherheit umfassend in den Software-Lebenszyklus integriert werden muss.

Umgang mit Multi-Cloud, Multi-Stack

Viele unserer Kunden experimentieren mit Technologien von verschiedenen Anbietern, die auf unterschiedlichen Cloud-Plattformen ausgeführt werden, und stellen Anwendungen sogar gleichzeitig auf mehreren Plattformen bereit. So halten sie sich die Option offen, entweder auf Kostenoptimierung zu setzen oder den Stack zu verwenden, der am besten zu einer bestimmten Anforderung passt, und verhindern gleichzeitig eine zu starke Bindung an einen Anbieter. Dies kann aber zu Problemen für Ihre Entwickler führen, insbesondere bei serverlosen Technologien, da sich die Standards in diesem Bereich gerade erst entwickeln. Gegen Experimente ist nichts einzuwenden, aber in der Produktion benötigen Sie eine Strategie, mit der Sie festlegen, welche Plattformen verwendet und wie die Sicherheitsrichtlinien für alle bereitgestellten Anwendungen unabhängig von Plattform oder Anbieter umgesetzt werden. Eine einzige Sicherheitslösung, die alle Ihre Betriebsumgebungen durch einheitliche Richtlinien, Managementtools und Berichtsfunktionen unterstützt, kann dies ermöglichen.

Cloud-native Umgebungen besitzen eine Reihe von Eigenschaften, die es einfacher machen, sie zu schützen. Hierzu müssen Unternehmen eine neue Art von Sicherheitsmodell umsetzen, bei dem die Container-Images mitsamt ihrer Inhalte schon bei der Generierung geprüft werden und die Unveränderlichkeit der Workload zur Laufzeit garantiert wird, um Änderungen an den ausgeführten Workloads zu verhindern. Das Ergebnis? Eine stark kontrollierte Umgebung, die die Angriffsfläche erheblich reduziert, bevor eine Anwendung bereitgestellt wird, und die zur Laufzeit überwacht wird, sodass es vergleichsweise einfach ist, Anomalien mithilfe deterministischer Methoden zu erkennen und darauf zu reagieren.

Arne Jacobsen

HERZSTÜCK DATENBANK

DIE SICHERHEIT BEGINNT HIER

Datenbanken sind der Ort, wo Daten gespeichert werden. Deshalb sind sie auch die erste Stufe in einem Datenschutzkonzept. Fehler oder Fahrlässigkeiten, die hier gemacht werden, sind später bei der Übermittlung und Weiterverarbeitung nicht mehr zu kompensieren. Deshalb zwingen regulatorische Vorgaben, mögliche Datenverluste und die zu bewahrende Reputation des jeweiligen Unternehmens dazu, bei Evaluation, Implementation und Betrieb der Datenbank besondere Sorgfalt walten zu lassen. Andernfalls drohen im Fall von Datenkorruption oder -diebstahl drakonische Strafzahlungen und geschäftliche Einbußen durch Wirtschaftsspionage oder den Verlust von Kundenvertrauen. Couchbase nennt die vier wichtigsten Sicherheitskriterien, die zum Schutz sensibler Daten erfüllt werden müssen:

1. **Access Control:** Bei der Zugangskontrolle haben sich zwei Vorgehensweisen bewährt: Durch die Funktionstrennung soll sichergestellt werden, das bestimmte Aufgaben nicht von einer einzigen Person allein erledigt werden. Beim Least Privileged Access erhält jeder Benutzer nur die für jeweiligen Tätigkeiten absolut notwendigen Zugriffsberechtigungen.

2. **Encryption:** Die Verschlüsselung gewährleistet die Datensicherheit auch dann, wenn die Zugangsrestriktionen versagt haben. Innerhalb der Datenbank werden dabei Nutzer-, Anwendungs- und Metadaten in Ciphertext konvertiert. Das sichert die Daten auch bei der Replikation zwischen verschiedenen Database-Clustern oder beim Transfer über das Netzwerk.

3. **Data Masking und Redaction:** Mit dieser Datenbank-Technologie werden sensible Daten für die Ausgabe in Echtzeit „maskiert“, um sie vor unbefugten Zugriffen zu schützen. Dabei werden nur die Abfrageergebnisse anonymisiert, während die zugrunde liegenden Originaldaten erhalten bleiben. Gängige Verfahren sind unter anderem Blacklist, Random First Name oder Random Last Name.

4. **Auditing und Reporting:** Nicht zuletzt müssen alle Transaktionen jederzeit transparent, kontrollierbar und nachvollziehbar sein. Die ausgegebenen Reports über die Datenbankaktivitäten sollten dabei die typischen W-Fragen beantworten: wer, was, wann und wie.

www.couchbase.com

DATA GOVERNANCE

DER LEITFADEN FÜR DIE PRAXIS

Das Buch bietet einen kompakten, praxisorientierten Einblick in das Thema Data Governance. Es geht dabei um die Rahmenbedingungen und Standards für die Verwaltung und Zugriffssteuerung großer Datenmengen. Im Kontext der digitalen Transformation kommt dem Datenmanagement eine wachsende Bedeutung zu. Dabei unterscheiden die Autorinnen nicht zwischen unterschiedlichen Datendomänen, sondern betrachten das Thema aus einer übergeordneten Perspektive.

Profitieren Sie von den Ergebnissen intensiver, praxisnaher Forschung und von jahrelanger Projekterfahrung in Unternehmen unterschiedlicher Größenordnung. Erfahren Sie, welche Vorgehensweisen wirklich funktionieren. Das Buch enthält praktische Handlungsempfehlungen, mit denen Sie schnell Data-Governance-Aktivitäten in Ihrem Unternehmen vorbereiten, umsetzen und so einen ersten Mehrwert schaffen.

Data Governance – Der Leitfaden für die Praxis, Kristin Weber, Christiana Klingenberg,

Carl Hanser Verlag, 12/2020

IT-SERVICE MANAGEMENT

ZUSAMMENARBEIT SYSTEMATISIEREN

Die IT hat sich zu einem zentralen Erfolgsfaktor für funktionierende Geschäftsprozesse entwickelt. Das verlangt von IT-Organisationen, neuen Anforderungen gerecht werden zu müssen. Als IT-Verantwortlicher können Sie diese Herausforderungen meistern, wenn Sie auf ein strukturiertes IT-Service Management setzen.

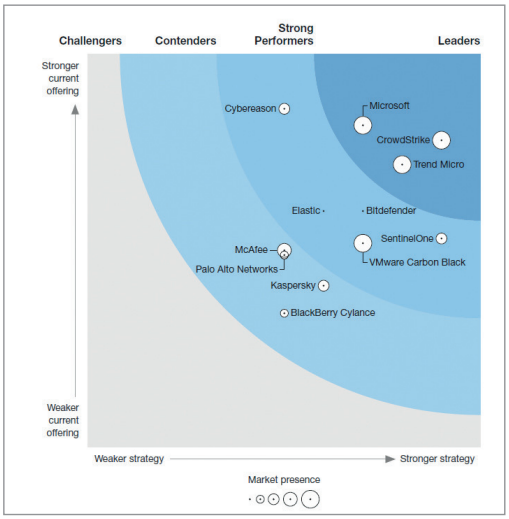
Dieses Buch zeigt Ihnen, wie Sie IT-Service-Management praxisgerecht planen und realisieren. Sie erfahren, wie Sie ITIL Ihren Zielen entsprechend richtig kombinieren und einsetzen. Als standardisierte Notation für Prozesse wird außerdem BPMN 2.0 beleuchtet. Ein ausführliches Fallbeispiel veranschaulicht, wie Sie das alles in die Praxis umsetzen und auf diese Weise kontinuierlich die Effizienz, die Qualität und die Wirtschaftlichkeit Ihrer IT-Organisation verbessern.

IT-Service Management in der Praxis mit ITIL – Zusammenarbeit systematisieren und relevante Ergebnisse erzielen (überarbeitete Auflage),

Carl Hanser Verlag, 12/2020

BITDEFENDER – DER EDR GEHEIMTIPP

FORRESTER EDR-REPORT



MSSPs und Sicherheitsspezialisten aufgehorcht: Wen bezeichnet das Analystenhaus Forrester als den „größten EDR-Anbieter, den Sie bisher nicht berücksichtigt haben, obwohl Sie es hätten tun sollen“ (The Forrester Wave: Enterprise Detection And Response, Q1 2020)? Die überraschende Antwort: Bitdefender. Das Cybersicherheitsunternehmen, das weltweit über 500 Millionen Systeme schützt, wird basierend auf seinem aktuellen Angebot, seiner Strategie und Marktpräsenz als „strong performer“ bezeichnet. Der Bericht betont zudem, dass „die Kunden nicht nur die Sicherheitsleistung des Produkts lobten, sondern auch die Managementfähigkeiten zu schätzen wussten.“

Demokratisierung der Sicherheitstechnologien

Die Anbieterbewertung weiter: „Bitdefender demokratisiert fortschrittliche Sicherheitstechnologien, indem es sich auf die Verhinderung von frühen Ereignissen in der Angriffskette und die Bereitstellung von automatisierten Abhilfemaßnahmen nach der Ausführung konzentriert.“ Die unabhängige Analystenfirma Forrester bewertet in dem Bericht, der IT-Sicherheitsprofis bei der Auswahl eines Anbieters helfen soll, zwölf EDR-Anbieter.

Zu den Kriterien, die bei der Bewertung durch Forrester verwendet wurden, gehören „die Stärke des aktuellen Angebots“ sowie „die Stärke der Strategien der Anbieter“ und die „Marktpräsenz“, die durch „die Unternehmenskunden jedes Anbieters, die eingesetzten Endgeräte und den Umsatz der Produktlinie“ bestimmt wurde.

Der Einsatz von EDR war lange Organisationen vorbehalten, die einerseits große Budgets in die EDR-Software investierten und die zweitens große IT-Security Teams hatten, um mit den umfassenden Informationen dann auch etwas anzufangen. Denn der allergrößte Teil der Meldungen früher EDR-Systeme waren Fehlalarme. Und die Sicherheitsanalysten konnten diese nicht unbedingt auf den ersten Blick von relevanten Meldungen unterscheiden.

False Positives auf ein Minimum reduzieren

Im Gegensatz dazu reduzieren moderne EDR-Lösungen, wie jene, die in Bitdefender GravityZone Ultra enthalten ist, durch Integration mit anderen Lösungen und Machine Learning die False Positives auf ein Minimum. Zudem geht es heute darum, aus der Vielzahl von Logs und Daten eine Angriffstechnik, zum Beispiel eine illegitime Rechteausweitung, abzuleiten: Technique Detection heißt diese Königsdisziplin des EDR. Alle Schritte des Angriffsprozesses werden übersichtlich bildlich dargestellt. Die IT-Verantwortlichen erhalten über EDR die komplette Zeitleiste aller Ereignisse, die zu einem Angriff geführt haben - zum Beispiel bis zurück zur ersten Phishing-Mail oder zum ersten Login mit gestohlenen Credentials.

Einheitliche Managementoberfläche

Und auch in einem weiteren Forrester-Bericht zu Cloud Security, wurde Bitdefender als „führend“ bezeichnet („The Forrester Wave: Cloud Workload Security (CWS)“, Q4 2019). Im Bericht heißt es, Bitdefender „zeichnet sich durch ein hervorragendes Datenbank-, Benutzer- und Agenten-Rollout-Management aus.“ Ein wesentlicher Vorteil von Bitdefender GravityZone ist, dass das Produkt nach dem Prinzip „One client, one console“ mit einem einheitlichen Software-Agenten für die unterschiedlichsten Endpunkte und einer einheitlichen Managementoberfläche sorgt. Dieser Agent umfasst sowohl Endpoint Security als auch EDR.

„Wir glauben, dass die Anerkennung, die wir in diesen Forrester-Berichten erhalten, nicht nur aus unserem Engagement für die Aufrechterhaltung des weltweit höchsten Sicherheitsniveaus resultiert“ sagt Dragos Gavrilut, Direktor des Cyber Threat Intelligence Lab bei Bitdefender, „sondern auch aus unserem Streben nach Einfachheit und Bedienbarkeit. Dies sind die wichtigsten Faktoren, die uns Jahr für Jahr in unabhängigen Tests und Evaluierungen Auszeichnungen und Lob einbringen.“

www.bitdefender.de

Den aktuellen Forrester-Bericht zu EDR stellt Bitdefender unter folgender URL kostenlos zur Verfügung: ***https://bit.ly/35hoBd9***

INSELLÖSUNGEN ADE

SECURITY GANZHEITLICH DENKEN

Die Gefahr durch Cyber-Kriminelle ist nicht neu, deren Opfer-Pool aufgrund des Corona-Homeoffice-Booms aber rasant gestiegen. Die Bedrohungslage für Unternehmen ist dadurch höher denn je. Wer in der Flut der immer neuen Security-Anforderungen und -Lösungen nicht untergehen will, muss Security ganzheitlich denken.

Um nur ein Beispiel zu nennen: Bis zu 9.000 COVID-19-bezogene Phishing-URLs täglich haben Akamai Sicherheitsexperten, die weltweite DNS-Auflösungsdaten in Echtzeit analysieren, in den vergangenen Corona-Wochen identifiziert. Ziel der Phishing-Attacken sind derzeit vor allem die Mitarbeiter im Homeoffice. Deren Zahl ist seit Ausbruch der Pandemie deutlich gestiegen – und das in vielen Fällen unter mangelhaften Security-Bedingungen; denn selten sind die Endgeräte im Homeoffice so gut geschützt wie im Büro. Cyber-Kriminelle frohlocken und steigern die Anzahl und Intensität ihrer Attacken. Der Verlust sensibler Daten und große finanzielle Verluste aufgrund der notwendigen „Aufräumarbeiten" sind bei vielen Unternehmen die Folge.

Insellösungen erschweren Verteidigung

Fakt ist: Das grundlegende Problem hierbei besteht nicht erst seit Corona-Zeiten. Schon mit Einzug der Cloud hat sich die IT-Landschaft nachhaltig verändert. Die Tatsache, dass Anwender mit beliebigen Endgeräten von unterschiedlichsten Orten auf Netzwerke und Anwendungen zugreifen können, brachte neue Angriffsflächen für Cyber-Kriminelle mit sich. In der Folge kamen und kommen immer neue Security-Lösungen für jede Art von Angriff auf den Markt. In den meisten Fällen existieren diese nebeneinanderher und verwandeln die IT-Landschaft der Unternehmen in ein Konglomerat aus Insellösungen – oder, anders ausgedrückt, in einen zeitfressenden Albtraum für die Security-Teams. Denn wird die IT-Sicherheitslandschaft selbst zu einer komplexen Herausforderung, bindet dies Ressourcen, die Unternehmen an anderer Stelle dringend benötigen, beispielweise bei der Untersuchung eingehender Warnungen. Gerade die sollte keinesfalls auf der Strecke bleiben.

An sich haben alle Cybersecurity-Produkte natürlich ihre Berechtigung. Will ein Unternehmen umfassend aufgestellt sein, müssen seine Sicherheitslösungen höchst sichere Firewall-, Web- und E-Mail-Ser-

vices bieten und gleichzeitig eine uneingeschränkte Mobilität sowie Telearbeit ermöglichen. Umfangreiche Cybersecurity-Portfolios – wie beispielsweise das von Cisco – decken in diesem Sinn die folgenden Produktbereiche ab (alphabetisch): Advanced Malware Protection, Cloud Security, E-Mail Security, Endpoint Security, mehrstufige Authentifizierung, Next-Generation Firewalls, Netzwerktransparenz und -segmentierung, Next Generation Intrusion Prevention Systems, Threat Response, Clients für VPN-Sicherheit sowie Web-Sicherheit. Kommt all dies aus einer Hand, entfällt für die Security-Teams im Problemfall zumindest die Suche nach der Zuständigkeit des Anbieters.

> UNTERNEHMEN BRAUCHEN EINE SICHERHEITSPLATTFORM, DIE SÄMTLICHE BEDROHUNGSVEKTOREN UND ACCESS POINTS ABDECKT.
>
> Stefan Gutekunst, Director Networking Collaboration & Security, Logicalis GmbH, www.logicalis.de

Ganzheitliche Denkweise erhöht Produktivität

Problematisch bleibt, dass viele komplizierte Oberflächen und Tools den Arbeitsalltag erschweren. Vision von Cisco ist es deshalb, die Sicherheitsarchitektur eines Unternehmens radikal zu vereinfachen, um effektiv zu sein und die digitale Transformation optimal zu unterstützen. Das jüngste Ergebnis dieser Bemühungen ist Cisco SecureX, eine native Cloud-Plattform mit einer völlig neuen Benutzeroberfläche. Sie verbindet das hauseigene Produktportfolio mit der bereits vorhandenen Sicherheitsarchitektur der Kunden unter einer einheitlichen Benutzeroberfläche. Produkte von Drittanbietern sind dabei eingeschlossen. Damit sorgt die Plattform für eine deutlich bessere Übersicht, erhöht die Transparenz und schafft vielfältige Automationsmöglichkeiten. Das Ergebnis: höhere Sicherheit von Netzwerken, Endgeräten, Anwendungen und Cloud-Diensten – und das bei deutlich geringerem Aufwand.

Im Detail heißt das: Unternehmen, die SecureX nutzen, kommen aktuellen und zukünftigen Sicherheitsanforderungen nach. Als umfassendste und am weitesten integrierte Sicherheitsplattform deckt sie sämtliche Bedrohungsvektoren und Access Points ab. Dabei liefert sie im Sinne einer einheitlichen Transparenz aussagekräftige Informationen aus der gesamten Sicherheitsinfrastruktur. Für eine schnellere Reaktion auf Bedrohungen und das Erzielen der gewünschten Ergebnisse zählen dazu unter anderem Netzwerk, Endgeräte, Cloud und Anwendungen. Unternehmen können mittels Automatisierung gleichzeitig die Effizienz und Präzision ihrer vorhandenen Ressourcen steigern. So können sie den Reifegrad von Sicherheitsprozessen und -verfahren verbessern und sind gegen die sich ständig verändernden Bedrohungen gewappnet. Ein weiterer Punkt: SecureX ermöglicht, dass IT-, Sicherheits- und Netzwerkabteilungen besser zusammenarbeiten. Auf diese Weise lassen sich Sicherheitsrichtlinien harmonisieren und bessere Workflow-Ergebnisse erzielen. Unternehmen, die ihre Cisco-Security-Investitionen weiter ausbauen wollen, können außerdem im Vorraus einer Kaufentscheidung mit nur einem Klick weitere Komponenten des Portfolios testen und sie dank ihrer Interoperabilität in ihre bestehende Sicherheitsinfrastruktur integrieren.

Schnell, fundiert und gebündelt

In den heutigen Zeiten ist eine derart ganzheitlich gedachte Security wichtig denn je, denn die Angriffe von Cyber-Kriminellen werden zunehmend einfallsreicher und aggressiver –insbesondere die Verunsicherung in Pandemie-Zeiten nutzen sie derzeit thematisch für sich aus. Dass die Angreifer sich darüber hinaus immer häufiger zusammenschließen und gemeinsame Attacken starten, erschwert die Lage für die Security-Experten der Unternehmen zusätzlich. Umso wichtiger ist es daher, Bedrohungen schnell zu untersuchen und auf sie zu reagieren. Hierfür müssen die Verantwortlichen begründete Entscheidungen treffen (Maßnahmen ergreifen und Fehler beheben) und die Zusammenarbeit der eigenen Teams dabei bestmöglich unterstützen. Dass SecureX zu diesen drei Aspekten wesentlich beiträgt, bestätigen mehr als 90 Prozent der bereits bestehenden Kunden.

Security-Performance

Das Problem: So klar die Herausforderungen für die Security auch sind, vielen Unternehmen fällt es schwer, die Leistungsfähigkeit ihrer Security-Infrastruktur umfassend zu bewerten und die richtigen Maßnahmen zu treffen. Oft fehlt es ihnen hierzu schlicht an den notwendigen internen Ressourcen. Externe Dienstleister wie Logicalis können in diesem Fall unterstützen, eine fundierte Einschätzung treffen, hinsichtlich notwendiger Maßnahmen beraten sowie eine effektive Sicherheitsinfrastruktur auswählen und implementieren. Bei Bedarf kann ein Security Operations Center (SOC) den Betrieb und das Monitoring der Sicherheitsinfrastruktur übernehmen sowie diese kontinuierlich weiterentwickeln. Die interne IT der Unternehmen kann sich so besser um die Unterstützung der Geschäftsstrategie kümmern. (Nur) so sind Unternehmen in der Lage, der aktuellen Bedrohungslage zu trotzen und Cyber-Kriminellen effektiv die Stirn zu bieten.

Stefan Gutekunst

VULNERABILITY DISCLOSURE POLICY (VDP)

FÜR DIE ZUSAMMENARBEIT MIT HACKERN

Die zunehmende digitale Vernetzung und Verwendung digitaler Geräte haben die Angriffsfläche von Unternehmen in den letzten Jahren vergrößert.

Um eigene Schwachstellen aufdecken und beheben zu können, ist die Zusammenarbeit mit Hackern eine vielversprechende Option. Dabei sind mitnichten Kriminelle gemeint. Vielmehr geht es um „Ethical Hacker", auch „White Hat Hacker" genannt, die zufällig auf Schwachstellen aufmerksam werden und diese Unternehmen in der guten Absicht, einen Cyberangriff zu verhindern, melden möchten.

Dabei gilt zu beachten: Eine VDP ist ein passiver Ansatz: Sie bietet einen sicheren Kommunikationskanal für jeden, der in guter Absicht einen Fehler melden möchte. Im Gegensatz dazu ist Bug-Bounty ein proaktiver Ansatz: Unternehmen laden ethische Hacker ein, Schwachstellen nach streng definierten Regeln zu identifizieren und zu melden. Dafür erhalten diese dann eine vorher festgelegte, finanzielle Vergütung.

Ein klar definierter Prozess

Damit die Zusammenarbeit zwischen Hackern und Unternehmen funktioniert, braucht es rechtlich verbindliche Richtlinien, die öffentlich kommuniziert werden und zu denen sich Organisationen a priori verpflichten: eine VDP. Diese definiert einen klaren Prozess und schafft für die Hacker einen rechtlich sicheren Rahmen, um Schwachstellen an ein Unternehmen zu melden. Gerade weil unkoordinierte Schwachstellenmeldungen in der Vergangenheit oft als Angriffsversuch missverstanden wurden, nehmen ethische Hacker das Risiko nicht auf sich. Eine VDP sorgt hier für Sicherheit und zeigt auf, wie und wo der Hacker seinen Bericht einreichen kann.

Rayna Stamboliyska
www.yeswehack.com

PASSWORT-RICHTLINIEN?

SCHUTZ ODER RISIKO?

Während sich das BSI von lang gehegten Passwortregeln wie der Angabe einer exakten Mindestlänge verabschiedet, stellen sich Unternehmen sowie Sicherheitsexperten die Frage: „Wann schaden Passwort-Richtlinien mehr als sie nützen?"

Wenn es um die sichere Erstellung und Verwaltung von Passwörtern geht, kann der Einzelne schnell überfordert sein. Gerade einmal jeder dritte wechselt deshalb sein Passwort regelmäßig. Je mehr Regeln noch hinzukommen, desto höher wird die Wahrscheinlichkeit, dass Mitarbeiter vor diesem fast schon unzumutbaren Passwörter-Regelwerk kapitulieren.

„Man nehme pro Person 15 Online-Zugänge, hierfür jeweils ein 12-stelliges Passwort, rüste es mit „x" Sonderzeichen und Co. auf, fordere alle 3 Monate einen Passwort-Wechsel an und entferne all Post-its in greifbarer Nähe ... Schon ist das Passwort-Chaos in Unternehmen vorprogrammiert!"

Es wird zu unsicheren Mitteln gegriffen, die unter dem Radar der IT ablaufen: Aktuellen Statistiken des Marktforschungsunternehmens Ipsos zufolge, merkt sich jeder Zweite sein Passwort selbst und fast jeder Fünfte schreibt es sogar im Klartext auf.

Als Folge greifen Empfehlungen wie ein regelmäßiger Passwort-Wechsel ins Leere, da es Mitarbeitern ohne notwendige Tools und Abläufe überhaupt nicht möglich ist, regelkonform zu handeln. Wenn diese daraufhin ihr Passwort nur leicht abwandeln, um es sich weiterhin merken zu können, wurde das Sicherheitsrisiko nicht umgangen, sondern nur verschlimmert: Diese gängigen Muster kennen auch Hacker und können auf Basis von Algorithmen das neu gesetzte Passwort sogar noch schneller knacken.

Warum Richtlinien trotzdem unabdingbar sind

Richtwerte können sogar kontraproduktiv sein, wenn Hacker diese ausspähen und so wichtige Tipps zum Konstrukt des Passworts erhalten. Dass das BSI deshalb keine präzisen Vorgaben mehr nennt, um Hacker lieber im Dunklen tappen zu lassen, bedeutet allerdings nicht, dass Unternehmen diese intern nicht selbst definieren und in einem Password Management Tool sicher verwalten sollten.

Dazu kommt: Je länger ein Passwort unverändert genutzt wird, desto größer ist die Gefahr einer Kompromittierung. Theoretisch könnten sich bereits Hacker im Unternehmen befinden, die durch das regelmäßige Neusetzen erfolgreich ausgesperrt würden.

Lassen Sie Ihre Mitarbeiter nicht im Stich!

Die „Berufshacker" Tim Schughart & Immanuel Bär von ProSec sehen die jüngste Empfehlung des BSI als eine Art Resignation mit positiver Intention: „In unserem Alltag als Pentester müssen wir täglich feststellen, dass keiner unserer Kunden – darunter auch Regierungen – unsere Angriffe zu 100 Prozent detektieren konnte." Denn nur die wenigsten würden den Verlust ihrer Logindaten überhaupt bemerken. Prosec und MATESO sehen daher User Awareness Schulungen in Verbindung mit einem Password Manager als essentiell an.

Password Guidelines sind also längst nicht passé, sondern ein notwendiger Schutz – sinnvoll angewandt. Das Abraten vom Passwort-Wechsel trifft deshalb nicht den Kern des Problems und kann sogar dazu führen, dass noch schlechtere Passwörter über einen längeren Zeitraum verwendet werden und Hackern so mehr Zeit geben, sie zu entwenden.

Definieren Sie klare Password Guidelines, die mit einem Password Management System praktisch umgesetzt und überwacht werden können. Dabei sollte das Password Management nie in den Händen von Einzelpersonen liegen, sondern – inklusive Passwort-Wechsel – automatisiert ablaufen. Im besten Fall kennt der eigene Mitarbeiter dabei seine Passwörter nicht einmal und loggt sich via Single-Sign-on automatisch ein!

Thomas Malchar | www.passwordsafe.de

MATESO PASSWORD SAFE

ERFOLGREICHE HACKS FRÜHER ERKENNEN

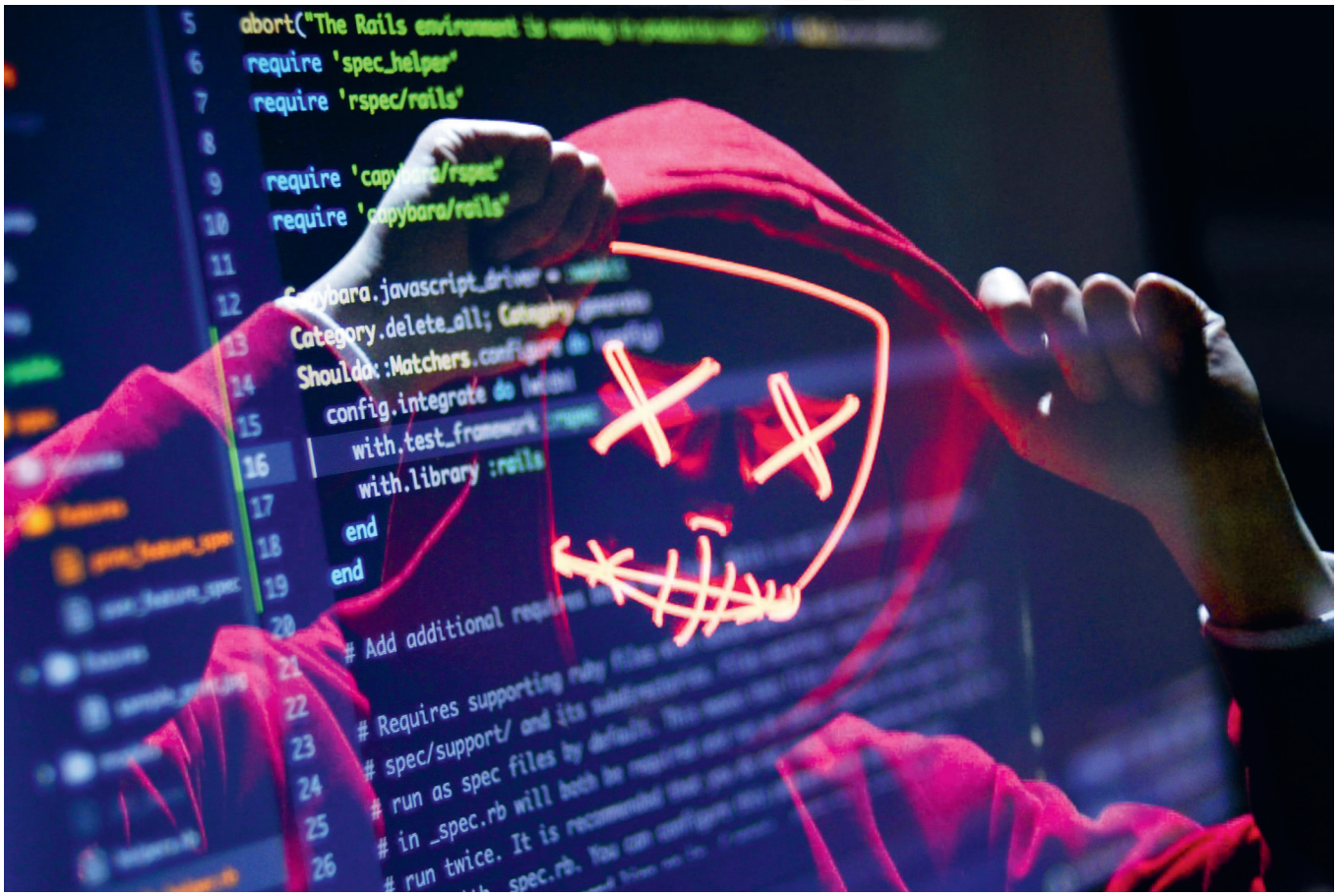
DIE VERHALTENSANALYSE MACHT'S MÖGLICH

Nach einem erfolgreichen Hack verbringen Cyberkriminelle - halten Sie sich fest - im Schnitt 56 Tage in ihrer Zielumgebung. Mitunter werden sie von der IT-Sicherheit erst nach Monaten oder Jahren entdeckt. Die „Dwell-time" zu verkürzen, also die Verweildauer in Netzwerk, ist für die meisten Sicherheitsteams ein massives Problem, weil diese bereits mit der Aufgabe überwältigt sind Angriffe abzuwehren.

In Filmen werden Hacks oft als eine Art digitaler Bankraub dargestellt: Die Hacker durchbrechen die Schutzmechanismen ihres Ziels auf dramatische Weise und haben dann nur wenige Minuten, um die begehrten Daten zu stehlen, während die IT-Sicherheit verzweifelt versucht die Angreifer zu stoppen. Die Realität sieht ganz anders aus, denn tatsächlich machen es sich die Cyberkriminellen meist im Netzwerk gemütlich und verbringen dort mitunter Monate oder Jahre, bevor sie entdeckt werden. Wer so viel Zeit hat, kann natürlich sehr großen Schaden anrichten und die Verweildauer, auf Englisch „Dwell time" genannt, ist bei der Analyse von erfolgreichen Hacks eine der wichtigsten Indikatoren, um festzustellen, wie schwerwiegend ein Angriff war. In vielen Fällen können bereits wenige Stunden Zugriff zu einer Kompromittierung erheblicher Datenmengen führen.

Angreifer machen es sich gemütlich

In einem kürzlich erschienenen Bericht lag der globale Mittelwert der Dwell Time von Cyberkriminellen vor ihrer Entdeckung bei 56 Tagen. Dieser Wert war zwar deutlich besser als der des Vorjahres, als die Angreifer noch satte 78 Tage Zeit hatten, bevor sie entdeckt wurden. In einigen Fällen blieben Verstöße jedoch mehrere Jahre lang unentdeckt, was für alle Beteiligten schwerwiegende Folgen



hatte. Einer der Gründe dafür, dass Angriffe so lange unentdeckt bleiben können, ist die zunehmende Ausdehnung der Netzwerke der meisten Organisationen. Je größer, verstreuter und unorganisierter solche Netzwerke werden, desto leichter fällt es Kriminellen, im Verborgenen zu bleiben.

> OFFENBAR IST ES UM DIE FERTIGKEITEN UND EINGESETZTEN LÖSUNGEN IN VIELEN UNTERNEHMEN NICHT GUT BESTELLT, WENN ANGREIFER IM SCHNITT GUT ZWEI MONATE ZEIT HABEN ES SICH IN EINER ZIELUMGEBUNG BEQUEM ZU MACHEN.
>
> Egon Kando, Regional Sales Director Central & Eastern Europe, Exabeam, www.exabeam.com

Einmal angekommen, navigieren die Angreifer unentdeckt durch das Netzwerk und scannen und exfiltrieren dabei Daten. Für Unternehmen, die sensible Kunden- oder geheime Forschungsdaten vorhalten, ist es natürlich ein Albtraum sich vorzustellen, dass sich Angreifer Monate oder gar Jahre unerkannt im Netzwerk aufhalten können. Wie schwerwiegend solche lang andauernden Datenlecks für die betroffenen Unternehmen sind, belegen zahlreiche Beispiele.

Der Albtraum der IT-Sicherheit

Es gibt unzählige Beispiele von Unternehmen, die Opfer von erfolgreichen Hacks wurden, deren Schäden in die Milliarden gingen. Der US-amerikanische Finanzdienstleister Equifax verlor nach Bekanntwerden eines großen Datenlecks 2017 beispielsweise 35 Prozent seines Börsenwerts, musste einen immensen Rufschaden hinnehmen und mehr als eine halbe Milliarde US-Dollar an Strafen bezahlen. Legendär, und in Sachen Verweildauer fast schon unerreicht, ist auch der Fall von Cathay Pacific aus dem Jahr 2018, bei dem 9,4 Millionen Passagierdaten kompromittiert wurden.

Cathay Pacific brauchte mehr als sechs Monate für die Untersuchung, die eine Reihe schockierender Enthüllungen aufdeckte: Der früheste bekannte Zeitpunkt des unbefugten Zugriffs auf das Netzwerk war fast vier Jahre alt, nämlich im Oktober 2014. Die Angreifer waren also ganze vier Jahre unentdeckt im Netzwerk! Und als wäre dies für Cathay Pacifics IT-Sicherheit nicht schon peinlich genug, war die Schwachstelle, über die die Angreifer eingedrungen waren, einfach auszunutzen und darüber hinaus sogar längst öffentlich bekannt.

Beide Fälle dienen als Warnungen dafür, was im schlimmsten Fall geschehen kann und als Beispiel, dass der Schaden begrenzt werden kann, wenn die Verletzung der IT-Sicherheit so früh wie möglich erkannt wird. Dabei hat sich längst die Erkenntnis breitgemacht, dass jedes Unternehmen angreifbar und es nur eine Frage der Zeit ist, bis eine Sicherheitsverletzung auftritt. Damit stellt sich die Frage, welche Lösungen und Fertigkeiten die IT-Sicherheit benötigt um diese böswilligen Aktivitäten so frühzeitig wie möglich erkennen zu können.

Frühwarnsystem

Offenbar ist es um die Fertigkeiten und eingesetzten Lösungen in vielen Unternehmen nicht gut bestellt, wenn Angreifer im Schnitt gut zwei Monate Zeit haben es sich in einer Zielumgebung bequem zu machen. Bei der Aufgabe, Angriffe entweder ganz zu verhindern oder die Verweildauer zu verkürzen, stehen viele Sicherheitsteams auf ziemlich verlorenem Posten. Denn viele gängige Sicherheitslösungen produzieren vor allem eines: Fehlalarme. Um die Flut von Alarmen manuell abzuarbeiten, müssen die Teams viel Zeit aufwenden. Dies lässt, wenn überhaupt, wenig Zeit sich mit dem noch längeren Prozess zu beschäftigen, Angreifer aufzuspüren, die es bereits ins Netzwerk geschafft haben, und diese zu beseitigen.

Eine Technologie, die deutliche effektiver ist als die manuelle Bewertung von Sicherheitswarnungen, ist die Verhaltensanalyse. Sie kann dabei helfen, verdächtige Benutzer- oder Netzwerkaktivitäten effektiver zu identifizieren. Lösungen zu Verhaltensanalyse nutzen bereits bestehende Logs für Sicherheitsvorfälle, was bedeutet, dass sie bereits den vollen Umfang und Kontext der zugehörigen Ereignisdetails kennen. Infolgedessen müssen Sicherheitsanalytiker nicht mehr eine große Anzahl von Ereignisprotokollen durchforsten, um von Hand Zeitleisten für Vorfälle zu erstellen. Durch den Wegfall dieses zeitaufwändigen Prozesses lassen sich potenzielle Sicherheitsverletzungen viel schneller erkennen, wodurch die Sicherheitsteams Angreifern schnell auf die Spur kommen und die Verweildauer der Angreifer praktisch eliminiert wird.

Analyse des Verhaltens

Moderne Datenschutzbestimmungen sind strenger denn je, was bedeutet, dass Unternehmen es sich einfach nicht mehr leisten können, in Sachen Datensicherheit selbstgefällig zu sein. Aber da die Netzwerke heute größer und verstreuter sind als je zuvor, ist es unrentabel geworden, sie mit traditionellen Sicherheitswerkzeugen und manueller Analyse zu schützen. Neue Technologien, wie etwa die fortschrittliche Verhaltensanalyse, machen die zeitraubende Kleinarbeit, die ältere Tools erfordern, überflüssig, vermeiden Fehlalarme und helfen echte Bedrohungen viel früher zu erkennen.

Egon Kando

PRIORITÄTEN RICHTIG SETZEN

RISIKOBASIERTER ANSATZ BEIM PATCH-MANAGEMENT

DURCH SCHWACHSTELLEN-MANAGEMENT MIT EINEM RISIKOBASIERTEN ANSATZ UND EINER UEM-LÖSUNG SIND ORGANISATIONEN ANGEMESSEN GEGEN ZUKÜNFTIGE ANGRIFFE GEWAPPNET.

Alexander Haugk, Senior Product Manager, baramundi software AG, www.baramundi.com

Gefühlt häufen sich die Meldungen über Hackerangriffe, die bei namhaften Unternehmen erfolgreich bekannte Schwachstellen ausgenutzt haben. So geschehen Anfang des Jahres bei WhatsApp: Eine Schwachstelle in der App ermöglichte es Hackern, mit einem einfachen SMS-Text auf Dateien der Opfer zuzugreifen. Bei solchen klaffenden Sicherheitslücken stellt sich die Frage, was diese Unternehmen sonst noch alles bisher übersehen haben und wieso diese Unmengen an Nutzern und Nutzerdaten nicht besser geschützt sind.

Auch wenn WhatsApp diese Lücke geschlossen hat, macht der Vorfall eine Diskussion über die richtige Strategie beim Schwachstellenmanagement nötig. Ein kürzlich veröffentlichter Gartner-Bericht untersuchte die Verbreitung von Bugs seit Anfang der 2000er Jahre. Darin wurde festgestellt, dass die Zahl der öffentlich bekannt gemachten Schwachstellen von 2006 bis 2016 um über 30 Prozent gestiegen ist. Für die IT-Infrastruktur stellen viele dieser bekannten Sicherheitslücken eine massive Gefahr dar.

Risiko abschätzen

IT-Teams haben häufig den Ehrgeiz, „immer und überall alles zu patchen". Dieser Ansatz ist zwar lobenswert und birgt ein inhärentes Risiko: Indem man versucht alle erkannten Schwachstellen gleichrangig zu beheben, bleiben kritische Lücken deutlich länger offen. Aber gerade solche, allgemein bekannten, aber nicht gepatchten Schwachstellen sind ein vorrangiges Ziel von Cyberangriffen.

Eine deutlich effektivere und kostengünstigere Patching-Strategie besteht darin, sich zuerst auf die größten Risiken zu konzentrieren. Laut der Gartner Studie gibt es etwa 50 bis 300 Hochrisiko-Schwachstellen pro Jahr, wie sie das Common Vulnerability Scoring System (CVSS) definiert. Auf Basis dieser Informationen, sollten IT-Teams dann untersuchen, welche dieser aufgeführten Schwachstellen in ihrem Unternehmen am ehesten ausgenutzt werden können. Als Ergebnis erhält man dann die Fälle, denen sich das Team mit Hochdruck widmen sollte.

Leichter gesagt als getan

Diese ziemlich offensichtliche Lösung ist den meisten IT-Teams bereits bekannt. Mit der Umsetzung ist es aber leichter gesagt als getan: Ebenso wie die „Alles Patchen" Strategie ist auch die Auseinandersetzung mit der CVSS-Einstufung zeitaufwändig und für kleine IT-Teams nicht immer möglich. Hinzu kommt, dass Patches an kritischen Systemen nicht nur verteilt, sondern vorher auch auf ihre Kompatibilität getestet werden sollten. Ein großflächiges Patch Roll Out, das die Office IT lahmlegt, kann sonst leicht mehr Schaden anrichten, als es verhindert.

Security Automation durch UEM

Gegen diesen Zeitmangel kann ein Unified Endpoint Management (UEM) Abhilfe schaffen. Durch Automatisierung beim Finden von Schwachstellen und Verteilen der entsprechenden Patches kann die benötigte Zeit für die Risikoabschätzung und das Testen der Patches gewonnen werden. Im Idealfall ist es damit dann auch möglich, alle nicht-kritischen Bugs zeitnah zu patchen.

Durch Schwachstellenmanagement mit einem risikobasierten Ansatz und einer UEM-Lösung sind Organisationen so angemessen gegen zukünftige Angriffe gewappnet.

Alexander Haugk

CYBERSECURITY

OPTIMIERUNG TROTZ RESSOURCENKNAPPHEIT? DAS GEHT!

In einer Welt mit COVID-19, in der sich unser Leben und unser Arbeiten zunehmend online abspielen, ist Cybersicherheit wichtiger denn je. Eine direkte Auswirkung der Pandemie auf CISOs besteht darin, dass sie Kosten für Cybersicherheit immer schwieriger vorhersehen können. Die Pandemie zwingt Unternehmen, ihre digitale Transformation noch schneller voranzutreiben. Gleichzeitig besteht weiterhin das Gebot zu sparen. Dazu kommt das Problem, qualifizierte IT-Security-Fachkräfte zu rekrutieren.

Zu Recht stellen sich daher viele CISOs aktuell die Frage, wie der Status quo der Cybersicherheit ihres Unternehmens mit knappen finanziellen und personellen Ressourcen aufrechterhalten oder sogar verbessert werden kann.

So profitieren Sie von Bug Bounty
Ein effizienter Weg ist die Suche nach Schwachstellen per Bug-Bounty-Programm, das in nur wenigen einfachen Schritten aufgesetzt werden kann. Die Schwachstellensuche läuft exakt nach von Ihnen vordefinierten Regeln ab. Sie erhalten meist schon am Tag des Programmstarts umfassende Berichte, müssen aber nur für den jeweils zuerst eingetroffenen Bericht bezahlen, sofern er Ihren Kriterien genügt.

Mehr Informationen unter www.yeswehack.com

IHRE VORTEILE VON BUG BOUNTY

- **Geschwindigkeit:** Reduzieren Sie die Zeit bis zur Erkennung und Behebung von Schwachstellen.
- **Agilität:** Richten Sie Ihre Sicherheitstests an Ihren Lieferterminen aus.
- **ROI:** Kontrollieren Sie Budget, Dauer, Umfang und Tiefe der Tests.
- **Vertrauen:** Zeigen Sie Ihren Kunden Ihr Engagement für die Sicherheit.
- **Empowerment:** Von der Expertise der YesWeHack-Community aus 17.000 ethischen Hackern profitiert Ihr internes IT-Team auch direkt!

PROTEKT 2020

SPANNENDES KONFERENZPROGRAMM MIT HOCHAKTUELLEN THEMEN

Die protekt findet wie geplant am 10. und 11. November 2020 in Leipzig statt. Das Programm der Konferenz für den Schutz kritischer Infrastrukturen widmet sich einem breiten Spektrum aktueller Themen aus den Bereichen IT-Sicherheit und physischer Schutz. Vor allem Fragestellungen, die sich im Zuge der Corona-Pandemie ergeben haben, werden ausführlich behandelt. Für die Sicherheit aller Konferenzteilnehmer sorgt ein bestätigtes Hygienekonzept, das unter anderem eine Begrenzung der Teilnehmerzahl auf 225 Tickets vorsieht.

Die protekt ist die einzige Konferenz in Deutschland, die sich dem Schutz kritischer Infrastrukturen widmet und dabei gleichermaßen die IT-Sicherheit und den physischen Schutz thematisiert. In Plenarvorträgen, zwei Vortrags-Tracks und einem Workshop-Track wird eine enorme inhaltliche Bandbreite abgedeckt - von gesetzlichen Rahmenbedingungen über Schwerpunktthemen für einzelne KRITIS-Sektoren bis hin zu Praxisbeispielen. Ein Get-Together am ersten Abend bietet allen Teilnehmern zudem die Möglichkeit zum Fach- und Erfahrungsaustausch.

Zu den Highlights der diesjährigen protekt zählen eine Keynote von Prof. Dr. Lothar H. Wieler, Präsident des Robert Koch-Instituts, sowie die Vorstellung der KRITIS-Highlights 2020 durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Weitere spannende Vorträge widmen sich Themen wie sicheren Cloud-Lösungen, Datenschutzmanagementsystemen, rechtskonformer KI und der Umsetzung eines C4i-Systems für kritische Infrastrukturen. Ein Workshop beschäftigt sich intensiv mit wirksamem Krisenmanagement in Theorie und Praxis.

www.protekt.de

protekt
10. – 11.11.2020
leipzig

konferenz für
den schutz kritischer
infrastrukturen

SICHERHEITSLÜCKE MENSCH

UNWISSENHEIT UND ARGLOSIGKEIT ALS GRÖSSTES PROBLEM

Nachdem Twitter zuletzt vermehrt in den Medien kursierte, da das Unternehmen im Zuge der Corona-Krise all seinen Mitarbeitern Home-Office auf Lebenszeit gewähren wollte, machte es nun erneut Schlagzeilen. Von CEO-Fraud bis Spear-Phishing: Warum der aktuelle Twitter-Vorfall ein Warnschuss für viele Unternehmen ist und die Sicherheitslücke Mensch immer noch zu sehr unterschätzt wird.

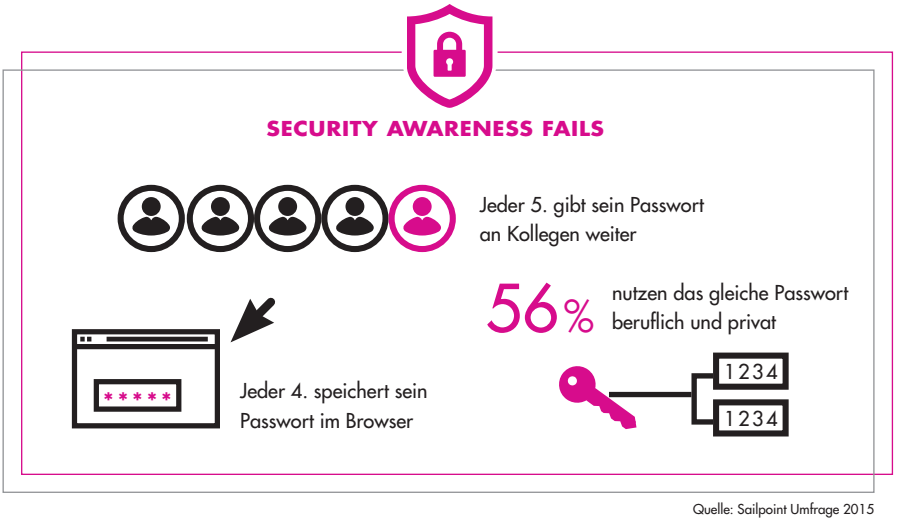
Dieser Tag hat bei Twitter Geschichte geschrieben – leider im negativen Sinne. Am 16. Juli 2020 war es Hackern gelungen, den bisher größten Angriff auf eine Social Media Plattform durchzuführen. Der Vorfall war vor allem in seinem Ausmaß und Umfang schockierend – nicht nur prominente, sondern tausende Profile waren betroffen. Auch hatte Twitter noch Stunden später mit der Wiederherstellung und vor allem damit zu kämpfen, herauszufinden, was überhaupt passiert war.

War Twitter nicht hinreichend geschützt?

Von komplexen Passwörtern bis hin zur Absicherung durch Zwei-Faktor-Authentifizierung mit einem zusätzlichen Code waren die Sicherheitsvorkehrungen der betroffenen Prominenten eigentlich überdurchschnittlich stark abgesichert.

Lag es dann also daran, dass bei Twitter zu viele Mitarbeiter Zugriff auf sicherheitskritische Daten und Konten hatten? Denn anscheinend konnten die Hacker interne Sicherheitsvorkehrungen aushebeln, um Datendiebstahl zu begehen. Nun hat Twitter in einem Blogbeitrag das Rätsel gelöst: Eine Mischung aus Social Engineering und Spear-Phishing auf einzelne Personen mithilfe von Telefonanrufen soll den Angreifern die virtuellen Tore geöffnet haben.

Auch bei einem amerikanischen Pipelinebetreiber sorgte Spear-Phishing für zwei Ausfalltage, indem zuerst trotz interner Sicherheitsvorkehrungen das firmeneigene Netzwerk durch Ransomware kompromittiert wurde, um im nächsten Schritt an Zugangsdaten zu Steuerungsanlagen zu gelangen. Die besten Sicherheits-Systeme nützen eher wenig, wenn der User anfällig für Manipulation und Täuschungsversuche ist.



Quelle: Sailpoint Umfrage 2015

IT-Sicherheit steht und fällt mit dem Mitarbeiter

Dies zeigt, dass trotz effektiver Systeme für Privileged Access und Account Management in Unternehmen ein essentieller Faktor zu sehr in den Hintergrund rücken kann – der gewöhnliche User, der zwar nicht direkt Zugriff auf wichtige Passwörter und Daten hat, aber trotzdem Bestandteil der Infrastruktur ist.

Er verwaltet also nicht den digitalen Tresor, aber vielleicht sitzt er an der Pforte im Eingangsbereich und winkt Hacker arglos durch. Haben diese erst einmal die erste Hürde ins Unternehmen genommen, ist es ein Leichtes, durch Spähattacken und Beobachtungen an notwendige Informationen zu gelangen und weiter vorzudringen.

Security Awareness als A und O

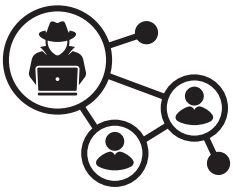
Fragt man Unternehmen, sehen zwar 67,6 Prozent die interne IT-Sicherheit durch das menschliche Fehlverhalten ihrer Mitarbeiter gefährdet (Statista Studie 2019). Jedoch nur 22,9 Prozent empfinden Social Engineering als große Cyberbedrohung. Unternehmen ist nicht klar, dass diese User dann als Einstiegstor genutzt werden können.

Die Schwachstelle Mensch beginnt bei Unwissenheit und Arglosigkeit im Umgang mit sensiblen Daten, führt über mangelndes technisches Know-how und endet mit fehlenden Anlaufstellen für deren Fragen und Belange. Nicht umsonst waren 2019 laut Bitkom 37 Prozent der Angriffsmethoden auf digitales oder analoges Social Engineering zurückzuführen.

Dazu kommt, dass sich Hacker bei ihren Angriffen oft mehreren Methoden bedienen, um das bestmögliche Ergebnis zu erzielen. Die einzelnen Attacken sind hierbei bestens verzahnt und Social Engineering ist als explosive Zutat fast immer dabei.

EIN EXPLOSIVER MIX AUS UNKENNTNIS UND TÄUSCHUNG

37% aller Cyberangiffe sind auf Social Engineering zurückzuführen.



67,7% sehen die größte Cybergefahr in menschlichem Fehlverhalten

Quelle: Web.de Online-Umfrage 2020; Bitkom Studienbericht 2018

Smart Work – eine neue Sicherheits-Challenge

Nun kommt noch eine andere Komponente ins Spiel – Smart-Work-Konzepte, die Mitarbeitern das orts- und zeitunabhängige Arbeiten ermöglichen. Ob die Home-Office-Regelung bei Twitter ihren Teil zum Sicherheitsvorfall beigetragen hat, lässt sich an dieser Stelle nur mutmaßen. Sicher ist, dass Mitarbeiter auf solch einschneidende Prozesse vorbereitet werden müssen, da das Risiko für Social Engineering sonst gerade in ungewohnter Arbeitsatmosphäre steigen kann. Laut aktuellen Berichten von Interpol hat Human Hacking besonders seit dem Ausbruch von COVID-19 weltweit zugenommen.

Gut ersichtlich ist diese Entwicklung auch an gängigen Angriffsmethoden wie CEO-Fraud, auch Chef-Betrug genannt, die im Home-Office noch zugenommen haben. Hier werden Mitarbeiter manipuliert, hohe Geldsummen zu überweisen. Die Gefahr, auf diese Tricks hereinzufallen, ist gerade für Mitarbeiter, die isoliert im Home-Office sitzen, besonders relevant.

Denn durch die physische Distanz und mangelnden Prozesse ist es nicht möglich, den Chef mal eben auf dem Flur über die gewünschte Transaktion anzusprechen. Und da soziale Interaktionen durch die physische Distanz im Home-Office eher abnehmen, steigt auch die Wahrscheinlichkeit, Mitarbeiter durch das Ausüben von Druck oder das Entgegenbringen von Wertschätzung eher manipulieren zu können. Dies bestätigt auch eine Online-Ausstellerbefragung der it-sa 2020, laut dieser fast jeder dritte von Kunden gemeldete Sicherheitsvorfall auf Social Engineering zurückzuführen ist.

Thomas Malchar,
CEO, MATESO GmbH

Vom Risiko- zum Sicherheitsfaktor

Social Engineering wird also so lange als sicherheitsrelevantes Thema bestehen bleiben, bis Unternehmen die Notwendigkeit erkennen, jeden Mitarbeiter aufzuklären, individuell zu schulen und besser in sicherheitskritische Prozesse miteinzubeziehen. Verantwortung für Systeme kann ein effizientes Werkzeug sein. Denn nur eine Kombination aus Security Awareness, regelmäßigen Schulungen und den notwendigen Tools und Prozessen zur Umsetzung der Inhalte kann die Sicherheitslücke Mensch nachhaltig schließen und das Unternehmen vor Datenmissbrauch schützen.

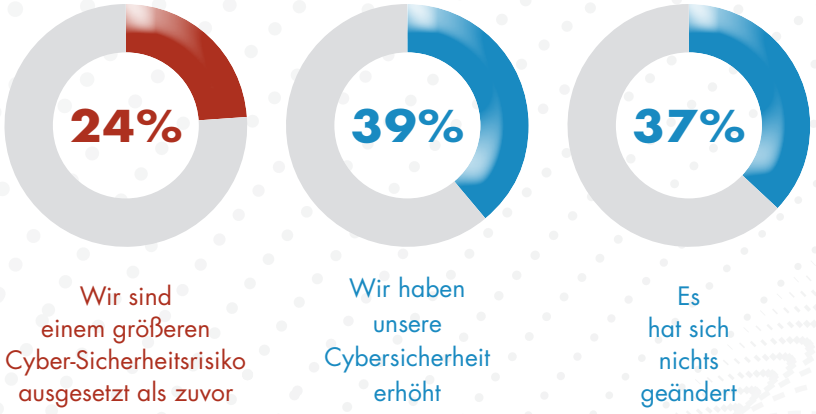
Human Hacking zeigt, dass sich jedes noch so gut durchdachte Sicherheitskonzept leicht aushebeln lässt, wenn Ihre Mitarbeiter freiwillig Passwörter oder andere Geheimnisse preisgeben. Da Hacker sich dabei immer neue Taktiken ausdenken, muss der Mensch als Schwachstelle immer wieder in den Mittelpunkt sicherheitskritischer Prozesse rücken, um sein Sicherheitsbewusstsein bestmöglich zu schärfen und Angreifern dadurch das Leben so schwer wie möglich zu machen.

Thomas Malchar | www.passwordsafe.de

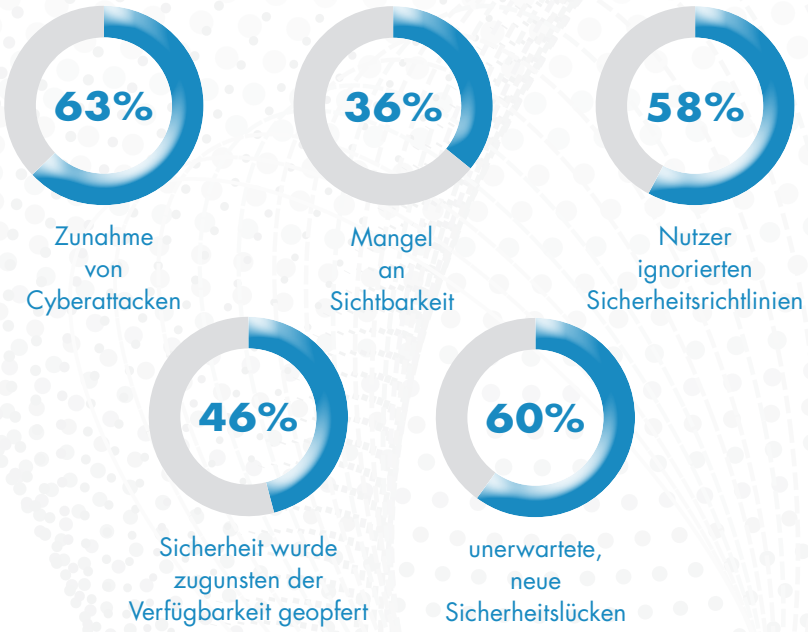
REMOTE ARBEITEN

SICHERHEIT GEOPFERT?

VERÄNDERUNG DER BEDROHUNGSLANDSCHAFT SEIT DEM ÜBERGANG ZUR FERNARBEIT/ZUM HOMEOFFICE



VON DEN 24% MELDETEN



Netwrix gab die Veröffentlichung seines 2020 Cyber Threats Report, bekannt. Der Anbieter führte diese Online-Umfrage im Juni 2020 durch, um zu verstehen, wie die Pandemie und die darauffolgenden Work-from-Home-Initiativen die IT-Risikolandschaft verändert haben.

Die Unternehmen wurden aufgefordert, die Vorfälle aufzulisten, die sie seit der Umstellung auf Remote-Arbeit erlebt haben. Die häufigsten Bedrohungsmuster hingen vom Faktor Mensch ab: Phishing (48 %), Admin-Fehler (27 %) und unsachgemäßer Datenaustausch durch Mitarbeiter (26 %).

Weitere Ergebnisse

25 Prozent gaben an, in den ersten drei Monaten der Pandemie einen Ransomware- oder anderen Malware-Angriff erlitten zu haben. 47 Prozent waren in der Lage, ihn innerhalb von Minuten zu erkennen.

Obwohl nur 14 Prozent der Unternehmen Datendiebstahl durch Mitarbeiter erlebten, sind 66 Prozent hinsichtlich dieses Szenarios besorgt. Vor der Pandemie waren es etwas mehr als die Hälfte.

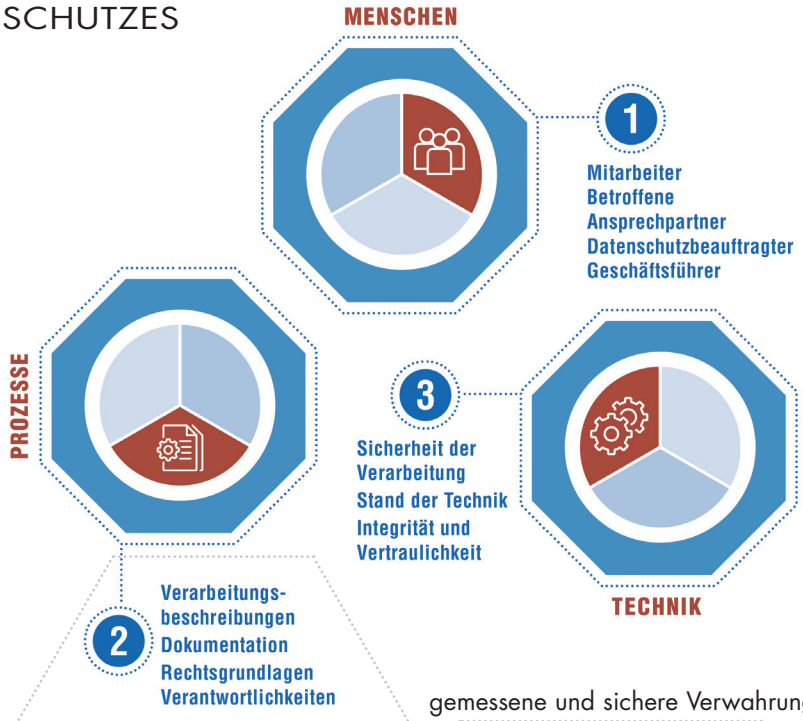
Am längsten dauerte es, Kompromittierungen in der Lieferkette zu erkennen: 55 Prozent benötigten Tage, Wochen oder sogar Monate, um diese Vorfälle zu kennzeichnen.

Die Ergebnisse der 105 deutschen Befragten zeigten, dass ein Drittel der Unternehmen in der Region (34 %) der Ansicht ist, dass sie derzeit einem höheren Cybersicherheitsrisiko ausgesetzt sind als vor der Pandemie. Entsprechend dem globalen Trend basierten die häufigsten Vorfallarten, die deutsche Unternehmen nach der Umstellung auf Remote Working erlebten, auf dem menschlichen Faktor. Tatsächlich erlitt jedes dritte deutsche Unternehmen (35 %) einen Phishing-Angriff, und jedes Vierte (25 %) meldete Vorfälle beim unsicheren Datenaustausch. Letztere waren schwierig zu erkennen, da 88 Prozent der Unternehmen Tage, Wochen oder Monate damit verbrachten, diese Vorfälle zu kennzeichnen.

www.netwrix.com

SICHER UND KONFORM

DIE DREI SÄULEN DES DATENSCHUTZES



Kleine und mittlere Unternehmen werden vermehrt mit den Herausforderungen des Datenschutzes konfrontiert – wie aber mit dem Thema umgehen, falls im eigenen Betrieb das nötige Fachwissen fehlt?

Personenbezogene Daten sind ein wertvolles und schützenswertes Gut. Oft bilden sie in Form von Leads oder Auswertungen einen wichtigen Aspekt für betriebswirtschaftliche oder strategische Entscheidungen. Doch mit der europäischen Datenschutz-Grundverordnung (EU DSGVO) müssen sie auch entsprechend sicher und konform verarbeitet werden. Wie aber sollen Unternehmen Vorgaben umsetzen, wenn ihnen die nötigen Mittel fehlen? Besonders kleine und mittlere Unternehmen (KMU) haben dafür häufig zu wenig Fachpersonal. Mit Hilfe unabhängiger Experten aber sind sie in der Lage, die drei Säulen des Datenschutzes zu meistern.

Der Mensch

Die erste Säule, auf die sich datenschutzkonformer Umgang mit personenbezogenen Daten stützt, ist der Mensch. Mitarbeiter, die im Unternehmen mit personenbezogenen Daten zu tun haben, sollten entsprechend geschult und sensibilisiert werden. Ab einer bestimmten Mitarbeiterzahl müssen Unternehmen zudem einen Datenschutzbeauftragten benennen, der nicht nur bei der Einhaltung der Vorschriften der EU DSGVO berät und diese kontrolliert, sondern auch mit der zuständigen Aufsichtsbehörde zusammenarbeitet. Dieser muss nicht im Unternehmen selbst beschäftigt sein. Externe Beratungsunternehmen bieten KMUs darum auch die Dienste eines externen Datenschutzbeauftragten an.

Die Prozesse

Als zweite Säule gilt es, die Prozesse, während derer personenbezogene Daten verarbeitet werden, zu dokumentieren und an die Vorgaben der EU DSGVO anzupassen. Das beginnt bereits bei der Sammlung von Daten, beispielsweise über die Webseite. Zwar ist es möglich, mittels Cookies gewisse Daten von Nutzern zu erfassen, allerdings muss der Anwender vorher oftmals einwilligen. Das passiert über Cookie-Banner, die beim ersten Besuch der Seite angezeigt werden. Welche Informationen darin enthalten sein müssen und wann eine Einwilligung konform ist, regelt die EU DSGVO. Ergänzend helfen Gerichtsurteile sowie Aufsichtsbehörden bei der Auslegung. Erneut kann KMUs eine unabhängige Beratung dabei helfen, den Überblick zu bewahren, Fallstricke zu erkennen und zu vermeiden.

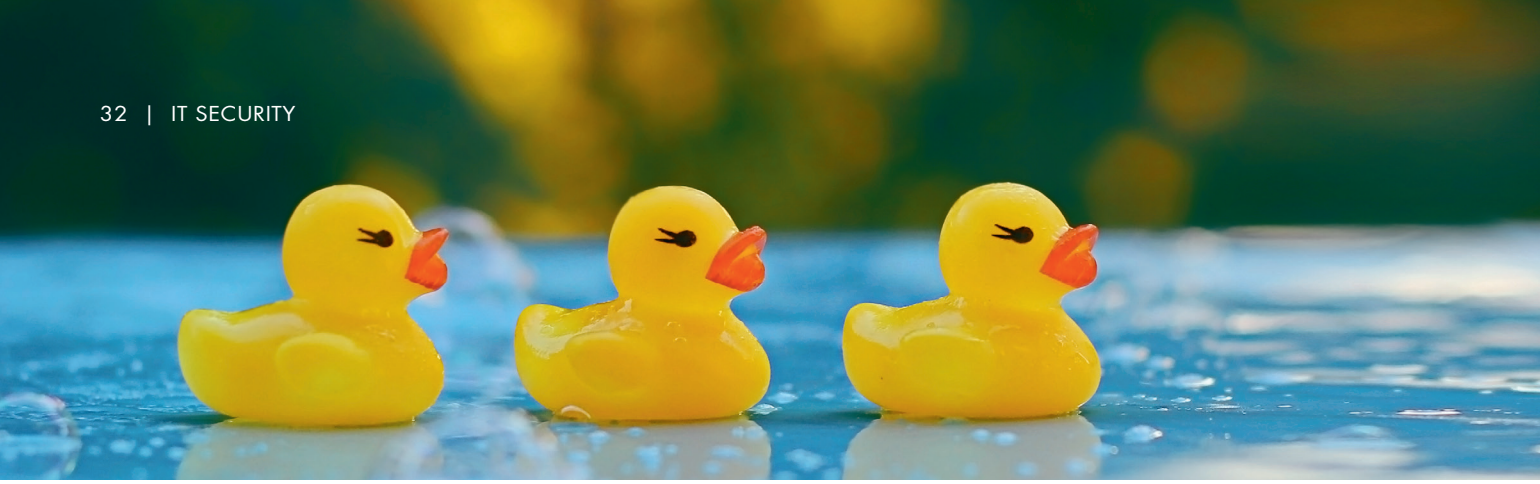
Die Technik

Die letzte Säule des Datenschutzes ist die Technik. Sie beinhaltet unter anderem die angemessene und sichere Verwahrung der Daten. Neben der grundsätzlichen Anforderung, muss auch gewährleistet sein, dass die Daten bei einem Zwischenfall wiederhergestellt werden können. Daher ist es sehr wichtig, die Technik und Systeme des Unternehmens regelmäßig zu überprüfen. Zudem sollten technische Weiterentwicklungen bedacht und Sicherheitsmaßnahmen angepasst werden.

Datenschutz gewinnt das Vertrauen der Kunden

Datenschutz-Konformität ist nicht nur eine gesetzliche Vorgabe, es wird für Kunden zunehmend zum Leistungsmerkmal. Umso wichtiger ist es, sich strategisch mit den Anforderungen der EU DSGVO auseinanderzusetzen und die drei Säulen entsprechend anzupassen. Da KMUs oft nicht die notwendigen Arbeitskräfte zur Verfügung haben, um der Herausforderung selbst zu begegnen, sollten sie auf externe Beratungsunternehmen zurückgreifen. Diese bieten entsprechende Unterstützung an und fungieren, falls benötigt, als externe Datenschutzbeauftragte.

Mareike Vogt | www.tuvsud.com



BEZIEHUNGSSTATUS: KOMPLIZIERT?

GRUNDSCHUTZ, DATENSCHUTZ UND NOTFALLMANAGEMENT

Ein Versuch der Annäherung zwischen Datenschutz, Grundschutz und Business Continuity Management (BCM) in Zeiten des Standard-Datenschutzmodells (SDM): „Gibt es Möglichkeiten, sinnvolle Synergien zwischen Datenschutz, Grundschutz und BCM herzustellen und wie kann man diese zum Wohle der jeweiligen Organisation skalieren und nutzen?"

Die drei genannten Managementsysteme besitzen auf den ersten Blick verschiedene Zielsetzungen, haben jedoch eine große Schnittmenge in Bezug auf die Mittel und Methoden zur Umsetzung der jeweiligen Regelwerke. Vor diesem Hintergrund lohnt es sich, einen Blick auf die Differenzen und die gemeinsame Basis zu werfen:

➤ Beim IT-Grundschutz liegt der Fokus auf dem Sicherheitsniveau aller (IT- gestützten) organisationseigenen Informationen. Die Risikobetrachtung erfolgt aus dem Blickwinkel der Organisation.

➤ Im BCM stehen vorrangig die für eine Organisation kritischen Prozesse und Assets und deren maximal tolerierbare Ausfallzeit im Zentrum. Hinzu kommt die Betrachtung von Risiken, welche die Aufrechterhaltung oder den abgestimmten Wiederanlauf des Normalbetriebes der kritischen Geschäftsprozesse betreffen.

SCHMERZFREIER DATENSCHUTZ IST MÖGLICH. DAFÜR HÄTTE ICH MIR IN MEINER ZEIT ALS DATENSCHUTZBEAUFTRAGTER EIN PROFESSIONELLES TOOL GEWÜNSCHT.

Daniel Linder,
Consultant, HiScout GmbH,
www.hiscout.com

➤ Im Datenschutz geht es um den Schutz personenbezogener Daten (pbD), die eine Teilmenge der oben erwähnten „organisationseigenen Informationen" sind. Für den Schutz dieser Daten werden die zugehörigen Risiken ermittelt und geeignete technische und organisatorische Maßnahmen (TOMs) zugeordnet. Der eingenommene Blickwinkel ist hier der des von der Verarbeitung Betroffenen.

Gemeinsam sind diesen drei Regelwerken die Betrachtungen der Risiken, denen Daten, (IT-) Assets und Prozesse unterliegen und die über entsprechende Maßnahmen gemindert werden. Das Management der entsprechenden Risiken soll im Idealfall die Sicherheit der organisationseigenen Systeme, der darauf befindlichen Daten und der von der Verarbeitung dieser Daten Betroffenen gewährleisten. Unterschiede ergeben sich durch die verschiedenen Perspektiven der Risikobetrachtung, die daraus abgeleiteten Interessenkonflikte in der Zielsetzung und die unterschiedliche Granularität der Schutzbedarfe. Hinzu kommt, dass im Falle des Datenschutzes ein noch größeres Augenmerk auf organisationsinterne Prozesse und Gefahren gerichtet werden muss, da die hohe Gewichtung der Betroffenenrechte nicht in Gänze durch andere Managementsysteme abgedeckt wird.

Unterschiedliche Blickwinkel

Der IT-Grundschutz und das BCM weisen hier die größte Deckungsgleichheit auf: Beide richten den Blick von der Führungsebene auf die Organisation als Ganzes. Schutzgut sind Assets und Prozesse sowie die darin vorkommenden Daten jeglicher Art. Schweregrade von Gefährdungen und Risiken sowie maxi-

Durch einen gemeinsamen Datenpool können mit HiScout sinnvolle Synergien zwischen Datenschutz, Grundschutz und BCM hergestellt, skaliert und genutzt werden.

mal tolerierbare Ausfallzeiten werden üblicherweise in drei beziehungsweise vier Kategorien eingeteilt.

Der Datenschutz weicht in seinen Bedürfnissen von den beiden vorgenannten Regelwerken ab: Für die Betrachtung der Risiken wird der Blickwinkel des Betroffenen eingenommen, es wird nur eine Teilmenge der vorhandenen Daten betrachtet und die Einteilung der Schutzbedarfe erfolgt in nur zwei Kategorien: „Hoher Schutzbedarf" (es sind pbD vorhanden) und „Sehr hoher Schutzbedarf" (es sind besondere Kategorien von pbD vorhanden).

Neben der unterschiedlichen Interessenlage der beiden Blickwinkel bei der Risikobetrachtung (Organisation versus Betroffene) liegt die größte Herausforderung für eine einheitliche Bewertung dieser Sichtweisen mit einem übergreifenden Managementsystem in den unterschiedlichen Einteilungen der Risiko- und Schutzbedarfsklassen. Hier mit einem einheitlichen System alle Bedarfe abzudecken ist vergleichbar mit dem Versuch, dreieckige Gegenstände in eine viereckige Aussparung passend einzusenken.

Integriertes Managementsystem

Am Beispiel der HiScout GRC Suite soll nun aufgezeigt werden, wie man trotz der genannten Herausforderungen die drei Bereiche IT-Grundschutz, BCM und Datenschutz in einem integrierten Managementsystem (IMS) sinnvoll und für die Organisation nutzenbringend vollumfänglich abdecken kann. Es wird gezeigt, dass sich der aus der Kombination der drei Bereiche ergebende Nutzen skalieren lässt und somit ein deutlicher Mehrwert durch den Einsatz eines einzelnen, übergreifenden Tools generiert werden kann.

Nutzt man eine einzige, der gesamten Applikation unterliegende Datenbasis, also einen Datenpool, bringt dies zunächst den Vorteil, dass man die gesamten betrachteten Stammdaten der Organisation wie Geschäftsprozesse, Daten, Anwendungen, Systeme etc. nur ein einziges Mal pflegen muss. Des Weiteren wird sichergestellt, dass in allen Systemen mit kongruenten Daten und Bewertungen gearbeitet wird. Beim Thema Risikobewertung kann der Datenschutz durch Zugriff auf die detailliert gepflegten Risikoregister der Module BCM und IT-Grundschutz aus dem Vollen schöpfen. Durch die im BSI Standard 200/2, „CON.2.A1 Umsetzung Standard-Datenschutzmodell" geforderte Umsetzung des Standard-Datenschutzmodells (SDM) bietet sich nun die hervorragende Möglichkeit, die Differenz der verschiedenen Einteilungen der Schutzbedarfe positiv zu nutzen: Die risikobasierten Teile des Datenschutzmanagementsystems folgen der Vierteilung der Risiko- und Schutzbedarfsgrade. Hier ist vor allem die Vorbereitung der Datenschutz-Folgenabschätzung (DSFA) zu nennen und die Schwellwertanalyse zur DSFA, die in HiScout komplett SDM-konform aufgesetzt ist. Die eigentliche Durchführung der DSFA wiederum basiert auf der dem Datenschutz inhärenten Zweiteilung in „hohen" und „sehr hohen" Schutzbedarf. Dabei kann der die DSFA durchführende Datenschützer die feingranulare Einschätzung der im Programm auf Basis der Daten aus BCM und Grundschutz erstellten Risikomatrix nutzen. Er kann diese mit den vom Programm ausgegebenen Bruttorisiken aus der Vorbereitung der DSFA subsummieren und in einer freitextlichen Einschätzung den vorhandenen Schutzbedarfen (hoch / sehr hoch) zuordnen. Eine abschließende Einschätzung der Verarbeitungstätigkeit wird am Ende dieses Prozesses dann aus der Gesamtsicht abgegeben. Die Differenz der verschiedenen Managementsysteme wird hier von einer Herausforderung zu einem Vorteil gewandelt.

Perspektivwechsel

Auch die im Datenschutz relevanten TOMs können direkt aus dem Pool der im BCM und/oder Grundschutz gepflegten Maßnahmen ausgewählt werden und müssen nicht „neu erfunden" werden. Die unterschiedliche Zuordnung der relevanten TOMs zu den im Datenschutz relevanten Verarbeitungstätigkeiten ermöglicht sowohl den Perspektivwechsel hin zum Betroffenen als auch die Betrachtung der Risiken aus Sicht des Verantwortlichen. So können im Datenschutz entweder nur Risiken aus Sicht des Betroffenen betrachtet werden oder alle Risiken aus Sicht des Verantwortlichen. Bei diesem sind die Risiken für die Betroffenen eine Teilmenge (realisierte Risiken des Betroffenen sind Schäden des Verantwortlichen).

Je größer und komplexer die Organisation ist, die die drei Bereiche abdecken möchte, desto lohnender wird ein einheitliches Datenmodell wie zum Beispiel in HiScout: Es reduziert Komplexität, vermeidet Fehler und Redundanzen und ermöglicht den Sprung im Blickwinkel und damit die Einpassung des dreieckigen Gegenstands in die viereckige Aussparung.

Daniel Linder

TOR, DARKNET UND DIE ANONYMITÄT

EIN HOCH AUF DIE PRIVATSPHÄRE

Die Berichterstattung zum Tor-Netzwerk konzentriert sich in Mainstream-Medien im Allgemeinen auf das Dark Web und die damit verbundenen kriminellen Aspekte wie beispielsweise den Ankauf von Drogen und Waffen. Aber wer nutzt Tor sonst noch und warum?

Das Tor-Projekt (The Onion Router) ist eine Non-Profit-Organisation, die Menschen dabei unterstützt, ihre Menschenrechte zu wahren und Freiheit zu fördern. Dazu entwickelt es Tools und Technologien, die Privatsphäre und Anonymität gewährleisten und Verfolgung, Überwachung und Zensur verhindern sollen. Und es gibt noch einen weiteren Aspekt. Die Technologie des Tor-Projekts soll dazu beitragen, den Menschen eine Stimme zu verleihen, für die das ohne diese Software-Unterstützung kaum möglich wäre, wie etwa Reporter und Korrespondenten in Ländern, die Zensur ausüben und Medienvertreter ins Gefängnis bringen oder mit dem Tod bedrohen.

Tor dient auch dazu, Menschen zu schützen, die Opfer von Misshandlung und häuslicher Gewalt geworden sind und vor Partnern oder anderen Peinigern fliehen mussten. Verfolgte haben so die Möglichkeit, weiterhin mit Freunden und Familie zu kommunizieren, ohne dass man sie ohne Weiteres ausfindig machen kann.

Vor- und Nachteile

Seit den Enthüllungen von Edward Snowden sichert Tor auch die Kommunikation von Internetnutzern, die großen Wert auf ihre Privatsphäre legen, beispielsweise vor dem Ausspionieren durch Behörden. Eines der häufigsten Einsatzgebiete von Tor, ist es, das Tracking von Browser-Aktivitäten zu verhindern. Google und Facebook etwa erstellen Profile ihrer Nutzer, um sie mit auf die Interessen des Anwenders zugeschnittener Werbung zu versorgen und diesen Dienst an möglichst viele Firmen weltweit zu vermarkten.

Aber auch wenn die Tor-Technologie mit den besten Absichten für eine allgemeine öffentliche Nutzung entwickelt worden ist, Missbrauch lässt sich nicht ausschließen. Das Silk Road Darknet-Portal ist wohl einer der bekanntesten Fälle, den Mainstream-Medien in großer Zahl aufgegriffen haben. Leider muss man davon ausgehen, dass es immer wieder Beispiele für den Missbrauch von Tor geben wird. Es ist natürlich richtig, dass Tor Networks eines der anonymisierenden Netzwerke ist, die den Zugriff auf das Dark Web ermöglichen. Und vermutlich ist es wohl auch das am häufigsten genutzte. In Bezug auf den Begriff des „Dark Web" kommt es allerdings immer wieder zu Missverständnissen.

Der Zweck eines Dark Web besteht nicht genuin darin, Ihnen Zugang zu Drogen, Hacking-Tools oder anderen „interessanten" Angeboten am Rande oder außerhalb der Legalität zu verschaffen. Das sind unerfreuliche Nebenprodukte

(gleichwohl attraktiv, gerade für die Mainstream-Berichterstattung). Der eigentliche Sinn und Zweck sind aber ein anderer. Das Dark Web bietet vielmehr denjenigen Privatsphäre und Anonymität, die aufgrund von Zensur ihre Meinung nicht frei äußern können. Es gibt Usern die Möglichkeit, in Kontakt zu bleiben, wenn ihnen übliche Technologien oder Kommunikationskanäle verwehrt sind. Das Dark Web ist kein bösartiges Netzwerk, sondern zunächst einmal ein Ort, der Anonymität erlaubt und Privatsphäre schützt.

Der Grad von Anonymität

Wer das Tor-Netzwerk verwendet, kann grundsätzlich von einem hohen Grad an Anonymität ausgehen. Und man kann unter den angebotenen Diensten zusätzlich auf das spezielle, von Tor entwickelte Protokoll zurückgreifen, das den so genannten „Onion Service Provider" (ein Dienst im Tor-Netzwerk) und den jeweiligen Nutzer dieses Dienstes absichert. Dabei werden sämtliche Informationen über den Dienst, wie beispielsweise der Standort etc. vor dem User verborgen und umgekehrt alle Informationen über den Nutzer vor dem Dienst. Ein Tracking oder Profiling innerhalb des Netzwerks ist damit ausgeschlossen, und das allein gewährleistet einen vergleichsweise hohen Grad an Anonymität.

Aber es lassen sich auch ganz normale Internetdienste über Tor nutzen, wie etwa auf google.com zuzugreifen. Das gibt dem Nutzer beim Benutzen von Google Anonymität. Google kann nicht erkennen, wer hier gerade Dienste nutzt, weil die Anfragen von einem der vielen Knoten innerhalb des Tor-Netzwerks kommen.

Der Tor-Browser

Der einfachste Weg, auf das Tor-Netzwerk zuzugreifen, ist der Tor-Browser. Der Tor-Browser ist automatisch mit dem Tor-Netzwerk verbunden und über ihn laufen sämtliche Anfragen, das heißt, er kümmert sich automatisch um Anonymität. Als „Extra" bietet er zusätzliche Funktionen, mit denen man den Sicherheitslevel sowie den Grad der Anonymität und Privatsphäre weiter erhöhen kann. Solche Einstellungen deaktivieren beispielsweise JavaSript, Bilder und Videos, bestimmte Schriftarten, Symbole um beim Surfen im Internet oder im Dark Web ein Höchstmaß an Anonymität und Sicherheit herzustellen.

Einen „Haken" hat die Sache allerdings: der User ist allein dafür verantwortlich, die Anonymität auf dem gewünschten Level zu halten. Wenn ich das Tor-Netzwerk benutze, um meine Surfgewohnheiten vor Dienstanbietern oder Website-Trackern zu verbergen, dann muss ich natürlich vermeiden, mich bei diesen Diensten einzuloggen. Wenn ich mich zum Beispiel an meinem Google-Konto anmelde, weiß Google definitiv, wonach ich suche, auch wenn ich dazu das Tor-Netzwerk verwendet habe. Ähnliches gilt für alle Dienste, die man auf seinem Rechner oder Smartphone installiert hat: sie senken potenziell den Grad der Anonymität.

ES IST SCHWIERIG BIS UNMÖGLICH ZU ERKENNEN, WOZU JEMAND TOR BENUTZT. SOBALD ICH MICH IM TOR-NETZWERK BEWEGE, WERDEN DIE BENUTZERDATEN VERSCHLÜSSELT.

Boris Cipot, Senior Security Engineer, Synopsys Software Integrity Group, www.synopsys.com

Für ein Höchstmaß an Anonymität, müsste man sämtliche Betriebssysteme oder Software loswerden, die ein betriebssystembezogenes Tracking installiert hat. Man müsste also das Internet oder das Tor-Netzwerk quasi von einem unbeschriebenen Blatt aus zu betreten. Das funktioniert über Betriebssysteme wie Tails oder Qubes, die von einem USB-Stick aus betrieben werden. Sie laufen vollständig im Speicher, so dass man sie sicher auf einer vorhandenen Hardware betreiben kann. Beim Starten hinterlassen sie keine Spuren einer Person. Man greift dann nicht nur als anonyme Person auf das Tor-Netzwerk oder das Internet zu, sondern tut das wie von einem unbeschriebenen Blatt aus. Sobald man das Betriebssystem herunterfährt, werden alle Daten gelöscht und beim nächsten Aufruf ist das Blatt genauso unbeschrieben wie zuvor.

Zwar gibt es auch bei diesen Betriebssystemen Möglichkeiten, Dinge dauerhaft einzurichten oder Dokumente und Daten zu speichern. Dies läuft aber dem eigentlichen Zweck zuwider. Selbst wenn solche Daten verschlüsselt sind, müssen Sie genau darauf achten, welche Daten Sie speichern und noch wichtiger, welche Software Sie installieren. Zudem sollte man von diesen Betriebssystemen aus nie auf Dienste wie Facebook- oder Google Mail-Konten zugreifen. Zumindest nicht mit einem Klarnamen. Normalerweise bieten die genannten Betriebssysteme Anonymität, und das Alter Ego oder ein Pseudonym verhindern Tracking und Zensur. Aber auch hier gilt: Der Nutzer ist allein verantwortlich dafür, was genau er mit seinem Betriebssystem tut und wie sicher alles bleibt."

Können Exekutivorgane Personen auf Tor tracken?

Es ist durchaus möglich, dass Exekutivorgane wie die Polizei oder auch ein ISP oder eine Behörde wissen, wer Tor benutzt. Das ist möglich, weil der Nutzer sich mit dem Tor-Netzwerk verbinden muss, wenn er es benutzen will, und man

kann erkennen, dass jemand einen Tor-Knoten hostet. Allerdings ist es schwierig bis unmöglich zu erkennen, wozu jemand Tor benutzt. Sobald ich mich im Tor-Netzwerk bewege, werden die Benutzerdaten verschlüsselt. Die Daten oder zum Beispiel eine Website-Anfrage passieren drei Knoten im Tor-Netzwerk, bevor sie das Tor-Netzwerk verlassen, um eine Verbindung mit dem gewünschten Dienst oder eine Verbindung zum Onion Service im Tor-Netzwerk herstellen.

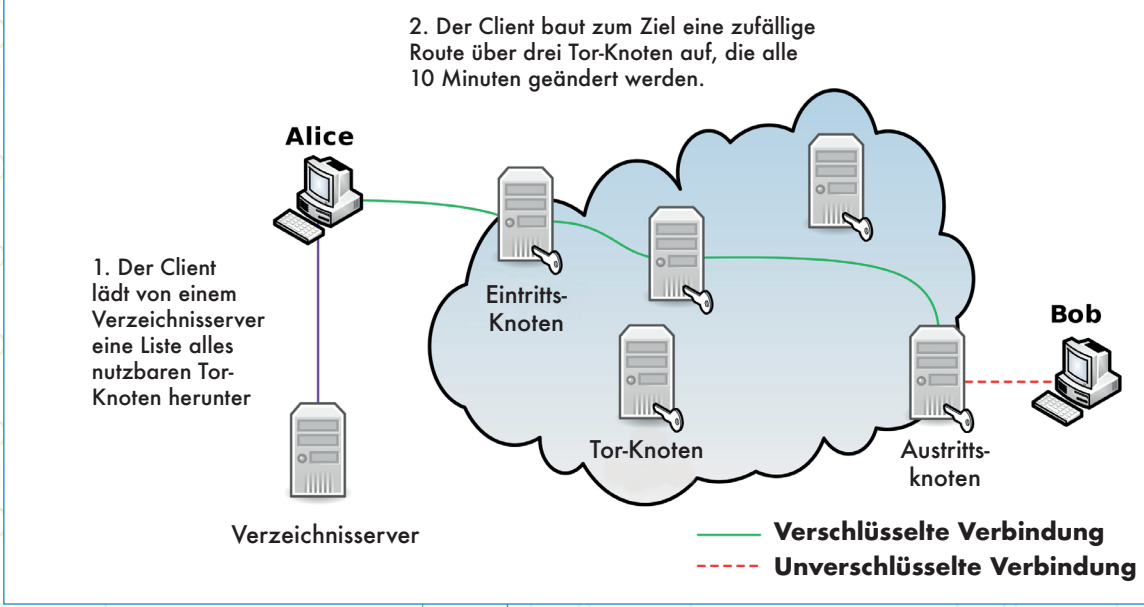
Die Server im Tor-Netzwerk erkennen nicht, woher die Anfrage kommt, und so ist es nicht möglich die Daten zu einem bestimmten User zurückzuverfolgen. Selbst wenn jemand über die nötigen Ressourcen verfügen würde, um nachzuverfolgen, was genau im Tor-Netzwerk geschieht, wäre dies aufgrund der Verschlüsselung der Daten und Vielzahl von Tor-Knoten im Netzwerk nicht möglich. Es sind zwar Fälle von Sicherheitsverletzungen gegen das Tor-Netzwerk bekannt geworden. Dabei wurden Knoten eingerichtet wurden, um das Verhalten der Benutzer zu tracken oder auszuspionieren. Aber das Tor Network behält seine Knoten genau im Auge, um zu verhindern, dass solche „Fake"-Knoten im Netzwerk auftauchen.

Zensur und ihre Folgen

Und dann ist da noch die Zensur. Wenn Behörden, Polizei oder ein ISP wissen, dass jemand Tor nutzt, können sie Verbindungen zum Tor-Netzwerk zu blockieren. Es gibt zwei Möglichkeiten, das zu verhindern. Die erste ist, einen VPN-Client zu verwenden. Dabei verbindet man sich zunächst mit dem VPN-Provider und greift von dort aus auf das Tor-Netzwerk zu. Die Verbindung vom Computer des Benutzers zum VPN-Anbieter ist verschlüsselt. Ein ISP oder eine Behörde kann nicht erkennen, dass jemand versucht, Tor zu nutzen. Es ist unnötig zu erwähnen, dass man dazu auf einen seriösen VPN-Anbieter angewiesen ist, der den Datenverkehr nicht protokolliert. Um die Verschlüsselung weiterhin zu schützen und Daten vor dem VPN-Anbieter zu verbergen, ist HTTPS Everywhere geeignet. Wenn man eine Zensur umgehen will, kann man auch auf die Tor-eigene Funktion „Bridges" zurückgreifen. In diesem Fall verbindet man sich zunächst mit einem Server außerhalb des Tor-Netzwerks, und dieser Server verbindet den Nutzer dann seinerseits mit dem Tor-Netzwerk.

Aber selbst, wenn die Tor-Technologie mit Netzwerk, Browser und Bridges die Privatsphäre und Anonymität schützt, selbst wenn Betriebssysteme wie Tails oder Qubes die Anonymität auf ein höheres Level schrauben und selbst, wenn man mehrere Verschlüsselungsebenen herstellt, muss man darauf achten nicht die kleinste Spur zu hinterlassen, die jemanden zur wahren Identität eines Benutzers führt oder einer Möglichkeit, die Aktivitäten dieses Nutzers nachzuvollziehen.

Boris Cipot



Alice erzeugt eine anonyme Verbindung zu Bob durch das Tor-Netzwerk. (Quelle: Wikipedia/Saman Vosoghi)

DIE ZUKUNFT DER ARBEIT

THE EVERYWHERE ENTERPRISE

Die Corona-Krise zwang Unternehmen zum Umdenken und veränderte so die Arbeitswelt. Große Büroräume in guter Lage werden nicht mehr derart nötig sein, denn quasi über Nacht verwandelten sich Unternehmen durch den Umzug in das Home-Office in ein „Everywhere Enterprise".

Die Pandemie hat einen Wandel auf wenige Monate verkürzt. Das hat auch langfristige Wirkungen darauf, wie, wann und wo in Zukunft gearbeitet wird. Ein „Everywhere Enterprise" wird das Arbeiten flexibler machen, braucht dafür aber die richtige Technologie, um gleichzeitig die Sicherheit zu gewährleisten.

Der neue Arbeitsplatz

Dauerhaft von zu Hause aus zu arbeiten, ist in vielen Unternehmen bereits Realität. Um die Mitarbeiter in diesem neuen Umfeld zu unterstützen, benötigen Unternehmen bessere Werkzeuge für die Zusammenarbeit und Geräte für den Zugriff. Mitarbeiter, die vor Ort sein müssen, brauchen neue mobile Geräte, um mit Backend-Systemen zu interagieren. Mitarbeiter mit Fernzugriff, benutzen stattdessen ihre eigenen Desktops und Mobilgeräte für die Arbeit, und diejenigen, die zeitweise im Büro sind, müssen ihre Mobilgeräte mitbringen.

All diese Mitarbeiter benötigen Technologien zur Zusammenarbeit, die besser integriert sind und ein reibungsloses und sicheres Benutzererlebnis bieten. Jetzt müssen Unternehmen die Herausforderungen meistern, mit denen sie während des Lockdowns konfrontiert waren. Viele hatten Probleme, Unternehmensdaten auf Mobilgeräten abzusichern, sicheren Zugriff auf Unternehmensressourcen zu gewähren und IT-Fernsupport zu leisten. Zudem erlebten die Unternehmen einen Anstieg der Bedrohungen durch Diebstahl von Identitätsinformationen, Malware-Angriffe, „Zoom-Bombings"- und Phishing-Angriffe.

Diese Bedrohungen werden sich noch weiter verschärfen, wenn die Mitarbeiter ihre Mobilgeräte intensiver nutzen. Auf PCs sind Mitarbeiter eher gewohnt, mit Phishing umzugehen, auf Mobilgeräten aber sind sie anfälliger für Angriffe über SMS-Mitteilungen sowie Messaging- und Social Media-Plattformen.

Zeit für modernere Technik

Um diese Probleme zu beseitigen, müssen Unternehmen geschützte Workspaces auf den Geräten einrichten und eine sichere Netzwerkverbindung zur Verfügung stellen. Dazu gehört es auch, Richtlinien für Geräte und Apps schnell zu implementieren und durchzusetzen. Zoom beispielsweise verbesserte während der ersten Phase der Pandemie laufend die Sicherheitsfunktionen, daher konnten IT-Abteilungen die erforderlichen Konfigurationen über Unified Endpoint Management (UEM) schnell für Geräte und Mitarbeiter bereitstellen.

Auch die Benutzerfreundlichkeit müssen viele Unternehmen noch verbessern. So verlangen sie häufig noch Passwörter für den Zugang zu Apps und anderen Ressourcen. Sicherer und einfacher zu nutzen sind passwortlose Authentifizierungssysteme mit biometrischen Identifikatoren, die zu einer eigenständigen Zugangs-ID werden.

Die Arbeit wird sich noch weiterentwickeln und dieser Wandel wird noch einige Herausforderungen mit sich bringen. Es ergeben sich damit jedoch auch Chancen, die Arbeitsweise als solche zu modernisieren und Kollegen, die von zu Hause aus arbeiten, durch bessere Kollaboration und einen intuitiveren Zugang zu unterstützen. Das „Everywhere Enterprise" ist keine vorübergehende Erscheinung, es ist bereits Realität und wird weiterhin wachsen und expandieren, wenn die Mitarbeiter neue Wege finden, um ortsunabhängig produktiv zu sein.

Simon Biddiscombe
www.mobileiron.com

KOMPLEX UND ROBUST

5 TIPPS, WIE SIE IHR DATENSCHUTZPROGRAMM AUF DIE NÄCHSTE STUFE BRINGEN

In diesem Webinar gibt Ihnen Marleen Oberheide, OneTrust, Tipps und Best Practices zu 5 wichtigen Themenpunkten an die Hand, die Sie dazu befähigen, Ihr Datenschutzprogramm auf das nächste Level zu bringen.

Seit dem Inkrafttreten der DSGVO vor über zwei Jahren hat sich in Unternehmen so einiges getan. Viele haben erste wichtige Schritte unternommen, um ein Datenschutzprogramm aufzubauen und zu integrieren. Allerdings sind diese häufig sehr einfach aufgestellt und für die komplexe, sich stetig wandelnde Datenschutzwelt mit ihren diversen Neuerungen nicht robust genug aufgebaut.

3 Punkte, warum man unbedingt an diesem Webinar teilnehmen sollte:

- Erfahren Sie, welche Auswirkungen das Schrems II Urteil und das Planet49 Urteil auf Ihr Unternehmen haben.
- Erhalten Sie Tipps, wie die Automatisierung von Datenschutzprozessen Ihre Arbeit erleichtern kann.
- Entdecken Sie, wie Sie in Ihrem Unternehmen den Spagat zwischen Datenschutz und IT-Sicherheit meistern können.

LIVE WEBINAR
AM 05.11.2020
11-12UHR

Marleen Oberheide ist Solutions Engineer bei OneTrust

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

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 21 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download

IT-SICHERHEIT IM MITTELSTAND

UNWISSENHEIT IST DAS GRÖSSTE ÜBEL

Während Mitarbeiter sich über neue Technologien oder Konzepte aus den Bereichen BYOD, IoT und Co. freuen, läuten in den IT-Abteilungen aus Sicherheitssicht die Alarmglocken.

Im Rahmen dieser Studie wurden 202 Unternehmen aller Branchen zu ihren IT-Sicherheitsmaßnahmen untersucht.

Ungesicherte Geräte, das Nutzen öffentlicher WLANs mit dem eigenen Smartphone oder täuschen echt wirkende E-Mails mit verseuchten Anhängen – die Angriffsvektoren für Cyberattacken sind vielfältig. Wer sich fahrlässig den Gefahren aussetzt, der muss mit schweren finanziellen oder auch imagetechnischen Konsequenzen leben.

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

WIE GEHT ES WEITER?

COVID-19 UND DIE RÜCKKEHR ZUR CYBERNORMALITÄT

Auf dem Höhepunkt der Gesundheitskrise mussten die Unternehmen ihre Bemühungen auf den Fortbestand ihrer Tätigkeiten konzentrieren. Auch auf die Gefahr hin, sich einige Freiheiten in Bezug auf Cybersicherheit zu nehmen. Wie geht`s nun weiter?

Die Gesundheitskrise hat von einem Tag auf den anderen Millionen Beschäftigte zur Telearbeit gedrängt, mit einer explosionsartigen Zunahme der Nachfrage nach Fernzugang und VPN. In den letzten beiden Märzwochen verzeichneten die Mitarbeiter des technischen Supports von Stormshield 30 Prozent mehr Aktivität, darunter Anfragen von Netzwerk- und Systemadministratoren, die über Nacht Fernzugriffe einrichten mussten. Doch nicht jedes Unternehmen wandte sich an den Hersteller der eingesetzten Sicherheitslösungen. So gingen viele CISOs Kompromisse ein, zum Teil wurden sogar hausinterne Sicherheitsrichtlinien abgebaut oder verändert, um für mehr Fernzugriffe zu sorgen, ohne übliche IT-Sicherheitsverfahren zu befolgen und ohne davor eine Risikoanalyse durchführen zu können. Geringere Wachsamkeit und digitale Verunsicherung kamen jedoch bekanntermaßen Cyberkriminellen zugute, besonders bei Organisationen, in denen Telearbeit noch nie oder nur selten durchgeführt wurde. Bei Regierungen, Ministerien, Gemeinden, Verbänden, im Gesundheitswesen, bei Körperschaften und anderen sensiblen öffentlichen Betrieben wie auch im Industrieumfeld wurden die IT-Systeme auf eine besonders harte Probe gestellt. Und ihre digitale Anfälligkeit zeigte sich deutlich! Auch in Deutschland, wo etwa das Bundesland Nordrhein-Westfalen einen Phishing-Angriff erlitt, der millionenschwere Schäden verursachte. Doch eigentlich hat die COVID-19-Pandemie branchenübergreifend infrastrukturelle Mängel ans Tageslicht treten lassen.

Infrastrukturanpassungen dringend nötig

Die Rückkehr zu einer nahezu normalen Situation scheint derzeit in kleinen Schritten zu erfolgen. Die Möglichkeit örtlich begrenzter Lockdowns ist allgegenwärtig, die Pandemie haben wir leider noch nicht hinter uns. In diesem Kontext darf die Telearbeit nicht mehr als Ausnahme gelten, sondern sie sollte als mögliche Praxis in die Sicherheitspolitik der Unternehmen einfließen, um dem aufkommenden Bedürfnis nach beruflicher Mobilität und flexibleren Infrastrukturen schnell und zuverlässig gerecht zu werden, ohne zusätzliche Cyberrisiken in Kauf nehmen zu müssen. Gerade jetzt ist die Zeit gekommen, erkannte Schwachstellen oder Unzulänglichkeiten der eigenen IT- und OT-Architektur auszumerzen und gegebenenfalls hinausgeschobene digitale Transformationsprozesse einzuleiten. Dabei ist es unerlässlich, einerseits die gesamte Infrastruktur von möglichen, notgedrungen übernommenen Shadow-IT-Anwendungen zu bereinigen und das den Anwendern zu Hause garantierte Sicherheitsniveau dem im Unternehmen anzugleichen. Unter Umständen erfordern die einzuleitenden Korrekturmaßnahmen und die Gewährleistung einer höheren Integration mobiler Arbeitnehmer eine Aufstockung des IT- und Cybersecurity-Budgets. Doch einigen Studien zufolge würden viele Organisationen lieber auf IT-Investitionen verzichten, um die Corona-Schäden auszugleichen. Diesen Ansatz wagen wir in Frage zu stellen: Der Lockdown hat gezeigt, wie hoch der Beitrag gut abgesicherter digitaler Architekturen zum erfolgreichen Fortbestand der Geschäftstätigkeit tatsächlich ist. Ob gut gemeistert oder um ein Haar geschafft, das Leben vieler Unternehmen ging zum Glück trotz harter Eindämmungsmaßnahmen weiter. Fraglich ist nur, wie lange diese der noch andauernden Gesundheitskrise standhalten können, wenn die notwendigen Schritte zur Anpassung der eigenen Infrastruktur an das neue Szenario nicht zeitig genug unternommen werden.

www.stormshield.com

STORMSHIELD

THREAT INTELLIGENCE

Sicherheit im SAP-Umfeld

Ein neuer Trend in der IT-Security ist Threat Intelligence. Dabei geht es darum, Daten bekannter Schadprogramme, Schwachstellen und Angriffsvektoren in einen Kontext zu stellen und so effektiver auf Bedrohungen reagieren zu können. Viele IT-Security-Anbieter sind dazu übergegangen, Threat Detection als Teil oder zusätzliches Feature Ihrer Lösungen zu verkaufen. Leider ist Threat Intelligence meistens – wie so oft in der IT-Sicherheit – auf die Infrastruktur beschränkt. Unternehmenskritische Anwendungen werden außen vor gelassen. Dabei ist es einerseits gerade in diesem Bereich erstens enorm wichtig, ungewöhnliche Aktivitäten als solche zu erkennen. Zweitens ist es durch die Fokussierung auf bestimmte Applikationen einfacher, Angriffe zu erkennen. Beispiel SAP.

SAP-Systeme enthalten die sensiblen Daten jedes Unternehmens. Ob Mitarbeiterdaten aus dem SAP HR, Finanzdaten aus SAP FI/CO oder Lieferantendaten aus SAP SRM, für Angreifer stellen SAP-Landschaften ein mehr als lohnenswertes Ziel dar. Das hat die Hacker-Community inzwischen erkannt und Angriffe auf SAP-Systeme werden nicht nur häufiger, sie werden immer professioneller durchgeführt.

Leider werden SAP-Systeme in gängigen Sicherheitslösungen oft ausgeklammert, das gilt auch für Threat Intelligence Lösungen. Das liegt zum einen an der grundlegend anderen Technologie, die der Softwarehersteller aus Walldorf verwendet, zum anderen waren SAP-Systeme in der Vergangenheit sowohl technisch als auch organisatorisch vom Rest der IT getrennt – was oft dazu führt, dass die Sicherheitsabteilung sich mit den Besonderheiten der Technologie nicht auskennt, geschweige denn Angriffe erkennen kann.

ES IST SCHLAUER, DIE NADEL IM HEUHAUFEN MIT EINEM MAGNET HERAUSZUZIEHEN ALS EINE DATENBANK ZU BETREIBEN, DIE JEDEN EINZELNEN GRASHALM SEPARAT UNTERSUCHT.

Christoph Nagy, Geschäftsführer und Gründungsmitglied ABEX, www.abap-experts.com

SAP-Sicherheit wird immer wichtiger

In den letzten Jahren hat ein Umdenken stattgefunden und sowohl die SAP selbst als auch deren Kunden haben die Sicherheit ihrer SAP-Systeme zur Priorität erklärt. SAP-Systeme werden daher immer häufiger in eine umfassende Überwachung der gesamten IT-Landschaft mit eingebunden.

Das Ziel einer Überwachung von SAP-Systemen sollte natürlich sein, mögliche Bedrohung zeitnah als solche zu erkennen und – viel wichtiger noch - reagieren zu können. Studien zeigen, dass zwischen einem eigentlichen Angriff und der Entdeckung dieses Angriffs im Durchschnitt 146 Tage vergehen. In dieser Zeit kann ein Angreifer natürlich immensen Schaden anrichten. Diesen Zeitraum auf wenige Tage oder Stunden zu verkürzen ist daher oberstes Gebot.

Es lohnt sich, den Begriff „Threat Intelligence“ in diesem Zusammenhang näher zu beleuchten. Wenn es um SAP-Systeme geht, werden Angriffe von Hackern zunehmend professioneller. In der Realität werden Angriffe oft orchestriert von langer Hand vorbereitet. Wer eine Analogie bemühen möchte: Hackerangriffe ähneln selten dem klassischen Banküberfall, bei dem ein maskierter Räuber mit der Pistole wedelt und schon nach wenigen Minuten mit einem Sack voller Geld die Bank verlässt. Ein passender Vergleich wäre eher ein Film wie „Oceans Eleven“, bei dem eine ausgeklügelte Vorbereitung dem eigentlichen Clou vorausgeht.

Aus Anomalien mögliche Angriffe erkennen

In IT-Systemen – und damit auch für SAP-Landschaften gültig – erkennt man diese Vorbereitung durch bestimmte Hinweise. Korreliert man diese Hinweise mit anderen auffälligen Aktivitäten, kann ein möglicher Angriff vorliegen. Die Indizien, die auf einen Angriff hinweisen, liegen dabei in der Regel zeitlich deutlich auseinander. Es ist also nicht notwendig, die Protokolldateien, die solche Indizien enthalten können, sekundengenau auswerten zu können. Das hat oft sogar den Nachteil, dass für die Auswertung der meist enorm großen Mengen von Log-Daten enorme Ressourcen benötigt werden. Wichtiger ist eine Korrelationsanalyse, die mögliche Bedrohungen zielsicher entdeckt.

Um eine solche Analyse durchführen zu können, sind vor allem zwei Dinge notwendig: SAP-spezifisches Wissen, um ungewöhnliche Aktivitäten überhaupt erst erkennen zu können. Zweitens müssen diese Daten überhaupt erst einmal erhoben werden.

In der IT-Sicherheit haben sich für diese Art des Security Monitorings in den vergangenen Jahren sogenannte SIEM-Lösungen etabliert (Security Information and Event Management), wie beispielsweise splunk, Q-Radar oder ArcSight. Eingesetzt werden diese SIEM-Lösungen im Rahmen einer kontinuierlichen Überwachung vor allem in Security Operation Center (SOCs). SIEM-Lösungen erkennen auffällige Verhaltensweisen und sind mit Hilfe komplexer Korrelationsregeln dazu in der Lage, sicherheitsrelevante Vorfälle zeitnah zu identifizieren. Allerdings fokussieren sich die SIEM-Lösungen ebenfalls fast ausschließlich auf die Infrastruktur, also Netzwerkkomponenten, Firewalls oder Router. Für die komplexen SAP-Systeme und die Daten, die innerhalb der verschiedenen Anwendungskomponenten anfallen, sind die meisten SIEM-Systeme blind.

Kontinuierliche Überwachung ist wichtig

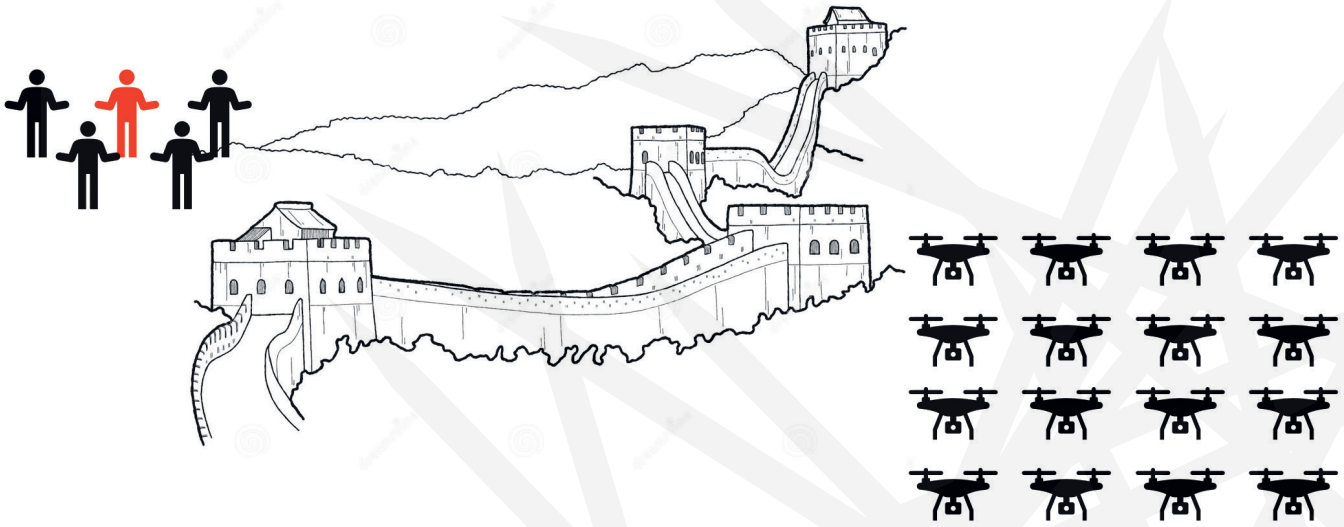
Für eine umfassende und lückenlose Überwachung von SAP-Landschaften ist eine Lösung notwendig, welche die Aufgaben eines SIEM für SAP-Systeme übernimmt oder eine Schnittstelle zu vorhandenen SIEM-Lösungen anbietet. Um dies zu realisieren müssen alle Vorgänge innerhalb der SAP-Systeme kontinuierlich im Hintergrund überwacht werden, um auffällige Vorgänge jederzeit erkennen zu können. Diese Vorgänge müssen dann miteinander korreliert werden. Dazu ist ein SAP-spezifisches Regelwerk erforderlich, das auch das Nutzerverhalten laufend analysiert. Des Weiteren müssen diese Informationen nicht nur an die Sicherheitsabteilung beziehungsweise an ein angeschlossenes SIEM-System weitergeleitet werden, sie müssen auch so aufbereitet werden, dass es kein SAP-Know-How erfordert, mögliche Bedrohung umgehend als solche zu erkennen.

Hier kommt die SAP-spezifische Threat Intelligence ins Spiel. SAP-Systeme sind extrem komplex, die meisten SAP-Landschaften bestehen aus mehreren, teils gar dutzenden oder hunderten einzelnen Systemen, die unterschiedliche Geschäftsprozesse wie Logistik, Personalwesen oder Produktion abdecken. Hinzu kommt, dass schon ein einziges SAP-System ein Vielfaches an Codezeilen enthält als beispielsweise ein Betriebssystem. Dementsprechend ist es wichtig, alle Schwachstellen innerhalb der SAP-Landschaft zu kennen. Dazu gehören Systemparameter, die Passwortregeln definieren, aber auch potentiell ungesicherte Schnittstellen oder – gerade im SAP-Bereich – von Kunden selbst erstellte Programmierungen. Eine Identifizierung und Absicherung dieser möglichen Schwachstellen ist nicht nur aufgrund der Komplexität der SAP-Systeme eine Herausforderung. Durch laufende Änderungen der Systemkonfiguration, dem Hinzufügen neuer Benutzer oder Berechtigungen und das Transportieren von Änderungen innerhalb der Systemlandschaft sind die Einstellungen zudem hoch dynamisch.

Alle SAP-Bereiche sollten abgedeckt sein

Ein großes Problem stellen auch die umfangreichen und komplexen Berechtigungen innerhalb eines SAP-Systems dar. Zu großzügig vergebene Berechtigungen führen oft dazu, dass ein Nutzer unwissentlich die Möglichkeit hat, kritische Einstellungen zu ändern – ein nicht zu unterschätzendes Sicherheitsrisiko. Und nicht nur das: auch das Thema Compliance ist im Berechtigungswesen ein wichtiger Faktor. Ein gutes Beispiel ist der soge-

Die Nadel im Heuhaufen kann nur mit kontextspezifischem Wissen gefunden werden.



Die Komplexität von SAP System kann nur durch automatisierte „Drohnen" überwacht werden – manuelle Überwachung ist hier nicht mehr möglich.

nannte Trainee-Effekt: ein Trainee durchläuft während seiner Ausbildung viele Abteilungen. Auf diese Weise kann es passieren, dass der Trainee am Ende der Ausbildung alle Rechte aller Abteilungen kumuliert hat – was nicht nur zu einem Sicherheitsrisiko führt, sondern auch den Wirtschaftsprüfern auffallen wird.

Um die Schwachstellen in den oben genannten Bereichen frühzeitig zu identifizieren ist ein Scanner erforderlich, der alle Bereiche wie Systemparameter, Schnittstellen aber auch Rollen und Berechtigungen auf mögliche Sicherheits- und Compliance-Probleme überprüft. Bedingt durch die hohe Komplexität schon eines einzelnen SAP-Systems sollte bei der Auswahl einer solchen Vulnerability Management-Lösung zwei Dingen besonders Beachtung geschenkt werden: Einerseits sollte eine Prüfung möglichst umfangreich sein. Die Sicherheitsleitfäden der SAP selbst sowie der Prüfleitfaden der DSAG bieten hier einen guten Anhaltspunkt. Zum anderen sollte ein solcher Scanner in die Echtzeitüberwachung möglichst nahtlos integriert sein, um Änderungen am System frühzeitig zu erkennen und an die verantwortlichen Stellen weiterleiten zu können.

Threat Intelligence im SAP Umfeld besteht dementsprechend aus mehreren Schritten: Schwachstellen müssen zunächst identifiziert werden, die Systeme müssen durch Härtung und passgenaue Berechtigungen geschützt werden und ein kontinuierliches Monitoring muss Anomalien erkennen und einordnen können. Mit diesen Schritten folgt eine SAP-Sicherheitsstrategie weitgehend dem NIST-Framework für Cybersecurity, das vom Nationalen Institut für Standard und Technologie der USA bereitgestellt wird und sich als de-facto-Standard etabliert hat.

Ohne Kontext keine Intelligenz

Für die Threat Intelligence wiederum ist entscheidend, dass diese separaten Schritte in einen anwendungsspezifischen Kontext gestellt werden. Es genügt nicht, eine Datenbank mit standardisierten Schwachstellen eines SAP-Systems vorzuhalten. Vielmehr müssen diese Daten miteinander korreliert werden, unter Berücksichtigung der von Angreifern verwendeten Vorgehensweise. Ein gutes Beispiel ist der 2019 entdeckte Expoit 10KBLAZE. Dieses „Werkzeug" versucht, über bekannte Schwachstellen und Fehlkonfigurationen in ein SAP-System einzudringen. Das Absichern einzelner Schwachstellen im Visier des Exploits bedeutet nicht notwendigerweise, dass es einem Angreifer nicht gelingen kann, die Systemlandschaft tatsächlich zu kompromittieren. Vielmehr sollte eine Lösung zur Absicherung Schwachstellen und Log-Einträge mit dem notwendigen Hintergrundwissen korrelieren. Nur so kann ein Angriff effektiv erkannt und abgewehrt werden.

Bei der Auswahl einer solchen Lösung sollten zwei Kriterien im Vordergrund stehen. Für die Identifizierung und Beseitigung von Schwachstellen sollte ein möglichst umfassender Katalog an Prüfungen bereitstehen, der sich nach etablierten Standards richtet. Für die Analyse der Aktivitäten wiederum ist eine intelligente Korrelationslösung wichtiger als eine Lösung, die eine sekundengenaue Auswertung verspricht. Anders gesagt: es ist schlauer, die Nadel im Heuhaufen mit einem Magnet herauszuziehen als eine Datenbank zu betreiben, die jeden einzelnen Grashalm separat untersucht.

Christoph Nagy

Bild: Antares-NetlogiX

SOC-AS-A-SERVICE

RUND UM DIE UHR IN SICHEREN HÄNDEN

Unternehmen, die ihre IT-Systeme, Daten und Anwendungen erfolgreich gegen Angriffe und Missbrauch absichern möchten, stehen vor wachsenden Herausforderungen. Die zunehmende Komplexität der Cyberattacken erfordert einen professionellen, aufwändigen Rundum-Schutz.

Da dieser Schutz gerade in kleinen und mittelständischen Unternehmen häufig nur mit hohem zeitlichen und finanziellen Aufwand gewährleistet werden kann, setzen immer mehr Unternehmen auf Managed Security Services Provider (MSSP) oder stoßen entsprechende Planungen an. Das merkt auch der österreichische Security-Experte iQSol. Deswegen bietet das Unternehmen diverse Lösungen, die als Gesamtpaket einen 360°-Schutz abdecken – auch als Managed Security Services.

Kommandozentrale für 360°-Schutz

Ob Log Management inklusive langfristiger Archivierung gemäß Compliance-Vorgaben, ob Schwachstellen-Management mit modernsten Tools und Sensoren, ob Analysen oder Patchen mithilfe täglich erneuerten Wissens: Um die verschiedenen Security-Maßnahmen zentral zu steuern, empfiehlt sich die Nutzung eines Security Operation Centers (SOC). Software-Hersteller wie iQSol bieten die kontinuierliche Überwachung und Betreuung der Kundensysteme über Partnerfirmen als „SOC-as-a-Service" an. Dabei ziehen immer mehr Firmen Leistungen aus einer Hand vor, bei denen sich ein erfahrener Partner zusätzlich zur Security auch um Datenschutz und Business Continuity Management kümmert. Hier fällt die Entscheidung häufig bewusst auf einen mittelständischen IT-Dienstleister wie Antares-NetlogiX, der neben vielfach zertifiziertem Security-Know-how auch hohe Servicequalität und Projekterfahrung mitbringt. Wenn der Partner zudem Rund-um-die-Uhr-Verfügbarkeit (24x7) gewährleisten kann, ist die IT-Sicherheit in besten Händen.

www.iqsol.biz

DATENDIEBSTAHL

DECEPTION HALBIERT KOSTEN

Unternehmen, die Deception-Technologien zur Früherkennung von Cyberangriffen einsetzen, können durch Datendiebstähle verursachte Kosten um mehr als die Hälfte (51 %) reduzieren. Dies ist das wichtigste Ergebnis der Studie „Cyber Deception Reduces Breach Costs & Increases SOC Efficiency", die Attivo Networks gemeinsam mit Kevin Fiscus von Deceptive Defense durchgeführt hat. Die Untersuchung zeigt, dass die durchschnittliche Reduzierung der Kosten für Datenschutzverletzungen 1,98 Millionen US-Dollar pro Vorfall oder 75,12 US-Dollar pro kompromittiertem Datensatz beträgt. Diese Kostensenkungen werden erreicht durch schnellere Erkennung und effektive Reaktion auf Vorfälle sowie durch eine geringere Komplexität bei deren Handhabung.

Mehr Effizienz für SOC-Agenten

Zudem kann Deception-Technologie laut diesem Bericht den Zeitaufwand für die Bearbeitung von Fehl-Warnungen (False Positives) erheblich reduzieren und die Effizienz des typischen Security Operations Center (SOC) steigern. Eine kürzlich von Ponemon und Exabeam durchgeführte SIEM-Produktivitätsstudie ergab, dass der durchschnittliche Zeitaufwand pro SOC-Analyst und Vorfall etwa 10 Minuten betrug und SOC-Analysten etwa 26 Prozent ihres Tages mit der Bearbeitung von Fehlalarmen verschwenden, was einem Produktivitätsverlust von über 18.000 US-Dollar pro Analyst und Jahr entspricht.

www.attivonetworks.com

IAM CONNECT 2020

Die Brücke zu neuen Geschäftsmodellen

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

Hybride Konferenz
30.11. bis 02.12.2020
in Berlin

www.iamconnect.de

Sie haben die Wahl

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

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

Hauptsponsor

ipg
EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Speed Demo Sessions

AIRLOCK®
SECURE ACCESS HUB

Auth0

betasystems

DIERICHSWEILER
Unternehmens- und Prozessberatung

Eine Veranstaltung von itmanagement & itsecurity

Highlights aus der Agenda

Vorträge

Wie alles begann

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

Kundenorientiertes Projekt-management mit Design Thinking

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

Ordnung im Berechtigungs-Dschungel: Erfahrungsbericht

Dr. Peter Katz,
KPT Krankenkasse

Einführung einer neuen IAM-Lösung bei der Thüringer Aufbaubank

Cindy Schöneck,
Thüringer Aufbaubank

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

Clemens Wunder,
Bundesagentur für Arbeit

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

Mathias Winter,
PI Informatik GmbH Berlin

Workshops

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

Dr. Ludwig Fuchs,
Nexis GmbH

IAM für Internet-Dinger (IoT)

Peter Weierich,
IPG GmbH Deutschland

Rechtliche Herausforderungen im IAM

Ralf Schulten, Rechtsanwalt,
avocado rechtsanwälte

NEXIS ONE IDENTITY Ping Identity. Telia

KEINE CHANCE FÜR HACKER

WORAUF SIE BEI PKI-LÖSUNGEN VON DRITTANBIETERN ACHTEN SOLLTEN

In den letzten zehn Jahren hat DevOps sich zunehmend zur Standardmethode entwickelt, mit der Software und Anwendungen in einem beispiellosen Tempo bereitgestellt werden. Allerdings sollte man die nötigen Vorkehrungen treffen, um potenzielle Cybersicherheitsrisiken zu senken. Insbesondere was den Zugang zu Netzwerkressourcen und damit auch zu geistigem Eigentum anbelangt. Wie die jüngsten Analysen gezeigt haben, lassen sich motivierte Cyberkriminelle selbst während der globalen Gesundheitskrise kaum aufhalten. Wenn Hacker ohne Zögern das Covid-19-Virus ausnutzen, werden sie es sich sicher nicht zweimal überlegen, den Entwicklungszyklus eines Unternehmens anzugreifen.

Im Rahmen von Developer Security Operations (DevSecOps) wird Sicherheit in allen Phasen der Anwendungsentwicklung (Planung, Codierung, Erstellung und Testen) implementiert. Tatsächlich erfordern die neuesten Datenschutzregeln es, Fragestellungen zur Sicherheit bereits in den Entwicklungszyklus einzubinden, und damit DevSecOps erfolgreich funktionieren. Erreichen lässt sich das mit Hilfe einer Public-Key-Infrastruktur (PKI). Eine PKI hat sich bereits als kosteneffiziente, sichere und skalierbare Methode bewährt, um starke Identitäten für Container, Endpunkte und sogar den Code für Mikro-Services zuzuweisen. Angesichts der Schnelllebigkeit von DevOps-Versionen sind starke Identitäten für die Verwaltung von Containern umso wichtiger, da die Endpunkte schnell auf- und wieder abgebaut werden.

Eine robuste, skalierbare Infrastruktur, die es erlaubt Mikro-Services kontinuierlich zu integrieren und bereitzustellen, verursacht nicht ganz unbeträchtliche Kosten. Das durchschnittliche Gehalt eines PKI-Ingenieurs im Jahr 2020 beläuft sich beispielsweise auf etwa 119.000 Dollar. Verlässt ein Unternehmen sich auf eine eigene Lösung, braucht man mit Sicherheit mehr als einen PKI-Experten. Die aufwendige Wartung sollte man nicht einem einzelnen Mitarbeiter überlassen.

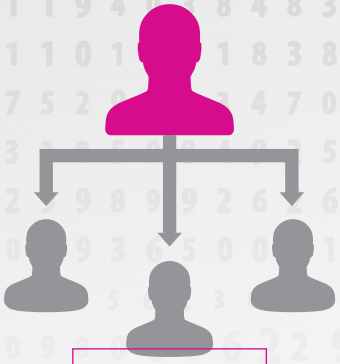
Dazu kommen weitere Herausforderungen für einen CISO:

- **Zeit –** Fachwissen aufzubauen braucht Zeit, und schon der Ausfall eines einzigen Mitarbeiters im Sicherheitsteam kann zu einer folgenreichen Überlastung führen.
- **Recruiting –** Personalmangel und der sogenannte „Skills Gap" können Serviceunterbrechungen oder unzureichende Compliance zur Folge haben – was wiederum Kosten nach sich zieht.

- **Delegieren –** Wenn wichtige Grundsatzentscheidungen von dazu nicht ausreichend qualifizierten und überforderten Mitarbeitern getroffen werden, führt das leicht zu neuen Herausforderungen. Die gleichen Aufgaben lassen sich aber auch in einen Cloud-Service auslagern, der auf Richtlinienkonformität hin konzipiert ist.

Den richtigen PKI-Partner finden

Gartner zufolge „müssen die Verantwortlichen für SRM (Sicherheits- und Risikomanagement) im Zuge der zunehmenden Verbreitung von DevOps und Virtualisierung die Sicherheit und Integrität dieser sich schnell verändernden Umgebungen berücksichtigen." Weiter heißt es: „Obwohl sich mehrere Methoden der Container-Identität (und -Sicherheit) bedienen, ist der Einsatz digitaler Zertifikate eine weite-



re mögliche Option. Das Verwalten von X.509-Zertifikaten in Containern ist eine Methode, mit der SRM-Führungskräfte diese virtuellen Umgebungen sichern können. Aufgrund der schnellen, elastischen Beschaffenheit von Containern sind sie jedoch für manuelle Zertifikatsverwaltungsmethoden nicht geeignet. Folglich können die mit der Sicherheit virtueller, containerisierter Systeme betrauten SRM-Führungskräfte X.509-Tools mit entsprechenden Integrationen verwenden, um diese Umgebungen zu schützen."

Zertifikate über ihre gesamte Lebensdauer hinweg nachzuverfolgen und zu verwalten ist ohnehin schwierig bis riskant. Denn die Gültigkeitsdauer von Zertifikaten ist begrenzt und erfordert eine spezielle technische Wartung. Die wiederum setzt fundierte PKI-Kenntnisse voraus. Wenn Sie Zertifikate von Drittanbietern nicht selbst verwalten können, laufen Sie Gefahr, genau denen gegenüber Schwachstellen offenzulegen, deren Hauptintention es ist, sie zu finden und auszunutzen.

Man sollte sich also einen Partner suchen, der die benötigte Anzahl von Zertifikaten bereitstellen kann, und zwar bedarfsgerecht. Verfügbarkeit ist der entscheidende Faktor, wenn Sie vermeiden wollen in der Bereitstellungsphase oder jedem anderen Entwicklungsstadium ohne Zertifikate dazustehen. Eine frei skalierbare Lösung ist ohne Automatisierung nicht möglich.

Operative Risiken vermeiden

In der Welt der kontinuierlichen Integration und Bereitstellung ist es umso wichtiger, dass der Code auf Containern geschützt ist. Dazu braucht man starke Identitäten, um alle Endpunkte zu authentifizieren und die Verbindungen zwischen den Computersystemen zu verschlüsseln. Das ist für eine vollständig unabhängige und richtlinienkonforme Implementierung unerlässlich. Wenn einzelne Mitarbeiter oder kleine Teams verantwortlich sind, Zertifikatskonfigurationen gemäß den Unternehmensrichtlinien zu erstellen und zu verwalten, kommt es schnell zu Fehlern. Wenn die Zahl der Zertifikate mit dem Wachstum einer Anwendung unübersichtlich wird, steigt die Gefahr menschlicher Fehler.

Ausfälle aufgrund abgelaufener Zertifikate oder aufgrund von fehlender Automatisierung führen letztlich zu massiven operativen Risiken. Die Folgen sind schwerwiegend. Mit solchen Versäumnissen bei der Erneuerung von Zertifikaten hatten Firmen und Institutionen in den letzten Jahren massiv zu kämpfen. Wenn eine Firma auf eine automatisierte Lösung umstellen will, braucht sie einen Partner mit einem starken Back-End, und er muss technisch in der Lage sein, den Grad der Automatisierung in dem jeweils benötigten Umfang zu unterstützen.

Nicht alle Zertifizierungsstellen/PKI-Partner sind gleich. Achten Sie darauf, einem Partner auszuwählen, der zu Ihrem Anforderungsprofil passt und der mit Ihrem Unternehmen mit wachsen kann und entsprechende Kapazitäten vorhält.

www.globalsign.com

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Simon Biddiscombe, Boris Cipot, Andreas Fuchs, Stefan Gutekunst, Alexander Haugk, Arne Jacobsen, Egon Kando, Daniel Linder, Thomas Malchar, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Sebastian Spethmann, Rayna Stamboliyska, Mareike Vogt

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. 27.
Preisliste gültig ab 1. Oktober 2019.

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

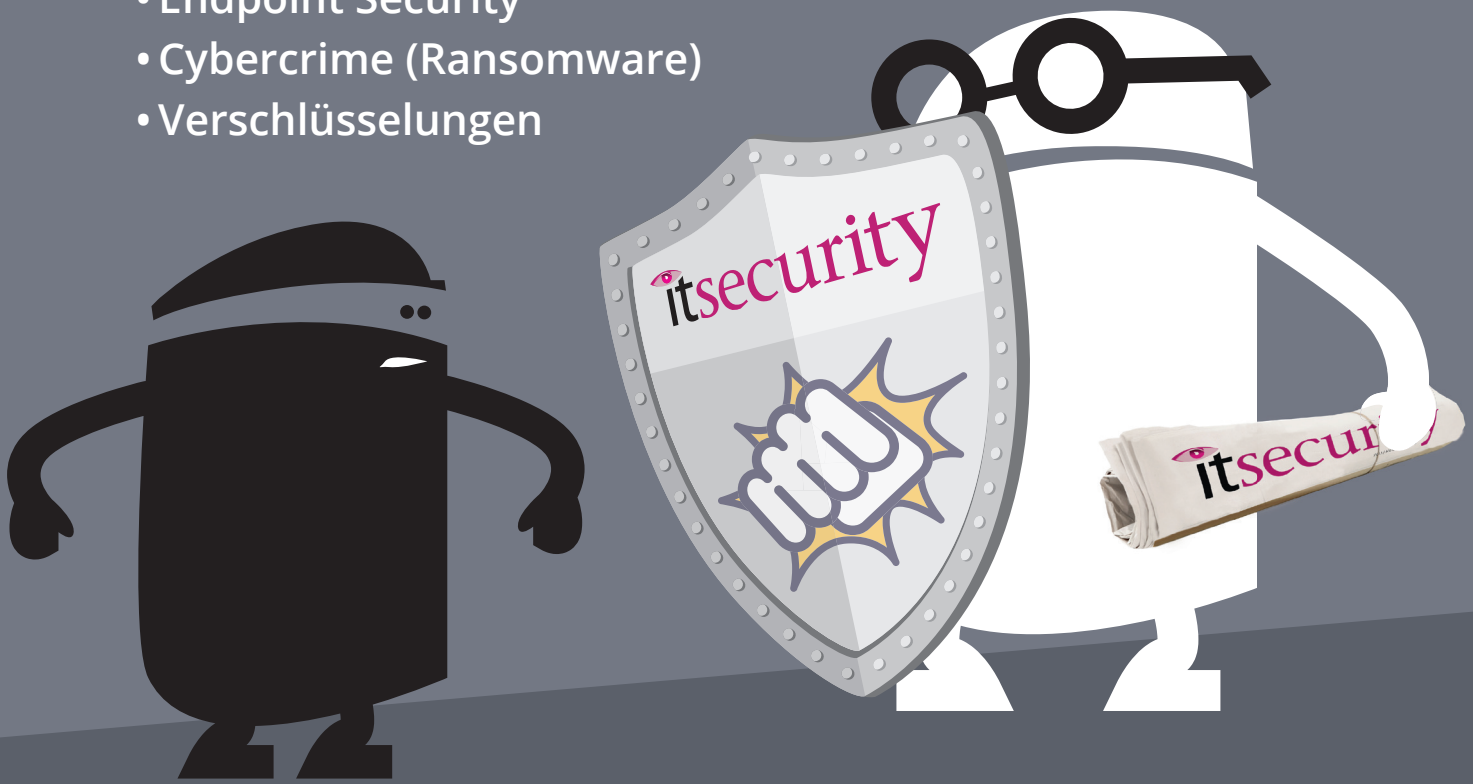
We secure IT

IT Security 2020 Digitalevent

17. November 2020

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

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



Jetzt anmelden

www.it-daily.net/wesecureit/