itmanagement

MAI 2022

INKLUSIVE 24 SEITEN
IT SECURITY

SAP-LIZENZIERUNG

Wie Unternehmen Kosten sparen

UNIFIED COMMUNICATIONS

Wettbewerbsvorteil Kommunikation

DIE HEIMLICH-STILL-UND-LEISE-EVOLUTION

WIRELESS WAN

Jan Willeke, Cradlepoint

www.it-daily.net

FAXT DU NOCH?

Kennen Sie diesen Witz? Das Gericht schreibt an den Angeklagten: „Sie können Ihre Aussage gern auch faxen!“ Antwort: „Da, wo ich bin, kann man nicht faxen!“ Das Gericht: „Wieso? Wo sind Sie denn?“ Angeklagter: „2021! Ich bin im Jahr 2021!“

Darüber können Sie lachen? Ich auch! Eigentlich sollte man aber weinen, denn das Fax ist in einigen Unternehmen und vorrangig in Behörden noch immer gang und gäbe und somit das Kommunikationsmittel der Wahl.

Erfolgreiche Kommunikation – intern, wie auch extern – ist für jedes Unternehmen enorm wichtig. Es bedeutet Verständigung untereinander, den Austausch miteinander und auch Repräsentation nach außen.

Die Art der Kommunikation hat sich gewandelt - von Telefon über Mail zu Video oder Messenger. Die nächste Stufe war Unified Communications (UC), also die Vereinheitlichung der Kommunikation auf einer Plattform. Das Ziel von UC ist es, Kommunikationsprozesse zu optimieren und effizienter zu gestalten. Das bedeutet, dass man nahtlos zwischen den verschiedenen Kommunikationsmodi, unabhängig vom Endgerät, das man gerade nutzt, wechseln kann. Und die Entwicklung schreitet weiter voran – lesen Sie mehr dazu ab Seite 28! Bleibt die Frage – warum sollte man heute noch faxen wollen und die, die es tun: Was hindert Euch daran, endlich darüber hinwegzukommen?

Außerdem in dieser Ausgabe: Unser großes SAP Spezial ab Seite 12. Bringen Sie sich auf den Stand der Dinge und wenn Sie Ihr Wissen vertiefen wollen: am 2. Juni findet unser Digitalevent No SurpRise with SAP statt. Melden Sie sich an unter www.it-daily.net/sap

Eine gute Lektüre wünscht

Carina Mitzschke | Redakteurin it management

INHALT

COVERSTORY

SAP SPEZIAL

IT MANAGEMENT

Inklusive
24 Seiten

IT SECURITY SPEZIAL

KLÜGER ARBEITEN MIT KI

UNTERSTÜTZUNG FÜR DIE INDUSTRIE

Künstliche Intelligenz (KI) gilt als die neue transformative Kraft der Wirtschaft. Doch was Unternehmen wie Google, Amazon und Meta längst erfolgreich nutzen, scheint für viele mittelständische Unternehmen bislang in weiter Ferne. Dabei gibt es laut dem Softwarehersteller Augmentir einige Bereiche, in denen KI-Algorithmen in Produktion und Instandhaltung bereits messbare Mehrwerte bringen.

Nachwuchskräfte werden seltener, erfahrene „alte Hasen" gehen in den Ruhestand. Vielerorts ist der Fachkräftemangel bereits deutlich spürbar. Das gilt ganz besonders in der Industrie, die laut DIHK-Report vom November 2021 derzeit den steilsten Anstieg an Stellenbesetzungsproblemen meldet. Den Unternehmen bleibt nichts anders übrig, als dieses Manko teils durch Leiharbeiter, teils durch Arbeitskräfte mit geringerem Ausbildungsstand zu kompensieren.

Aber selbst die jungen Talente, die an Bord kommen, gilt es möglichst rasch anzulernen und einzuarbeiten. Für langwierige Onboardings oder Schulungen fehlt die Zeit, Unternehmen müsse neue Wege einschlagen. Dies gelingt, indem sie Einarbeitung oder Fortbildung eng mit der praktischen Arbeit verzahnen.

Damit dies gelingt, braucht es allerdings mehr als nur statische Papier-Anleitungen auf den Screen zu bringen. Mehr Flexibilität versprechen moderne KI-Verfahren: Während erfahrenere Kolleginnen und Kollegen nur die wesentlichen Punkte abarbeiten und rückmelden müssen, erhalten Novizen detailliertere Schritt-für-Schritt-Anleitungen. Auch ein verpflichtender Schulterblick eines Experten kann hier eingefordert werden. Welche Lernschritte das System wem angezeigt, bestimmt jedes Unternehmen für sich – unterstützt von Machine-Learning-Methoden.

www.augmentir.com/de/

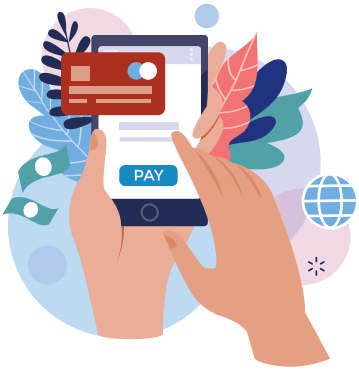
KI-UNTERSTÜTZUNG IN DER INDUSTRIE – DAS SIND DIE VORTEILE

DIE WICHTIGSTEN GRÜNDE, KEINE FINANZ-APPS ZU NUTZEN

36 % Sicherheitsbedenken

30 % Datenschutzbedenken

21 % Technologieskepsis



FINANZ-APPS

SICHERHEITSBEDENKEN ALS GRÖSSTES HEMMNIS

Bezahl-Apps und andere digitale Finanzangebote sind aus unserem Alltag nicht mehr wegzudenken. Das bestätigt eine aktuelle Umfrage von DE-CIX. Die Marktdurchdringung der Apps beläuft sich demnach auf fast zwei Drittel der Deutschen. Die größten Vorteile sehen Anwender in der Zeitunabhängigkeit (68 Prozent), Benutzerfreundlichkeit (66 Prozent) und Ortsunabhängigkeit (58 Prozent). Besonders beliebt sind die Apps in der Altersgruppe der 25- bis 34-Jährigen, wo sie fast drei Viertel (74 Prozent) der Befragten nutzen. Doch auch mehr als die Hälfte (58 Prozent) der über 55-Jährigen nutzt solche Angebote.

Eine für alles?

Der Gedanke, die vielen verschiedenen auf dem Markt verfügbaren Finanzdienste in einer einzigen App zu bündeln, ist bei der hohen allgemeinen Akzeptanz der Nutzer naheliegend. Bereits 28 Prozent der Befragten könnten sich vorstellen, ein solches Angebot zu nutzen.

„Die Umfrageergebnisse zeigen, dass Finanz-Apps und digitale Bezahldienste ein integraler Bestandteil des täglichen Lebens geworden sind“, sagt Dr. Thomas King, Technikchef bei DE-CIX. „Der nächste logische Schritt ist es, mehrere Angebote in einer App zu kombinieren. Das stellt Banken vor große Herausforderungen, denn sie müssen Daten außerhalb ihrer eigenen, hochsicheren Systeme mit Partnern direkt austauschen können, um Ihren Kunden entsprechende Angebote in ihrer App zu präsentieren. Banken müssen die Bedenken der Endnutzer ernstnehmen und sowohl bei der Verbindung zum Endnutzer als auch bei der Verbindung zu Partnern auf höchste technische Sicherheitsstandards und strengen Datenschutz achten.“

www.de-cix.net

WIRELESS WAN

DIE HEIMLICH-STILL-UND-LEISE-EVOLUTION

Jede Veränderung in der Netzwerktechnik ist auf eine Veränderung der Computerarchitekturen und der Art der daran angeschlossenen Geräte zurückzuführen. Vom Mainframe über verteiltes Computing, Client-Server und SD-WAN bis zu Hybrid-Cloud- und Edge-Computing. Wir bewegen uns weiter über feste Standorte hinaus und verbinden Geräte, Orte und Dinge zunehmend drahtlos. Jan Willeke, Area Director Central Europe bei Cradlepoint, im Gespräch mit Ulrich Parthier, Publisher it management.

? **Ulrich Parthier:** *Lassen Sie uns einen Blick in die Vergangenheit werfen, um die Zukunft besser zu verstehen. Die 2000er Jahre waren ja geprägt vom virtualisierten, Server-zentrierten Computing.*

Jan Willeke: Mit der zunehmenden Globalisierung der Unternehmen traten Server-Farmen an die Stelle von Mainframes und verteilten Midrange-Computern. Die Anwendungen wurden stärker zentralisiert, während auch virtuelle private Netzwerke und Multiprotocol Label Switching, kurz MPLS, in den Mittelpunkt rückten. Das TCP/IP-native MPLS bot eine Möglichkeit, den Verkehr zu priorisieren und eine effizientere Weiterleitung von Daten über geleaste Leitungen zu schaffen.

Intelligente Netzwerke erkannten damals, dass verschiedene Arten von Datenverkehr aus den Geschäftsstandorten unterschiedliche Prioritäten erforderten. Dank MPLS ließen sich unterschiedliche Dienstqualitäten über das WAN nutzen, was eine nahtlose End-to-End-Konnektivität von Anwendungen und entfernten LANs ermöglichte. Das Netzwerk wurde zu einem differenzierten, vom Betreiber bereitgestellten Dienst.

? **Ulrich Parthier:** *Und dann begann ab 2010 der Aufstieg von Cloud Computing und SD-WAN.*

Jan Willeke: Die Tech-Szene boomte in dieser Zeit, um es vorsichtig auszudrücken. In den 2010er Jahren kamen das iPad, Microsoft Azure und die erste LTE-Aktivierung auf den Markt. Als Netzwerke, Geräte und Anwendungen immer mobiler wurden und die Bandbreitennutzung geradezu explodierte, begann der Aufstieg des Cloud Computing.

Die Befragten einer Studie der International Data Corporation (IDC) gaben an, dass einer ihrer Hauptgründe für die Einführung von SD-WAN die „Vereinfachung der WAN-Verwaltung zur Unterstützung von Hybrid-IT/Multicloud" sei. SD-WAN ist die letzte Epoche der kabelgebundenen Netzwerkwelt für feste Standorte.

? **Ulrich Parthier:** *Was uns in die Gegenwart bringt: die 2020er Jahre, das Zeitalter des hybriden Cloud-Computing und drahtlosen WAN.*

Jan Willeke: Dank geringer Latenz und hoher Bandbreite von 4G- und 5G-Lösungen sind drahtlose Verbindungen heute zu einem wesentlichen Bestandteil vom WAN-Infrastrukturen geworden.

Wireless WAN (WWAN) bietet die Agilität und Reichweite, die moderne WANs benötigen, um eine schnelle Bereitstellung zu ermöglichen, einen hochverfügbaren Cloud-Zugang zu unterstützen und Menschen, Orte und Dinge überall zu verbinden – und das mit viel weniger Personalaufwand als je zuvor.

? **Ulrich Parthier:** *Dann sehen Sie die WAN-Modernisierung als eine kontinuierliche Entwicklung?*

Jan Willeke: Mit Sicherheit. Wide Area Networks: die drei kleinen Worte, die

unsere Welt verbinden. Von den bescheidenen Anfängen bis zu einem verzweigten, globalen Netz wird sich das WAN zusammen mit den Anforderungen von Computern, Geräten, Konnektivität und Unternehmen weiterentwickeln.

Jede Änderung in der Netzwerktechnik ist auf eine Änderung der Computerarchitekturen und der Art der daran angeschlossenen Geräte zurückzuführen. Beides findet parallel statt, und das Netzwerk folgt immer: vom Mainframe über verteiltes Computing, Client-Server und SD-WAN bis zu Hybrid-Cloud- und Edge-Computing.

Ulrich Parthier: *Lassen Sie uns nochmals zu den Vorteilen von Wireless WAN kommen. Welche Argumente sprechen dafür?*

Jan Willeke: Ich sehe da mit Blick auf Unternehmen die Lösung vieler Netzprobleme, zudem bieten sich neue Chancen – die wiederum Basis für weitere Umgestaltungen sind. Das lässt sich an mehreren Punkten veranschaulichen. Stichwort Netzwerkausfallsicherung: Die digitale Transformation von Unternehmen braucht funktionierende Netze, die durchgehend verfügbar sein müssen. Dies gelingt durch mehrschichtige Systeme mit unterschiedlichen Verbindungsarten, mit und ohne Kabel. Failover springt ohne Unterbrechung von einem zum anderen Verbindungstyp, ob nun wired oder wireless. Haben LTE-Verbindungen eine geringere Bandbreite, erkennen und gewichten SD-WAN-Richtlinien den kritischen Datenverkehr. Bei LTE- und 5G-Verbindungen der Gigabit-Klasse ist ein Failover des gesamten Verkehrs möglich. Alles in allem lassen sich Wireless-Failover-Funktionen viel schneller und leichter bereitstellen als neue Kabel installieren.

Ulrich Parthier: *Wie sieht es mit einer Erweiterung der Netzwerkbandbreite aus?*

Jan Willeke: Das ist ein weiteres Plus von SD-WAN: Es kann zeitgleich mehrere Verbindungen zusammenfassen und generiert so eine höhere Bandbreite. Das Hinzufügen einer drahtlosen Verbindung zum Kabelnetz oder der Gebrauch verschiedener drahtloser Verbindungen ist eine gute Alternative zur Erhöhung der Bandbreite.

Drahtlose Verbindungsoptionen übersteigen mit Geschwindigkeiten von über 1 Gbit/s bei 5G relativ zügig das Leistungspotenzial kabelgebundener Verbindungen.

Ulrich Parthier: *Sollte man die mobile Konnektivität zur Hauptverbindung machen?*

> WAS WIR DERZEIT SEHEN, IST EINE DRAMATISCHE TRANSFORMATION DES NETZWERK-EDGE. DIE AUSWEITUNG DES NETZWERK-EDGE ERLAUBT ZAHLREICHE NEUE STANDORTE, DIENSTE UND INITIATIVEN ZUR DIGITALEN TRANSFORMATION.
>
> Jan Willeke,
> Area Director Central Europe, Cradlepoint,
> https://cradlepoint.com/de-de/

Jan Willeke: In jedem Fall. Drahtlose WANs bieten eine bessere betriebliche Flexibilität für verschiedene Unternehmensstandorte. Eröffnung oder Wechsel von Zweigstellen und Büros werden dadurch erheblich einfacher. Die Technologie ist auch auf Baustellen oder in Pop-up-Stores sinnvoll, in denen nur drahtlose Netzwerke möglich sind. Auch wenn ein hochredundantes Netz mit geringen Betriebskosten aufgebaut werden soll, bietet sich Wireless als starke Alternative zu kabelgebundenen Verbindungen an.

Ulrich Parthier: *Gibt es ein weiteres Plus, das für Wireless WAN spricht?*

Jan Willeke: Ja, die Ausweitung der IoT-Funktionen. Dabei geht es nicht um nur gelegentlichen Datenaustausch, gängige Anwendungsfälle sind Videoüberwachung oder Prozesse in Medizin, Fertigung und Industrie. Hierfür sind geringe Latenzzeit und hohe Bandbreite von Drahtlosverbindungen besonders wichtig.

Ulrich Parthier: *Und wie sieht es insgesamt mit der veränderten Unternehmensmobilität aus?*

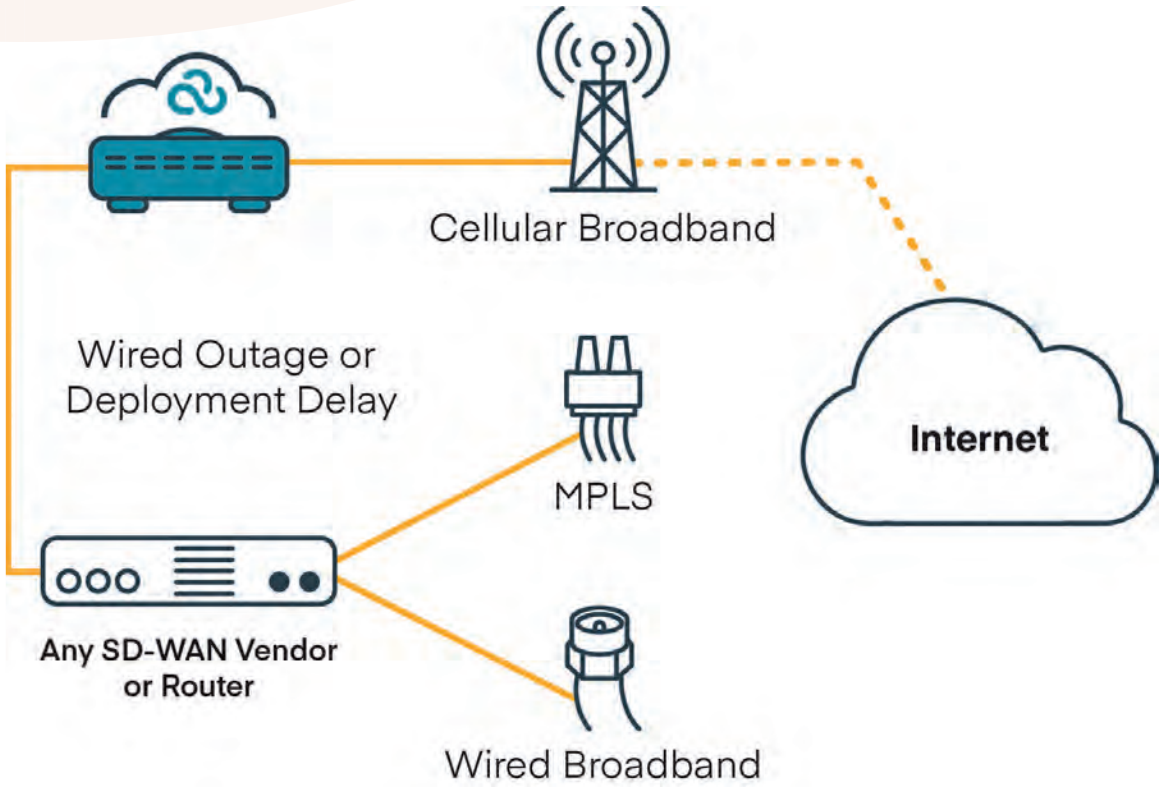
Jan Willeke: Prozesse mobil zu unterstützen wird als wachsender Markt für Datenkonnektivität angesehen, da sich Unternehmen bemühen, zu papierlosen Büros überzugehen und die Datenerfassung zu intensivieren. Durch LTE wird hier schon vieles umgesetzt, 5G wird noch weitere Möglichkeiten eröffnen. Man denke an Daten- und Video-Uploads in Echtzeit, automatisierte Routenplanungen und die Konnektivität ganzer Fahrzeuge.

Ulrich Parthier: *Vielleicht noch ein Fazit zum Abschluss?*

Jan Willeke: Was wir derzeit sehen, ist eine dramatische Transformation des Netzwerk-Edge. Unternehmensnetze sind heute nicht mehr an feste Standorte gebunden. Sie formieren sich aus Menschen, Cloud-Diensten, Fahrzeugen, Pop-up-Standorten und einem immer größer werdenden Kosmos an IoT-Geräten.

Die Edge-Ausweitung erlaubt auch neue Initiativen zur digitalen Transformation. Insgesamt ergibt sich für Unternehmen eine große Flexibilität, die auf der hohen Reichweite und den sich weiter entwickelnden Fähigkeiten der Wireless WANs beruht.

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



OPERATIONAL SERVICES
YOUR ICT PARTNER

Microsoft Partner

Microsoft

- Gold Cloud Platform
- Gold Datacenter
- Silver Messaging
- Silver Application Development
- Silver Collaboration and Content

MOBILE ARBEITSPLÄTZE MIT MICROSOFT 365 KLUG DURCHDACHT

und professionell umgesetzt

Die Erwartungen an moderne Arbeitsplätze sind heutzutage extrem hoch. Unternehmen, die ihre Teams mit einem umfassenden Service begeistern, profitieren von der hohen Zufriedenheit und Motivation ihrer Mitarbeiter. Doch die professionelle Einrichtung und den 24/7 IT Service Desk für den sorglosen Agile Workplace können viele Betriebe nicht alleine abdecken.

Setzen Sie auf unser Microsoft-zertifiziertes Expertenteam, das Sie von der vollautomatischen Konfiguration über die Administration bis hin zu Conditional Access und Security-Konzept rundum zuverlässig mit allen wichtigen Services versorgt.

So werden mobile Arbeitsplätze auch in Ihrem Unternehmen zur Erfolgsgeschichte. Profitieren Sie von unserer Expertise als langjährig erfahrener Microsoft Gold Partner.

operational-services.de/microsoft-365

Machen Sie mit uns Agile Workplace schnell, einfach und sicher zum Firmenstandard

NO SURPRISE WITH SAP

STRATEGIE & OPERATIONS

DIE COVID-PANDEMIE UND JETZT DER UKRAINE & CYBER-KRIEG HABEN DAS THEMA DIGITALISIERUNG ETWAS IN DEN HINTERGRUND TRETEN LASSEN. ABER: DIE KRISEN UNSERER ZEIT MACHEN ES IMMER DEUTLICHER: DIE AUS SORGE VOR AUFWAND UND RISIKEN AUFGESCHOBENEN TRANSFORMATIONSPROJEKTE MÜSSEN JETZT ANGEGANGEN WERDEN, DAMIT UNTERNEHMEN ZUKUNFTSFÄHIG BLEIBEN. NEUE TECHNOLOGIEN SPIELEN DABEI EINE WICHTIGE ROLLE. ABER WELCHE INNOVATION IST SINNVOLL FÜR DAS EIGENE UNTERNEHMEN UND WAS MUSS BEDACHT WERDEN, UM DAS POTENZIAL VOLLUMFÄNGLICH ZU HEBEN?

Quelle: Christian Lue

SAUBERE DATENTRENNUNG BEIM CARVE-OUT

STADT HAMBURG LEGT BEIM DATENEXPORT AUS SAP HOHE MASSSTÄBE AN

Der Wechsel zwischen Privatisierungsbestrebungen und Re-Kommunalisierungskonzepten gehört seit Jahren zum Instrumentarium der Politik – sei es auf Bundes- oder auf Kommunalebene. Eine solche Rückführung wurde jüngst von der Stadt Hamburg durchgeführt, die die Vattenfall Fernwärme GmbH übernahm, um dieses Netz wieder in Eigenregie zu führen. Damit setzt der Hamburger Senat den aus einem Volksentscheid resultierenden Auftrag zur Re-Kommunalisierung der Strom-, Gas- und Fernwärmenetze um. Mit dem Erwerb allein war es jedoch nicht getan, denn beim Carve-Out (Unternehmensabspaltung) wechselten nicht nur mehr als 600 Beschäftigte ihren Arbeitgeber, sondern auch 23 Prozent der Daten ihren Besitzer.

CARVE-OUT

Unter einem Carve-Out versteht man die Abspaltung beziehungsweise Veräußerung von Unternehmensteilen. Vielfach ist ein Carve-Out Bestandteil eines Restrukturierungsplans, wenn Unternehmen beispielsweise im Rahmen der Fokussierung auf das Kerngeschäft einen Unternehmensbereich abstoßen.

Als der Konzern den Unternehmensbereich der Wärmeenergieversorgung zurück in die Verantwortung der öffentlichen Hand geben sollte, galt es nach der Unterzeichnung des Kaufvertrags, einen komplexen und sicherheitskritischen Datenumzug zu realisieren. Das Besondere bei diesem Datentransfer war, dass bei Vattenfall nur die in diesem Kontext relevanten Daten das SAP-System und damit den Konzern verlassen durften. Aber wie lassen sich diese Daten identifizieren? Und vor allem wie können diese in das SAP-System der neugegründeten Wärme Hamburg GmbH integriert werden? Diese Aufgabe entpuppte sich von Beginn an als sehr komplex. Deshalb entschied man sich frühzeitig, für dieses Projekt ausgewiesene Transformationsexperten hinzuzuziehen – Umzugsspezialisten für Daten. Gefordert war Spezialwissen und vor allem praktische Erfahrung im Umgang mit komplexen Datentransfers einer solchen Relevanz und Größenordnung.

Genau hinschauen

Die Verantwortlichen von Vattenfall und der Wärme Hamburg machten sich auf die Suche nach Experten, die in der Lage waren, die betroffenen geschäftskritischen Daten und Prozesse zu identifizieren und ein Konzept für deren Transfor-

mation zu erstellen. Auch dezidiertes SAP-Knowhow war gefragt sowie Kenntnisse im Energiesektor beziehungsweise über die Strukturen der öffentlichen Hand. Nicht zuletzt aufgrund der zahlreichen Transformationsprojekte, die das digitale Umzugsunternehmen Natuvion schon erfolgreich bestritten hatte, entschied man sich für die ERP-Transformations-Experten des Walldorfer Beratungsunternehmens.

SAP-MIGRATION
Tipps für eine erfolgreiche Migration

1. Intensive Analyse der bestehenden Systemlandschaft
2. Custom Code anpassen
3. Migrationsstrategie wählen
4. Unternehmensprozesse vereinfachen
5. Migrations-Etappen definieren
6. Digitalisierungsinitiativen vorantreiben
7. SAP-Landschaft bereinigen

Diese starteten gemeinsam mit Vattenfall eine eingehende Analyse der Ist-Situation. Dafür nahmen sie nicht nur den Status Quo des bestehenden SAP-Systems unter die Lupe, sondern definierten zugleich die Anforderungen an den Carve-Out. Herausfordernd war dabei von Anfang an, dass seitens der Stadt Hamburg für die Transformation ein maximales Zeitfenster von neun Monaten sowie der konkrete Migrationstermin festgelegt wurden. Umso akribischer führte man die Analysen durch, stellte das Transformationskonzept auf und traf alle erforderlichen Vorbereitungen.

Trockenübungen für den Carve-Out

Nach der konzeptionellen Ausarbeitung des Datenumzugs war die genaue Differenzierung der Daten entscheidend. Hier musste unterschieden werden, welche Daten aus SAP in die neue SAP ECC-Landschaft der Wärme Hamburg GmbH transformiert werden durften und welche gelöscht werden mussten. Für die Selektion der löschrelevanten Daten kamen das SAP Landscape Transformation Tool (LT) und der Natuvion-eigene Data Conversion Server (DCS) zum Einsatz. Das LT versetzte Vattenfall in die Lage, zusammenhängende logische Datenobjekte auf der Ebene der Datenbanktabellen zu transformieren und sogar die gesamte Datenhistorie eines einzelnen Objekts zu migrieren. Der Natuvion DCS wiederum ist eine vollständige Extract-, Transform- und Load (ETL)-Plattform, die den Datentransfer technisch unterstützt. Die Software liest, analysiert, extrahiert, transformiert und validiert Daten aus verschiedensten Quellen (Systemen, Datenbanken, Dateien, Webservices) und schreibt diese zu unterschiedlichen Zielen.

Die Vorgehensweise bei der Selektion und dem Transfer war bei diesem Projekt folgende:

1. Kopie des produktiven Systems von Vattenfall
2. Löschung der Vattenfall-Daten aus dieser Kopie
3. Überprüfungen der Löschung durch Vattenfall
4. Export der Daten aus dem Vattenfall-SAP
5. Import der Daten in das SAP-System der Wärme Hamburg
6. Test der Ergebnisse

Hürden überwinden

Nach einem ersten Testdurchlauf mussten sich die Transformations-Experten allerdings nochmal auf eine neue Anforderung einstellen. Das Problem: Daten aus einem alten SAP-Buchungskreis mussten zu Auskunftszwecken an die Wärme Hamburg GmbH übergeben werden – allerdings wurde dieser Buchungskreis sowohl weiterhin von Vattenfall als auch von der Wärme Hamburg genutzt. Das zog Anpassungen bei den nachfolgenden Testläufen nach sich: Parallel zum klassischen Carve-Out musste deshalb auch ein Buchungskreissplit vorgenommen werden. Das war insofern eine Herausforderung, weil für die Wärme Hamburg aus dem Buchungskreis nur logistische Daten, beispielsweise aus dem Einkauf, von Bedeutung waren – nicht aber die zusätzlich im System enthaltenen Finanzdaten. Das machte den Verantwortlichen Sorgen und sie befürchteten, dass das gesamte Transformationsprojekt aufgrund des kurzfristigen Buchungskreissplits aus den Fugen geraten könnte. Doch das war nicht der Fall, da man sich lösungsorientiert auf das Wesentliche dieser zusätzlichen Herausforderungen konzentrierte.

Bevor die Daten – immerhin 23 Prozent der gesamten Vattenfall-Daten – schlussendlich das System und den Besitzer wechselten, wurden drei Massentests sowie eine Generalprobe durchgeführt. Danach wurden letzte Anpassungen vorgenommen, damit es beim finalen Go-Live keine Überraschungen gab – weder auf Seiten von Vattenfall noch bei der Stadt Hamburg. Mit dem finalen Datentransfer schafften Vattenfall, die Wärme Hamburg und die Spezialisten von Natuvion eine Punktlandung – aus Kosten-, Zeit- und Datensicht. Seither sind die Systeme der beiden Unternehmen voneinander getrennt und alle Daten da, wo sie hingehören. Diese reibungslose Umsetzung hat beide Energieunternehmen beeindruckt und deshalb könnte schon bald ein weiteres Projekt in Angriff genommen werden: der Carve-Out der Fernkälte-Sparte von Vattenfall.

Philipp von der Brüggen
www.natuvion.com

DATENQUALITÄTSANALYSE

EINSTIEG IN DAS STAMMDATENMANAGEMENT

Nicht wenige Unternehmen haben mit ihren Stammdaten ein Problem. Mit dem Data Quality Analyzer (DQA) von zetVisions können sie diesem Problem auf den Grund gehen und in ihren SAP-Systemen inkonsistente, doppelte, unvollständige und veraltete Datensätze in den Stammdatendomänen – Kunden/Lieferanten beziehungsweise Debitoren/Kreditoren, Produkt- und Materialstammdaten – aufspüren.

Über die Validierungsregeln können Datenqualitätsregeln erstellt werden, die zu Regelsätzen zur Prüfung der Daten auf Konsistenz, Vollständigkeit, Aktualität und Eindeutigkeit zusammengefasst werden. Die Regelsätze dienen dazu, einen Stammdatensatz mit einem Qualitäts-Score zu versehen. Für jeden Stammdatensatz lässt sich so evaluieren, ob er gut, ausreichend oder mangelhaft gepflegt ist. Für jede Regel eines Regelsatzes kann die Gewichtung frei definiert werden.

#SAPDIGITAL22

Auf dem Event erfahren Sie mehr zu diesem Thema, besuchen Sie unseren Slot am 02.06.2022 um 10:00 Uhr zum Thema „Data Quality", wir freuen uns auf Ihre Teilnahme.

www.it-daily.net/sap/

zetVISIONS

Zusätzlich lassen sich KPI definieren, also „Schwellen", ab wann Datensätze als gut, ausreichend oder mangelhaft gelten. Die Regelsätze werden turnusgemäß angewandt, so dass Trends über einen längeren Zeitraum dargestellt werden können. Korrekturaufgaben lassen sich automatisch anstoßen, in dem bei Auftreten eines Fehlers eine Information gesandt wird. Die Korrekturen sind bequem aus dem DQA durch „Absprung" in den SAP-Datensatz oder per Massenupload möglich.

Der Data Quality Analyzer, der zu einer vollständigen Stammdatenmanagement-Lösung (zetVisions SPoT) ausgebaut werden kann, ist der Einstiegspunkt, um die Datenqualität in den Griff zu bekommen.

www.zetvisions.de

WIDERSTAND GEGEN DIE DIGITALE ÜBERWACHUNG

WOFÜR JULIAN ASSANGE UND EDWARD SNOWDEN KÄMPFTEN

Die digitale Überwachung schreitet mit großen Schritten voran. Wir werden immer gläserner. Wenn sich diese Entwicklung fortsetzt, verschwindet unsere Privatsphäre auf Nimmerwiedersehen. In diesem Buch beschreiben die beiden Autoren, wie sehr wir heute schon digital bespitzelt werden, welche Rolle die Staaten, die Digitalwirtschaft und die Hacker dabei spielen und wie real die Gefahr wirklich ist, wenn wir uns nicht wehren. Seite für Seite decken sie auf, wie Behörden und Digitalkonzerne in unsere Privatsphäre eindringen. Schonungslos rechnen sie mit einer Politik ab, die den gläsernen Bürger zum Ziel hat. Julian Assange und Edward Snowden haben ihr Leben aufs Spiel gesetzt, um uns aufzuwecken. Werden wir wach und wehren uns. Zahlreiche praxisnahe Hinweise, wie man sich gegen die digitale Bespitzelung wehren kann, finden sich im Buch.

Widerstand gegen die digitale Überwachung – Wofür Julian Assange und Edward Snowden kämpften; Marc Ruberg, Detlef Schmuck; DC Publishing, 04-2022

SPEERSPITZE TRANSFORMATION

DIGITALISIERUNG SCHAFFT ZUKUNFT

BEI DER MIGRATION VON SAP-SYSTEMEN IN DIE CLOUD IST SICHERHEIT UND EINE MINIMALE DOWNTIME ENTSCHEIDEND.

Gregor Stöckler, COO, SNP SE, www.snpgroup.com

Die Krisen unserer Zeit machen es immer deutlicher: Die aus Sorge vor Aufwand und Risiken aufgeschobenen Transformationsprojekte müssen jetzt angegangen werden, damit Unternehmen zukunftsfähig bleiben. Neue Technologien spielen dabei eine wichtige Rolle. Aber welche Innovation ist sinnvoll für das eigene Unternehmen und was muss bedacht werden, um das Potenzial vollumfänglich zu heben?

Entscheider stehen angesichts der aktuellen Herausforderungen vor enormen Aufgaben: Im Krisenmodus geht es vorwiegend darum, die dringendsten Probleme zu lösen. Dabei sollte der digitale Fortschritt stets mitgedacht werden. Die vergangenen Pandemiejahre, Klima- und andere Krisen haben gezeigt: Je digitaler Unternehmen aufgestellt sind, desto flexibler können sie auf massive Marktveränderungen reagieren. Die Führungsetage sollte sich deshalb gerade jetzt mit den Chancen auseinandersetzen, die mit neuen Technologien einhergehen.

Immer klarer: Es geht nur mit

Eine repräsentative Umfrage unter 602 Unternehmen ab 20 Beschäftigten in Deutschland im Auftrag des Digitalverbands Bitkom zeigt, dass eine große Mehrheit der Unternehmen in Deutschland die Digitalisierung inzwischen strategisch angehen. Nur noch 16 Prozent verfügten über keine Digitalisierungsstrategie. Vor zwei Jahren lag laut Bitkom der Anteil mit 26 Prozent noch deutlich höher. 95 Prozent sehen die Digitalisierung für das eigene Unternehmen überwiegend oder ausschließlich als Chance (2018: 89 Prozent). Nur noch 4 Prozent der Unternehmen sehen die Digitalisierung vor allem oder ausschließlich als Risiko, 2018 war der Anteil mit 8 Prozent noch doppelt so hoch.

Die Wahl der richtigen Technologie

Bei der Auswahl einer Technologie sollte ausgehend von dem Ziel gedacht werden. Der Mehrwert für das eigene Unternehmen muss offensichtlich sein: So könnten sich Logistiker, die Störfaktoren in ihrer Lieferkette schneller und exakter vorhersagen sowie transparenter mit den anderen Supply-Chain-Akteuren zusammenarbeiten wollen, mit den Vorteilen von Big Data auseinandersetzen. Händler, die ihren Kunden ein personalisiertes Einkaufserlebnis ermöglichen und das Kaufverhalten analysieren möchten, um Geschäfts- und Marketingstrategien darauf abzustimmen, erwägen vielleicht den Einsatz von Künstlicher Intelligenz. Und wer in der Produktion zur Kosteneinsparung und Produktivitätssteigerung die vorausschauende Wartung von Anlangen (Predictive Maintenance) anstrebt, könnte den Einsatz einer Internet-of-Things-Lösung (IoT) prüfen.

Ist Ihr Unternehmen bereit?

Neuerungen ergeben nur Sinn, wenn sie sich nutzbringend in den eigenen Geschäftsalltag integrieren lassen. Ausgehend von dem aktuellen Ist-Zustand gilt es, den angestrebten Soll-Zustand für die Zukunft zu definieren. Entscheider sind gut beraten, schon in der Analysephase Experten einzubinden: Für die Erstellung einer klar definierten Roadmap müssen sie tief in die komplexen IT-Landschaften

blicken und die gewonnen Informationen richtig einordnen können. Herkömmliche Methoden sind zu fehleranfällig. Softwarebasierte Verfahren hingegen ermöglichen Unternehmen umfassende Analysen, mit denen sie die Digitalisierung, den Wechsel nach SAP S/4HANA und den in die Cloud gut planen sowie schnell und risikominimiert umsetzen können.

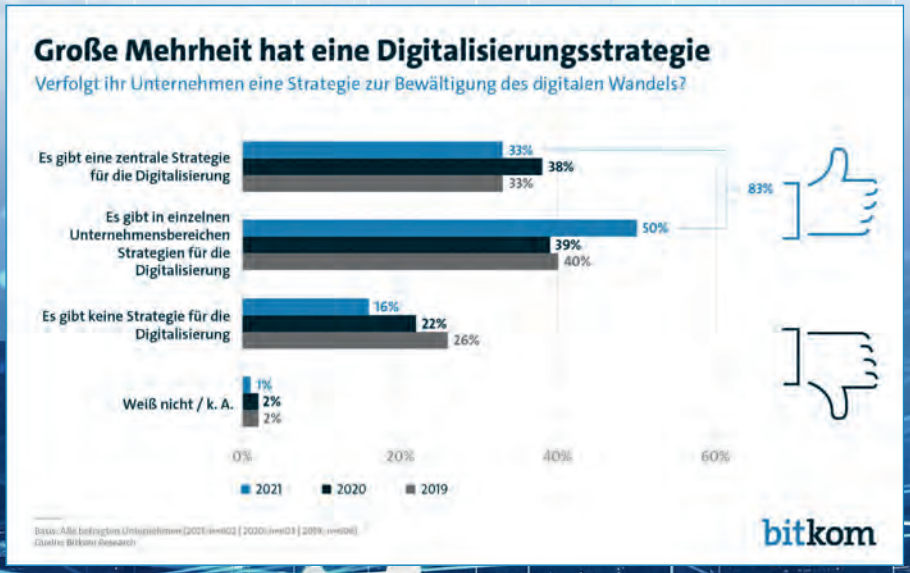
Um neue Technologien optimal einsetzen und ihr volles Potenzial schnell ausschöpfen zu können, müssen Grundlagen geschaffen werden. Eine hohe Relevanz spielt in diesem Kontext beispielsweise der Schritt in die Cloud: Durch das Auslagern der eigenen Anwendungen und IT-Leistungen in das Internet wird ein permanenter und ortsunabhängiger Datenverkehr zwischen Menschen, Maschinen und Fahrzeugen ermöglicht, was beispielsweise die professionelle Erhebung, Sammlung und Analyse großer Datenmengen (Big Data) begünstigt.

Sollten IT-Landschaften noch nicht dem erforderlichen Technikstand entsprechen, muss exakt geprüft werden, welche Vorarbeiten notwendig sind. So ist gewährleistet, dass das Transformationsvorhaben in einem angestrebten Zeitraum umgesetzt werden kann. Zudem behalten Projektverantwortliche den Gesamtüberblick über Kosten sowie den technischen und zeitlichen Aufwand.

Entscheider sollten digitale Technologien als wichtiges Instrument zum Erreichen der Unternehmensziele sehen sowie möglichst aktuell – und schneller als die Konkurrenz – über neue Entwicklungen informiert bleiben. Neuheiten gilt es stets auf den Nutzen für das eigene Unternehmen beziehungsweise die Branche zu durchleuchten. Dabei ist die Führungsetage nicht auf sich alleine gestellt: Spezialisierte Dienstleister helfen dabei, eine Vorstellung davon zu entwickeln, wie Unternehmensprozesse mit digitalen Lösungen aussehen könnten.

Cloud-Nutzen für Digitalisierung und Automatisierung

Eine im letzten Jahr im Auftrag von KPMG durchgeführte Cloud-Monitor-Untersuchung des Digitalverbandes Bitkom zeigte, dass neun von zehn Entscheidern (88 Prozent) der Cloud-Technologie einen eher großen bis sehr großen Beitrag zur Digitalisierung ihres Unternehmens zuschreiben. Zum Vergleich: 2019 waren es erst 77 Prozent. Den größten Mehrwert sehen die Befragten bei der Digitalisierung interner Prozesse und der Automatisierung von Workflows. Zudem sehen jeweils drei Viertel einen eher großen bis sehr großen Einfluss von Cloud-Computing auf eine bessere Zusammenarbeit zwischen Fach- und IT-Abteilung (78 Prozent) und den Aufbau von Plattformen zur flexiblen Kooperation mit Dritten (75 Prozent).



SAP-Systeme in die Cloud zu migrieren ist eine Herausforderung, die Unternehmen mit innovativen Lösungen und einem erfahrenen Partner meistern.

Innovationstreiber Cloud

Für Unternehmen gibt es zahlreiche gute Gründe, die Cloud-Nutzung voranzutreiben. Dazu sollten aber die Cloud-Strategie und die angestrebten Ziele mit der Cloud klar sein – laut Gartner berichtet fast ein Drittel der für eine Studie Befragten von erfolglosen oder ineffektiv implementierten Cloud-Lösungen. Um Herausforderungen zu meistern und Fallstricke auf dem Weg zu vermeiden, sollten Unternehmen daher ihren Weg in die Cloud mit einer systematischen Planung und klaren Zieldefinition beginnen. Zu erreichende Ziele müssen im Einklang mit der allgemeinen Unternehmensstrategie stehen und – wie Anforderungen und Rahmenbedingungen – in einer Cloud-Roadmap festgehalten werden. Da der Erfolg einer Cloud-Transformation erheblich von der technischen Umsetzung abhängt, muss zudem frühzeitig geklärt werden, welcher Partner die Daten, Anwendungen und Systeme migrieren soll. Insbesondere der Umzug bestehender SAP-Systeme mit langjähriger Betriebsgeschichte ist für IT-Experten eine anspruchsvolle Aufgabe. Mit einer flexiblen, softwarebasierten Lösung lassen sich aber selbst komplexe Migrationsvorhaben risikominimiert und nahezu ohne Ausfallzeiten realisieren. So können auch lange und aufwändige Vorprojekte vermieden – und schnell die notwendige Transparenz über die beste Cloud-Strategie und damit verbundene Kosten und Zeitaufwände geschaffen werden.

Gregor Stöckler

SAVE THE DATE

Das E-3 Magazin

itmanagement

No SurpRISE with SAP

Strategie & Operations

02. Juni 2022 | ab 9:00 Uhr | Digitalevent

#SAPdigital22

SCAN ME

WARUM KI MEHR ALS NUR EIN MODEBEGRIFF IST

KÜNSTLICHE INTELLIGENZ IN MODERNEN BACKOFFICE-PROZESSEN

Künstliche Intelligenz (KI) ist heute ein viel und divers genutzter Begriff. Während im privaten Bereich neben den Vorteilen von KI auch immer ein wenig Dystopie mitschwingt (denken wir nur an verschiedene Hollywood-Blockbuster), sind wir im Business-Kontext deutlich positiver eingestellt und dafür gibt es auch gute Gründe.

Der zentrale Vorteil des Einsatzes von KI in Backoffice-Prozessen ist die Eliminierung von repetitiven Aufgaben. Anstatt eingehende Rechnungen oder Kundenaufträge per Hand zu bearbeiten, überlässt man gerne „der Maschine" die Arbeit. Dass diese automatisierte Verarbeitung immer effizienter wird, verdanken wir der Tatsache, dass die dahinter stehenden Technologien immer besser werden. Durch die stetige Weiterentwicklung kann KI mittlerweile mehr als das reine Auslesen und Aufbereiten von Daten. Ebenso werden mit KI schon jetzt Prozesse, die eine umfassendere Interpretation von Daten erfordern, automatisiert durchgeführt, beispielsweise das Splitting von Dokumentenstapeln oder die Erkennung von Anomalien.

Die Entwicklung bleibt nicht stehen. Bei Esker setzen wir KI kontinuierlich in unseren Lösungen ein, entwickeln unsere KI-Fähigkeiten stetig weiter und befreien Finanz- und Kundendienstabteilungen so von zeitaufwendigen Aufgaben. Gleichzeitig werden durch effiziente Prozesse Beziehungen zu Kunden und Lieferanten gestärkt. Das ist die Grundlage für positives Wachstum: Höhere Produktivität, verbesserte Mitarbeitermotivation und größeres Vertrauen zwischen Unternehmen. Um einen der eingangs erwähnten Blockbuster zu zitieren: Hasta la vista, Ineffizienz!

www.esker.de

ECM TRANSFORMATION

5 DINGE, DIE BERÜCKSICHTIGT WERDEN SOLLTEN

Die digitale Transformation zwingt Unternehmen zu überdenken, wie Zusammenarbeit und Prozesse in ihrem erweiterten Unternehmen stattfinden, wobei die Definitionen für „Backoffice" und „Frontoffice" verschwimmen. Sie macht es auch immer wichtiger, mehr Wert aus ihren Inhalten herauszubekommen, während gleichzeitig auch moderne Sicherheits- und regulatorische Anforderungen thematisiert werden. Obwohl Altsysteme des Enterprise-Content-Managements geholfen haben, die sensibelsten Inhalte zu verwalten, wurden sie nie entwickelt, um den neuen mobilen, sehr agilen Geschäftsprozessen des digitalen Zeitalters Rechnung zu tragen. Eine neue Strategie muss her.

Erfahren Sie in diesem Whitepaper fünf Dinge, die bei der Transformation Ihrer ECM-Strategie mit dem Cloud-Content-Management berücksichtigt werden sollte.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 4 Seiten und steht kostenlos zum Download bereit. ***www.it-daily.net/Download***

DATENSPEICHER NEU GEDACHT

LEITFADEN FÜR EINE ERFOLGREICHE IT-TRANSFORMATION

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 13 Seiten und steht zum kostenlosen Download bereit: ***www.it-daily.net/download***

In den letzten zehn Jahren hat das rasante Tempo mit dem sich die IT-Technologie weiterentwickelt, die zugrunde liegende Datenspeicherinfrastruktur enorm unter Druck gesetzt. Um mit den gestiegenen Anforderungen Schritt zu halten, hat Software-Defined Storage kontinuierlich bewiesen, die optimale Grundlage für jede Speicherinfrastruktur zu sein.

Dank ihrer extremen Flexibilität und nie dagewesenen Agilität erobern sich softwaredefinierte Technologien stetig neue Bereiche. Durch die Abstrahierung der Speicherdienste von der Speicherhardware gewinnen IT-Abteilungen beispiellose Kontrolle über die Speicherung, den Schutz und den Abruf von Daten.

SAP CONNECTOR FOR MICROSOFT SENTINEL

ALLER GUTEN DINGE SIND DREI: SAP, MICROSOFT UND SOC

Das Warten hat ein Ende: Der SAP Connector for Microsoft Sentinel ist da. War es bisher schwierig, SAP an bestehende Detection-Lösungen anzubinden, gibt es mit dem SAP Connector for Microsoft Sentinel nun ein leistungsstarkes Tool, das Sie lizenzkostenfrei nutzen können – unabhängig davon, ob Sie Ihre SAP-Systeme im Rechenzentrum oder in der Cloud betreiben. Der Connector lässt sich mit 16 Log-Quellen verknüpfen und konsolidiert Daten aus komplexen SAP-Landschaften so, dass sie für eine zielführende Verarbeitung und aussagekräftige Analyse in Microsoft Sentinel bereitstehen. Das SIEM-System wertet die Daten aus und generiert im Falle von Anomalien entsprechende Alerts.

Nicht ohne meine MDR-Services

Der Clou: SAP und Microsoft haben gemeinsam rund 100 Use Cases vordefiniert, die Sie für Ihre eigenen Zwecke bedarfsgerecht anpassen oder um eigene Security-Szenarien erweitern können. Um Bedrohungen abzuwehren, braucht es neben der Technologie auch professionelle Managed Detection and Response Services (MDR). Dabei überwachen und bewerten erfahrene Security-Experten und fachlich versierte Datenanalysten in einem Security Operations Center (SOC) die eingehenden Alarme. Je nach Bedrohungslage setzen sich vorab definierte Maßnahmen automatisch in Gang oder die Fachleute im SOC leiten eine individuelle Incident Response in die Wege. Durch den interdisziplinären Austausch mit SAP-Fachleuten ist sichergestellt, dass der MDR-Service jederzeit alle SAP-Spezifika berücksichtigt. Damit sind sie ein echtes Dreamteam: der SAP Connector for Microsoft Sentinel sowie der weltweit erste und einzige MDR-Service speziell für SAP.

www.arvato-systems.de

NACHHALTIGKEIT

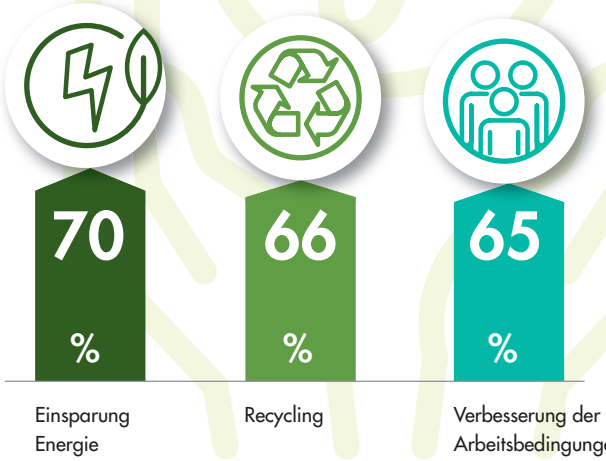
… STEHT BEI KMU HOCH IM KURS

Viele Großunternehmen und Konzerne beschäftigen heutzutage ganze Abteilungen, die sich um die Nachhaltigkeitsagenda kümmern. Doch welche Bedeutung hat da Thema für KMU? Eine YouGov-Studie im Auftrag von IONOS gibt Aufschluss.

Mehr als zwei Drittel (68 %) der deutschen KMU halten das Thema „Nachhaltigkeit und Umweltschutz" insgesamt für sehr wichtig. Doch fehlende finanzielle Ressourcen sind eine der drei größten Hürden für mehr Nachhaltigkeit. Weitere Bremsen sind die fehlende Notwendigkeit und dass Unternehmen nichts daran hindere, nachhaltiger zu werden.

www.ionos.de

DIE WICHTIGSTEN NACHHALTIGKEITSASPEKTE



SAP-LIZENZIERUNG: WIE UNTERNEHMEN KOSTEN SPAREN

BENUTZERAKTIVITÄTEN ANALYSIEREN UND DIGITAL ACCESS NUTZEN

SAP-Systeme kommen zwar in vielen Unternehmen zum Einsatz, doch die entsprechende SAP-Lizenzierung gibt es nicht. So verfügt jeder Betrieb über individuelle Typen und Kombinationen. Durch regelmäßige Nachkäufe wächst das System dann unstrukturiert weiter. Dies hat nicht nur zur Folge, dass die Lizenzierungen mit der Zeit unübersichtlicher werden, sondern auch schnell unnötige Kosten entstehen. Denn häufig stimmen die Lizenzen nicht mit den tatsächlichen Benutzeraktivitäten überein. In Sachen Lizenzierung gilt es daher, ein paar grundlegende Dinge zu beachten. Dazu gehört auch, sich mit dem Thema Digital Access zu befassen. Hier eröffnet sich für Unternehmen eine Chance, um unternehmensweite Kosten nachhaltig zu reduzieren.

LIZENZEN UND BERECHTIGUNGEN SIND ANHAND DER TATSÄCHLICHEN BENUTZERAKTIVITÄTEN REGELMÄSSIG ZU ÜBERPRÜFEN UND OPTIMIEREN.

Andreas Knab,
Experte für SAP-Berechtigungen und Lizenzierung bei der SIVIS, sivis.com

Das Thema SAP-Lizenzierungen rückt in Unternehmen immer dann in den Fokus, wenn beispielsweise neue Benutzer hinzukommen, bestehende Lizenzen erweitert werden oder der jährliche Vermessungstermin ansteht. Hier kommt es oftmals zu Über- und Nach-Lizenzierungen. Diese können Unternehmen mit wenig Aufwand vermeiden.

Mit Vorlauf und konkreten Wünschen in die Verhandlung gehen

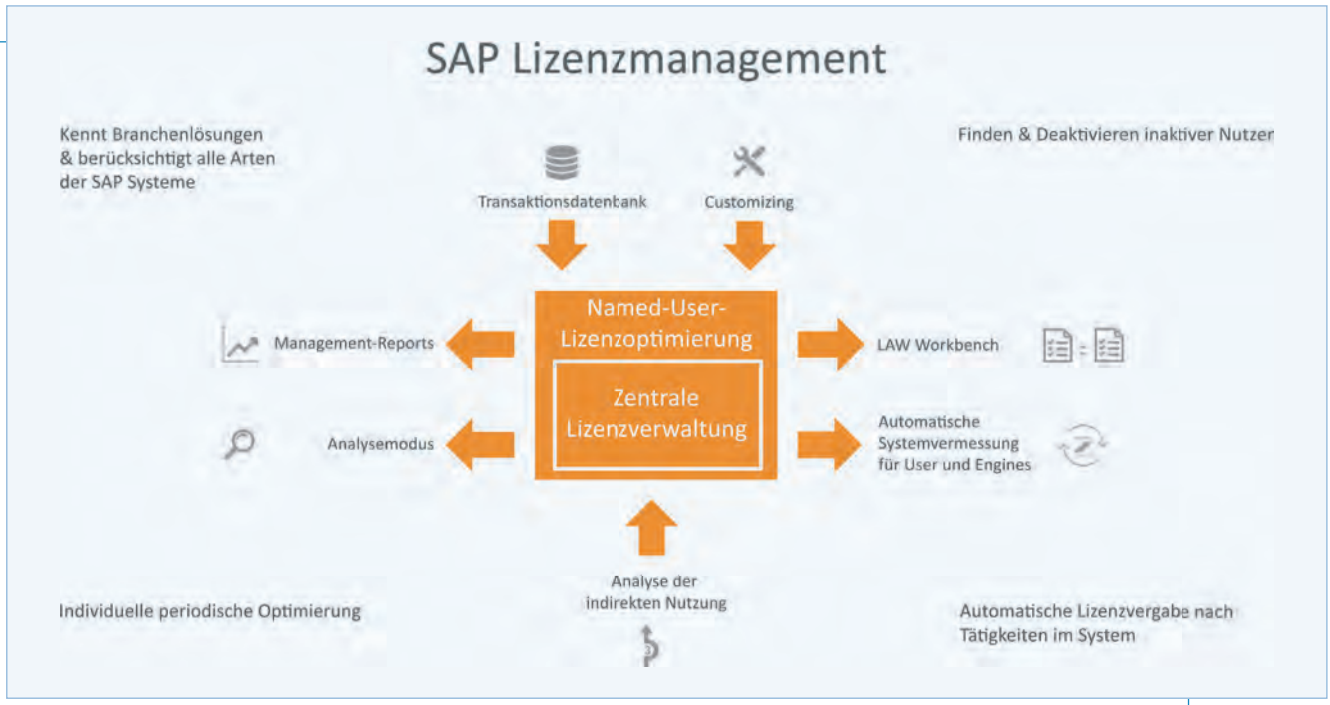
Unternehmen sollten sich nicht erst mit dem Lizenzmanagement auseinandersetzen, wenn der Vermessungstermin kurz vor der Tür steht. Denn dann drängt die Zeit. Um auf Augenhöhe zu verhandeln, brauchen Unternehmen ausreichend zeitlichen Vorlauf und fundierte Informationen zu den wirklich notwendigen Lizenztypen. Verlässt sich die Administration blind darauf, dass über das Jahr die richtigen Lizenzen verteilt wurden, sorgt das spätestens bei der SAP-Vermessungsaufforderung für hastige Nachkäufe. Ausgehandelte Unternehmensrabatte gehen dann häufig verloren und es werden Listenpreise aufgerufen. Daher empfiehlt es sich, proaktiv und mit konkreten Lizenzwünschen auf SAP zuzugehen. Ist das Angebot nicht zufriedenstellend, haben Unternehmen noch ausreichend Zeit, um nachzujustieren oder sich nach Alternativen umzusehen.

Regelmäßiges Prüfen legt tatsächlichen Bedarf offen

Darüber hinaus sollten Unternehmen vorhandene Lizenzen und Berechtigungen regelmäßig überprüfen – und zwar anhand der tatsächlichen Benutzeraktivitäten. Hier reichen manuelle Prüfungen nicht aus. Sie ermöglichen im Grunde nur Schätzungen. Hinzu kommt, dass die SAP ihre Lizenzierungen nach Berechtigungen erteilt. Das bedeutet: Einzelne Nutzer haben dann zwar viele Berechtigungen im System, von denen sie aber einige gar nicht verwenden. Mit einer technischen Analyse lassen sich die Benutzeraktivitäten genau ermitteln – und damit auch der tatsächliche Bedarf an Berechtigungen und entsprechenden Lizenzen. Eine solch softwarebasierte Analyse deckt ebenso ungenutzte Tätigkeiten in den Berechtigungen auf. Hebt man diese Berechtigungen auf, werden teure Lizenzen frei. Diese stehen dann bei Fehlbeträgen in der Vermessung zur Verfügung. Unnötige Nachkäufe und damit verbundene Kosten lassen sich mithilfe einer genauen Analyse zuverlässig vermeiden. Zudem weisen solche Lizenzierungsmanager jedem Nutzer anhand seiner Berechtigungen automatisch die kostengünstigste Lizenz zu.

Mit S/4HANA Kapital wieder freisetzen

Es gibt auch andere Optionen für die Lizenz-Optimierung. Der Umstieg von ECC auf S/4HANA etwa bietet Unternehmen nicht nur eine zukunftsorientiertere Arbeitsweise, sondern auch eine ideale Gelegenheit, die Lizenzierung neu anzugehen. Denn die Einführung kann als Product Conversion oder Contract Conversion erfolgen. Während bei ersterem die bestehenden Verträge weitgehend bestehen bleiben, lässt sich bei zweiterem der SAP-Lizenzvertrag komplett neu aufrollen. So können Unternehmen Kapital, das über viele Jahre in zu teure Lizenzen in-



Quelle: Sivis-GmbH

vestiert wurde, wieder freisetzen. Nicht benötigte Lizenzen werden in Credits umgewandelt und lassen sich für Neukäufe nutzen. Neben „Developer" und „Professional" bietet S/4HANA noch zwei weitere Lizenztypen an. Beide sind mit umfangreichen Funktionalitäten ausgestattet. Dazu müssen Unternehmen aber wissen, was sie wirklich brauchen. Sich an den Mappingtabellen der SAP zu orientieren oder gar die SAP den Bedarf schätzen zu lassen, gestattet nur eine grobe Annäherung an den tatsächlichen Bedarf. Dies führt dazu, dass Unternehmen eventuell zu viele oder falsche Lizenzen erwerben. Deshalb ist eine Analyse der tatsächlichen Benutzertätigkeiten sinnvoll. Zudem sollten Entscheider vor dem Kauf zunächst eine S/4HANA Testsimulation laufen lassen. So können sie noch vor Vertragsabschluss bei den Lizenzen nachsteuern.

Digital Access jetzt angehen und Kosten sparen

Bereits seit einigen Jahren bereitet SAP die flächendeckende Bepreisung von Digital Access, also den Zugriff von fremden Systemen auf SAP, vor und wird diese auch in absehbarer Zeit geltend machen. Sofern noch nicht vertraglich geregelt, ist ein Fremdzugriff kostenpflichtig. Um dann nicht von teuren Rechnungen überrascht zu werden, ist es ratsam, dass sich Unternehmen Klarheit bezüglich ihrer Digital Access verschaffen. Zum einen verhindern sie so ein böses, weil kostspieliges, Erwachen, zum anderen können sie proaktiv mit SAP ins Gespräch gehen. Wenn sich Unternehmen jetzt darum kümmern, werden sie mit einem großzügigen Entgegenkommen durch die SAP belohnt. Hinsichtlich Digital Access müssen Betriebe generell entscheiden, ob sie die Aktivitäten individuell oder nach erzeugten Dokumenten lizenzieren möchten. Beide Wege können sinnvoll sein. Für eine gute Verhandlung mit der SAP sollte aber die reelle Basis auf Dokumenten-Ebene bekannt sein. Zu beachten ist auch, dass das SAP-Tool Passport oftmals nicht ganz fehlerfrei vermisst. Es empfiehlt sich eine Analyse durch einen Lizenzierungsmanager, um sowohl eine korrekte Zählung als auch die Herkunft der Dokumente und die Verhandlungsvarianten zu ermitteln.

Vorteile des Digital Access Adaption Program nutzen

Für Unternehmen, die sich mit Digital Access noch auseinandersetzen müssen, empfiehlt es sich, das Digital Access Adoption Program (DAAP) in Anspruch zu nehmen. Das Programm wurde erneut verlängert und läuft noch bis Ende 2022. SAP bietet Kunden Sonderkonditionen, wenn sie bereits jetzt auf das neue, dokumentenbasierte Lizenzmodell umsteigen. Die benötigten Dokumente können im Zuge des DAAP zum Beispiel mit einem Rabatt von 90 Prozent bezogen werden. Zudem sind bei der Teilnahme am Digital Access dann alle anderen indirekten Tätigkeiten kostenfrei.

Fazit: Proaktiv und schnell sein zahlt sich aus

Keine Frage: Die Beschäftigung mit SAP-Lizenzierungen ist komplex und für Unternehmen im Alleingang nur schwer zu durchdringen. Doch mit der richtigen Strategie gehören unnötige Nachkäufe und Kosten der Vergangenheit an. Unternehmen sind daher gut beraten, ihre Benutzeraktivitäten technisch genau zu analysieren und ihren Status quo hinsichtlich des Fremdzugriffs der eigenen Systeme auf SAP frühzeitig zu klären. Wer proaktiv auf die SAP zugeht und den Digital Access zügig regelt, profitiert von Sonderkonditionen und reduziert nachhaltig Kosten.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 7 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download

5 SCHRITTE ZUR GUTEN UNTERNEHMENSFÜHRUNG

WIE SELBSTVERWALTETE DOKUMENTE DIE INFORMATION GOVERNANCE VEREINFACHEN KÖNNEN

Seien wir doch ehrlich: Information Governance ist wahrscheinlich nicht Ihr Lieblingsthema. Deshalb sollte sie effizient und nahtlos erfolgen, damit die Mitarbeiter sich auf spannendere, innovative und geschäftsfördernde Ziele konzentrieren können.

Es gibt viele Gründe, warum Unternehmen sich nicht mit Information Governance befassen. Und viele gute Gründe, warum sie es doch tun sollten.

Moderne, zentrale, cloudbasierte Content Management-Lösungen mit selbstverwalteten Dokumenten machen Compliance-Prozesse für Mitarbeiter intuitiver und ermöglichen eine sichere Zusammenarbeit.

Dieses Whitepaper gibt Ihnen einen Überblick, wie selbstverwaltete Dokumente die Information Governance vereinfachen können.

DIGITALE TRANSFORMATION MIT SAP/S/4HANA

ZUKUNFTSSICHERHEIT DURCH END-TO-END-PROZESSE

In Zeiten digitalisierter Prozesse, Predictive Analytics und unbegrenzter Mobilität müssen die Systeme von Unternehmen immer größere Datenmengen bewältigen. Doch was nützen unzählige Daten, wenn Ihr System diese nur schleppend analysieren und auswerten kann? Als Antwort darauf hat SAP S/4HANA mit der zugehörigen Datenbank SAP HANA entwickelt.

Damit der Umstieg auf S/4HANA reibungslos gelingt, ist die Zusammenarbeit mit einem Partner unerlässlich, der End-to-End sämtliche Prozesse der Migration begleitet und über ein großes Maß an Implementierungsverfahren verfügt. Dieses Whitepaper zeigt auf, welche Schritte dafür von der Planung bis zum erfolgreichen Abschluss notwendig sind und was es dabei zu beachten gibt.

WHITEPAPER DOWNLOAD

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

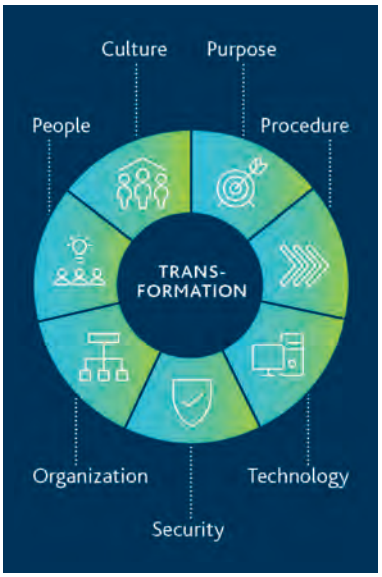
VOM ERP-MONOLITH ZUM FLEXIBLEN ÖKOSYSTEM

MODERNISIERUNG DER APPLIKATIONSARCHITEKTUR

Ab einer gewissen Größe kommt kaum ein Unternehmen an SAP vorbei. Als omnipräsenter Backbone stellt das ERP-System vielerorts einen reibungslosen Geschäftsablauf sicher. Dementsprechend muss SAP die individuellen Prozesse jedes Unternehmens bestmöglich abbilden. Weil es jedoch keine generell für alle passenden SAP-Komponenten oder -Applikationen am Markt gab, sind mit der Zeit individuell entwickelte, monolithische SAP-Landschaften entstanden, die wegen ihrer Komplexität sehr aufwändig zu managen und weiterzuentwickeln sind.

Mehr Individualität dank Standardisierung

Der Aufbau einer modernen Applikationslandschaft geht mit einem Paradigmen-Wechsel einher: weg vom individuellen On-Premises-System hin zu SAP S/4HANA als standardisiertem SAP-System samt flexiblem Betrieb in der Cloud und Zugang zu innovativen, Cloud-nativen Services. Sein SAP-System derart zu modernisieren, ist ein wirkungsvolles Transformationsinstrument – sofern die Migration mit der Geschäftsstrategie im Einklang steht. SAP S/4HANA bildet die technologische Grundlage für nutzerfreundliche Ökosysteme, welche durch die bedarfsgerechte Integration von Subsystemen und Cloud-nativen Drittlösungen entstehen. Eine solche Plattform-Ökonomie ist die Antwort auf aktuelle Business-Anforderungen: Unternehmen adaptieren alte Prozesse und bilden zugleich neue Abläufe passgenau ab – in einer Dynamik und Geschwindigkeit, die ihresgleichen sucht. So senken Firmen nicht nur ihre Kosten für Betrieb und Wartung, sie verkürzen auch die Time-to-Market. Sinnvolle Zusatzservices sind in kürzester Zeit verfügbar - dank der Architektur eines flexiblen Ökosystems und durch einen Dienstleister, der Unternehmen bei ihrer Transformation ganzheitlich unterstützt.



arva.to/sapdigital22

INTEGRATION MIT SAP

EFFIZIENTE UNTERNEHMENSSTEUERUNG DURCH INTEGRIERTES UND INTELLIGENTES VERTRAGSMANAGEMENT

Die Geschwindigkeit der digitalen Transformation hat in den letzten Jahren in Deutschland viele Unternehmen gezwungen, ihre Geschäftsprozesse komplett neu zu konzipieren und zu implementieren. Dies betrifft keineswegs nur Prozesse in der Fertigung oder die Unternehmensplanung mit den CRM- und ERP-Anwendungen, sondern auch das Vertragswesen.

Und Verträge sind für jedes Unternehmen relevant, seien es die Arbeitsverträge mit den Mitarbeitenden oder Verträge mit Lieferanten, Kunden und Partnern. Durch die Vielzahl der geschäftlichen Verbindungen kann die Zahl der Verträge in einem global tätigen Konzern durchaus im siebenstelligen Bereich liegen. Daraus wir deutlich, welche Rolle das Vertragswesen angesichts der Verwaltung von Millionen von Verträgen in den Unternehmen zuweilen spielt. An einem leistungsfähigen Vertragsmanagement (CLM, Contract Lifecycle Management) kommen große Organisationen heutzutage kaum vorbei.

Unter CLM ist jedoch keinesfalls zu verstehen, lediglich neue Verträge auf Basis existenter Word-Vorlagen zu erstellen. Es geht bei intelligentem CLM auch darum, Klauseln und Bedingungen neuer und bestehender Verträge zu prüfen, doch in vielen Unternehmen ist das nach wie vor ein manueller Prozess. Ein automatisierter Vergleich, der für den Vertrag wichtige Parameter beispielsweise aus SAP Ariba, automatisch extrahieren oder auch die allgemeinen Geschäftsbedingungen berücksichtigen kann, ist dort oft nicht vorgesehen.

Doch es steht wohl außer Frage, dass neue Verträge nicht nur die Metadaten einer Word-Vorlage übernehmen, sondern die bereits existierenden Preise, Lieferbedingungen, Fristen und vieles mehr in aktuell gültiger Form berücksichtigen müssen. Auf diese Weise wird das intelligente CLM-System ein zentrales und integratives Element der Unternehmenssteuerung. Dies unterstützt gleichzeitig auch das Risikomanagement im Unternehmen.

Doch wie lassen sich intelligentes CLM und SAP Ariba integrieren? Ein Beispiel hierfür ist ICI (Icertis Contract Intelligence), die Plattform des US-Herstellers Icertis, die unter anderem bei deutschen Unternehmen wie BASF, Daimler, der DATEV, der EMAG-Gruppe, Porsche oder auch Rentschler zum Einsatz kommt.

Verträge als Kern der Organisation

Für den Integrationsansatz muss man sich zunächst darüber im Klaren sein, dass alle formalen Beziehungen eines Unternehmens über Verträge definiert sind.

Eine moderne CLM-Lösung kann dabei nicht nur neue, digital erstellte Verträge verwalten, sondern unterstützt auch sogenannte Legacy-Verträge, also alte Verträge, die möglicherweise bisher nur in Papierform existierten. ICI kann dann gescannte Verträge automatisch über OCR „lesen", interpretieren und mit Hilfe künstlicher Intelligenz die darin enthaltenen Vereinbarungen analysieren und Attribute identifizieren, Klauseln zuordnen und vollständig durchsuchbar bereitstellen. Es entsteht somit nicht nur ein digitales Foto der Verträge, sondern echte, durchsuchbare und wiederverwendbare Dokumente.

Nachdem das intelligente Vertragsmanagement die gescannten Inhalte und Vertragsklauseln erfasst und analysiert hat, lassen sich diese mit Daten vergleichen, die in SAP Ariba für den Einkauf oder für den Vertrieb hinterlegt sind. Auf diese Weise kann sehr schnell jeder papierbasierte Vertrag integrativer Teil eines Geschäftsprozesses werden und seine Klauseln für weitere, neue Verträge als Musterklauseln und Vorschläge dienen.

EIN SYSTEM WIE ICI KANN ÜBER EINE BEWERTUNG DER PARAMETER EINES VERTRAGS WERTVOLLE INFORMATIONEN FÜR DAS RISIKO-MANAGEMENT LIEFERN UND DAMIT DIE COMPLIANCE IM UNTERNEHMEN VERBESSERN.

Martin Mohr,
Vice President Business Development & Alliances EMEA, Icertis, www.icertis.com

Unterstützung für Vertragsverhandlungen

Umgekehrt kann das CLM die Anwender auch darüber informieren, dass der soeben gescannte Vertrag veraltet ist, die Klauseln ungültig und überholt sind. „Auf Basis künstlicher Intelligenz kann sie diese alten Vertragsinhalte mit aktuellen, passenden in Beziehung setzen und auf

diese Weise für Verhandlungen direkt Vorschläge liefern", erklärt Martin Mohr, Vice President Business Development & Alliances EMEA von Icertis. „Neu erstellte Verträge hingegen verwenden automatisch die aktuellen Klauseln."

Die SAP-Integration ermöglicht zudem Widersprüche zwischen unterschiedlichen Verträgen zu vermeiden. Beispielweise könnte ein Mitarbeiter einem Kunden unabsichtlich falsche Konditionen für eine Lieferung zusagen. Doch noch bevor der Vertrag unterschrieben ist, erkennt das CLM, dass sich die Lieferkonditionen im Entwurf des Vertrags von denjenigen in SAP Ariba unterscheiden. Ein Vertrag mit falschen oder ungültigen Konditionen ließe sich dann gar nicht erst erstellen.

Kennzahlen für das Management

Allerdings ergeben sich nicht nur bei der Vertragserstellung Vorteile durch die Integration von CLM mit SAP. Es lassen sich auch wesentliche Kennzahlen, die auf diese Weise direkt mit den Verträgen verbunden sind, über Dashboards analysieren. Diese Dashboards müssen dabei keineswegs proprietäre Lösungen der CLM-Lösung sein. Weitaus sinnvoller ist es, wenn sich das Vertragsmanagement in existierende Angebote wie Power-BI, Tableau oder QlikView integrieren lässt.

Dies wiederum führt zum nächsten Aspekt: die Überwachung des Erfüllungsgrades eines Vertrags – stimmen die vereinbarten Lieferfristen, die Preise und die Qualität der Lieferungen? Mit Hilfe von Alerts kann das CLM die jeweils Verantwortlichen zum Handeln auffordern, falls KPIs von zuvor definierten Grenzwerten abweichen. Ein Abgleich von Daten, ob unter Umständen der Vertrag etwas anderes vorgibt als das ERP- oder CRM-System, sind schlicht überflüssig, da der Vertrag eben automatisch genau diese Werte enthält. „Zudem kann ein System wie ICI über eine Bewertung der Parameter eines Vertrags wertvolle Informationen für das Risiko-Management liefern und damit die Compliance im Unternehmen verbessern", so Mohr.

Integration beschleunigt Prozesse

Auf diese Weise wird deutlich, dass die Integration von CLM mit SAP-Lösungen ein hohes Potenzial an Produktivitätssteigerung bei gleichzeitiger Entlastung der Mitarbeitenden ermöglicht. Ist das CLM mit SAP Ariba integriert, können bei einem neuen Vertrag direkt die Einkaufskonditionen aus SAP in den Vertrag übernommen werden. Großer Abstimmungsbedarf zwischen Rechtsabteilung und Einkauf oder Vertrieb ist nicht länger notwendig. Der Vorteil dieser Vorgehensweise ist offensichtlich: Da die Basis der rechtlichen Vorschläge bereits im CLM abgebildet ist und gleichzeitig die Daten aus SAP Ariba einfließen, lassen sich Vertragsabschlüsse mit Kunden und Lieferanten bei gleichzeitiger Entlastung aller Beteiligten deutlich schneller erreichen.

Frank Mihm-Gebauer

SICHERHEIT UND NUTZERFR

REMOTE WORK TOOLS MÜSSEN LEICHT ZU BEDIENEN SEIN, OHNE DEN SICHERHEITS

Wenn Unternehmen an Sicherheit denken, denken sie oftmals an Passwörter, Verschlüsselung und Hackerangriffe. Mit dem Übergang zu flexibler, hybrider oder vollständiger Fernarbeit gibt es viele neue Aspekte, die in der Sicherheitsgleichung auftauchen und vor allem auch den Anforderungen an Unternehmensstandards standhalten müssen. Business-Software hat dabei meist den Nachteil, dass die Nutzerfreundlichkeit vernachlässigt wird. Doch die Anwender sind mitunter nicht technikaffin, sodass Benutzeroberflächen nicht intuitiv bedienbar sind. Laut einer Untersuchung von Lünendonk sehen Unternehmen die Digital Experience zwar als ein Schlüsselelement zur Kundengewinnung und -bindung, doch die Mehrheit der Unternehmen (65 Prozent) empfindet die Qualität ihrer digitalen Nutzererfahrung im Wettbewerbsvergleich jedoch nur „auf Augenhöhe". Als Vorreiter sieht sich nur jedes zehnte Unternehmen (9 Prozent).

Consumer-orientiert aber sicher vernetzen

Vor allem in den Bereichen Kommunikation und Support sind Menschen aus dem Privaten an Messenger, Videotelefonie und Social-Media-Apps gewöhnt und wünschen sich die gleiche intuitive Bedienbarkeit für Unternehmensanwendungen im Browser. Consumer-orientierte Usability spart am Ende Zeit und Geld, gerade auch bei Unified-Communication-and-Collaboration-Tools (UCC) oder Remote-Support-Anwendungen, da die Nutzer einwandfrei remote mit Kollegen und Kunden kommunizieren können. Diese Plattformen müssen jedoch sicher sein, um sichere und private digitale Räume für Anrufe, Meetings, virtuelle Veranstaltungen, Supportanfragen und vieles mehr zu bieten.

UCC und Support sind für flexibles Arbeiten unverzichtbar, aber Systeme vor Ort sind teuer und ressourcenintensiv in der Wartung und Gewährleistung der Sicherheit. Cloud-basierte Systeme ermöglichen einen schlanken und nahtlosen Betrieb, da Infrastruktur und Know-how an den Anbieter ausgelagert werden. Die höhere Anwenderzufriedenheit ist dabei oft ein unterschätzter Aspekt, da Unzufriedenheit gerade im Cloud-Zeitalter zum schnellen Anbieterwechsel führen kann. Sicherheit und Datenschutz führen jedoch meist dazu, dass Cloud-Anwendungen an Komplexität zunehmen und zusätzliche Sicherheitshürden ausgerollt sind, um den Zugriff zu Apps und Dateien besser zu sichern. Hier gilt es von IT-Seite einen guten Kompromiss zu finden, um die Sicherheitsstandards im Unternehmen weiterhin hoch zu halten, den Mitarbeitern aber gleichzeitig einfach zu nutzende und schnell zugängliche Anwendungen zur Verfügung zu stellen.

GoTo zeigt, wie wichtig Datenschutz und Sicherheit zum Schutz persönlicher und vertraulicher Informationen gerade auch bei Kommunikations- und Supporttools ist und nennt drei unerlässliche Sicherheitsfunktionen, die eine UCC- oder Support-Lösung für den Business-Einsatz benötigt, um externe Datenzugriffe zu verhindern:

1. Konsolidierung in einer Anwendung

Für eine einheitliche Sicherheitsstruktur sorgen All-in-One-Lösungen für Unified Communications as a Service (UCaaS), Contact-Center-as-a-Service (CCaaS) und Remote-Support. Über sie führen Mitarbeiter Anrufe, Meetings und Nachrichten oder bearbeiten Supportanfragen von einer einzigen Plattform aus und wechseln innerhalb derselben Anwendung problemlos zwischen den Kanälen. Auch IT-Teams haben so nur ein einziges Verwaltungsportal und können die Einstellungen, die zuvor in verschiedenen Anwendungen erfolgten, gesammelt managen. Durch die Konsolidierung auf einen Anbieter profitieren Unternehmen von Konnektivität und Zuverlässigkeit und bieten oftmals eine Vielzahl von Integrationen mit bestehenden CRMs und Kollaborationstools wie Slack und Microsoft Teams.

> SICHERHEIT UND DATENSCHUTZ FÜHREN MEIST DAZU, DASS CLOUD-ANWENDUNGEN AN KOMPLEXITÄT ZUNEHMEN UND ZUSÄTZLICHE SICHERHEITSHÜRDEN AUSGEROLLT SIND, UM DEN ZUGRIFF ZU APPS UND DATEIEN BESSER ZU SICHERN.
>
> Sion Lewis, VP und Managing Director EMEA, GoTo, www.go.to.com

2. Implementierung von Sicherheitskontrollen

Um die Kommunikations- und Supportinfrastruktur und die darin enthaltenen

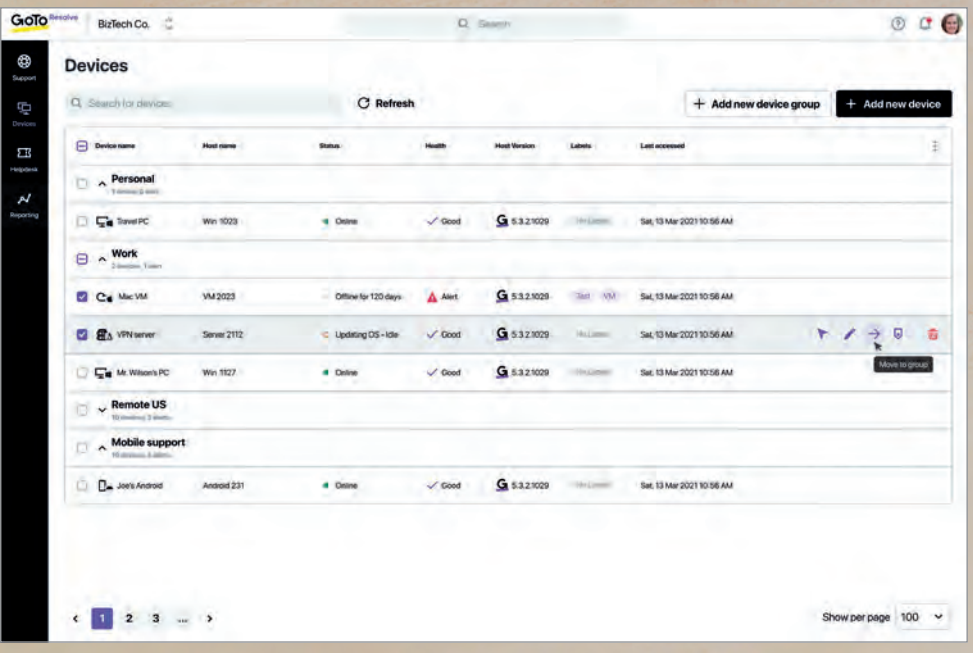
EUNDLICHKEIT

STANDARD ZU VERNACHLÄSSIGEN

Daten zu schützen, gilt es branchenübliche Sicherheitskontrollen einzusetzen. Mithilfe von logischer Zugriffskontrolle oder einem Perimeterschutz-Tool vermindern Administratoren die Bedrohung durch unbefugte Anwendungszugriffe oder nicht autorisierten Netzwerkverkehr. Cloud-Lösungen wie UCaaS oder CCaaS haben darüber hinaus den Vorteil, dass die Daten zentral gespeichert vorliegen und IT-Verantwortliche Backups zentral und automatisiert erstellen können. Neben dem Schutz vor Malware und einer Ende-zu-Ende-Verschlüsselung (E2EE) für die schriftliche und verbale Kommunikation gilt es vor allem auch Schwachstellenmanagement und monatliche Netzwerk-Scans zu betreiben, um die Nutzung der Remote-Work-Lösungen immer im Blick zu behalten. Mithilfe einer Protokollierung erhalten Administratoren in Verdachtsfällen einen Alarm und können einem missbräuchlichen Datenverkehr schnell entgegenwirken. Diese Funktionen erfolgen zum großen Teil im Hintergrund und beeinträchtigen die Nutzung der Kommunikationssoftware nur geringfügig, bieten aber ein hohes Maß an Sicherheit und Datenschutz.

3. Ein engagiertes Sicherheitsteam

Ein ausgereifter Business-Continuity-Plan stellt sicher, dass alle Produkt- und Betriebsteams auch dann voll funktionsfähig sind, wenn sie aus der Ferne arbeiten. Seit der COVID-19-Pandemie ist es ratsam die Netzwerkkapazität und die Fähigkeit, Datenverkehr zu verschieben, zu erhöhen. Nur so kann die IT-Abteilung einen Single Point of Failure vermeiden.



Ein Monitoring aller Cloud-Dienste rund um die Uhr hilft dabei, die Datenschutz- und Informationssicherheitsstandards in Unternehmen zu erfüllen oder sogar zu übertreffen.

Leider kam es während der Pandemie und mit der Zunahme an Remote Work in den Unternehmen in vielen Branchen zu einem sprunghaften Anstieg von Cyberangriffen, darunter Malware, Phishing-Angriffe, gefälschte Websites, Spammer und Scammer. Laut BSI bewerten über 26 Prozent der befragten Unternehmen, die aktiv auf Cyber-Angriffe reagieren mussten, die Schäden als „existenzbedrohend" oder sehr „schwer" und es entstanden Schäden in Höhe von 52,5 Milliarden Euro durch Angriffe im Homeoffice.

Eine implementierte risikobasierte Authentifizierung hilft solchen Schäden entgegenzuwirken. Denn Plattformen, die verdächtiges Verhalten in den Nutzerprofilen vor allem bei der Anmeldung per Fernzugriff von einem nicht-autorisierten Gerät erkennen, können Fremdzugriffe von Hackern vermeiden und geben der Unternehmens-IT ein zusätzliches Security-Layer. Autorisierte Nutzer innerhalb der Belegschaft hingegen profitieren von nutzerfreundlichen, einfachen Anmeldeprozessen via Single-Sign-on, um schnell Zugang zu Daten und virtuellen Meetings zu erhalten.

Sion Lewis

DIGITAL OFFICE CONFERENCE

ERFOLGSFAKTOR FÜR DIGITALES ARBEITEN

Das Digital Office ist wichtiger denn je, da die täglichen Anforderungen an unsere Arbeit gewachsen sind und digitale Geschäfts- und Verwaltungsprozessen erfordern, die agil und ortsunabhängig umgesetzt werden können. Verschiedenste Prozesse zu digitalisieren kann nicht nur auf die Effizienz, Innovation und Wachstum eines Unternehmens einwirken, sondern auch das Fundament für neue Geschäftsmodelle legen. Der Schlüssel zum Erfolg liegt darin, die richtigen Entscheidungen für das „Digital Office" zu treffen. Cloud statt Aktenschrank, Online-Meeting statt Geschäftsreise, Bestellungen und Rechnungsversand über Kundenportale statt per Brief und Fax!

Diskutieren Sie auf der Digital Office Conference (#doc22) am 18. Mai 2022, wie das Zusammenspiel zwischen menschlichem Know-how und innovativen Technologien unsere Unternehmensprozesse einfacher, schneller und transparenter gestaltet.

Wir unterstützen die #doc22 als Partner und laden Sie herzlich dazu ein, sich gemeinsam mit uns über das digitale Büro der Zukunft auszutauschen.

Ort: Online
Eintrittspreis: kostenlos anmelden
Veranstalter: Bitkom e. V. in Kooperation mit Bitkom Servicegesellschaft mbH
Albrechtstr. 10, 10117 Berlin

© Carolina Garcia Tavizon – unsplash.com

MANAGED SERVICES

MARKT WELTWEIT AUF HÖCHSTSTAND

Die IT-Dienstleistungsbranche geht gestärkt aus der Pandemie hervor. So auch im Markt für Managed Services. 2021 belief sich der jährliche Vertragswert (Annual Contract Value, ACV) der Neuabschlüsse weltweit auf fast 33 Milliarden Dollar. Der ACV umfasst alle Dienstleisterverträge, deren jährliche Erlöse mindestens 5 Millionen US-Dollar betragen. Darüber hinaus hat das Marktforschungs- und Beratungsunternehmen Information Services Group (ISG) ausgewertet, welchen Anteil die unterschiedlichen Anbietergruppen am Gesamtmarkt haben. Multinationale Provider, so etwa große US-amerikanische und europäische Dienstleister, gewannen im Jahr 2021 etwa 40 Prozent des ACV. Unmittelbar dahinter liegen indische Unternehmen. Sie erzielten einen Anteil von rund 30 Prozent. Mittelgroße IT-Dienstleister und BPO-Anbieter (Business Process Outsourcing) gewannen jeweils etwa 10 Prozent. Die übrigen 7 Prozent verteilten sich auf eine Reihe unterschiedlicher Spezialanbieter, so etwa Engineering-Dienstleister.

www.isg-one.com

UNIFIED COMMUNICATIONS

WETTBEWERBSVORTEIL KOMMUNIKATION

FLEXIBLE NUTZUNGSSZENARIEN UND INTUITIVE BEDIENUNG VON UC-PLATTFORMEN BILDEN DIE GRUNDLAGE FÜR MODERNES, HYBRIDES ARBEITEN.

Dr. Klaus von Rottkay, CEO, NFON AG, www.nfnon.com/de

Hybride Arbeitsmodelle werden immer mehr zur Norm und entsprechen den modernen Anforderungen von Mitarbeitern. Für Unternehmen, die sicherstellen möchten, dass ihre Teams zu jeder Zeit produktiv arbeiten können, führt deshalb kein Weg an Unified Communications (UC) vorbei. Denn UC können einen entscheidenden Erfolgsfaktor darstellen.

Effektive Kommunikations-Lösungen ermöglichen einen optimalen Austausch von Informationen, erleichtern die Zusammenarbeit und sorgen so für eine erhöhte Produktivität. Eine moderne UC-Plattform bietet ein einheitliches System, in das alle Kommunikationskanäle eines Unternehmens eingebettet werden. Bestenfalls wird es sogar in der Cloud gehostet und sorgt so für zusätzliche Flexibilität für Mitarbeiter im Büro, Homeoffice oder unterwegs.

Der große Vorteil von UC-Lösungen ist die zentrale Bündelung von Kommunikations- und Kooperations-Apps. So können Teammitglieder über eine einzige Schnittstelle Anrufe tätigen, Chatnachrichten versenden, Videokonferenzen öffnen oder Dateien austauschen. Das erleichtert die Echtzeit-Kommunikation mit Kollegen enorm, denn es ist nicht mehr nötig andauernd zwischen verschiedenen Anwendungen oder sogar Geräten zu wechseln.

Jederzeit und von überall aus arbeiten

Unified Communications Plattformen verbinden Schnittstellen, wie Serververwaltung, Videoüberbrückungen oder VoIP Systeme, um nahtlose Benutzererfahrungen zu schaffen. Gleichzeitig bietet der Front-End-Client Zugang zu allen integrierten Anwendungen und Lösungen.

Diese Kombination von leistungsstarker Technik und intuitiver Bedienung macht UC zu einer äußerst praktischen Lösung. Denn Nutzer können alle Tools in Echtzeit verwenden, ohne sich in unendlichen E-Mails zu verlieren oder die nächste Besprechung zu verpassen, weil der Link verschwunden ist. UCs ermöglichen somit eine optimierte digitale Arbeitsumgebung für alle Mitarbeiter und dabei spielt es keine Rolle, ob diese lieber im Büro oder von Zuhause aus arbeiten wollen.

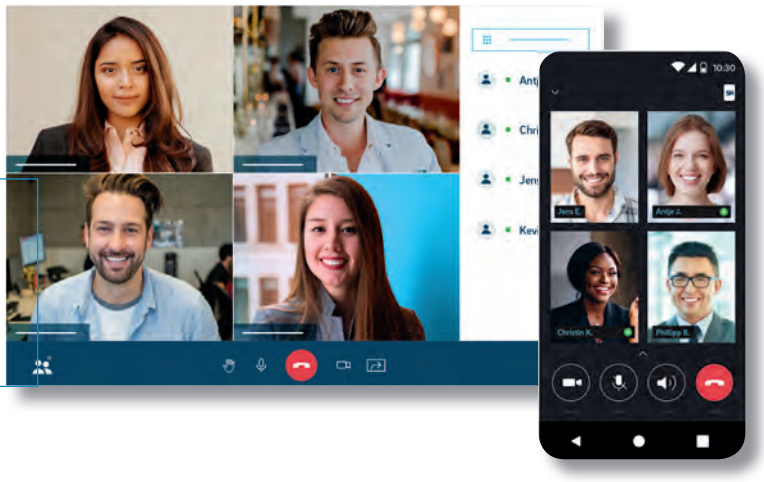
Mehr Flexibilität

Der Trend geht ganz klar in Richtung hybrider Arbeit. Deshalb benötigen Unternehmen UC-Lösungen, die von überall und ständig zugänglich sind. Hier bieten sich Unified Communications as a Service (UCaaS) an, um von der Vielseitigkeit der Cloud zu profitieren. UCaaS Plattformen werden online bereitgestellt, wodurch Benutzer von jedem Gerät aus auf die Cloud Anwendungen zugreifen können.

Cloud Unified Communications Plattformen können darüber hinaus durch ihre Anpassungsfähigkeit, einfache Skalierbarkeit und Kosteneinsparungen überzeugen. Unternehmen müssen keine großen Investitionen für eine lokale Plattform tätigen. Stattdessen zahlen Sie eine monatliche Gebühr für die Cloud-UC-Dienste, die jederzeit um zusätzliche Anwendungen erweitert werden können.

Produktive und sichere Arbeitsumgebungen

UCs ermöglichen effektiveres Arbeiten, nahtlose Zusammenarbeit und mehr Flexibilität bei der Wahl der alltäglichen Kommunikations-Tools. Das verbessert interne Arbeitsabläufe und Kundenerlebnisse gleichermaßen. Unternehmen profitieren von erhöhter Sicherheit, da UCs mehrere potenzielle Angriffspunkte vereinen und somit sensible Daten durch eine einheitliche Verschlüsselung schützen können. So schaffen sie produktive und sichere virtuelle Arbeitsplätze für eine digital geprägte Zukunft.



Unified Communications ermöglichen reibungslose Business-Kommunikation

ZENTRALE RECHENKAPAZITÄTEN NACHHALTIG AUSBAUEN

DAS UMWELTZEICHEN BLAUER ENGEL ZERTIFIZIERT BESONDERS KLIMA- UND RESSOURCENSCHONENDE RECHENZENTREN

Konferenzen und Meetings online durchzuführen, gehört mittlerweile zum Arbeitsalltag vieler. Die Pandemie hat den digitalen Wandel in einigen Bereichen beschleunigt, und auch unabhängig davon wird durch den digitalen Umbau in allen Lebensbereichen die Nachfrage nach zentraler Rechenleistung immer größer. Rechenzentren benötigen jedoch besonders viel Energie, weswegen neue Einrichtungen ab 2027 klimaneutral betrieben werden sollen. Zudem sollen für IT-Beschaffungen des Bundes Zertifizierungen wie der Blaue Engel Standard werden. Das Umweltzeichen Blauer Engel zeichnet schon heute vorbildliche Rechenzentren aus und setzt mit den Kriterien den Standard für klima- und ressourcenschonende Rechenzentren.

Blauer Engel

Seit dem Jahr 2011 gibt es den Blauen Engel für den Rechenzentrumsbetrieb und seit dem Jahr 2020 den für Co-Location-Rechenzentren. Der Blaue Engel ist damit das erste Umweltzeichen weltweit, das Rechenzentren auszeichnet. „Das oberste Ziel des Blauen Engel für Rechenzentren ist es, die Effizienz im Bestand zu erhöhen. Es geht in erster Linie nicht darum, die Technik auszutauschen (Stichwort Ressourcenverschwendung), sondern die Rechen- und Speicherkapazität besser zu nutzen", erklärt Marina Köhn, die beim Umweltbundesamt (UBA) für das Thema Green IT sowie für die Kriterienerarbeitung für Rechenzentren beim Blauen Engel hauptverantwortlich zuständig ist.

In Rechenzentren bestehen erhebliche Energieeinsparpotenziale, die durch ein professionelles Management der Rechenzentrumskomponenten und der Gebäudetechnik ausgeschöpft werden können. Einrichtungen, die den Blauen Engel erhalten, reduzieren den Energieverbrauch, kommen ohne klimaschädliche Klimatisierung aus und nutzen die eingesetzte Technik effizienter. Der Blaue Engel stellt zudem hohe Ansprüche an Transparenz, die durch das Monitoring der Energiebereitstellung, Klimatisierung und IT-Leistung der Zentrumskomponenten gewährleistet ist.

Neu kalibriertes Umweltzeichen

Die bestehenden Anforderungen werden regelmäßig überprüft und dem Stand der Technik und Betriebsführung angepasst. Sie stellen eine fundamentale Grundlage dafür dar, den hohen Energieverbrauch von Rechenzentren zu reduzieren, die Auslastung der Informations- und Gebäudetechnik zu erhöhen und zur Transparenz beizutragen. In diesem Jahr werden die Vergabekriterien beider Umweltzeichen neu kalibriert und zu einem modularen Umweltzeichen, je nach Zuständigkeitsbereich, zu-

ONLINE-WORKSHOPS

Termine und Anmeldemöglichkeiten unter **www.be-rechenzentren.de**

- **RZ-Management** Energiemonitoring, Kennzahlen und Transparenzmaßnahmen
- **Energieeffiziente Gebäudetechnik** Energieversorgung, Kälteanlagen und Abwärmenutzung
- **Energieeffiziente Informationstechnik** KPIs, Ökodesign-Anforderungen, Inventarlisten, Lastmonitoring

sammengefasst. Das UBA arbeitet dazu im Rahmen eines Forschungsvorhabens mit dem Öko-Institut e.V. und der Data Center Excellence GmbH zusammen. Voraussichtlich Anfang 2023 wird die neue Fassung veröffentlicht.

Um Best-Practice-Beispiele zu berücksichtigen und Anregungen aus der Praxis einzubeziehen, findet die Überarbeitung im engen Austausch mit Betreibern, Planern und Kunden von Rechenzentren statt. Das Umweltzeichen wird zwar überwiegend von den umweltbewussten Unternehmen getragen, die Akzeptanz innerhalb der Branche ist jedoch wichtig, um seine Verbreitung und Wirkung zu erhöhen. Dazu sind mehrere Workshops zu unterschiedlichen Themen geplant, um die Kriterien vorstellen, zu diskutieren und im Detail mit den Teilnehmenden zu verhandeln.

Beratung erforderlich

Weiterhin hat das UBA ein Programm zur kostenlosen Beratung von Rechenzentren zur energetischen Optimierung und Zertifizierung mit dem Umweltzeichen gestartet. Interessierte Betreiber können sich an Berater wenden, um sich über die Zertifizierung mit dem Blauen Engel zu informieren. Die Beratungen können ausschließlich die Berater vornehmen, die bereits als Auditoren und Berater vom UBA geschult und zugelassen sind. Die Liste der zugelassenen Personen ist in der Anlage 3 der Antragsunterlagen der Umweltzeichen DE-UZ 214 und DE-UZ 161 veröffentlicht und stehen in der Box „Weitere Informationen" zum Download zur Verfügung.

Janine Braumann, Marina Köhn

WEITERE INFORMATIONEN:

Kriterien: www.blauer-engel.de/uz161, www.blauer-engel.de/uz214

Workshopreihe und Beratungsprogram: www.be-rechenzentren.de

UBA Green-IT: https://bit.ly/3KVgUuR

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
30. JUNI 2022

DIGITALISIERUNG: Erfolgreiche Geschäftsmodelle
KÜNSTLICHE INTELLIGENZ: Vorurteile vermeiden
DAS SPEZIAL: Banking, Finance & Controlling

DIE AUSGABE 06/2022
VON IT MANAGEMENT
ERSCHEINT AM 31. MAI 2022

INSERENTENVERZEICHNIS

WIR WOLLEN IHR FEEDBACK

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

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Carina Mitzschke, Silvia Parthier (-26)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Janine Braumann, Philipp von der Brüggen, Andreas Knab, Marina Köhn, Sion Lewis, Frank Mihm-Gebauer, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Dr. Klaus von Rottkay, Gregor Stöckler

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.

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 29. Preisliste gültig ab 1. Oktober 2021.

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

Das E-3 Magazin

Information und Bildungsarbeit von und für die SAP-Community

Wir leben alle unter dem gleichen Himmel, aber wir haben nicht alle den gleichen Horizont.

Konrad Adenauer

© Yevhenii_Chulovskyi, Shutterstock.com

e-3.de | e3zine.com



Perfekte Telefonie-Lösungen



Unabhängig von Ihren geschäftlichen Anforderungen und Entwicklungen, Snom bietet Ihnen passgenaue Kommunikationslösungen. Und das seit 25 Jahren.

www.snom.com

25 Jahre snom

snom

itsecurity
MAI 2022

DAS SPEZIAL

CYBERATTACKEN THOUGHT LEADERSHIP

INTELLEKTUELLES KOPF-AN-KOPF-RENNEN
AB **SEITE 8**

DriveLock

RACHE FÜR SANKTIONEN?
AB **SEITE 10**

macmon intelligent einfach

ZERO TRUST

ALLES EINE FRAGE DER IDENTIFIKATION

Jochen Koehler, HYPR

SICHERE WORKSTATIONS

Schwachstellen reduzieren

MUSTER ERKENNBAR

Ransomware unter der Lupe

AD HOC-BERICHTE FÜR COMPLIANCE

Vom Alptraum zur Routine

Foto: HYPR

TÜV SÜD

Datenschutz

ab Seite 12

RISIKO RANSOM-WARE

Schützen Sie Ihre Daten. **Schützen Sie Ihre Backups.**

Verschlüsseln Sie Ihre Daten für mehr Sicherheit bei Datenlecks und in der Cloud.

Boxcryptor schützt Ihre Dokumente mit starker Ende-zu-Ende-Verschlüsselung.

Jetzt informieren und testen:
www.boxcryptor.info/ransomitd

boxcryptor

INHALT

4 COVERSTORY

18

ALLES EINE FRAGE DER IDENTIFIKATION

ZERO TRUST HAT SICH ALS GRUNDLEGENDE STRATEGIE IN UNTERNEHMEN ETABLIERT

Banken, Versicherungen, Automobilhersteller, Pharma-Konzerne und Chemie-Industrie – es gibt kaum eine Branche, die nicht von einer Zero-Trust-Strategie spricht. Für CISOs und CIOs ist das Thema dauerpräsent, obwohl Unternehmen doch eigentlich Trust suchen. Wie gelingt es also, Mitarbeitern und ihren Zugriffen auf die Unternehmens-IT gänzlich vertrauen zu können?

Ob bei der Anmeldung auf dem PC, dem Öffnen von Applikationen oder dem Zugriff auf Social Media – Passwörter bestimmen auch heute noch den Großteil der Authentifizierungsverfahren in unserem digitalen Alltag. Das Problem dabei: Passwörter sind umständlich zu merken und anfällig für Angriffe von Kriminellen. Abhilfe kann die vollständige Eliminierung von passwortbasierten Anmeldungen in Verbindung mit mehreren Faktoren zur Identifikation eines Anwenders verschaffen, meint Jochen Koehler, Leiter der Region Zentraleuropa beim Authentifizierungsspezialist HYPR.

Ulrich Parthier: *Herr Koehler, Zero Trust gewinnt als Sicherheitsmodell immer mehr Popularität. Was macht es so sicher und damit bei CISOs und CIOs gleichermaßen beliebt?*

Jochen Koehler: Zero Trust ist im Gegensatz zu eher kurzlebigen Sicherheitsmodellen im Cybersecurity-Bereich mehr als nur ein Hype, es hat sich regelrecht als eine grundlegende Strategie vieler Unternehmen etabliert. Wie der Name es bereits vermuten lässt, verfolgt Zero Trust einen Ansatz, der nichts und niemandem innerhalb und außerhalb der Unternehmensgrenzen per se vertraut, seien es Mitarbeiter, Kunden oder Anwendungen. Entstanden ist dieses Misstrauen, da aufgrund der sich immer weiter aus dem Perimeter hinausbewegenden Geräte und Anwendungen keine Zugriffssicherheit mehr gegeben ist. Das macht eine eindeutige Identifikation von Gerät und Anwender unmöglich. Das wichtigste Element einer Zero-Trust-Strategie ist deshalb die Identität. Hier spielt die Anwenderauthentifizierung eine entscheidende Rolle, denn sie liefert den Nachweis über die Identität der Person, die auf und über das entsprechende Gerät zugreift. Diese eindeutige Identifizierung des Anwenders steht am Anfang einer jeden Zero-Trust-Architektur. Richtig umgesetzt wird diese letztendlich zu einer Trust-Architektur, denn das eigentliche Ziel der Unternehmen ist ja das Vertrauen, und nicht das Nicht-Vertrauen. Moderne Lösungen müssen also in der Lage sein, nicht nur das Gerät, sondern auch den Anwender zweifelsfrei zu identifizieren. Und spätestens da haben passwortbasierte Authentifizierungsverfahren ihre Grenzen erreicht.

Ulrich Parthier: *Auf Passwörter alleine verlassen sich heute schon die wenigstens Unternehmen. Welche Formen der Multi-Faktor-Authentifizierung (MFA) werden heute eingesetzt und welche Rolle spielt Single Sign-On in diesem Kontext?*

Jochen Koehler: Unternehmen haben längst erkannt, dass der Einsatz von Passwörtern als Authentifizierungsfaktor schlicht nicht mehr sicher ist. Nachweise über Zugangsberechtigungen und Identitäten müssen heute über eine Multi-Faktor-Authentifizierung (MFA) erbracht werden, die zusätzliche Faktoren zur Identifikation erfordert.

In der Praxis kommen MFA-Lösungen jedoch oft erst als Sekundär-Authentifizierung zum Einsatz, also nachdem der Benutzer sich bereits mit einem Passwort, zum Beispiel am PC, anmelden musste. In diesen Fällen kann natürlich weder von Single Sign-On, noch von einer passwortlosen Anmeldung gesprochen werden. Eine sinnvolle Strategie zieht den MFA-Prozess vor, sodass die Identität nicht erst bei dem Zugriff auf eine Anwendung oder ein Single-Sign-On-Portal überprüft wird, sondern bereits, wenn sich die Person an ihrem Gerät anmeldet. Ähnlich wie bei dem Betreten eines gesicherten Gebäudes wird so der Haupteingang zum System abgesichert und die Identität per MFA überprüft.

Entsprechende Technologien gibt es seit wenigen Jahren auf dem Markt, Unternehmen sollten bei der Auswahl aber sehr genau hinschauen. Oftmals ersetzen Touch ID, Hello-Kamera und andere Anmeldemechanismen den Einsatz von Passwörtern gar nicht, sondern verschieben sie lediglich in den Hintergrund. Das eingestellte Passwort ist dabei an den Fingerabdruck oder die biometrischen Gesichtserkennungspunkte gekoppelt. Sobald das System eine Zugangsberechtigung abfragt, kann der Nutzer es automatisch bestätigen. Die Gefahr von passwortbasierten Angriffen bleibt bestehen, während sich Unternehmen in falscher Sicherheit wiegen. Von dem gleichen Problem sind auch Ansätze auf Basis von One-Time-Password-Token (OTP) oder Authenticator-Apps betroffen. Sie funktionieren mit so genannten Shared Secrets, die vergleichbar mit hinterlegten Passwörtern sind, und bleiben so weiterhin vulnerabel. Die grundsätzliche Frage, die sich Unternehmen vor dem Hintergrund der aktuellen Sicherheitslage im digitalen Raum stellen müssen, lautet daher: Verbleibt die IT-Abteilung bei veralteten, passwortbasierten Technologien oder wendet sie sich modernen Alternativen wie den Authentifizierungs-Standards der FIDO (Fast Identity Online)-Allianz oder Public-Key-Kryptografie zu? Mithilfe intelligenter Lösungen sollte das Ziel sein, Zero Trust und eine vollständig passwortlose MFA zu verbinden.

Ulrich Parthier: *Warum ist der angesprochene Passwordless-Ansatz so wichtig?*

Jochen Koehler: Auf der einen Seite haben wir den Sicherheits-Aspekt. Passwörter sind immer wieder Ziel von Attacken und schon seit langem auf Platz eins der Ursachen für erfolgreiche Angriffe gelistet. Zu schwache und oft verwendete Passwörter können leicht erraten oder ausgespäht werden – und sind so für rund 80 Prozent der IT-Sicherheitsvorfälle verantwortlich. Allein mit einem einzigen Data Breach im vergangenen Jahr, bekannt geworden als RockYou2021, wurden annähernd 9 Milliarden Passwörter erbeutet. Gleiches gilt für Multi-Faktor-Authentifikationen, die mit Shared Secrets und Push-Mitteilungen arbeiten. Besonders Phishing-Angriffe sind hier ein Problem und führen mit manipulierten Nachrichten zu kompromittierten Identitäten.

Aktuelle Beispiele wie die Angriffe der Gruppe „Lapsu$" führen uns ganz konkret vor Augen, dass passwortbasierte MFA-Anmeldeprozesse nicht sicher sind. Auf der anderen Seite steht die Benutzerfreundlichkeit. Für die Mehrzahl der Anwender sind Passwörter einfach nur lästig. Permanent immer komplexer werdende Passwörter einzugeben, sich diese zu merken und noch dazu regelmäßig ändern zu müssen, sorgt für Unmut. Besonders ärgerlich wird es bei mehrfacher Falscheingabe für den Helpdesk, der diversen unabhängigen Erhebungen zufolge zwischen 25 und 40 Prozent seiner Support-Arbeiten mit Passwort-Resets verbringt. Passwörter verbrauchen unzählige Ressourcen und verursachen unnötige Kosten. Das verdeutlicht einmal mehr, dass die Umstellung auf passwortlose Authentifikationslösungen nicht nur eine erhöhte Anmelde-Sicherheit, sondern auch einen größeren Anwender-Komfort mit sich bringt – und im besten Fall spart sie sogar Kosten.

MIT DER ELIMINIERUNG VON PASSWÖRTERN KÖNNTEN 80 PROZENT DER CYBERANGRIFFE VERMIEDEN WERDEN.

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

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

CYBERATTACKEN

GLAUBT MAN DEN ZAHLEN, SO STEIGEN DIE CYBERATTACKEN KONTINUIERLICH AN. SIE REICHEN VON DDOS-ATTACKEN, DIE DIE WEBSITE LAHMLEGEN, BIS HIN ZU MITTLERWEILE IMMER RAFFINIERTER WERDENDEN RANSOMWARE-ANGRIFFEN. DIE GUTE NACHRICHT IST, ES GIBT DURCHAUS ABWEHRMECHANISMEN.

Sie reichen von Honeypots über Ransomware-Software, die eine Bereinigungsfunktion enthalten und diese Art von Angriffen blockieren oder den Inhalt von verschlüsselten Dateien automatisch wieder herstellen, ohne das Lösegeld bezahlen zu müssen, bis hin zu physikalischem Backup in Form von Tapes oder Immutable Speicher.

Schlecht ist es nur, wenn sie nicht proaktiv im Securityplan berücksichtigt werden. Denn dann tut es richtig weh und kostet nicht nur Zeit, Geld und Reputation sondern gegebenenfalls auch noch den Job.

INTELLEKTUELLES KOPF-AN-KOPF-RENNEN

DIE ROLLE DES MENSCHEN IN DER IT-SICHERHEIT

Wenn wir den Begriff „Cyberattacke" hören, denken wir an gesichtslose Hacker, die nach vielen trickreichen Angriffswellen in ein System eindringen und dieses kompromittieren. In der Realität stehen hinter diesen Angriffen kriminelle Organisationen, die bewusst eine ganz bestimmte Schwachstelle in der IT-Sicherheitsarchitektur ausnutzen – den Menschen – und der entscheidende Auslöser für den Angriff ist oft nur ein einfacher Klick. Nicht umsonst wird der Faktor Mensch oft als das wichtigste – und zugleich schwächste – Glied eines ganzheitlichen Sicherheitskonzepts bezeichnet.

IT-Netzwerke von Unternehmen und Organisationen sind gegen externe Angriffe oft gut geschützt. In der Regel kommen verschiedene Präventionswerkzeuge und Sicherheitslösungen zum Einsatz. Aus diesem Grund nutzen Cyberkriminelle gezielt Methoden, in deren Mittelpunkt menschliches Verhalten steht. Die Rede ist dann von Social Engineering und dem Ziel, den Zugriff auf Systeme über die Manipulation von Anwendern innerhalb einer Organisation zu erhalten. Phishing- und Smishing-Nachrichten werden an aktuelle Geschehnisse, Krisen, Inhalte aus Fernsehsendungen oder bekannte Personen angepasst, mit dem Ziel, den Menschen zum Öffnen des Anhangs einer E-Mail oder SMS zu verleiten.

DIE BESTEN IT-SICHERHEITSMODELLE NUTZEN DIE FÄHIGKEIT ZU KRITISCHEM DENKEN UND KREATIVITÄT, UNTERSTÜTZT VON MODERNEN CYBERSECURITY-TECHNOLOGIEN.

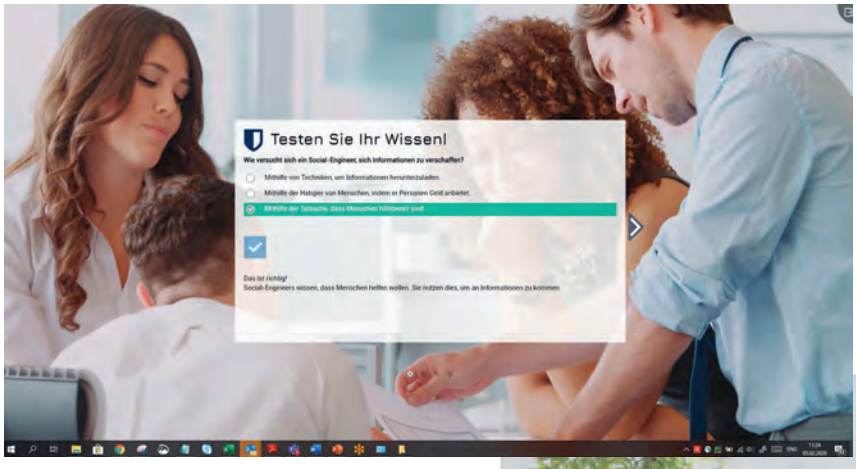
Andreas Fuchs, Head of Strategy & Vision, DriveLock SE, www.drivelock.com

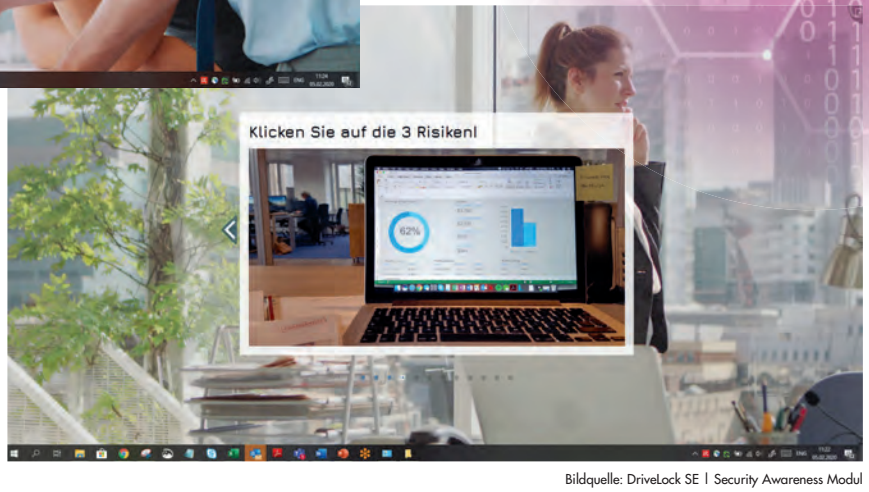
Die unschlagbaren Security-Features

Für Erfolg und Misserfolg von Social Engineering spielen menschliche Fähigkeiten wie Kreativität, ein Verständnis für Sprache und das kritische Denken eine ganz entscheidende Rolle. Sowohl die Angreifenden wie auch die Verteidigenden nutzen diese Fähigkeiten. Beide Seiten nutzen kritisches Denkvermögen für ihre Pläne und Methoden, finden kreative Lösungen für schwierige Probleme und haben die Fähigkeit, Informationen frei zu kommunizieren. Anders gesagt: Cybersecurity ist vor allem auch ein intellektuelles Kopf-an-Kopf Rennen.

Cyberkriminelle bedienen sich beispielsweise brisanter Situationen, wie zuletzt Pandemien oder Kriege, um Menschen genau dort zu treffen, wo sie verwundbar sind: in ihren Emotionen. Aus diesem Grund funktionieren Spear-Phishing oder CEO Fraud (gefälschte Mails, angeblich von der Geschäftsführung) besonders gut, weil sie auf ein Verständnis von (Macht-)Konstellationen und kollegialen Beziehungen innerhalb eines Unternehmens aufbauen und entsprechend gezielt agieren.

Noch wichtiger sind menschliche Fähigkeiten auf Seite der Verteidiger. Versuche, den Menschen in diesem Wettbewerb durch künstliche Intelligenz (KI) zu ersetzen, haben nur begrenzten Erfolg. KI hat festgelegte Limits basierend auf existierender Information – menschliche Kreativität nicht. Wenn Hacker eine neue Angriffsmethode entwickeln, wird eine datenbasierte Lösung möglicherweise keinen Angriff erkennen. Menschen aber haben ein feines Gespür für Nuancen, wie ungewöhnliche Betreffzeilen und Absender im Falle von Phishing-Mails oder Veränderungen im Sprachgebrauch im Kontext von CEO-Fraud. Zudem sind Menschen in der Lage, die Zeichen der Zeit zu lesen und so zum Beispiel Phishing-Trends zu antizipieren. Regelmäßige Warnungen des BSI über bestimmte Betrugsmaschen sind ein gutes Beispiel dafür, wie Menschen eine neue Bedrohung identifizieren und kommunizieren.





Bildquelle: DriveLock SE I Security Awareness Modul

Unsere einzigartigen Fähigkeiten machen die Rolle des Menschen in der Verteidigung so wichtig. Die besten IT-Sicherheitsmodelle nutzen die Fähigkeit zu kritischem Denken und Kreativität, unterstützt von modernen Cybersecurity-Technologien.

Für Sicherheitsrisiken sensibilisieren

In der Theorie sollte die Mehrzahl der digital arbeitenden Menschen wissen, wie sicheres Verhalten im Netz aussieht. Dennoch notieren sich User weiterhin Passwörter oder speichern diese ungeschützt elektronisch ab, umgehen Sicherheitsmaßnahmen, wenn diese ihnen im Weg stehen, oder zeigen unsichere Verhaltensweisen im Netz. Daher muss das Ziel einer guten Unternehmensstrategie nicht nur sein, ein Bewusstsein für die Gefahren im Netz zu schaffen, sondern eine nachhaltige Verhaltensänderung und somit eine Kultur der Cybersicherheit herbeizuführen.

Gelingen kann dies mit kontinuierlichen Sensibilisierungsmaßnahmen wie Security Awareness Kampagnen mit situationsbedingten Sicherheitsschulungen. Wichtig für den Erfolg dieser Sicherheitsschulungen ist es, dass die Security Awareness Trainings nicht zu trocken erscheinen. Erfolgreiche Initiativen sprechen sowohl emotional als auch intellektuell an, nutzen moderne Lernmethoden, wie Gamification (etwa ein Quiz) oder Videos, und halten die User bei Laune mit kurzen, knackigen Inhalten. Wenn diese Inhalte zum passenden Zeitpunkt ausgespielt werden, sind sie deutlich effektiver als ein zweistündiger Vortrag über Hacker und Schadsoftware. Zum Beispiel erscheint ein 30-sekündiges Pop-up Video über Bad USB, wenn User einen privaten USB-Stick an den Unternehmensrechner anschließen. Mit diesem Video werden sie vor möglichen Risiken gewarnt und können so nochmal entscheiden, ob sie die auf dem Stick enthaltenen Dateien wirklich im Unternehmensnetzwerk öffnen möchten. So lässt sich mit einfachen Mitteln eine nachhaltige Kultur für Cybersicherheit etablieren.

Auf der Ebene der technischen Maßnahmen werden Sicherheitslösungen mit Fokus auf User-Centric Behaviour populärer. Diese analysieren das Anwenderverhalten und prüfen es auf Unregelmäßigkeiten.

Lösungen wie die Threat Detection and Response von DriveLock leiten direkt Gegenmaßnahmen ein, falls Abweichungen erkannt werden. Solche Lösungen lassen sich sehr gut mit einer Security Awareness Kampagne kombinieren.

Diese Maßnahmen sind auch wesentliche Bestandteile des Zero Trust Security Modells bei DriveLock. Zero Trust behandelt Benutzer und Geräte so, dass ihnen zunächst misstraut wird. Unbekannte und somit unerwünschte Aktionen werden somit unterbunden und potenziell gefährliche Aktivitäten werden frühzeitig erkannt und entsprechend blockiert. Das betrifft nicht nur die technologischen Aspekte. DriveLock möchte die menschlichen Fähigkeiten zur Verteidigung stärken, Menschen und Organisationen unterstützen und so auch zur Bildung einer verantwortungsbewussten, sicheren Unternehmenskultur beitragen. Letztlich geht es darum, User und Systeme mit dem richtigen Zusammenspiel von modernen Technologien und menschlichen Fähigkeiten vor andauernden Cyberbedrohungen zu schützen.

Andreas Fuchs

RUSSISCHE CYBER-ATTACKEN ALS RACHE FÜR SANKTIONEN?

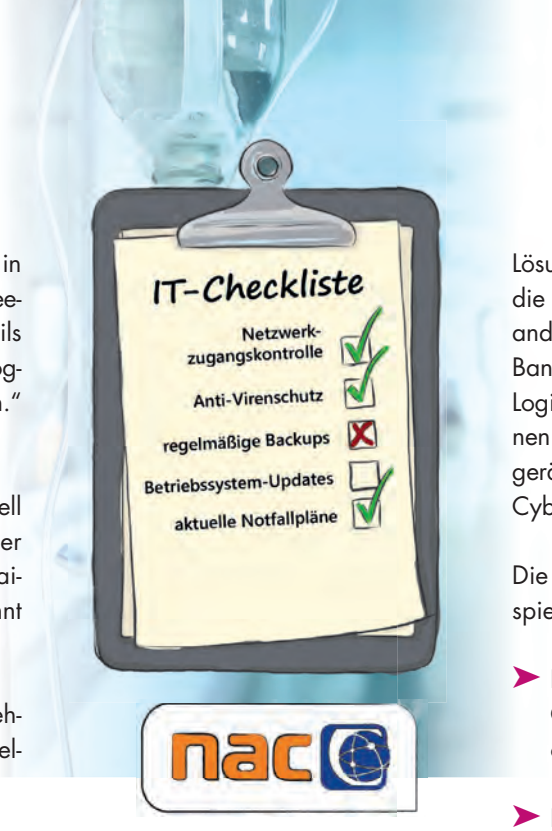
NACH SANKTIONIERUNGEN WESTLICHER STAATEN GEGEN RUSSLAND WARNEN IT-SICHERHEITSEXPERTEN VOR RACHEAKTIONEN DURCH HACKERANGRIFFE

Die Tagesschau berichtete am 3. März 2022: Bundesinnenministerin Nancy Faeser appellierte, die Bedrohung durch Cyberangriffe ernst zu nehmen: „Wir gehen von einer erhöhten Gefährdung dieser Tage aus, weil im Kriegsgeschehen Cyber-Attacken auch eine Form der Kriegsführung sind." Die Ministerin kündigte an, den Bereich der IT-Sicherheit weiter zu stärken, um frühzeitig mögliche Angriffe auf die sogenannten Kritische Infrastruktur (KRITIS) erkennen zu können. Als Kritische Infrastrukturen (KRITIS) bezeichnet das Bundesamt für Sicherheit in der Informationstechnik (BSI) jene Organisationen und Einrichtungen, deren ernsthafte Beeinträchtigung oder Ausfall dramatische Folgen für das staatliche Gemeinwohl hätte (Versorgungsengpässe und Störungen der öffentlichen Sicherheit).

Zu den Kritischen Einrichtungen zählen öffentliche und privatwirtschaftliche Institutionen:

- Ernährung (Ernährungswirtschaft, Lebensmittelhandel)
- Gesundheit (medizinische Versorgung, Arzneimittel, Impfstoffe, Labore)
- Finanz- und Versicherungswesen (Banken, Versicherungen, Finanzdienstleister)
- Wasser (öffentliche Wasserversorgung)
- Energie (Elektrizität, Gas, Mineralöl, Fernwärme)
- Transport und Verkehr (Luftfahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr)
- Informationstechnik und Telekommunikation
- NEU: Kommunale Abfallentsorgung

Mittlerweile verschickt das BSI an Unternehmen täglich nicht-öffentliche Einschätzungen über die Lage in der Ukraine, mit besonderem Fokus auf den „Cyber-Raum". Die Bedrohungslage ist derzeit auf „Orange", also nach Definition des BSI „geschäftskritisch". Eine „massive Beeinträchtigung des Regelbetriebs" sei denkbar. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt zudem nach §7 BSI-Gesetz seit dem 15. März vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky. Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen. Kurz vor und während dem Einmarsch der russischen Truppen in die Ukraine gab es zahlreiche digitale Angriffe auf ukrainische Infrastrukturen und auf regierungsnahe Unternehmen. Nachrichten über Cyber-Angriffe und einen „Krieg im Netz" schüren auch in Deutschland Unsicherheit und Sorge. Das BSI ruft deutsche Unternehmen auf: „Bleiben Sie wachsam und machen Sie Ihre „digitalen Hausaufgaben". Aktualisieren Sie Ihre Notfallpläne, machen Sie regelmäßig Back-Ups, halten Sie Ihre Systeme aktuell und holen sich, da wo Ressourcen und Kompetenzen fehlen, die entsprechende Unterstützung durch Dienstleister hinzu. Zudem sollten Ihre Mitarbeitenden



in der aktuellen Situation sensibilisiert in Bezug auf Phishing-Mails, Social Engineering und Fake News werden. Denn Mails mit Ukraine-Bezug könnten jetzt ein mögliches Einfallstor für Kriminelle werden." Denn:

- Cyberkriminelle passen sich schnell gesellschaftlichen Notlagen wie der Corona-Pandemie oder dem Ukraine-Krieg an und nutzen diese gekonnt für ihre Zwecke aus.
- Sie greifen Institutionen und Unternehmen mit gesellschaftlich hohem Stellenwert an.
- Eine erhöhte Cyber-Security-Awareness ist beim Schutz von IT-Infrastrukturen und Unternehmensnetzwerken essenziell. Sie sollte daher in jedem Unternehmen gefördert werden.
- Das Gefährdungspotenzial, welches von Cyberangriffen ausgeht, ist auf einem hohen Niveau. Angriffe auf Akteure, die für die Krisenbewältigung relevant sind, finden infolge ihrer Bedeutung für Politik, Gesellschaft und Wirtschaft vermehrt statt.

Großer Handlungsbedarf im Gesundheitssektor

Die wachsende Bedrohung für Krankenhäuser als tragende Säulen der kritischen Infrastrukturen wurde vom Bund bereits 2019 erkannt und als neuen Fördertatbestand in den Krankenhausstrukturfonds aufgenommen. Für die aktuelle Förderperiode 2019-2024 stehen beim Amt für Soziale Sicherung rund vier Milliarden Euro zur Verfügung. Für Krankenhäuser bedeutet dies, dass insofern sie den Förderrichtlinien entsprechen, auch Anschaffungen im Bereich der IT-Sicherheit förderbar sind. Klassische IT-Netzwerke, die Endgeräte wie beispielsweise MRT-Systeme integrieren, werden zu medizinischen Netzwerken. Die Kontrolle und Sicherheit in diesen gemischten Netzwerken sind essenziell, eine Störung kann für Patienten lebensbedrohliche Folgen haben, für die Klinik ein erheblicher finanzieller Schaden entstehen. Auch ein Imageschaden ist bei dem Bekanntwerden von Vorfällen ein großes Problem.

Netzwerkzugangskontrolle – zentrale Säule der IT-Sicherheit

Bei einem umfassenden IT-Sicherheitskonzept im Gesundheitswesen muss das Thema Netzwerkzugangskontrolle (NAC) integriert werden: Das unbekannte Gerät eines Angreifers erhält im Krankenhaus – bei entsprechendem Schutz – keinen Zugriff auf das Krankenhausnetzwerk und kann somit keinen Schaden anrichten. In Zusammenarbeit mit anderen IT-Security-Lösungen kann die technologisch führende Lösung macmon NAC ein non-konformes, nicht den definierten Sicherheitsregeln entsprechendes Gerät automatisch in Quarantäne stellen, und den Netzwerk-Administrator über eine Attacke informieren noch bevor eine Ausbreitung stattfindet.

Die Corona-Pandemie hat gezeigt, welchen zentralen Stellenwert eine reibungslos funktionierende Gesundheits-Infrastruktur für die medizinische Versorgung unserer Gesellschaft hat. Neben vielen weiteren Herausforderungen sollten sich Krankenhäuser jetzt für die staatliche Förderung, von über 500 Millionen Euro pro Jahr, bewerben. Mit der erprobten NAC-Lösung der Berliner Sicherheitsexperten, die bereits in vielen Krankenhäusern und anderen kritischen Infrastrukturen wie Banken, der Energieversorgung oder der Logistik erfolgreich eingesetzt wird, können Netzwerke mit ihren vielfältigen Endgeräten vor ungewolltem Zugriff durch Cyber-Kriminelle sicher geschützt werden.

Die Vorteile von macmon NAC am Beispiel Krankenhaus:

- Einbinden aller Medizintechnik ohne Gefahr für das bestehende Netzwerk oder die medizinischen Geräte
- Ermöglichung des zeitlich und räumlich flexiblen Zugriffs auf Patientendaten für Ärzte bei gleichzeitigem Schutz vor unbefugtem Zugriff
- Bereitstellen von dedizierten und zeitlich befristeten Internetzugängen für Gäste und Patienten, ohne für Ärzte und Patienten getrennte WLAN-Infrastrukturen aufbauen zu müssen
- Sicherstellung der Integrität des Netzwerkes durch ausschließliches Gewähren des Netzwerkzugangs für die definierten (eigenen und zugelassenen) Geräte
- Überwachung und Kontrolle aller im Netzwerk befindlichen Geräte (Live-Bestandsmanagement) und Dokumentation aller Zugriffe auf das Krankenhausnetzwerk
- Unterstützung bei Zertifizierung nach ISO 27001, der Umsetzung der BSI-Standards zum Informationssicherheitsmanagement, der IT-Grundschutz-Kataloge und von Krankenhaus-Zertifizierungsverfahren (KTQ-Zertifizierung oder DIN EN 80001)

Sabine Kuch

Weitere Informationen:
www.macmon.eu

DATENSCHUTZ

MUT ZUR LÜCKE MACHT SICH HIER NICHT BEZAHLT

Bislang scheinen viele kleine und mittlere Unternehmen unter dem Radar geflogen zu sein, wenn es um Bußgelder für Verstöße gegen die DSGVO ging. Obwohl die Übergangsfrist für die EU-weit gültige Verordnung im Mai 2018 endete, gibt es weiterhin viel Nachholbedarf bei ihrer Umsetzung – vor allem in kleineren Betrieben. Die Aufsichtsbehörden könnten hier aber bald wesentlich genauer hinschauen, davon ist Steffen Reimann, Produkt- und Partnermanager bei TÜV SÜD überzeugt. Umso wichtiger ist es, dass die Verantwortlichen in den Unternehmen jetzt die Weichen für datenschutzkonforme Geschäftsprozesse stellen.

? it security: *Seit 2016 ist die EU-DSGVO in Kraft, die Übergangsfrist lief im Mai 2018 aus. Worauf sollten sich Unternehmen einstellen, die immer noch große Lücken bei der Umsetzung der Verordnung haben?*

Steffen Reimann: Die Aufsichtsbehörden werden genauer hinschauen und auch höhere Geldstrafen verhängen, hier gab es bereits eine Trendwende. Was Bußgelder betrifft war 2021 ein Rekordjahr, erstmals wurde die Milliardengrenze überschritten. Rund 1,2 Milliarden Euro mussten Unternehmen aufgrund ihrer Verstöße gegen die DSGVO zahlen, im Vergleich zum Vorjahr mit knapp 170 Millionen also eine enorme Steigerung. Das zeigt, dass Europäische Behörden mittlerweile bereit sind, hart durchzugreifen. Dieser Trend wird sich mutmaßlich auch im Jahr 2022 weiter fortsetzen.

? it security: *Gibt es noch weitere Entwicklungen und Trends, die man beim Thema Datenschutz im Blick haben sollte?*

Steffen Reimann: Die Anzahl der privat geführten datenschutzrechtlichen Verfahren, die mit Verstößen gegen die DSGVO in Zusammenhang stehen, hat im vergangenen Jahr merklich zugenommen. Immer mehr Betroffene klagen auf Schadensersatz. Die Medienberichterstattung der vergangenen Jahre hat das Bewusstsein der breiten europäischen Öffentlichkeit für ihre Rechte und für mögliche Rechtsmittel im Fall eines DSGVO-Verstoßes bedeutend geschärft. Die derzeitige Entwicklung lässt deshalb erwarten, dass sich Unternehmen in Zukunft immer häufiger neben Strafzahlungen auch mit Schadensersatzforderungen Betroffener konfrontiert sehen werden. Es ist mit Sammelklagen in enormer Höhe zu rechnen. Erste Anwaltskanzleien haben sich bereits in Stellung gebracht, um hier proaktiv vorzugehen. Denkt man dann einmal Bußgelder und Schadensersatzansprüche zusammen, dürften bereits 2022 noch einmal ganz andere Summen auf Unternehmen zukommen.

? it security: *Was sind die Hintergründe für diese Entwicklung?*

Steffen Reimann: Bezüglich der Bußgelder ist sicherlich die „Schonfrist" vorbei – fast vier Jahre nach In-Kraft-Treten der DSGVO erwarten Behörden ein adäquates Datenschutzniveau – dies gilt auch für kleinere und mittelgroße Unternehmen (KMU). Sie werden gleichermaßen auch selbst bei der Prüfung von Unternehmen proaktiv tätig.

Hinsichtlich des Schadenersatzes ist sicherlich ein wesentlicher Aspekt, dass die DSGVO für einen Schadensersatzanspruch zumindest keine explizite Erheblichkeitsschwelle benennt. Dies bedeutet, dass selbst kleinere datenschutzrechtliche Verstöße (etwa der einmalige Versand einer unzulässigen Werbe-E-Mail) einen Schadensersatzanspruch begründen können. Dies wird noch dadurch verschärft, dass ein Schadensersatzanspruch nach DSGVO auch für immaterielle Schäden – wie etwa den Verlust der Kontrolle über die eigenen Daten – besteht.

Waren die deutschen Gerichte in der Vergangenheit eher restriktiv bei der Bejahung eines immateriellen Schadens, so zeigt sich mittlerweile eine deutlich höhere Tendenz einen solchen anzunehmen – ebenso wie die Tendenz, höhere Schadensersatzansprüche zuzusprechen. Unternehmen sollten sich deshalb darauf einstellen, dass Gerichte künftig stärker im Sinne der Betroffenen entscheiden.

> DIE ANZAHL DER PRIVAT GEFÜHRTEN DATENSCHUTZRECHTLICHEN VERFAHREN, DIE MIT VERSTÖSSEN GEGEN DIE DSGVO IN ZUSAMMENHANG STEHEN, HAT IM VERGANGENEN JAHR MERKLICH ZUGENOMMEN.
>
> Steffen Reimann, Produkt- und Partnermanager, TÜV SÜD, www.tuvsud.com

it security: *Sind die Verantwortlichen in den Unternehmen also auf der sicheren Seite, wenn die DSGVO dort bereits umgesetzt wird?*

Steffen Reimann: Zur Einhaltung der DSGVO bedarf es kontinuierlicher Anstrengungen. Jedes Mal, wenn ein neues Verfahren, in welchem personenbezogene Daten verarbeitet werden, im Unternehmen implementiert wird, muss dieses zuvor auf seine Kompatibilität hinsichtlich der DSGVO und der damit in Zusammenhang stehenden Urteile abgeklopft werden. Viele fühlen sich da überfordert. Vor allem bei kleinen und mittleren Unternehmen, herrscht nach wie vor große Unsicherheit. Ihnen mangelt es oft an den erforderlichen Ressourcen, um eigene Experten für Datenschutz und Informationssicherheit zu beschäftigen. Hier können externe Experten unterstützen. Denn für Prozesse, in denen personenbezogene Daten zum Einsatz kommen, müssen regelmäßig die in der DSGVO normierten Anforderungen erfüllt werden. Wenn hierzu nicht ausreichend eigene Ressourcen zur Verfügung stehen, sollte auf Unterstützung von außen zurückgegriffen werden. So kann auch gleich eine externe, neutrale Beurteilung der eigenen Datenschutzlage vorgenommen werden. TÜV SÜD unterstützt KMU beispielsweise mit Datenschutzberatung und -Audits, Stellung des (auch für viele KMU verpflichtende) externen Datenschutzbeauftragten, datenschutzrechtliche Weiterbildungen, GAP-Analysen oder Zertifizierung des Informationssicherheitsmanagements (ISMS) nach ISO 27001. Damit decken wir das gesamte Spektrum ab. Und mit einer solchen externen Unterstützung können dann auch kleiner Unternehmen mit geringen Ressourcen ihre Datenverarbeitungsprozesse DSGVO-konform gestalten.

it security: *Herr Reimann, wir danken für dieses Gespräch.*

VOM ALPTRAUM ZUR ROUTINEAUFGABE

AD HOC-MANAGEMENTBERICHTE FÜR COMPLIANCE UND INFORMATIONSSICHERHEIT

Der Bedarf an einer aktuellen Berichterstattung zum Status Quo der Managementsysteme kommt oft aus heiterem Himmel – zum Beispiel auf Anfrage der Aufsichtsbehörden oder oberer Managementebenen. Verantwortliche für Compliance und Informationssicherheit sollen nun kurzfristig aussagekräftige Kennzahlen und professionell aufbereitete Dokumente liefern, mit denen die komplexen Zusammenhänge auf einen Blick erfasst werden können.

Wie gut sind Sie auf diese Situation vorbereitet?

Variante 1: Sie müssen alles stehen und liegen lassen und die notwendigen Informationen manuell zusammenstellen. Das Ergebnis stellt Ihre Arbeit nicht vollständig und nicht professionell genug dar. Das Management gerät unter Druck und gibt diesen Druck an Sie weiter.

Variante 2: Ihre GRC-Software bietet Ihnen die Möglichkeit, vorkonfigurierte Key Performance Indicators (KPIs) tagesaktuell abzurufen und in Managementberichten mit übersichtlichen Diagrammen aufzubereiten. Ihre Präsentation trägt zur Aufwertung Ihrer Position bei.

Leider ist es mit der Beschaffung eines leistungsfähigen Softwaretools nicht getan. Die meisten Organisationen erkennen das Bedürfnis für einen KPI erst in dem Moment, in dem er benötigt wird. Handeln Sie also vorausschauend und stellen Sie sich im ersten Schritt die Frage, welche Trends und Fakten Sie über Ihr Compliance- oder IT-Security-Rahmenwerk kennen möchten und worüber diese Ihnen in Ihrer Organisation Auskunft geben sollen. Im Datenschutz könnten es zum Beispiel folgende Punkte sein:

Informationen zum Reifegrad des Datenschutzmanagementsystems

- Wie viele Verarbeitungstätigkeiten umfasst das Verzeichnis der Verarbeitungstätigkeiten (VVT) meiner Organisation und für wie viele davon ist der Eintrag im Verzeichnis komplett angelegt und prüffähig?
- Wie viele Verarbeitungstätigkeiten benötigen eine Datenschutzfolgenabschätzung (DSFA) und wie viele davon sind bereits abgeschlossen?
- Für wie viele meiner Datenarten besitze ich ein tragfähiges Löschkonzept?

Informationen zum täglichen Betrieb

- Wie viele Anfragen zu Betroffenenrechten wurden in einem definierten Zeitraum gestellt?
- Wie viele davon sind aktuell in meiner Organisation in aktiver Bearbeitung und wie viele sind abgeschlossen?
- Wie viele Datenschutzvorfälle mit welcher Schwere kamen in einem definierten Zeitraum vor?

Im zweiten Schritt müssen Sie dafür sorgen, dass die Key Performance Indicators zur Beantwortung dieser Fragen hinreichend effektiv ermittelt werden können. Selbst wenn eine Organisation die entsprechenden Kennzahlen definiert hat und die notwendigen Basisdaten abrufbar bereitstehen, kann es einen erheblichen Aufwand verursachen, die für die aktuelle Situation relevanten Rohdaten aus dem vorgehaltenen Datenpool zu extrahieren und die benötigten KPIs akkurat zu berechnen.

Im besten Fall bietet Ihre GRC-Software hierfür komfortable Funktionen an, wie zum Beispiel das „KPI Management Summary Dashboard" von HiScout. Es ermöglicht dem Nutzer, vorkonfigurierte Kennzahlen in einer Übersicht zusammenzustellen und bei Bedarf tagesaktuell automatisch berechnen zu lassen. Wenn Ihnen dieser Komfort nicht zur Verfügung steht, müssen Sie selbst ein Verfahren für den Datenexport und die Berechnungsmethoden entwickeln.

Fazit: Die Anforderung, kurzfristig belastbare Informationen über den Status Quo von Managementsystemen ausgeben zu können, wird häufig erst im Ernstfall erkannt. Eine GRC-Software kann Sie dabei mit vorkonfigurierten Kennzahlen, Diagrammen und Managementberichten unterstützen.

Daniel Linder | www.hiscout.com

KEINE BLINDEN FLECKEN

EXTENDED DETECTION AND RESPONSE

In dem Maße, in dem Unternehmen wachsen, die Zahl ihrer Mitarbeiter zunimmt und auch immer mehr Mitarbeiter von zuhause oder verschiedenen Standorten aus agieren, investieren sie auch immer mehr in Lösungen verschiedener Anbieter. Dies führt zu wachsender Komplexität und erfordert den Einsatz neuer Sicherheitstechnologien, mit denen sie diese neuen Bereiche absichern können. Regelmäßige Neuinvestitionen unterstützen die Betroffenen dabei, sich proaktiv gegen ständig zunehmende Angriffe und immer ausgefeiltere Bedrohungen zu wehren.

Immer häufiger sind dabei sogenannte Endpoint-Detection-and-Response-Lösungen anzutreffen, mit denen sich Funktionen zur Erkennung und Reaktion effizient verwalten lassen. Neben EDR haben sich MDR-Dienste (Managed Detection and Response) als hervorragende Option für Unternehmen erwiesen, die gemeinsam mit einem IT-Sicherheitsanbieter ihre Security trotz begrenzter Personalressourcen im Griff behalten möchten.

Der nächste Schritt in der technologischen Entwicklung heißt XDR (Extended Detection and Response). Dabei werden die bekannten Funktionen einer EDR-Lösung zum Beobachten, Erkennen und Reagieren auf Bedrohungen noch weiter ausgebaut, um der sich ständig verändernden Bedrohungslandschaft einen Schritt voraus zu sein. Die zusätzliche Integration Nicht-Endpunkt-bezogener Telemetriedaten bei der Analyse steht hier im Fokus.

Warum XDR?

XDR ermöglicht es Organisationen, innerhalb der gesamten Infrastruktur über sämtliche Anwendungen und Workloads hinweg das Geschehen präzise zu analysieren, Bedrohungen zu erkennen und schnell darauf zu reagieren. Dabei werden neben Informationen an den Endpoints auch die Telemetrie-Daten von Cloud-, Identitäts-, Netzwerk- und produktiven Applikationsdaten ausgewertet. Durch die Korrelation der Daten unterschiedlichster Sensoren lassen sich so schnell detailliert Zusammenhänge erkennen, was zu einer schnellen Beurteilung von Incidents und letztlich einer Eindämmung von Angriffsversuchen durch automatisierte und gesteuerte Reaktionen führen kann.

Unternehmen profitieren von vielen Vorteilen:

Schnelle Response: Verkürzte Reaktionszeiten führen dazu, dass Angreifer schnell aufgespürt und Bedrohungen eingedämmt werden können, noch bevor größere Schäden entstehen.

Reduzierte Betriebskosten: Das Zusammenfassen der gesamten Analytik an einem zentralen Punkt bedeutet eine Kostenoptimierung sowie eine geringere Belastung des Security-Teams.

Verbesserter Kontext für Entscheidungen: Automatisierte und KI-gestützte Funktionen erlauben bessere Ursachenanalysen, Reaktionsempfehlungen und automatisiertes Handeln.

> XDR ERMÖGLICHT ES ORGANISATIONEN, INNERHALB DER GESAMTEN INFRASTRUKTUR ÜBER SÄMTLICHE ANWENDUNGEN UND WORKLOADS HINWEG DAS GESCHEHEN PRÄZISE ZU ANALYSIEREN, BEDROHUNGEN ZU ERKENNEN UND SCHNELL DARAUF ZU REAGIEREN.
>
> Jörg von der Heydt, Regional Director DACH, Bitdefender, www.bitdefender.de

Offenes XDR vs. Natives XDR

Sogenannte offene oder hybride XDR-Ansätze erfordern die Integration mit Lösungen von Drittanbietern, um deren nicht-Endpoint-bezogene Telemetriedaten zu erfassen und, darauf aufbauend, die richtigen Response-Optionen bereitzustellen. Bitdefender hingegen setzt auf ein natives XDR. Bei diesem Single-Vendor-Konzept profitieren Organisationen von den Vorteilen einer offenen beziehungsweise hybriden Lösung, können dies aber mit einem wesentlich geringeren Bereitstellungsaufwand verbinden. Denn sämtliche Quellen für die Analyse der Telemetriedaten sind bereits Teil der Lösung und lassen sich nach deren Einrichtung sofort nutzen. Eine native XDR-Lösung eignet sich somit besonders für Organisationen mit kleinen Security-Teams, die von den zusätzlichen Threat-Intelligence-Quellen und der schnellen Bereitstellung und Integration der Lösung profitieren möchten.

Jörg von der Heydt

Bitdefender

MUSTER ERKENNBAR

RANSOMWARE UNTER DER LUPE

In den letzten zwei Jahren haben sowohl die Häufigkeit als auch die Raffinesse von Ransomware-Angriffen deutlich zugenommen. Zu diesem Schluss gelangt eine Studie von Ivanti, Cyber Security Works und Cyware. Ein Blick auf die Statistik verdeutlicht die Gefahrenlage: Gegenüber dem Vorjahr konnten Ende 2021 29 Prozent mehr CVEs gezählt werden, die per Ransomware ausgenutzt wurden. Parallel stieg die Anzahl der Ransomware-Familien um 26 Prozent. Doch die Gefahr lauert nicht in der schieren Quantität der Angriffsmöglichkeiten. Es geht primär darum, wie Kriminelle Schwachstellen nutzen und wer am stärksten gefährdet ist. Aus den Studienergebnissen lassen sich einige Muster ablesen.

Muster 1: Ungepatchte Sicherheitslücken

Ungepatchte Sicherheitslücken sind die häufigsten Angriffsvektoren für Ransomware-Gruppen. Von den Schwachstellen, die der Bericht für 2021 identifiziert hat, waren mehr als ein Drittel auch Trendthemen im Dark Web und wurden wiederholt ausgenutzt. Und mehr als die Hälfte der Schwachstellen vor 2021 werden heute noch für Angriffe genutzt. Das verdeutlicht, dass Unternehmen bereitstehende Patches einspielen müssen, egal wie alt sie sind. Doch bleiben wir realistisch: Kein Sicherheitsteam ist mehr in der Lage, jede Sicherheitslücke manuell zu patchen. Umso wichtiger ist es, das Patchmanagement zu automatisieren. Eine Lösung muss allerdings mit risikobasierten Patch-Informationen arbeiten, um den gefährlichsten CVEs die nötige Aufmerksamkeit zu schenken.

Muster 2: Ausnutzung von Zero-Day-Schwachstellen

Cyberkriminelle handeln schnell. Sie sind in der Lage Zero-Day-Schwachstellen auszunutzen, bevor sie in die National Vulnerability Database (NVD) aufgenommen werden. Dieser Trend unterstreicht den Bedarf an Lösungen, die von sich aus Zero-Day-Schwachstellen erkennen und beheben können. Er zeigt auch, dass sich Unternehmen nicht allein auf die NVD verlassen können. Bei der Priorisierung zu patchender CVEs müssen sie daher auch ein Auge auf Schwachstellentrends, Beispiele für ausgenutzte Schwachstellen oder Warnungen von Sicherheitsbehörden werfen.

Muster 3: Angriffe auf die Lieferkette

Ransomware-Gruppen nehmen zunehmend die Lieferketten ins Visier. Schon eine einzige Kompromittierung in der Lieferkette kann dazu führen, dass die komplette System-Distribution in Hunderten von Opfernetzwerken gekapert wird. Unternehmen, die in Supply Chains eingebunden sind, müssen besonders wachsam sein. Denn ein einzelner erfolgreicher Angriff hat nicht nur Auswirkungen auf die eigenen Geschäftswerte, sondern auch auf die Zusammenarbeit mit den Partnern innerhalb der Lieferkette – Imageschaden miteingeschlossen.

Muster 4: Ransomware-as-a-Service

Bei Ransomware-as-a-Service bieten Ransomware-Entwickler ihre Dienste, Varianten, Kits oder ihren Code anderen bösartigen Akteuren gegen Bezahlung an. Das beschleunigt zum einen die Ausbreitung von Bedrohungen – und erschwert es zum anderen, den Ursprung der Bedrohung auszumachen.

HEUTZUTAGE STEHEN DER INTENSITÄT VON ANGRIFFEN IMMER AUSGEFEILTERE SICHERHEITSKONZEPTE GEGENÜBER.

Johannes Carl, Expert Manager PreSales – UEM, Ivanti, www.ivanti.de

Heutzutage stehen der Intensität von Angriffen immer ausgefeiltere Sicherheitskonzepte gegenüber. Eine proaktive, risikobasierte Security-Strategie ist dabei unverzichtbar. Gleiches gilt für automatisierte Patch-Intelligenz: Hiermit können Unternehmen ihr Patchmanagement risikobasiert steuern und sich auf die CVEs konzentrieren, von denen die größte Gefahr ausgeht – auch wenn die IT-Abteilung mit Personalmangel zu kämpfen hat.

Johannes Carl

Der Ransomware Spotlight Report steht kostenfrei auf ***www.ivanti.de*** zum Download bereit.

ZERO TRUST

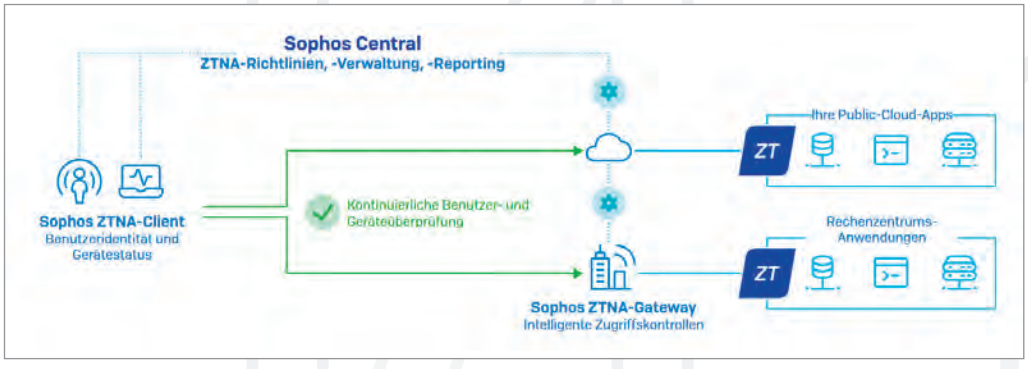
WARUM ES INSBESONDERE JETZT WICHTIG IST

Zero Trust ist ein Prinzip, das eine wesentlich höhere Sicherheit vor Cyberattacken verspricht. Und es existieren valide Gründe, weshalb sich viele Firmen über den Paradigmenwechsel jetzt Gedanken machen sollten. Hauptgrund dafür ist nicht die ständig wachsende Gefahrenlage durch Cyberkriminelle, die raffiniert jedes Unternehmen aufs Korn nehmen. Es ist vielmehr die neue Realität der Arbeitsweise, die Unternehmen zum Nachdenken anregen sollte. Denn die meisten Unternehmen haben während der letzten Jahre notgedrungen und schnell auf eine Technologie gesetzt, die sich in Punkto Cybersecurity drastisch auswirkt. Die Rede ist vom Homeoffice mit Zugriff auf Unternehmensressourcen via Remote Access (RAS) VPN (Virtual Private Networking).

Das RAS VPN ist augenscheinlich eine tolle Sache. Es hat beispielsweise viele Unternehmen während der letzten beiden Jahre maßgeblich dabei unterstützt, einsatzfähig zu bleiben, indem die Mitarbeiter im Homeoffice arbeiten konnten. Für viele ist das heute eine große und unverzichtbare Errungenschaft. Für Security-Experten aber, ist das VPN eine höchst kritische Technologie. Denn die VPN-Remote-Verbindung für zuhause simuliert nichts anderes als ein langes Netzwerkkabel vom Homeoffice direkt in das Unternehmen – und zwar ohne die entsprechenden Schutzmaßnahmen, die man üblicherweise gegenüber Externem walten lassen würde.

Große Chancen für Cyberkriminelle

Das Problem besteht darin, dass klassische Security-Konzepte alles nach außen abschirmen, prüfen und sichern, während sie alles, was sich innerhalb der Sicherheitsperimeter befindet, grundsätzlich als vertrauenswürdig betrachten. Die VPN-Verbindung führt dieses Prinzip ad absurdum, indem es das externe und aus Sicht der Security weitgehend unkontrollierte Homeoffice, als vertrauenswürdig innerhalb der Sicherheitsperimeters ansieht. Das bietet Cyberkriminellen große Chancen, sich über Homeoffice-Rechner direkt in den Kern des Unternehmens und ohne größere Hürden einzuschleusen.



Mehr Sicherheit mit Zero Trust

Das Zero-Trust-Modell bietet ein wesentlich höheres Sicherheitsniveau, weil grundsätzlich keinem Gerät vertraut wird, nur weil es sich in einem bestimmten Netzwerk befindet. Stattdessen wird bei jedem Zugriff überprüft, wer zugreifen möchte, ob sich das Gerät in einem sicheren Zustand befindet und ob der Anwender für den Zugriff auf die gewünschte Anwendung berechtigt ist. Ein ZTNA (Zero Trust Network Access)-Gateway, wie es der Security-Spezialist Sophos anbietet, etabliert diesen erweiterten Schutz. Über das Gateway werden alle Unternehmensressourcen und Applikationen inklusive der Berechtigungen gesteuert. Im Gegensatz zu klassischen VPN-Anwendern, werden die Benutzer über das Gateway valide authentifiziert und erhalten genau auf die Ressourcen und Anwendungen Zugang, für die sie freigeschaltet wurden. Dabei werden weder Nutzer noch deren Rechner zu einem vertrauenswürdigen Teil des Netzwerks. Cyberkriminelle, die sich über einen infizierten Rechner am Remote-Arbeitsplatz Zugriff auf das gesamte Unternehmensnetz verschaffen wollen, haben damit keine Chance. Zusätzlich kann das ZTNA-Gateway im automatischen Informationsaustausch mit der Endpoint-Security auf dem Rechner im Homeoffice stehen. Der Vorteil besteht darin, dass zusätzlich zur Zero Trust-Authentifizierung eine Prüfung des Gesundheitszustands des externen Rechners stattfindet und dieser im Zweifelsfall automatisch von jeglicher Kommunikation mit dem Unternehmen isoliert wird.

Zero Trust ist also weit mehr als Zukunftsmusik für Organisationen, die sich besondere Sorgen um ihre Cybersecurity machen müssen. Es ist eine Technologie, die sehr vielen Unternehmen heute hilft, das existierende Sicherheitsproblem mit VPN-Netzwerkverbindungen schnell und elegant zu lösen.

Michael Veit

SOPHOS
www.sophos.de

HANNOVER MESSE 2022

DIESES MAL GEHT ES UM DATENVERNICHTUNG

Anfang März entschied sich die US-amerikanische NSA dazu, einen Leitfaden Network Infrastructure Security Guidance zu veröffentlichen. Auf etwas mehr als 50 Seiten erklären die Experten für Cybersicherheit IT-Security-Grundlagen. Die Sorge vor Angriffen ist groß in den westlichen Staaten. Das FBI und das deutsche BSI haben ihre Warnstufen nach dem Überfall auf die Ukraine und die darauffolgenden Sanktionen erhöht. In der Zusammenfassung sprechen die Verantwortlichen von der Verringerung des Risikos einer Gefährdung. Verhindern ist kaum möglich. Das deckt sich mit den Erfahrungen von IT-Experteninnen und Experten.

Wiper-Attacken

Jürgen Weiß ist einer von ihnen. Der Österreicher warnte im Tagesspiegel Background vor Angriffen in den nächsten Wochen. Dort heißt es: Es gehe nicht mehr um Ransomware, sondern um Vernichtung von Daten, sogenannte Wiper-Angriffe. Gegenwärtig seien die russischen Cyberkräfte noch in der Defensive, er warnt jedoch ausdrücklich vor Angriffsszenarien auf die kritische Infrastruktur und Finanzinstitute in den nächsten Wochen. „Es wird kein Zug entgleisen, aber die Wasserversorgung streikt nach 48 Stunden ohne Strom." In seinem Heimatland Österreich seien 80 Prozent der Unternehmen anfällig, so der Geschäftsführer von ARES Cyber Intelligence. Deutschland sei beim Thema Cybersecurity im Mittelfeld, so der Experte. Wiper-Attacken drohen und gleichzeitig warnt Weiß auch ausdrücklich vor Trittbrettfahrern.

Ein Jahr vor dem Angriff auf die Ukraine warnte der IT-Experte Christopher Bleckmann Dreher gegenüber der HANNOVER MESSE: „Liebe Industrie, warum wartet ihr auf den großen Knall? Die unaufhaltsame digitale Transformation sorgt noch dafür, dass sich auch der letzte Industriezweig nicht mehr davor verwehren kann, den Schritt in die digitale Welt zu wagen, um konkurrenzfähig zu bleiben. Das Thema IT-Sicherheit steht dabei oftmals nicht direkt auf der Agenda." Der Knall ist da. Heute kann sich Bleckmann Dreher vor Aufträgen kaum retten. Doch Expertinnen und Experten sind sich einig: Wer jetzt anfängt, der kommt zu spät. In einem Artikel gab der Schwabe grundlegende Hinweise, wie Unternehmen die ersten Schritte bei IT-Security gehen sollten.

Monitoring der OT-Landschaft

Doch nicht nur auf der IT-Seite kämpfen die Unternehmen mit Schwachstellen. Ebenso betroffen ist die OT in den Firmen und dort betrifft es vor allem die Industrieunternehmen und die Automatisierungsebene. Im Podcast von Bosch Rexroth erklärt Klaus Mochalski von Rhebo, wie das Unternehmen die ctrlX CORE Steuerung als Netzwerk-Sensor nutzt. Er und seine Kolleginnen und Kollegen haben sich auf das Monitoring der OT-Landschaft spezialisiert. Sie sehen noch Telnet-Verbindungen, Raspberry Pis aus Studentenprojekten, die mit der Außenwelt kommunizieren und niemand weiß, was die dort in der Fabrik tun und viele Unternehmen haben keine Übersicht über ihre Assets. Ein Problem, das auch schon Bleckmann Dreher identifizierte.

www.hannovermesse.de

30. Mai bis 2. Juni 2022

Erste Schritte
für IT Security:

SICHERE WORKSTATIONS

SCHWACHSTELLEN REDUZIEREN

Die Pandemie-bedingt veränderte Arbeitssituation stellt Unternehmen und Arbeitnehmer bekanntermaßen immer wieder vor neue Herausforderungen. Uwe Gries, Country-Manager DACH bei Stormshield, spricht über einen kontextuellen Ansatz für mehr Sicherheit.

? it security: *Trotz vieler Security-Awareness-Trainings erfolgt ein Großteil der Cyberangriffe aufgrund der Unachtsamkeit der Mitarbeiter. Welche Tricks wenden Angreifer hier an?*

Uwe Gries: Zusätzlich zu den üblichen Ransomware-Delikten (man spricht mittlerweile von einer dreifachen Erpressung) müssen sich Mitarbeitende vor allen Betrugsmaschen vorsehen, die sie dazu motivieren, Maßnahmen zu ergreifen. Dazu zählt etwa das Anklicken eines unbekannten Links oder die direkte Installation einer (Schad-)Software auf den Rechner. Gleiches gilt für den CEO-, Zahlungs- und Bestellungsbetrug. Alles Maschen, die nur dann erfolgreich durchgeführt werden können, wenn Cyberkriminelle über Detailwissen zu bestimmten Vorgängen verfügen. Erlangen können sie dies über Phishing, die Kompromittierung von E-Mail- oder Nutzer-Accounts oder „klassischere" Methoden wie manipulierte Wechseldatenträger.

? it security: *Warum sind gerade Wechseldatenträger so anfällig für Angriffe? Und wie kann man sie am effektivsten schützen?*

Uwe Gries: Naturgemäß werden Wechseldatenträger zum Datenaustausch an verschiedene Workstations angeschlossen, getrennt und erneut angeschlossen. Ob es um USB-Sticks, externe Festplatten oder mobile Geräte geht: Alle können unwissentlich Malware enthalten und sie bei Anschluss auf Geräte übertragen, die mit dem Unternehmensnetzwerk verbunden sind. Spezifische Systemeinstellungen oder Cybersicherheitslösungen untersagen die Nutzung von USB-Ports oder lassen nur die Nutzung von Wechseldatenträgern zu, die bestimmte Kriterien erfüllen. Allerdings muss diese Regelung kontextbasiert erfolgen, denn etwa in der Industrie erfolgt die Wartung der Systeme oft per USB.

? it security: *Herr Gries, mit Stormshield Endpoint Security Evolution stellen Sie eine neue Generation an Cybersicherheitslösungen vor. Was ist das Besondere an der Lösung, wodurch unterscheidet sie sich von herkömmlichen Lösungen?*

Uwe Gries: SES Evolution kombiniert die Fähigkeiten eines innovativen EPP-Schutzes („Endpoint Protection Platform") und einer EDR-Lösung („Endpoint Detection & Response") in einer einzigen Sicherheitslösung, die sich an den Nutzungskontext anpasst und entsprechend dynamisch agiert. So erhärtet sie automatisch die Sicherheitsmaßnahmen in erkannten Risikosituationen (mobiles Arbeiten, unsichere Verbindungen, Nutzungsrechte nach Tageszeit) und schützt dadurch die gesamte Infrastruktur.

SES Evolution bildet eine Barriere auf Betriebssystemebene. Sie verhindert abnormales Verhalten in Echtzeit (wie etwa die plötzliche Verschlüsselung des Systems) und wehrt dadurch die Ausnutzung von bekannten wie unbekannten Sicherheitslücken erfolgreich ab. Dafür benötigt die Lösung keine ständig zu aktualisierenden Signaturen, dementsprechend auch keinen Internetanschluss für ihr reibungsloses Funktionieren. Letzteres wird zudem durch Selbstschutz- und Selbstreparaturmechanismen zugesichert.

? it security: *Thema dynamische Anpassbarkeit der Sicherheitsrichtlinie: Können Sie das genauer erläutern?*

Uwe Gries: Stormshield Endpoint Security Evolution fügt Verhaltensanalyse und Kontrolle der Peripheriegeräte zusammen, um das gebotene Schutzniveau anzupassen. Es ist ein Unterschied, ob man unterwegs beziehungsweise im Home-Office oder im Unternehmen arbeitet. Die Umgebung ist nicht dieselbe. Die dynamische Anpassbarkeit der Sicherheitsrichtlinien garantiert eine optimale Absicherung.

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

STÄRKERE PASSWÖRTER

DREI TIPPS ZUR VERBESSERUNG DER PASSWORTSICHERHEIT

Weltweit kommt es immer häufiger zu Datenschutzverletzungen, bei denen sensible Unternehmensdaten, wie proprietäre Informationen und Anmeldeinformationen der Mitarbeiter offengelegt werden. Sieht man sich diese Vorkommnisse genauer an, stellt man fest, dass oft selbst die grundlegendsten Regeln zur Passwortsicherheit nicht befolgt wurden und so kein ausreichender Schutz gegen Cyberkriminelle bestand. Was tun?

Leicht geraten, leicht gehackt

Was genau Passwörter zum schwächsten Glied macht, hat Specops Software erstmalig im Rahmen eines „Weak Password Reports" untersucht. Die Forschungsergebnisse in diesem Bericht basieren auf eigenen Erhebungen und der Analyse von 800 Millionen kompromittierten Passwörtern.

Der Report verdeutlicht, dass in einer zunehmend volatilen Cybersicherheitslandschaft selbst vermeintlich starke Passwörter anfällig für Verstöße sind.

WIE BEHALTEN SIE IHRE PASSWÖRTER?

So wurde festgestellt, dass

- viele Passwörter auf leicht zu erratenen Begriffen basieren, mehrfach eingesetzt oder nur leicht abgewandelt werden für unterschiedliche Einsätze.
- 93 Prozent der Passwörter, die bei Brute-Force-Angriffen verwendet werden, aus 8 oder mehr Zeichen bestehen.
- 54 Prozent der Unternehmen über kein Tool zu Verwaltung von Passwörtern verfügen.

Doch trotz der steigenden Bedrohung gelingt es vielen Unternehmen nicht, strengere Passwortregeln und -richtlinien für Mitarbeiter zu implementieren.

Woran liegt das? Unsere Untersuchung hat einige Schwachstellen offengelegt. Auf diesen fußen unsere drei folgenden Tipps zur Erhöhung der Passwortsicherheit.

TIPP 1: Blockieren Sie schwache und kompromittierte Passwörter

Häufig verlangen Unternehmen längere Passwörter. Darüber hinaus sollten sie die Konten sichern, indem sie verhindern, dass Mitarbeiter schwache und bereits gehackte Kennwörter verwenden.

Milliarden von kompromittierten Passwörtern, die durch verschiedene Angriffsmethoden aggregiert wurden, sind derzeit im Dark Web verfügbar. Wöchentlich werden etwa 1 Millionen weitere Passwörter entschlüsselt und gestohlen. Ein Beispiel zu den Folgen: Im Jahr 2021 legten Hacker die Anmeldeinformationen von über 68 Millionen Dropbox Nutzern offen. Ursache dafür war die Wiederverwendung eines, von einer anderen Website gehackten, Passwortes.

Der Einsatz möglichst langer Passphrasen, die Nutzung eines benutzerdefinierten Passwortwörterbuchs und einer Breached Password-Liste während des Passworterstellungsprozesses kann Mitarbeiter daran hindern, schwache, kompromittierte Passwörter zu verwenden und vor Brute-Force-Angriffen schützen.

TIPP 2: Fügen Sie weitere Ebenen der Multi-Faktor-Authentifizierung hinzu

Eine weitere Maßnahme, Passwortangriffe zu verhindern, ist die Einführung einer Multi-Faktor-Authentifizierung (MFA). Zu den Multi-Faktoren zählen zum Beispiel Biometrie, Authentifizierungstoken/-codes, Sicherheitsfragen und Authentifizierungs-Apps. Biometrische Methoden, wie Fingerabdruck- oder Netzhautscan sind hochsicher, können aber je nach eingesetzter Hardware teuer werden. Da viele Cloud-Dienste heute MFA anbieten, ist es einfach, diese an die Unternehmensanforderungen anzupassen.

Allein durch den Einsatz von MFA, können 80 bis 90 Prozent der Cyberangriffe verhindert werden.

TIPP 3: Benutzerüberprüfung am Service Desk

Nur die Verwendung von Multi-Faktor-Authentifizierung allein reicht nicht immer aus, um sich sicher zu schützen. Häufig ist die deutsche Wirtschaft Ziel, von Social Engineering Angriffen. Insgesamt entstand durch Cyberangriffe auf Unternehmen im Jahr 2021 ein Gesamtschaden von 223 Milliarden Euro. Laut dem Digitalverband Bitkom ist die Schadenssumme damit mehr als doppelt so hoch wie in den Jahren 2018/2019, als sie noch 103 Milliarden Euro pro Jahr betrug. Neun von zehn Unternehmen (88 %) waren 2020/2021 von Angriffen betroffen, im Vergleich zu 75 Prozent in den Jahren 2018/2019.

Diese Zahlen verdeutlichen: Alle Unternehmen sind potenzielle Ziele für Cyberattacken. Social-Engineering-Angriffe sind hierbei besonders skrupellos, da Kriminelle versuchen, die IT-Profis unter Druck zu manipulieren und sie unwissentlich zu Komplizen des Verbrechens zu machen. Dennoch haben laut Erhebungen von Specops Software nur 48 Prozent der Unternehmen eine Benutzerüberprüfungsrichtlinie für eingehende Anrufe an Service Desks. Doch diese ist dringend geboten. Denn die Durchsetzung der Benutzerüberprüfung am Service Desk ermöglicht es Service-Desk-Profis, Betrug zu erkennen und mit Mitarbeitern in Kontakt zu treten.

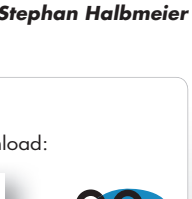
Ein Beispiel: Wenn ein Benutzer ein mobiles Gerät bei einem Service Desk registriert, können die Service-Desk-Profis einen Mitarbeiter anrufen und einen Code an das mobile Gerät senden. Durch diesen wird die Identität geprüft und so verhindert, dass unwissentlich wertvolle Daten an Betrüger weitergegeben werden.

Das Fazit – Zeit zu handeln

Die Bedrohungslage durch Cyberkriminelle nimmt weiter zu, auch getrieben durch weltpolitische Krisenherde. Nötig ist daher die Diversifizierung von Sicherheitsprozessen mit Breached-Password-Listen, Passwortwörterbüchern, verschiedenen MFA-Methoden in Kombination mit einem leistungsstarken Service Desk. Nur so können Unternehmen ihre Cybersicherheit an mehreren Fronten stärken und sicherstellen, dass Kriminelle keinen Einstiegspunkt finden.

Stephan Halbmeier

Weak Password Report zum Download:



IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Johannes Carl, Andreas Fuchs, Stephan Halbmeier, Sabine Kuch, Daniel Linder, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Steffen Reimann, Michael Veit, Jörg von der Heydt

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 29,
gültig ab 1. Oktober 2021.

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

Karen Reetz-Resch
Home Office: 08121-9775-94,
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

SICHERER FERNZUGRIFF PER VPN

IN 6 SCHRITTEN ZUR LANGFRISTIGE FLEXIBLEN REMOTE-WORK-UMGEBUNG

Die Corona-Krise hat zu einem Boom bei VPN-Diensten in Unternehmen geführt. Viele Umsetzungen mussten überstürzt und unter großem Zeitdruck vorgenommen werden. Mit der erneuten massenhaften Rückkehr ins Homeoffice im Januar 2021 zeigte sich, dass bei vielen Unternehmen die bestehende Remote-Access-Infrastruktur dringende Anpassungen benötigt. Um künftig flexibel auf zu erwartende Schwankungen reagieren zu können, müssen bestehende Strukturen überdacht werden. Der nahtlose Übergang zwischen Homeoffice und Büroarbeitsplatz ist ein entscheidender Faktor für die Produktivität und Business Continuity von Unternehmen.

Wir zeigen Ihnen in diesem Whitepaper in sechs Schritten, wie Sie mithilfe einer durchdachten Remote-Access-Lösung zur langfristig flexiblen Remote-Work-Umgebung kommen.

Das Whitepaper umfasst 19 Seiten und steht zum kostenlosen Download bereit: www.it-daily.net/download

We secure IT

19.05.22 | Digitalevent

Die We secure IT geht in die fünfte Runde!
Wir informieren Sie über alle Themen der Cybersecurity, die uns aktuell beschäftigen.
Seien Sie dabei. Es erwarten Sie spannende Vorträge, Live Demos sowie Q&A-Runden.

Highlights aus der Agenda

Zero Trust

- **Zero Trust als Wegbereiter für die moderne Arbeitswelt**
  Michael Veit, Technology Evangelist, SOPHOS

- **Warum auch Ihre Mitarbeiter Zero Trust lieben werden**
  Carsten Hoffmann, Manager Sales Engineering, Forcepoint

Security Awareness

- **Sicherheit und Produktivität für das moderne Unternehmen**
  Andreas Fuchs, Head of Strategy & Vision, DriveLock

Cybersecurity

- **V*rsc5lü§§*|u=g – Lassen Sie sich nicht in Ihre Daten schauen**
  Philipp Wittek, Technical Sales Manager, Secomba GmbH

- **Cyber Space Wars – Auf den Spuren der Hacker**
  Jochen Meyer, Senior SOC Analyst, suresecure GmbH

Cloud Security

- **Datenschutz durchsetzen und Compliance gewährleisten in der Cloud**
  Michael Mors, General Manager Central Europe, Box

SCAN ME

Jetzt anmelden

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

#WesecureIT2022


STORMSHIELD
Die europäische Wahl für Cybersicherheit
Ihr zuverlässiger Partner
für die
maximale Freiheit,
sich auf das Kerngeschäft
zu konzentrieren,
in aller Gelassenheit
IT
OT
www.stormshield.com