itmanagement
JULI/AUGUST 2022

INKLUSIVE 32 SEITEN
IT SECURITY SPEZIAL

ab Seite 20

DIGITALISIERUNG ALS PROZESS

MOBIL, SICHER UND NACHHALTIG

Bernd Rischer, Kyocera Document Solutions

UNTERNEHMENS-KULTUR

Die Zukunft der Arbeitswelt

LIZENZEN-DSCHUNGEL

Raus mit dem Software-Müll

LOW-CODE-ANWENDUNGEN

Design Thinking als Motor

www.it-daily.net


itsa EXPO CONGRESS
HOME OF IT SECURITY
HIT HACKERS HARD
LET'S TALK ABOUT IT SECURITY!
25. – 27. Oktober 2022
Nürnberg, Germany
Jetzt Gratis-Ticket sichern:
itsa365.de/hit-hackers-hard
NÜRNBERG MESSE

LIEBE LESER,

jede unserer Ausgaben konzentriert sich auf ein Fokusthema und diverse Schwerpunkte, die von Ausgabe zu Ausgabe rotieren, über die Jahre angepasst und ergänzt werden – sowohl im it management als auch im it security.

Diese Ausgabe des it management fokussiert sich mal wieder auf das Thema Digitalisierung, ein Thema, das uns nun schon eine Weile begleitet und auch weiterhin begleiten wird. Ein sehr umfassender Bereich, denn er greift auch viele unserer Schwerpunkte, wie Cloud Computing, New Work oder KI auf, so dass eine klare thematische Abgrenzung manchmal schwer möglich ist.

Die Digitalisierung selbst ist bekanntermaßen ein Veränderungsprozess von Gesellschaft und Unternehmen und wirkt somit grenzüberschreitend – zieht also offensichtlich keine Grenzen – und das ist auch gut so. Digitalisierung kann nämlich nur funktionieren, wenn alle Bereiche mitziehen und interagieren. Wie das geht, wie man dank Digitalisierung mobiler, sicherer und nachhaltiger arbeiten und wie die Umsetzung erfolgreich funktionieren kann, lesen Sie in dieser Ausgabe ab Seite 10.

Was es Neues im Bereich Cybersecurity, Datenschutz und Verschlüsselung gibt, lesen Sie im aktuellen Supplement it security. Auch hier gilt: Mit Interaktion und Kommunikation kommt man schneller und besser weiter, als im Alleingang.

Übrigens: ein Bereich, der im Rahmen der Digitalisierung zunehmend an Bedeutung gewinnt, ist das Thema Nachhaltigkeit – Fokusthema der Ausgabe 9. Falls Sie hier etwas Interessantes beitragen möchten, lassen Sie es mich wissen.

Herzlichst

Carina Mitzschke | Redakteurin it management

Künstliche Intelligenz

Fluch oder Segen?

SCAN ME

Mehr Infos dazu im Printmagazin

itmanagement

und online auf www.it-daily.net

16

12

INHALT

COVERSTORY

IT MANAGEMENT

Inklusive
32 Seiten

IT SECURITY SPEZIAL

ANATOMIE REALER CYBERATTACKEN IM JAHR 2021

DIE WICHTIGSTEN ERKENNTNISSE VON INCIDENT-RESPONSE-UNTERSUCHUNGEN

Die Herausforderung, ein Unternehmen gegen sich schnell entwickelnde, immer komplexer werdende Cyberbedrohungen zu verteidigen, kann beträchtlich sein. Angreifer passen ihr Verhalten und ihre Toolsets kontinuierlich an und entwickeln sie weiter, nutzen neue Schwachstellen und missbrauchen alltägliche IT-Tools, um der Entdeckung zu entgehen und den Sicherheitsteams immer einen Schritt voraus zu sein.

Aus diesem Grund stellt Sophos den Sicherheitsteams in Unternehmen das neue Active Adversary Playbook 2022 zur Verfügung. Das Playbook beschreibt einerseits genau, wie Cyberkriminelle bei ihren Angriffen vorgehen und zeigt andererseits konkrete Wege auf, wie schädliche Aktivitäten im Netzwerk erkannt und abgewehrt werden können.

www.sophos.de

47%
der Cyberangriffe hatten ihren Anfang in einer ausgenutzten Schwachstelle

82%
der Zugriffe via RDP dienten internen Zugriffen und der Erkundung – 2020 waren es 69 Prozent

73%
aller Angriffe beinhalten Ransomware

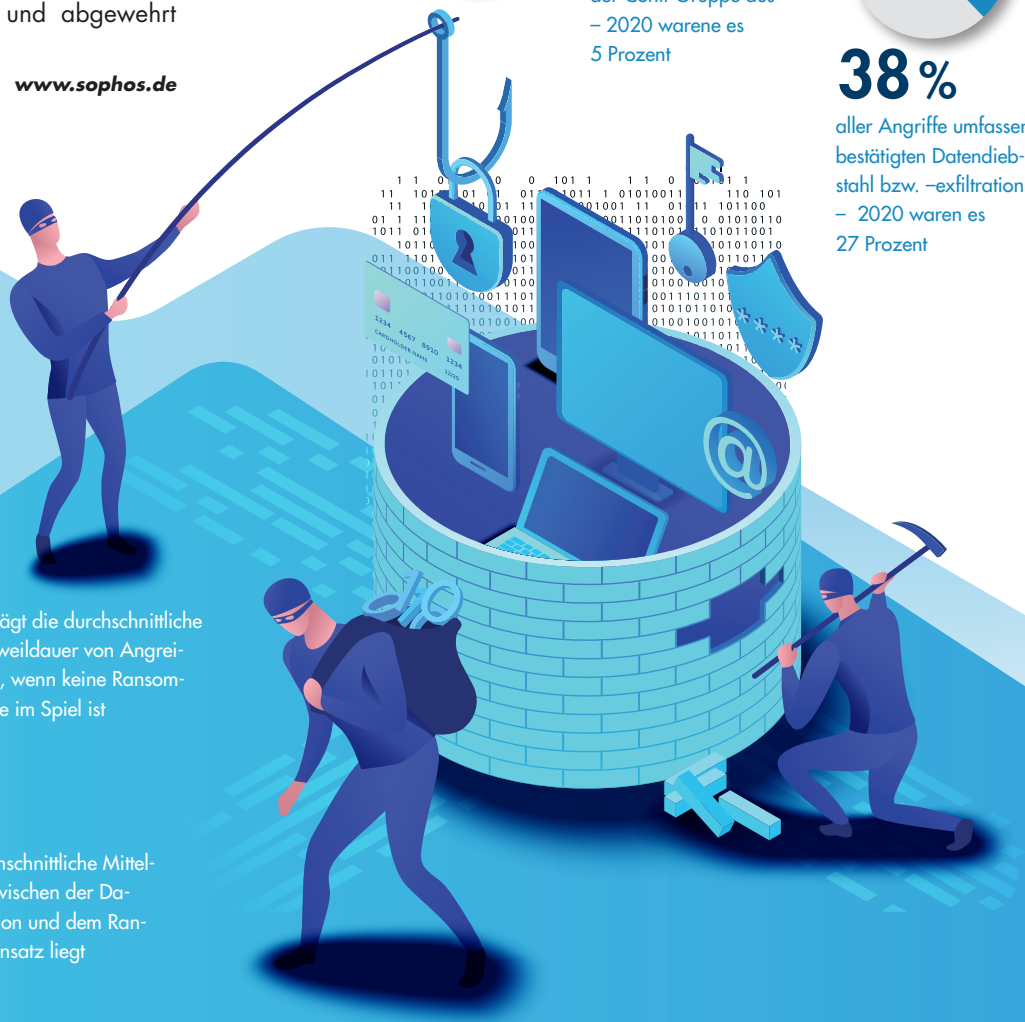
18%
aller Ransomware-Angriffe gingen von der Conti-Gruppe aus – 2020 warene es 5 Prozent

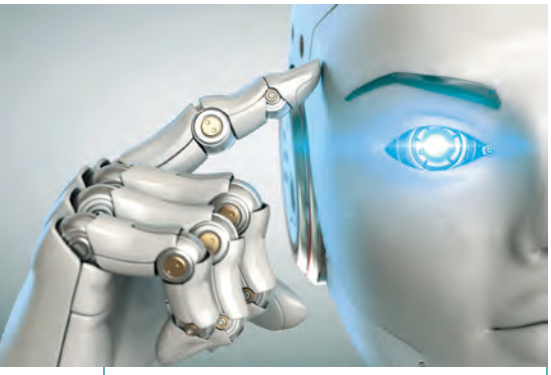
38%
aller Angriffe umfassen bestätigten Datendiebstahl bzw. –exfiltration – 2020 waren es 27 Prozent

15 TAGE
beträgt die durchschnittliche Verweildauer von Angreifern im Netzwerk – 2020 waren es 11 Tage

34 TAGE
beträgt die durchschnittliche Verweildauer von Angreifern, wenn keine Ransomware im Spiel ist

4,28 TAGE
ist der durchschnittliche Mittelwert, der zwischen der Daten-Exfiltration und dem Ransomware-Einsatz liegt





KÜNSTLICHE INTELLIGENZ

HERAUSFORDERUNGEN FÜR UNTERNEHMEN

HERAUSFORDERUNGEN BEIM EINSATZ VON KI

65 % Finden oder Anpassen von Modellen und Algorithmen

54 % Aufbereitung der Daten

46 % Aufbau der Infrastruktur

KI wird für Unternehmen künftig von enormem Wert sein und in den nächsten zehn Jahren immens zum Wachstum der Weltwirtschaft beitragen. Führungskräfte sind sich des Potenzials von KI durchaus bewusst. Um davon zu profitieren sind die IT-Teams gefordert, doch hier treten bei der Einführung von KI bei den meisten Unternehmen erste Herausforderungen auf.

Die Ergebnisse einer aktuellen Umfrage zeigen, dass IT-Führungskräfte in deutschen Unternehmen mit großem Engagement neue KI-Modelle und Algorithmen übernehmen. Es ist allerdings eine zunehmende Herausforderung für sie, mit der Geschwindigkeit des Modell- und Datenwachstums schritthalten zu können. Das gaben 73 Prozent der befragten deutschen IT-Führungskräfte an. Darüber hinaus meinten sie, dass es schwierig sein würde, neue Algorithmen einzusetzen.

KI-Implementierung

Mit 56 Prozent geben mehr als die Hälfte der Führungskräfte in deutschen Unternehmen an, dass die geschäftlichen Auswirkungen von KI in den nächsten 12 bis 24 Monaten „transformierend" sein oder das „Geschäft erheblich verbessern" werden. Nur 16 Prozent erwarten, dass KI „überhaupt keine Auswirkungen" auf ihr Geschäft haben wird.

sambanova.ai

MIGRATION AUF WINDOWS 11

WENIGER ALS DIE HÄLFTE DER IT-GERÄTE IST BEREIT

Nexthink veröffentlichte kürzlich den Report „Predicting Windows 11 Upgrades in Corporate IT".

Windows 11 wird zum 24. Oktober 2025 Microsofts primäres Betriebssystem, damit verbunden sind striktere Anforderungen im Vergleich zum Vorgänger Windows 10. Auch wenn der Termin in weiter Ferne zu liegen scheint – die aktuellen Daten deuten darauf hin, dass viele Unternehmen diese Zeit durchaus zur Vorbereitung benötigen. Der erforderliche Aufwand, um die 60 Prozent der nicht-kompatiblen Geräte zu aktualisieren, liegt bei mehr als 4,2 Millionen manuellen Arbeitsstunden.

Wichtig ist, dass IT-Teams frühzeitig und genau die Kompatibilität und Leistung von Geräten bewerten, um Kosten, Verzögerungen und Unterbrechungen zu minimieren. Dies zeigen auch die zentralen Ergebnisse der Studie.

www.nexthink.com/de

40 % der gesamten Geräteflotte sind für die Migration bereit

26 % der Geräte haben die unterstützte CPU, aber das Betriebssystem muss migriert werden

17 % der Geräte können mit dem neuesten Upgrade von Win 10 OS länger genutzt werden

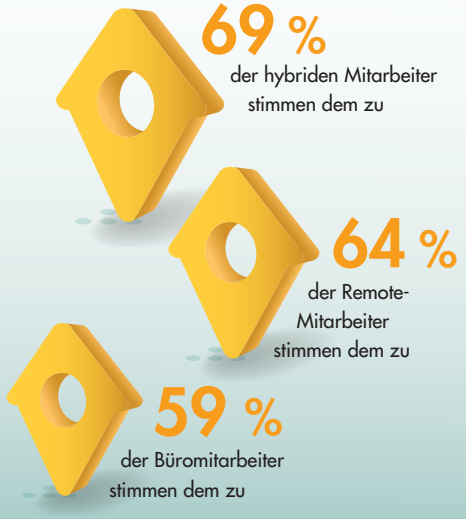
18 % der Geräte müssen aufgefrischt werden, da sie nicht auf Win 11 aktualisiert werden können

HYBRIDE ARBEIT IST ERFOLGREICH

HÖHERES ENGAGEMENT UND GRÖSSERE PRODUKTIVITÄT

Ob es Unternehmen gefällt oder nicht, Arbeitnehmer mögen hybrides Arbeiten – und das Modell funktioniert: Laut Work Rebalanced, der neusten Studie von Citrix, sind hybride Mitarbeiter – diejenigen, die teilweise remote, teilweise im Büro arbeiten – produktiver und engagierter als die Arbeitnehmer, die gänzlich remote oder im Büro arbeiten. Zudem ist ihr körperliches und geistiges Wohlbefinden besser und sie haben eine positivere Einstellung zu ihrem Unternehmen.

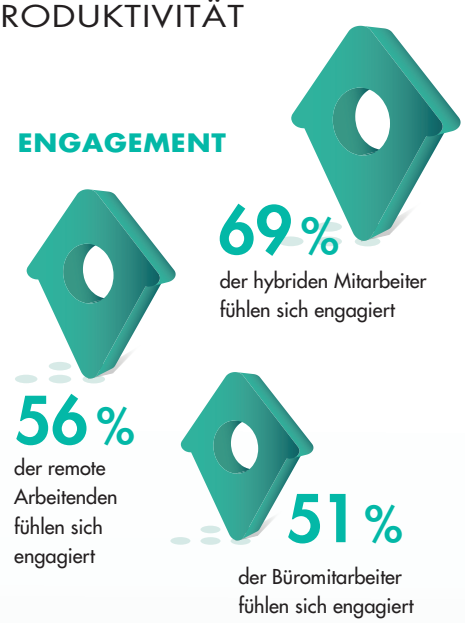
FÜHLEN SIE SICH PRODUKTIV?



Der große Reset

Ob und wie flexible Arbeitsformen eingeführt werden sollten, ist für Unternehmen weltweit ein akutes Thema. Um sie bei dieser Entscheidung zu unterstützen, hat Citrix in Zusammenarbeit mit den Marktforschungsunternehmen Man Bites Dog und Coleman Parkes Research eine Befragung von insgesamt 900 Führungskräften und 1.800 Wissensarbeitern durchgeführt. Das Ergebnis: Werden hybride Arbeitsmodelle richtig umgesetzt, können sie zu einer produktiveren und gesünderen Belegschaft führen.

ENGAGEMENT



Ein virtuelles Erlebnis

Die Umfrage ergab auch, dass Technologie ein wichtiger Erfolgsfaktor ist, um hybrides Arbeiten zu ermöglichen und die von dezentral arbeitenden Angestellten geforderte „Virtual-First-Experience" zu schaffen. Die Mitarbeiter wollen Zugang zu Tools, mit denen sie dort arbeiten können, wo sie möchten und wo sie am produktivsten sind. Und sie erwarten von ihren Arbeitgebern, dass sie ihnen dies bieten.

Von entscheidender Bedeutung ist dabei die Beseitigung von Störungen und Ablenkungen, die Technologie am Arbeitsplatz verursachen kann. Im Durchschnitt muss ein Arbeitnehmer beispielsweise vier oder mehr Anwendungen bedienen, um nur einen einzigen Geschäftsprozess durchzuführen. Und für den Zugriff auf diese Anwendungen muss er sich mehrere Passwörter merken und durch eine Vielzahl von Schnittstellen navigieren. In der Studie wird deutlich, dass dies für die Mitarbeiter frustrierend ist und sie ausbremst. So verbringt ein Mitarbeiter durchschnittlich am Tag etwa 54 Minuten nur damit, sich mit technologischen Herausforderungen zu beschäftigen.

www.citrix.de

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

DIGITALISIERUNG ALS PROZESS BEGREIFEN

MOBILER, SICHERER UND NACHHALTIGER ARBEITEN

Im Rahmen der Digitalisierung kommt Geschäftsprozessen eine zentrale Bedeutung zu. Bernd Rischer, Group Director Sales bei Kyocera Document Solutions, beantwortet hierzu die Fragen von it management-Herausgeber Ulrich Parthier.

Ulrich Parthier: *Herr Rischer, bei der Digitalisierung von Geschäftsprozessen stellen sich die Unternehmen die Ausgangsfrage: „Wo stehen wir und wie stehen wir im Vergleich zum Mitbewerb?" Die meisten Firmen dürften wohl kaum ihren digitalen Reifegrad kennen. Wie hilfreich sind da Modelle zur Ermittlung des Reifegrads digitaler Geschäftsprozesse, wie sie zum Beispiel der BITKOM anbietet?*

Bernd Rischer: Im Unternehmen müssen Informationen zum richtigen Zeitpunkt am richtigen Ort verfügbar sein. Potenzialanalysen und Reifegradmodelle können aufzeigen, inwieweit man den eigenen Anforderungen bisher gerecht wird. Um Fortschritte nachverfolgen zu können, sollte der Status quo regelmäßig auf den Prüfstand kommen. Weil die Digitalisierung ein Prozess ist, werden sich immer auch Optimierungspotenziale offenbaren. Es gibt aber auch offensichtliche Anzeichen für Nachholbedarf: Wenn ein Manager zur Freigabe von Rechnungen ins Büro kommen muss oder bei der Suche nach Informationen Aktenordner im Archiv durchforstet werden, können die Prozesse im Unternehmen nicht wirklich State-of-the-Art sein.

Ulrich Parthier: *Die digitale Transformation verfolgt ja als ein wesentliches Ziel, Prozesse in Unternehmen anzupassen und zu optimieren. Kyocera hat dazu das Leistungsversprechen „Making information faster" formuliert. Geschwindigkeit ist also ein weiterer Aspekt. Wie genau sieht Ihre Idee dahinter aus?*

Bernd Rischer: „Making information faster" verdeutlicht, wie sehr sich Kyocera weiterentwickelt hat. Wir kümmern uns nicht nur um das gedruckte Dokument, sondern um das gesamte Informationsmanagement. Dazu gehören Capturing und Informationsverarbeitung genauso wie das digitale Dokumentenmanagement und der Output. Damit sind wir als Unternehmensverbund von Kyocera und den Tochterunternehmen ALOS und AKI in der Lage, Geschäftsprozesse nicht nur zu digitalisieren, sondern auch zukunftsfähig zu machen. Das bedeutet sowohl schneller und einfacher als auch mobiler, sicherer und nachhaltiger.

Ulrich Parthier: *Der Mittelstand ist einer der großen Wachstumstreiber der deutschen Wirtschaft. Warum tun sich insbesondere mittelständische Unternehmen bei der Digitalisierung von Geschäftsprozessen schwer?*

Bernd Rischer: Die größte Hürde bei der Einführung neuer Hard- und Software ist gerade für kleine und mittlere Unternehmen die fehlende Zeit im Alltagsgeschäft. Digitalisierungsinitiativen sind häufig Nebenprojekte, bei denen es an Ressourcen und Know-how mangelt. Zudem ist für viele Entscheider der Mehrwert nur schwer greifbar, weil es um eine langfristige Entwicklung geht. Hinzu kommt, dass viele Mittelständler zeit- und kostenintensive Projekte fürchten, weil damit auch immer ein Risiko einhergeht. Deshalb zeichnet sich unsere hauseigene Dokumentenmanagement-Lösung, der Kyocera Workflow Manager, dadurch aus, modular und schnell implementierbar zu sein. Das schrittweise Einführen und individuelle Skalieren von Prozessen macht die Digitalisierung insbesondere für kleinere Betriebe einfach und schnell umsetzbar. So lässt sich stets der Überblick über Fortschritte, Hindernisse und Kosten behalten.

Ulrich Parthier: *Neben der richtigen Strategie und Methodik ist die Auswahl der passenden IT-Lösungen ein weiterer Schlüssel für eine erfolgreiche Digitalisierung in jedem Unternehmen. Gibt es dazu ein Vorgehensmodell und Partner, die dies zusammen mit Kunden umsetzen können?*

Bernd Rischer: Weil die Digitalisierung als Prozess zu begreifen ist, müssen Vorgänge im Unternehmen regelmäßig kritisch betrachtet und geprüft werden, ob sie die aktuellen und zukünftigen Anforderungen erfüllen. Dazu entwickeln wir gemeinsam mit unseren Fachhandelspartnern Optimierungsstrategien, mit denen Kunden die Digitalisierung möglichst schnell angehen können. Besonders lohnen sich dokumentenintensive Prozesse, weil Erfolge hier schnell sichtbar werden – etwa bei der Freigabe von Rechnungen. Mit leistungsfähiger Hardware, digitalen Lösungen und Services können solche Prozesse und ihre Durchlaufzeiten deutlich beschleunigt werden.

Ulrich Parthier: *Wichtig ist bei allen Initiativen immer ein ganzheitlicher Ansatz, um Geschäftsprozesse zukunftsfähig zu machen. Sie haben sich in den vergangenen Jahren vom reinen Druckerhersteller hin zu einem Anbieter vom In-*

put- bis hin zum Outputmanagement entwickelt. Wie haben sie diesen Shift bewerkstelligt?

Bernd Rischer: Immer mehr Dokumente sind digital statt analog. Im Umgang mit Informationen ergeben sich dadurch unzählige Möglichkeiten, die aufeinander abgestimmt werden müssen. Unser Leistungsspektrum umfasst den gesamten Lebenszyklus von Dokumenten und stellt Geschäftsprozesse in den Mittelpunkt. Dadurch sind wir seit Jahren weit mehr als ein reiner Output-Experte. Systeme, Software und Services müssen ineinandergreifen, um die Digitalisierung und Optimierung von Geschäftsprozessen ganzheitlich voranzutreiben. Um dies bestmöglich abzubilden, haben wir unsere Kompetenzen durch strategische Zukäufe und Investitionen in die Weiterentwicklung erweitert.

> WEIL DIE DIGITALISIERUNG ALS PROZESS ZU BEGREIFEN IST, MÜSSEN VORGÄNGE IM UNTERNEHMEN REGELMÄSSIG KRITISCH BETRACHTET UND GEPRÜFT WERDEN, OB SIE DIE AKTUELLEN UND ZUKÜNFTIGEN ANFORDERUNGEN ERFÜLLEN.
>
> Bernd Rischer,
> Group Director Sales, Kyocera Document Solutions,
> www.kyoceradocumentsolutions.de

? **Ulrich Parthier:** *Von den angesprochenen Akquisitionen erwarten sie Synergieeffekte. Gleichzeitig agieren die Unternehmen weiterhin eigenständig. Wie klappt da der Erfahrungsaustausch?*

Bernd Rischer: Auch, wenn jedes Unternehmen eigenständig operiert, ergeben sich innerhalb der Kyocera-Gruppe viele Synergien. Zudem ergänzen sich die unterschiedlichen Expertisen und Erfahrungsschätze sehr gut: Kyoceras umfassendes Know-how im Office-Druck und die Erfahrung im Mittelstandsgeschäft mit unseren Fachhandelspartnern haben sich über mehr als 35 Jahre bewährt. Die ALOS GmbH ist auf die Implementierung und Umsetzung von Dokumentenmanagement-Systemen spezialisiert und die AKI GmbH ist Infrastruktur-Experte für die Optimierung von Druckprozessen und des Output-Managements. Kyocera bündelt dieses Wissen und kann so die ganzheitliche Optimierung von Informationsprozessen aus einer Hand bieten.

? **Ulrich Parthier:** *Hat die Corona-Pandemie dem Fortschritt in Sachen Digitalisierung einen zusätzlichen Schub verliehen? Und welche Rolle spielt die Digitalisierung in einer hybriden Arbeitswelt?*

Bernd Rischer: Viele Unternehmen haben sich in den letzten zwei Jahren neue Fragen gestellt, weil ihre Geschäftsprozesse ortsunabhängig funktionieren mussten. Manche von ihnen standen der Automatisierung dokumentenintensiver Prozesse lange ablehnend gegenüber und das Know-how im Unternehmen fehlte. Dadurch haben sich der Bedarf und der Anspruch in Sachen Digitalisierung stark gewandelt. Bei der zukunftsfähigen Gestaltung von Geschäftsprozessen spielen Dokumentenmanagement-Lösungen eine wichtige Rolle, denn sie ermöglichen Unternehmen, Dokumente digital, ortsunabhängig und auch mit mehreren Nutzern gleichzeitig zu bearbeiten. Solche Lösungen sind bei immer mehr Unternehmen im Einsatz und gewährleisten hohe Effizienz bei Geschäftsprozessen.

! **Ulrich Parthier:** *Herr Rischer, wir danken Ihnen für das Gespräch.*

THANK YOU

DÄMPFER FÜR DIE DIGITALISIERUNG

WELTLAGE BREMST DIGITALE TRANSFORMATION DER WIRTSCHAFT

In 94 Prozent der deutschen Unternehmen hat die Digitalisierung zwar durch die Pandemie an Bedeutung gewonnen, aber 95 Prozent erwarten, dass Störungen in den Lieferketten nun die Digitalisierung bremsen werden. 92 Prozent haben diese Sorge aufgrund der hohen Inflationsrate, 78 Prozent wegen steigender Energiekosten und 57 Prozent aufgrund des russischen Angriffs auf die Ukraine. Zugleich gehen zwei Drittel (69 Prozent) davon aus, dass in fünf Jahren digitale Geschäftsmodelle von sehr großer Bedeutung oder sogar entscheidend für den eigenen wirtschaftlichen Erfolg sein werden.

Das sind Ergebnisse einer repräsentativen Befragung von 604 Unternehmen ab 20 Beschäftigten in Deutschland.

Digitalisierung fällt vielen schwer

In der Vergangenheit sind viele Unternehmen bei der Digitalisierung auf unerwartete Schwierigkeiten gestoßen. Das geben 9 von 10 (89 Prozent) Befragten an. Gleichzeitig sind 61 Prozent überzeugt: Digitalisierung hat unser Unternehmen wettbewerbsfähiger gemacht. Und 51 Prozent stellen fest, dass sie durch Digitalisierung als Arbeitgeber attraktiver geworden sind. „Digitalisierung ist kein Selbstläufer und lässt sich nicht nebenher aus dem Ärmel schütteln. Digitalisierung braucht Strategie, Kompetenz und Ressourcen. Digitalisierung erfordert neben Investitionen in Hardware und Software auch einschlägiges Know-how auf allen Ebenen und die Bereitschaft, Prozesse umzubauen und nicht selten auch die Unternehmenskultur fortzuentwickeln“, so Bitkom-Präsident Achim Berg.

Digitale Angebote sind zum Standard geworden

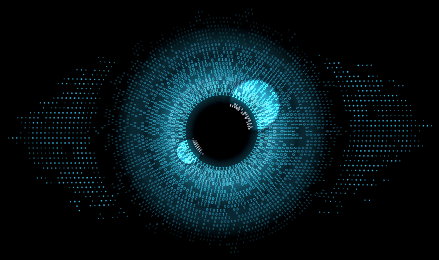
Fast alle Unternehmen haben in den vergangenen fünf Jahren ihr Angebot digitalisiert. So geben 10 Prozent an, neue digitale Produkte auf den Markt gebracht zu haben, bestehende Produkte haben 7 Prozent durch digitale ersetzt und 14 Prozent mit digitalen ergänzt. Ein Drittel (33 Prozent) hat neue digitale Dienstleistungen ins Angebot genommen, 56 Prozent haben bestehende Dienstleistungen mit digitalen ergänzt und 10 Prozent haben bestehende Dienstleistungen durch digitale ersetzt. Nur 3 Prozent der Unternehmen geben an, in den vergangenen fünf Jahren überhaupt keine digitalen Produkte oder Dienstleistungen entwickelt zu haben.

Die große Mehrheit der Unternehmen geht davon aus, dass digitale Geschäftsmodelle für den eigenen wirtschaftlichen Erfolg wichtiger werden.

Aktuell werden die Umsätze vor allem noch in der analogen Welt gemacht. Nur 5 Prozent der Unternehmen erzielen heute mindestens die Hälfte ihrer Umsätze mit digitalen Produkten und Dienstleistungen, ein Fünftel des Umsatzes oder mehr erreicht jedes zweite dieser Unternehmen (52 Prozent).

Entsprechend kritisch gehen die befragten Unternehmen auch mit der deutschen Wirtschaft insgesamt um. Nur 2 Prozent der Unternehmen sehen Deutschland im weltweiten Vergleich bei der Digitalisierung als führend an, 24 Prozent sehen die Wirtschaft in der Spitzengruppe. Aber ein Drittel (36 Prozent) verortet Deutschland im Mittelfeld, 27 Prozent unter den Nachzüglern und 8 Prozent sogar als abgeschlagen.

www.bitkom.org



DIGITALISIERUNG

SO GELINGT DIE UMSETZUNG

In der Zusammenarbeit mit Unternehmen beobachten wir von Planview, dass derzeit viele ihre Strukturen und Prozesse digitalisieren, um sich der Dynamik der Märkte anzupassen. Aufgrund unserer Praxiserfahrung wissen wir, worauf es bei einer Neuausrichtung ankommt. Unsere Work-Management-Spezialisten haben deshalb sieben Empfehlungen für die erfolgreiche Umsetzung einer Digitalisierungsstrategie zusammengestellt.

1. Den Überblick behalten

Vor dem Start eines Digitalisierungsprojekts gilt es, das Ziel zu definieren und zu klären, wie sich relevante Informationen und Echtzeitanalysen unkompliziert abrufen lassen. Ein zentraler Überblick ist entscheidend, um auf Marktveränderungen frühzeitig zu reagieren. Dafür wird ein strategisches Dashboard benötigt, das eine Kontrolle über unternehmensweite Finanz-, Leistungs- und Investitionsdaten bietet.

MIT DER RICHTIGEN PORTFOLIO-MANAGEMENT-LÖSUNG GELINGT DIE EFFEKTIVE NEUVERNETZUNG VON STRATEGIE UND UMSETZUNG UND DEM GESCHÄFTSERFOLG STEHT NICHTS MEHR IM WEGE.

Michael Biechele,
Group Vice President, Sales, Planview,
www.planview.com

2. Die Strategie konkret umsetzen

Eine Strategieplanung sollte sowohl eine konkrete Top-Down- als auch eine Bottom-Up-Planung beinhalten, mit der sich Initiativen priorisieren, Finanzierungen bewerten und die Verfügbarkeit von Ressourcen sicherstellen lassen. Zudem sind eine allgemeinverständliche Kommunikation sowie eine transparente und zentrale Steuerung für die Umsetzungsphase unerlässlich.

3. Produkte und Technologien verknüpfen

Wer seine Strukturen transformieren möchte, benötigt eine Vernetzung von Technologie, Anwendung, Datensicherheit und Kundenerfahrung. Deshalb sollte man unbedingt das Betriebsmodell einer Organisation auf die Verbindungen zwischen den Produkten und Technologien überprüfen, denn dort lauern nicht selten versteckte Risiken. Aus diesen Erkenntnissen wiederum lassen sich neue Chancen ableiten.

4. Gute Ideen nutzen

Innovation ist das Herzstück der digitalen Transformation. Um innovativ zu sein, müssen Kundenanforderungen verstanden und mit Markttrends abgeglichen werden. Wem es gelingt, aus diesen Informationen die richtigen Ideen abzuleiten, ist schon einen Schritt weiter. Die Kür ist dann die Automatisierung der Innovationsprozesse, was schlussendlich zu neuen Produkten und Services führt.

5. Durchdachte Investitionsentscheidungen treffen

Um Potenziale zu maximieren, braucht es valide Echtzeitdaten und schnelle Entscheidungsprozesse – zumal sich Technologien verändern und täglich neue Herausforderungen hinzukommen. Eine Status-Quo-Analyse und die Simulation von Szenarien sind deshalb wichtige Instrumente zur Entscheidungsfindung.

6. Schnellere Marktreife von Produkten und Services

Letztlich hängt der Erfolg jedoch davon ab, wie schnell sich Umsatz erzielen lässt. Deshalb sind die richtigen Tools und Prozesse unerlässlich. Wer das Potenzial intelligenter Mitarbeiter und moderner Automatisierungs-Tools nutzt, um eine konsistente, replizierbare Produktbereitstellung zu erreichen, wird seine Markteinführungszeiten verkürzen.

7. Initiativen schneller und intelligenter umsetzen

Die digitale Transformation erfordert Lösungen, die verschiedene Arbeitsmethoden automatisieren - von Agile über iterative Verfahren bis hin zu Collaborative Work Management etc. Die Mitarbeiter sollten sich deshalb das für sie am besten geeignete Tool aussuchen, um nach ihren eigenen Vorstellungen arbeiten zu können. So bekommt das Digitalisierungsprojekt ganz von allein die nötige Dynamik.

Wir von Planview wissen, dass sich Unternehmen ständig an neue Gegebenheiten anpassen müssen. Mit der richtigen Portfolio-Management-Lösung gelingt die effektive Neuvernetzung von Strategie und Umsetzung und dem Geschäftserfolg steht nichts mehr im Wege.

Michael Biechele

Das eBook umfasst 46 Seiten und steht zum kostenlosen Download bereit.
www.it-daily.net/download

STORAGE

WHAT`S NEW?

Daten entwickeln sich in der modernen digitalen Wirtschaft zur wichtigsten Währung. Gleichzeitig steigen Kosten, Komplexität und Bedrohungen für die Datensicherung. Ein effizienter Schutz der Daten tut Not, unabhängig davon soll der Nutz- und Mehrwert dieser „Assets" als Active Archive voll ausgeschöpft werden.

Das Backup hat sich zu einer existentiellen Anforderung für Unternehmen in der digitalen Transformation und angesichts der bekannten Cyber-Bedrohungen entwickelt. Doch wie sieht die Zukunft des Backups aus? Diese und weitere Fragen werden im eBook „Storage: What`s new?" beantwortet.

Weitere Artikel aus dem eBook

- Storage-Strategie: Der richtige Mix macht`s
- PPR: Prevention, Protection & Recovery
- Zukunftssichere Speicherinfrastrukturen
- Always on: Unveränderbare Snapshots

DMS, ECM UND EIM

BEGRIFFLICHKEITEN IM ECM-UMFELD

Akronyme haben Konjunktur in der IT. DMS, ECM und EIM sind ein gutes Beispiel dafür. Viele Unternehmen verwenden die Begrifflichkeiten Dokumentenmanagement-System (DMS), Enterprise-Content-Management-System (ECM) und Enterprise-Information-Management-System (EIM) häufig als Synonyme.

Die Systemintegration ist eines der zentralen Themen bei der Einführung neuer Software. So unterschiedlich die verschiedenen DMS-Anwendungen und Einsatzfelder auch sind: Es gibt kein Projekt, in dem nicht die Anforderung zur Integration der DMS-Anwendung in andere Anwendungssoftware besteht. Warum also das Rad neu erfinden und nicht auf ein Vorgehensmodell setzen?

Silos aufbrechen, 360 Grad Sicht auf alle Dokumente, verbesserte Workflows, Wiederverwendung von Informationen, Beseitigung von Redundanz, Zugriffsrechte steuern, keine Datenverluste und compliant: Das sind die Highlights von Content-Management-Lösungen der nächsten Generation.

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

DIGITALE TRANSFORMATION

MEHR ERFOLG DURCH AGILERE PROZESSE

Damit Unternehmen weiterhin erfolgreich bleiben, benötigen sie agilere, digitale Prozesse. Nur dann können sie mit den immer schnelleren Veränderungen mithalten. Mithilfe dieser vier Schritte gelingt die digitale Transformation.

Ob Klimaschutz, unterbrochene Lieferketten, Inflation, Pandemie oder Fachkräftemangel: Unternehmen stehen vor immer neuen Herausforderungen. Entsprechend müssen sie schnell darauf reagieren und die richtigen Antworten finden.

Dazu benötigen sie agilere Abläufe, die sich mit Hilfe einer umfassenden digitalen Transformation erreichen lassen. Damit erschließen sie nicht nur Effizienzpotenziale, sondern meistern auch in Krisenzeiten die Herausforderungen für ihre Wettbewerbs- und Zukunftsfähigkeit.

In vier Schritten zur digitalen Transformation

Der Weg von der Theorie in die Praxis ist nicht immer leicht. So bringen manche Initiativen leider nicht den gewünschten Erfolg. Eine der großen Herausforderungen ist, die Digitalisierung mit geeigneten Organisationsstrukturen und Kundenangeboten zu begleiten. Erfahrungsgemäß kommen dabei vier Elemente in häufiger Regelmäßigkeit immer wieder auf:

1. Strategie entwickeln:
Zunächst sollten Unternehmen ermitteln, welche konkreten Themen für sie höchste Priorität besitzen. Das kann zum Beispiel mehr Resilienz oder Agilität in den Bereichen Lieferketten, Rohstoffversorgung oder Ressourcen sein. Zu den möglichen Lösungen gehören dann digitales Supply Chain Management oder Enterprise Ressource Planning.

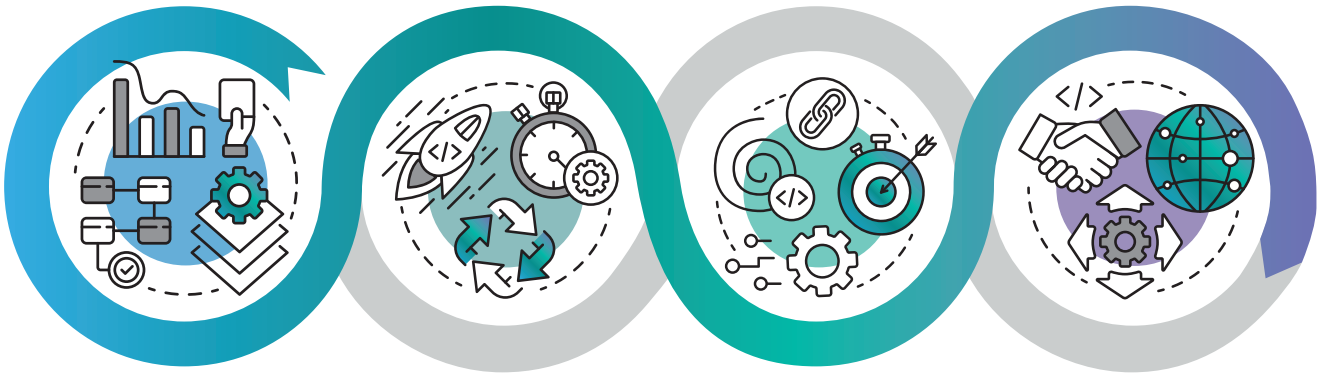
2. Organisation transformieren:
Nach der Entwicklung der Strategie gilt es, konkrete Ziele für den Umbau der Organisation festzulegen. Dazu können flache Hierarchien, schnelle Feedbackschleifen und schlanke Freigabeprozesse zählen, aber auch Zusammenschlüsse (M&A) oder Ausgliederungen (Carve-Out) innerhalb des Unternehmens, sowie auch in und mit anderen Unternehmen.

3. Arbeit transformieren:
Sowohl Arbeits- als auch Führungskräfte benötigen fachliche Begleitung und Unterstützung bei der digitalen Transformation. Geeignete Ansätze für Employee Experience unterstützen Mitarbeitende bei der Umstellung. Lösungen für Citizen Development ermöglichen das eigenständige Digitalisieren und Automatisieren von Prozessen. Mit Hilfe von Leadership Business Transformation werden Führungskräfte befähigt, mit diesem Thema umzugehen. Bei den entsprechenden Ansätzen für New Work sind insbesondere die Mitarbeitenden zu berücksichtigen, die nicht im Büro arbeiten.

4. Kundenerlebnis transformieren:
Unternehmen dürfen nicht bei der Innensicht bleiben, sondern müssen auch die Auswirkungen der digitalen Transformation auf die Kunden berücksichtigen. So sollten sie ermitteln, wie sich die Bedürfnisse von Kundinnen und Kunden aktuell verändern. Die aktuellen Erwartungen der Kundschaft sind über eine moderne Customer Journey zu erfüllen. Das reicht bis zur Veränderung der angebotenen Produkte und Services. Die Neuerungen müssen dann gegenüber den Kunden adressiert und verargumentiert werden.

Damit diese vier Schritte gelingen, ist Erfahrung unabdingbar. Zusätzlich sollte der Weg zur digitalen Transformation fortlaufend geprüft und optimiert werden. Dies erfordert ein umfassendes Projektmanagement, um unter den gegebenen Bedingungen die richtigen Lösungen auszuwählen. Gemeinsam mit einem versierten Partner lässt sich die digitale Transformation agil und strategisch zielführend vorantreiben, bis sie in den konkreten Geschäftsprozessen greift.

Christoph Gudernatsch
www.campana-schott.com



INNOVATION MIT EMPATHIE VORANTREIBEN

DESIGN THINKING ALS MOTOR FÜR LOW-CODE-ANWENDUNGEN

Wie viele Apps nutzen wir heutzutage regelmäßig für die Arbeit? Ob für Zeiterfassung, Termine, E-Mails oder Scannen - Die meisten von uns nutzen täglich mindestens eine mobile oder Desktop-App. Das wichtigste dabei ist, dass diese Apps benutzerfreundlich und intuitiv sind. Solche Apps zu erstellen geht zum Glück immer einfacher. Doch bevor sie in Betrieb genommen werden, durchlaufen sie verschiedene Phasen. Die wohl wichtigste Phase für den Erfolg jeder neuen technologischen Lösung ist das Design Thinking. Während sich die besten Ideen wie ein roter Faden durch alle vier Phasen des kreativen Prozesses ziehen - Problemdefinition, Ideenfindung, Prototyping und Testen - gibt es einen Pfeiler des Design Thinking, der die gesamte Schöpfung zusammenhält: die Empathie. Aus diesem Grund gilt Design Thinking, also der Prozess für die kreative Problemlösung, als eines der Kernelemente der digitalen Transformation für moderne Unternehmen. Eine menschenorien-

tierte Designstrategie erhöht nachweislich die Erfolgsquote eines Unternehmens in Sachen Innovation.

Mit Empathie auf die Probleme schauen

Gerade bei vielen alten Systemen in den deutschen Unternehmen (zum Beispiel auf SAP basierend) ist es umso wichtiger, dass das Endziel für neue Lösungen immer die Benutzererfahrung (UX) darstellt. Design Thinking fokussiert sich deshalb auf Empathie als Grundvoraussetzung und fördert benutzerfreundliches Design für neue Produkte. Das bedeutet, dass technische Lösungen als Antwort auf die genauen Bedürfnisse eines Unternehmens entwickelt werden und nicht nach den Launen oder Wünschen eines Entwicklers oder des IT-Teams. Die Verknüpfung von Design Thinking mit dem Ziel, die Nutzererfahrung zu verbessern, bildet daher die Grundlage für Unternehmen, die im Jahr 2022 die Grenzen des Technologiedesigns verschieben wollen.

LOW-CODE PLATTFORMEN ERLEICHTERN DAS DESIGN THINKING, INDEM SIE ES ÜBERFLÜSSIG MACHEN, SICH MIT MEHREREN PRODUKTEN AUSEINANDERSETZEN ZU MÜSSEN, UM EINE EINZIGE LÖSUNG ZU ERSTELLEN.

Andreas Grydeland Sulejewski,
CEO, Neptune Software,
www.neptune-software.com/de/

Vom kleinsten Datenproblem bis hin zum größten Logistikunternehmen funktionieren technische Lösungen am erfolgreichsten, wenn sie auf dem Verständnis menschlicher Bedürfnisse und dem Wunsch basieren, einen entsprechenden Missstand zu beheben. Um Unternehmen auf eine einzigartige Reise der Transformation durch technologisches Design mitzunehmen, ist es entscheidend, Zeit mit den Teams zu verbringen, um die individuellen Bedürfnisse und die genauen Probleme zu verstehen, die es zu lösen gilt. Es ist unglaublich schwierig, die Nuancen der Bedürfnisse aus der Ferne zu erkennen; man muss in unmittelbarer Nähe sein, um ein empathisches Design zu kultivieren.

Bei allen Digitalisierungsprojekten und insbesondere beim Low-Code-Ansatz braucht es daher das richtige Einfühlungsvermögen, um die Teams sowohl auf der operativen als auch auf der technischen Seite des Prozesses zu begleiten. Wenn Firmen zu uns kommen und eine Technologie suchen, die es Ihnen ermöglicht Anlagen, Maschinen oder HR prozesseffizienter abzubilden, müssen wir das Problem aus deren Perspektive betrachten. Ein Besuch am Standort und Gespräche mit den Mitarbeitern bringen oft wichtige Einblicke in das Projekt, die es Low-Code Anbieter ermöglichen sich auf die spezifischen Problembereiche zu konzentrieren.

Dank Low-Code designorientierter denken

Unabhängig davon, ob sie intern an der Entwicklung von Lösungen arbeiten oder mit externen Parteien zusammenarbeiten, müssen IT-Experten Applikationen nicht mehr von null programmieren. Tools wie Low-Code-Entwicklungsplattformen geben Mitarbeitern die richtigen Werkzeuge an die Hand, um in kürzester Zeit die benötigten Anwendungen für ihre IT-Landschaft zu erstellen - unabhängig davon, ob sie wenig oder kaum Programmierkenntnisse haben oder ein Experte sind. Ziel ist es, Benutzer in die Lage zu versetzen, den Erfolg in ihren eigenen Branchen durch eine Software voranzutreiben, die Innovationen fördert.

Low-Code Plattformen erleichtern das Design Thinking, indem sie es überflüssig machen, sich mit mehreren Produkten auseinandersetzen zu müssen, um eine einzige Lösung zu erstellen. IT-Fachleute sparen dadurch Zeit und Energie und Teams werden mit Tools ausgestattet, die ihre Fähigkeiten erweitern und sogar aufwändige Prozesse bekämpfen, die mit der Arbeit auf mehreren Plattformen einhergeht. Mit Plattformen wie beispielsweise Neptune DXP & Co können Ideen schnell und effizient in Prototypen verwandelt, getestet, angepasst und schließlich zum Endprodukt werden.

Unabhängig davon, für welchen Low-Code Anbieter man sich entscheidet, besteht der Schlüssel zur Innovationsstrategie 2022 darin, sich auf die Entwicklung von Lösungen zu konzentrieren, die den Menschen in den Mittelpunkt stellen.

Der Entwicklungsprozess von Applikationen und neuen Technologien sollte immer mit Empathie beginnen und enden.

Andreas Grydeland Sulejewski

LANGFRISTIGE DATENAUFBEWAHRUNG

AKTIVES ARCHIV ALS ALTERNATIVE ZU TAPE UND CLOUD

DIE STÄRKEN DES SWARM-OBJEKTSPEICHERS LIEGEN IN SEINER EXTREMEN SKALIERBARKEIT, VERGLEICHSWEISE GÜNSTIGEN KOSTEN UND UMFANGREICHEN MECHANISMEN ZUM SCHUTZ VON DATEN.

Alfons Michels, Senior Product Marketing Manager, DataCore, www.datacore.com

Angesichts ihres astronomischen Wachstums müssen Daten je nach Anforderung auf entsprechendem Speicher abgelegt werden. Auch um teuren Primärspeicher zu entlasten, sind preiswertere Archive für kaum genutzte Daten unabdingbar. Heute werden diese „kalten" Daten oft auf Cloud oder Tape ausgelagert. Doch was geschieht mit Daten, auf die selten, aber doch ab und zu und dann schnell zugegriffen werden soll? Aktive Archive auf Basis von Objektspeicher bieten hier eine Alternative.

Die Herausforderung besteht darin: Der Lebenszyklus für mehr als 80 Prozent der Daten beträgt nur wenige Minuten, zum Beispiel von der Erstellung bis zum Versand per E-Mail. Das bedeutet, diese Daten liegen auf Primärspeicher, obwohl sie qualifiziert wären, auf einem günstigeren Archivmedium abgelegt zu werden. Das Dilemma für IT-Verantwortliche: Sie dürfen nicht gelöscht werden, eine Auslagerung ist unerwünscht, da sie bei Bedarf direkt zugreifbar sein sollen. Kaum sind die Daten weg, wird danach gefragt!

Was ist ein aktives Archiv?

Neben dem Backup von Daten, auf das in der Regel nur im Notfall zugegriffen wird, steigt gleichzeitig der Bedarf, ältere Daten ständig zugreifbar zu haben. Dabei kommt es vorrangig darauf an, dass dies kostengünstiger ist als mit dem 'normalen' Speicher, die Daten aber trotzdem geschützt sind und natürlich direkt auf sie zugegriffen werden kann. Oftmals spricht man in dem Zusammenhang von einem aktiven Archiv.

Cloud und Tape sind zwar mögliche Optionen, bringen jedoch diverse Herausforderungen in Bezug auf Kosten, Sicherheit und Performance mit sich. Diese Probleme lassen sich mit einem aktiven Archiv lösen. Diese sind speziell für die sichere, kosteneffiziente und langfristige Datenaufbewahrung konzipiert, und bieten als lokale Lösung gleichzeitig einen schnellen Zugriff.

Vergleich zwischen aktivem Archiv und herkömmlichem Backup

ARCHIV	BACKUP
Daten werden verdrängt	Zusätzliche Kopie
Daten einmalig vorhanden	Daten mehrfach vorhanden
Ad hoc Zugriff	Zugriff nur im Fehlerfall
Archiv System regelt Zugriff	Backup System regelt Zugriff
Zugriff für viele	Zugriff für wenige
Medienbruch unerwünscht	Medienbruch erwünscht
Offline Ablage unerwünscht	Offline Ablage erwünscht

Aktive Archive kommen also dort zum Einsatz, wo die Datenmengen Kapazität und Kosten der primären Speicherinfrastruktur übersteigen, gleichzeitig aber ein verteilter Zugriff ermöglicht werden soll. Ein bewährter Ansatz dazu sind softwaredefinierte Objektspeicherlösung als On-Premises-Archiv. Sie können schrittweise als sekundärer Langzeitspeicher von einigen TB bis hin zu Exabyte (EB)-Bereich ausgebaut werden. Und mit der richtigen Integration müssen weder Dateisysteme umstrukturiert oder Zugriffsmuster geändert werden.

Aktives Archiv mit DataCore Swarm

Swarm ist Teil des softwaredefinierten Portfolios von DataCore zum Aufbau von Block-, Datei- und Objektspeicherlösungen. Swarm erlaubt die Festplatten und SSDs in x86-Servern beliebiger Hersteller in leistungsfähigen Objektspeicher zu verwandeln.

Bei der Nutzung als aktives Archiv bietet Swarm gegenüber anderen Archivierungsmethoden wie etwa der Speicherung in der Public Cloud oder auf Band signifikante Vorteile. Durch die Speicherung der Daten On-Premises werden Bedenken hinsichtlich der Datenhoheit und lange Netzwerklatenzzeiten ausgeräumt. Die monatlichen Kosten sind vorhersehbar, sodass unliebsame Überraschungen bei steigender Nutzung des Cloud-Speichers vermieden werden. Im Gegensatz zu Bändern, die nicht ständig überprüft werden können und deren Wiederherstellung schwie-

rig sein kann, lassen sich auf Festplatten lokal archivierte Dateien schnell und zuverlässig wiederherstellen.

Leistungsmerkmale von DataCore Swarm sind:

- Einfaches Management, automatisierte Aufgaben: 1 Admin verwaltet in Teilzeit mehr als 50 PB und tausende Mandanten
- 90 Sekunden um zusätzliche Kapazität oder Performance hinzuzufügen
- Kein darunterliegendes Betriebssystem oder Datenbank zu verwalten
- 95 Prozent der Speicherkapazität ist ausschließlich für Daten
- Beliebiges mischen der Hardware (CPU, RAM, HDD, SSD…)
- Zusätzliche Verteidigungslinie gegen Ransomware: optionale Immutability macht Dateien unveränderbar

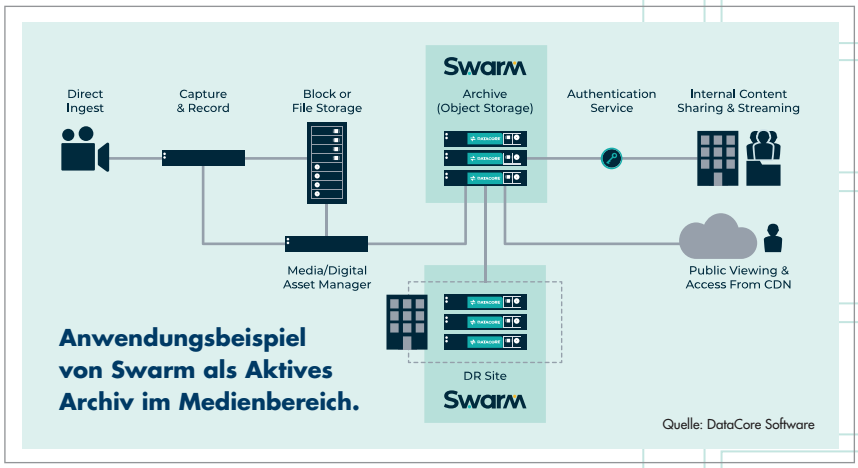
Ein weiterer charmanter Aspekt an Swarm ist, dass er zu allen gängigen Datenauslagerungstools kompatibel ist und so eine transparente Verbindung vom günstigen Objektspeicher zum hoch-performanten, aber auch teureren Primärspeicher hergestellt werden kann. Ein solches Tool ist DataCore FileFly. Mit FileFly werden die eigentlichen Daten in das aktive Archiv anhand von frei definierbaren Regeln verschoben. Am vorherigen Speicherort verbleibt dann nur ein Archiv-Zeiger, die Nutzer können wie auf Ihre Daten zugreifen. Gleichzeitig werden weniger Backupspeicher und -zeit benötigt, da nur der Zeiger und nicht die komplette Datei gesichert werden muss. Die saubere Trennung unterschiedlicher Anwendungsfälle von Swarm ist durch seine Mehrmandantenfähigkeit sichergestellt.

Use Case: Mediendaten im aktiven Archiv

Mediendateien (Videos, Audioaufzeichnungen, Multimedia-Bilder) sind ein gutes Beispiel für Daten, die selten geändert, oft geteilt und zu einem späteren Zeitpunkt gern aufgerufen werden. Sie sind ein idealer Kandidat für die aktive Archivierung. Medien- und Unterhaltungsunternehmen verwalten dabei enorme Mengen an Dateien. Daher sollten sie in einem möglichst günstigen Archiv abgelegt werden, das aber einen direkten Zugriff auf die Dateien ermöglicht. Praktischerweise sollte dabei die Archivierung in die Videoerstellung, Produktion und Bereitstellung integriert sein.

Im Resultat wird der primäre Speicher durch die aktive Archivierung von Medien- und anderen Dateien auf preiswertere Objektspeicher entlastet. Gleichzeitig bleiben die Dateien für beispielsweise Videoproduktionsabläufe oder Medienmanagementsysteme zugänglich und integriert.

Zugang, Suche oder Abruf von Dateien aus dem Archiv erfolgt über ein webbasiertes Inhaltsportal (Zugriff über HTTP/S3).



Die Vorteile im Überblick:

- Mehr Speicherplatz im primären Speicher durch die Archivierung von Mediendateien auf preiswerterem Objektspeicher
- Integration in Videoproduktionsabläufe und Medienmanagementsysteme
- Einfacher Zugang, einfache Suche und einfaches Abrufen von Dateien aus dem Archiv über ein webbasiertes Inhaltsportal (Zugriff über HTTP/S3)
- Konfigurierbare rollenbasierte Zugriffskontrolle für Nutzer gemäß festgelegter Sicherheitsrichtlinien
- Streamen von Videos aus dem Archiv, ohne sie in einen lokalen Ordner herunterzuladen
- Einfaches Bearbeiten und Ausschneiden von Filmclips aus großen Videodateien und Freigabe an andere Benutzer

Resümee: Integriertes Archiv mit Primärspeicher-Eigenschaften

Die Stärken des Swarm-Objektspeichers liegen in seiner extremen Skalierbarkeit, vergleichsweise günstigen Kosten und umfangreichen Mechanismen zum Schutz von Daten. Typischerweise wird er für Daten verwendet, die keinen regelmäßigen Änderungen unterliegen und ermöglicht deren verteilte Nutzung. Somit ist er hervorragend als aktives Archiv geeignet.

Lokaler Objektspeicher als Basis für ein aktives Archiv lohnt sich ab etwa 100 Terabyte und kann bis zu hunderten Petabyte skalieren. Ob Sicherungsdaten, Mediendateien, inaktive/kalte Daten aus dem Primärspeicher, Auswertungsdaten oder Ähnliches, der softwaredefinierte Objektspeicher gewährleistet den lückenlosen Datenschutz und minimiert das Risiko von Datenverlusten, Ausfallzeiten und Unterbrechungen.

Alfons Michels

VERTRAUEN IN CYBERSICHERHEIT

MAXIMALE TRANSPARENZ UND KONTINUIERLICHE PROZESSÜBERPRÜFUNG

Sicherheitsprodukte greifen tief in das Betriebssystem ein. Deshalb müssen Anwender den Produkten und Anbietern vertrauen. Über nachprüfbare Bewertungskriterien für eine sichere, vertrauenswürdige Digitalisierung sprach it management mit Christian Milde, Geschäftsführer Central Europe bei Kaspersky.

it management: *Herr Milde, Cybersicherheit gewinnt, gerade aufgrund der zunehmenden Digitalisierung, immer mehr an Bedeutung. Welche Kriterien muss digitale Sicherheitstechnologie Ihrer Meinung nach erfüllen, um die IT-Infrastruktur und sensiblen Daten von Unternehmen, Organisationen und Privatanwendern zu schützen?*

Christian Milde: Hierbei geht es insbesondere um die Bereiche Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und Datenschutz. Diese Parameter müssen uneingeschränkt erfüllt sein, um ein Maximum an Sicherheit zu gewährleisten. Hierbei legen wir Wert auf wiederkehrende Auditierungen nach internationalen Standards. 2019 wurden die Entwicklungs- und Freigabeprozesse der Kaspersky-AV-Datenbanken nach den Richtlinien des vom American Institute of Certified Public Accounts (AICPA) [1] entwickelten Standards SOC 2 erstmals erfolgreich auditiert. Dabei analysieren die Prüfer die Beschreibungen und Dokumentationen, bewerten diese und evaluieren die Systemkontrollen im Produktivbetrieb. Dieser Auditierungsprozess wurde dieses Jahr von einer der vier großen Wirtschaftsprüfungsgesellschaften wiederholt. Auditierungen und Zertifizierungen nach anerkannten Industriestandards leisten einen großen Beitrag zur Steigerung von Vertrauen und Sicherheit. Kunden und Partner erhalten wichtige Informationen und Argumente für eine Kaufentscheidung.

it management: *Wie kann man sich einen derartigen Audit-Prozess im Detail vorstellen?*

Christian Milde: Zunächst wurden die für die genannten Prozesse verantwortlichen Führungskräfte, firmeninternen Prüfteams sowie unmittelbar beteiligten Mitarbeiter befragt. Zudem haben die Prüfer alle Unterlagen, Aufzeichnungen und Dokumentationen geprüft. Hierzu zählen Standardreports, wie im System konfigurierte, parametergesteuerte Berichte, die von unseren Systemen generiert werden. Weitere Beispiele sind benutzerdefinierte Berichte, die nicht zum Standard der Anwendung gehören.

EIN SCHLÜSSEL ZU MEHR SICHERHEIT LIEGT DARIN, WIE DER ZUGRIFF AUF DATEN, SOFTWARE, FUNKTIONEN UND ANDERE GESCHÜTZTE INFORMATIONSBESTÄNDE AUTORISIERT, GEÄNDERT ODER AUFGEHOBEN WIRD.

Christian Milde,
Geschäftsführer Central Europe, Kaspersky,
www.kaspersky.de

it management: *Bei Zertifizierungsprozessen geht es häufig um gemeinsam anzuwendende Kriterien, damit ein Standard gesetzt werden kann. Welche Merkmale wurden im Laufe des Audits bewertet?*

Christian Milde: Es ging hierbei hauptsächlich um den Systembetrieb, logische und physische Zugriffskontrollen, das Kontrollumfeld und die Kontrolltätigkeiten, sowie um Kommunikation und Information, Change Management, die Risikobewertung und die Risikominimierung.

it management: *Könnten Sie auf einzelne Punkte etwas näher eingehen?*

Christian Milde: Kaspersky setzt modernste Erkennungs- und Kontrollverfahren ein, um Änderungen an Konfigurationen zu identifizieren, die zum versehentlichen oder bewussten Einbau von Schwachstellen führen können. Dabei überwacht Kaspersky die Systemkomponenten und den Betrieb dieser Komponenten auf Anomalien, die auf schädliche Handlungen, Systemstörungen und Fehler hinweisen, die die Fähigkeit des Unternehmens beeinträchtigen könnten, die Schutzziele zu gewährleisten. Jede Änderung am Quellcode durchläuft ein dezidiertes Prüfverfahren, um ihre Integrität und Sicherheit zu bestätigen. Bei den Review-Prozessen zur Erstellung von Updates sind Kaspersky-Experten außerhalb Russlands immer mit einbezogen – bei-

spielsweise Kaspersky-Teams in den USA und Kanada.

Ein weiteres Beispiel ist die Risikominimierung: Kaspersky identifiziert, entwickelt und setzt alle erforderlichen Risikominimierungsmaßnahmen um, die sich aus potenziellen Geschäftsunterbrechungen ergeben können. Dabei werden kontinuierlich alle Risiken mit Blick auf Zulieferer sowie die gesamte Supply-Chain bewertet. Genau diese Prozesse hat der Auditor geprüft.

it management: *Ist eine strikte Aufgabentrennung innerhalb des Unternehmens der Schlüssel zu mehr Sicherheit?*

Christian Milde: Eindeutig ja. Ein Schlüssel zu mehr Sicherheit liegt darin, wie der Zugriff auf Daten, Software, Funktionen und andere geschützte Informationsbestände auf der Grundlage von Rollen, Zuständigkeiten oder des Systemdesigns autorisiert, geändert oder aufgehoben wird. Kaspersky verfolgt dabei stringent die Konzepte der geringsten Privilegien und der Aufgabentrennung, um höchste Schutzziele zu erreichen.

it management: *IT-Sicherheit beruht auf Vertrauen – und Vertrauen auf Transparenz. Welche Maßnahmen ergreift Kaspersky neben dem besprochenen Audit zusätzlich?*

Christian Milde: Wir haben in den vergangenen Jahren viele Anstrengungen unternommen, um technologische Transparenz und die Vertrauenswürdigkeit Kasperskys zu steigern. Die Verlagerung der Verarbeitung und Speicherung von Bedrohungsdaten in Rechenzentren in die Schweiz und die Eröffnung globaler Transparenzzentren, in denen der Quellcode unseres Unternehmens, die Software-Updates und die Regeln zur Bedrohungserkennung von vertrauenswürdigen Partnern, Kunden und Regierungsbehörden eingesehen werden können, sind für uns ein Grundpfeiler und ein Zeichen unserer Verpflichtung für mehr Transparenz. Das machen wir übrigens als erster Anbieter der Branche schon seit 2018 und haben damit ein Benchmark gesetzt! Die Erneuerung des SOC-2-Typ-1-Berichts ist Teil dieser Globalen Transparenzinitiative und zeigt unser kontinuierliches Engagement für Rechenschaftspflicht. Anfang dieses Jahres erneuerten wir zudem auch die Zertifizierung nach ISO 27001:2013, einem international anerkannten Sicherheitsstandard, der von der unabhängigen Zertifizierungsstelle TÜV AUSTRIA ausgestellt wird.

it management: *Das BSI hat vor dem Hintergrund des Kriegs in der Ukraine vor dem Einsatz von Kaspersky-Virenschutzprodukten gewarnt. Können Sie dazu Stellung beziehen?*

Christian Milde: Das BSI hat aus geopolitischen Gründen gewarnt, ohne die Kaspersky-Produkte und unsere Schutzmechanismen vor unberechtigtem Zugriff technisch und organisatorisch zu bewerten. Mit den jetzt erneut zertifizierten Sicherheitsstandards und organisatorischen Maßnahmen durch das SOC 2-Audit können Partner und Kunden weiterhin auf die Qualität und Integrität von Kaspersky und der Produkte und Services vertrauen. Weitere eindeutige und nachprüfbare Bewertungskriterien finden Sie auf unserer Website kas.pr/vertrauen.

it management: *Herr Milde, wir danken für dieses Gespräch.*

[1] Quelle: https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative

DIE WICHTIGSTEN AUSWAHLKRITERIEN

E-MAIL-SICHERHEIT

UNTERNEHMEN SETZEN AUF LÖSUNG AUS DER CLOUD

Zur Sicherung einer verlässlichen E-Mail-Kommunikation nutzen Unternehmen und andere Organisationen vermehrt Cloud Services. Dabei sind die Möglichkeiten zur individuellen Konfiguration und die Support-Qualität die entscheidenden Auswahlkriterien. Das ist das Ergebnis einer aktuellen Focus-Point-Umfrage des unabhängigen Analystenhauses techconsult im Auftrag von Net at Work.

Relevanz von E-Mail-Sicherheit

9 von 10 der befragten Organisationen räumen E-Mail-Sicherheit eine überdurchschnittlich hohe Bedeutung ein. Dabei gibt es keine signifikanten Unterschiede mit Blick auf die Größe der Organisation. Als Anforderungen an entsprechende Lösungen ergaben sich drei große Leistungsbereiche als besonders wichtig: Erstens der Schutz vor Malware, Phishing und Spam. Zweitens, die Sicherung einer vertraulichen Kommunikation durch Signatur und Verschlüsselung und drittens die sichere Übertragung großer Dateien.

Eigeneinschätzung schwierig

In Summe sehen rund 62 Prozent der Befragten konkreten Handlungsbedarf bei der E-Mail-Sicherheit. Davon haben mehr als 12 Prozent bereits konkrete Lücken mit Blick auf aktuelle Bedrohungen erkannt und gelangen zu der Einschätzung, dass sie etwas tun müssen. Weitere rund 22 Prozent sind sich dessen bewusst, dass sie aufgrund von Personalmangel nicht dazu in der Lage sind, die Konfiguration regelmäßig zu prüfen und anzupassen, und schätzen ihre Situation daher als nicht sicher ein. Jedes vierte Unternehmen kann die Qualität der eigenen E-Mail-Sicherheit aufgrund von fehlendem Know-how und Personal nicht beurteilen und hält einen erheblichen Handlungsbedarf für wahrscheinlich.

Vertrauen auf externes Know-how

Getrieben vom Mangel an geeigneten internen Kräften würden der Umfrage zufolge fast zwei von drei der befragten Unternehmen ihre E-Mail-Sicherheit in externe Hände legen. Dabei präferieren knapp 24 Prozent die Auslagerung als Managed Service an einen lokalen Dienstleister und mehr als 40 Prozent die Nutzung eines Cloud Security Service für E-Mail-Sicherheit. Interessanterweise liegen der öffentliche Sektor, der Handel und die Finanzindustrie in ihrer Präferenz für Cloud Services signifikant über dem Durchschnitt aller Branchen. Dabei ist die Nutzung eines nationalen Rechenzentrums für rund jeden Dritten ein entscheidendes Kriterium.

www.netatwork.de

MONITORING

UMFASSENDE PERFORMANCE- UND NUTZUNGSANALYSE LEICHT GEMACHT

Eine weitreichende Neuerung stellt ams seinen Kunden mit der im April 2022 erschienen neuesten Version seines ERP-Systems zur Verfügung: Mit ams.Monitoring ist es erstmalig möglich, im Rahmen einer umfassenden Leistungs- und Benutzungsanalyse sämtliche Aktivitäten und Events in ams.erp über beliebige Zeiträume hinweg aufzuzeichnen, um die Ursachen für etwaige Performance-Defizite schnell ausfindig zu machen und zu beseitigen. Die neue Funktionalität ist Teil des Standardpakets und überzeugt durch einfache und unkomplizierte Bedienbarkeit.

In Zukunft wird die Anzahl der Fälle, in denen der Support mit nicht näher spezifizierbaren Performance-Problemen von den Nutzern kontaktiert wird, drastisch abnehmen. Sämtliche Interaktionen mit dem ERP-Programm können aufgezeichnet und bei Bedarf zusätzlich mit SQL-Profiling-Informationen angereichert werden. Diese granularen Informationen ermöglichen den Kunden eine zielgerichtete Problemanalyse. Dank übersichtlicher Auswertungen über die Monitoring-Dashboards werden sowohl aktuelle als auch vergangene Leistungsspitzen angezeigt und stehen zur Analyse bereit.

IN ZUKUNFT WIRD DIE ANZAHL DER FÄLLE, IN DENEN DER SUPPORT MIT NICHT NÄHER SPEZIFIZIERBAREN PERFORMANCE-PROBLEMEN VON DEN NUTZERN KONTAKTIERT WIRD, DRASTISCH ABNEHMEN.

Hans-Werner Schmidt,
Softwareentwickler, ams.Solution AG,
www.ams-erp.com

Deutlich schnellere Problemlösung

Die Lösung wurde explizit so konzipiert, dass Kunden selbst die Möglichkeit haben, etwaige Schwachstellen und Einflussfaktoren im und um das System herum zu ermitteln. Sollte dies zu keinem zufriedenstellenden Ergebnis führen, können sie selbstverständlich weiterhin Kontakt zum ams-Support aufnehmen. Dieser kann auf Basis der umfangreichen und präzisen Datenlage nun natürlich viel effektiver als bisher Lösungen erarbeiten. Auf Wunsch können die Kunden diese Informationen dem Hersteller zur Verfügung stellen und somit aktiv dazu beitragen, die ERP-Software nachhaltig zu verbessern.

Besonders hilfreich werden die Analyse-Möglichkeiten im Zusammenspiel mit der ams.Testautomation bei Releasewechseln sein. Bei aktiviertem Monitoring der Testautomation gewinnt man schnell exakte Hinweise darauf, ob und wo das System Veränderungen im Vergleich zum Vorgänger-Release zeigt. Dies wird der Qualität der Lösung einen zusätzlichen deutlichen Schub geben.

Das Monitoring-Dashboard erlaubt es, ausgehend von generellen Informationen zur Systemauslastung in immer tiefere Detailebenen einzutauchen. Neben der Möglichkeit des Rückblicks auf die vergangenen Kalenderwochen lässt sich in der nächsten Stufe die Systemarbeit der aktuellen Kalenderwoche genauer beleuchten. Beim Einzoomen auf die Tagesauflösung erkennt man schließlich sehr präzise, welche einzelnen Ereignisse oder welche speziellen Dienste die größten Lastspitzen verursachten.

Tests erfolgreich verlaufen

Das Tool wurde in der Entwicklungsphase bei mehreren Kunden getestet. Die Resonanz fiel dabei durchweg positiv aus. Bei einem der größten ams-Kunden konnten viele tausend Ereignisse aufzeichnet werden. Aus diesen Daten ließen sich eine Vielzahl von Erkenntnissen gewinnen, ohne dass die zusätzliche Analyse negativen Auswirkungen auf den laufenden Betrieb gehabt hätte.

Die Analysedaten werden darüber hinaus helfen, den Weg in Richtung Predictive Maintenance zu ebnen. Dann nämlich lassen sich recht konkrete Vorhersagen dahingehend treffen, wann ein ams.erp-System bei gleichbleibender Nutzung Leistungsschwierigkeiten bekommen wird. Mittels des Vergleichs mit Kunden mit ähnlichen Voraussetzungen kann der Hersteller Vorschläge zur Verringerung der Serverlast machen.

Insgesamt wird die Lösung dazu beitragen, ein viel detaillierteres Bild über die ERP-Nutzung zu gewinnen und zudem ein besseres Verständnis für die Anforderungen der Kunden zu erlangen.Support-Anfragen können zielgerichtet bearbeitet werden, weil die Gründe für Performance-Engpässe leichter ersichtlich sind.

Hans-Werner Schmidt

HYBRID WORK

KEINE SINNKRISE FÜR DAS BÜRO

Nach zwei Jahren der Einschnitte und weitreichenden Veränderungen, setzt sich der Wandel in der Arbeitswelt stetig fort. Zurecht erwarten Beschäftigte, dass sich ihr Arbeitgeber an die Spitze dieses Wandels setzt. Jedoch zeigt eine aktuelle Studie von Ricoh, dass viele Arbeitgeber in Deutschland die Möglichkeiten zur Modernisierung und digitalen Transformation von Büroräumen im Rahmen ihrer Hybrid-Working-Strategien zu wenig nutzen. Dies kann nicht nur negative Auswirkungen auf die Produktivität am Arbeitsplatz haben, sondern birgt für Unternehmen auch die Gefahr Toptalente zu verlieren, da diese eher zu Arbeitgebern wechseln, die flexiblere Arbeitsmodelle erfolgreich implementiert haben. Oft erschweren unzureichende Technologien kollaborativ ausgerichtete Arbeitsumgebungen und die Verwirklichung von flexibleren Arbeitsformen – aber auch entsprechende Richtlinien sind vielerorts Mangelware.

Dies spiegelt auch die Ricoh-Umfrage wider: Nur 16 Prozent der Befragten gab an, dass ihr Arbeitsplatz über Richtlinien für hybrides Arbeiten verfügt. Auch ein Ausbau der Kommunikationsausstattung in Besprechungsräumen zur Unterstützung hybrider Arbeitsformen bestätigte weniger als die Hälfte der Befragten (47 %). Für Arbeitgeber ist es jedoch von entscheidender Bedeutung, die richtigen Tools für die Zusammenarbeit zur Verfügung zu stellen. Denn Hybrides Arbeiten ist für Unternehmen eine Chance, sowohl die Arbeitserfahrung als auch die Produktivität der Beschäftigten zu verbessern. Bei der Ausgestaltung des entsprechenden Konzepts sollten Unternehmen die geschäftlichen Anforderungen mit den Präferenzen der Beschäftigten in Einklang bringen. Das vielerorts bereits gefestigte Vertrauensverhältnis der Unternehmen zu ihren Mitarbeitern zeigt, dass Hybrid Work als Arbeitsmodell der Zukunft funktionieren kann: Mehr als die Hälfte der Befragten sagt, dass das Vertrauen der Führungsebene in ihre Fähigkeit, im Homeoffice motiviert und produktiv zu arbeiten, in den letzten Monaten zugenommen hat.

Standortübergreifende Zusammenarbeit

Die eine Masterlösung zum perfekten Hybrid Work Konzept gibt es nicht – sie unterscheidet sich von Unternehmen zu Unternehmen. Genauso wie der richtige strategische Ansatzpunkt. Individuelle Analysen mit einem erfahrenen Technologiepartner helfen, die Pain Points des Arbeitsalltags zu erkennen und mit maßgeschneiderten Lösungen zu beheben. Moderne, skalierbare Tools, wie beispielsweise Ricoh Meeting Spaces, können Teil dieses individuell anpassbaren Lösungskonzepts sein. Sie helfen nicht nur, Meetingräume zu gestalten und treiben zeitgleich die technologische Weiterentwicklung von Unternehmen weiter voran, sondern fördern auch die idealen Rahmenbedingungen für Hybrid Work. Ob Zuhause oder im Büro – Ziel ist es, dass die Mitarbeiter reibungslos und standortübergreifend zusammenarbeiten können. Damit diese Zusammenarbeit funktioniert, benötigen kollaborative Systeme eine Reihe von technologischen Lösungen, die für professionelle Präsentation und Videokonferenzen zentral und für hybride Arbeitsmethoden essentiell sind, um neue Meeting-Erlebnisse für alle Mitarbeiter zu schaffen.

Auch „Bring your own device" ist vielerorts zum Standard geworden, sodass Systeme mit allen gängigen Geräten kompatibel und flexibel einsetzbar sein müssen. Ricoh Meeting Spaces bietet zahlreiche Lösungen zur Arbeitsplatzoptimierung und versetzt Unternehmen jeder Größe, von der Integration der führenden Videokonferenz-Plattformen, wie beispielsweise Microsoft Teams oder Zoom, über die Nutzung von Ultra-HD-Displays und All-In-One-Kameras mit einer Wiedergabe in 4K-Qualität bis hin zur smarten Audiotechnik, in die Lage, die Digitalisierung ihrer Besprechungsräume weiter

voranzutreiben und so eine zukunftsorientierte, intelligente und standardisierte Arbeitsumgebung zu schaffen.

Das Büro als Sinnbild für technologischen Wandel und Kollaboration

Hybrid Work is here to stay – deshalb sollten Mitarbeiter in einem digitalen Umfeld arbeiten, das sowohl die Arbeit im Büro als auch die Zusammenarbeit mit den Kollegen im Homeoffice erleichtert. Die kontinuierliche technologische Innovation sichert die Zukunftsfähigkeit von Unternehmen. Das Werben um die Toptalente auf dem Arbeitsmarkt beispielsweise birgt viele Herausforderungen. Meetingräume müssen so digitalisiert und standardisiert werden, dass sie flexibel mit den Anforderungen an Unternehmen mitwachsen und gleichzeitig neue Impulse für die Zusammenarbeit setzen können. Auch den Führungskräften kommt jetzt eine bedeutende Rolle zu: Sie müssen zum einen auf die Wünsche und Anregungen der Mitarbeiter eingehen und zum anderen vorleben, wie man sich in einer hybriden Arbeitswelt vernetzt und engagiert. Führungskräfte möchten mit gutem Beispiel vorangehen und im Büro anwesend sein. Mitarbeiter könnten so das Gefühl bekommen, dass ihre Arbeit nur in Präsenz wertgeschätzt wird. Es gilt das Prinzip der Vertrauenskultur, unabhängig von dem Ort, von dem aus die Arbeit verrichtet wird. „Leading Change at Work" bedeutet neben der digitalen Transformation auch einen Wandel in der Meeting-Kultur: Nutzen Sie digitale und physische Räume für die Zusammenarbeit und investieren Sie Energie in beide Seiten der Arbeitserfahrung – ob im Office oder remote.

Ingo Wittrock

HYBRID WORK IS HERE TO STAY – DESHALB SOLLTEN MITARBEITER IN EINEM DIGITALEN UMFELD ARBEITEN, DAS SOWOHL DIE ARBEIT IM BÜRO ALS AUCH DIE ZUSAMMENARBEIT MIT DEN KOLLEGEN IM HOMEOFFICE ERLEICHTERT.

Ingo Wittrock,
Regional Marketing Director
Central Europe und New Work Experte,
Ricoh, www.ricoh.de

FUNKTIONIERENDE UNTERNEHMENSKULTUR

DIE ZUKUNFT DER ARBEITSWELT BAUT AUF VERTRAUEN

Krisen und fortschrittliche Technologien verändern die Art und Weise, wie wir arbeiten, sehr schnell. Arbeitgeber sind gut beraten, sich für Änderungen der Unternehmenskultur offen zu zeigen – denn es geht um mehr als nur Homeoffice und Obstkörbe.

Wir leben in spannenden Zeiten. Der technologische Fortschritt in der IT, dessen Ursprünge bis zu der Erfindung von Mikrochips in den 1950er-Jahren und noch weiter zurückreichen, verändert nicht nur unsere alltäglichen Lebensweisen und das Warenangebot, sondern auch die Arbeitswelt. All diese Transformationen geschehen in einer atemberaubend schnellen Zeitspanne und erhielten besonders im digitalen Sektor durch die Corona-Krise einen zusätzlichen Boom.

DER AUSTAUSCH UND DIE KOMMUNIKATION SIND NICHT NUR BEI ARBEITSBEZOGENEN THEMEN WICHTIG, SONDERN AUCH BEI DER GEMEINSAMEN ORGANISATION VON ARBEITSSTRUKTUREN UND DER FRAGE, WIE DAS TEAM UND DIE EINZELPERSONEN EFFEKTIV ARBEITEN KÖNNEN..

Barry Schillemans,
HR Director, Macaw, www.macaw.net

Die weltweite Pandemie war eine unvorstellbare Tragödie, die globalen Auswirkungen sind auch nach zwei Jahren noch nicht endgültig absehbar. Vieles hat diese Krise verändert, unter anderem auch das Verbraucherverhalten und eine verstärkte Konzentration auf die Online-Welt. Im gleichen Zuge wurden Arbeitgeber gezwungen, auf eine neue Arbeitskultur zu setzen, die vermehrt auf Homeoffice, mobiles Arbeiten und Kollaborations-Software aufbaut. Auch wenn für einige Unternehmen hier die Herausforderungen größer waren als für andere, ist dem Prozess dieser Umstellung unter dem Strich ein positives Ergebnis zu attestieren. Arbeitnehmer erhielten mehr Flexibilität, sie waren nicht mehr auf die Arbeit im Büro angewiesen und konnten Berufliches mit Privatem einfacher vereinbaren. Es war möglich, sich um pflegebedürftige Angehörige besser zu kümmern, Ehrenämter auszuüben und das Privatleben einfacher zu organisieren.

Nun wird die Zukunft unserer Arbeitsweise nicht alleine vom Faktor Homeoffice bestimmt. Allerdings bietet das Konzept zahlreiche Vorteile für alle Beteiligten, von Ressourcen- und Zeitersparnissen dank entfallendem Arbeitsweg über mehr Freiheiten für Mitarbeiter bis zu sinkenden Mietkosten aufgrund weniger benötigter Büroflächen. In Zeiten des Klimawandels und der steigenden Bedeutung an nachhaltigen Unternehmensentscheidungen keine unwichtigen Aspekte.

Althergebrachte Methoden überdenken

Wenn wir aber von der zukünftigen Arbeitswelt sprechen, kann Homeoffice nur ein Baustein sein. Mitarbeiter wollen flexibel sein, Arbeitsorte selbst bestimmen und in Unternehmen mit offenen Strukturen arbeiten. Strukturen, die ihnen möglichst viele Freiheiten geben und damit die Produktivität steigern. Diese Anforderungen gehen Hand in Hand mit einer wichtigen Voraussetzung: Vertrauen. Die Zeiten von alternativloser Büroarbeit sind vorbei, Arbeitgeber müssen ihren Angestellten das Vertrauen entgegenbringen, die anfallenden Workloads auch außerhalb der Büroräume in verteilten Teams und eigenständig zu bewältigen. Die dafür notwendigen Software-Tools erhielten durch die Corona-Krise ebenfalls einen gewaltigen Boost, sodass asynchrones Arbeiten, zeitlich sowie räumlich, keine Herausforderung mehr darstellt.

Mit all den genannten Möglichkeiten sollten Unternehmen erkennen, dass die Zeit für ein Überdenken der herkömmlichen Arbeitsmethoden nie günstiger war. Und sie sollten nicht den Fehler begehen, zu Vor-Corona-Praktiken zurückzuwechseln. Nicht nur, dass Arbeitnehmer verstärkt die Möglichkeit der flexiblen Arbeit einer Beförderung oder Gehaltserhöhung vorziehen, auch der Aspekt der mentalen Gesundheit von Mitarbeitern wird in der Zukunft wichtiger werden. Stress am Arbeitsplatz bis hin zu Burnouts ist ein massives Problem, bei dem Unternehmen verstärkt handeln müssen. Hier gilt es, Mitarbeiter

Wie ich mir die Zukunft der Arbeit vorstelle – die Schaukel ist wie das Leben … es gibt Höhen und Tiefen im Leben und in der Arbeit. Manchmal müssen wir uns stärker anstrengen, um höher zu kommen, aber wir sollten nie vergessen, dass die Schaukel zurückgeht und es eine Ruhephase geben wird, in der sich nicht alles um die Arbeit dreht, sondern wir unsere Zeit auf unsere eigene Weise genießen können.

(Bild: Aco Todoroski – PowerApps Developer)

zu unterstützen, zu coachen und auf individuelle Stärken und Schwächen einzugehen. Während einige Arbeitnehmer kaum noch eine Grenze zwischen Arbeit und Privatem im Homeoffice kennen und so erhöhtem Stress ausgesetzt sind, vereinsamen andere aufgrund der fehlenden sozialen Kontakte und Schnittstellen, wie sie beispielsweise ein Büro bietet.

Funktionierende Unternehmenskultur

Führungskräften kommt in diesem möglichen Spannungsverhältnis eine besondere Rolle zu, denn sie setzen die Grundlagen einer funktionierenden Unternehmenskultur – Werte schaffen und nicht nur Arbeit delegieren. Auch sollten sie dafür Sorge tragen, dass Mitarbeiter nicht das Gefühl bekommen, Wertschätzung und Beförderungen würden mit der Präsenz im Büro zusammenhängen. Überwachung durch den Arbeitgeber ist in diesem Zuge ebenfalls ein Aspekt, der nicht mehr in die moderne Arbeitskultur von innovativen Unternehmen passen will. Im Kern dieses Problems liegt die falsche Annahme begründet, dass die Produktivität der Belegschaft mit der Anwesenheit am Arbeitsplatz verbunden ist. Diese Denkweise ist nicht nur veraltet, sie schadet der Firma. Zukunftsgerichtete Unternehmenskulturen legen den Fokus auf die individuellen Stärken und Schwächen des Einzelnen, sie fördern und helfen. Sie geben Platz für Inspirationen und die Freiheiten für ein eigenständiges Arbeiten.

Bei der Umsetzung dieser Strategien gibt es kaum so gute Ratgeber wie die Mitarbeiter selbst. Möglichkeiten, Wünsche und nötige Unterstützung sollten daher immer direkt individuell oder im Team besprochen werden – gesteigerte Produktivität und erhöhtes Wohlbefinden können die Folgen sein. Der Austausch und die Kommunikation sind daher nicht nur bei arbeitsbezogenen Themen wichtig, sondern auch bei der gemeinsamen Organisation von Arbeitsstrukturen und der Frage, wie das Team und die Einzelpersonen effektiv arbeiten können. Generell stehen Unternehmen dabei vor der Herausforderung, die Verbundenheit einzelner Angestellter zu ihrem Team, aber auch zu ihrer Firma sicherzustellen.

In der Praxis stehen virtuelle Videokonferenzen zur Verfügung, bei denen Vorgesetzte dafür sorgen müssen, dass jedes Teammitglied zu Wort kommt und die nötige Sichtbarkeit erhält. Als IT-Dienstleister und mit einem hohen eigenen Anspruch, New-Work-Prinzipien umzusetzen, bringt Macaw seinen Mitarbeitern von Anfang an Vertrauen entgegen, die Arbeit selbstständig zu erledigen und die Tagesabläufe in Eigenregie zu strukturieren. Und das spiegelt sich in der Zufriedenheit wider. Durch eine vertrauensvolle Umgebung fühlen sich Angestellte nicht nur sicher und inspiriert, sie spüren auch die individuelle Wertschätzung und identifizieren sich mit dem Unternehmen. Hier liegen die Grundlagen für ein angenehmes und produktives Betriebsklima, das nicht nur die Wettbewerbsfähigkeit stärkt, sondern auch die richtigen Anreize für junge Talente und High Professionals setzt.

Barry Schillemans

MODERN & FLEXIBEL

MIT DIGITALEN ARBEITSPLÄTZEN ZU HÖHERER KRISENSICHERHEIT

Die Corona-Krise hat gezeigt, dass Flexibilität bei der Gestaltung von Arbeitsplätzen über die Zukunft von Unternehmen entscheiden kann. Homeoffice Modelle und hybride Modelle sind zentrale Aspekte bei der Art und Weise, wie in Zukunft gearbeitet wird – dafür müssen Unternehmen sie jetzt richtig organisieren.

Das Konzept von digitalen Arbeitsplätzen, Homeoffice und mobiler Arbeit ist keineswegs neu, ihm wurde nur lange Zeit nicht die nötige Geltung zugemessen. Auch wenn einige Unternehmen diese „New Work"-Ansätze bereits vor der Pandemie umgesetzt haben, zeigten sich viele Arbeitgeber von der staatlich verordneten Homeoffice-Pflicht auf dem kalten Fuß erwischt. Doch obwohl oft weder die nötige Infrastruktur, noch die benötigte Hardware zur Verfügung standen, schafften die meisten Firmen dennoch die Umstellung auf den digitalen Arbeitsplatz – auch dank der großen Anzahl an SaaS- und Cloud-Lösungen auf dem Markt.

Wie die Erfahrungen gezeigt haben, benötigt ein strategischer Umstieg auf den digitalen Arbeitsplatz neben den technologischen Grundlagen wie VPN-Verbindungen, belastbaren Servern oder Laptops vor allem auch eine angepasste Unternehmenskultur sowie geschulte Mitarbeiter. Bei der praktischen Umsetzung dieser Aspekte gilt es daher einige Herausforderungen zu überwinden.

Die richtigen Technologien richtig einsetzen

Die Grundlage einer funktionierenden, ortsunabhängigen Zusammenarbeit besteht in der geeigneten Hardware. Unternehmen müssen sicherstellen, dass ihre Mitarbeiter mit den modernen Endgeräten und Webcams ausgestattet sind, damit eine eingeschränkte Performance nicht die Produktivität verhindert. In diesem Zuge muss auch die erforderliche Bandbreite sichergestellt sein – und zwar sowohl auf Client- wie auch auf Server-Seite. Hier lohnen sich Investitionen in die richtigen Ressourcen.

IDEALERWEISE UNTERSTÜTZT EINE PLATTFORM FÜR DEN DIGITALEN ARBEITSPLATZ DIE UNTERSCHIEDLICHSTEN BEREICHE EINES UNTERNEHMENS UND BIETET FÜR EINE HOHE PRODUKTIVITÄT EIN EINHEITLICHES BENUTZERERLEBNIS.

Sridhar Iyengar, Managing Director, Zoho Europe, www.zoho.com

Dezentrale Arbeitsmodelle stellen auch eine breite Angriffsfläche für Cyberkriminelle dar. Unternehmen müssen aus diesem Grund einen besonderen Fokus auf entsprechende Sicherheitsmaßnahmen legen.

Die Arbeitskultur updaten

Die Bedeutung von Vertrauen muss im Vordergrund stehen. Besonders jetzt, da Mitarbeiter nicht mehr jeden Tag im Büro sind und möglicherweise flexiblere Arbeitszeiten haben. Manchen Führungskräften mag dies schwerfallen – aber die Anpassungsfähigkeit ist erforderlich, damit sie moderne und für Arbeitnehmer attraktive Arbeitsmodelle erfolgreich im Unternehmen verankert können. Um dieses Ziel zu erreichen, müssen neue Konzepte von der Führungsebene angetrieben und Mitarbeiter bei der Umsetzung unterstützt werden.

Neben der Vermittlung der neuen Arbeitsweisen und ihrer Vorteile, darf auch die technologische Seite nicht vergessen werden, die diese neuen Konzepte mit sich bringen. Die Schulung des technischen Verständnisses sollte daher Priorität haben, insbesondere im Zeitalter von SaaS- und Cloud-Anwendungen. Mit internen Trainings, die auch online stattfinden können, sollten Mitarbeiter von Experten für neue Anwendungen geschult werden – ergänzend können Support-Hotlines und Anleitungen helfen.

Die Corona-Krise hat vieles verändert. Mit neuen Ansätzen für flexible Arbeitsweisen, innovativen Technologien und einer verbesserten Organisation gilt es nun, die neue Arbeitskultur rund um den digitalen Arbeitsplatz abzusichern und Unternehmen nachhaltig wettbewerbsfähig zu machen.

Sridhar Iyengar

AUS DREI KLICKS MACH EINEN

MEHR EFFIZIENZ DURCH PASSGENAUE OBERFLÄCHEN

In Zeiten des Fachkräftemangels ist Effizienz zum zentralen Erfolgsfaktor geworden. Diese beginnt bereits bei der genutzten Geschäftslösung, die benötigte Steuerelemente und Daten möglichst einfach und schnell erreichbar zur Verfügung stellen muss – und das passgenau für jeden Mitarbeiter. Hier kann KI unterstützen, eine maßgeschneiderte Oberfläche für jeden Anwender zu erstellen.

Drei Klicks oder nur einer: Was nach wenig Unterschied klingt, hat über einen ganzen Tag hinweg gesehen einen deutlichen Einfluss auf die Produktivität eines Mitarbeiters. Entsprechend stellen bereits viele Geschäftssysteme Personalisierungsoptionen zur Verfügung, die es ermöglichen, die Oberfläche an die individuellen Bedürfnisse eines Anwenders anzupassen. In der Regel ist dies jedoch mit teils hohem manuellem Aufwand verbunden.

Automatische Personalisierung

Mithilfe von künstlicher Intelligenz lassen sich entsprechende Prozesse automatisieren. Durch anonymisiertes Beobachten des individuellen Verhaltens eines Mitarbeiters in der Geschäftslösung können intelligente Algorithmen ein Verständnis von dessen täglichen Aufgaben erhalten. Daraufhin können sie genau die Elemente vorschlagen, die der Anwender tatsächlich benötigt, von Möglichkeiten zur Rechnungsfreigabe bis hin zu einem Überblick über erledigte Lieferscheine. Nimmt der Anwender den Vorschlag der KI an oder lehnt er diesen ab, lernt die KI-Technik wiederum hinzu – und ist anschließend noch besser in der Lage, dafür zu sorgen, dass für jeden Mitarbeiter alle wichtigen Schaltflächen nicht mehr als einen Klick entfernt sind.

Christian Leopoldseder
www.applus-erp.de

DATENSPEICHER NEU GEDACHT

LEITFADEN FÜR EINE ERFOLGREICHE IT-TRANSFORMATION

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.

WHITEPAPER DOWNLOAD

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

LIZENZEN-DSCHUNGEL IM EVERYWHERE WORKPLACE

ES IST AN DER ZEIT, SICH VOM SOFTWARE-MÜLL ZU TRENNEN

Viele Unternehmen sind sich darüber im Klaren, dass sie erhebliche Ausgaben für ungenutzte oder nicht ausreichend genutzte Software verschwenden. Eine vor einigen Jahren durchgeführte Benchmark-Studie schätzte die vergeudeten Softwareausgaben in den USA auf 30 Milliarden US-Dollar beziehungsweise auf durchschnittlich 259 US-Dollar pro Desktop. Verfügt ein Unternehmen beispielsweise über 20.000 Desktops, entspricht das einer Investition von 5,2 Millionen Dollar, die keinen Gewinn abwirft. Kosteneinsparungen und Initiativen zur Kostenvermeidung stehen bei SAM-Teams deshalb ganz oben auf der Liste. Insbesondere für Software-Assets, die sich zu „Shelfware" oder Cloud-Müll entwickelt haben und deren Lizenzen schon Staub ansetzen, gilt es potenzielle Budgetbelastung zu optimieren.

Einsparpotenziale liegen auf der Hand

In einer weiteren Studie gaben die befragten Unternehmen an, die größten Budgetentlastungen durch die Wiederverwendung vorhandener Lizenzen zu erzielen. Außerdem sparen sie, wenn sie Anbieterverträge besser aushandeln und die Wartungsausgaben für nicht genutzte Software reduzieren. Zudem wurde festgestellt, dass SAM-Teams den größten Teil ihrer Zeit für Audits aufwenden. Dadurch lassen sich zwar Optimierungsmöglichkeiten aufdecken – der beträchtliche Zeitaufwand verhindert jedoch, dass IT-Teams proaktiv kostensenkende Maßnahmen implementieren und den Anwendungsbereich von SAM auf Software-as-a-Service (SaaS), die Cloud und Container ausweiten. Einsparungspotenzial besteht auch bei der Zeit, die IT-Abteilungen für die Betreuung von Assets benötigen: Laut einer Umfrage von Ivanti unter IT-Fachleuten wenden 28 Prozent der Befragten jede Woche zig Arbeitsstunden dafür auf, Assets zu pflegen, die nicht mehr unter die Garantie oder den Support fallen. 20 Prozent der befragten Personen gaben zu, dass sie keinen Überblick haben, welche Assets überhaupt veraltet sind. Diese Kombination aus ungenutzter Software und abgelaufenen Lizenzen ist eine Schwachstelle in der IT- und CIO-Charta.

Neue Herausforderungen durch neue Arbeitswelten

Im Zeitalter des Everywhere Workplace unterstützen IT-Teams zudem vermehrt Mitarbeiter, die sich überwiegend in remoten Umgebungen aufhalten. Die damit verbundenen Sicherheitsherausforderungen führen dazu, dass Firmen verstärkt in Unternehmenssoftware investieren und immer mehr Software einsetzen – in On-Premises-, Cloud- und Edge-Umgebungen. Waren vor fünf bis zehn Jahren etwa nahezu alle installierten Anwendungen On-Premises, sind heute die meisten aller Anwendungen SaaS-basiert. Dadurch wird auch der Ruf nach Shelfware und unkontrollierter Cloud-Nutzung zunehmend lauter. Die Herausforderung: Unternehmen müssen nicht nur wissen, welche Software sie lokal oder cloudbasiert bereitstellen, sondern auch, ob diese sicher ist, den Compliance-Regeln entspricht und im Budget liegt. Derzeit konzentrieren sich laut Gartner jedoch nur 41 Prozent der IT-Asset-Management- (ITAM) und SAM-Teams auf die Verwaltung von SaaS. Verlieren Unternehmen den Überblick, kann es zudem teuer werden. Beispielsweise dann, wenn Unternehmen mehr Lizenzen kaufen, als sie tatsächlich benötigen. Übersteigt die Zahl der Nutzer hingegen die der verfügbaren Lizenzen, steigt das Audit-Risiko: Es kann zu Compliance-Problemen kommen, wenn Benutzer Konten gemeinsam nutzen. Moderne, zukunftsfähige Arbeitsumgebungen und technologische Fortschritte verlangen Unternehmen also einiges ab: Wer mit der Zeit geht, muss sich zugleich neuen Herausforderungen stellen.

MODERNE, ZUKUNFTSFÄHIGE ARBEITSUMGEBUNGEN UND TECHNOLOGISCHE FORTSCHRITTE VERLANGEN UNTERNEHMEN EINIGES AB: WER MIT DER ZEIT GEHT, MUSS SICH ZUGLEICH NEUEN HERAUSFORDERUNGEN STELLEN.

Andreas Schmid, Sales Engineering Manager für EMEA Central, Ivanti, www.ivanti.de

Den Überblick bewahren dank Automatisierung

Um nicht an diesen neuen Herausforderungen zu scheitern und um der Verschwendung von Shelfware und Cloud-Budgets Einhalt zu gebieten, sollten Unternehmen nicht nur wissen, welche ungenutzten Software-Assets bereits vorhanden sind – sondern auch verhindern, dass

weitere dieser Assets ungenutzt bleiben. Dazu müssen Nutzung, Lizenztypen, Käufe, Abonnements, Verlängerungen, auslaufende Verträge und laufende Ausgaben sorgfältig verfolgt werden. Was einfach klingt, gestaltet sich in der Praxis oft kompliziert. Manuell lässt sich das Lizenzmanagement aufgrund der hybriden Arbeitsumgebungen, knapper personeller und zeitlicher Ressourcen und der stetig wachsenden Softwarelandschaft kaum noch bewältigen. Software aus der Cloud oder SaaS wird zudem nicht erfasst, wenn das Lizenzmanagement nur zentral eingekaufte On-Premises-Software listet. Unternehmen benötigen deshalb eine intelligente, automatisierte und einfach nutzbare Lösung. Diese besteht darin, Automatisierung, maschinelles Lernen und Datenanalyse in die Untersuchung der Softwareausgaben einzubeziehen. Auf diese Weise erhält man einen schnelleren Überblick darüber, wie gut ein Unternehmen seine aktuelle Software-Asset-Umgebung nutzt, und kann alle Assets, die zu Ladenhütern geworden sind, mit einem Laserlicht beleuchten.

Starke Verhandlungsposition und Budgetkontrolle

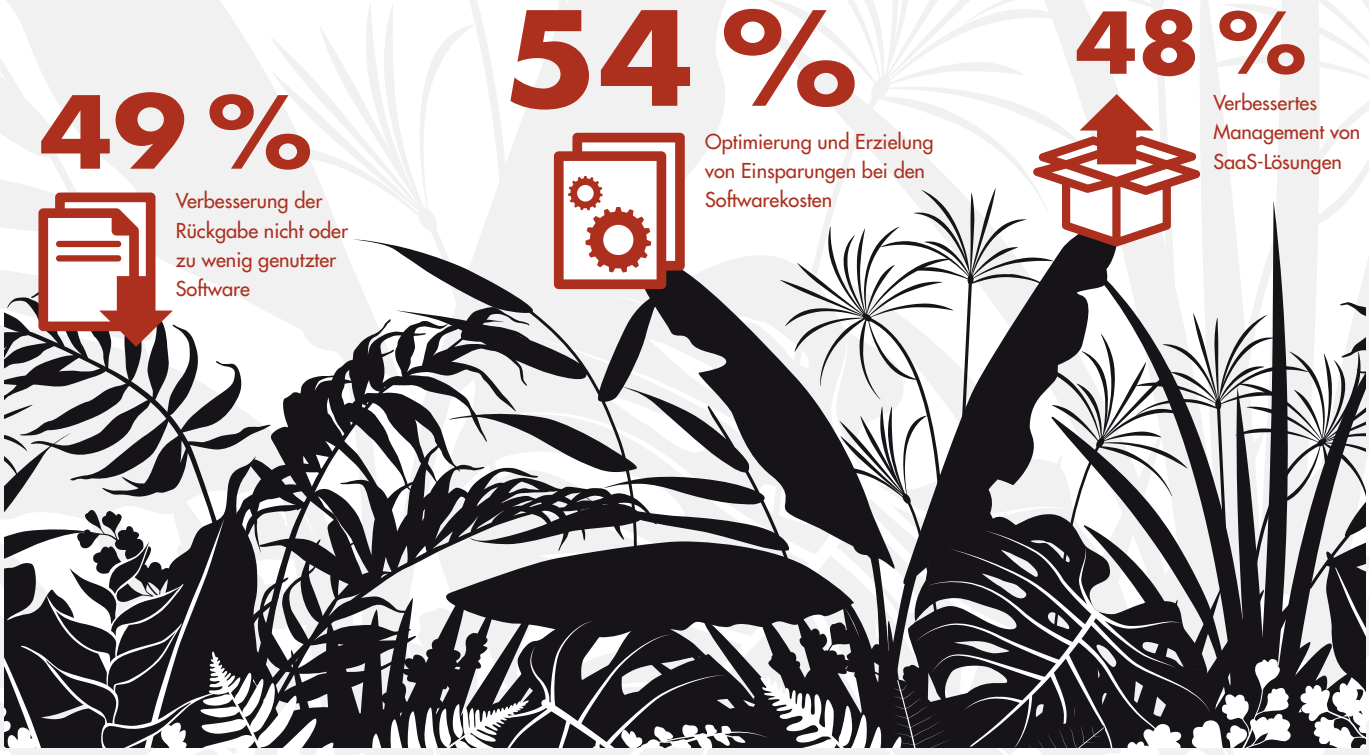
IT-Teams müssen heute alle Ressourcen betrachten, die sich vor Ort, in der Cloud oder in Edge-Umgebungen befinden. Mit Blick auf das Budget wird von der IT-Abteilung zudem erwartet, dass sie einen gründlichen, aussagekräftigen Bericht über die „Spend Intelligence" in Bezug auf die Softwarenutzung vorlegt und darlegt, ob diese Ressourcen zu den gewünschten Geschäftsergebnissen beitragen oder einfach nur Geld verschlingen. Moderne SAM-Tools verschaffen Verantwortlichen gute Argumente für die Neuverhandlung von Budgets und Verträgen oder die Rechtfertigung laufender Kosten und Abonnementgebühren: Sie liefern detaillierte Reportings über den gesamten Softwarebestand, die als Grundlage für fundierte Entscheidungen bei der Softwarelizenzierung dienen. Spend Intelligence ist ein geeignetes Mittel, um die Kontrolle über die Nutzung von Shelfware und Cloud zu erhalten. Sie erfasst Daten über alle Ausgaben für Software-Assets und die Nutzung von Cloud-Anwendungen und bewertet die tatsächliche Nutzung. So lassen sich Software- und Cloudressourcen während ihres gesamten Lebenszyklus besser verwalten und aus dem Verkehr ziehen beziehungsweise neu nutzen.

Den Fortschritt vorantreiben

Moderne SAM-Tools, die auch die Cloud miteinbeziehen, verschaffen Unternehmen in einer digitalisierten Arbeitswelt einen besseren Überblick über Ausgaben, Nutzung und vertragliche Vereinbarungen von Assets. IT-Teams identifizieren damit Bereiche, die zu hohe Kosten verursachen – und gewinnen Gelder für Software-Assets zurück, die zu Shelfware oder Cloud-Müll geworden oder veraltet sind. Mit einem automatisiertem Lizenzmanagement treffen Unternehmen fundiertere Entscheidungen, sparen Kosten ein, verbessern Workflows, verhindern negative Audits und versetzen nicht zuletzt ihre IT-Teams in eine perfekte Ausgangslage, um Audits zu bestehen und compliant zu sein.

Andreas Schmid

WELCHE SAM-INITIATIVEN MÖCHTEN SIE IM NÄCHSTEN JAHR UNTERSTÜTZEN?



Quelle: Flexera; ITAM-Report 2022

LIZENZMANAGEMENT

PFLICHT ODER KÜR? **TEIL I VON II**

Software-Lizenzmanagement ist schon längst eine der wichtigsten Disziplinen in Unternehmen zur Wahrung der Compliance, aber auch ein Schlüssel zur Wertschöpfung der erworbenen Assets geworden. Mitunter ist die Disziplin aber auch von einem Narrativ geprägt, welches die Abhängigkeit und Dominanz der großen Softwarehersteller zum Ausdruck bringt. Dabei bestehen für Unternehmen Potenziale, hiermit die Herausforderungen der Digitalisierung zu unterstützen und Mehrwerte zu schaffen, wenn infolgedessen nachhaltige Möglichkeiten etwa wie Gebrauchtsoftware effizient unterstützt werden.

Was ist Software-Lizenzmanagement?

Während es früher in der IT überwiegend um physische Ressourcen wie Server, PCs und weitere Hardware ging, steht seit Langem Software wie auch Cloud-Services im Mittelpunkt der Betrachtung und damit das Management der Softwarelizenzen. Nicht selten gestaltet sich dies als schwierig, da Lizenzbestimmungen oftmals – unter Umständen von Herstellern bewusst – kompliziert und unverständlich gehalten sind sowie noch dazu häufigen Änderungen unterzogen werden.

Software-Lizenzmanagement umfasst insbesondere Prozesse und Tools, um den Erwerb und Einsatz von Softwareprodukten zu kontrollieren, zu dokumentieren und deren Zuweisung festzulegen. Es geht dabei im Wesentlichen um den – gemäß dem zu klärenden Rechtsrahmen aus Gesetz und Vertrag – rechtskonformen und effizienten Einsatz von Softwarelizenzen und Services.

Genauso wie Unternehmen spezifisch sind, verhält es sich hingegen mit der Umsetzung des Software-Lizenzmanagements. Wichtig erscheint es gerade infolge des damit verbundenen vermehrten Einsatzes von Cloud-Services und der allgegenwärtigen Digitalisierung mit dem damit verbundenen datenzentrierten Ansatz, die Prämissen von Software-Lizenzmanagement zu hinterfragen und erforderlichenfalls neu auszurichten.

Die Rollen des Software-Lizenzmanagements

Das Software-Lizenzmanagement ordnet sich als wichtiges Element in das sogenannte Software-Asset-Management (SAM) ein, welches wiederum Teil des auch physische Einheiten umfassenden IT-Asset-Managements ist. Dessen wesentliche Aufgaben ist das Identifizieren von Hard- und Software-Assets, deren Inventarisierung und das Managen von Konfigurationen, Vorfällen, Problemen,

Änderungen und Beziehungen. Wie Software-Lizenz-, Software-Asset- und IT-Asset-Management voneinander abzugrenzen und umzusetzen sind, kann allenfalls unternehmensspezifisch beantwortet werden.

Die Frage nach dem Recht

Im Zentrum des Software-Lizenzmanagements steht der rechtskonforme Einsatz der erworbenen Softwareprodukte und Cloud-Services. Dabei handelt es sich um eine häufig einseitig oder gar unrichtig beantwortete Grundsatzfrage. Rechtskonformität bedeutet nämlich nicht, dass allein die Lizenzbestimmungen des Herstellers oder noch dazu dessen Auslegung maßgeblich sind. Vielmehr besteht zunächst ein allgemeingültiger gesetzlich normierter Rechtsrahmen. Vertragliche Vereinbarungen wie Lizenzverträge haben sich in diesen Rahmen einzuordnen.

Für den Rechtsrahmen wäre hierzulande mangels bestehendem „Lizenzrechts" zum einen das Urheberrecht zu befragen, da Software hier spezialgesetzlich geregelt ist. Zum anderen gelten strenge Anforderungen an für eine Vielzahl von Verträgen einseitig vorformulierte vertragliche Bestimmungen, wie etwa Lizenzverträge oder Lizenzbestimmungen. Infolgedessen gehen insbesondere unklare Bestimmungen zulasten des Herstellers und noch dazu sind Regelungen, die im Widerspruch zu wesentlichen gesetzlichen Grundgedanken stehen, unwirksam. In diesem Rahmen bewegt sich das vertraglich vereinbarte, also vorformulierte Lizenzverträge und deren Anlagen. Gerade oftmals komplexe Lizenzbestimmungen dürften sich mit diesen Anforderungen schwertun, wenn Unklarheiten trotz großer Anstrengungen verbleiben.

Damit muss es zunächst einmal grundsätzlich zu einem Umdenken kommen, wenn der Hersteller meint, mehrdeutige vertragliche Regelungen zu seinen Gunsten auslegen zu wollen und hierfür Hilfestellungen anbietet. Auch inhaltliche Fragen für das Lizenz-Management nach dem Verständnis von Lizenzen, Zuweisung und Nutzung bestimmt der zuvor skizzierte gesetzliche Rechtsrahmen.

IM ZENTRUM DES SOFTWARE-LIZENZMANAGEMENTS STEHT DER RECHTSKONFORME EINSATZ DER ERWORBENEN SOFTWAREPRODUKTE UND CLOUD-SERVICES.

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

Das Software-Lizenzmanagement muss sich von der Hersteller-Doktrin also zunächst einmal loslösen und eigene Sichtweisen zu den vereinbarten vertraglichen Regelungen entwickeln. Daher ist elementar wichtig, die zwingend geltende höchstrichterliche Rechtsprechung und geltenden Gesetze vorrangig zu berücksichtigen. Infolgedessen ist eine Entzerrung zwischen Angeboten des Herstellers oder dessen Partnern und dem Management der Lizenzen anzuraten.

Was machen Tools (richtig)?

Es gibt eine Vielzahl von Software-Lizenz-, Software-Vertrags- und Software-Asset-Management-Tools und -Services. Genauso unterschiedlich sind Preise, Metriken und zusätzliche Serviceangebote. Anbieter dieser Tools und Services sind teilweise die Software-Hersteller selbst oder aber unmittelbare Partner. Einerseits können damit Vorteile verbunden sein, andererseits ist gerade eine solche Verzahnung für Kunden oftmals problematisch. Denn gleichermaßen kann es hier zu einer Interessenkollision und Verflechtung kommen, da die Interessen von Hersteller und Kunden nicht deckungsgleich sind.

Weiterhin darf sich nicht der Illusion hingegeben werden, Tools erledigen das Lizenz-Management von selbst. Das Gegenteil ist richtig und gilt auch bei Tools, die teilweise automatisiert tätig sind. Entscheidend ist aber, dass es nicht das eine Tool für alle gibt. Vielmehr muss das eigene Bedürfnis anhand der Unternehmensstrukturen, Verantwortlichkeiten und Fähigkeiten sowie des zur Verfügung stehenden Budgets ermittelt werden. Nicht selten werden teure Tools eingekauft, aber mangels eigener Kompetenz oder Kapazität oder auch aufgrund ihrer Überkomplexität nie eingesetzt. Das ist doppelt schlecht, da damit auch das jeweilige Tool nicht überzeugen kann und ohne Mehrwert Kosten entstanden sind. Unterschiedliche Tools für verschiedene Aufgaben im Zusammenhang mit Software-Lizenzen und Software-Verträgen können bei sorgsamer Auswahl den Vorteil der maßgeschneiderten Spezialisierung, etwa zu einem Hersteller, haben. Umgekehrt lässt eine einzige Lösung für alle Aufgaben in diesem Komplex oftmals die speziellen Anforderungen etwa aufgrund der Eigenarten der Lizenzbestimmungen, Vertragsstrukturen, Terminologien und Metriken vermissen.

Folglich ist gemeinhin bekannt, dass eine genaue Prüfung vor einer Anschaffung stehen und auch in der Folge eine Evaluierung von Kosten, Nutzen und Einsatz erfolgen muss.

Andreas E. Thyen

VORSCHAU

Im zweiten Teil in der nächsten Ausgabe wird es um die spürbare Angst vor dem Audit, Mehrwerte des Lizenzmanagements für das Business sowie die große Bedeutung eines neutralen Lizenzmanagements gehen sowie ein Fazit gezogen werden.

DAS NÄCHSTE

SPEZIAL

itsecurity

ERSCHEINT AM
30. SEPTEMBER 2022

IT & NACHHALTIGKEIT: Es gibt viel zu tun

MANAGED SERVICES: Einfach bessere Qualität

CLOUD COMPUTING: Hochsicher unterwegs

DIE AUSGABE 09/2022
VON IT MANAGEMENT
ERSCHEINT AM 31. AUGUST 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

Geschäftsführer und Herausgeber:
Ulrich Parthier (-14)

Chefredaktion:
Silvia Parthier (-26)

Redaktion:
Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Michael Biechele, Andreas Grydeland Sulejewski, Christoph Gudernatsch, Sridhar Iyengar, Christian Leopoldseder, Alfons Michels, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Barry Schillemans, Andreas Schmid, Hans-Werner Schmidt, Andreas E. Thyen, Ingo Wittrock

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

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

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

itsecurity
JULI/AUGUST 2022

DAS SPEZIAL

THOUGHT LEADERSHIP

INTEGRIERTER SCHUTZ

GEMEINSAM SIND WIR SICHER

Christian Bücker, macmon secure GmbH und Oliver Kleineberg, Belden

KI-GESTÜTZTE HELFER

Cybersicherheit erhöhen

SEGREGATION OF DUTY

Kontrollen erfolgreich einführen

EFFIZIENTE KRYPTOGRAFIE

Multi-Tool des Datenschutzes

www.it-daily.net


itsa EXPO
CONGRESS
HOME OF IT SECURITY
HIT
HACKERS
HARD
LET'S TALK ABOUT IT SECURITY!
25. – 27. Oktober 2022
Nürnberg, Germany
Jetzt Gratis-Ticket sichern:
itsa365.de/hit-hackers-hard
NÜRNBERG MESSE

INHALT

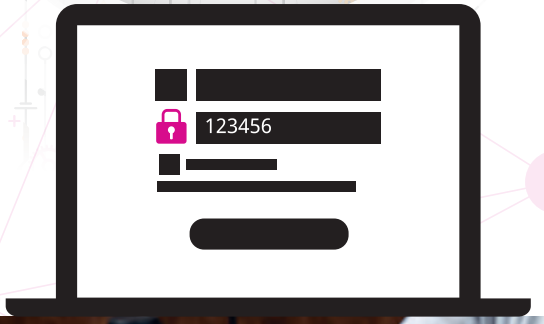
COVERSTORY

THOUGHT LEADERSHIP

IT SECURITY

4 COVERSTORY

12



24

07

GEMEINSAM SIND WIR SICHER

INTEGRIERTER SCHUTZ VOR KRIMINELLEN IN IT- UND OT-NETZWERKEN

Die Belden Gruppe hat die macmon secure GmbH, Anbieter von Produkten für Netzwerkzugangskontrolle (Network Access Control und Zero Trust Network Access / ZTNA) mit Sitz in Berlin, Anfang 2022 übernommen. Business Director Christian Bücker und Chief Technology Officer Oliver Kleineberg im Interview mit Ulrich Parthier, Herausgeber it security, zu den Hintergründen, der industriellen Logik und der Vision des fusionierten Unternehmens.

Ulrich Parthier: *Herr Kleineberg, Belden als global Player kauft die IT-Security-Experten macmon. Wie wurden Sie auf macmon aufmerksam?*

Oliver Kleineberg: Im Bereich Netzwerkzugangskontrolle hat sich macmon in den vergangenen Jahren eine führende Marktposition erarbeitet. Durch die Einführung von macmon SDP und der Verfolgung einer Zero-Trust-Network-Access-Strategie hat das Unternehmen einen wichtigen strategischen Schritt in die Cloud vollzogen. Wir sind bei Kundeninstallationen verstärkt auf macmon aufmerksam geworden. Und da das Thema IT-Sicherheit in der Belden Gruppe deutlich an Bedeutung gewonnen hat, haben wir das Gespräch mit macmon gesucht. Schnell wurde uns klar, dass wir unseren Kunden gemeinsam einen deutlichen Mehrwert anbieten können, denn IT- und OT-Netzwerke wachsen durch die Digitalisierung mehr und mehr zusammen, mit deutlich erhöhten Anforderungen an die Cybersicherheit in Automatisierungsnetzen.

Ulrich Parthier: *Herr Bücker, diese Fusion hat viele in der Branche überrascht. Was wird aus macmon?*

Christian Bücker: macmon wird von Belden in den Geschäftsbereich Industrial Network Solutions (INS) mit Hauptsitz in der Region Stuttgart eingegliedert. Zu ihr gehören bereits führende Technologieanbieter wie Hirschmann, ProSoft Technology, OTN Systems und Lumberg Automation. Wir besetzen innerhalb der Belden Gruppe das Thema IT-Security und sehen die große Chance, als Mitglied in einem globalen Technologiekonzern, unsere Lösungen für ein sicheres Netzwerkmanagement auch weltweit vermarkten, und unsere Innovationen durch die Nutzung der F&E-Kapazitäten von Belden weiter vorantreiben zu können.

Ulrich Parthier: *Im industriellen Umfeld ist das sehr viel Entwicklungspower. Was ist das Ziel?*

Oliver Kleineberg: Cybersicherheitsvorfälle bei industriellen Steuerungssystemen gehen auf mehrere Vektoren zurück, wie etwa Systemschwachstellen, Lücken in der Netzwerkarchitektur, fehlende Netzwerksegmentierung, vulnerable Hardware- und Softwarekonfigurationen und menschliche Fehler. Die zunehmende Vernetzung der Produktionssysteme steigert die Komplexität und Anfälligkeit der Netze. Im Gegensatz zur Office-Welt können die sensiblen Komponenten in den Produktionsnetzen, wie Roboter, Maschinen und Steuerungen, nicht mit den üblichen Mitteln geschützt werden. Hier können wir eine starke Kombination anbieten – das Netzwerksicherheits-Portfolio und Know-how von macmon gekoppelt mit Hirschmanns Kompetenz im Bereich Industrial Internet of Things (IIOT) Netzwerkinfrastruktur.

Ulrich Parthier: *IoT, Cloud, steigende Datenmengen, IT-Sicherheit gerade im KRITIS-Umfeld, Branchen wie Automotive, es gibt viele Faktoren zu berücksichtigen.*

Christian Bücker: Die Digitalisierung der Office- und Produktions-Umgebungen führen zu einer immer stärkeren Vernetzung von Systemen (IT) und Prozessen

> GEMEINSAM STEHEN WIR FÜR INNOVATION, QUALITÄT UND ZUVERLÄSSIGKEIT, WIR HABEN EINE GLEICHWERTIGE UNTERNEHMENS-DNA.
>
> Christian Bücker, Business Director,
> macmon secure GmbH, www.macmon.eu

(OT). Viele aktuelle Studien aus verschiedenen Perspektiven zeigen auf, dass dabei die Cloud-Nutzung massiv steigt und somit die Notwendigkeit für den Einsatz einer ZTNA-Lösung umso wichtiger wird. In diesem dynamischen Umfeld positionieren wir uns mit einer einzigartigen Kombination als Anbieter für Hardware- und Software-Lösungen für IT- und OT-Umgebungen mit dem Schwerpunkt Sicherheitstechnologie. Verschiedene Branchen bedeuten auch verschiedene und teils spezielle Anforderungen an Sicherheits-Konzepte, die durch individuelle Regulatorien geprägt sind. Einige Beispiele: macmon NAC hilft bei der TISAX-Zertifizierung, dem Branchenstandard für Informationssicherheit in der Automobilindustrie. Unsere Lösungen sind im Einsatz bei öffentlichen Verwaltungen, die über eine Fülle an sensiblen Daten verfügen, bei Banken, Kreditinstituten, Finanzdienstleistern und Versicherungsunternehmen, die mit Daten arbeiten, deren Missbrauch erheblichen finanziellen Schaden verursacht. Im Gesundheitswesen werden IT-Netzwerke, die Medizinprodukte integrieren, zu medizinischen Netzwerken. Kontrolle und Sicherheit in gemischten Netzwerken sind lebenswichtig und ausbleibend sogar lebensbedrohlich. Hier sind wir in zahlreichen Kliniken aktiv.

Ulrich Parthier: *Herr Kleineberg, welche Expertise bringt Belden mit?*

> MIT INNOVATIVEN LÖSUNGEN FÜR DIE ZUVERLÄSSIGE UND SICHERE ÜBERTRAGUNG STETIG WACHSENDER DATENMENGEN ÜBERNIMMT BELDEN EINE SCHLÜSSELROLLE BEIM GLOBALEN WANDEL HIN ZU EINER VERNETZTEN WELT.
>
> Oliver Kleineberg, CTO, Belden, www.belden.com

Oliver Kleineberg: Durch strategische Übernahmen und hervorragende interne Produkt- und Lösungsentwicklung ist Belden für die Herausforderungen der Zukunft dank des Portfolios und seiner Wissensbasis ausgezeichnet aufgestellt. Das 1902 gegründete Unternehmen hat seine Wurzeln in der Kabeltechnik. Ziel ist es, Kunden zu betreuen, die die Vernetzung und Automatisierung in Fertigung, Facility Management und Telekommunikation erhöhen wollen. Wir sind heute schon in der Lage, Unternehmen mit einer Vielzahl an Komponenten bei ihren Schritten in die digitalisierte Vernetzung zu begleiten und zu unterstützen. Mit macmon kommt nun die Absicherung genau dieser Vernetzung hinzu.

Mit der auf Automatisierungsnetzwerke spezialisierten Belden-Sparte Hirschmann arbeitet macmon bereits an diversen großen gemeinsamen Projekten. Die langjährige Erfahrung und Expertise des Belden-Teams im OT-Umfeld sorgt dann gemeinsam mit macmon für einzigartige Lösungen, die dem steigenden Bedarf an umfassenden Cybersicherheitslösungen im Automatisierungsumfeld gerecht werden.

Ulrich Parthier: *Was erwarten sich die Unternehmen von der Fusion?*

Christian Bücker: Ziel ist es, Synergien zu nutzen und sich gemeinsam zu einem führenden Lösungsanbieter für Hardware- und Software für IT- und OT-Umgebungen zu transformieren. Zu diesem Zweck gibt es bereits diverse gemeinsame Arbeitsgruppen, um in gemeinsamen Workshops Integrationsmöglichkeiten weiterführend zu identifizieren und deren Umsetzung zu initiieren. Wir bieten eine starke Kombination - das Netzwerksicherheits-Portfolio inklusive Netzwerkmanagement gekoppelt mit Hirschmanns Industrial Internet of Things (IIOT)-Kompetenz.

Dabei wird macmon den Fokus auf IT-Umgebungen nicht aufgeben, sondern ganz im Gegenteil die Erfahrungen und Technologien mit in die OT-Welt bringen und weiterhin Wert auf die Herstellerunabhängigkeit und Technologieoffenheit legen.

Oliver Kleineberg: Belden produziert und vertreibt ein umfassendes Portfolio von Kabel-, Connectivity- und Networking-Produkten. Hirschmann, ein Unternehmen der Belden Gruppe, ist Technologie- und Marktführer für industrielle Netzwerke. Hirschmann entwickelt innovative Lösungen, die sich an den Anforderungen der Kunden hinsichtlich Leistung, Effizienz und Investitionssicherheit orientieren. Dadurch verfügen wir über langjährige Erfahrungen im Bereich von Produktions-Netzwerken. Durch die Globalisierung und ihre vernetzten Lieferketten muss das Produktionsnetzwerk ausfallsicher sein, die Risikobetrachtung bei OT-Systemen hat das Augenmerk auch auf IT-Sicherheit gelenkt, nicht nur die der Office-Netzwerke, sondern auch der OT-Netzwerke. Gemeinsam mit macmon haben wir Antworten auf diese geänderten Herausforderungen. Ein entscheidendes Kriterium bei der Entscheidung für die Übernahme von macmon war, dass die macmon Produkte durch ihr vorausschauendes Design in der Lage sind, wertvolle Aspekte der IT-Technologie auf OT-Netzwerke anzuwenden – eine absolutes Alleinstellungsmerkmal.

Ulrich Parthier: *Gibt es schon eine gemeinsame Vision?*

Christian Bücker, Oliver Kleineberg: Gemeinsam stehen wir für Innovation, Qualität und Zuverlässigkeit, wir haben eine ähnliche Unternehmens-DNS. Wir arbeiten kontinuierlich an der technischen Weiterentwicklung unseres Portfolios, bieten Zuverlässigkeit unserer Produkte und Lösungen, verfolgen eine absolute Kundenorientierung, pflegen faire Partnerschaften und investieren in die Förderung unserer talentierten und engagierten Mitarbeiter*innen. Aber seien Sie gewiss – da kommen in naher Zukunft noch weitere und konkretere Lösungen aus der nun gemeinsamen Schmiede.

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

THOUGHT LEADERSHIP

SECURITY AWARENESS LÖSUNGEN

WIE SIE AM BESTEN EINGESETZT WERDEN

Besonders im Bereich IT-Sicherheit befinden sich Cyberkriminelle und Security-Teams in einem Wettrennen um die bessere Technologie – und wollen der anderen Seite stets einen Schritt voraus sein. Dabei ist Software allein nicht ausreichend, um einen Vorsprung auf- beziehungsweise auszubauen. Beide Seiten setzen daher auf Fähigkeiten, die der Mensch besser beherrscht, als es Technologie und künstliche Intelligenz können. Wenn es um kreatives und vor allem kritisches Denken geht, sind Menschen den „Maschinen" überlegen. Organisationen sollten diese Fähigkeiten daher nachhaltig und strategisch für ihre Cyberabwehr nutzen.

Ist der Faktor Mensch eine Schwachstelle für die IT-Sicherheit?

Betrachten wir die aktuelle Cyberbedrohungslage, lässt sich diese Frage schnell mit einem „Ja" beantworten. Denn Hacker setzen bei ihren Cyberangriffen gezielt auf Emotionen und zwischenmenschliche Beziehungen, um E-Mail-Empfänger zum Klicken oder Öffnen von Dateien zu bewegen. Laut dem Bundeslagebild Cybercrime 2021 des Bundeskriminalamts (S. 13ff.) haben besonders Phishing-Angriffe mit Bezug auf die Covid-19-Pandemie zugenommen. Diese Social-Engineering-Methode zielt darauf ab, beispielsweise über gefälschte Mails von Kollegen Malware zu verteilen oder über gefälschte Webseiten Nutzer zur Weitergabe ihrer Zugangsdaten zu bewegen. Die repräsentative Studie von Bitkom von August 2021 bestätigt, dass viele Cyberattacken ihren Ursprung in Social Engineering haben. So werden beispielsweise die Inhalte von Spear-Phishing-Angriffen flexibel an das aktuelle Zeitgeschehen angepasst (FFP2-Masken, Ukraine-Krieg). Hinzu kommt, dass sich der Markt für Cybercrime zunehmend professionalisiert. Die Folgen sind leichterer Zugang zu Malware für Kriminelle, da Hacking Tools mittlerweile auch als „as-a-Service"-Modell angeboten werden. Das bedeutet, dass böswillige Akteure nicht mehr technisch versiert sein müssen. Sie können zum Beispiel mit Malware-as-a-Service in wenigen Schritten eine breit angelegte oder gezielte (je nach Bedarf) Malware-Attacke initiieren.

DAS ZIEL VON SECURITY AWARENESS IST ES, DEN FAKTOR MENSCH ZU EINEM FESTEN BESTANDTEIL EINER LANGFRISTIGEN IT-SICHERHEITSSTRATEGIE UND SOMIT ZU EINEM ENTSCHEIDENDEN SECURITY-VORTEIL ZU ENTWICKELN.

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

Fest steht, dass Cyberkriminelle ganz gezielt menschliches Verhalten im Fokus ihrer Angriffe haben und versuchen, dieses für ihre Zwecke zu nutzen. Nur wenn Organisationen menschliches Verhalten in ihrer Security außen vor lassen, kann der Faktor Mensch tatsächlich eine Schwachstelle für ihre IT-Sicherheit darstellen. Daher ist es essenziell, Mitarbeitende nachhaltig in die Cybersecurity-Strategie zu integrieren und eine Kultur der Cybersicherheit aufzubauen. Das gilt besonders für Organisationen, die zur kritischen Infrastruktur (KRITIS) zählen. Sie sind ein beliebtes Ziel für Cyberattacken und sollten daher so viele Sicherheitsebenen wie möglich effektiv umsetzen. Einige Security-Anbieter, wie der Security Spezialist DriveLock, sind diesem Bedarf nachgekommen und bieten entsprechende Lösungen, die das Sicherheitsbewusstsein von Mitarbeitenden fördern und ausbauen.

In diesem Beitrag zeigen wir am Beispiel eines Krankenhauses, wie der Einsatz einer solchen Lösung in der Praxis aussehen kann. Krankenhäuser und Kliniken waren in den vergangenen Jahren besonders stark von Cyberattacken betroffen.

Security Awareness am Beispiel Krankenhaus

Das Krankenhaus eignet sich besonders gut zur Veranschaulichung, weil es gleich mehrere Herausforderungen angehen muss.

KRANKENHÄUSER UND KLINIKEN:

- sind einem erhöhten Cyberrisiko ausgesetzt. Beispielsweise wurden der Klinikverbund „Medizin Campus Bodensee" im Januar 2022, wenige Monate zuvor das Klinikum Dessau (September 2021), oder die Uniklinik Düsseldorf (September 2020) bereits Opfer von Cyberangriffen.
- sind KRITIS-Organisationen beziehungsweise müssen auch unabhängig von ihrer Größe IT-Sicherheit nach dem aktuellen Stand der Technik umsetzen.
- müssen daher Regularien erfüllen wie den Branchenspezifischen Sicherheitsstandard (B3S).
- verwalten eine Vielzahl vernetzter medizinischer Geräte, die jederzeit online und einsatzfähig sein müssen (ähnlich Industrial IoT). Gleichzeitig wird Telemedizin immer häufiger eingesetzt.
- verfügen über Personal, das nicht immer über ausreichendes IT-Wissen verfügt. Zudem ist es schwierig, dieses Wissen aufzubauen aufgrund von Schichtarbeit, Personalrotation, einem stark ausgelasteten Arbeitsalltag und daraus folgend einem mangelnden Austausch zwischen IT-Teams und Klinikpersonal.
- können als öffentliche Gebäude den Zugang nicht einfach einschränken wie Privatunternehmen. Das heißt, der Zugang zu nicht gesperrten Computern und damit Zugang zu sensiblen Daten ist für böswillige Akteure einfacher.
- haben viele E-Mail-Adressen in öffentlichen Verzeichnissen. Gezieltes Phishing (Spear-Phishing) oder CEO Fraud sind daher einfacher umzusetzen.
- müssen sich schützen trotz geringer Budgets für IT-Sicherheit und fehlenden IT-Fachkräften.

Wie kann Security Awareness zum Cyberschutz beitragen?

Das Ziel einer guten Sensibilisierung für IT-Sicherheit ist, das Bewusstsein für die Gefahren im Netz zu erweitern und gleichzeitig eine nachhaltige Verhaltensänderung, also eine Kultur der Cybersicherheit zu schaffen – ergänzend zu technischen Sicherheitslösungen. Darüber hinaus helfen Security-Awareness-Lösungen, gesetzlich vorgeschriebene Trainings oder andere Compliance-Vorgaben umzusetzen. Sowohl die DSGVO als auch B3S schreiben diese in regelmäßigen Abständen für Führungskräfte und Mitarbeitende vor. Letztlich geht es immer darum, Menschen und Systeme vor Cyberangriffen zu schützen. Die Sensibilisierung der Belegschaft für Cybersicherheit im Alltag verbessert das Schutzniveau fast exponentiell.

Zurück zum Fallbeispiel: Vor allem in Krankenhäusern und Kliniken passiert es, dass aufgrund des Drucks und der Notwendigkeit, dringende medizinische Versorgung zu leisten, medizinische Fachkräfte gegebenenfalls gute Security-Praktiken aufgeben, um die Patienten zu versorgen (ENISA Procurement Guidelines for Cybersecurity in Hospitals, S. 19). So werden in der Praxis Passwörter sichtbar notiert, damit sie schnell gefunden werden oder medizinische Geräte nicht ausgeloggt und sind damit frei zugänglich. Via E-Mail werden mit einer Vielzahl von anderen Einrichtungen auch sensible Daten ausgetauscht und verdächtige E-Mails eher zugelassen und geöffnet, weil sie wichtige Informationen für die Patientenversorgung enthalten könnten.

Aus diesen Gründen ist das Zusammenspiel von Technologie und Mensch sehr wichtig. Die Kreativität und das kritische Denken des Menschen können Spam- und Phishing-Angriffe besser erkennen und abwehren als jedes noch so intelligente Tool. Schlüpft eine Phishing-Mail durch das Sicherheitsnetz, können sensibilisierte und aufmerksame Empfänger diese identifizieren.

1. Für eine erfolgreiche Einführung einer Security-Awareness-Lösung sollte das Krankenhaus daher folgende acht Faktoren beachten:

1. Security Awareness braucht das Buy-in der Führungsebene.
2. Die Lösung sollte fester Bestandteil einer ganzheitlichen Security-Strategie sein.
3. Die Verantwortung liegt bei den Security-Verantwortlichen (CISOs o.ä. Rollen), vor allem im Zusammenhang mit Zertifizierungen, Audits, Maturity Models.
4. Idealerweise sollte das Thema abteilungsübergreifend in Zusammenarbeit mit HR und weiteren Verantwortlichen für Personalentwicklung getrieben werden.
5. Natürlich muss das gesamte Personal bei der Entwicklung des Security-Awareness-Programms einbezogen werden, um alle potenziellen Risikoszenarien einzubeziehen.
6. Der Fokus muss auf den Menschen liegen, die die Systeme jeden Tag in Anspruch nehmen (People-centric Approach).
7. Zunächst muss ein Problembewusstsein für Cybersicherheit geschaffen werden. Daher sollten sich Trainingseinheiten auch inhaltlich am Alltag und den Prioritäten der Zielgruppe ausrichten. Dazu rät auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinen Cybersicherheits-Empfehlungen zu Awareness.
8. Pädagogisch durchdachte und interaktive Schulungseinheiten sind wichtig: Die Lösung sollte Microlearning, spielerische Aspekte (Gamification) und ähnliches umfassen, damit Mitarbeitende motiviert bleiben und eine nachhaltige Verhaltensänderung erreicht wird.

2. Was macht den erfolgreichen Einsatz von Security Awareness im Arbeitsalltag aus?

Wichtig ist vor allem, dass das Sensibilisierungs-Programm nicht nur als eine Checkbox für Audits betrachtet, sondern gewissenhaft und mit Nachdruck umgesetzt wird. Am effektivsten sind die Initiativen, die moderne Lernmethoden anwenden und das Interesse der Anwender und Anwenderinnen wecken. Daher sind die bereits erwähnten Gamification-Ansätze oder kurzweilige Formate wie Videos oder ein Quiz sinnvoll, damit Anwender motiviert bleiben. Eine Grundvoraussetzung dafür ist, dass diese Trainings in einem angstfreien Raum stattfinden. Die Belegschaft sollte keine negativen Konsequenzen fürchten müssen, wenn sie während der Schulung Fehler macht. Der Fokus liegt stets auf dem Lerneffekt und einer nachhaltigen Verhaltensänderung. Für ersteres sind kurze, anlassbezogene Erinnerungen im Alltag sowie regelmäßiges Wiederholen sinnvoll.

3. Die Ergebnisse einer erfolgreichen Security-Awareness-Lösung

Die messbaren Ergebnisse sehen bei einem erfolgreichen Zusammenspiel von Mensch und Technologie wie folgt aus:

- Geringere Klickraten bei Phishing-Mails
- Transparenz für Verantwortliche, etwa via Dashboards über den Awareness-Status und -Fortschritt der Mitarbeitenden durch anonymisierte Kurztests.
- Verantwortliche können jederzeit den aktuellen Risk Score sehen.
- Security ist in der DNA der Organisation verankert.
- Das Personal ist für mehr Cybersicherheit motiviert und befähigt.

Laut dem Bayerischen Landesamt für Sicherheit in der Informationstechnik sollten Security-Awareness-Maßnahmen in der Praxis folgende Punkte aufgreifen:

- Grundlagen der Informations- und Datensicherheit (Rechtsnormen, DSGVO, BDSG, § 35 SGB I, § 30 AO)
- Sensibilisierung hinsichtlich der Zugangskontrolle zu Gebäuden und Gebäudeteilen
- Sicheres Surfen im Internet
- Umgang mit E-Mails, deren Anhängen und Links
- Gefährdung durch Phishing-Angriffe
- Umgang mit Passwörtern (Aufbau, Richtlinien, Vertraulichkeit)
- Schadsoftware und deren Verbreitungs- und Bedrohungspotenzial
- Aufbewahrung und Zugriffsschutz von (mobilen) Datenträgern
- Bedrohung durch Nutzung nicht zugelassener Software
- Social Engineering
- Verhalten beim Erkennen von Gefahren und sicherheitsrelevanten Ereignissen

Das Ziel von Security Awareness ist es, den Faktor Mensch zu einem festen Bestandteil einer langfristigen IT-Sicherheitsstrategie und somit zu einem entscheidenden Security-Vorteil zu entwickeln. Es handelt sich dabei nicht um eine einmalige Aktion, sondern vielmehr einen stetigen Prozess, um eine verantwortungsbewusste, sichere Unternehmenskultur zu etablieren. So tragen Security-Awareness-Lösungen dazu bei, User und Systeme mit dem richtigen Zusammenspiel von Technologien und dem Intellekt des Menschen vor Cyberbedrohungen zu schützen.

Andreas Fuchs

LESSONS LEARNED AUS ECHTEN CYBERANGRIFFEN

7 TIPPS, MIT DENEN SIE IHR UNTERNEHMEN BESSER SCHÜTZEN

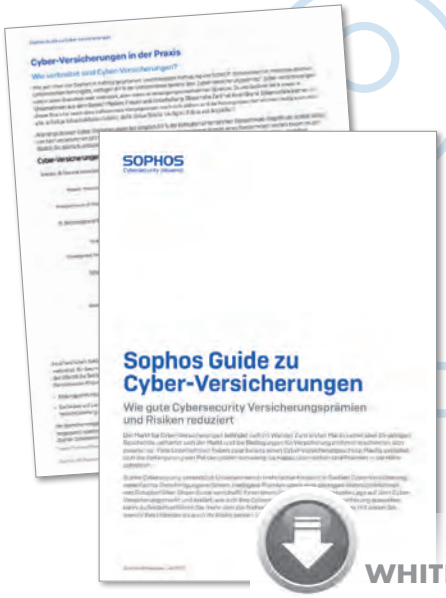
Rob Collins, Specialist Systems Engineer für Sophos Managed Threat Response und Rapid Response, hat in diesem Whitepaper die Sieben wichtigsten Erkenntnisse von Unternehmen zusammengefasst, die von Cyberangriffen betroffen waren. Aus diesen Erkenntnissen abgeleitet werden sieben Tipps, mit denen Sie Ihr Unternehmen besser schützen können und so vermeiden, selbst Opfer eines Angriffs zu werden. Dabei sind die meisten dieser Vorschläge ganz ohne die Anschaffung von Tools umsetzbar.

WHITEPAPER DOWNLOAD

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

GUIDE ZU CYBER-VERSICHERUNGEN

WIE GUTE CYBERSECURITY VERSICHERUNGSPRÄMIEN UND RISIKEN REDUZIERT



Der Markt für Cyber-Versicherungen befindet sich im Wandel: Zum ersten Mal in seiner über 15-jährigen Geschichte verhärtet sich der Markt und die Bedingungen für Versicherungsnehmer erschweren sich zusehends. Viele Unternehmen haben zwar bereits einen Cyber-Versicherungsschutz, häufig gestaltet sich die Verlängerung von Policen jedoch schwierig, da Kapazitäten sinken und Prämien in die Höhe schnellen.

Starke Cybersecurity unterstützt Unternehmen in mehrfacher Hinsicht in Sachen Cyber-Versicherung: vereinfachte Genehmigungsverfahren, niedrigere Prämien sowie eine geringere Wahrscheinlichkeit von Schadenfällen.

Gut zu wissen

Der Guide verschafft Ihnen einen Überblick über die aktuelle Lage auf dem Cyber-Versicherungsmarkt und erklärt, wie sich Ihre Cybersecurity positiv auf Ihre Versicherung auswirken kann. Außerdem erfahren Sie mehr über die Technologien und Services von Sophos, mit denen Sie sowohl Ihre Prämien als auch Ihr Risiko senken können.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 10 Seiten und steht kostenlos zum Download bereit. ***www.it-daily.net/download***

CREDENTIAL STUFFING

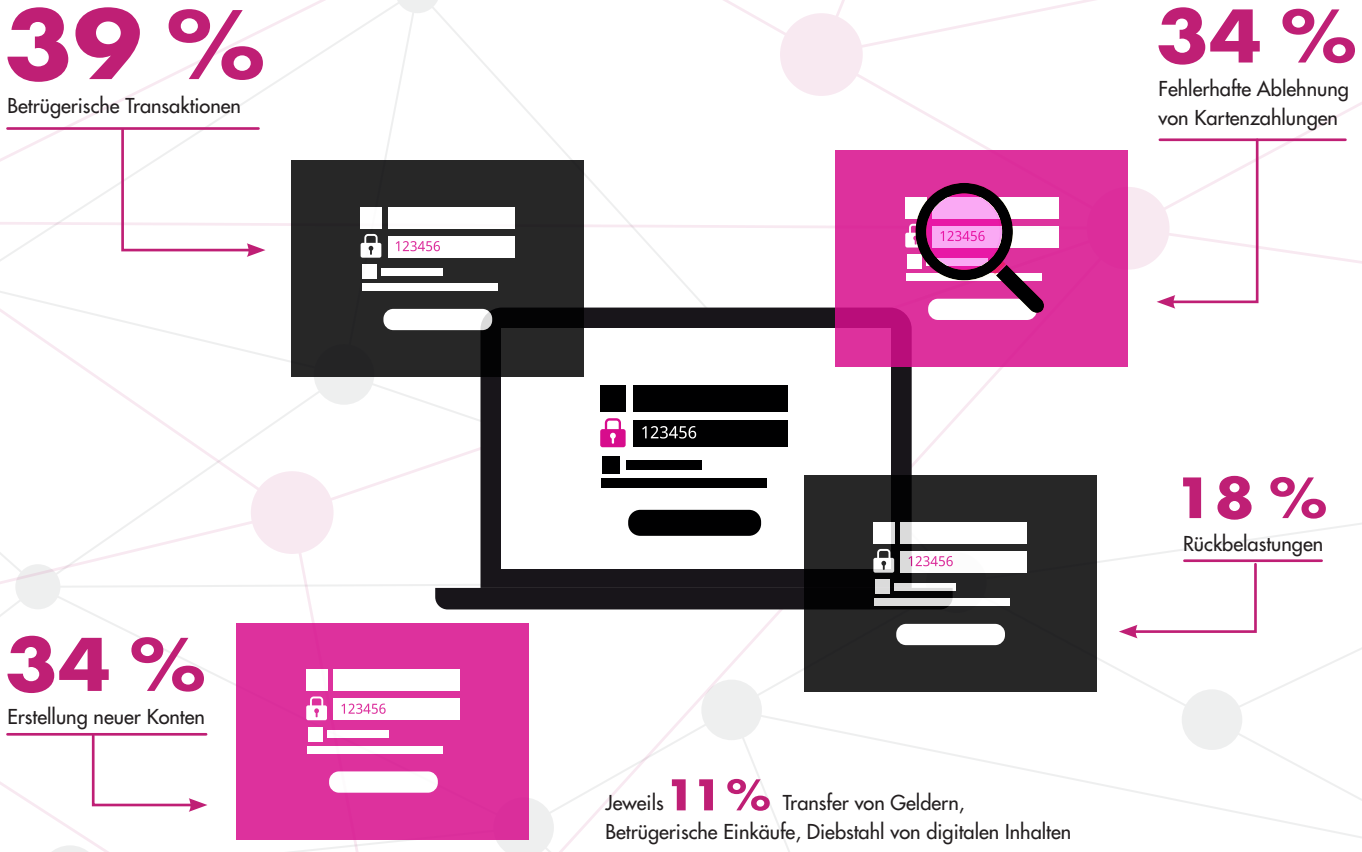
PASSWORTLOS SICHERER UNTERWEGS

Ransomware-Attacken und DDoS-Angriffe gehören mittlerweile zu den Standardverfahren im Bereich Cyber-Crime. Ein Thema das in den letzten Jahren zunehmend in den Mittelpunkt gerückt ist, ist Credential Stuffing. Was bedeutet das und wie kann man sich davor schützen - darüber sprach it security mit Stephan Schweizer, CEO bei Nevis Security.

it security: *Herr Schweizer, bei Credential Stuffing handelt es sich um eine Betrugsmasche, die sich einer zunehmenden Beliebtheit erfreut. Was genau versteht man aber darunter und wie läuft so ein Angriff ab?*

Stephan Schweizer: Unter Credential Stuffing versteht man das hochautomatisierte Durchprobieren von bekannten Username / Passwort Kombinationen gegen Webportale. Die Username / Passwort Kombinationen werden als sogenannte Combo-Lists im Darknet gekauft, die Daten stammen entweder aus Data Breaches oder Phishing-Attacken. Aktuelle Schätzungen gehen davon aus, dass zurzeit ca. 3,3 Milliarden solcher

KONSEQUENZEN ERFOLGREICHER KONTOÜBERNAHMEN FÜR AUSGEWÄHLTE B2C-KATEGORIEN:



(Quelle: Aberdeen Strategy Research; Quantifizierung der Auswirkungen von Credential Stuffing und Kontoübernahmen für 10 B2C-Kategorien in der EMEA-Region, Januar 2022)

Username / Passwort Kombinationen zum Verkauf angeboten werden. Diese Combo-Lists werden anschließend auf speziellen Hacking-Tool-Suiten eingespielt, welche als SaaS Service ebenfalls im Darknet gemietet werden können. Dahinter verbirgt sich typischerweise ein Bot-Netzwerk, das dann die ausgewählten Ziele über einen verteilten Ansatz angreift, indem die Credential-Kombinationen durchprobiert werden. Da die Anfragen von verschiedenen Clients mit relativ tiefer Kadenz erfolgen, sind die Attacken für das angegriffene Webportal gar nicht so einfach zu erkennen. Je nach Aktualität der verwendeten Combolist liegt die Erfolgsrate der Angriffe bei circa 0,5 bis 3 Prozent. Das klingt auf den ersten Blick nach wenig – wenn aber zum Beispiel eine Combolist mit 1 Million Einträgen verwendet wird, so wird der Angreifer Zugriff auf etwa 5.000 bis 30.000 Accounts erhalten. Die erwähnten Tool-Suiten enthalten dann typischerweise auch maßgeschneiderte Tools, welche im Erfolgsfall direkt eine Transaktion oder eine Angriffs-Aktion auslösen. Dies natürlich zum Schaden des betroffenen Endbenutzers.

it security: *Warum ist bei Cyberkriminellen ausgerechnet Credential Stuffing so beliebt?*

Stephan Schweizer: Die Beliebtheit beruht auf der Tatsache, dass die Attacken hochautomatisiert und großflächig ausgeführt werden können. Zudem ist das Risiko für den Angreifer relativ gering, bei gleichzeitig sehr guten Erfolgs- und Gewinnaussichten. Daher lohnt es sich für die Angreifer auch, die Automatismen laufend zu optimieren und sich neue Ziele zu suchen.

it security: *Welche Schäden verursachen Credential Stuffings beziehungsweise Account Takeovers?*

Stephan Schweizer: Wir haben dies im Rahmen einer repräsentativen Studie in Zusammenarbeit mit Aberdeen Research untersucht. Die Studie erstreckt sich über 10 Branchen (Finanzindustrie, E-Commerce, Telekom, Online Gambling). Zusammengefasst lässt sich sagen, dass das Problem größer ist, als wir ursprünglich vermutet hatten: 84 Prozent der Befragten gaben an, dass ihre Organisation im Verlauf der letzten 12 Monate nachgewiesene Fälle von Account Takeovers zu beklagen hatten. Die daraus resultierenden direkten und indirekten Schäden erreichen für die betroffenen Unternehmen schnell einmal mehrere Millionen pro Jahr. Natürlich hängt der absolute Betrag stark davon ab, wie viel Umsatz über den Online-Kanal erzielt wird. Im Fall von Finanzinstituten hat die Studie beispielsweise gezeigt, dass die Schäden zwischen 2,7 und 7,5 Prozent des jährlichen Online-Umsatzes ausmachen können - das sind substanzielle Beträge, die nicht einfach als „cost of doing business" abgehakt werden können. Außerdem gilt es zu berücksichtigen, dass ein Account Takeover für den betroffenen Kunden und Endbenutzer ein schon fast traumatisches Erlebnis sein kann. Die Gefahr, dass ein solcher Benutzer zur Konkurrenz abwandert, ist daher sehr groß. Das belegen auch die Zahlen unserer Studie.

DER FLÄCHENDECKENDE ERSATZ DES PASSWORTES DURCH ALTERNATIVE VERFAHREN IST DIE EINZIGE LÖSUNG, UM DAS PROBLEM NACHHALTIG IN DEN GRIFF ZU BEKOMMEN.

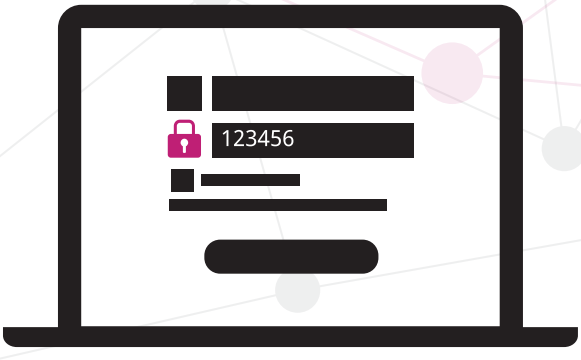
Stephan Schweizer, CEO, Nevis Security, www.nevis.net

it security: *Besonders die Finanzbranche leidet stark unter Account Takeovers. Warum ist gerade diese Branche so ein „leichtes" oder bevorzugtes Ziel?*

Stephan Schweizer: Die Credential Stuffing Angriffe sind primär finanziell motiviert - daher ist die Finanzbranche natürlich besonders exponiert und daher auch ein bevorzugtes Ziel. Ich würde jedoch nicht behaupten, dass die Finanzbranche generell ein leichtes Ziel ist. Gerade im DACH-Raum haben beispielsweise die meisten Banken ihre Hausaufgaben gemacht und verwenden verschiedene Formen von Multi-Faktor-Authentisierung. Anders sieht es aber teilweise im angelsächsischen Raum aus: Dort wird vielerorts E-Banking nur durch Benutzername und Passwort geschützt - eine Einladung mit rotem Teppich für Angreifer.

it security: *Eine Möglichkeit, sein Passwort zu schützen ist, erst gar keins zu verwenden und stattdessen auf Biometrie zu setzen. Der Vorteil einer biometrischen Identifikation ist klar, doch wie lässt sich das unternehmensintern umsetzen, welche Möglichkeiten gibt es?*

Stephan Schweizer: Der flächendeckende Ersatz des Passwortes durch alternati-



ve Verfahren ist in der Tat die einzige Lösung, um das Problem nachhaltig in den Griff zu bekommen. Glücklicherweise ist die Technik dafür mittlerweile vorhanden: Die FIDO-Alliance hat hier hervorragende Grundlagenarbeit geleistet, indem sie Standards in den Bereichen Authentisierungs-Protokolle, Kryptographie und Hardware geschaffen hat. Der konsequente Einsatz der FIDO-Standards ermöglicht es, das Passwort auf allen Kanälen der Kundenkommunikation (Mobile und Desktop) komplett zu eliminieren und gleichzeitig auch noch das Kundenerlebnis zu verbessern. Der FIDO-Standard ist sehr breit abgestützt; auch IT-Giganten wie Apple, Google und Microsoft unterstützen den Standard sowohl hardware- wie auch softwareseitig. Somit kann heute davon ausgegangen werden, dass der digitale Kunde bereits über Geräte verfügt, die den Einsatz von FIDO-basierten Authentisierungs-Lösungen ermöglichen. Damit kann sich das Unternehmen auf den serverseitigen Part fokussieren. Vereinfacht ausgedrückt funktioniert FIDO dann wie folgt: Bei der Registrierung wird auf dem FIDO-fähigen Gerät des Endbenutzers ein Schlüsselpaar generiert. Der private Schlüssel wird sicher auf dem Gerät in einem speziell dafür vorgesehenen Chipset gespeichert, der öffentliche Schlüssel wird über das FIDO Protokoll an die Serverseite übermittelt. Die Rolle der Biometrie besteht in der Folge darin, den privaten Schlüssel auf dem Gerät während eines Authentisierungs-Prozesses freizuschalten. Damit ist sichergestellt, dass die biometrischen Informationen das Gerät niemals verlassen - das Verfahren erfüllt somit höchste Anforderungen bezüglich Sicherheit und Datenschutz.

it security: *Wie können sich Unternehmen darüber hinaus vor dieser Art Angriffe schützen? Welche Bedeutung kommt dabei IAM- oder CIAM-Lösungen zu?*

Stephan Schweizer: Der Serverseitige Teil der FIDO Infrastruktur wird typischerweise durch das CIAM System out-of-the Box zur Verfügung gestellt. Damit fügen sich die passwortlose Authentisierung sowie die dafür benötigten Prozesse wie zum Beispiel die Geräteverknüpfung nahtlos in die bestehenden IAM-Prozesse ein. Dies ermöglicht dann auch den Parallelbetrieb sowie die schrittweise Migration bestehender Benutzer auf die passwortlose Authentisierung.

Unternehmen, die eine FIDO-basierte passwortlose Authentisierung flächig ausgerollt haben, sind umfassend gegen Credential-Stuffing Attacken geschützt. Dies aus zwei Gründen: Erstens sind die zur Authentisierung verwendeten Schlüsselpaare individuell pro Benutzer, Gerät und Web-Portal. Dies verunmöglicht großflächige Attacken, wie wir sie heute im Bereich Credential Stuffing sehen. Der zweite Grund liegt in der verwendeten asymmetrischen Verschlüsselung: Selbst wenn es einem Angreifer gelingen würde, die Serverseitig hinterlegten öffentlichen Schlüssel zu entwenden, so sind diese ohne die an die Geräte gebundenen privaten Schlüssel absolut wertlos.

it security: *Anhand von künstlicher Intelligenz können Betrugsversuche ermittelt werden. Wie schnell kann nach so einer Meldung dann tatsächlich gehandelt werden, wie hoch ist die Wahrscheinlichkeit, den Angriff noch abzuwehren?*

Stephan Schweizer: AI-basierte Ansätze welche zum Beispiel das Tippverhalten

des Benutzers berücksichtigen, können in der Tat helfen, Betrugsversuche zu erkennen. Diese Ansätze haben aber immer eine gewisse Unschärfe: Die Algorithmen liefern typischerweise einen Score zurück, zum Beispiel: das Tippverhalten passt zu 95 Prozent auf das bekannte Benutzerprofil. Außerdem brauchen die AI-Ansätze eine gewisse Lernphase und es muss sichergestellt werden, dass das System das Richtige lernt: So wäre ein AI-system, welches das Tippverhalten eines Angreifers gelernt hat, nicht im Sinne des Erfinders.

Wir empfehlen daher, AI-Ansätze nur begleitend und nachgelagert zu einer FIDO-basierten Authentisierung einzusetzen. So können AI-basierte Ansätze wertvolle Dienste leisten, um anders geartete Attacken wie etwa Session-Hijacking zu erkennen. In solchen Fällen muss das System in Echtzeit und anhand von definierten Schwellenwerten entscheiden können. Wenn zwischen Erkennung und Reaktion des Systems zu viel Zeit (mehr als 5 Sekunden) verstreicht, ist es in der Regel schon zu spät.

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

CYBERKRIMINALITÄT

GEDRÄNGEL IM FIRMENNETZ

Studien, Whitepaper und Meinungsbeiträge im Bereich der Security lassen Leserinnen und Leser oft damit alleine, den Nutzen für sich und das Unternehmen zu ziehen. Genau aus diesem Grund stellt Sophos den Sicherheitsteams in Unternehmen das neue Active Adversary Playbook 2022 zur Verfügung. Das Playbook beschreibt einerseits genau, wie Cyberkriminelle bei ihren Angriffen vorgehen und zeigt andererseits konkrete Wege auf, wie schädliche Aktivitäten im Netzwerk erkannt und abgewehrt werden können.

IN EINER ZUNEHMEND DYNAMISCHEN UND SPEZIALISIERTEN CYBER-BEDROHUNGSLANDSCHAFT IST ES FÜR VIELE UNTERNEHMEN SCHWIERIG, MIT DEN SICH STÄNDIG ÄNDERNDEN TOOLS UND METHODEN DER ANGREIFENDEN SCHRITT ZU HALTEN.

Michael Veit, Technology Evangelist, Sophos Technology GmbH, www.sophos.de

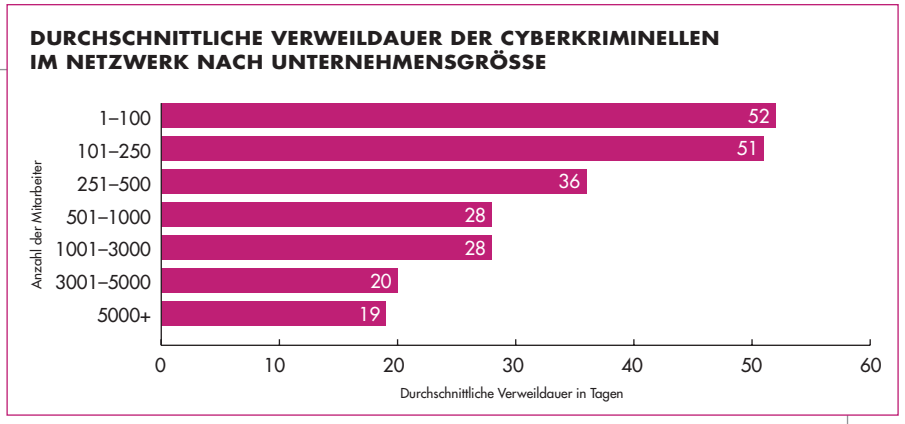
Cyberkriminalität heute

Das Active Adversary Playbook 2022 beschreibt das Verhalten von Cyberkriminellen, wie es das Rapid Response Team von Sophos im Laufe des Jahres 2021 bei konkreten Fällen beobachtet hat. Dabei haben die Experten neben vielen anderen Parametern auch die Verweildauer der Cyberkriminellen in den Netzwerken analysiert: Die Untersuchungen zeigen einen drastischen Anstieg der Verweildauer um 36 Prozent wobei der durchschnittliche, unentdeckte Aufenthalt im Netzwerk bei 34 Tagen liegt. Schuld daran sind unter anderem die ProxyShell-Schwachstellen in Microsoft Exchange, die dem Sophos Rapid Response Team zufolge von Initial Access Brokern (IABs) ausgenutzt werden, um in Netzwerke einzudringen und den Zugang dann an andere Cybergangster zu verkaufen.

„Initial Access Broker haben eine neue Cybercrime-Industrie entwickelt, indem sie in ein Ziel eindringen, es auskundschaften oder eine Backdoor installieren. Den quasi schlüsselfertigen Zugang verkaufen sie dann an Ransomware-Banden, die dies als Grundlage für die eigenen Angriffe nutzen. In einer zunehmend dynamischen und spezialisierten Cyber-Bedrohungslandschaft ist es für viele Unternehmen schwierig, mit den sich ständig ändernden Tools und Methoden der Angreifenden Schritt zu halten. Es ist wichtig, dass sie wissen, worauf sie in jeder Phase der Angriffskette achten müssen, damit sie Angriffe so schnell wie möglich erkennen und neutralisieren können“, erklärt Sophos Security-Experte Michael Veit.

Unterschiedliche Branchen, unterschiedliche Verweildauer

Die Untersuchungen von Sophos zeigen auch, dass die Cyberkriminellen in kleineren Unternehmen länger verweilen als in größeren Unternehmen. Bei Unternehmen mit bis zu 250 Beschäftigten sind es etwa 51 Tage. In Unternehmen mit 3.000 bis 5.000 Beschäftigten sind es in der Regel „nur“ 20 Tage. Einen Sonderfall stellen Ransomware-Attacken dar.



Traditionelle Abwehr ist moderner Cyberkriminalität nicht gewachsen

Ein wichtiger Aspekt im neuen Playbook ist die zunehmende Etablierung von sogenannten IT-Sicherheit-Ökosystemen – eine Strategie, die Sophos mit seinem Adaptive Cybersecurity Ecosystem (ACE) realisiert. Dieses basiert auf den gesammelten Bedrohungsdaten der Sophos-Labs, Sophos Security Operations (menschliche Analysten, die über das Sophos Managed Threat Response-Programm in Tausenden von Kundenumgebungen eingebunden sind) und Künstlicher Intelligenz (KI). In einem einzigen, integrierten Data Lake sind Informationen aus allen Lösungen und Threat Intelligence-Quellen zusammengefasst. Echtzeit-Analysen ermöglichen es Verteidigern, Einbrüche zu verhindern, indem sie verdächtige Signale finden. Parallel dazu ermöglichen offene APIs Kunden, Partnern und Entwicklern, Tools und Lösungen zu entwickeln, die mit dem System interagieren. Alles wird zentral verwaltet über die Sophos Central Management-Plattform.

„Dass an wirkungsvollen Security Ecosystemen kein Weg vorbei geht, zeigt unsere Forensik anhand weiterer erschreckender Daten", ergänzt Veit. „Durch die Kombination ungepatchter ProxyLogon- und ProxyShell-Schwachstellen und dem Aufkommen von IABs sehen wir verstärkt, dass sich gleich mehrere Angreifer in ein und demselben Ziel-Netzwerk befinden und um Zugänge, Informationen, Daten oder im schlimmsten Fall um Lösegelder konkurrieren."

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 19 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/Download

SECURITY 360

JÄHRLICHER SICHERHEITSREPORT

Zu Beginn der weltweiten Pandemie sahen sich Unternehmen mit der schwierigen Aufgabe konfrontiert, die Kontinuität des Geschäftsbetriebes sicherzustellen. Gleichzeitig musste der Übergang zu einer hybriden oder vollständig ferngesteuerten Arbeitsumgebung im Handumdrehen gewährleistet werden. Zwei Jahre später hat sich die Arbeitsumgebung weitgehend auf Remote-Technologien und Cloud-basierte Software umgestellt. Wie hat sich das auf die Sicherheitslage von Unternehmen ausgewirkt?

Der jährliche Sicherheitsreport befasst sich mit fünf wichtigen Sicherheitstrends und deren Auswirkungen auf Unternehmen weltweit. Er gibt praktische Tipps für die Konfiguration von Unternehmenstools. User profitieren dadurch auch im Jahr 2022 von einer schnellen und sicheren Konnektivität.

ÜBER VERTRAUEN UND TRANSPARENZ

KASPERSKY LEGT ALS EINZIGER ANBIETER SEINEN QUELLCODE OFFEN

Der anhaltende Krieg in der Ukraine hat die Welt, wie wir sie kennen, erschüttert. Neben dem menschlichen Leid im Kriegsgebiet spüren wir alle die wirtschaftlichen, politischen und sozialen Auswirkungen. Bei Kaspersky sind wir überzeugt davon, dass der friedliche Dialog das einzig mögliche Instrument zur Lösung von Konflikten ist. Krieg ist für niemanden gut.

Auch wir sind direkt von der geopolitischen Lage betroffen. Seit 25 Jahren schützt unser privat geführtes, internationales Cybersicherheitsunternehmen Kunden und Partner auf der ganzen Welt vor Cyberbedrohungen, unabhängig von deren Herkunft. Der Krieg hat uns in ein anderes Licht gerückt. Besonders schmerzhaft trifft uns die Warnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vor der Nutzung von Kaspersky-Virenschutzprodukten; diese beruht nicht auf technischen, sondern auf geopolitischen Gründen.

SOC 2-Audit und ISO 27001-Zertifizierung

Seit jeher legen wir bei Kaspersky großen Wert auf Transparenz, Vertrauen, Sicherheit und Integrität. Externe Audits von unabhängigen und anerkannten Organisationen weisen die Sicherheit und Zuverlässigkeit unserer Produkte und Praktiken nach. So hat Kaspersky im April 2022 erneut das Typ-1-SOC-2-Audit erfolgreich bestanden [1]. Dies belegt, dass unsere Antivirus-Datenbanken durch starke Sicherheitsmaßnahmen vor unbefugten Änderungen geschützt sind.

Wir sind zudem seit 2020 nach ISO/IEC 27001: 2013, dem international anerkannten Best-Practice-Industrie- und Sicherheits-Standard, zertifiziert [2] und haben diese Zertifizierung im Februar 2022 erneuert [3]. Damit bestätigt TÜV AUSTRIA, dass unsere Datensicherheitssysteme, einschließlich des Kaspersky Security Network, den besten Datensicherheitspraktiken der Branche entsprechen.

Unser Engagement für Vertrauen und Transparenz

Des weiteren haben wir als erstes Unternehmen unserer Branche mit unserer Globalen Transparenzinitiative [4] schon seit 2017 und als erster Cybersicherheitsanbieter überhaupt konkrete Maßnahmen ergriffen, die auf eine noch größere Datensicherheit, stärkere Transparenz, mehr Vertrauen und Integrität sowie Sicherheit allgemein einzahlen. Kaspersky hat weltweit vier Transparenzzentren eröffnet, um Sicherheitsbedenken gemeinsam mit Kunden, vertrauenswürdigen Partnern und Regierungsvertretern auszuräumen, indem vor Ort oder per Remote-Zugang unser Quellcode, Software-Updates und die Regeln zur Erkennung von Bedrohungen unabhängig überprüft werden können; die Datenverarbeitung von Nutzern unter anderem aus Europa, und damit auch Deutschland, findet in Rechenzentren in Zürich statt.

Menschen, Mitarbeiter und internationale Community

Kaspersky ist ein globales Unternehmen, das in rund 200 Ländern mit 34 Niederlassungen tätig ist. Der Sitz der Holding als Oberste Konzerngesellschaft befindet sich in Großbritannien. Unsere Server sind auf der ganzen Welt verteilt (einschließlich der Schweiz, Deutschland, China und Kanada); dadurch können wir Informationen schneller verarbeiten und die Verfügbarkeit der Server jederzeit gewährleisten. Wir engagieren uns sowohl global als auch lokal für Cybersicherheit und arbeiten daher mit internationalen Strafverfolgungs- und Regierungsorganisationen [5] wie INTERPOL im Kampf gegen Cyberkriminalität zusammen.

Christian Milde

Literatur

[1] https://www.kaspersky.com/about/compliance-soc2
[2] https://www.kaspersky.de/about/press-releases/2020_kaspersky-erhaelt-iso-27001-zertifizierung
[3] https://www.kaspersky.de/about/press-releases/2022_kaspersky-erhalt-rezertifizierung-durch-den-tuv-austria
[4] https://www.kaspersky.de/about/transparency
[5] https://www.kaspersky.com/about/law-enforcement-cooperation

KI-GESTÜTZTE HELFER

CYBERSICHERHEIT IN KOMPLEXEN NETZWERKEN ERHÖHEN

Die Komplexität in IT-Netzwerken wird in den kommenden Jahren weiter massiv wachsen. Für das menschliche Gehirn ist sie kaum noch zu durchdringen. Für die Cybersicherheit wird dies immer mehr zum Problem. Mit erweiterten Methoden der Künstlichen Intelligenz (KI) und des Machine Learning (ML) kann das Chaos im Netzwerk auch langfristig beherrscht werden.

Beim Thema KI in der Cybersicherheit muss zwischen Hype und tatsächlich wirksamen Methoden unterschieden werden. Gemeinsam mit ihren Forschungspartnern erforscht die genua GmbH im BMBF-geförderten Forschungsprojekt Wintermute[1], wie IT-Administratoren mittels verschiedener KI- und ML-gestützter Methoden realistisch unterstützt werden können, um die IT-Sicherheit in Organisationen zu erhöhen. Dabei werden drei wesentliche Probleme adressiert:

- die Lagebeurteilung im Netzwerk – Klassifizierung des Systemverhaltens sowie Rückmeldung über Auffälligkeiten,
- die Policy Definition – individuelle Regelerstellung,
- die Durchsetzung von Sicherheit in komplexen Netzen.

Insbesondere die Nutzerfreundlichkeit (Usability) gewinnt dabei weiter an Bedeutung, denn es geht darum, hochgradig vernetzte Systeme besser zu verstehen um Risikoanalyse und -management sowie die Bedienbarkeit zu vereinfachen. Ziel ist es, den IT-Administrator dabei zu unterstützen, geeignete Regeln und Sicherheitspolicies festzulegen. KI soll außerdem helfen, den Umgang mit dynamischen Veränderungen im Netz zu erleichtern. Dabei wird kein komplett automatisches System für die Netzwerksicherheit angestrebt, sondern es sollen Technologien geschaffen werden, die dem Administrator als Unterstützung dienen.

Herausforderungen für die IT

Keine Organisation betreibt den Aufwand der IT zum Selbstzweck. Die Digitalisierung der Geschäftsprozesse und damit der Wertschöpfung wird durch „die IT" bereitgestellt und ermöglicht. Die Ziele der IT sind damit die Ziele des Unternehmens. Die Risiken des Unternehmens sind damit allerdings auch stark von den Risiken der IT beeinflusst (siehe Bild 1). Speziell der Ressourcenmangel in der IT, besonders in der IT-Sicherheit, macht dabei vielen Unternehmen zu schaffen. Generell fehlt es an Personal und Wissen, um den Herausforderungen der Zeit gut gewappnet zu begegnen.

Die Computernetzwerke der IT dienen dazu, die Geschäftsprozesse der Organisationen zu stützen. Die Komplexität der heutigen Geschäftsprozesse schlägt sich damit in der Komplexität der IT-Systeme und Netzwerke nieder. Damit wird es für System- und Netzwerkadministratoren immer schwerer, den Überblick zu behalten – häufig ist dieser verloren gegangen. Auch für neue Kollegen oder Consultants, die für eine kurze Zeit unterstützen sollen, ist es fast unmöglich, sich kurzfristig Überblick über ein Netzwerk zu verschaffen. Damit ist aber auch der Überblick über die Risiken nicht mehr gegeben; ein Zustand, der für verantwortungsvoll geführte Unternehmen nicht haltbar ist.

Den Überblick über Assets und Prozesse behalten

Um wirksame Maßnahmen der Risikominimierung zu betreiben, braucht es einen Überblick über die Prozesse und Assets eines Unternehmens, in der IT also über das Netzwerk und seine Geräte. Nur wer die eigenen Assets kennt,

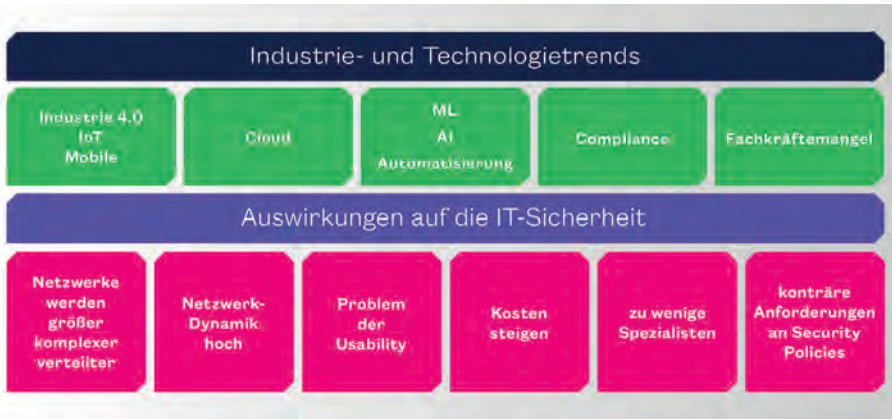


Bild 1. Übersicht aktueller Markt- und Technologietrends sowie ihre Auswirkungen auf die IT-Sicherheit. Beispielsweise entstehen durch das Internet of Things komplexe, stark verteilte, dynamische Kommunikationsnetzwerke.

1 Im Verbund der Forschungspartner übernimmt Genua die Rolle des Konsortialführers. Projektpartner sind die Universitäten Bamberg, Bremen und Würzburg. Weitere Partner sind das Bundesamt für Sicherheit in der Informationstechnik (BSI), acs plus, DB Systel, IsarNet Software Solutions, Renk und Xitaso.

kann passende Maßnahmen der Strukturierung und Risikominimierung einführen und auf ihre Wirksamkeit hin prüfen. Und nur wenn der Administrator den Überblick über die real vorhandenen Assets hat, kann er Abweichungen zwischen dem Soll-Zustand und realem Ist-Zustand erkennen und angemessen handeln. Solche Abweichungen können viele Ursachen haben, von historisch gewachsenen Zuständen über Fehlkonfigurationen bis hin zu bewussten Angriffen durch Dritte.

Das ISMS und die tägliche Arbeit des Administrators

Frameworks wie ein Informationssicherheitsmanagementsystem (ISMS) nach ISO27001 oder der IT-Grundschutz bieten den geeigneten Rahmen für ein strukturiertes Vorgehen zur Erfassung, Einschätzung und Behandlung von Risiken und notwendigen Maßnahmen. Der Netzwerkadministrator steht dabei vor der Herausforderung, dass er die theoretischen Vorgaben des ISMS im realen Netzwerk umsetzen muss. Dafür sind die real existierenden Geräte (Assets) im Netzwerk zu finden und zu bestimmen. KI-gestützte Werkzeuge für die interne Netzwerksicherheit wie der cognitix Threat Defender unterstützen den Menschen an dieser Stelle mit einer Analyse des Netzwerkverkehrs und der Erkennung der Assets. Die Kommunikationspfade im Netzwerk und das Kommunikationsverhalten liefern Informationen über die Art und Funktion der vorhandenen Geräte, sodass eine Klassifizierung stattfinden kann. Als Basis für eine einheitliche Klassifizierung dient das Schema des IT-Grundschutz. Bei der Klassifizierung können überraschende Erkenntnisse zu Tage treten, wenn beispielsweise die Smart-TVs in Meetingräumen richtigerweise als Webserver erkannt werden.

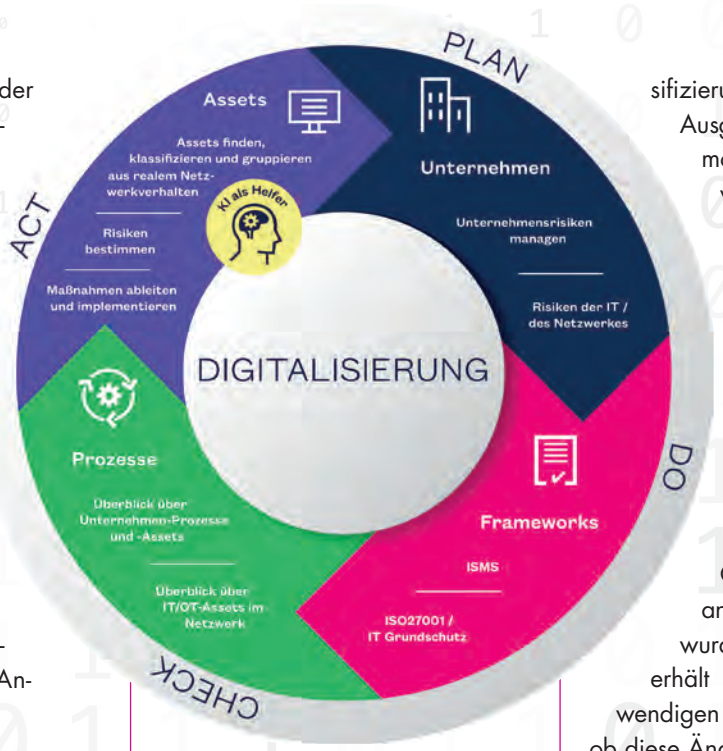


Bild 2: KI-gestütztes Vorgehensmodell für das IT- und Informationssicherheitsmanagement. Die KI als „Helfer" erlaubt die Integration von Unternehmenssicht und Realität im Netzwerk.

Bei der Klassifizierung von Geräten hilft KI in Form von Expertensystemen.

Zur einfacheren Handhabung können im nächsten Schritt die Assets gleicher Klassifizierung gruppiert werden, um sie bei technischen und organisatorischen Maßnahmen gebündelt zu behandeln. Weiterhin hilft es dem Administrator, wenn die Komplexität des Netzwerkes vereinfacht wird oder zumindest eine vereinfachte Darstellung gefunden wird.

Für die „High Value Assets", also die für das Unternehmen kritischen Prozesse und Systeme, ist eine individuelle Betrachtung einzelner Systeme oder sich gleich verhaltender Gruppen notwendig. Die weniger kritischen Systeme können häufig zu weicheren Clustern von ähnlichem Verhalten und ähnlichen Anforderungen des ISMS zusammengefasst werden. Bei diesem Clustering helfen KI-Methoden des Machine Learnings. Da für dieses Clustering neben dem Verhalten der Assets die Klassifizierung nach IT-Grundschutz als Ausgangsbasis genutzt wird, ermöglicht dies erklärbare, nachvollziehbare Cluster. Das KI-System kann damit für den Administrator nachvollziehbar darstellen, warum ein Asset Teil eines Clusters ist. Auch lässt sich erklären, welche Änderung im Verhalten eines Assets dafür gesorgt hat, dass es nicht mehr einem bestimmten Cluster und eventuell einem anderen Cluster zugeordnet wurde. Mit diesen Informationen erhält der Administrator den notwendigen Kontext, um zu entscheiden, ob diese Änderung eine Anomalie durch einen Angriff darstellt oder eine durch eine Maßnahme ausgelöste erwartete Änderung darstellt.

Die Inventarisierung und Klassifizierung sowie die Gruppen und Cluster erlauben es, das Risiko von individuellen Assets, Gruppen und Asset-Clustern anhand des real im Netzwerk vorhandenen Verhaltens der Geräte und der auftretenden Verdachtsmomente zu messen – aber auch das der gesamten Infrastruktur einer Organisation, und damit eine Grundlage für die Risikobetrachtung und die Bestimmung der Security-Posture eines Unternehmens zu liefern.

Mit dem beschriebenen, in Bild 2 illustrierten Vorgehensmodell gehen die tägliche Arbeit des Netzwerkadministrators, des Security-Experten und des ISMS Hand in Hand. Die Sicht des Unternehmens auf seine digitalen Prozesse und die damit verbundenen Risiken werden mit der realen Situation des Netzwerks verknüpft. Für den Administrator reduziert sich der Aufwand im Rahmen der Compliance-Vorgaben. Und für das Risikomanagement des Unternehmens ist sichergestellt, dass die dokumentierte Situation der Realität entspricht.

Arnold Krille | www.genua.de

SECURITY ESSEN

DIGITALER SCHUTZ IN DER SICHERHEITSBRANCHE

Nicht nur physischer, sondern auch digitaler Schutz steht im Fokus der Security Essen, die vom 20. bis 23. September 2022 in der Messe Essen stattfindet. Denn: IOT-Devices und die Internet-Anbindung von Produkten und Dienstleistungen stellen neue mögliche Angriffsziele für Cyber-Kriminelle dar. Wie sich Unternehmen, Behörden, aber auch die Industrie und Kommunen schützen können, darüber informiert die Fachmesse. In der Messehallte 8 direkt am neuen Eingang Ost werden unter anderem Advancis Software & Services, Deutsche Telekom Security GmbH und Prysm Software ihre Produkte und Dienstleistungen präsentieren.

Am ersten und zweiten Messetag sensibilisiert die Digital Networking Security Konferenz die Fachbesucher und Aussteller ganz besonders für IT-Security. Hier berichten Experten über aktuelle Vorfälle, wichtige Schnittstellen zwischen der Corporate- und IT-Security, rechtliche Vorgaben und praktische Umsetzungsbeispiele – sowohl für Sicherheitsverantwortliche in Unternehmen und Behörden als auch für Anbieter und Errichter von Sicherheitstechnik. Hacking von Gebäudenetzen ist dabei ebenso ein Thema wie IT-Sicherheit für das Sicherheitsmanagement.

Als Treffpunkt der internationalen Sicherheitsbranche bietet die Security Essen einen breiten Überblick über alle Bereiche dieses immer wichtiger werdenden Wirtschaftszweiges. Die Veranstaltung ist marktgerecht gegliedert in die Themenbereiche „Digital Networking Security", „Dienstleistungen", „Zutritt, Mechatronik, Mechanik und Systeme", „Perimeter", „Video" sowie „Brand, Einbruch und Systeme". In der Messe Essen können sich Fachbesucher auf kurzen Wegen über Neuheiten und Innovationen in der Branche informieren. Abgerundet wird die Messe durch ein thematisch passendes hochkarätiges Rahmenprogramm.

www.security-essen.de

IT SECURITY

RANSOMWARE, DDOS & SOME MORE

Wenn man die Angriffsszenarien der Hacking-Industrie betrachtet, dann fällt bei allen Mitteilungen über die ständig wachsende Anzahl an neuer Malware vor allem eines auf: Man hört viel über Phishing- und Ransomwareattacken, aber wenig über DDoS-Angriffe. Da fragt man sich, woran das liegen könnte?

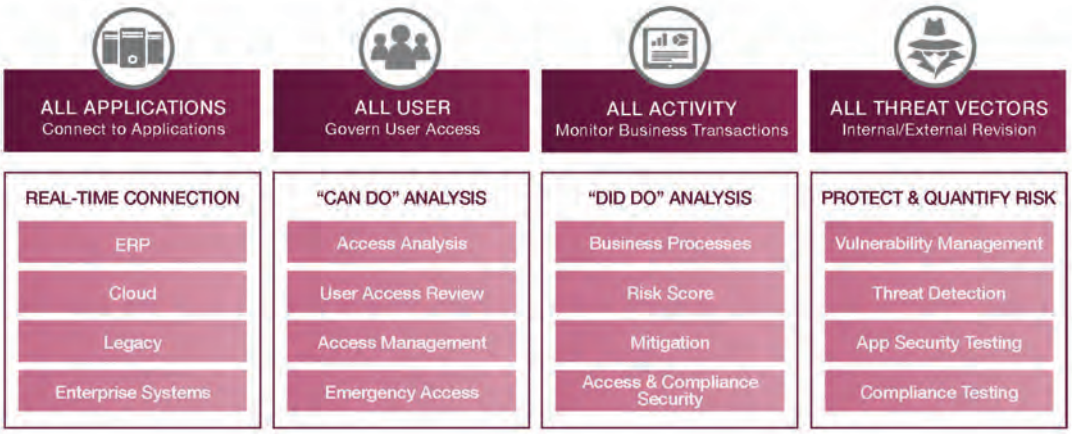
Auch dieser Industriezweig ist zunehmend von Effizienz betrieben. Warum soviel Zeit und Ressourcen verschwenden, wenn man einfacher und schneller zum Ziel kommen kann?

Mittlerweile gibt es zahlreiche Softwarelösungen, die allesamt versprechen, das Problem in Echtzeit zu verhindern. Allerdings sollte eine Verteidigungsstrategie immer mehrstufig ausgelegt sein.

Themen in diesem eBook

Container: Gefahr für die IT-Sicherheit
Im Trend: Anlassbezogenes Phishing
Zero Trust: Who are you?
Ist Ihr Browser sicher?

Das eBook umfasst 34 Seiten und steht zum kostenlosen Download bereit.
www.it-daily.net/download



SAST SOLUTIONS: NEUER PLAYER IM CYBERWAR

GLOBALE BEDROHUNGEN ERFORDERN GLOBALE ANTWORTEN

Seit Beginn des russischen Angriffskrieges stellt das BSI eine erhöhte Bedrohungslage für Deutschland fest und ruft Unternehmen, Organisationen und Behörden auf, ihre IT-Sicherheitsmaßnahmen anzupassen. Digitalminister Volker Wissing betonte beim Treffen der G7 im Mai: „Dies ist auch ein Krieg im Internet." Und weil dieser an vielen Fronten geführt werden müsse, erklärt der Security-Experte Ralf Kempf, CTO von SAST SOLUTIONS, „ist es unerlässlich, internationale Allianzen zu schmieden und neue Lösungen der IT Security zu entwickeln."

Laut Europäischer Akademie für Informationsfreiheit und Datenschutz zielen russische Angriffe verstärkt auf erneuerbare Energien als Alternativen zu russischem Gas ab. Hier gehe es nicht mehr um Daten oder finanzielle Ausbeuten, sondern um das bloße Zerstören. „Dennoch", so Ralf Kempf von SAST SOLUTIONS, die zahlreiche KRITIS-Betreiber betreuen, „wäre es sträflich, sich nur auf Attacken aus einer Richtung zu konzentrieren, denn das Gefährder-Spektrum ist international, kooperiert weltweit und respektiert keine Grenzen." Als letzten November etwa die Log4shell-Angriffswellen rollten, mischten laut Verfassungsschutz Staatshacker wie die chinesische APT 27, Phosphorus aus dem Iran, Nordkoreas Lazarus Group oder Aslan Neferler aus der Türkei mit.

„Bereits jetzt hat 2022 unmissverständlich bewiesen, dass die IT-Sicherheitsbranche sich neu und ganzheitlich aufstellen muss", betont Ralf Kempf. Auch deshalb haben sich SAST SOLUTIONS und weitere international führende Unternehmen der IT Security zur Pathlock-Gruppe formiert. Außer SAST und der aufgrund ihrer Bekanntheit namensgebenden Pathlock sind dies Appsian, Security Weaver, CSI Tools, Xpandion und QSoftware. Strategie des Verbunds mit 15 Standorten in den USA, Europa, Israel und Indien ist, die Lösungen aller Partner unkompliziert und übergreifend einzubinden, um durch vereinigte Expertise internationale Lösungen für weltweite IT-Bedrohungslagen zu bieten.

Gemeinsam wird so ein Leistungsspektrum erreicht, das tiefer und breiter ist als alle bisherigen Einzellösungen und sowohl den Bereich User Identity und Access Management als auch Cyber Security, Vulnerability Management, Threat Detection und Data Protection beinhaltet. Die neue Lösung der Pathlock-Gruppe, die den Bereich ERP Security (Enterprise Ressource Planning) als Ganzes in großer Tiefe und Expertise umfasst, deckt nun alle namhaften ERP-Anbieter ab, sei es JD Edwards, SAP, Oracle oder Salesforce.

Ein wesentliches Mindset der Pathlock-Gruppe ist dabei, dass alle Partner ihre neuen und Bestandskunden vollumfänglich selbst beraten und supporten. SAST SOLUTIONS vertreiben alle Produkte der Gruppe in der DACH-Region, sind Vertrags- und Ansprechpartner, auch im Support. Dazu Ralf Kempf: „Kunden bekommen also alles von uns aus einer Hand, und selbstverständlich gemäß Europäischer Datenschutzgrundverordnung." Für SAST SOLUTIONS und ihre Kunden bedeutet dies, mit einem umfassend erweiterten Leistungsportfolio der Automatisierung von Access Orchestration und Cyber Security sämtlicher Business Applikationen den neuen Herausforderungen gewachsen zu sein. So gelingt es, alles Schützenswerte im Land zu belassen und zu sichern – jedoch mit vereintem länderübergreifendem Knowhow und geballter internationaler Expertise.

Ralf Kempf | www.sast-solutions.de

WEIL KONTINUITÄT TRUMPF IST

CYBER SECURITY ALS GESCHÄFTSPROZESS VERSTEHEN

Die Zahl der Cyber-Attacken steigt. Dem beugen die meisten Unternehmen inzwischen vor, indem sie individuelle Security-Konzepte erarbeiten und IT-Krisenprozesse definieren. Doch sich dem Thema IT-Sicherheit einmalig zu widmen, ist nicht genug. Cyber Security ist ein fortlaufender Prozess.

Es besteht Handlungsbedarf. Bereits eigene Mitarbeiter gefährden das Unternehmen – Stichwort Social Engineering. Ein kleiner Moment der Unachtsamkeit genügt, und Mitarbeitende geben sensible Informationen preis. In jedem Falle gilt es, schnelle, überlegte Entscheidungen zur Abwehr der Angreifer zu treffen. Unternehmen müssen verstehen, dass IT-Sicherheit als Business-Prozess zu sehen ist. Als Prozess, der zu modellieren, mit Metriken zu steuern, mit Tools zu überwachen und kontinuierlich zu optimieren ist.

DIE KERNFRAGE FÜR DATA-CENTER-ANBIETER: WIE DIFFERENZIERT MAN SICH AM BESTEN FÜR DIE ZEIT NACH CORONA?

Timo Schlüter, Arvato Systems, Business Consultant Cyber Security, www.arvato-systems.de

Schwachstellen finden

Dafür braucht es zunächst eine gründliche Analyse: Wo sind Firmen am verwundbarsten? Mit dem MITRE ATT&CK Framework finden sie heraus, wie sie am wahrscheinlichsten angegriffen werden. Das Framework listet alle bekannten Angriffstechniken tagesaktuell auf und erklärt, wie man sie erkennt und mögliche Angriffe abwehrt. Wichtig ist auch, sich mit der Bedrohungslage in der eigenen Branche zu beschäftigen.

Eigene IT kennen

Ebenso unverzichtbar sind messbare Kennzahlen. Nur so ist es möglich, Prozesse und ergriffene Maßnahmen im Hinblick auf das angestrebte Ziel zu bewerten und valide Ergebnisse zu erzielen. Um einen belastbaren Prozess zu modellieren, müssen sich Unternehmen einen Überblick über ihre unternehmensinterne IT-Landschaft verschaffen. Dabei ist es jedoch nicht mit vereinzelten Security Scans getan. Denn: IT-Sicherheit ist alles andere als statisch. Ein Security Score hilft nicht weiter. Er zeigt nur die Qualität der Prevention an, nicht aber die Wirksamkeit von Detection- und Response-Maßnahmen im zeitlichen Verlauf.

Permanentes Monitoring schützt

Klarheit schafft nur ein permanentes Monitoring. Im Rahmen eines CIS-Assessments lassen sich Daten systemübergreifend in ein Scoring überführen, das Aufschluss über die Kritikalität und etwaige Schwachstellen gibt (Vulnerability Management). Ebenso hilfreich ist ein EDR-Tool, das Aktivitäten wie das Öffnen einer Datei oder aufgebaute Netzwerkverbindungen auf Endgeräten wie PCs, Notebooks, Tablets und Smartphones aufzeichnet, also ein Prozessmonitoring bietet. Doch dennoch gilt: Selbst das beste Monitoring eröffnet keinen vollständigen Schutz gegen Zero Day Exploit Attacks und APTs.

Hochqualifiziertes Personal

Konzerne haben häufig ein eigenes Security-Team, mittelständische Unternehmen greifen üblicherweise auf das Security Operations Center (SOC) eines Managed Security Service Providers (MSSP) zurück. Die Fachleute in einem SOC überwachen alle eingehenden Alerts und bewerten, ob es sich um kritische Incidents handelt. Sie ziehen neben Logging-Daten auch Informationen aus dem EDR-System sowie dem Netzwerk-Monitoring heran und analysieren auffällige Systeme. Zumeist konzentrieren sie sich auf Active Directory, DMZ und besonders schützenswerte Bereiche.

Rückschau unerlässlich

Liegt ein Angriff vor, informiert das SOC das Incident Response Team. Es entscheidet, welche Handlungen ad hoc vorzunehmen und welche vordefinierten Maßnahmenpakete anzuwenden sind. Denn die Abwehr muss den Methoden und Techniken des Angreifers entsprechen. Wer den Vorfall nachbereitet, ist auf den nächsten Angriff vorbereitet.

Timo Schlüter

AUTHENTIFIZIERUNG

PASSWORTLOSE ANMELDUNGEN SIND EINFACH SICHERER

Die Authentifizierung per Passwort ist keine sichere Lösung mehr. Alternative Konzepte und wirklich passwortlose Technologien gibt es bereits – Unternehmen müssen den Ernst der Lage aber noch erkennen und ihre Strategien neu überdenken.

Neue Technologien, clevere Applikationen und flexible Arbeitsmodelle haben bereits lange Einzug in unseren Alltag gehalten. Mit dem steigenden Einsatz von komplexen digitalen Lösungen im Arbeitsalltag, oft in Verbindung mit dezentralen Arbeitsplätzen, wächst allerdings auch ein nicht zu unterschätzendes Sicherheitsrisiko für Unternehmen. Eine gängige Strategie, um Cyber-Bedrohungen wie Phishing-Attacken entgegenzutreten, ist das Zero-Trust-Prinzip. Der Ansatz vertraut nichts und niemandem innerhalb und außerhalb der Unternehmensgrenzen – eine Strategie, die sich bereits fest etabliert hat.

DER FAKTOR DER UNSICHEREN PASSWÖRTER WIRD DURCH NEUE TECHNOLOGIEN ERSETZT, DIE AUF ETABLIERTE UND SICHERE STANDARDS WIE FAST IDENTITY ONLINE (FIDO) SETZEN.

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

Neue Wege gehen

Im Alltag bedeutet das für die Anwender oftmals zeitraubende Anmeldeverfahren für einzelne Anwendungen sowie die damit verbundene Eingabe von komplexen Passwörtern. Die in vielen Fällen verwendete Multi-Faktor-Authentifizierung (MFA) soll dabei für erhöhte Sicherheit und die Bestätigung der Identität des Nutzers sorgen, führt aber nicht selten aufgrund der miserablen Usability zu Frust und Zeitverlust. Unternehmen müssen deshalb neue Wege gehen: Einerseits sind unnötige Anmeldeverfahren für Systeme und Anwendungen zu vermeiden – hier kommt Single Sign-on (SSO) ins Spiel, also die einmalige Authentifizierung für den Zugriff auf diverse Anwendungen. Andererseits ist es dringend notwendig, dass Unternehmen sich den Gefahren von Passwörtern bewusst werden. Nicht nur, dass Kriminelle die persönlichen Zugangsdaten entwenden können, etwa durch Phishing-Attacken oder Data Breaches, auch neigen Mitarbeiter dazu, einfach zu erratende Passwörter zu wählen und diese für mehrere Zugänge zu verwenden.

Single Sign-on und passwortlos

Eine sichere sowie benutzerfreundliche Lösung arbeitet daher mit Single Sign-on und ist passwortlos. Dabei sollte die einmalige Anmeldung mittels einer MFA mit Blick auf die Usability so unkompliziert wie möglich gestaltet sein: Idealerweise startet man damit direkt am Desktop, also bei der Anmeldung am AD-Konto, sodass der Anwender nach erfolgreicher MFA erst gar keine weiteren Anmeldungen mehr durchführen muss. Der Faktor der unsicheren Passwörter wird durch neue Technologien ersetzt, die auf etablierte und sichere Standards wie Fast Identity Online (FIDO) setzen. Viele Lösungen verzichten zwar oberflächig auf die Eingabe eines Passwortes und setzen beispielsweise auf biometrische Authentifizierung – unter der Haube sind die Informationen dennoch an Kennwörter gebunden und sind dementsprechend anfällig für Angriffe. Wirklich passwortlose Technologien verfügen über die entsprechende Zertifizierung und basieren etwa auf Public-Key-Kryptografie. Sie verbinden damit nicht nur Sicherheit und einfache Bedienung, sondern verringern auch gleichzeitig Kosten sowie den administrativen Aufwand, der bei dem Verlust oder dem Zurücksetzen von Passwörtern im Helpdesk-Bereich entsteht.

Jochen Koehler

KRYPTOGRAFIE

MULTI-TOOL DES DATENSCHUTZES

In den letzten Jahren sind die Anforderungen an den Datenschutz ständig gewachsen. Nicht nur sind zahlreiche Gesetze und Vorgaben aufgestellt und präzisiert worden, auch neuere Entwicklungen im Geschäftsleben legen verstärkten Wert auf den Schutz sensibler Daten. Unternehmen und Behörden müssen sich dieser Anforderungen bewusst werden und entsprechende Maßnahmen ergreifen. Grundsätzlich liegt es im Interesse eines Unternehmens, die Kontrolle über seine Daten zu behalten und diese entsprechend zu sichern.

Environmental, Social & Corporate Governance (ESG)

ESG ist ein relativ neuer Ansatz, um zu bewerten, in welchem Maße Unternehmen sich für Ziele einsetzen, die über die Gewinnmaximierung für ihre Aktionäre, Eigentümer oder Stakeholder hinausgehen. Innerhalb der ESG-relevanten Aspekte gewinnt in zunehmendem Maße auch der Umgang mit Daten an Bedeutung. Unternehmen werden auch daran gemessen, wie sorgfältig sie mit sensiblen Daten ihrer Angestellten, Kunden und Partner umgehen. Die bestgeeignete Technik, um diesen sorgfältigen Umgang zu gewährleisten, ist die Verschlüsselung, bevor die sensiblen Daten die geschützte Unternehmensumgebung verlassen.

KRYPTOGRAFIE IST DER SCHLÜSSEL ZU EINER REIHE VON THEMEN, DEREN BEDEUTUNG STÄNDIG WEITERWÄCHST.

Elmar Eperiesi-Beck, Gründer und CEO, eperi, https://eperi.com/de/

DSGVO, Schrems-II-Urteil und die Cloud

Die DSGVO (Datenschutzgrundverordnung) legt einen noch viel größeren Wert auf den sorgfältigen Umgang mit Daten und hält diesen juristisch verbindlich fest. Insbesondere das Schrems-II-Urteil hat geklärt, welche Folgen die DSGVO für die Nutzung von Cloud-Diensten hat:

- Die Nutzung nichteuropäischer Cloud-Dienste ist ohne weitere Maßnahmen nicht DSGVO-konform (auch wenn die Server in Europa stehen).
- Standardvertragsklauseln sind nicht mehr ausreichend, um DSGVO-Konformität zu gewährleisten.
- Die von Cloud-Anbietern angebotenen Sicherheitslösungen (wie Microsoft E5 Lizenz) sind nicht ausreichend, um DSGVO-Konformität zu erreichen.

Der Europäische Datenschutzausschuss (EDSA) hat beschlossen, dass Unternehmen weiterhin personenbezogene Daten an außereuropäische Cloud-Dienste übertragen dürfen, wenn sie geeignete technische Maßnahmen zum Schutz dieser Daten treffen. Explizit nennt der EDSA die Verschlüsselung oder Pseudonymisierung von Daten nach dem aktuellen Stand der Technik, bevor diese an die Cloud übertragen werden. Auch hier ist also Verschlüsselung das Mittel der Wahl.

Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

Einen bisher wenig beachteten Grund für den Einsatz von Verschlüsselungstechnologien liefert das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), das seit 2019 entsprechende EU-Richtlinien in deutsches Recht umsetzt. In die Definition fließt unter anderem die Bestimmung ein, dass nur dann ein Geschäftsgeheimnis vorliegt, wenn das Unternehmen angemessene Geheimhaltungsmaßnahmen getroffen hat. Was als angemessene Geheimhaltungsmaßnahme gilt, kann sich dabei von Fall zu Fall unterscheiden, nicht zuletzt in Abhängigkeit von der Wichtigkeit der fraglichen Geheimnisse. Auch in diesem Fall gilt allerdings, dass Unternehmen mit Verschlüsselung der Daten nach dem aktuellen Stand der Technik auf der sicheren Seite sind.

Die richtige Lösung

Eine selbst kontrollierte Verschlüsselung ist also die beste Möglichkeit für ein Unternehmen, sich beim Thema ESG zu profilieren, außereuropäische Cloud-Dienste DSGVO-konform zu nutzen sowie seine Geschäftsgeheimnisse On-Premises und in der Cloud zu schützen. Alle anderen Systeme sind fallibel. Verschlüsselte Daten sind zwar auch nicht vor Diebstahl geschützt, aber sie sind (kommerziell) unbrauchbar für Kriminelle. Einen stärkeren technischen Schutz kann es nicht geben.

Die technisch effizienteste und einfachste Umsetzung der Verschlüsselung besteht dabei in der Nutzung eines Kryptogra-

fie-Gateways, das die Daten verschlüsselt, bevor sie On-Premises gespeichert oder in die Cloud übertragen werden. Der Vorteil der Datenverschlüsselung innerhalb eines Gateways liegt per se in der Tatsache, dass das Unternehmen jederzeit die Kontrolle über die Verschlüsselungsmethode und die verwendeten Schlüssel behält und so die Einhaltung der DSGVO gewährleisten kann.

Indexierung

Mit dem richtigen Gateway lassen sich auch Nachteile vermeiden, die eine herkömmliche Datenverschlüsselung mit sich bringt. Verschlüsselte Daten sind an sich nicht entzifferbar, auch nicht für die Anwendung, in der diese erstellt wurden. Eine Suche in verschlüsselten Daten zum Beispiel stellt darum eine technische Herausforderung dar. Diese lässt sich durch die interne Indexierung der Datenfelder in der Anwendung bewältigen. Hierbei werden die Datenfelder bei der Verschlüsselung im Gateway indexiert und die entsprechenden Indizes in einer separaten, dedizierten Datenbank beim Unternehmen abgelegt. Sucht ein Anwender nach einer bestimmten verschlüsselten Information, findet das Gateway die Indizes in der Datenbank und sendet eine entsprechend modifizierte Suchanafrage an die Anwendung. Die Anwendung sendet die betroffenen Datensätze zurück an das Gateway, das diese entschlüsselt und dem Anwender zur Verfügung stellt. Bei diesem Prozess verlassen zu keinem Zeitpunkt Daten im Klartext das Unternehmen. Bei entsprechender technischer Umsetzung nimmt der Prozess nicht mehr als wenige Millisekunden in Anspruch.

Flexibilität

Je nach (Cloud-) Anwendung müssen die Verschlüsselung und Indexierung angepasst werden, weil dieselbe Art Daten, abhängig von der Anwendung, an verschiedenen Stellen im Datenstrom zu finden ist – eine Adresse in SAP beispielsweise an anderer Stelle als bei Salesforce. Diese Anpassung lässt sich am besten durch Templates bewerkstelligen. In dem Template kann ein Unternehmen dann auf einfache Weise definieren, welche Art von Daten es als sensibel erachtet und darum verschlüsseln will. Es wird sich dabei immer nur um einen verhältnismäßig kleinen Teil der Daten handeln. Das Motto lautet: So wenig wie möglich und so viel wie nötig verschlüsseln.

Das Template generiert eine Beschreibung, die festlegt, wo im Datenstrom der jeweiligen Anwendung das Kryptografie-Gateway die zu verschlüsselnden Daten finden kann. Für viele gängige Anwendungen sind vorgefertigte Templates vorhanden, und es ist kein Hexenwerk, ein neues Template auch für Eigenentwicklungen von Unternehmen oder Behörden zu erstellen.

Multi-Tool Datenverschlüsselung

Kryptografie ist der Schlüssel zu einer Vielzahl verschiedenster Themen, deren Bedeutung ständig weiterwächst. Auch Unternehmen, denen ihr Eigeninteresse nicht ausreicht, strikte Maßnahmen zum Schutz ihrer sensiblen Daten zu ergreifen, erhalten durch ESG, DSGVO und Schrems-II-Urteil sowie GeschGehG mehr als ausreichend Gründe für den Einsatz von Kryptografie. Wie jedes gute Multi-Tool kann ein Kryptografie-Gateway hohe Gebrauchsfreundlichkeit gewährleisten: die gewohnten Geschäftsabläufe bleiben erhalten, die Prozesse laufen effizient mit minimalen Latenzzeiten und Plugins sind nicht erforderlich.

Elmar Eperiesi-Beck

SO EINFACH!

DATENSCHUTZ IN DER CLOUD

VIELE UNTERNEHMEN KENNEN IHRE SICHERHEITSPROBLEME. DOCH ZU WENIGE KÜMMERN SICH AKTIV UM DIE LÖSUNG.

Robert Freudenreich, CTO und Gründer, Secomba GmbH/Boxcryptor, www.boxcryptor.com

Was für ein Glück, wenn man es zur Abwechslung mal mit Problemen zu tun hat, die sich leicht lösen lassen. Datenschutz in der Cloud ist eines davon. Schwer zu glauben: Obwohl Daten in der Cloud oft im Ausland gespeichert werden, ist dieser Datenspeicher für Unternehmen die sicherste Variante, um DSGVO-konform Dateien abzulegen. Das Zauberwort lautet Verschlüsselung.

Daten liegen bereits in der Cloud

Wachsende Datenmengen und der Wunsch nach Flexibilität machen die Cloud als Datenspeicher immer beliebter. Die Vorteile liegen auf der Hand: Die Dateien brauchen kaum lokalen Speicherplatz, die Cloud hat eine hohe Verfügbarkeit und der Zugriff auf die Daten ist von überall aus möglich.

Viele Programme nutzen die Cloud als Datenspeicher oder Backup ohne, dass das den Kunden bewusst ist. Das passiert, wenn die Synchronisation standardmäßig eingestellt ist oder wenn das Programm speziell für die Cloud-Nutzung gestaltet wurde. Das ist beispielsweise bei Microsoft Office der Fall. Hier liegt die Ursache für ein ernstzunehmendes Problem im Bereich Datenschutz: Kontrollverlust. Schließlich werden die Informationen an Server übermittelt, die nicht im Einflussbereich desjenigen liegen, dem die Daten gehören.

Vorsicht bei Kollaborationssoftware

Vorbehalte gegenüber der Cloud beziehen sich vor allem auf den mangelnden Datenschutz. Trotzdem ergreifen noch zu wenige Unternehmen die Initiative. Gegenmaßnahmen laufen nur schleppend an. Das führt dazu, dass die Zahl der Datenlecks von Jahr zu Jahr weiter steigt. Fast die Hälfte aller deutschen Unternehmen gab an, bereits mindestens einmal Ziel einer Cyberattacke gewesen zu sein.

Vorsicht ist besonders beim Einsatz von Kollaborationstools geboten: Software wie Microsoft Teams ermöglicht den einfachen Austausch von Nachrichten und Dateien. Die Nutzer haben sich an die praktischen Desktop-Anwendungen gewöhnt und vergessen dabei: Hier werden Daten in die Cloud geschickt.

Meine Beobachtung: Die Unternehmen kennen die Probleme. Doch zu wenige kümmern sich aktiv um die Lösung. Datenschutzgesetze und Compliance-Vorgaben sind als Sicherheitsmaßnahmen nur so gut wie ihre Umsetzung.

Die Lösung ist einfach

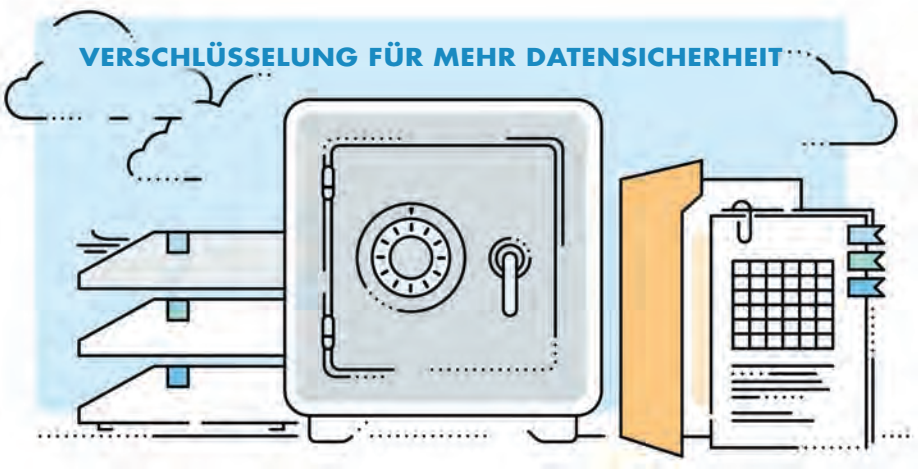
Schütteln Sie den Gedanken ab, dass Ihr Unternehmen Angriffen auf die Cloud-Dateien hilflos ausgeliefert ist oder dass Sie Datenlecks hinnehmen müssen. Nehmen Sie stattdessen den Schutz der Daten selbst in die Hand. Ihr wichtigstes Werkzeug: Verschlüsselung.

Die Verschlüsselung ist dann wirkungsvoll, wenn die Dateien noch auf dem jeweiligen Gerät verschlüsselt werden, auf dem sie erstellt oder bearbeitet werden. So sind die Informationen während der Übermittlung in die Cloud und während der gesamten Speicherdauer geschützt. Sie wehren damit Angriffe durch Ransomware und Leakware ab und schützen sich vor Zugriffen durch den Cloud-Anbieter oder ausländischer Behörden.

Kontrolle ohne Mehraufwand

Verschlüsselung ist ein gutes Werkzeug für mehr Datensicherheit. Hochwertige Verschlüsselungssoftware fügt sich nahtlos in bestehende Arbeitsabläufe ein. Auch für Backups eignet sich diese zusätzliche Schutzschicht hervorragend. Das Motto sicherer Cloud-Nutzung heißt also: Kontrolle behalten. Verschlüsselung ist dafür eine effektive Maßnahme.

Robert Freudenreich



DATENSCHUTZ

VORSICHT VOR LÜCKEN IN DER STRATEGIE UND UMSETZUNG

Die Übergangsfrist, die Unternehmen zur Umsetzung von DSGVO-Richtlinien gegeben wurde, ist seit Mitte 2018 ausgelaufen – dennoch scheinen viele kleine und mittlere Unternehmen unter dem Radar geflogen zu sein, wenn es um Bußgelder für Verstöße gegen die Richtlinien ging. Steffen Reimann, Produkt- und Partnermanager bei TÜV SÜD, warnt davor, dass kontinuierlicher Mut zur Lücke teuer werden kann.

Bei den Aufsichtsbehörden zeichnet sich eine Trendwende ab: Europäische Behörden sind mittlerweile bereit, hart durchzugreifen. Diese Entwicklung wird sich mutmaßlich auch im Jahr 2022 weiter fortsetzen. 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 Bewusstsein wächst

Das liegt unter anderem auch daran, dass die Anzahl der privat geführten datenschutzrechtlichen Verfahren, die mit Verstößen gegen die DSGVO in Zusammenhang stehen, im vergangenen Jahr merklich zugenommen hat. Immer mehr Betroffene klagen auf Schadensersatz. Ein Grund hierfür könnte die Medienberichterstattung der vergangenen Jahre sein, die das Bewusstsein der breiten europäischen Öffentlichkeit für ihre Rechte und für mögliche Rechtsmittel im Fall eines DSGVO-Verstoßes bedeutend geschärft hat. Unternehmen werden sich daher in Zukunft vermutlich immer häufiger neben Strafzahlungen auch mit Schadensersatzforderungen Betroffener konfrontiert sehen werden. Auch mit Sammelklagen ist in dem Zusammenhang zu rechnen – dabei könnten neue Höchstwerte an Bußgeldern resultieren.

Lückenlose Konformität

Um dieser Entwicklung entgegenzutreten, bleibt Unternehmen nur eine Option: die lückenlose Konformität mit den Anforderungen der DSGVO und die regelmäßige Überprüfung selbiger. Zur Einhaltung 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. Nicht alle Unternehmen sind dabei in der Lage, diese Anforderungen alleine zu stemmen. Vor allem bei kleinen und mittleren Unternehmen herrscht nach wie vor große Unsicherheit oder aber der Mangel an dem notwendigen Fachwissen und Ressourcen.

Allerdings können sie hierbei auf die Unterstützung durch externe Experten zurückgreifen. So kann auch gleich eine externe, neutrale Beurteilung der eigenen Datenschutzlage vorgenommen werden, um zusätzliche Sicherheit zu schaffen. Diese Experten sind dazu in der Lage, 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 zu unterstützen. Kurz gesagt: Sie sind in der Lage, das gesamte Spektrum abzudecken. Mit einer solchen externen Unterstützung können dann auch kleiner Unternehmen mit geringen Ressourcen ihre Datenverarbeitungsprozesse DSGVO-konform gestalten und potentielle kostspielige Lücken aufdecken und schließen, bevor es überhaupt zu Datenlecks, Verfahren oder Bußgeldern kommt.

www.tuvsud.com

UNTERNEHMEN WERDEN SICH IN ZUKUNFT VERMUTLICH IMMER HÄUFIGER NEBEN STRAFZAHLUNGEN AUCH MIT SCHADENSERSATZFORDERUNGEN BETROFFENER KONFRONTIERT SEHEN.

Steffen Reimann, Produkt- und Partnermanager, TÜV SÜD, www.tuvsud.com

SEGREGATION OF DUTY KONTROLLEN ERFOLGREICH EINFÜHREN

PITFALLS UND BEST PRACTICES

Segregation of Duty (SOD) Regeln stellen ein wichtiges Werkzeug dar, um Sicherheitsprinzipien und Compliance-Anforderungen wie das 4-Augen-Prinzip oder das Prinzip der minimalen Berechtigungsvergabe im Identity and Access Management (IAM) umzusetzen. Eine SOD-Regel definiert konkret, dass zur Funktionstrennung bestimmte Berechtigungen nicht gleichzeitig vergeben sein dürfen, sodass schadhafte Aktionen nicht von Einzelnen ausgeführt werden können. Das häufig zitierte Beispiel, dass Angestellte nicht gleichzeitig Dienstleister im Zahlungssystem anlegen und dort auch deren Zahlungen autorisieren dürfen, veranschaulicht plakativ, dass durch die kontrollierte Vergabe von Berechtigungen betrügerischen Handlungen ein Riegel vorgeschoben werden kann.

Gleichwohl stellen die Einführung und langfristige Verwaltung von SOD-Regeln Unternehmen immer wieder vor Herausforderungen. Im Folgenden wird dargestellt, welche typischen Fehler hierbei auftreten, und wie man mithilfe von Tool-Unterstützung SOD-Management langfristig etablieren kann.

Pitfall 1: Fokus auf systemspezifische Definitionen

Um SOD-Regeln unternehmensweit zu etablieren, ist zunächst ein Verständnis wichtig, in welchen Bereichen SOD-Konflikte auftreten können. Viele Unternehmen beginnen mit der Einführung von SOD-Regeln auf Basis von Audit-Findings von Wirtschaftsprüfern, meist direkt in unternehmenskritischen Systemen, wie beispielsweise dem ERP System. Eine solche Herangehensweise unterschlägt aber, dass auch systemübergreifende Berechtigungen Funktionstrennungskonflikte verursachen. Daher ist ein geschäftsprozess-orientierter Ansatz zur Einführung elementar.

Pitfall 2: Vernachlässigung von Ebenen des Berechtigungsmodells

Ebenso ist häufig unklar, auf welchen Ebenen des Berechtigungsmodells Konflikte auftreten können. Viele Unternehmen erzielen durch die Bündelung von IT-Berechtigungen in Rollen oder durch hierarchische Verschachtelungen eine Vereinfachung der Berechtigungsvergabe. Die Notwendigkeit zur Beachtung von SOD-Regeln wird meist in derartigen Modellierungsprojekten unterschlagen, und erfordert dann aufwändigere Änderungen am bereits etablierten Rollen- und Berechtigungsmodell. Um dieser Problematik zu entgegnen, empfiehlt es sich, alle beteiligten Ebenen des Berechtigungsmanagements bereits bei Einführung des Modells einer SOD-Betrachtung zu unterziehen.

Pitfall 3: Versäumnis der Definition von SOD-Lebenszyklus-Prozesse

Weiterhin fokussieren sich viele Unternehmen auf die Einführung des Regelwerks und schenken dem Prozess der Konfliktidentifikation, -behandlung und der Adaption der Regeln im organisatorischen Wandel wenig Beachtung. Der Lebenszyklus des Regelwerks ist jedoch wichtig, um eine Nachhaltigkeit des SOD-Modells zu erreichen. Prüfprozesse der Regeln sowie Beantragungs-, Freigabe- und Löschprozesse von Änderungen an der SOD-Matrix sind notwendig, um auf Änderungen im betrieblichen Ablauf reagieren zu können. Die organisatorische Verankerung von Verantwortlichkeiten für Regeln, der Konfliktbehandlung und die Einbettung in verwandte Prozesse (Beantragung neuer Geschäftsrollen) hilft, das SOD-Regelwerk nachvollziehbar dokumentiert und aktuell zu halten.

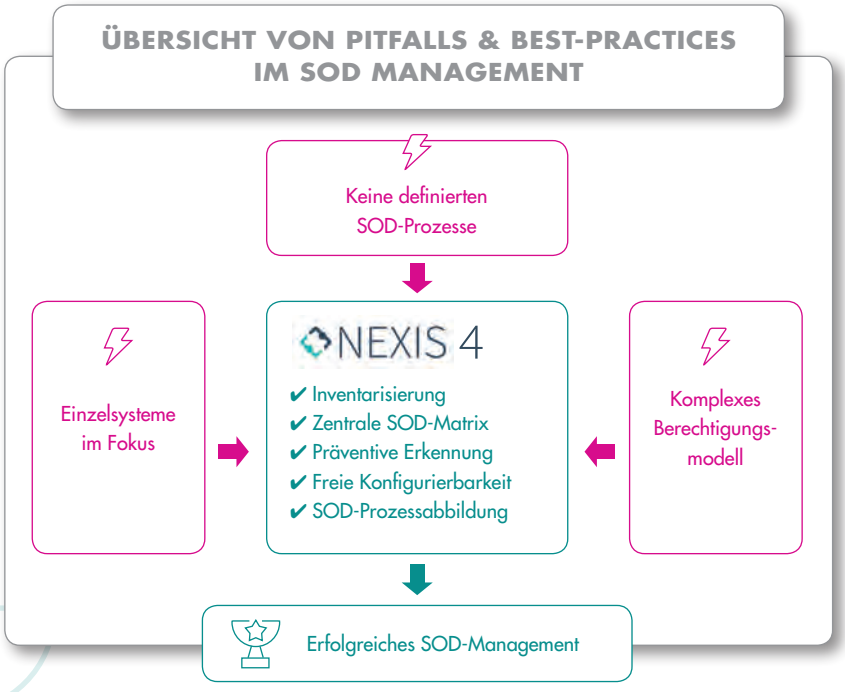
Dass für erfolgreiche SOD-Kontrollen ein System notwendig ist, das das Regelwerk zentralisiert und die Konfliktidentifikation

SOD-MANAGEMENT IST EINE UMFASSENDE, SOWOHL TECHNISCHE ALS AUCH INSBESONDERE ORGANISATORISCHE AUFGABE. BEIDES IN EINKLANG ZU BRINGEN KANN NUR MIT EINEM STRUKTURIERTEN ANSATZ GELINGEN.

Dr. Michael Kunz, Head of Professional Services, Nexis GmbH, www.nexis-secure.com

sowie deren Behandlung übernimmt, ist schnell klar. Die obigen Pitfalls zeigen aber, dass die reine Regeldefinition und Konfliktidentifikation zu kurz gedacht sind, um SOD-Management ganzheitlich zu betreiben.

Die SOD-Engine der Identity and Access Governance (IAG) Plattform NEXIS 4 ist auf Basis von Projekt- und Kundenerfahrungen entwickelt worden. So bietet sie Best-Practice-Funktionalitäten, um den typischen Herausforderungen von SOD-Projekten zu begegnen:



1. Inventarisierung des Berechtigungsmodells

Mithilfe der Analyse- und Modellierungsfunktionalitäten von NEXIS 4 kann der Berechtigungskatalog schnell und schrittweise um SOD-Klassen für die Regelprüfung erweitert werden. Die Massenbearbeitung erlaubt es, große Berechtigungsmengen schnell um SOD-Klassen zu erweitern.

2. Zentralisierte und anwendungs-übergreifende SOD-Matrix

Durch den Regel-Editor können in NEXIS 4 beliebige Kombinationen aus SOD-Klassen, oder aus den beteiligten Berechtigungen und Rollen, in einem vollwertigen SOD-Regelmodell abgebildet werden. Die Regeln sind in einem zentralen Repository gesichert und können per API oder Export mit anderen Systemen, wie zum Beispiel Dokumentationsplattformen, synchronisiert werden. NEXIS 4 kann somit die SOD-Regeln für alle IAG-relevanten Anwendungssysteme auf Einhaltung kontrollieren.

3. Detektive und präventive SOD-Kontrollen zur Konfliktidentifikation

NEXIS 4 führt eine Prüfung des SOD-Regelwerks zeit- oder ereignisbasiert aus. Neben diesen detektiven Kontrollen, können aber auch in den Beantragungs- und Veränderungsprozessen der Berechtigungsdaten präventive Checks verankert werden. Durch die Integration mit der Workflow-Engine können SOD-Prüfungen in Workflows punktuell inkludiert werden. Werden solche Prozesse von anderen Systemen übernommen, kann trotzdem die NEXIS 4 SOD-Engine verwendet werden. Mithilfe von REST-API-Calls kann sie Verstöße jederzeit identifizieren.

4. Individualisierbare und endnutzerfreundliche Bearbeitung von Konflikten

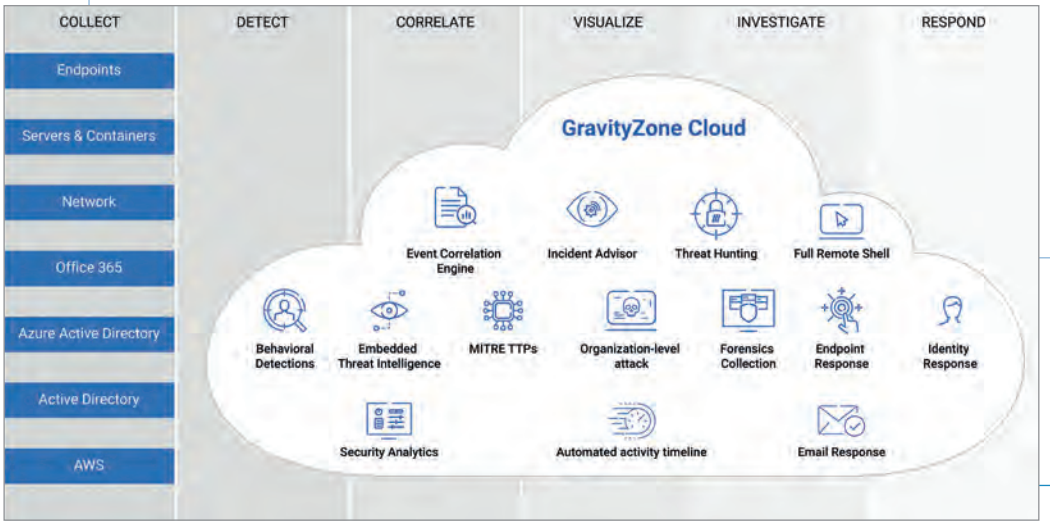
Die User Experience der beteiligten Verantwortlichen zur Konfliktbearbeitung ist ein wesentlicher Erfolgsfaktor für SOD-Projekte. Da die Mitigation von Konflikten wesentlich mit den verursachenden Berechtigungsstrukturen zusammenhängt, ist die Bearbeitung nicht immer trivial. Umso mehr muss die Oberfläche für den jeweiligen Empfängerkreis individuell konfigurierbar sein. So müssen typischerweise Ausnahmegenehmigungen beantragt werden, optionale Unterschriftsdokumente hochgeladen oder der Entzug von Berechtigungen initiiert werden. Durch die Konfigurierbarkeit von NEXIS 4 ist eine Anpassung an diese Bedürfnisse schnell realisierbar.

5. Lebenszyklus-Prozesse und Dokumentation

Zur strategischen und nachhaltigen Verwaltung der SOD-Regeln, bietet NEXIS 4 ein einzigartiges System Prozesse darzustellen, die bei der Erstellung, Veränderung oder Löschung von SOD-Regeln zum Einsatz kommt. Damit kann sichergestellt werden, dass Sicherheitslücken, die durch schadhafte Veränderung des Regelwerks selbst entstehen könnten, geschlossen werden und die historische Entwicklung des Regelwerks, der Konflikte und der SOD-Prozesse jederzeit transparent und nachvollziehbar einsehbar sind.

SOD-Management wird von Unternehmen aufgrund einer Vielzahl von Regulatorien und Compliance-Anforderungen wie SOX, MaRisk oder auch dem internen Risiko- und Sicherheitsmanagement betrieben. Die umfassende und langfristige Einführung von SOD-Kontrollen birgt aber viele Herausforderungen. Mit IAG-Lösungen, wie NEXIS 4, die Best-Practices direkt berücksichtigen, können Unternehmen durch Tool-Unterstützung schneller und gezielter auf diese Anforderungen reagieren.

Dr. Michael Kunz



Eine umfassende Beobachtung und Abwehr sind notwendig, um komplexe IT-Infrastrukturen zu schützen.

Bildquelle: Bitdefender

EIN WEITES FELD

IT-SICHERHEIT HÖRT NICHT BEIM ENDPUNKT AUF

Cyberkriminelle haben längst die gesamte Angriffsfläche einer IT-Infrastruktur für sich entdeckt und nutzen sie aus. Der Endpunkt ist – aus Sicht des Hackers - nach wie vor das erklärte Ziel. Wer diesen schützen will, benötigt eine umfassende Sicherheitslösung, die Informationen aus verschiedenen IT-Bereichen im Kontext erfasst, analysiert und Angriffe schließlich abwehrt.

Geschäftsprozesse in digitalisierten Unternehmen basieren auf heterogenen Technologien und Infrastrukturen, zu denen nicht nur Endpunkte, sondern auch Dienste und Infrastrukturen in zumeist hybriden Cloud-Umgebungen zählen. Das gilt zunehmend auch für mittelständische Betriebe, die etwa in der Pandemie ihre Mitarbeiter ins Homeoffice geschickt haben.

Für einen Angreifer sind sämtliche IT-Systeme und -Applikationen potenzielle Ziele. Lücken in der Abwehr und exponierte Schwachstellen einer Unternehmens-IT zu identifizieren, ist daher eine unverzichtbare Grundlage, um die IT-Abwehr proaktiv vorzubereiten und neue Bedrohungen abzuwehren. IT-Sicherheitsverantwortliche, die sich zukunftssicher aufstellen wollen, benötigen deshalb möglichst umfassende Informationen, um eine Gesamtsichtbarkeit der Gefahrenlage zu erhalten.

Zum Beispiel Cloud

Ein wichtiges Beispiel für die Notwendigkeit, neue Informationsquellen zu erschließen, ist die Cloud. Cloud Workloads spielten im Zuge des Pandemie-Homeoffice eine wachsende Bedeutung. Wer die möglichen Angriffe auf diese neuen Endpunkte in ihrem Ursprung erkennen, aus ihrem Kontext verstehen, analysieren und dadurch besser abwehren will, benötigt Extended Endpoint Detection and Response (XDR). XDR-Technologien ermöglichen eine erweiterte Analyse der Telemetrie und berücksichtigen die hier relevante Threat Intelligence.

Informationen ohne Agenten

XDR korreliert dafür Daten aus verschiedensten Quellen – auch dort, wo die Installation eines Agenten nicht möglich ist, wie zum Beispiel in einem Amazon Web Services S3-Bucket oder in der Amazon Web Services Konsole. Hacker, die ein S3-Bucket ausspähen, werden für XDR sichtbar. Eine umfassende Sicherheitsanalyse wird in einer Multicloud noch wichtiger.

Eine Fülle an Endpunkten

Die Cloud ist nur ein Beispiel für die Notwendigkeit, den Horizont der IT-Sicherheit zu erweitern. Die Angriffsfläche der IT besteht nicht mehr nur aus physikalischen Systemen und virtuellen Maschinen: Container werden zunehmend wichtiger und müssen daher in die Analyse einbezogen werden. Sie sind durch die Flexibilität der mit ihnen portierten Dienste ein geeigneter Kanal, um Malware zum Beispiel für Kryptomining oder Datenspionage zu verbreiten. Ein Office 365 in der Cloud ist ebenfalls ein wichtiger zu beobachtender Schauplatz im Gegensatz zu einer lokalen Installation. Auch der Verkehr im Netzwerk oder aus IoT-Umgebungen hat hohe Sicherheitsrelevanz. Dazu kommen noch Identity Access Management Systeme (IAM).

Der umfassende Blick

XDR sammelt via Sensoren Daten, erkennt Risiken, korreliert diese und visualisiert sie, um eine ganzheitliche Abwehr zu ermöglichen. Angriffe, die an einem oder an mehreren Punkten starten, können die ganze IT betreffen. Eine umfassende Abwehr verlangt daher umfassende Informationsquellen.

Jörg von der Heydt | www.bitdefender.de

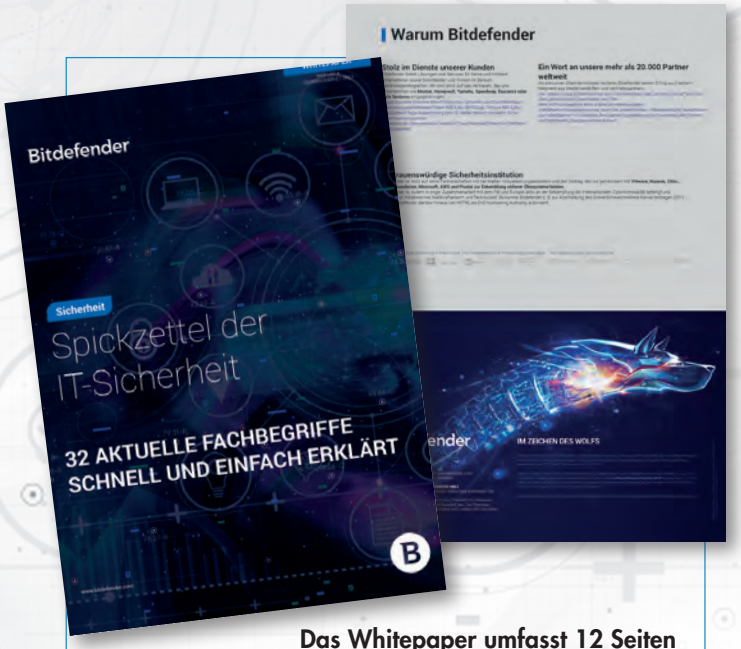
SPICKZETTEL DER IT-SECURITY

32 FACHBEGRIFFE SCHNELL UND EINFACH ERKLÄRT

Was ist eigentlich der Unterschied zwischen APT und ATP? Da verhaspeln sich selbst IT-Profis manchmal. Abteilungsleiter und andere Entscheidungsträger verlieren sich gern im Branchenjargon. Doch wenn IT-Sicherheit Teil der allgemeinen Geschäftsstrategie und Risikobewertung werden soll, muss sich die Kommunikation verbessern. Nur so gelingt es, das wichtige Thema in Sitzungen von Vorständen und Geschäftsleitungen zu platzieren.

Gerade deshalb wünscht man sich bei vielen Fachbegriffen der schnelllebigen Welt der IT-Sicherheit einen Blick in ein Wörterbuch, um den Begriff richtig zu verwenden oder anderen schnell und einfach erklären zu können.

Zu diesem Zweck finden Sie in diesem Whitepaper eine Erklärung von 32 hochaktuellen Begriffen der IT-Security. Unser Ziel ist es, mit wenigen Sätzen das Wichtigste zu den Begriffen zu erklären – nicht nur für Fachleute, sondern auch für Laien.



Das Whitepaper umfasst 12 Seiten und steht kostenlos zum Download bereit: www.it-daily.net/download

IMPRESSUM

Geschäftsführer und Herausgeber:
Ulrich Parthier (-14)

Chefredaktion:
Silvia Parthier (-26)

Redaktion:
Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Elmar Eperiesi-Beck, Robert Freudenreich, Andreas Fuchs, Jörg von der Heydt, Jochen Koehler, Arnold Krille, Dr. Michael Kunz, Christian Milde, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Steffen Reimann, Timo Schlüter, Stephan Schweizer

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 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

Noch nie war jemand verärgert, dass seine Cloud zu sicher war.

Cloud Security: Vertrauen Sie auf ein Team, das Ihnen mit maßgeschneiderten Lösungen dabei hilft, die Sicherheit Ihrer Cloud zu maximieren. So schaffen wir gemeinsam mit Ihnen nachhaltige Werte und Vertrauen – heute und in Zukunft. www.pwc.de/cloudsecurity

pwc