itmanagement
DEZEMBER 2022

INKLUSIVE 32 SEITEN
IT SECURITY SPEZIAL

CYBERRESILIENZ

MEHR WIDERSTAND GEGEN CYBERBEDROHUNGEN

Waldemar Bergstreiser, Kaspersky

GREEN IT

Nachhaltigkeit effektiv planen

IT TRENDS

Programmieren leicht gemacht

STORAGE

Hybride Multicloud-Umgebung

LIEBE LESERINNEN UND LESER,

die Zeiten ändern sich! Einerseits eine Floskel, andererseits eine Tatsache. Aber Veränderung bringt immer auch Entwicklung und davon leben wir ja schließlich alle!

In diesem Sinne.

Uns als it verlag gibt es bereits seit über 30 Jahren, wir haben uns stetig weiterentwickelt, von ISDN bis Metaverse, haben Trends aufgegriffen, neue Bereiche erschlossen und unser Portfolio ausgebaut.

Nun, mit Erscheinen der Ausgabe 1-2 2023 werden wir den nächsten Schritt unternehmen – uns wieder weiterentwickeln: nachhaltiger, zeitgemäßer, informativer und innovativer. Was das konkret bedeutet, sehen Sie dann in Ausgabe 1-2.

Apropos weiterentwickeln: Cybersecurity ist nach wie vor ein Thema das jedes Unternehmen beschäftigt hält. Offensichtlich reicht Software und Wissen allein aber nicht aus, um Cyberattacken nicht länger lohnenswert erscheinen zu lassen. Wie eine Alternative aussehen könnte, lesen Sie in unserm Supplement it security ab Seite 10.

Und apropos nachhaltiger: Green IT sollte dieses Jahr eigentlich auf jeder Unternehmensagenda stehen. Wer aber noch immer Gründe benötigt, warum man sich unbedingt mit dieser Thematik beschäftigen sollte, sollte sich unserem Themenschwerpunkt ab Seite 10 widmen.

Dies ist die letzte Ausgabe des it management und it security für dieses Jahr. Im neuen Jahr starten wir neu und frisch durch. Wir als Team wünschen Ihnen schöne Feiertage und einen guten Start in das neue Jahr.

Herzlichst
Carina Mitzschke und das gesamte it verlag-Team

Carina Mitzschke | Redakteurin it management

Künstliche Intelligenz

Fluch oder Segen?

28

24

INHALT

COVERSTORY

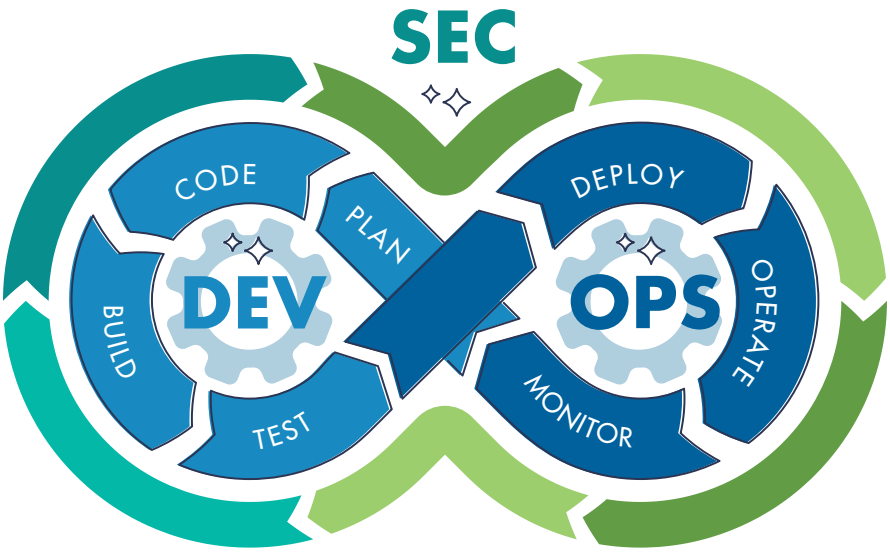
IT MANAGEMENT

COVERSTORY

STORAGE SPEZIAL

Inklusive
32 Seiten

IT SECURITY SPEZIAL



DEVOPS UND DEVSECOPS

ES HOLPERT NOCH

Die Umfrage 2022 „DevSecOps: Simplifying Complexity in a Changing World" untersucht den Status quo der DevOps- und DevSecOps-Adaption. Im Auftrag von Progress befragte das Technologieforschungsunternehmen Insight Avenue dazu weltweit Entscheidungsträger aus den Bereichen IT, IT-Security, Anwendungsentwicklung und DevOps. An der Umfrage nahmen auch zahlreiche deutsche Unternehmen teil.

Zu den zentralen Erkenntnissen der Umfrage für Deutschland zählen:

1. Viele Unternehmen hinken ihren DevOps- und DevSecOps-Zielen hinterher. 80 Prozent der Befragten gaben zu, dass sie mehr tun könnten und ebenfalls 80 Prozent räumten ein, dass sie beim Management von DevSecOps strategischer vorgehen müssten. 14 Prozent befinden sich nach eigener Aussage nach wie vor in einer Sondierungs- und Proof-of-Concept-Phase.

2. Sicherheit ist der wichtigste Grund für die meisten DevOps- und DevSecOps-Implementierungen. Allerdings vertrauen nur 27 Prozent der Unternehmen der Zusammenarbeit von IT-Security und Entwicklung. 78 Prozent sehen sich bei ihren Ansätzen zur IT-Sicherheit mit Herausforderungen konfrontiert und 57 Prozent räumen ein, nicht genau zu verstehen, wie sich IT-Sicherheit in DevSecOps einfügt.

3. Als größtes Hindernis für Fortschritte bei der Implementierung von DevOps und DevSecOps sehen 51 Prozent die Kultur. Dennoch betrachten nur 8 Prozent die Kultur als einen Bereich, den sie in den nächsten 12 bis 18 Monaten optimieren wollen.

4. Unternehmen, die Richtlinien und Praktiken von DevOps und DevSecOps erfolgreich umsetzen, betonen die Bedeutung von übergreifenden Schulungen und Weiterbildungen zur IT-Sicherheit. Sie helfen ihnen dabei, ein höheres Niveau bei der kontinuierlichen und langfristigen Zusammenarbeit zwischen Sicherheits- und Entwicklungs-Teams zu erreichen.

5. Als wichtigste Business-Faktoren für die Einführung und Weiterentwicklung von DevOps in ihren Unternehmen nennen die Befragten mehr Agilität sowie ein geringeres Risiko für Qualitäts-, Sicherheits- und Leistungsprobleme und Ausfallzeiten. Zudem sehen sie die Implementierung von DevOps als Notwendigkeit, um einen Cloud-Auftrag zu erfüllen oder eine Cloud-Migration zu unterstützen.

„Unsere Umfrage zeigt, dass sich Unternehmen in Deutschland der Vorteile von DevSecOps bewusst sind und die Implementierung auch angehen. Viele von ihnen haben dabei allerdings mit der Schaffung einer effektiven DevSecOps-Kultur zu kämpfen", kommentiert Thomas Schuller, Regional Director DACH bei Progress. „Eine solche Kultur lässt sich natürlich nicht über Nacht erreichen, Führungskräfte können aber einen wichtigen Beitrag leisten, indem sie der funktionsübergreifenden Kommunikation hohe Priorität einräumen."

www.progress.com

Die Studie kann hier kostenlos abgerufen werden:
https://prgress.co/3ED6cc0

METAVERSE

CHANCEN UND RISIKEN

Beim Metaverse handelt es sich um einen digitalen Raum, der durch das Zusammenwirken virtueller, erweiterter und physischer Realität entsteht. In einer von KnowBe4 im September 2022 durchgeführten Umfrage wurden 201 Personen zum Thema Metaverse befragt. Die Mehrheit der Befragten hat eine klare Vorstellung vom Metaverse, so stellt sich etwa die Hälfte darunter eine virtuelle Realität vor. Je rund ein Zehntel denken dabei an eine reine Gaming-Welt und rund 20 Prozent haben bisher noch gar nichts davon gehört. Es ist interessant zu beobachten, dass für ein gutes Drittel (35 Prozent) die Vorteile des neuen digitalen Raums überwiegen. Lediglich ein geringer Anteil (14 Prozent) sehen das Metaverse kritisch und nur drei Prozent bewerten es klar negativ.

Chancen und Risiken des Metaverse

Die neue Technologie bringt viele Chancen und Risiken mit sich, wobei die Umfrageteilnehmer sich uneinig sind welche Seite überwiegt. Etwa die Hälfte der Befragten sehen die Potenziale des Metaverse besonders im sozialen Bereich und 37 Prozent denken, dass es Vorteile für die gesamte Gesellschaft bedeuten könnte. 36 Prozent sehen die Möglichkeit, dass es die Wissenschaft vorantreiben kann und rund ein Drittel halten es im wirtschaftlichen Spektrum für vorteilhaft. Nur 18 Prozent gaben an, dass sie in keinem Bereich besondere Chancen für das Metaverse erkennen.

Die Befragten waren sich aber durchaus bewusst, dass in einigen Bereichen auch potenzielle Risiken im Zusammenhang mit dem Metaverse auftreten können. Hierbei sehen über 60 Prozent der Teilnehmer die größte Gefahr für die Nutzer in einer möglichen Suchtgefahr und drohendem Realitätsverlust. Der noch fehlende rechtliche Rahmen bei der Nutzung dieser Innovation bereitet fast der Hälfte Sorgen und rund 40 Prozent stufen den die Möglichkeit des Missbrauchs des Metaverse durch Kriminelle als eine Bedrohung ein.

Viele Personen denken, dass das Metaverse in Zukunft äußerst relevant sein wird für ganz verschiedene Spektren des Lebens. So gehen über 35 Prozent der Befragten sogar davon aus, dass es auf alle Lebensbereiche Einfluss nehmen wird. Knapp 37 Prozent vermuten, dass es im Freizeitbereich relevant sein wird, wohingegen lediglich 14 Prozent davon ausgehen, dass es in Zukunft auch im beruflichen Umfeld wichtig wird.

www.knowbe4.de

NUTZEN SIE DAS METAVERSE?

60% nutzen das Metaverse noch nicht, planen es aber

9% sind aktiv im Metaverse unterwegs

30% haben kein Interesse das Metaverse jetzt oder später zu nutzen

SO STÄRKEN KMU IHRE CYBERRESILIENZ

MEHR WIDERSTANDSKRAFT GEGENÜBER CYBERBEDROHUNGEN

Resilienz – dieser Begriff aus der Psychologie bezeichnet die Fähigkeit, Lebenskrisen und Rückschläge zu meistern. Immer häufiger wird das Konzept auch auf Cybersicherheit angewendet. Wie widerstandsfähig sind kleine und mittlere Unternehmen (KMU) gegenüber Cyberbedrohungen? Und wie können KMU ihre Cyberresilienz steigern? Darüber sprach Ulrich Parthier, Publisher it management, mit Waldemar Bergstreiser, Head of B2B Germany bei Kaspersky.

? **Ulrich Parthier:** *Herr Bergstreiser, die Corona-Pandemie hat KMU in den letzten Jahren auf eine harte Bewährungsprobe gestellt. Wenn es überall brennt, fällt es schwer zu entscheiden, wo man zuerst löschen soll. Wo sehen Sie das Thema Cybersicherheit inmitten vieler konkurrierender Prioritäten angesiedelt?*

Waldemar Bergstreiser: Leider gehen KMU ihre Cybersicherheit häufig per Vogel-Strauß-Taktik an. Einerseits ist ihnen bewusst, dass ein Cyberangriff eine ernstzunehmende Krise für ihr Unternehmen darstellen würde. Laut dem aktuellen Cyberresilienz-Report von Kaspersky rangieren Cybervorfälle gleich auf Platz zwei der härtesten Krisen, vor denen sich KMU in Deutschland fürchten – direkt hinter Umsatzverlusten. 13 Prozent der Befragten in Deutschland gaben sogar an, dass sie einen Cyberangriff als die bedrohlichste Art von Krise für den eigenen Betrieb sehen würden.

Andererseits haben nur wenige Unternehmen (38 Prozent) eine Strategie für den Fall einer Cyberattacke in petto; 17 Prozent denken, sie brauchen keinen IT-Notfallplan, weil sie davon ausgehen, dass sie im Falle eines Angriffs auf einer ad-hoc-Basis entscheiden können. Bei einer Cyberattacke ist es jedoch extrem wichtig, vorbereitet zu sein. Nur so ist es möglich, schnell und vor allem wirksam zu reagieren, um den Schaden zu minimieren.

? **Ulrich Parthier:** *Wie erklären Sie sich diese Kluft zwischen Fühlen und Handeln?*

Waldemar Bergstreiser: Häufig denken KMU, dass sie durch ihre geringe Größe weniger gefährdet sind, weil sie meinen sie befänden sich noch quasi unter der Aufmerksamkeitsschwelle der Cyberkriminellen.

? **Ulrich Parthier:** *Und das stimmt nicht?*

Waldemar Bergstreiser: Das stimmt immer weniger, je mehr die Angreifer ihre Methoden perfektionieren. Zum Beispiel lassen sich Unternehmenszugänge im Darknet schon ab wenigen Hundert Euro kaufen [1]. Der Preis hängt oft vom Umsatz des Unternehmens ab. Sind die Kosten eines Cyberangriffs niedriger als der erwartete Gewinn, lohnt sich ein Angriff für die Täter. Das ist eine simple Kosten-Nutzen-Rechnung.

Der Schaden für das betroffene Unternehmen ist dagegen viel dramatischer. Neben direkten finanziellen Kosten entstehen weitere schwer messbare Verluste – zum Beispiel durch die Rufschädigung und daraus resultierende Wettbewerbsnachteile.

? **Ulrich Parthier:** *Welche Empfehlung leiten Sie aus dieser Erkenntnis für Entscheider in kleinen und mittelständischen Unternehmen ab?*

Waldemar Bergstreiser: Machen Sie den Angreifern das Leben schwer, schließen Sie offenkundige Sicherheitslücken. Ein vermeidbares Risiko ist veraltete Software. Updates von Software- und Geräteherstellern sollten schnellstmöglich installiert werden. Meist enthalten diese nicht nur neue Features, sondern beheben auch bereits erkannte Schwachstellen. Und erstellen Sie regelmäßige Backups Ihrer wichtigsten Daten. Dann können Sie einfach auf die Sicherungskopie

CYBERRESILIENZ-REPORT

Den neuen Cyberresilienz-Report von Kaspersky mit vielen Tipps, wie KMU ihre Widerstandsfähigkeit gegen Cyberangriffe steigern können, gibt es hier kostenfrei zum Download: **kas.pr/cyberresilienz**

[1] https://www.kaspersky.de/about/press-releases/2022_unternehmenszugange-kosten-im-dark-web-2000-us-dollar
[2] https://www.kaspersky.de/password-manager
[3] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents
[4] https://asap.kaspersky.com/de
[5] https://www.kaspersky.de/small-to-medium-business-security/cloud
[6] https://www.kaspersky.de/about/press-releases/2021_av-test-bestatigt-kaspersky-endpoint-security-cloud-bietet-100-prozent-schutz-vor-ransomware
[7] https://go.kaspersky.com/de_optimum

> HÄUFIG GEHEN KMU IHRE CYBERSICHERHEIT PER VOGEL-STRAUSS-TAKTIK AN. BEI EINER CYBERATTACKE IST ES JEDOCH EXTREM WICHTIG, VORBEREITET ZU SEIN.
>
> Waldemar Bergstreiser,
> Head of B2B Germany, Kaspersky,
> www.kaspersky.de

zugreifen, wenn ihre Daten durch einen Angriff per Ransomware, also Erpressersoftware, verschlüsselt wurden.

? **Ulrich Parthier:** *Können Sie weitere Beispiele für einfache, aber wirksame Sicherheitsmaßnahmen nennen?*

Waldemar Bergstreiser: Unternehmen brauchen eine solide Passwortpolitik: Mitarbeiter sollten für jeden Dienst ein eigenes starkes Passwort verwenden. Eine Sicherheitslösung mit einem integrierten Passwort Manager erleichtert dies [2]. Sehr wichtig ist auch, dass Berechtigungen jederzeit up-to-date sind. Mitarbeiter sollten immer nur Zugriff auf diejenigen Systeme und Bereiche haben, die sie wirklich auch benötigen. Wenn Mitarbeiter das Unternehmen verlassen, muss ihr Zugang sofort gesperrt werden. Unsere Umfrage hat jedoch gezeigt, dass Systemzugänge in KMU häufig eine Blackbox sind. Nur 46 Prozent, weniger als die Hälfte der Befragten in Deutschland, konnten ausschließen, dass Ex-Mitarbeiter noch auf ihre Unternehmensaccounts zugreifen können.

? **Ulrich Parthier:** *Würden Sie sagen, dass der Mensch der größte Risikofaktor für Cybersicherheit ist?*

Waldemar Bergstreiser: Über 80 Prozent aller Cybersicherheitsvorfälle gehen auf menschliche Fehler zurück [3]. Deshalb ist es wichtig, Cybersicherheit im Unternehmen zum Thema zu machen. Es sollten regelmäßig praxisnahe Security Awareness-Schulungen in den Arbeitsalltag integriert werden. Eine interaktive Online-Trainingsplattform wie Kaspersky Automated Security Awareness Platform bietet den Mitarbeitern Gelegenheit, sich mit typischen Angriffsszenarien auseinanderzusetzen. So können sie – zum Beispiel anhand von simulierten Phishing-Mails – ihr Sicherheitsbewusstsein schärfen [4].

Cyberhygiene funktioniert aber nicht wirklich, solange sie im Unternehmen nicht als Chefsache angekommen ist. Eine besorgniserregende Erkenntnis aus dem aktuellen Report: Immerhin 12 Prozent der Entscheider in KMU würden sogar raubkopierte Software kaufen, wenn sie ihr IT-Budget reduzieren müssten. Vermutlich ist denjenigen nicht bewusst, wie hoch das Risiko ist, dass sie sich mit Software von dubiosen Quellen nicht nur eine, sondern verschiedenste Arten von Schadsoftware einfangen können.

? **Ulrich Parthier:** *Damit kommen wir wieder zum Thema Ressourcenknappheit! Diese trifft KMU doch auf allen Ebenen. Oft haben sie wenig Geld, wenig Fachkräfte, wenig Zeit…*

Waldemar Bergstreiser: Umso wichtiger ist es, dass sie eine zuverlässige umfassende Sicherheitslösung einsetzen, die ihnen manuelle Tätigkeiten abnimmt. Zum Funktionsumfang sollte die Erkennung und Blockierung unbekannter Malware gehören, bevor diese ausgeführt wird, sowie das Anlegen automatischer Backup-Kopien. Kaspersky Endpoint Security Cloud [5] schützt vor einer Vielzahl an Bedrohungen, auch zu 100 Prozent vor Ransomware – das bestätigt AV-TEST [6]. Entwickelt sich das Unternehmen weiter, sollte auch die Sicherheitsstufe erhöht werden. Wir bieten eine skalierbare Produktpalette, die mit den Anforderungen wächst.

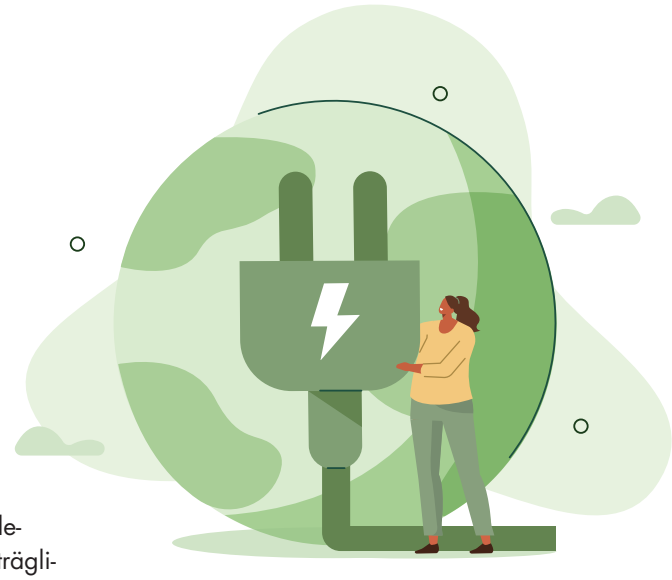
? **Ulrich Parthier:** *Wie könnte ein Upgrade für Cybersecurity aussehen?*

Waldemar Bergstreiser: Es wird immer wichtiger, Cyberangriffe so früh wie möglich zu erkennen und zu neutralisieren. Dafür ist menschliche Expertise gefragt. Gibt es dieses Fachwissen im Unternehmen nicht oder sind die Ressourcen knapp, können externe Sicherheitsexperten unterstützen. Der Managed Detection und Response (MDR) Service von Kaspersky bietet vielseitige Funktionen – fortschrittliche Schutzmechanismen, proaktives Threat Hunting oder Automated and Guided Response. Durch die Kombination aus einer automatisierten Sicherheitslösung (Endpoint Detection and Response) mit MDR erreichen Unternehmen ein hohes Sicherheitslevel. Gerade für agile Kleinunternehmen in Zeiten hoher Unsicherheit ist es ein großer Vorteil, ihre Cybersicherheit zu erhöhen ohne die internen Ressourcen dafür erweitern zu müssen [7].

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

GREEN IT

NACHHALTIGKEIT EFFEKTIV PLANEN UND NACHWEISEN



Durch die zunehmende Digitalisierung benötigen Rechenzentren und IT-Infrastrukturen immer mehr Strom. Daher müssen Unternehmen über geeignete Ansätze und Tools für mehr Transparenz im Nachhaltigkeitsportfolio verfügen.

16 Milliarden Kilowattstunden: So viel Energie haben die Rechenzentren in Deutschland im Jahr 2020 laut Bitkom verbraucht. Das war deutlich mehr als der

Strombedarf der Stadt Berlin im gleichen Zeitraum. Und der Energieverbrauch wird weiter steigen, da immer mehr Daten zu übertragen und zu bearbeiten sind.

In Zeiten rasant steigender Strompreise können sich immer weniger Unternehmen den Risiken der durch IT-Systeme verursachten laufenden Kosten verschließen. Dieser Gedanke ist aber bislang für viele CTOs noch weit entfernt. Denn sie haben sich auf andere Probleme wie die Bewältigung des Personalmangels oder den Schutz vor modernen Angriffen konzentriert. Doch diese Zeiten sind vorbei. Green IT muss ab sofort im Fokus aller Unternehmen stehen.

Was gehört zu Green IT?

Das Bundesumweltministerium definiert Green IT als „umweltverträgliche Produkte und Dienstleistungen der Informations- und Kommunikationstechnik (IKT) sowie der Nutzung von IKT zur Umweltschonung." Dies umfasst jedoch den gesamten Lebensweg von IKT-Produkten sowie deren Auswirkungen auf Klima und Umwelt, zum Beispiel durch kritische Rohstoffe.

Damit wird klar, dass es bei Green IT nicht nur um die Vermeidung von Energieverbrauch und somit auch die Reduzierung des CO_2-Ausstoßes geht, sondern auch um Schwermetalle oder andere umweltschädliche Stoffe. Diese sind in vielen IKT-Komponenten – von Laptops über Smartphones, Router und Switches bis hin zu Druckern – enthalten.

Daher müssen Unternehmen darauf achten, dass Neugeräte umweltschonend hergestellt werden sowie ausgemusterte Geräte und Komponenten nicht einfach im Müll landen. Sie sollten gezielt an zertifizierte Dienstleister, Gerätehersteller oder IT-Händler gegeben werden, die diese wiederaufbereiten oder umweltgerecht entsorgen.

Gesamtstrategie entwickeln

Unternehmen sollten entsprechend eine Gesamtstrategie für Green IT erstellen, die alle Bereiche umfasst. Diese basiert auf einer Ist-Analyse, die den aktuellen Stromverbrauch der dadurch erreichten Leistung gegenüberstellt. Bei dieser Energiebilanz müssen jedoch alle IT-Komponenten und Infrastrukturen vom Rechenzentrum über die Netzwerke und Endgeräte bis zu mobilen und IoT-Devices berücksichtigt sein. Alleine durch den direkten Vergleich fallen schon die größten Stromfresser auf.

Zusätzlich sollte die Ist-Analyse das Alter und die Zusammensetzung der Komponenten ermitteln. Ältere Geräte verbrauchen meist mehr Energie für weniger Leistung. Sie sind oft auch störanfälliger und weisen mehr Sicherheitslücken auf. Ausfälle erhöhen jedoch ebenfalls den Stromverbrauch aufgrund der anfallenden Reparatur- und Behebungsprozesse.

Nicht zuletzt sind die Geräte auf umweltschädliche Stoffe zu prüfen. Bei Druckern

MIT DER ENERGIEKRISE RÜCKT GREEN IT ZUNEHMEND IN DEN FOKUS. ALLERDINGS IST DER STROMVERBRAUCH DABEI NUR EIN ASPEKT. UNTERNEHMEN BRAUCHEN EINE GESAMTSTRATEGIE, DIE ALLE BEREICHE UMFASST.

Lea Kraus, Consultant, Campana & Schott, www.campana-schott.com

geht es zusätzlich um das Feinstaubthema. Aber auch die erzeugte Abwärme kann eine Herausforderung darstellen, da sie den Kühlaufwand erhöht. Zudem sind die Kühlprozesse und Klimaanlagen selbst zu prüfen: Wie viel Energie und Wasser verbrauchen sie und welche Kühlflüssigkeit wird genutzt?

Die Fortschritte messen

Anhand dieser Ist-Analyse lassen sich die notwendigen Maßnahmen ermitteln und priorisieren. Daraus ergibt sich die Green-IT-Strategie, die einen Gesamtüberblick über die Projekte bietet. Diese sollte bei Bedarf mit der IT- und Geschäftsstrategie abgeglichen werden. Die nächste Herausforderung liegt jedoch in der Umsetzung und Erfolgsmessung der Projekte. So sollten von Anfang an Metriken klar anzeigen, ob die getroffenen Maßnahmen auch ihren Zweck erreichen und das Unternehmen sich insgesamt auf dem richtigen Weg befindet.

Zum Beispiel möchte ein Unternehmen bis zum Jahr 2030 im IT-Bereich klimaneutral werden. Um den Fortschritt der Zielerreichung messen zu können, ist ein standardisierter Indikator festzulegen, in diesem Fall die CO_2-Reduktion. Nach Analyse des Status quo ermittelt das Unternehmen etwa, dass es 10.000 Tonnen CO_2 einsparen muss, um Klimaneutralität zu erreichen. Auf ähnliche Weise werden alle Nachhaltigkeitsziele formuliert und können mit Hilfe eines einheitlichen KPI-Registers standardisiert messbar gemacht werden.

Auch wenn viele Unternehmen bereits Maßnahmen im Bereich Green IT planen oder umsetzen: Einem Großteil fehlt noch der Überblick über die laufenden Projekte. Doch genau diese Transparenz ist ein wichtiger Erfolgsfaktor bei der Steuerung von Maßnahmen und der Herleitung von Synergien zwischen verschiedenen Nachhaltigkeitsprojekten. Ein umfassendes Projektportfoliomanagement mit einer Erfolgsmessung der einzelnen Projekte anhand von KPIs bietet genau diesen Gesamtüberblick.

UNTERNEHMEN, DIE IHRE NACHHALTIGKEITSZIELE ERNST NEHMEN, KOMMEN AN GREEN IT NICHT VORBEI. MIT EINER SUSTAINABILITY TRACKING APP STEUERN SIE ENTSPRECHENDE PROJEKTE SYSTEMATISCH UND HOCHWIRKUNGSVOLL.

Lennard Everwien, Head of Business Sustainability, Campana & Schott
www.campana-schott.com

Die Sustainbility Tracking App

Eine praktische Möglichkeit zum systematischen Erfassen und Verfolgen von Nachhaltigkeitsmaßnahmen bietet etwa die CS Sustainability Tracking App. Sie zeigt auf einen Blick, welche Maßnahmen auf welche Ziele einzahlen und welchen Status diese besitzen. Neben allgemeinen Informationen können Finanzkennzahlen sowie weitere Nachhaltigkeits-Frameworks integriert werden. Die Maßnahmen lassen sich in unterschiedliche Phasen einteilen, damit der Projektfortschritt vergleichbar und der Realisierungsstand kontinuierlich verfolgt wird.

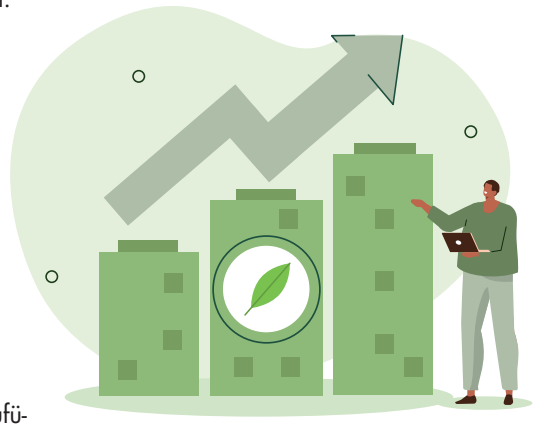
Technologisch basiert die App auf der Microsoft Power Platform. Diese Low-/No-Code-Lösung ermöglicht es, ohne spezielle Programmierkenntnisse mit Hilfe einfacher Bausteine, Funktionalitäten einzubauen und individuell zu gestalten. So lassen sich Änderungswünsche schnell umsetzen und das Nachhaltigkeits-Framework erweitern. Dazu gehören etwa das Hinzufügen von ESG-Faktoren oder die Individualisierung des Berichtswesens um weitere KPI-Analysen.

Die App zeigt auch, welchen konkreten Nutzen die geplanten Projekte in Bezug auf die strategischen Nachhaltigkeitsziele bieten. Dies hilft bei der Priorisierung der Schritte, bei gleichzeitiger Beachtung limitierter Budgets und Ressourcen. Über ein integriertes KPI Tracking Board können Verantwortliche immer den aktuellen Fortschritt der Maßnahmen sehen und bei Bedarf anpassen. Durch konkrete Kennzahlen wird der tatsächliche Impact der einzelnen Maßnahme auf ein oder mehrere Nachhaltigkeitsziele messbar. Das Sustainability Dashboard teilt die Maßnahmen in Handlungsfelder ein und gibt mit thematischen Clustern einen noch besseren Überblick. Dadurch wird der gegenwärtige Erreichungsgrad jedes Nachhaltigkeitsziels aufgezeigt und der Nutzen einzelner Maßnahmen transparent gemacht.

Fazit

Ob Klima- oder Energiekrise: Green IT wird zu einer wirtschaftlichen Notwendigkeit für Unternehmen. Durch die Erfolgsmessung einzelner Maßnahmen können sie das Erreichen der Nachhaltigkeitsziele steuern. Die CS Sustainability Tracking App hilft dabei, diese Ziele zu definieren, passende Maßnahmen systematisch und transparent zu erfassen sowie die Zielerreichung laufender Maßnahmen kontinuierlich zu tracken.

Lea Kraus, Lennard Everwien



NACHHALTIGKEIT IST KEINE BUDGETFRAGE

GREENTECH-STUDIE VON MHP ZEIGT, DASS DIGITALE TECHNOLOGIEN DER ERFOLGSFAKTOR SIND

Der Preis für Strom steigt und damit auch die Kosten für Rechenzentren. Mittelfristig sollen sich laut Bitkom auch die Cloud-Dienste verteuern. Dennoch kann die IT trotz aktueller Kostenexplosionen nachhaltiger und budgetfreundlicher werden.

Die IT-Verantwortlichen haben zum Ende des Jahres einiges auf dem Zettel. Vermutlich werden die steigenden Kosten und Einsparungspotenziale in der IT für das Jahr 2023 ganz oben auf der Liste stehen. Die gute Nachricht: IT-Abteilungen erhalten laut der Lünendonk-Studie „Der Markt für IT-Dienstleistungen in Deutschland" mehr Budget. Dabei liegt der Fokus der Investitionen für 2023 auf der IT-Modernisierung, Cloud-Transformation oder im Aufbau digitalisierter und intelligent automatisierter Prozessketten sowie in Datenanalysen. Die schlechte Nachricht: Eine grüne IT ist weder in der Budgetplanung ein Schwerpunkt, noch haben viele Unternehmen Nachhaltigkeitsstrategien in der IT bereits umgesetzt. Das ist zu wenig angesichts der CSRD-Richtlinie, die ab 2023 Nachhaltigkeitsberichte auch für kleinere und mittelständische Unternehmen ab einer Belegschaftsgröße von 250 Mitarbeitenden vorschreibt. Dabei können IT-Lösungen bei der Umsetzung ökologischer und ökonomischer Ziele eine bedeutende Rolle spielen. Deshalb ist es wichtig, den Blick auf die IT in den Unternehmen und über die gesamte Lieferkette hinweg zu richten.

Quo vadis Green IT?

Das Problem: Die wenigsten Unternehmen haben Kenntnis über ihren CO_2-Austoß – und es besteht laut der Lünendonk-Studie auch keine Transparenz darüber. Nur 18 Prozent der befragten Unternehmen kennen ihren CO_2-Verbrauch, und wiederum nur 12 Prozent davon können den CO_2-Austoß auf ihre IT herunterbrechen. Ein Viertel der Unternehmen plant nicht einmal, den CO_2-Fußabdruck in der IT-Lieferkette zu messen und transparent aufzubereiten. Ein Grund

dafür könnte die befürchtete Komplexität der Aufgabe sein. Denn hier müssen zwei Seiten betrachtet werden: Zum einen die in den Unternehmen selbst eingesetzte Hardware. Damit ist in erster Linie der Betrieb von Client PCs und Servern in den Rechenzentren gemeint, außerdem die Herstellung und Entsorgung der Arbeitsgeräte. Zum anderen müssen auch alle SaaS- und IaaS-Lösungen betrachtet werden. Denn jede digitale und virtuelle Anwendung verbraucht Energie und Rohstoffe – und verursacht damit irgendwo auf dem Planeten Emissionen.

Quadratur des Kreises

Ein Beispiel: KI-Anwendungen können helfen, CO_2-Emissionen zu ermitteln und damit steuerbar zu machen. Gleichzeitig fordert der Einsatz von KI viel Rechenleistung, insbesondere das Trainieren eines KI-Modells mit großen Datenmengen. Dadurch steigt der Bedarf an Servern und zugleich die Energiemenge zur Kühlung der Rechenzentren. Und doch kommt digitalen Technologien eine besondere Rolle bei der Erreichung von Nachhaltigkeitszielen zu. Zur Erinnerung: Deutschland muss in den kommenden zehn Jahren 372 Millionen Tonnen CO_2 einsparen. Werden digitale Technologien wie KI, IoT und digitaler Zwilling weiter ausgebaut, können jährlich bis zu 126 Millionen Tonnen CO_2 netto reduziert werden. Auch die Autoren der Bitkom-Studie „Klimaeffekte der Digitalisierung" stellen fest, dass eine gezielte und beschleunigte Digitalisierung bis zu 58 Prozent CO_2 einsparen kann. Dabei ist das CO_2-Einsparpotenzial dieser Technologien bis zu sechs Mal größer als ihr Ausstoß. Zu einem ähnlichen Ergebnis kommt unsere aktuelle Studie „GreenTech - Made in Germany", die wir gemeinsam mit der Hochschule Reutlingen veröffentlicht haben. Die Expert*innen sind sich einig, dass digitale Technologien einen entscheidenden Beitrag für die Nachhaltigkeitsziele leisten können.

KLIMAPFADE ZU DEFINIEREN UND ZU SIMULIEREN, IST EIN WIRKUNGSVOLLES VORGEHEN, UM DEKARBONISIERUNGSZIELE ZU ERREICHEN.

Simon Alexander Appel,
Senior Consultant Sustainability and Mobility Transformation, MHP,
www.mhp.com

Wie kann es aber in der Praxis gelingen, dass digitale Technologien einen verbesserten CO_2-Fußabdruck der Unternehmen und insbesondere in der IT-Lieferkette hinterlassen? Und wie gelingt das Unterfangen vor dem Hintergrund des aktuellen Kostendrucks, beispielsweise durch steigende Strompreise und den damit erhöhten finanziellen Aufwand für das Betreiben von Rechenzentren?

Unsere These: Beide Ziele, können gleichzeitig gelingen. Dabei müssen CIOs und IT-Verantwortliche nicht zwingend erst das ganz große Circular-Economy-Konzept abwarten, bei dem ganzheitlich im Unternehmen ein geschlossener Materialkreislauf realisiert wird. Auch kurz- und mittelfristig lassen sich mit einem reinen Green IT-Projekt Emissionen und Kosten einsparen – bei künftig weiter steigenden Preisen für Primärrohstoffe und CO_2-Abgaben kann das ein entscheidender Wettbewerbsfaktor sein.

Drei Schritte: CO_2-Status, Roadmap und Dekarbonisierung

In einem ersten Schritt sollte entlang der Dimensionen Infrastruktur, Software und Hardware der Stand der CO_2-Emissionen ermittelt werden, beispielsweise auf Basis des Greenhouse Gas Protocols. In einem zweiten Schritt ist dann eine Roadmap entlang dieser Dimensionen zu entwickeln. Mithilfe von Climate-Impact-Modellen sind IT-Verantwortliche in der Lage, einen spezifischen Klimapfad festzulegen und im Sinne eines Top-down-Ansatzes eine individuelle Dekarbonisierungszielesystematik im Einklang mit dem 1,5-Grad-Ziel sowie dem vorher definierten Carbon Budget der IT aufzustellen. Für jede Dimension lassen sich dann Dekarbonisierungsmaßnahmen entwickeln. So können sie später auf ihre Wirksamkeit hin validiert werden.

WER NACHHALTIGKEIT ZU EINEM ZENTRALEN UND GANZHEITLICHEN THEMA IM UNTERNEHMEN MACHT, WIRD DAVON AUCH IM BUSINESS PROFITIEREN.

Nikolas Bradford,
Associated Partner und Head of Sustainability Services, MHP,
www.mhp.com

Wir sehen vor allem auf der Ebene der IT-Infrastruktur einen der größten Hebel, um Kosten und Emissionen einzusparen. Hier könnte eine Dekarbonisierungsmaßnahme sein, das Rechenzentrum oder Teile davon in die Cloud auszulagern. Cloud-Services können gegenüber einem herkömmlichen Rechenzentrum bis zu 93 Prozent Energie- und bis zu 98 Prozent CO_2-Emissionen einsparen.

Auf der Ebene Hardware lassen sich die gewünschten Ziele schnell und mit einfachen Maßnahmen erreichen: Der Einkauf erstellt neue Richtlinien (Entscheidungskriterien) für einen „nachhaltigen" Hard-

wareeinkauf. Wir setzen verstärkt refurbished Geräte ein und verlängern die Laufzeit bestehender Geräte um bis zu zwei Jahre. Dadurch lässt sich einerseits eine komplette Gerätegeneration einsparen – samt der bei ihrer Herstellung entstehenden Emissionen. Andererseits sparen Unternehmen mit dem Einsatz von refurbished Hardware bares Geld, da sie bis zu 50 Prozent günstiger als vergleichbare Neuware ist.

Neue Konzepte wie smart- oder ressourcenschonendes Programmieren können Unternehmen auf der Software-Ebene umsetzen, wobei KI der größte zukünftige CO_2 Treiber werden wird. Auch hier gibt es gute Ansätze, beispielsweise. optimierte Machine- Learning-Modell-Architekturen, die Nutzung von speziell für KI entwickelte Prozessoren sowie die Verlagerung in „grüne" Cloud-Regionen und das vermehrte Finetuning von vortrainierten Modellen. Auch auf den Einkauf werden unter der Überschrift Responsible KI bald weitere neue Aufgaben zukommen.

Fazit

Green IT-Projekte lassen sich schnell starten und realisieren damit auch kurzfristig Quick-Wins. Dekarbonisierungsmaßnahmen in der IT können aber am Ende nur so gut sein, wie CIOs und IT-Verantwortliche eine nachhaltige IT vorleben und die Mitarbeiter*innen auf diesem Weg mitnehmen. Die Umsetzung wird nur dann erfolgreich, wenn das richtige Bewusstsein bei den Mitarbeitenden geschaffen wird und sie von Anfang an in Maßnahmen, wie die längere Nutzung von Geräten oder gebrauchte Geräte, eingebunden werden.

Nikolas Bradford, Simon Alexander Appel, Christian Rudolf

DURCH GREEN IT WERDEN DIE POTENZIALE DER DIGITALISIERUNG GENUTZT UND GLEICHZEITIG EIN IMMENSER BEITRAG ZUR ERREICHUNG DER NACHHALTIGKEITSZIELE IM UNTERNEHMEN GELEISTET.

Christian Rudolf,
Manager Sustainability Transformation/
Expert GreenIT, MHP, www.mhp.com

IT-STRUKTUREN NACHHALTIG OPTIMIEREN

ZUKUNFTSFÄHIGE AUSRICHTUNG DANK GRÜNER MANAGED IT SERVICES

Die heutige IT-Welt ist schnelllebiger und anspruchsvoller als je zuvor. Im Unternehmensalltag ist es kaum noch möglich, die neuesten technologischen Weiterentwicklungen immer im Blick zu haben. Insbesondere kleine und mittelständische Unternehmen verfügen nicht über ausreichende Ressourcen, um ihre IT-Landschaft flächendeckend und ganzheitlich zu steuern.

Daher werden vermehrt externe Spezialistinnen und Spezialisten engagiert, die die Sicherstellung des reibungslosen IT-Betriebs im Unternehmen übernehmen. Zunehmend geht es nicht mehr nur darum, auf Probleme und Störungen zu reagieren, sondern vielmehr steht eine strategische Partnerschaft auf Augenhöhe im Fokus. Entsprechende Dienstleister beraten proaktiv in Digitalisierungsthemen und befähigen ihre Kunden dazu, sich durch nachhaltige Konzepte zukunftsfähig auszurichten. Ein smarter Weg, um IT-Ressourcen auszulagern.

EIN MANAGED SERVICE PROVIDER WEISS, DASS JEDER KUNDE, JEDES PROJEKT EINZIGARTIG IST. FOKUS LIEGT AUF DER GANZHEITLICHEN BETRACHTUNG, WEG VON INSELLÖSUNGEN, HIN ZU EINER RESSOURCENSCHONENDEN UND SKALIERBAREN IT-LÖSUNG FÜR DEN DIGITALEN BÜROALLTAG.

Christian Hoffmeister,
CIO, GREEN IT Das Systemhaus GmbH,
www.greenit.systems

Managed Services

Als Managed Service Provider, kurz MSP, bezeichnet man den Anbieter, welcher im Auftrag eines Unternehmens wiederkehrende IT-Dienstleistungen extern durchführt. Dabei stehen die ganzheitliche Beratung und Betreuung rund um den IT-Arbeitsplatz im Fokus. Ein MSP kümmert sich um die Beschaffung von Hard- und Software, integriert die Bereiche Cloud Solutions, IT Security und im Idealfall auch die digitale Kommunikation, das Dokumentenmanagement sowie Print Services.

Durch die Zusammenarbeit mit einem MSP können Unternehmen zahlreiche Vorteile bei der Virtualisierung, Konsolidierung und Optimierung von IT-Infrastrukturen erreichen – und das gänzlich ohne Schnittstellenverluste. Dabei haben MSPs ein klares Ziel vor Augen: die Schaffung langfristig stabiler Strukturen und Prozesse statt kurzfristige Fehlerbehebung.

Durch proaktive Wartung im Umfeld der wichtigsten digitalen Infrastrukturen wird die Fehleranfälligkeit eines Systems deutlich reduziert und so die unternehmensinterne Effizienz signifikant gesteigert. Weiterer Vorteil: Durch die vorab vereinbarten Leistungen fallen keine unerwarteten Zusatzkosten an, die Ausgaben sind demnach optimal planbar.

Nachhaltige Vorteile

Die zunehmende Digitalisierung hat sich durch den überproportional steigenden Stromverbrauch zu einem wichtigen Faktor für den Klimaschutz entwickelt. Nachhaltig denkende IT-Dienstleister setzen genau dort an, um die IT in Unternehmen klimaneutral zu gestalten. Eine optimale Beratung durch externe MSPs ist demnach strategisch ausgerichtet und hat die Themen Nachhaltigkeit und Zukunftsfähigkeit der eingesetzten IT stets im Fokus. Kunde und Dienstleister arbeiten gemeinsam an der Vision des Green Digital Office. Eine große Rolle spielt dabei der Einsatz von grüner IT, also langlebiger und energieeffizienter Hardware, digitaler und papierloser Arbeitsweise sowie Strombezug aus erneuerbaren Energien. Ein MSP kennt die Möglichkeiten, nachhaltige Lösungen und Tools zu integrieren, wie zum Beispiel Hosting im grünen Rechenzentrum, Strombezug durch mobile All-in-one-Solaranlagen oder stationäre Photovoltaik.

Stephanie van de Straat

UMWELTBEWUSSTSEIN IN UNTERNEHMEN

5 TIPPS ZUM ENERGIE- UND KOSTENSPAREN

Neben Themen wie Remote Work, Mental Health und Work-Life-Balance gewinnt auch das Thema Nachhaltigkeit für die Unternehmenskultur weiter an Bedeutung. Angesichts der stetig steigenden Energiepreise sind Unternehmen bestrebt, ihre Energiekosten dauerhaft zu minimieren.

Das bestätigt auch eine aktuelle Umfrage von Verivox: Mehr als die Hälfte der Deutschen (57 Prozent) möchte ihren Energieverbrauch senken. Gleiches gilt für Unternehmen, denn gerade im Cloud-Geschäft führt die immer größer werdende Datenmenge zu einem enormen Stromverbrauch. Auf die IT-Branche entfielen im Jahr 2020 fünf bis 15 Prozent des globalen Energieverbrauchs. Damit zählt der nach wie vor schnell wachsende Sektor zu einem der wichtigsten Zielbereiche für nachhaltige Umstrukturierungen. Bei Kommunikationsnetzen (36 Prozent), Rechenzentren (30 Prozent) und Computern (34 Prozent) ist der Energieverbrauch nach Auswertungen von Digital Information World besonders hoch und bietet Ansätze für Einsparungen.

1. Umzug in die Cloud

Die Migration von Daten in die Cloud spielt eine entscheidende Rolle bei der Senkung des Energieverbrauchs in Unternehmen. Denn Cloud-Server ermöglichen einen schnellen Zugriff auf Systemressourcen wie Datenspeicher, Datenbanken und Software. Infolgedessen benötigen Unternehmen weniger eigene Server und können ihren Energieverbrauch und die Umweltbelastung durch das interne Rechenzentrum minimieren.

Zusätzlich können sie die eigene Hardware-Ausstattung überdenken. Viele Unternehmen haben niedrige Auslastungsraten, weil sie in Erwartung von Serverlastspitzen zusätzliche Geräte angeschafft haben. Bei Servern in der Cloud hingegen ist die Hardware-Nutzung konsolidiert, sie lassen sich daher mit hoher Effizienz betreiben. Insgesamt soll Cloud Computing bis zu 2024 Milliarden Tonnen an CO_2-Emissionen einsparen, da große Cloud-Speicherzentren den Strombedarf und die Kühlungsleistung effektiver managen und energieeffizientere Server einsetzen.

2. Virtualisierung verhilft zu effizienter Servernutzung

Wenn Unternehmen ihre Server für bestimmte Anwendungen einplanen, die nur mit einem Bruchteil ihrer tatsächlichen Kapazität arbeiten, ist dies äußerst ineffizient und führt zu einer Überkapazität an Serverleistung, die nicht dauerhaft genutzt wird. Dadurch steigen sowohl der Energieverbrauch als auch die Betriebskosten, ohne wirtschaftlichen Mehrwert. Mithilfe von Virtualisierung können Unternehmen jedoch virtuelle Versionen von Servern, Betriebssystemen, Netzwerkressourcen oder Speichergeräten erstellen und auch mehrere Betriebssysteme und Anwendungen auf weniger Servern laufen lassen. Das schont die Server-Ressourcen um etwa 40 Prozent.

VIRTUALISIERUNG UND CLOUD-SERVICES HELFEN, DIE SERVERAUSLASTUNG ZU STEIGERN UND GLEICHZEITIG DEN HARDWARE- UND ENERGIEBEDARF DEUTLICH ZU REDUZIEREN

Prashant Ketkar, Chief Technology and Product Officer, Alludo, www.alludo.com

Zusätzlich reduziert eine virtualisierte IT-Umgebung die Kosten für Speicherplatz, Strom, Heizung und Kühlung im Data Center. Auf diese Weise lassen sich die Energiekosten eines Unternehmens um 40 bis 80 Prozent senken.

3. Ungenutzte Geräte entsorgen

Häufig sind die IT-Geräte in Relation zu ihrer Kapazität nicht voll ausgelastet. Doch auch Geräte, die selten oder gar nicht genutzt werden, benötigen Strom und führen allein dadurch zu höheren Betriebskosten. Firmen können 300 bis 500 Euro an Energiekosten pro Jahr einspa-

ren, wenn sie einen einzigen ungenutzten oder zu wenig genutzten Server entfernen. Die Einsparungen an Hardware und Lizenzen sind darin noch nicht enthalten. Allein deshalb lohnt sich eine Bestandsaufnahme des eigenen Rechenzentrums inklusive aller Server, um die Geräte zu identifizieren, die begrenzte, einzelne oder seltene Aufgaben ausführen.

Administratoren können Computer über ein Netzwerk zu Clustern zusammenschließen, um verteiltes Rechnen zu ermöglichen. Dadurch können Datenspeicher und Verarbeitungsleistung eine Serverressource gemeinsam nutzen. Höhere Lasten lassen sich durch größere Cluster bewältigen, statt neue Hardware anzuschaffen. Die Scale-Out-Architektur erleichtert zudem die Skalierbarkeit. Zwar sind die anfänglichen Einrichtungskosten in der Regel höher als bei einem Einzelsystem, doch können verteilte Systeme dank ihrer Skalierbarkeit bei langfristiger Nutzung kostengünstiger sein.

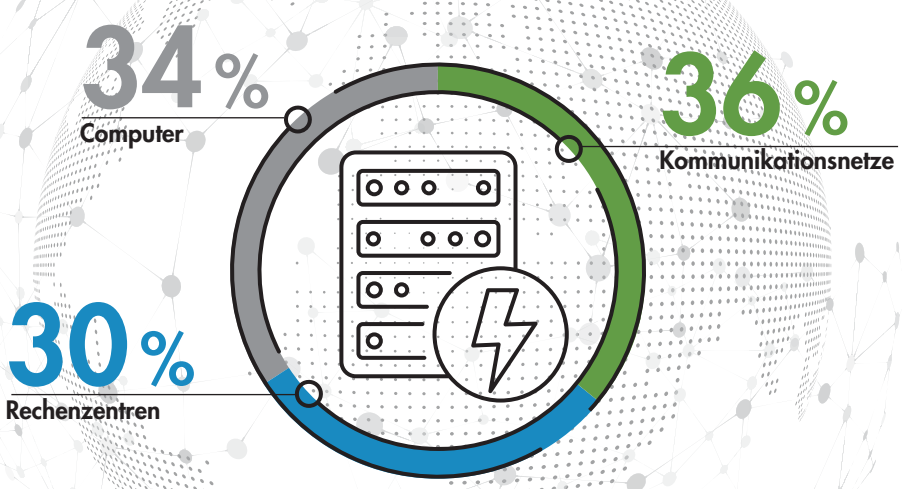
4. Effiziente Kühlprozesse

Etwa 40 Prozent der Energieressourcen eines Rechenzentrums entfallen auf Kühlsysteme. Auf der anderen Seite können Luft- und Flüssigkeitskühlsysteme den Stromverbrauch senken und gleichzeitig die temperaturempfindlichen Geräte schützen.

In den meisten Computerraumklimageräten (CRAC = Computer Room Air Conditioning) kommen Standardventilatoren zum Einsatz, deren Drehzahl sich nicht an die Wärmelast des Rechenzentrums anpassen lässt. Die nachhaltige Alternative sind Systeme mit variabler Drehzahl. Denn sie verbrauchen nur während des Betriebs Strom und bestimmen ihre Drehzahl über innovative Raumtemperaturanalysen. Eine geringe CPU-Auslastung der Server verringert also gleichzeitig den Stromverbrauch beim Einsatz von drehzahlvariablen Lüftern um bis zu 20 Prozent.

Effektiver als Lüfter arbeitet die Flüssigkeitskühlung. Hier wird die Kühlflüssigkeit durch ein geschlossenes System von Schläuchen von einer Komponente zur anderen geleitet, um die Systeme zu kühlen. Die dafür benötigten Pumpen, benötigen weniger Energie als Lüftersysteme in konventionellen CRAC/CRAH-Einheiten. Die Lösungen variieren von Wärmetauschern an der Hinterseite der Racks bis zu Direct-to-Chip-Kühlung. Flüssigkeitskühlung ist zwar deutlich teurer in der Anschaffung als gängige Luftkühlungssysteme, sie arbeitet aber auch wesentlich effizienter und ressourcenschonender. Zusätzlich dazu ermöglicht sie eine bessere Raumausnutzung im Rechenzentrum.

AUFTEILUNG DES GESAMTEN GLOBALEN STROMVERBRAUCHS (im Verhältnis zum gesamten IT-Verbrauch)



5. Hybrid Work langfristig etablieren

Zu den offensichtlichsten Folgen der Pandemie gehört die Verlagerung des Arbeitsplatzes vom Büro ins Homeoffice. Inzwischen verfügen die meisten Unternehmen über die erforderlichen Technologien, wie beispielsweise eine virtuelle Desktop-Infrastruktur (VDI). Dadurch können alle Mitarbeiter sowohl von zuhause als auch vom Büro auf Desktops, Anwendungen und Diensten zugreifen und profitieren von weniger Pendelei und mehr Zeit für die Familie.

Unternehmen sind damit in der Position, den Büroraumbedarf neu zu überdenken und können je nach Konzept ein kleineres Büro wählen, die Räume für andere Zwecke umgestalten oder Standorte komplett remote aufstellen. Eine Verkleinerung der Büroräume senkt nicht nur die Energiekosten für Beleuchtung, Heizung und Klimatisierung. Sie reduziert auch die CO_2-Emissionen der Angestellten, die weniger pendeln müssen.

Nachhaltigkeit in Unternehmensstrategie implementieren

In den nächsten Jahren wird es immer mehr Unternehmen geben, die energieeffizientes und emissionsarmes Arbeiten in ihre Unternehmensstrategie aufnehmen und ihren Betrieb umstrukturieren. Im Vordergrund steht dabei vor allem die IT, da sie einen hohen Energiebedarf hat. Virtualisierung und Cloud-Services helfen, die Serverauslastung zu steigern und gleichzeitig den Hardware-und Energiebedarf deutlich zu reduzieren. Dank Remote Work können Unternehmen zudem Büroflächen verkleinern und umgestalten und dadurch zusätzlich ihren CO_2-Fußabdruck verringern. Durch solche Maßnahmen kommen sie ihrem Pflichtbewusstsein gegenüber ihren Mitarbeitern und der Umwelt nach. Durch flexible Arbeitsangebote verbessern sie die Work-Life-Balance und entlasten mit ihrem nachhaltigen und ressourcenschonenden Engagement den Planeten.

Prashant Ketkar

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

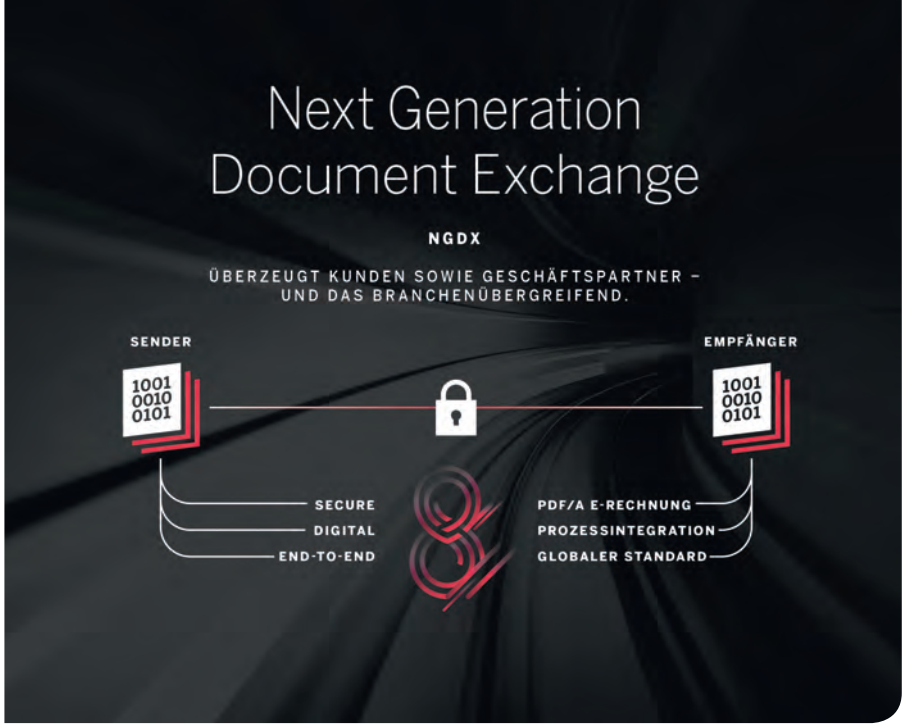
INNOVATIONEN IM ECM-UMFELD

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



Manipulationssicherer Dokumentenaustausch mit der OfficeMaster Suite von Ferrari electronic

VOM SONDERFALL ZUM STANDARD

HYBRIDES ARBEITEN – VERLUSTFREI UND SICHER

Das physische Büro ist längst nicht mehr der einzige Ort, an dem ein effektives Arbeiten möglich ist. Flexible Beschäftigungsmodelle wie Homeoffice und hybrides Arbeiten haben sich längst als berechtigte Alternative bewiesen und entwickeln sich mehr und mehr zum Standard. Intelligente Dokumentenaustauschlösungen unterstützen diese Entwicklung und stellen sicher, dass bestehende Prozesse auch remote fortgeführt werden.

Welches Beschäftigungsmodell ökonomisch am sinnvollsten und auch umsetzbar ist, zählt zu den Überlegungen, die das Management von Unternehmen seit Jahren wohl mit am meisten beschäftigen. Was über die Jahre immer mehr an Relevanz gewann, erfuhr mit der Pandemie schließlich ihren Höhepunkt. Knapp drei Jahre später hat sich das Modell des hybriden Arbeitens weitestgehend durchgesetzt.

„New Work" ist zweifellos mit einer hohen Erwartungshaltung verknüpft. Zukunftsfähig sind Unternehmen nur, wenn sie mit dieser Entwicklung gehen und das technisch erforderliche Fundament legen. Anders als häufig vermutet, braucht es hierfür nicht nur entsprechende Hardware. Um bestehende Prozesse und ein verlustfreies Dokumentenmanagement auch im Wechsel zwischen Büro und Homeoffice aufrecht zu erhalten, sind vollständig digitalisierte Dokumente und Lösungen für deren manipulationssicheren Austausch gefragt.

Prozesse remote aufrechterhalten

Eine Lösung, die Unternehmen bei der Umsetzung flexibler Beschäftigungsmodelle unterstützt, ist die OfficeMaster Suite des Berliner Unified-Communications-Herstellers Ferrari electronic. Sie entspricht dem international gültigen ITU-Standard und befähigt damit selbst Unternehmen mit europaweit verteilten Standorten zu einem verlustfreien, hybriden Arbeiten. Die Softwarelösung lässt sich nahtlos in bereits vorhandene E-Mail-Systeme integrieren, ermöglicht einen DSGVO-konformen, rechtssicheren Dokumentenaustausch und legt die Basis für zahlreiche digital integrierte Prozesse.

Herzstück der OfficeMaster Suite ist der Standard Next Generation Document Exchange (NGDX). Dokumente gehen damit im Original und End-to-end als PDF im E-Mail-Postfach des Empfängers ein. Auch den Transfer hybrider Dokumente unterstützt NGDX. Da Metadaten und Schlagworte ebenfalls übertragen werden, ist eine nahtlose Weiterverarbeitung in BPM- und Dokumentenmanagementsystemen möglich.

Automatisiertes Auslesen und Verarbeiten

Noch mehr Möglichkeiten, Prozesse auch im Homeoffice aufrechtzuerhalten, bietet das neue Major Release OfficeMaster Suite 8. Durch eine Anbindung an die E-Post-Schnittstelle der Deutschen Post, beispielsweise aus Microsoft Dynamics 365, lassen sich postalische Massenversände nun auch schnell und unkompliziert aus dem Homeoffice tätigen. Ebenfalls vollautomatisch läuft das Konvertieren von Rechnungen in die Formate ZUGFeRD und XRechnung ab, die anschließend versendet, beziehungsweise über eine Web-Schnittstelle direkt ins Portal der Bundesdruckerei hochgeladen werden können. Dokumente, die nicht per NGDX eingehen, werden mit einem Textlayer zur Texterkennung versehen, was deren automatisiertes Auslesen und Verarbeiten erlaubt. Auch gescannte oder abfotografierte Texte, wie sie häufig über Upload-Portale eingehen, lassen sich auf diese Weise extrahieren.

Ein sicherer und reibungsloser Wechsel zwischen Firmenbüro, Homeoffice und verschiedenen Unternehmensstandorten ist möglich. Die technischen Voraussetzungen lassen sich mit softwarebasierten Dokumentenaustauschlösungen wie der OfficeMaster Suite von Ferrari electronic schaffen.

www.ferrari-electronic.de

Ferrari electronic

COMPLIANCE-GERECHTES ARBEITEN

WIRELESS-EDGE-ROUTER SORGEN FÜR SICHERHEIT UND PERFORMANCE

Eine dedizierte, belastbare 4G LTE- oder, wo verfügbar, 5G-Verbindung verhindert Ressourcen- und Bandbreitenkonkurrenz mit anderen Geräten im Heimnetzwerk und beugt damit Leistungsproblemen vor. Wireless-Router stellen dabei ein eigenes, isoliertes WLAN-Netzwerk bereit und isolieren Arbeitsgeräte wie Laptops und Drucker, um Sicherheits- und Compliance-Richtlinien zu erfüllen. Unternehmen halten die eigenen, firmenweiten Sicherheitsstandards ein – indem sie diese auf alle vernetzten Unternehmensressourcen ausweiten und Home-Office- oder mobile Mitarbeiter aus der Zentrale mit den gleichen IT-Funktionen und der gleichen Endbenutzererfahrung wie im Büronetzwerk ausstatten.

„Work From Anywhere" ist für viele Mitarbeiter außerhalb von Produktionsstätten längst Realität. Diese Entwicklung wurde durch die Pandemie nur noch weiter verstärkt, und ein Ende ist nicht in Sicht. Die mobilen Mitarbeiter und Home-Office-Arbeitskräfte sind damit ein wesentlicher Teil des modernen Edge-Computings. Die zentrale Verwaltung bereitet jedoch IT-Entscheidern wie Administratoren nicht selten Kopfzerbrechen. Dabei sind Sichtbarkeit und Kontrolle der Netzwerkkonnektivität ebenso wie die Informationssicherheit für das Unternehmen essenziell.

Herausforderungen für das Netzwerk

Mitarbeiter, die beruflich von zu Hause arbeiten, teilen sich vorhandene Bandbreiten (über Kabel oder Mobilfunk) häufig mit Haushalts- oder Familienmitgliedern, ob in professioneller oder privater Nutzung. Das kann zur Folge haben, dass Netzwerkunterbrechungen auftreten oder eine schlechte Übertragung die Produktivität beeinträchtigt.

„WORK FROM ANYWHERE" IST FÜR VIELE MITARBEITER AUSSERHALB VON PRODUKTIONSSTÄTTEN LÄNGST REALITÄT.

Jan Willeke, Area Director Central Europe, Cradlepoint, https://cradlepoint.com/de-de

Die Netzwerkverwaltung ist bei diesen privaten Edge-Verbindungen für IT-Teams erheblich erschwert, das Einrichten von Maßnahmen für die Informationssicherheit und den Schutz der Unternehmensdaten nahezu unmöglich. Herkömmliche Optionen für den administrativen Fernzugriff bestehen in VPN- und SD-WAN-Lösungen (Virtual Private Networks oder Software-Defined Wide Area Networks). VPN-Anwendungen haben den Nachteil, dass sie die Herausforderungen an Bandbreite und Betriebszeit nicht lösen können und schwierig zu verwalten sein können. SD-WAN-Systeme schaffen Abhilfe, indem sie VPN-Verbindungen selbstverständlich neben anderen Verbindungen mitverwalten. Mögliche Sicherheits- oder Verbindungsprobleme am Netzwerkrand können sie aber nicht lösen, weil der Zugriff auf private WAN-Verbindungen nicht möglich ist.

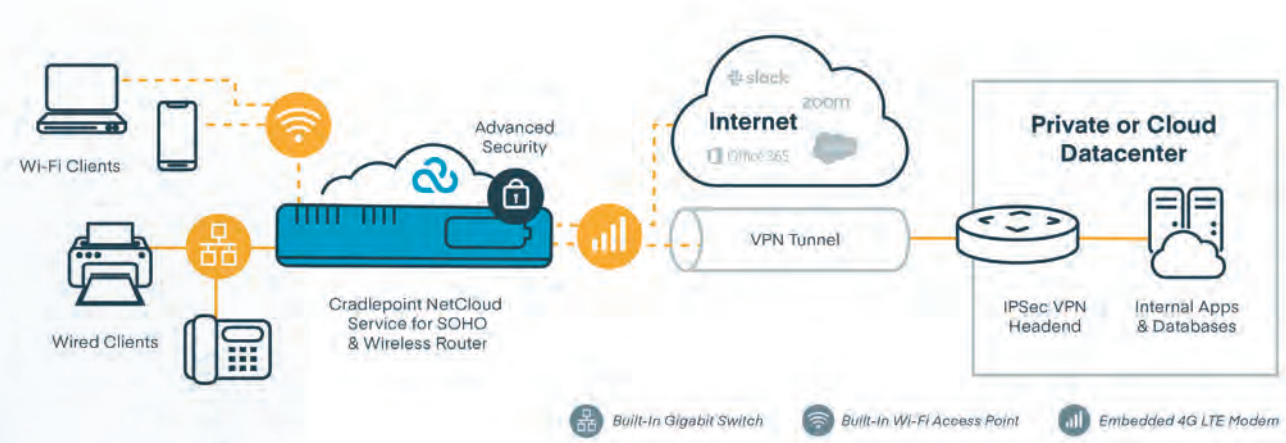
Sicherheit und Verfügbarkeit auch am Netzwerkrand

Das so genannte CIA-Modell klassifiziert die Herausforderungen in Netzwerken als Dreieck und unterscheidet:

- **Vertraulichkeit (Confidentiality)** Verhindern, dass sensible Informationen in die falschen Hände geraten.
- **Integrität (Integrity)** Wahrung der Konsistenz, Genauigkeit und Vertrauenswürdigkeit von Daten über den gesamten Lebenszyklus.
- **Verfügbarkeit (Availability)** Gewährleistung einer konstanten Netzwerkverfügbarkeit für Personen, Orte und Dinge.

Insbesondere die Punkte „Vertraulichkeit" und „Verfügbarkeit" sind am Netzwerkrand gefährdet, etwa weil das Heimnetzwerk nicht gut genug gegen Eindringlinge geschützt ist oder weil Datenströme nicht priorisiert werden können.

Dedizierte Wireless-Edge-Router schaffen hier Abhilfe. Sie isolieren im Home-Office Arbeitsgeräte wie Computer, Notebooks und Drucker vollständig vom häuslichen Streaming. Over-the-Air-Verbindungen über 4G LTE und 5G verursachen dabei weniger Ausfälle als kabelgebundene Breitbandleitungen, die beispielsweise



Nach innen bildet ein Wireless-Router ein isoliertes Netzwerk für unterschiedliche Geräte. Die Verbindung ins Rechenzentrum wird über geschützte Verbindungen geleitet, die Administratoren in einer zugrundeliegenden SD-WAN-Lösung definieren.

durch Bauarbeiten beschädigt werden können oder schlichtweg nicht genügend Bandbreite für alle angeschlossenen Nutzer bereitstellen. So wird hohe Leistung für wichtige Anwendungen gewährleistet und eine physische Ebene des Daten- und Informationsschutzes geschaffen.

Netzwerkadministratoren verwalten die Wireless-Edge-Router als Ressource ihrer Netzwerkinfrastruktur und nutzen in der Regel Cloud-basierte SD-WAN-Plattformen. In der Verbindungsverwaltung orchestrieren sie Routing und Sicherheitsdienste. Dabei kommen die gleichen Sicherheits- und Zugriffskontrollen der Unternehmensklasse zum Einsatz, die IT-Teams auch im Büro bereitstellen. Außerdem behalten Administratoren so Kostenpläne im Blick und können bei Verbindungsproblemen aus der Ferne helfen, wenn es sein muss, sogar via Out-of-Band-Management.

Zur Sicherheit tragen dabei auch die einfache Bereitstellung und die hohe Skalierbarkeit der Wireless-Edge-Lösungen bei. Mitarbeiter müssen vorkonfigurierte Wireless-Edge-Router lediglich im Home-Office verbinden. Binnen weniger Minuten arbeiten sie dann automatisch mit Konnektivität auf Unternehmensniveau, ohne dass Änderungen im Rechenzentrum erforderlich sind.

Kostenvorteile und ROI

Ausfälle oder Verzögerungen im Netzwerk bedeuten Einbußen bei Umsatz und Produktivität oder machen es unmöglich, Anfragen zu bedienen. Einer der wichtigsten Gründe für die Nutzung von 4G LTE- und 5G-Routern am Netzwerkrand ist deshalb der Kostenfaktor. Die genannten Aspekte erhöhen nicht nur die Produktivität von Mitarbeitern und IT-Fachkräften, auch der Einsatz von Mitarbeitern vor Ort, etwa zur Installation und Wartung, entfällt. Der Einsatz von Wireless-Edge-Routern ist somit keineswegs lediglich eine Überbrückungsinvestition in der COVID-Zeit, der ROI ist vielmehr langfristig und nachhaltig.

Kabelgebundene Router und andere Lösungen für die Remote-Arbeit können heutige Bedürfnisse nicht mehr erfüllen – vor allem, wenn mehrere Personen im eigenen Haushalt parallel arbeiten. Heimnetzwerke sind eben nicht für die Arbeit in Unternehmen konzipiert, und es ist für IT-Teams nahezu unmöglich, Konnektivität, Informationssicherheit und Anwendungsleistung zu kontrollieren.

Eine eigenständige, zentral verwaltete Wireless-WAN-Lösung für zu Hause, bringt dagegen die Stabilität und Verfügbarkeit, die für Remote-Arbeit erforderlich sind.

Jan Willeke

https://cradlepoint.com/de-de

ÜBERSICHT VORTEILE VON WIRELESS-EDGE-ROUTERN

Für Unternehmen:

- Zentralisierte Steuerung
- Richtlinien für Gruppen (Sicherheit, Datennutzung)
- Sicherheitskontrollen (Firewall, IPS/IDS und Inhaltsfilterung)
- Dashboards zur Überwachung von Zustand, Sicherheit und Leistung
- Out-of-Band-Management zur Fehlerbehebung
- Bereitstellung neuer Anwendungen – eigener und jener von Drittanbietern
- Höhere Betriebszeit und schnellere Fehlerbehebung als in Heimnetzwerken; damit geringere Kosten
- 4G LTE- und 5G- Verbindungen verursachen weniger Ausfälle als kabelgebundene Breitbandleitungen

Für Mitarbeitende:

- Zero-Touch-Setup
- Senden großer Dateien möglich, ohne dass das Netzwerk zusammenbricht
- Zuverlässige sichere Konnektivität, stabile Telefonkonferenzen
- Portabilität

UNIFIED ENDPOINT MANAGEMENT

DAS RECHTE MASS BEI DEN LIZENZEN FINDEN

„Lieber zu viel als zu wenig", dieser Devise folgen IT-Abteilungen allzu oft, wenn es um Lizenzen geht. Bloß keine Strafzahlungen riskieren! Eine Überlizenzierung kostet das Unternehmen aber auf der anderen Seite letzten Endes womöglich genauso viel. Hier verschafft Lizenzmanagement-Software den Überblick. Sie sorgt dafür, dass ein Unternehmen nur die Softwarelizenzen bezahlt, die es auch benötigt, nicht mehr und nicht weniger. Das Lizenzmanagement sollte idealerweise in den übergeordneten Rahmen einer Unified-Endpoint-Management-Lösung eingebettet sein.

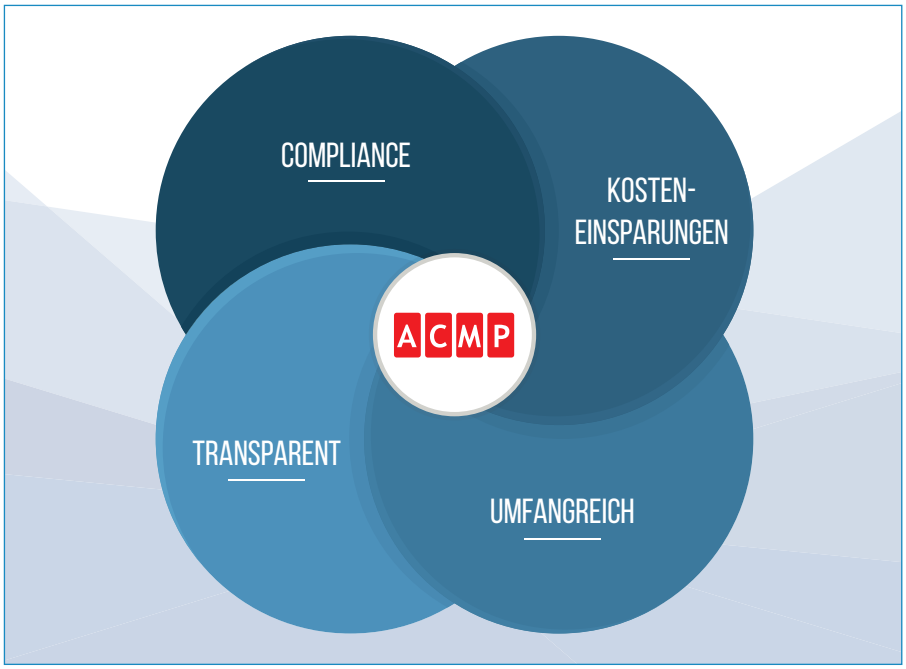
Nicht weniger gefürchtet als eine Steuerprüfung dürften Anrufe von Microsoft, IBM und Co. sein. Die großen Softwarehersteller wollen von ihren Kunden zwischendurch immer mal wieder wissen, wie viele Lizenzen ihrer Software bei ihnen eigentlich im Einsatz sind. Solche Audits sind sogar die Regel und werden angekündigt. Die Hersteller machen damit bis zu 30 Prozent ihrer Gewinne. Dabei wird die Softwarenutzung gezählt und gegen den Lizenzbestand geprüft. In der Regel ergibt sich ein Delta, und Nachzahlungen samt Strafgebühren werden fällig. Auch Fragen von Compliance und Rechtssicherheit werden im Rahmen von Audits berührt.

Sofort schrillen bei einer Audit-Ankündigung die Alarmglocken: Sollte eine Unterlizenzierung vorliegen? Das heißt das Programm ist an mehr Arbeitsplätzen im Einsatz, als Lizenzen erworben wurden? Dies ist gerade in großen Unternehmen mit zahlreichen Abteilungen oft unbeabsichtigt der Fall – es fehlt schlichtweg der Überblick. Die Standardverträge der Hersteller sind schwer auf den eigenen Betrieb anzuwenden, und man muss die eigene Software, Vertragsbestimmungen und Lizenzmetriken schon sehr genau kennen.

Auf der anderen Seite ist auch eine Überlizenzierung ärgerlich. Denn dabei zahlt die Firma für Software, die sie gar nicht benötigt. So wird IT-Budget verschwendet, das sich strukturierter einsetzen ließe. Während bei zu wenig Lizenzen also Strafen drohen, lässt das Unternehmen im umgekehrten Falle Einsparpotenziale ungenutzt.

Wer Ruhe vor Audits haben will...

Diesem Dilemma entzieht sich, wer ein funktionierendes Lizenzmanagement einsetzt. Softwarehersteller Aagon beispielsweise liefert dieses als Modul seiner UEM-Suite ACMP mit aus. Systeme



Symbiose von UEM und Lizenzmanagement (Quelle: Aagon)

für Unified Endpoint Management, kurz UEM (oder auch Client Management) übernehmen die zentrale Verwaltung und Steuerung von Arbeitsplatzrechnern und Servern in einem Unternehmensnetzwerk. Administrationsabteilungen regeln damit die erforderlichen administrativen Aufgaben auf den Clients zentral und im Idealfall komplett automatisiert. Die Automatisierung reduziert den Zeitaufwand und erhöht sowohl Zuverlässigkeit, Sicherheit als auch Produktivität von Usern und Administrationsabteilung gleichermaßen.

Klassische Bereiche des UEM sind Inventarisierung, Softwareverteilung, Patch Management und eben das Lizenzmanagement. Hinsichtlich begrenzter IT-Budgets und der Gefahr einer Über- oder Unterlizenzierung ist beim Thema Lizenzmanagement strukturiertes und smartes Vorgehen gefragt. Dies gilt für die meisten Unternehmen, denn einen wirklich stets aktuellen Überblick über Nutzung und Vorhandensein von Lizenzen haben in der Realität nur wenige. Wird ein solches Tool im Vorfeld eines angekündigten Audits implementiert, erstellt es eine unternehmensweite Übersicht der installierten Softwarelizenzen. „Diese haben wir Microsoft übermittelt, seitdem haben wir Ruhe", wie der IT-Administrator eines Aagon-Kunden zufrieden berichtet.

Natürlich lässt sich das Management von Lizenzen auch manuell erledigen. Ab einer Unternehmensgröße von 100 Clients ist dies dann zwar noch theoretisch möglich, in der Praxis jedoch kaum mehr zu bewerkstelligen; der Aufwand, den Lizenzbestand permanent zu erfassen und aktuell zu halten, ist einfach viel zu groß. Wer diese Aufgaben an ein automatisiertes Lizenzmanagement auslagert, spart viel Zeit, die sich für andere wichtige Projekte nutzen lässt.

Umzugshilfe

Das ACMP Lizenzmanagement von Aagon ermöglicht eine Inventarisierung und Verwaltung aller im Unternehmen eingesetzten Lizenzen. Es erfasst unterschiedliche Hersteller, Lizenztypen, Über- oder Unterlizenzierung sowie Abhängigkeiten zwischen den Lizenzen. Die Signatur der installierten Software wird erkannt und mit einer internen Datenbank abgeglichen, die 17.000 Hersteller, knapp 700.000 Software-Einträge und über 8.000 Software-Produkte mit mehr als 43.000 Versionsständen umfasst. Das erfasste Programm ordnet die Software den bestehenden Lizenzen zu. Lizenzpflichtige Software wird ausfindig gemacht, ebenso wie unerwünschte, die dann gelöscht werden kann.

Produkte (Name der Software sowie ihre Edition) inventarisiert das Modul über zwei Arten von Erkennungsmustern. Das Add-on ACMP DNA ermöglicht über das DNA-Erkennungsmuster eine automatische Identifizierung von Software und reichert es dabei direkt mit lizenztechnischen Daten an. Dies geschieht auf der Grundlage eines Softwarekatalogs. Ergänzend dazu lassen sich auch ohne ACMP DNA selbst Erkennungsmuster erzeugen und Produkte generieren. Nachdem die passenden Lizenzen sowie die Lizenzverbraucher zu dem Produkt eingepflegt wurden, wird in der Compliance eine Lizenzbilanz errechnet. Diese zeigt dann an, ob man überlizenziert, unter- oder passend lizenziert ist.

Über Reporting-Funktionen und ein übersichtliches Dashboard erhält die IT-Leitung vollständige Transparenz über das Vorhandensein und den Einsatz von Lizenzen. Sie hat auslaufende Lizenzen stets im Blick, kann bestehende „umziehen" lassen und über die UEM-Lösung einem anderen Client zuweisen. Verträge können Lizenzen zugeordnet werden, diese wiederum bestimmten Stammdaten wie Abteilung, Kostenstelle und so weiter. Ein automatisiertes Reporting versorgt alle Stakeholder via E-Mail mit relevanten Lizenzinformationen, so ist es beispielsweise möglich, automatisiert Benachrichtigungen über auslaufende Verträge oder Unterlizensierung zu erhalten.

Steigende Bedeutung in Zeiten hybriden Arbeitens

Insbesondere mit der Ausweitung von Homeoffice-Arbeit hat Lizenzmanagement an Bedeutung gewonnen. Es hilft IT-Abteilungen dabei, die neu geschaffenen Work-Arounds lizenztechnisch zu stabilisieren. Denn Sicherheit beim Client- und Lizenzmanagement ist immens wichtig, wenn sich ein Teil der Arbeitsplätze außerhalb des abgesicherten internen IT-Netzwerkes befindet.

Fazit

Ein präzises Management der genutzten und ungenutzten Lizenzen spart Kosten und sichert das Unternehmen rechtlich ab. Notwendige Lizenzen werden damit auch für Homeoffice-Lösungen innerhalb eines Tages bereitgestellt.

www.aagon.com

Eine kostenlose ACMP Testversion erhalten Sie über die Website **www.aagon.com**

IT-TRENDS

NEUE HERAUSFORDERUNGEN FÜR DAS IT-MONITORING

Die IT-Welt ist im Wandel: Dauerthemen wie die ständig zunehmende Komplexität der IT oder die immer bedrohlicher werdende Cyberkriminalität, aber auch aktuelle Probleme wie steigende Energiekosten oder Lieferengpässe bei Hardware fordern IT-Verantwortliche jeden Tag aufs Neue heraus. Somit wird es immer wichtiger, dass Monitoring-Tools nicht nur dazu beitragen, einen Überblick über die gesamte IT-Infrastruktur von Unternehmen und Organisationen zu haben – sondern auch zur Ressourcenoptimierung genutzt werden.

Die IT-Welt entwickelt sich ständig weiter. Dabei rückt besonders das Datacenter in den Fokus – schließlich ist es die Basis aller Prozesse in so gut wie jedem Unternehmen. Doch auch in der Unternehmensstruktur finden Veränderungen statt – Remote Work sorgt dafür, dass Unternehmen flexibler werden müssen. Wie können Monitoring-Tools bei diesem Wandel helfen, und wie wirken sich die Veränderungen auf das Monitoring aus?

Dauerbrenner Cloud

Die Cloud hat sich in vielen Unternehmen schon lange als Lösung etabliert. Mittlerweile gibt es kaum noch ein Unternehmen ohne hybride Infrastruktur. Bereits vor der Pandemie hatte die Cloud an Bedeutung in der IT-Welt gewonnen, doch mit der pandemiebedingten Verlagerung ins Homeoffice – die aller Voraussicht nach zum neuen Standard werden dürfte – ist sie noch mehr in den Fokus gerückt. IT-Services und komplette Geschäftsprozesse werden immer häufiger in die Cloud verlagert. Auch Monitoring-Lösungen müssen sich dieser Entwicklung anpassen: Cloud-Applikationen und -Anbieter müssen in das zentrale Monitoring integriert werden, ohne die lokale IT zu vernachlässigen. Nur so haben die IT-Verantwortlichen einen Überblick über Verfügbarkeit und Performance der gesamten IT.

Immer mehr Monitoring-Lösungen werden heute als Service angeboten. Entscheidet man sich als Unternehmen für eine Cloud-basierte oder gehostete Monitoring-Lösung, erspart man sich regelmäßige Wartungen und Updates durch die eigenen Mitarbeiter. Der Anbieter hält das Tool stets auf dem neusten Stand – damit wird der alltägliche Betrieb entlastet, Geld gespart und Ressourcen werden geschont. Allerdings muss sichergestellt sein, dass die Cloud-Lösung auch die IT vor Ort umfassend und zuverlässig integriert und das grundlegende IT-Monitoring nicht vernachlässigt.

Safety first

Sicherheit ist und bleibt nicht nur ein relevantes Thema für die IT-Welt, tatsächlich werden die Bedrohungen immer ernstzunehmender. Nicht nur Kriminelle bedrohen Unternehmen, immer häufiger stehen Staaten unter Verdacht, mit enormen Ressourcen kritische Unternehmen und Behörden in anderen Ländern anzugreifen. Immer neue Konzepte und Lösungen versprechen Sicherheit, aber zunehmende Komplexität, hohe Kosten und natürlich der Faktor Mensch werden jedoch auch

zukünftig dafür sorgen, dass Systeme nie 100 Prozent sicher sein können.

Monitoring bildet einen wichtigen Baustein bei einem umfassenden Sicherheitskonzept. Auch wenn Monitoring per Definition keine Security-Lösung darstellt, leisten geeignete Monitoring-Tools einen wertvollen Beitrag zur Überwachung der Funktion und Aktualität von dedizierten Security-Komponenten wie Virenscannern oder Firewalls. Darüber hinaus können manche Monitoring-Lösungen ungewöhnliche Aktivitäten aufdecken und so eine zusätzliche Ebene in einem umfassenden Sicherheitskonzept bilden. Und natürlich überwachen Monitoring-Tools den Zustand von Geräten und schlagen Alarm, bevor es zu Ausfällen kommt. Damit können Produktionsstopps verhindert und unter Umständen sogar feindliche Angriffe erkannt werden.

Monitoring und Digitalisierung

Häufig wird die Digitalisierung nicht als Teil der IT-Welt gesehen. Doch die Anforderungen an die IT-Verantwortlichen sind in den letzten Jahren stetig gestiegen: Waren Produktionsanlagen, medizinische Infrastrukturen oder Gebäudetechnik früher von der IT getrennt, sind sie durch die Digitalisierung heute zumindest teilweise in der Verantwortung der IT-Teams. Methoden wie OPC UA oder Protokolle wie MQTT oder Modbus können Produktionsanlagen und OT-Systeme, aber auch Gebäudetechnik (etwa im Rechenzentrum) monitoren, DICOM und HL7 ermöglichen die Überwachung von medizinischen Systemen und Geräten. Monitoring-Lösungen, die diese Protokolle und Methoden unterstützen, reduzieren die Komplexität und sparen Kosten (eine Lösung für alles) und liefern neben dedizierten Dachboards für einzelne Abteilungen auch einen umfassenden Überblick für das Management.

Ressourcen schonen

Klimawandel und Globalisierung verursachen zunehmend neue Krisen und fordern ein generelles Umdenken. IT benötigt Ressourcen nicht nur in Form von Strom bei Betrieb, sondern jedes Gerät, dass neu angeschafft wird, bedeutet einen massiven Einsatz von wertvollen Ressourcen für Produktion und Transport. Dazu kommen immer wieder Lieferengpässe aufgrund von Pannen oder der Corona-Pandemie.

Monitoring unterstützt die Verantwortlichen im Rechenzentrum, indem es Verbrauchswerte und Umweltparameter im Blick behält und so das Optimieren des Energieverbrauchs ermöglicht. Darüber hinaus hilft Monitoring aber auch, die Lebensdauer von IT-Komponenten zu verlängern, die sich bei ungeeigneten Umweltbedingungen (zu hohe Temperaturen oder Feuchtigkeit) signifikant verkürzt. Geräte müssen häufiger ersetzt werden, es werden unnötige Ressourcen vergeudet. Monitoring spart so nicht nur Geld, es unterstützt auch beim Kampf gegen Klimawandel und globale Krisen.

Um eine ganz andere Art von Ressource geht es bei dem häufig beklagten Fachkräftemangel in der IT. Auch hier können geeignete Monitoring-Lösungen einen Beitrag zur Linderung des Problems leisten. Richtig eingesetzt schafft Monitoring Transparenz und Überblick und verringert die Komplexität großer IT-Umgebungen für die Verantwortlichen. Speziell wenn es im Zuge der Digitalisierung um das Zusammenwachsen der IT mit anderen Bereichen geht, kann eine umfassende Monitoring-Lösung hilfreich sein. Vor allem, wenn ein einziges Tool ausreicht, um all diese unterschiedlichen Anforderungen zu meistern und so die Komplexität des Monitorings selbst zu senken: Eine einzige Lösung für IT, OT, medizinische Infrastrukturen und Umgebungsparameter vereinfacht das Monitoring und senkt die Kosten.

Monitoring-Trends im Blick behalten

Die IT-Welt verändert sich ständig – das Zusammenwachsen von IT und OT, immer neue Technologien, wachsende Datacenter-Komplexität und steigende Energiepreise schaffen fortlaufend neue Herausforderungen für IT-Verantwortliche. Monitoring geht mittlerweile über das reine Überwachen von Geräten und IT-Systemen hinaus. Vor allem die Digitalisierung spielt eine immer wichtigere Rolle beim Einsatz von Monitoring-Tools. Auch zur Ressourcenschonung können Monitoring-Lösungen beitragen. Entscheidend ist, dass die eingesetzte Monitoring-Lösung allen Anforderungen genügt:

DAS ZUSAMMENWACHSEN VON IT UND OT, IMMER NEUE TECHNOLOGIEN, WACHSENDE DATACENTER-KOMPLEXITÄT UND STEIGENDE ENERGIEPREISE SCHAFFEN FORTLAUFEND NEUE HERAUSFORDERUNGEN FÜR IT-VERANTWORTLICHE.

Thomas Timmermann,
Senior Market Expert, Paessler AG,
www.paessler.com

1. Monitoring von Cloud-Umgebungen und Vor-Ort-Strukturen;
2. Einbindung digitalisierter Umgebungen (Produktion, Krankenhaus, Rechenzentrum …) dank Unterstützung entsprechender Methoden;
3. Einbindung von Umgebungsparametern und Verbrauchswerten (Strom, Wasser …);
4. einfache Bedienbarkeit und realistisches Preis-Leistungs-Verhältnis.

Thomas Timmermann

JAHRESKONGRESS 2022

MIT VERÄNDERUNGEN SCHRITT HALTEN

„Auf der Suche nach Erfolg" lautete das Motto des 23. Jahreskongresses der Deutschsprachigen SAP-Anwendergruppe e. V. (DSAG) vom 11. bis 13. Oktober 2022 in Leipzig. Mehr als 3.600 Teilnehmer waren vor Ort. Den Rahmen der Veranstaltung bildeten acht Keynotes, 52 Themensitzungen mit 156 Vorträgen, 48 Partnervorträge und 33 Espresso-Sessions.

Durch die Digitalisierung, Transformation und politische Zeitenwende ist der Erfolg der Unternehmen davon abhängig, wie sie mit den Veränderungen Schritt halten. Laut einer aktuellen Umfrage der DSAG, Americas SAP Users' Group (ASUG) und der Japan SAP Users' Group (JSUG) gelingt dies nach eigenen Angaben dem Großteil der befragten Unternehmen. Was die Bedeutung der IT-Lösungen jetzt und in Zukunft betrifft, liegt der On-Premises-Ansatz immer noch an der Spitze, wenn auch die SAP-Lösungen deutlich zulegen werden. Das bestätigt die Tendenz: Die Zukunft ist hybrid!

Von SAP wünscht sich die DSAG unter anderem transparente, flexible und skalierbare Cloud-Verträge mit den entsprechenden Metriken sowie verbindliche Statements und Roadmaps zur Produktstrategie in der Cloud und On-Premises. Zudem bedarf es im Hinblick auf die hybriden Landschaften klarer Modelle für die Integration und den Betrieb. „Durch neue SAP-Lösungen und Hybrid-Ansätze darf kein Prozess-Vakuum entstehen. Hier ist es wichtig, dass SAP dazu beiträgt, dieses Vakuum zu verhindern", so Jens Hungershausen, Vorstandsvorsitzender der DSAG.
Weitere Informationen unter

www.dsag.de/jahreskongress

SHIELDS UP

DAS NEUE NORMAL IM ZEITALTER DER DATEN

LIVE WEBINAR AM 08.12.2022 UM 10:00 UHR

Andreas Fuchs,
Head of Strategy & Vision,
DriveLock SE

Wenn Unternehmen auf die Cloud umsteigen und die Belegschaft von verschiedenen Standorten aus arbeitet, von überall und zu jeder Zeit auf Unternehmensdaten zugreift, sind Daten schneller in Gefahr. Auch bei Cyberangriffen stehen sie als wertvolles Gut im Mittelpunkt. Digitale Unternehmen benötigen daher eine moderne Data-Loss-Prevention-Lösung (DLP), die sensible Daten identifiziert und überwacht, den autorisierten Zugriff regelt, Datenverluste durch geeignete Präventionsmaßnahmen verhindert und Datenlecks nicht erst erkennt, wenn es bereits zu spät ist.

Die zunehmende Nutzung der Cloud und anderer Dienste bedeutet, dass Kontrolle und Schutz komplexer und schwieriger werden. Für Unternehmen ist es daher von entscheidender Bedeutung, sensible Daten nicht nur auf ihren eigenen Netzwerken und Geräten, sondern auch plattformübergreifend, von überall her und in der Cloud zu schützen.

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

PROGRAMMIEREN LEICHT GEMACHT

WO LOW-CODE HILFT, DIE AUTOMATISIERUNG VORANZUTREIBEN

CITIZEN DEVELOPER KÖNNEN ENGPÄSSEN IN DER IT ENTGEGENWIRKEN UND MITHILFE VON NO-CODE- UND LOW-CODE-AUTOMATION DIGITALE WORKFLOWS IN KÜRZESTER ZEIT ERSTELLEN.

Dina Haack, Head of Marketing, xSuite Group GmbH, www.xsuite.de

„Citizen Developer", ein wenig scheint mit diesem neuen Begriff der Exklusivitätsanspruch hochspezialisierter Fachleute in der Softwareentwicklung verloren zu gehen. Doch dies wirkt zunächst nur so. Denn auch wenn an manchen Arbeitsplätzen in einem Unternehmen – sei es Buchhaltung, Marketing oder Rechtsabteilung – auf einmal die sogenannten Citizen Developer sitzen, müssen diese eben nicht fit sein in Java, C++ & Co. Das ist der Unterschied. „Programmieren" wird hier vielmehr zu einer sehr einfachen Aufgabe, durch die sich mittels weniger Klicks Automatismen in täglichen Geschäftsroutinen erstellen lassen. Das sorgt für höhere Produktivität und Arbeitszufriedenheit. Und weil es keine Programmierkunst ist, heißt es auch so: Low-Code oder wahlweise No-Code.

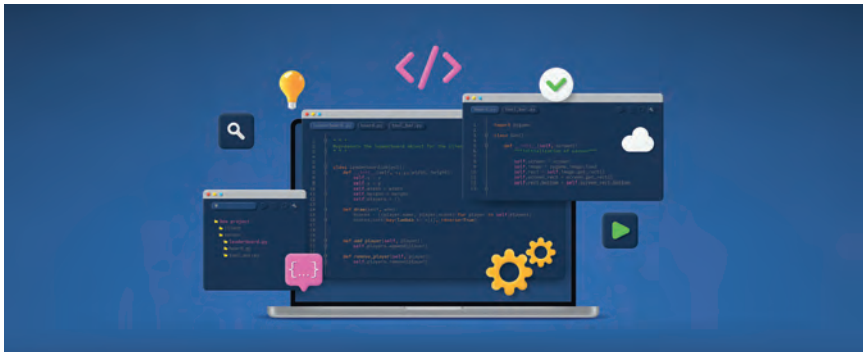
Von RPA zu Low-Code / No-Code

Alles, was sich irgendwie automatisieren lässt, wurde in den vergangenen Jahren unter dem Begriff Robotic Process Automation, kurz RPA, subsummiert. Blickt man einmal in die Praxis, stellt sich heraus: Viel mehr als Excel-Makros zusammenzubauen steckt oft nicht dahinter. RPA bedeutet: Man nimmt sich einen Prozess, für dessen Durchführung am Rechner die immer gleichen Arbeitsschritte notwendig sind, fasst sie zusammen und kann ihren Ablauf dann durch einmaliges Klicken dauerhaft automatisiert auslösen.

Was aber eigentlich interessant ist, ist das grundlegende Bedürfnis der Fachabteilungen, ihre Prozesse in Eigenregie zu optimieren, ohne dass sie wegen jeder Kleinigkeit gleich die IT fragen müssen. Hier schlagen RPA und „Low Code/No Code" in dieselbe Kerbe. Mit solchen Ansätzen können die neuen „Citizen Developer" (also wir alle) Anwendungen programmieren ohne Programmiersprache. Automatisiert ablaufende Prozesse werden aus Modul-, Formular- und/oder Workflowkatalogen per drag & drop grafisch zusammengeklickt, welche die Software zur Verfügung stellt.

Praxisbeispiel Mailroom: Einfache Workflows selbst konfigurieren

Für SAP stellt „Low Code/No Code" neben Prozessautomatisierung, Daten und künstlicher Intelligenz einen der momentan wichtigsten Innovationstreiber dar. Der SAP-Partner xSuite Group zum Beispiel operiert in seinen Softwarelösungen bereits mit Low-Code-/No-Code-Möglichkeiten, damit User in Eigenregie automatische Prozesse anstoßen können. In der xSuite-Cloudlösung Mailroom kann der Anwendende selbständig Belege trainieren und Workflows einstellen, welche die Belege gezielt an verschiedener Stelle ablegen.



Engpässen in der IT entgegenwirken

Automatisierung ist ein wesentlicher Faktor, ob ein Unternehmen auch künftig erfolgreich bleibt. Wer sich hier aufgeschlossen für neue Lösungen zeigt, ermöglicht es seinen Beschäftigten, auch bei dünner Personaldecke handlungsfähig zu bleiben oder sich verstärkt auf anspruchsvollere Tätigkeiten zu konzentrieren. Auch die begehrten Fachkräfte von heute – insbesondere wenn sie gut ausgebildet sind – sollten bedacht werden. Denn sie können sich ihre Jobs aussuchen. Und sie werden lieber dorthin gehen, wo Arbeitsprozesse interessant, automatisiert gesteuert und modern sind. So greift gerade hier das Prinzip des Citizen Developer, der Engpässen in der IT entgegenwirken und mithilfe von No-Code- und Low-Code-Automation digitale Workflows in kürzester Zeit erstellen kann. Eine wichtige Tätigkeit und eine interessante dazu.

Dina Haack

CYBERCRIME-TRENDS 2023

WELCHE THEMEN BEWEGEN UNTERNEHMEN UND IT-SECURITY-ANBIETER

Unser privates und berufliches Leben wird immer digitaler - mit signifikanten Auswirkungen. Digitalisierung bietet eine Fülle von Vorteilen – beschleunigte und effizientere Produktionsabläufe, den Einzug digitaler Diagnostik-Technologien in Krankenhäuser, die Erleichterung von Verwaltungsprozessen durch die Nutzung von Bürgerportalen, mobiles Arbeiten und Lernen, die Hochverfügbarkeit von Daten. Aber diese immense Datenflut ruft auch Kriminelle auf den Plan, die aus dem Diebstahl, der Manipulation der Daten, dem neuen Gold, ihren Profit generieren. Einige der nachfolgenden Themen werden uns im kommenden Jahr in der Abwehr von Cybercrime verstärkt beschäftigen.

1. Blockchain – Virtuelle Werte benötigen neue Sicherheitskonzepte

Cyberkriminelle haben es auf digitale Identitäten und kommerzielle Transaktionen abgesehen. Die Blockchain-Technologie, ein dezentrales Netzwerk, in dem Daten nicht an einem bestimmten Ort gespeichert, sondern über einen Cloud-Dienst verschlüsselt werden, ist die derzeitige Sicherheitslösung für Datensilos im Metaverse. Die jüngsten Blockchain-Angriffe und -Verletzungen zeigen jedoch, dass dieser Weg nicht die gewünschte Datensicherheit im virtuellen Raum bietet. Blockchain-Sicherheit ist besonders kompliziert, da auch traditionelle Anwendungen genutzt werden. Beispielsweise ein Web-Frontend für einen NFT-Marktplatz oder ein als Browser-Erweiterung implementiertes Wallet. Hacks können sogar irreversibel sein. Blockchain-Anwendungen und intelligente Verträge sind in der Regel auf eine bestimmte Funktionalität ausgerichtet, sodass eine Verletzung dieser Funktionalität eine vollständige Zerstörung bedeutet. Die Experten von sycope thematisierten Blockchain-Security auf der vergangenen it-sa. Das Unternehmen konzentriert sich auf die Konzeption und Entwicklung hochspezialisierter IT-Lösungen zur Überwachung und Verbesserung der Netzwerkleistung.

2. Cyber-Kriegsführung wird immer subtiler

Die Spannungen zwischen den USA, dem Iran und China, die Unterstützung der Ukraine durch die Europäische Union, die Ablehnung des russischen Angriffskrieges, der schwelende Konflikt zwischen China und Taiwan, Heimat des globalen Chip-Marktführer TSMC, das Säbelrasseln Nordkoreas vor der Küste Japans - die Welt ist im Umbruch und politische Einstellungen und daraus hervorgehende Wahlergebnisse werden über die klassischen Medien und Social Media massiv manipuliert. Gezielte Hackerangriffe, öffentlichkeitswirksame Datenschutzverletzungen und die politische und industrielle Spionage werden einer der gravierendsten Trends im Bereich der Cybersicherheit im Jahr 2023 werden. Somit ist die Cyberverteidigung kritischer Infrastrukturen heute eine Schlüsselkomponente der nationalen Sicherheit. Cyber-Resilienz als zentrales Leitbild innerhalb der IT-Strategie beschreibt die Fähigkeit eines Unternehmens, trotz widriger Umstände und Ereignisse in der Sicherheit ihrer Informations- und Kommunikationstechnik, kontinuierlich die beabsichtigten Ergebnisse zu erzielen.

Das kann beispielsweise dadurch realisiert werden, dass nicht konformen Geräten der Zugriff verweigert wird, oder unbekannte oder verdächtige Endgeräte unter Quarantäne gestellt, also isoliert werden. Dadurch bleibt der Rest des Netzwerks, und damit die Produktionsnetze, geschützt. Andere, sichere Geräte dürfen weiterhin auf Unternehmensdaten und vorher definierte Ressourcen zugreifen. Die Produktion und Logistik kommen nicht zum Erliegen. LAN- und WLAN-Zugänge werden mit dieser Funktion einer Netzwerkzugangskontrolle (Network Access Control = NAC) geschützt und mit dem Zero-Trust-Network-Access (ZTNA) erweitert.

3. IT und OT wachsen zusammen – neue Sicherheitskonzepte sind gefragt

Unternehmen befinden sich in der Transformation. Isolierte Office- und Produktionsnetze werden neu strukturiert. Die Digitalisierung schreitet voran, dadurch interagieren OT- und IT-Netzwerke zunehmend. Die Zahl der vernetzten Geräte – bekannt als das Internet der Dinge (IoT) – wird Prognosen zufolge in 2022 18 Milliarden erreichen. Dies hat unter anderem zur Folge, dass die Zahl der potenziellen Angriffspunkte für Cyberkriminelle, die sich Zugang zu sicheren digitalen Systemen verschaffen wollen, enorm steigt. Der dadurch explodierende Datenverkehr findet intern, hybrid und in der Cloud statt. Unternehmen müssen umdenken und neue IT-Sicherheitskonzepte implementieren, die auch außerhalb des eigenen Unternehmensnetzwerks greifen. Hier besteht in Deutschland ein immenser Nachholbedarf. Laut Belden, ein weltweit führender Anbieter von Lösungen für die Signalübertragung, ist die Berücksichtigung der Sicherheit in der Anfangsphase eines Netzwerkdesigns ein wichtiger Schritt zu einem sichereren industriellen Steuerungssystem. Jedoch sollten bei der Umsetzung von Best Practices, etwa durch den Einsatz von Firewalls und des Zonen- und Leitungen-Konzepts, Aspekte aus der IT- und OT-Welt grundsätzlich mit einbezogen werden, die eine umfassende Netzwerksicherheit sowohl für unterschiedliche Angriffsmethoden als auch verschiedene Angreifer berücksichtigen. Sobald ein Angreifer in ein Netzwerk eingedrungen ist, kann er schnell großen Schaden anrichten. Deshalb ist eine zuverlässige Netzwerkzugangskontrolle ein zentrales Element einer integrierten Sicherheitsstrategie.

4. ZTNA schützt Transformation der Arbeitswelt

Die Arbeitswelt befindet sich in einem disruptiven Wandel von der 5-Tage Woche hin zu flexiblen, individuellen Arbeitsmodellen mit ganz neuen Anforderungen an die Arbeitsweisen der Mitarbeiter und die Führungskompetenz des Managements. Diese signifikante Transformation wird durch technologische Fortschritte in der Kommunikation begleitet. Die Digitalisierung befähigt die Mitarbeiter zur globalen Vernetzung, dem Teilen von Daten, dem standortübergreifenden, gemeinsamen Arbeiten an Themen (Kollaboration) und ermöglicht letztendlich eine höhere Produktivität. Diese digitale, effektive sowie zeit- und ortsunabhängige Arbeitsgestaltung beinhaltet aber auch Risiken,

denn sie macht Unternehmen verwundbarer für Wirtschafts-Kriminelle, für externe und interne Angreifer.

Mit dem ZTNA-Ansatz erteilt man nur nach erfolgreichem Berechtigungsnachweis auf Grundlage klar definierter Zugriffskontrollrichtlinien sicheren Zugriff auf Unternehmensanwendungen, -daten und -services. Eine Lösung – Intelligent einfach für Netzwerke und Cloud.

5. 5G-Netz – höhere Interkonnektivität kann zu steigenden Netzwerkangriffen führen

Mit dem Aufkommen und dem Wachstum von 5G-Netzen wird mit dem Internet der Dinge (IoT) eine neue Ära der Interkonnektivität ohne Verzögerungszeiten Realität. Die Kommunikation zwischen mehreren Geräten erhöht die Anfälligkeiten durch Ransomware, gezielte Angriffe oder unbekannte Softwarefehler. Die 5G-Architektur ist vergleichsweise neu und könnte eine Fülle von Netzwerkangriffen mit sich bringen, die uns aktuell noch nicht bewusst sind. Unternehmen erlangen mit 5G eine verbesserte Konnektivität, dedizierte Bandbreite mit Kapazität und Reichweite. Durch die Nutzung privater Netzwerke müssen sie sich Unternehmen auch mit der Absicherung dieser Netzwerke befassen, damit der Sicherheitsstandard, der für IP-Netzwerke in Unternehmen gilt, auch für den Mobilfunkbereich realisiert wird.

6. Deepfakes – Fälschung von Gesichtern, Bildern, Stimmen immer einfacher

Laut Wikipedia sind „Deepfakes… realistisch wirkende Medieninhalte (Foto, Audio und Video), die durch Techniken der künstlichen Intelligenz abgeändert und verfälscht worden sind." Deepfakes nutzen Methoden des maschinellen Lernens, genauer künstliche neuronale Netzwerke, um Fälschungen weitgehend autonom zu erzeugen. Deepfakes stellen auch eine erhebliche Gefahr für die Reputation von Personen, Institutionen und Unternehmen dar. Kriminelle nutzen diese Technologie zunehmend, um an sensible Daten zu gelangen, falsche Informationen zu verbreiten und so den Ruf eines Unternehmens zu schädigen. Es ist davon auszugehen, dass es unter Nutzung von Deepfakes mehr gezielte Phishing-Angriffe („Spear-Phishing") geben wird, um wertvolle Informationen und unternehmenskritische Daten zu gewinnen. Auch kann ein Angreifer diese Social-Engineering Technologie nutzen und eine Person mit der Stimme von deren Führungskraft anrufen, um eine Geldtransaktion auszulösen („CEO-Fraud").

IT-SICHERHEIT IST KEINE AUFGABE, AN DIE MAN EINEN HAKEN MACHEN KANN, SIE ERFORDERT PERMANENTE WACHSAMKEIT UND DIE VERTRAUENSVOLLE KOOPERATION VON INTERNEN UND EXTERNEN EXPERTEN AUF VERSCHIEDENEN EBENEN.

Sabine Kuch,
Selbständige Kommunikations-Beraterin
mit Fokus IT & Technologie
www.macmon.eu

Fazit

Die Bedrohungen von Privatpersonen, Unternehmen und Kritischen Infrastrukturen werden raffinierter und gezielter, ein steter Wettlauf zwischen Cyberkriminellen und deren Gegenspielern. IT-Sicherheit ist deshalb keine Aufgabe, an die man einen Haken machen kann, sie erfordert permanente Wachsamkeit und die vertrauensvolle Kooperation von internen und externen Experten auf verschiedenen Ebenen. Laut dem Statista Research Department sollen im Jahr 2022 Deutschland rund 7,8 Milliarden Euro für IT-Sicherheit ausgegeben werden. Laut Quelle sollen sich die Ausgaben im Jahr 2025 auf rund 10,3 Milliarden Euro belaufen.

Sabine Kuch

HYBRIDE MULTICLOUD-UMGEBUNGEN

DAS MAXIMUM HERAUSHOLEN

DER CLOUD ALS RÜCKGRAT EINER ZUNEHMEND DATENGETRIEBENEN UNTERNEHMENSWELT MANGELT ES AN EINER EINHEITLICHEN MANAGEMENTLÖSUNG.

Marc Kleff, Director Solutions Engineering, NetApp, www.netapp.com

Unternehmen nutzen zunehmend kombinierte Daten-Management-Lösungen, bestehend aus On-Premises- und Cloud-Storage: hybride Multicloud-Umgebungen. Neben den offensichtlichen Vorteilen birgt die Verwaltung dieser unterschiedlichen Umgebungen Herausforderungen, die die Innovationskraft des Unternehmens hemmen. Doch Anbieter von Datendiensten ebnen bereits den Weg zur „Evolved Cloud" – mit einer einfachen Managementplattform, die für eine Kosten- und Performance-Optimierung sowie hohe Sicherheit sorgt und flexible „Consumption"-Modelle abdeckt.

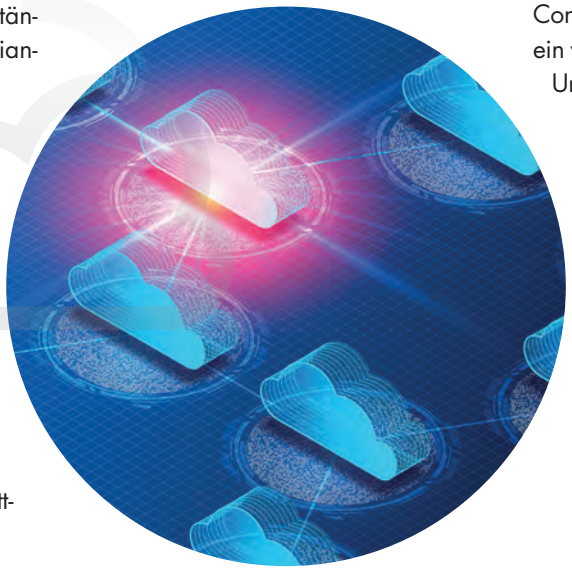
Die digitale Transformation ist im Gange – und Unternehmen halten Schritt, indem sie zunehmend hybride Cloud-Umgebungen nutzen. Inzwischen setzen laut dem Flexera State of the Cloud Report 2021 sogar bereits 92 Prozent von ihnen auf eine Multicloud-Strategie. Damit steigen die Ansprüche der Anwender: Sie möchten ihre Applikationen und Services einheitlich verwalten, auch über verschiedene Cloud-Anbieter hinweg; ihre Leistung, Kostenbilanz und Nachhaltigkeit beständig optimieren; und natürlich Compliance sicherstellen.

Hybrid, aber unkompliziert

Der Cloud als Rückgrat einer zunehmend datengetriebenen Unternehmenswelt mangelt es also aus Unternehmenssicht an einer einheitlichen Managementlösung. Sie ist ein zentraler Bestandteil der „Evolved Cloud" – der nächsten Entwicklungsstufe der hybriden Multicloud. In der Evolved Cloud liefert eine Managementplattform die notwendige Übersicht und stellt eine einheitliche, übergeordnete Plattform für unterschiedlichste Verwaltungsfunktionen und Datenservices bereit. Die Unternehmensdaten einschließlich On-Premises-Storage und Public Cloud-Storage sind darüber einsehbar und verwaltbar. Damit ist beispielsweise das Kopieren, Synchronisieren, Tiering und Zwischenspeichern von Daten nach einem einfachen „Drag and Drop"-Prinzip über alle großen Clouds und das unternehmenseigene Rechenzentrum hinweg möglich. Softwareanbieter wie NetApp stellen derlei Plattformen als SaaS bereit.

Optimierung und Sicherheit dank integrierter KI

Komplettiert wird die Evolved Cloud durch weitere leistungsstarke Funktionalitäten zur Optimierung und Bereitstellung von IT-Services: AIOps-gestützte Analysen und Automatisierung reduzieren den Personalbedarf, die Ressourcenbelastung und das Risikoprofil. Eine KI-gestützte Zustands- und Statusüberwachung warnt nicht nur vor Infrastruktur- und Workload-Problemen, sondern gibt auch proaktive Empfehlungen zur Vermeidung von Problemszenarien. Für den Schutz und die Sicherheit sorgen Data-Protection-Mechanismen gemäß eines Zero-Trust-Modells sowie ein Ransomware-Dashboard zur Beseitigung entsprechender Schwachstellen. Dazu gehören KI/ML-Funktionen, welche die Infrastruktur zum Schutz vor Ransomware-Attacken in Echtzeit überwachen.



„Consumption" ist König

Damit Unternehmen auch wirklich das Maximum aus ihren Cloud-Umgebungen herausholen, ohne viel zu investieren, sind Consumption-basierte Nutzungsmodelle ein weiterer Eckpfeiler der Evolved Cloud. Unternehmen zahlen nur für das, was sie brauchen, also die tatsächlich in Anspruch genommenen Leistungen. Das Lizenzmanagement dafür findet Cloudanbieter-unabhängig in der Managementplattform statt.

Fazit: Das Evolved Cloud-Paradigma gibt die neue Richtung vor – schnelle Anwender treiben Innovationen effektiver voran und sind erfolgreicher.

Marc Kleff

ECHTZEIT-DATENVERARBEITUNG

WENN ES MAL SCHNELLER GEHEN SOLL

Wartezeiten kommen immer mehr aus der Mode. Stehen Daten nicht sofort zur Verfügung, werden die Anwender schnell ungeduldig. Wie verhält es sich mit Echtzeit-Anwendungen? Worauf sollte man achten, wenn Daten und IOs schnell verarbeitet werden müssen und kurzfristig viele Daten anfallen. Wir denken hier auch an das Metaverse.

Big-Data breitet sich seit längerem überall aus, auch wenn die meisten nur sehr schwammige Definitionen dieses Begriffes parat haben. Unternehmen und Organisationen benötigen Rechen- und Speichersysteme zur Verarbeitung dieser riesigen Datenmengen im Moment der Erfassung, oder eben sehr zeitnah. Die Online-Berechnung von Routen über entsprechende Anwendungen wird immer präziser, je mehr Störungen oder schnellere Alternativen in die Kalkulation einbezogen werden können.

Und wir als Anwender erwarten schon heut praktisch als Selbstverständlichkeit, dass all diese Berücksichtigungen in „Echtzeit" geschehen und das tatsächliche Geschehen auf den Straßen metergenau nachzeichnen. Um die für eine echtzeit-Datenverarbeitung notwendige sehr hohe Datenrate für Annahme, Verarbeitung und Ausgabe von Informationen zu erzielen, ist der Einsatz von Echtzeit-Verarbeitungssystemen unumgänglich. Entsprechende Systeme sind in solchen Fällen nicht nur nützlich, sondern daneben auch zu praktisch zwingender Voraussetzung für Marketing-, Vertriebs-, Finanz- oder Kundendienstsysteme geworden. Nur so können Unternehmen zeitgemäße Dienstleistungen anbieten und ihre verwöhnten Kunden zufrieden stellen.

Datenverarbeitung ein sechsstufiger Prozess

Bei der Verarbeitung von Daten werden diese klassisch in eine nutzbare Form umgewandelt, um sie dann analysieren und aus ihnen Schlussfolgerungen ziehen zu können. Für das Sammeln dieser Daten ist in sich für modern haltenden Unternehmen die Berufsgruppe der „Data Scientists" geschaffen worden. Digitale oder elektronische Datenverarbeitungsmethoden (EDV) verwenden Maschinen, Computer, Arbeitsstationen, Server und schließlich Software zur Aufbereitung jeglicher Informationen. Einschlägige Werkzeuge generieren Grafiken, Diagramme, Bilder, Tabellen, Audio- oder Videodateien neben vielen anderen Formaten, um diese verständlich zu machen. Generell betrachtet ist die Datenverarbeitung ein sechsstufiger Prozess, welcher das Aufnehmen, Vorbereiten, Sortieren, Verarbeiten, Analysieren, Ausgeben und Speichern von Daten umfasst.

Von Cybersicherheit bis zu Banktransaktionen

Eine in Echtzeit arbeitende Maschine nimmt Eingaben entgegen, verarbeitet diese und liefert in möglichst kürzester Zeit, heute im Bereich weniger Millisekunden, eine Ausgabe zurück. Mit Echtzeitverarbeitung ist also eine kontinuierliche Eingabe zu konstanter Verarbeitung von Daten aus verschiedenen Quellen mit sehr kurzer Latenz gemeint.

Da Unternehmen fast schon gezwungen sind immer mehr Daten sammeln, ist es zwingend notwendig, diese Informationen ebenfalls immer schneller zu analysieren, um sich damit einen Wettbewerbsvorteil zu verschaffen. In vielfältigen Bereichen der Überwachung von Netzwerken und Rechner, der „Cybersicherheit", in Banken bis hin zum elektronischen Handel wird Echtzeit-Datenverarbeitung benötigt, um beispielsweise Betrugsversuche zu erkennen, Transaktionen zu überwachen und darüber hinaus Möglichkeiten zur Verbesserung des Geschäftsbetriebes zu erkennen.

Ein bereits erwähntes Beispiel der Echtzeitverarbeitung ist die Verwendung von Online-Routensystemen. Diese Software aktualisiert automatisch Staumeldungen auf Basis von Informationen, welche durch andere mobile Geräte und stationären Straßensensoren erfasst und weitergeleitet werden. Auf dieser Grundlage kann die Software mit minimalen Updatezeiten die kürzesten, schnellsten oder verbrauchsgünstigsten Alternativen zum Ziel vorschlagen.

Auch Banken verarbeiten täglich unzählige Transaktionen von Kunden und mit anderen Instituten. Durch die Integration von Echtzeit-Datenverarbeitungsmethoden in die Transaktionsprotokollierung lässt sich sicherstellen, dass ausschließlich legitime Transaktionen genehmigt und betrügerische Transaktionen ausgeschlossen werden.

Echtzeitverarbeitung

Die Vorteile dieser Echtzeit-Datenverarbeitungssysteme liegen klar auf der Hand. Benutzeranfragen können sofort beantwortet und Datenbanken ohne Wartezeiten aktualisiert werden. Da es keine Verzögerungen mehr gibt, sorgen die Systeme für zeitnahes Handeln. In Szenarien mit einem hohen Anteil an Änderungen in den Nutzerdaten stellt die

Echtzeitverarbeitung sicher, dass neue Datensätze in kurzer Zeit synchronisiert werden und zur Verfügung stehen. Auch die Datenlade- und Speicherzeiten verbessern sich spürbar, so dass auch aus diesem Bereich die schnellere Gewinnung neuer Erkenntnisse unterstützt wird.

Darüber hinaus sind Daten so gut wie nie veraltet. Alle Sätze sind aktuell und korrekt. Dies ermöglicht schnellere und hoffentlich auch intelligentere Reaktionen auf ein sich ändernde Umfelder. Auf Basis immer aktueller Daten können Unternehmen kurzfristig auf Neuerungen im Markt oder sich ändernde Kundenpräferenzen reagieren. Volle Lager mit nicht mehr passenden Produkten oder nicht zielführende Werbung gehören der Vergangenheit an. Echtzeitberichte halten über alle aktuellen Abläufe auf dem Laufenden, Engpässe und damit verbundene Probleme lassen sich schnell erkennen oder gar im Vorlauf vermeiden.

Echtzeitarchitekturen aus vier Komponenten

Echtzeitarchitekturen bestehen grundsätzlich aus vier Komponenten. Nachrichtenaufnahmesysteme nehmen eingehende Datenströme oder Nachrichten aus einer Vielzahl von Quellen entgegen. Die Daten werden dann durch einen Stream Processing Consumer verarbeitet. Dieser kann als einfacher Datenspeicher aufgebaut sein, der neue Informationen in bestimmten Ordnern speichert. Meistens wird jedoch auch ein Message Broker als Puffer für die Informationen eingesetzt, wodurch eine Scale-out-Verarbeitung und eine zuverlässige Übermittlung gewährleistet wird. Weiter geht es dann zu den Stream-Prozessoren. Diese verarbeiten die aufgenommenen Informationen, indem sie typische Vorgänge wie Filtern, Zusammenfassen oder Vorbereitung für die folgende Datenanalyse durchführen.

Der Analytical Data Store ist auf die Aufbereitung und Verwaltung großer Datenmengen spezialisiert. Hier werden Daten für die Analyse vorbereitet um sie dann strukturiert bereitzustellen, so dass sie sich dann durch eine Analyse-Software abfragen lassen. Dieser Analytical-Data-Storage ist für schnellste Antwortzeiten, sowohl für Abfragen als auch für erweiterte Analysen optimiert. Der letzte Schritt bei der Echtzeit-Datenverarbeitung besteht schließlich darin, Diagramme, Berichte oder Grafiken zu erstellen und praktisch umsetzbare Erkenntnisse bereitzustellen, die leicht verfügbar und für alle verständlich sind (oder zumindest sein sollten).

Stapelverarbeitung ist, wie der Name schon sagt, eine serialisierte Verarbeitung von Daten in großen Mengen. Anstatt in Echtzeit zu arbeiten, sammelt die Stapelverarbeitung Transaktionen über einen bestimmten Zeitraum und plant ihre Weiterverarbeitung zu einem späteren Zeitpunkt. Als Ergebnis der Nachbearbeitung lassen sich die Ausgaben von Anwendungen anzeigen. Diese Ausgaben können dann durch geeignetes Personal analysiert werden, um fundierte Entscheidungen zu treffen. Im Gegensatz zur Echtzeitverarbeitung zeichnet sich die Stapelverarbeitung durch eine größere architekturelle Flexibilität, allerdings auch durch eine deutlich langsamere Reaktion auf sich ändernde externe Bedingungen aus.

Doc Storage

DOC STORAGE beantwortet alle Ihre technischen Fragen zum Thema Storage, Backup und Co.

docstorage@speicherguide.de

War der Artikel interessant?
Dann lesen Sie hier weiter:

Computational-Storage: Speicher für Echtzeit-Datenverarbeitung

ERSTMALIG
SUPPLEMENT
it security

AUSGABE 01-02/2023
ERSCHEINT AM
31. JANUAR 2023

IT MANAGEMENT

IT & Nachhaltigkeit
Web 3.0
Cloud Computing

IT SECURITY

Security Awareness
Threat Intelligence
Security-Innovationen

DAS NEUE IT MANAGEMENT 01/02 2023
ERSCHEINT AM 31. JANUAR 2023

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:
Simon Alexander Appel, Nikolas Bradford, Lennard Everwien, Dina Haack, Prashant Ketkar, Marc Kleff, Lea Kraus, Sabine Kuch, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Christian Rudolf, Stephanie van de Straat, Thomas Timmermann, Jan Willeke

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 30. Preisliste gültig ab 1. Oktober 2022.

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

IT WELT.at is IT

IT NEWS

Der tägliche Newsletter der ITWELT.at bringt die aktuellen IT Nachrichten aus Österreich und dem Rest der Welt. Wer immer up to date sein will, bestellt den kostenlosen Newsletter itwelt.at/newsletter und ist damit jeden Tag schon am Morgen am neuesten Informationsstand.

itwelt.at

IT TERMINE

In Österreichs umfangreichster IT-Termindatenbank gibt es Termine für IT-Events wie Messen, Konferenzen, Roadshows, Seminare, Kurse und Vorträge. Über die Suchfunktion kann man Thema und Termin suchen und sich bei Bedarf auch gleich anmelden. Mit Terminkoordination und Erinnerung per E-Mail.

itwelt.at/events

IT UNTERNEHMEN

TOP 1001 ist Österreichs größte IT-Firmendatenbank. Mit einer Rangliste der umsatzstärksten IT- und Telekommunikations-Unternehmen. Die Datenbank bietet einen Komplettüberblick der TOP IKT-Firmen und ermöglicht die gezielte Abfrage nach Tätigkeitsschwer-punkten, Produkten und Dienstleistungen.

itwelt.at/top-1001

IT JOBS

Hier sind laufend aktuelle IT Job-Angebote zu finden. In Zusammenarbeit mit der Standard.at/Karriere, dem Jobportal der Tageszeitung Der Standard, findet man auf dieser Plattform permanent hunderte offene Stellen aus dem Bereich IT und Telekom. Eine aktive Jobsuche nach Tätigkeitsfeld und Ort ist natürlich möglich.

itwelt.at/jobs

Eine Veranstaltung von itsecurity & it-daily.net
Das Online-Portal von Itmanagement & Itsecurity

SAVE THE DATE

IAM CONNECT 2022

Dynamisches IAM

07.12.2022 | Digitalevent

#dynamicIAM
#IAMConnect2022

itsecurity
DEZEMBER 2022

DAS SPEZIAL

CYBERSICHERHEIT

DIE INDUSTRIE MUSS AUFHOLEN

Dr. Kai Martius, secunet Security Networks AG

THOUGHT LEADERSHIP

DISASTER RECOVERY

Kein Weg führt am Active Directory vorbei

RISIKO SCHATTEN-IT

Verborgene Gefahren im Netzwerk

RANSOMWARE-ANGRIFFE

E-Mails versenden ohne Risiko

www.it-daily.net

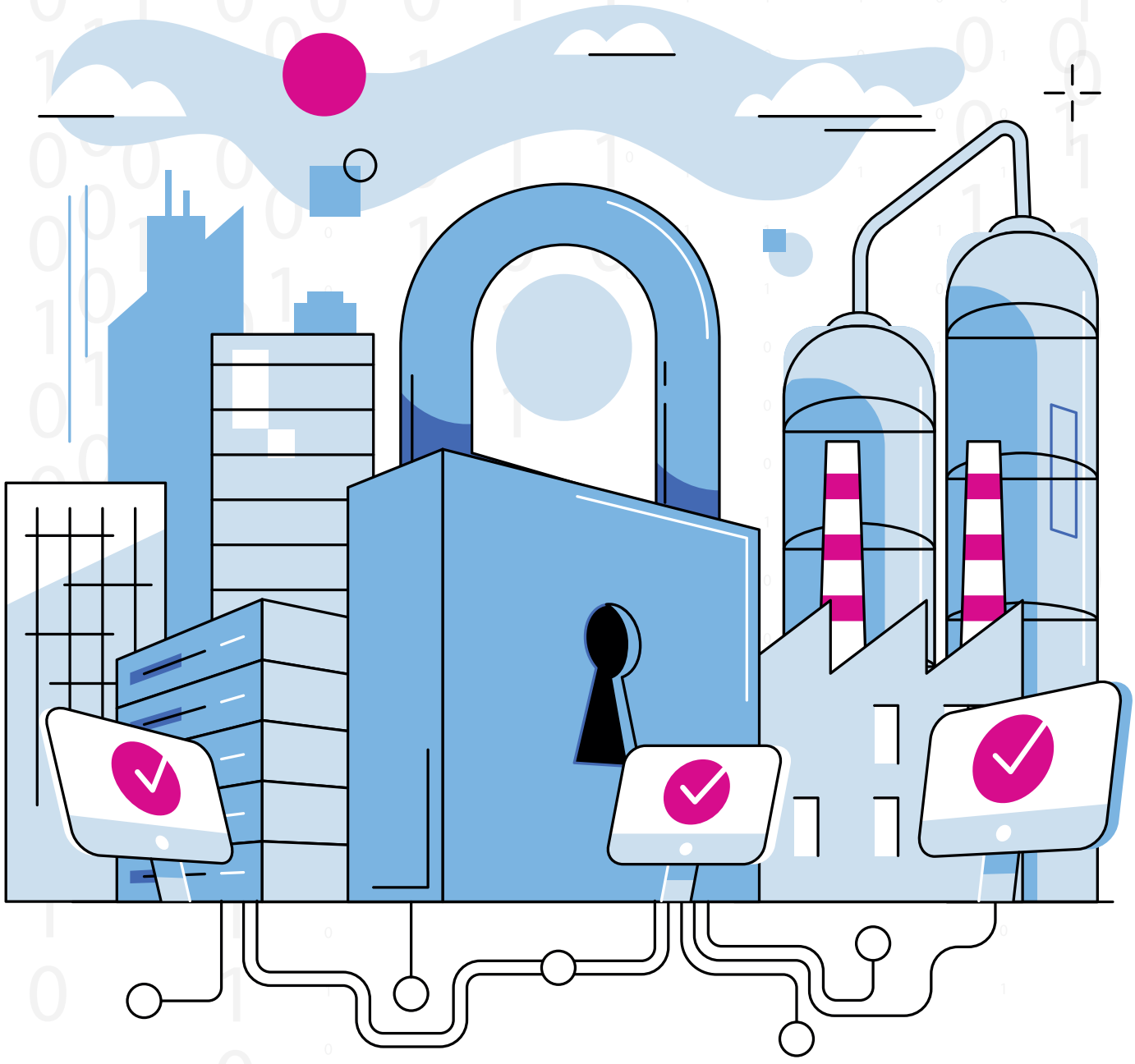
13

4 COVERSTORY

INHALT

NACHHOLBEDARF IN PUNKTO CYBERSICHERHEIT

DIGITALE TRANSFORMATION IN DER INDUSTRIE



Bei der Absicherung industrieller Netzwerke besteht vielerorts Verbesserungspotenzial. Woran das liegt und was Unternehmen dagegen tun können, erklärt Dr. Kai Martius, Chief Technology Officer von secunet im Interview mit it security.

it security: *Herr Dr. Martius, wie steht es um die Cybersicherheit in Deutschland?*

Dr. Kai Martius: Das Cybersicherheitsniveau ist recht unterschiedlich, je nachdem ob wir uns staatliche Institutionen, kritische Infrastrukturen oder die freie Wirtschaft einschließlich der Industrie anschauen. In der strikt regulierten öffentlichen Verwaltung besteht schon seit Langem ein hohes Sicherheitsniveau. Bei den kritischen Infrastrukturen gibt es demgegenüber noch Potenzial, doch seit 2015 lassen das IT-Sicherheitsgesetz (IT-SiG) und dessen Novelle IT-SiG 2.0 das Cybersecurity-Level steigen.

Industrieunternehmen hingegen können selbst über ihr Cybersicherheitsniveau entscheiden. Das bedeutet, dass sich mögliche Investitionen in die Cybersicherheit stets gegen andere Vorhaben mit eindeutigeren, kurzfristigen Erfolgsaussichten durchsetzen müssen. Zudem fehlen gerade mittelständischen Unternehmen oftmals schlicht die Ressourcen beziehungsweise das Fachpersonal, um größere Cybersecurity-Projekte zu stemmen.

it security: *Dabei sind Cyberangriffe eine reale Gefahr und auch ein wirtschaftlicher Faktor.*

Dr. Kai Martius: Richtig, mittlerweile sprechen auch die Umfragen in dieser Hinsicht eine deutliche Sprache. In der kürzlich veröffentlichten IDC-Studie „Cybersecurity in Deutschland 2022" gaben 32 Prozent der befragten Unternehmen an, in den letzten zwölf Monaten Opfer einer Ransomware-Attacke geworden zu sein. 79 Prozent der Betroffenen haben Lösegeld bezahlt. Darüber hinaus müssen angegriffene Unternehmen mit wirtschaftlichen Schäden etwa durch Produktionsausfälle rechnen. Neben Ransomware werden Industrieunternehmen auch mit Sabotageabsichten angegriffen oder zum Zweck der Wirtschaftsspionage.

Doch das Rad der digitalen Transformation zurückdrehen will niemand. Die Vernetzung von Geräten und Maschinen im industriellen Internet der Dinge (IIoT) bringt den Unternehmen klare operative und wirtschaftliche Vorteile – etwa in Form von Effizienzsteigerungen, Kostenoptimierung oder neuen Geschäftspotentialen. Vor diesem Hintergrund ist eine sichere und zuverlässige IT-Infrastruktur essenziell für den Unternehmenserfolg.

it security: *Sind sich Industrieunternehmen Ihrer Erfahrung nach dessen bewusst?*

Dr. Kai Martius: Es ist zumindest eine positive Entwicklung zu beobachten. Die IT-Abteilungen schätzen die Zusammenhänge und Risiken schon länger korrekt ein. Allerdings fehlte oft der Rückhalt durch die Führungsebene. In der erwähnten IDC-Studie gaben nun immerhin 61 Prozent der befragten Unternehmen an, Cybersecurity sei durch ein Mitglied der Geschäftsführung oder durch ein nicht geschäftsführendes Vorstandsmitglied auf oberster Ebene vertreten. Dennoch besteht noch Aufholpotenzial im Vergleich zu kritischen Infrastrukturen. Aus diesem Grund sollten sich Industrieunternehmen aus meiner Sicht am IT-SiG 2.0 orientieren, auch wenn dessen Bestimmungen für sie nicht verpflichtend sind. Sinnvoll sind sie aber dennoch.

it security: *Was sind die Einfallstore, die am meisten Aufmerksamkeit erfordern?*

Dr. Kai Martius: Zunächst sollte man die klassische Büro-IT nicht vergessen, die zum Beispiel mittels Phishing oder Sicherheitslücken in Office-Software angegriffen werden kann. Ansonsten ist vor allem die fortschreitende Vernetzung von Maschinen und Anlagen über das IIoT sicherheitstechnisch anspruchsvoll – insbesondere dann, wenn die Netzwerke für Szenarien wie Fernwartung auch an externe Stellen angebunden sind. Diesen Ansprüchen wird man oft nicht gerecht, schon weil die Unternehmen bei der Digitalisierung und Vernetzung nicht bei Null anfangen können, sondern mit dem arbeiten müssen, was sie haben. Im Ergebnis hängen an den Operational Technology (OT)-Netzwerken nicht selten Maschinen, die 30 Jahre oder noch älter sind. Diese Maschinen wurden nicht für eine Vernetzung geschaffen. Findet diese dennoch statt, fehlen oft die nötigen Sicherheitsmaßnahmen.

WER EIN NETZWERK BETREIBT, SOLLTE JEDERZEIT WISSEN, WAS DARIN PASSIERT.

Dr. Kai Martius,
Chief Technology Officer,
secunet Security Networks AG,
www.secunet.com

In vielen Industrieunternehmen besteht darüber hinaus kein vollständiger Überblick, welche Geräte überhaupt an das Netzwerk angeschlossen sind. Dann fällt mitunter erst im Nachhinein bei der Analyse eines erfolgreichen Angriffs auf, dass es da noch diesen alten Industrie-PC gab, der in keiner Dokumentation auftauchte, über den die Angreifer es aber ins Netzwerk geschafft haben.

it security: *Wie sollten sich Industrieunternehmen gegen diese Risiken wappnen?*

Dr. Kai Martius: Mit Blick auf die Büro-IT sind zunächst einmal die Basics wichtig, zum Beispiel aktuelle Firewalls, regelmäßige und funktionierende Backups und Patches, feingranulare Zugriffskontrolle und turnusmäßige Passwortänderungen. Das ist nicht immer selbstverständlich. Auch Awareness-Schulungen für Mitarbeitende können sehr hilfreich sein.

Um die industriellen IT/OT-Netzwerke abzusichern, muss in der Regel erst einmal eine Bestandsaufnahme gemacht werden. Dabei werden alle Systeme, darunter auch veraltete Legacy-Geräte, vollständig erfasst. In Penetrationstests ermitteln „ethische Hacker" Sicherheitslücken. Auf dieser Basis werden die neuen Anforderungen festgestellt. Und erst dann werden die passenden Maßnahmen definiert und umgesetzt. Die Systeme werden sicher vernetzt, vor allem werden die Übertragungswege zwischen Maschine und Verarbeitungsort abgesichert. Dabei handelt es sich oftmals um hybride Infrastrukturen, beispielsweise der eigenen Infrastruktur oder der Cloud.

Auch kann der Einsatz einer vertrauenswürdigen „Private Cloud" sinnvoll sein, um die Vorteile der zuvor genannten Betriebsarten zu kombinieren und zudem die Datenhoheit zu behalten. secunet baut gerade eine sichere und souveräne Cloud-Infrastruktur made in Germany auf, an die industrielle Systeme angebunden werden können, um etwa besonders sensible Daten zu verarbeiten.

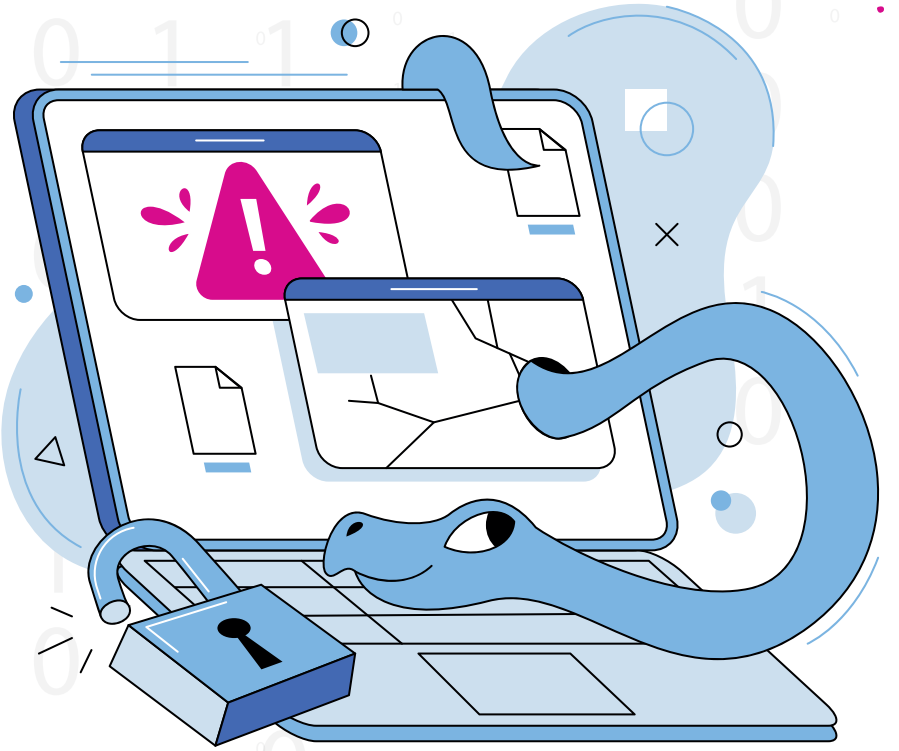
it security: *Was sind aus Ihrer Sicht die wichtigsten Bausteine bei der Absicherung industrieller Netzwerke?*

Dr. Kai Martius: Für die sichere Anbindung von Maschinen gibt es Lösungen, die IIoT-Gateway, Edge-Computing-Plattform und Firewall in sich vereinen. Sie werden dezentral in Form von Appliances implementiert und bringen auch Legacy-Maschinen sicher ans IIoT. Ein Retrofit bestehender Maschinen und Anlagen ist damit also möglich. Zudem können auf den Appliances auch Anwendungen wie etwa Fernwartung und Monitoring laufen, und sie ermöglichen auch eine sichere Cloud-Anbindung.

Ein weiterer wichtiger Baustein ist ein System zur Angriffserkennung, wie es auch im IT-SiG gefordert wird. Wer ein Netzwerk betreibt, sollte jederzeit wissen, was darin passiert. Je früher ein Vorfall erkannt wird, desto effektiver können Schäden eingedämmt werden. Monitoring-Systeme, die mit passiven Sensoren arbeiten, erfassen den Netzwerkverkehr datenschutzkonform und ohne negativen Einfluss auf die überwachten Netzwerke und Geräte. Die Daten werden dann zentral analysiert, korreliert und erlernt, um Schwachstellen, Compliance-Abweichungen, Anomalien, unerwünschte Kommunikationspartner und mögliche Angriffe zu erkennen.

Wie immer in der Cybersecurity gilt auch hier: Wirksame Komponenten und ein ganzheitlicher Blick sind die Erfolgsfaktoren. Gelingt es Industrieunternehmen, eine sichere und zuverlässige IT-/OT-Infrastruktur aufzubauen, ist das jedenfalls eine gute Investition in die Zukunft.

it security: *Herr Dr. Martius, vielen Dank für das Gespräch.*



THANK YOU

CYBERCRIME UND CYBERSICHERHEIT

EINS BEDINGT DAS ANDERE

Je besser die Sicherheitsstrategie, desto größer ist die Herausforderung für den Angreifer.
Je hartnäckiger der Angreifer, umso ausgefeilter muss die Sicherheitstechnologie sein.
Es ist wie ein Wettkampf: Wer ist besser, wer ist schneller, wer effizienter?

Nur, wenn das angegriffene Unternehmen der Verlierer ist, gibt es keinen Trostpreis,
sondern einen immensen Schaden, der viel Zeit und Geld kostet.
Wenn der Angreifer der Verlierer ist, sucht er sich einfach das nächste Opfer.

Das sollte nicht so sein, besonders nicht so einfach!

SECURITY-VERANTWORTLICHE MÜSSEN DEFIZITE AUFHOLEN

NEVIS SICHERHEITSBAROMETER

Cyberangriffe mit Ransomware und Phishing sowie Onlinebetrug sind laut Polizisten und Polizistinnen in aller Welt aktuell die größten kriminellen Bedrohungen; lediglich die Gefahr durch Geldwäsche wird als noch höher eingeschätzt – so die alarmierende Meldung aus dem 2022 erstmals veröffentlichen Interpol-Report. Über 70 Prozent der Befragten erwarten laut Interpol, dass Angriffe mit Ransomware und Phishing-Attacken in den kommenden drei bis fünf Jahren stark oder sehr stark zunehmen werden. Dementsprechend sollten sich Unternehmen und Verbraucher für weiter zunehmende Angriffsversuche der Cyberkriminellen wappnen – doch sind sie darauf angemessen vorbereitet? Dieser Frage geht das aktuelle Nevis Sicherheitsbarometer auf den Grund. Die Resultate der Studie zeigen, dass es hier viel Verbesserungspotenzial gibt. Besonders auffällig sind die Diskrepanzen zwischen den Erwartungen der Kunden und der Sicht der Unternehmen. Nicht zuletzt verhindern Wissensdefizite der IT-Entscheider, dass Verbesserungen rasch umgesetzt werden.

Für das Nevis Sicherheitsbarometer hat Nevis in Zusammenarbeit mit den Meinungsforschungsunternehmen Civey und mo'web research im Juli und August dieses Jahres 500 deutsche IT-Entscheider und 1.000 deutsche Konsumenten ab 14 Jahren zu Themen wie Passwortsicherheit und Loginverhalten online befragt.

Wachsende Gefahren

Die Mehrzahl der für das Nevis Sicherheitsbarometer befragten IT-Entscheider bestätigt die Diagnose des Interpol-Reports: Rund 57 Prozent gaben an, im letzten Jahr in ihrem beruflichen Umfeld einen Anstieg der Cyberkriminalität wahrgenommen zu haben; 39 Prozent sehen eher ein gleichbleibendes Niveau. 54 Prozent der IT-Profis erklärten zudem, dass ihr eigenes Unternehmen innerhalb der letzten 12 Monate Opfer einer Cyberattacke wurde. Dabei lässt sich nach ihren Angaben ein Viertel (26 Prozent) der registrierten Angriffe dem Bereich

Ransomware zuordnen. Auf den weiteren Plätzen folgen Denial of Service (DoS) mit 20 Prozent, Brute-Force-Angriffe (18 Prozent) und Social Engineering (17 Prozent). Auffallend ist die mit 6 Prozent relativ seltene Nennung von Credential Stuffing – hier ist von einer hohen Dunkelziffer auszugehen, da bei dieser Angriffsvariante gestohlene Login-Daten zum Einsatz kommen, wodurch sie oft über lange Zeit unentdeckt bleibt.

IT-Entscheider mit Wissenslücken

Trotz der wachsenden Bedrohung ist die Cybersicherheit bei vielen Unternehmen längst nicht so gut, wie sie sein könnte – und auch der Informationsstand vieler IT-Entscheider könnte durchaus besser sein. Die meistgenannten Vorkehrungen sind, wie schon im Sicherheitsbarometer des Vorjahres, das Vorschreiben von Mindestlängen für Passwörter (65 Prozent) und die Verpflichtung zu regelmäßigen Passwortänderungen (41 Prozent). Auf die Zwei-Faktor-Authentifizierung per SMS setzen lediglich 34 Prozent; auf eine biometrische Zwei-Faktor-Authentifizierung nur 21 Prozent. Besonders erschreckend: rund 10 Prozent der befragten IT-Verantwortlichen geben an, keine Vorkehrungen für erhöhte IT-Sicherheit zu treffen. Und wenn es um Cybersecurity-Standards wie FIDO, Oauth oder WebAuthn geht, zeigt sich gerade einmal die Hälfte der Befragten mehr oder weniger gut informiert. Die andere Hälfte (47 Prozent) ist nach eigenem Bekunden mit keinem einzigen der gängigen Standards vertraut.

Die Gefahren aus Kundensicht

Und wie ist es auf Verbraucherseite um das Gefahrenbewusstsein in puncto IT-Sicherheit bestellt? Hier zeigt das Nevis Sicherheitsbarometer: Die Angst vor Cyberattacken und die Sorge um persönliche Daten ist unvermindert groß. Lediglich 5 Prozent der Befragten zeigen sich bezüglich der Sicherheit ihrer Daten absolut unbesorgt. Im Vergleich zum Vorjahr sind die Werte hier praktisch unverändert geblieben.

Wovor fürchten sich die Verbraucher konkret? Rund 68 Prozent sehen im Missbrauch der persönlichen Daten die größte Gefahr. Mit jeweils 59 Prozent ebenfalls weit oben in der Gefahrenliste sind die Angst vor Internetbetrug sowie die Angst, dass ein Fremder die persönlichen Internetkonten übernimmt. Die Bedenken gegenüber staatlicher Überwachung sind demgegenüber weniger stark ausgeprägt. Nur 28 Prozent der Befragten sehen darin eine Gefahr – eine Abnahme um sieben Prozent im Vergleich zur letzten Ausgabe des Nevis Sicherheitsbarometers.

Gleichzeitig nehmen es private Nutzer mit der Sicherheit nicht immer so genau, wie es eigentlich wünschenswert wäre: Im Rahmen der Befragung gaben 54 Prozent an, ein und dasselbe Passwort für mehrere Online-Konten zu verwenden – für Security-Experten ein absolutes No-Go. Trotz solcher Nachlässigkeiten ist sich die Mehrzahl über die Grundlagen der Passwortsicherheit durchaus im Klaren: 59 Prozent nutzen besonders komplexe Passwörter, die von Hackern nicht einfach erraten werden können, und immerhin 44 Prozent verwenden verschiedene komplexe Passworte für unterschiedliche Konten. Noch ausbaufähig ist die Nutzung moderner Sicherheitsverfahren: So greifen nur 34 Prozent auf die besonders sichere Zwei-Faktor-Authentifizierung zurück, um sich in ihre Konten einzuloggen; bei der biometrischen Authentifizierung – beispielsweise via FaceID oder Fingerbadruck – sind es sogar nur 17 Prozent. Dass dies nicht zuletzt daran liegt, dass viele Unternehmen diese Verfahren noch nicht im Einsatz haben, zeigt der Vergleich zwischen Kundenerwartungen und der Einschätzung durch die IT-Profis.

Kunden und Unternehmen mit unterschiedlichen Erwartungen

Für die Dienstleister im Internet ist es ein Dilemma: Ihre Kunden mögen selbst in puncto IT-Sicherheit noch Nachholbedarf haben, an die Unternehmensseite stellen sie aber hohe Erwartungen in Bezug auf Datenschutz und Cybersecurity – Erwartungen, die die Unternehmen nicht immer erfüllen. Besonders ins Auge fällt das beim Thema Zwei-Faktor-Authentifizierung: Während nur 4 Prozent der IT-Experten davon ausgehen, dass Kunden sich eine Zwei-Faktor-Authentifizierung (2FA) zur Konten-Absicherung wünschen, sind es tatsächlich 64 Prozent! Nicht zuletzt würden sich 45 Prozent der befragten Konsumenten sicherer fühlen, wenn ihre biometrischen Daten zum Login genutzt würden – dagegen gehen 57 Prozent der IT-Verantwortlichen davon aus, dass auf Kundenseite nur eine geringe Bereitschaft zur Nutzung dieses besonders sicheren Verfahrens bestehe.

www.nevis.net

Das Nevis Sicherheitsbarometer steht unter folgendem Link zum Download bereit:

ALLIIERTE FÜR CYBERSICHERHEIT

MENSCH, MASCHINE UND TELEMETRIE

Sophos hat kürzlich neue Kompatibilitäten zwischen Sicherheitstechnologien von Drittanbietern und seinem Service Sophos Managed Detection and Response (MDR) vorgestellt. Ziel dieser entscheidenden Neuerung innerhalb der IT-Sicherheitsbranche ist es, Angriffe in unterschiedlichen Kunden- und Betriebsumgebungen noch schneller und präziser zu erkennen und zu beheben. Sophos MDR mit aktuell mehr als 12.000 Kunden integriert die Telemetrie von Endpoint-, Firewall-, Cloud-, Identitäts-, E-Mail- und weiteren Sicherheitstechnologien anderer Hersteller als Teil des Sophos Adaptive Cybersecurity Ecosystem.

So richtungsweisend diese Neuerung erscheint, so notwendig und folgerichtig ist sie. Denn wohin die Reise der Cybersicherheit geht, ist durch das unglaublich hohe kriminelle Potenzial der Cyberkriminellen klar definiert. Wie ernstzunehmend die Bedrohungslage ist, belegen Zahlen des BSI: So wurden 2021 nicht weniger als rund 144 Millionen neue Schadprogramme identifiziert. Ein gutes Viertel der betroffenen Unternehmen und Organisationen bewerteten die Angriffe, mit denen sie konfrontiert waren, als eine schwerwiegende oder existenzbedrohende Gefahr. Und dieses Gefahrenpotenzial wiegt umso schwerer, wenn etwa kritische Infrastrukturen (Unternehmen oder Organisationen, etwa aus den Bereichen, Energie, Gesundheit, Wasser oder Ernährung) das Ziel cyberkriminellen Angriffe sind.

Klassische Sicherheitsmodelle scheitern

Die Gefahren für Unternehmen sind zum Teil hausgemacht und wie eine offene Einladung für Cybergangster. Unternehmen stehen unter dem kontinuierlichen Druck, Prozesse und Budgets zu optimieren. Nahezu jeder Bereich lässt sich dabei auslagern bzw. extern hinzukaufen. Die Nutzung der Cloud und das Zugreifen auf Fremd-Software findet aber nicht nur im eigenen Betrieb statt. Auch Partner und Kunden sind von außen an die Kernsysteme des Unternehmens angebunden. Auch die Entscheidung für Software-as-a-Service (SaaS) hat für Unternehmen zunächst einmal viele Vorteile. Ressourcen wie technische Ausstattungen, Räumlichkeiten, Know-how aber

auch Personal müssen nicht vorgehalten werden. Die Verwendung extern gelagerter Software bedeutet aber oftmals auch, dass die Angriffsfläche für Cyberkriminelle steigt und diese immer mehr Möglichkeiten erhalten, in Geräte und Netzwerke eines Unternehmens einzudringen.

Im Ergebnis jedenfalls existiert zunehmend nicht mehr das eine Netzwerk, in dem alle eingebundenen Systeme sicher sind, sondern ein weit verzweigtes Netzwerk-Ökosystem, das mit klassischen Mitteln der Security nicht mehr effizient abgesichert werden kann.

Die IT-Sicherheitsbranche reagiert auf diese neuen Anforderungen mit immer intelligenteren Lösungen, die unter anderem auch auf Machine Learning und komplexen Algorithmen aufbauen. Je nach Unternehmensgröße, Budget und Mentalität lässt sich der existierende Schutz mit einer Strategie, Services und Technik inhouse oder mit externem Expertentum erweitern, ohne die individuellen Arbeitsprozesse maßgeblich zu tangieren.

Schlüsselrolle und zugleich Mangelware: Menschliche Expertise

In einem effektiven und modernen Security-Ökosystem werden zusätzlich immer mehr auch menschliche Fähigkeiten benötigt, um das zu ergänzen, was bis heute keine Schutztechnologie leisten kann. Dazu gehören beispielsweise Forensiker oder Task-Teams mit jahrelanger Expertise.

DIE SOPHOS EXPERTENTEAMS SIND IN DER LAGE, BEDROHUNGEN IN EINER VIELZAHL VON UMGEBUNGEN ZU ERKENNEN UND ZU BESEITIGEN – EINSCHLIESSLICH KOMPLEXER SZENARIEN MIT LÖSUNGEN MEHRERER ANBIETER.

Michael Veit, Security-Experte, Sophos, www.sophos.com

Die Rolle menschlicher Expertise beim Aufspüren, Identifizieren und Beseitigen von Cyberbedrohungen als Ergänzung zu Softwarelösungen hat vor dem Hintergrund hoch professionalisierter Cyberkrimineller und einer gestiegenen Bedrohungslage weltweit noch mehr an Bedeutung hinzugewonnen: Menschliche Bedrohungsjagd durch ausgewiesene Spezialisten ist für die Abwehr der immer komplexer werdenden Cybergefahren essenziell. Forensische Erkenntnisse in der Cybersecurity zeigen, dass eine rein automatisierte Bedrohungsjagd, -abwehr und -prävention den Herausforderungen, die die moderne Cyberkriminalität an die Verteidiger – Softwarelösungen, Strategien und das IT-Sicherheits-Personal – stellen, allein nicht mehr gewachsen ist. Angriffe erfolgen zunehmend anhand einer strategisch geplanten Dramaturgie, die sich die Zeit lässt, ihre Zerstörung ganz in Ruhe zu entfalten: Angreifer führen ihre Attacken oft über Wochen und Monate hinaus durch, und betreiben dabei teilweise manuelle Präzisionsarbeit. Genau das ist der Punkt, an dem automatisierte Sicherheitsmechanismen an ihre Grenzen stoßen. Hier bedarf es erfahrener Expertinnen und Experten, die die Strategien der Cyberkriminellen verstehen, entschlüsseln und abwehren können.

Ein Sicherheitsteam, das diese Disziplin vollständig beherrscht, setzt angemessenes Budget und verfügbare Fachkräfte voraus. Beides ist dieser Tage bekanntlich Mangelware. In einer aktuellen Management-Studie von Sophos nannten Geschäftsleitungen die Verfügbarkeit von qualifiziertem Personal als die größte Herausforderung bei der Umsetzung und Sicherstellung von IT-Sicherheit in ihren Unternehmen. In Deutschland antworteten 62,7 Prozent der Befragten entsprechend, in Österreich gar 69,8 Prozent und in der Schweiz 58,8 Prozent.

Da entsprechende Expertenteams also vor allem in kleineren und mittelständischen Unternehmen intern kaum aufgestellt werden können, wird auch hier ähnlich wie bei Großunternehmen zunehmend auf zusätzliche externe Expertise gesetzt. Der Sophos Management-Studie zufolge trägt die Hauptverantwortung für Cybersicherheit in größeren Unternehmen zu 49,1 Prozent die eigene IT-Abteilung, bei 36,5 Prozent der kleineren Unternehmen sind ebenfalls die eigenen IT-Teams in der Pflicht. Mit 35,8 Prozent bei den größeren sowie 33,1 Prozent bei den kleineren Unternehmen überträgt zudem jeweils ein gutes Drittel aller Unternehmen die Verantwortung für ihre IT-Sicherheit auf externe Dienstleister.

Vertrauen auf externe Expertise

Unternehmen können das Fachwissen ausgewiesener Spezialisten-Teams für Cybersicherheit hinzukaufen. Eine solche Expertise ist aber umso erfolgreicher, wenn die geballte Schlagkraft in ein sinnvolles System eingebunden ist, wie es

zum Beispiel Sophos Adaptive Cybersecurity Ecosystem darstellt. Hier werden intelligente Automatisierung und Vernetzung der Security-Komponenten und die Einbeziehung menschlicher Kompetenz kombiniert, um Angriffen vorzubeugen. Von der Notfallplanung über den präventiven Schutz mit Security-Technologie und Künstlicher Intelligenz bis hin zu menschengeführter Erkennung und Bekämpfung werden in diesem System alle Maßnahmen zentral koordiniert. Das Ökosystem lernt dabei kontinuierlich. Es basiert auf den gesammelten Bedrohungsdaten von forensischen Laboren und Forschungsorganisationen und auf Künstlicher Intelligenz. Für Unternehmen ist der entscheidende Vorteil eines Cybersecurity-Ökosystems, dass innerhalb dieses Ansatzes nicht einzelne Komponenten eingerichtet und verwaltet werden müssen, sondern alles über eine zentrale Oberfläche vergleichsweise leicht intern vom eigenen IT-Team oder vom vertrauten externen Dienstleister administriert werden kann.

Dabei spielt neben technischer Innovation mit Künstlicher Intelligenz oder Anomalie-basierter, automatischer Reaktion die menschliche Expertise eine gewichtige Rolle. Durch Managed Detection and Response-Services (MDR) können raffinierte Angriffe, die den Software-basierten Schutzlösungen entgehen, frühzeitig entdeckt und eliminiert werden.

MDR-Services wie das von Sophos kombinieren technische Security-Lösungen mit einem Expertenteam, das auf Prävention, Früherkennung und Schadensbeseitigung fokussiert ist. Die Spezialisten ergreifen Maßnahmen, um nicht nur die klassischen Cyberbedrohungen, sondern vor allem die immer besser getarnten Schleichfahrten der Kriminellen im Netzwerk zu eliminieren und geben konkrete Ratschläge, um die Ursachen zu bekämpfen.

Und dies neuerdings auch unter Zugriff auf die Telemetriedaten anderer Hersteller: Sophos MDR integriert jetzt auch Telemetrie von Endpoint-, Firewall-, Cloud-, Identitäts-, E-Mail- und anderen Sicherheitslösungen von Drittanbietern in das Sophos Adaptive Cybersecurity Ecosystem.

Die Sophos Expertenteams sind in der Lage, Bedrohungen in einer Vielzahl von Umgebungen zu erkennen und zu beseitigen – einschließlich komplexer Szenarien mit Lösungen mehrerer Anbieter. Und das, bevor weitreichender Schaden angerichtet werden kann, wie etwa das Aktivieren von Ransomware oder umfassende Datenverletzungen. MDR macht in der Praxis oft den Unterschied zwischen Erfolg und Misserfolg der Verteidigung.

Mehr Schlagkraft durch Kompatibilität mit anderen Lösungen

Durch den Einsatz maßgeschneiderter Datenverarbeitungs- und Korrelationstechniken für die breite Palette an Telemetriedaten ist das Sophos MDR-Team in der Lage, das Wer, Was, Wann und Wie eines Angriffs schnell zu verstehen und innerhalb von Minuten auf Bedrohungen im gesamten Ökosystem der Kunden zu reagieren. Das Team kann hierbei auch Telemetriedaten von Drittanbietern nutzen, um Bedrohungen zu verfolgen und Angreifer zu identifizieren, die versuchen sich der Erkennung durch Verschleierungstechniken entziehen.

Sophos MDR ist mit Sicherheitstelemetrie von Anbietern wie Microsoft, Palo Alto Networks, CrowdStrike, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace und vielen anderen kompatibel. Telemetriedaten können automatisch konsolidiert, korreliert und mit Erkenntnissen aus dem Sophos Adaptive Cybersecurity Ecosystem und der Sophos X-Ops Threat Intelligence Unit priorisiert werden.

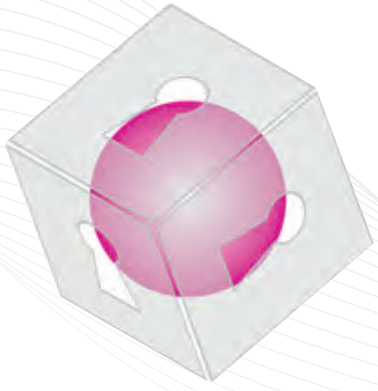
Kunden wählen, welchen Service sie in Anspruch nehmen

Sophos MDR ist mit verschiedenen Servicestufen und Threat-Response-Optionen anpassbar. Kunden können wählen, ob das Sophos-MDR-Team eine umfassende Reaktion auf einen Vorfall durchführen, bei bestätigten Bedrohungen Unterstützung leisten oder detaillierte Alert-Benachrichtigungen liefern soll, die ihre Security Operations Teams selbst verwalten und bearbeiten können.

Michael Veit

IT SECURITY AWARDS 2022

GEWINNER IM RAHMEN DER „IT-SA 2022" AUSGEZEICHNET



Die it-sa war auch in diesem Jahr wieder Plattform für die Verleihung der it security Awards. Die Preisträger in den vier Kategorien Management Security, Web/Internet Security, Cloud Security sowie Identity & Access Management sind VAREDY von arvato, der Radware Bot Manager, Versa Networks sowie Ping Identity.

Management Security

VAREDY

Das Problem: Unternehmen sind von der Menge an Daten überwältigt, die sie von Vulnerability-Scan-Tools erhalten. VAREDY übersetzt diese Daten in Remediation Tasks und bietet klare Lösungen.

Die Lösung: Hier handelt es um ein innovatives Tool für IT Security-Professionals, das dabei hilft, Prozesse im Vulnerability Management zu automatisieren und zu vereinfachen: Dazu verarbeitet das Tool Daten von gängigen Schwachstellen-Scannern (etwa von Tenable oder Rapid7) und vom Asset-Inventar. Es klassifiziert erkannte Schwachstellen, aggregiert und übersetzt diese in kompakte, ausführbare Arbeitspakete und gibt Handlungsempfehlungen, jeweils auf der Basis von Best-Practice-Ansätzen und im Unternehmen bewährter Methoden.

Das Vorgehen für Schwachstellen-Management mit sieht wie folgt aus:

- **Scan:** Ein oder mehrere Schwachstellen-Scanner untersuchen Ihre IT-Infrastruktur im Hinblick auf etwaige Sicherheitslücken. Das Ergebnis sind umfangreiche, aber meist wenig aussagekräftige Schwachstellen-Listen in Form von CVE-Codes.
- **Aufbereitung:** VAREDY importiert die Scan-Daten, analysiert sie nach Ursachen und korreliert sie mit Inventar-Informationen, um nötigen Asset-Kontext herzustellen.
- **Anreicherung:** Das Tool übersetzt die geclusterten Rohdaten in verständliche, kompakte Remediation Tasks und ergänzt Lösungshinweise, basierend auf bewährten Best Practices.
- **Planung:** Anhand dieser kompakten Aufgabenlisten priorisiert, plant und dokumentiert ein Schwachstellen-Manager die Maßnahmen zur Vulnerability Remediation.
- **Remediation:** Für eine effektive Vulnerability Remediation steuert der Schwachstellen-Manager die Umsetzung der Remediation Task direkt aus dem Tool an ein Ticket-System.
- **Verifikation:** Die Software trackt den Fortschritt des Tickets automatisch und validiert auf Basis neuer Scan Daten ob die Schwachstellen erfolgreich behoben wurden.

Fazit: Die automatisierte Übersetzung der Daten zu ausführbaren Arbeitspaketen sorgt für ein einfaches Tracking von Maßnahmen zur Schwachstellen-Behebung im Zeitverlauf und eine auditsichere Dokumentation. Durch den Einsatz der Software reduzieren sich die Kosten für das Schwachstellen Management bis zu 90 Prozent und das Unternehmen ist so in der Lage Schwachstellen schneller zu schließen und Schäden vorzubeugen.

Web/Internet Security

Bot-Manager von Radware

Das Problem: Unternehmen müssen ihre Webanwendungen und ihre Kundendaten vor bösartigen Bots schützen, aber CAPTCHAs als Standardlösung sind bei Endkunden unbeliebt.

Die Lösung: Radware hat einen Bot-Manager entwickelt, der eine Bot-Abwehr ohne CAPTCHAs ermöglicht. Er hilft Unternehmen, bösartige Bot-Aktivitäten zu erkennen, zu klassifizieren und zu verhindern.

Die Software-Lösung stellt umfassenden Schutz von Webanwendungen, mobilen

> AUCH 2022 SEHEN WIR VIELE INNOVATIVE PRODUKTE. ANWENDER SOLLTEN VERSTÄRKT AUF DEN MEHRWERT UND DEN INTEGRATIONSAUFWAND ACHTEN.
>
> Ulrich Parthier, Herausgeber it management und it security, www.it-daily.net

Apps und APIs vor automatisierten Bedrohungen wie Bots bereit. Bot Manager bietet präzises Bot-Management über alle Kanäle hinweg durch die Kombination von Verhaltensmodellierung für granulare Absichtsanalyse, kollektiver Botintelligenz und Fingerprinting von Browsern, Geräten und Maschinen. Er schützt vor allen Formen der Kontoübernahme (Credential Stuffing, Brute Force), Denial of Inventory, DDoS, Werbe- und Zahlungsbetrug und Web Scraping und hilft Organisationen, ihre Online-Aktivitäten zu schützen und auszubauen.

Mit der jüngsten Erweiterung auf Basis von Blockchain-Technologien ermöglicht der Radware Bot Manager Unternehmen mit öffentlichen Websites, vollständig auf CAPTCHAs zu verzichten, um die Benutzerfreundlichkeit ohne Einschränkung der Sicherheit zu optimieren. Zudem schlagen diese KI-Algorithmen zurück, indem sie durch kontinuierliche neue Challenges die Ressourcen des Angriffs-Servers erschöpfen – quasi ein DoS-Angriff auf den Bot-Betreiber als Antwort auf dessen bösartige Intention.

Die Erkennungs- und Eindämmungs-Engine des Radware Bot Manager bietet eine sehr umfassende Lösung zum Schutz von Webanwendungen vor Bot-Bedrohungen. Sie beinhaltet eine tiefgreifende, Intent-basierte Verhaltensanalyse, eingebettete Machine-Learning-Module, die aus dem erhaltenen Feedback lernen und sich weiterentwickeln, Geräte- und Browser-Fingerprinting sowie Anomalie-Erkennung basierend auf der automatischen Identifizierung realer Benutzer-Datenflüsse.

Fazit: Es fallen nur geringe Kosten (keine internen Aufwände) an, es gibt keine Risiken (Tools für Sizing und Funtionstests vorab, „non-intrusive"), und es gibt einen bestmöglichen Schutz durch Intelligenz (KI incl. Crypto-Challenge) bei einem gleichzeitigen Mehr an Benutzerfreundlichkeit.

Cloud Security

Versa Networks

Das Problem: Viele Lösungen benötigen nach wie vor mehrere Software-Stacks, mehrere VNFs, VMs oder separate Boxen, um das gleiche Maß an Funktionalität zu erreichen – was zu verminderter Leistung, mangelnder Sichtbarkeit, Benutzerunfreundlichkeit, höheren Kosten und letztlich einer größeren Angriffsfläche führt.

Die Lösung: Versa SASE integriert Security, Networking, SD-WAN sowie anspruchsvolle Analysen in einem einzigen Software-Betriebssystem, das über die Cloud, on-premises oder als Kombination aus beidem bereitgestellt wird. Versa SASE wurde für den Einsatz in komplexen Umgebungen entwickelt und bietet Flexibilität für einfache, skalierbare und sichere Implementierungen bei gleichzeitiger drastischer Kostenreduzierung. Die Lösung erfüllt die Netzwerk- und Sicherheitsanforderungen aller Arten von Unternehmen.

Das SASE-Sicherheitskonzept, das die Leistungsfähigkeit des WAN mit umfassenden Netzwerksicherheitsfunktionen kombiniert, hat sich gerade für Remote-Arbeitsplätze als praktische Lösung für Unternehmen erwiesen. Es ermöglicht Geschäftskontinuität, indem es konsistente Richtlinien zum Schutz des Zugriffs und zur Optimierung der Leistung weltweit bereitstellt.

Versa SASE stellt integrierte Dienste vor Ort und über die Cloud bereit und verwendet dabei dieselbe Betriebssystemsoftware innerhalb eines Software-Stacks.

Diese Architektur macht Versa SASE skalierbar, leistungsfähig, elastisch, sicher und grenzenlos durchsetzbar in einer Zeit zunehmender Mobilität, Cloud und Remote-Arbeit.

Über die it security Awards 2022 freuen sich: Ulrich Parthier, it verlag GmbH; Pantelis Astenburg, Versa Networks; Mehmet Yaliman und Thomas Schneider, Ping Identity; Michael Geigenscheder, Radware; Alexander Steiner, Arvato Systems (v.l.n.r.)

Versa SASE ist Cloud-nativ, softwarebasiert und hardware-neutral. Die einzigartige Single-Pass-Parallel-Processing-Architektur kombiniert SD-WAN, integrierte Sicherheit, fortschrittliches Routing, Mandantenfähigkeit und Analysen auf eine Art und Weise, dass die Latenzzeit verringert, die Leistung verbessert und Sicherheitsschwachstellen, die bei der Ausführung mehrerer Software-Stacks, Serviceketten oder Appliances entstehen, entschärft werden.

Fazit: Im Gegensatz zu Wettbewerbslösungen wurde Versa SASE von Grund auf so konzipiert, dass den Kunden eine integrierte Lösung innerhalb eines einzigen Software-Stacks zur Verfügung steht. Die Architektur minimiert die Verwaltungs- und IT-Kosten, die mehrere Management-Schnittstellen nach sich ziehen würden, um über 50 Prozent.

Identity & Access Management

Ping Identity

Das Problem: Die Entwicklung, Implementierung und Optimierung der passenden Lösung, die Integration von Identitätsanbietern, Datenbanken und Risikoprovidern nimmt viel Zeit in Anspruch.

Die Lösung: PingOne DaVinci ist eine cloudbasierte Plattform zur schnellen, unkomplizierten und sicheren Orchestrierung von Identitäten – über einzelne Anwendungen, ganze Ökosysteme und Anbieter hinweg.

Der Prozess der „Identitätsorchestrierung' ermöglicht die Entwicklung dynamischer User Journeys auf Basis einheitlicher Identitätsstrukturen. Für gewöhnlich ist dies ein sehr arbeits- und zeitaufwendiges Verfahren, das viel Entwicklungserfahrung voraussetzt. Orchestrierungsplattformen ermöglichen es auch Nicht-Entwicklern, sich ein effektives und effizientes Identitäts- und Zugriffsmanagement (IAM) einzurichten – von der Erstellung, über die Prüfung und Optimierung, bis hin zur Bereitstellung und Pflege.

Mit PingOne DaVinci erhalten Anwender einen besonders flexiblen und adaptiven Rahmen für die Entwicklung und Implementierung ihrer identitätsbasierten User Journeys. Innerhalb kürzester Zeit können automatisierte Workflows für verschiedenste Anwendungsbereiche, die den gesamten Identitätslebenszyklus abdecken, entwickelt werden. Registrierung, Verifizierung der Identität, Authentifizierung, Autorisierung, Risikobewertung, Betrugserkennung, privilegierter Zugriff und vieles mehr werden so erleichtert.

Tiefgehendes Spezialwissen im Entwicklungsbereich ist nicht mehr erforderlich.

Ermöglicht wird dies durch die No Code-Nutzeroberfläche der Plattform. Per einfachem Drag-and-Drop-Verfahren können ansprechende Benutzererlebnisse und Geschäftslogiken entworfen werden. Die Bereitstellung erfolgt über eine einzige API mit einem eingebetteten Widget, mit dem Änderungen in kurzer Zeit entworfen, getestet und veröffentlicht werden können. Mit der Plattform wird das Gestalten digitaler User Journeys über mehrere Anwendungen, Ökosysteme und Anbieter hinweg ermöglicht und erleichtert.

Fazit: Es gibt mehr als 100 vorkonfi-gurierte Integrationen mit Ping-Lösungen und Drittanbietern/No-Code-Workflows dank Drag-and-Drop-Benutzeroberfläche. Die Orchestrierungs-Arbeitslast der IT-Abteilung wird deutlich reduziert. Neu auftretende Kundenbedürfnisse können schneller befriedigt, das Kaufverhalten optimaler analysiert und umgesetzt werden.

Ulrich Parthier

SICHERHEITS-THERAPEUTEN GEFRAGT

EXPERTISE DANK MANAGED SECURITY PROVIDER

Die IT-Sicherheitslage stellt IT-Teams vor wachsende Herausforderungen. Angesichts neuer Bedrohungen rufen Sicherheitsverantwortliche schnell nach neuen Lösungen. Risiken sind jedoch nicht nur ein Problem fehlender Technologien. Der lang befürchtete Fachkräftemangel ist schon lange zur Realität in der Cyberabwehr geworden. Zudem werden Abwehrtechnologien ebenso wie die Angriffe immer komplexer. Viele – oft zu kleine – IT-Teams sind hier schnell überfordert. Ein Managed Detection and Response (MDR)-Service liefert die dringend benötigte Expertise.

Neue Technologien allein sind keine nachhaltige, hinreichende Sicherheit. Sie erfordern aktive Interaktion, da komplexere Angriffe nicht mehr vollautomatisch abgewehrt werden können. Es bedarf nicht nur einer 360°-Rundumsicht auf die gesamte Infrastruktur, sondern auch entsprechender Security-Experten, die diese Informationen bewerten und adäquat handeln können.

GERADE BEI KOMPLEXEREN ANGRIFFEN BRAUCHEN DIE MEISTEN IT-TEAMS EXTERNE UNTERSTÜTZUNG.

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

Mehr Endpunkte, aber nicht mehr Ressourcen

Um beispielsweise nicht verwaltbare IoT-Geräte etwa in der Gebäudesicherheit oder aus der Video- und Telefonkommunikation zu erfassen, bedarf es zusätzlicher Sensoren, die den Netzwerkverkehr analysieren. Auch Cloud Plattformen, Cloud Workloads, Container oder die für den Schutz digitaler Identitäten wichtigen Directories müssen für einen vollständigen Blick mit einbezogen werden. Die technologische Lösung Extended Detection and Response (XDR) bindet eben diese Sensoren mit ein, um eine Abwehr mit Daten aus der erweiterten Angriffsoberfläche zu beliefern. Die Korrelation dieser Daten mittels KI liefert wertvolle Informationen über bevorstehende oder bereits stattfindende Angriffsprozesse. So lassen sich zum Beispiel die Kommunikationswege der Angreifer verfolgen, unterbrechen oder ein ungewünschter Identitäts-Missbrauch erkennen und stoppen. Gerade bei komplexeren Angriffen brauchen die meisten IT-Teams hier aber externe Unterstützung.

Diagnose, Anamnese und Therapie

Jedes IT-Team, aber auch viele Managed Security Provider benötigen meist Hilfe in Form zusätzlicher Experten, da eine Technologie die kundenspezifischen Lücken nicht schließen kann. KI ist sehr wichtig, aber sie erkennt zunächst nur statistische Befunde und kann Gefahren nicht nachhaltig abwehren. Gut ausgebildete Security Spezialisten stehen ebenso wie die nötigen Tools oft nicht zur Verfügung. Daher bedarf es zusätzlicher Ressourcen, die auf nachhaltige Sicherheit schaffen. Sie sind die Sicherheitstherapeuten einer komplexen IT-Abwehr.

Eine solche Expertise können immer häufiger nur die Anbieter von Managed Security Services anbieten. Deren Experten in einem Security Operation Center sind aber mehr als eine schnelle Eingreiftruppe. Als Sicherheitstherapeuten übernehmen sie die Diagnose und Anamnese der Sicherheitslage. Im Baselining definieren sie das Normalverhalten in der zu schützenden Infrastruktur. In der Folge überprüfen und verstehen Experten die von einer Künstlichen Intelligenz nach Korrelation der Endpunktinformationen erzeugten Alarme. Proaktives Threat Hunting ermöglicht unter anderem die Berücksichtigung geographischer oder branchenspezifischer Auffälligkeiten und kann damit frühzeitig die richtigen Weichen in der Abwehr stellen. Die für ein aktives Blocken der Angriffe notwendigen Prozesse legen die externen Experten zuvor mit dem Unternehmen fest. Sobald der Schaden eingedämmt ist, optimieren sie die IT-Strategie des Kunden für eine zukunftssichere Verteidigung.

Jörg von der Heydt

ARMIS ASSET VULNERABILITY MANAGEMENT (AVM)

FÜR UMFASSENDES CYBER RISK MANAGEMENT

Die beiden größten Probleme bei der Behebung von Schwachstellen liegen in der Priorisierung und den Ressourcen. Jedes Team hat zu wenig Fachpersonal, und gleichzeitig zu viele Schwachstellen. Teams müssen in der Lage sein, bei der Behebung von Schwachstellen klug zu priorisieren, damit sie ihre begrenzte Zeit effizient nutzen. Asset Intelligence und Asset Context spielen dabei eine zentrale Rolle.

Bei Angriffen auf ungesicherte Geräte kann es sich beispielsweise um einen Angreifer von außen handeln, der Geräte oder Maschinen remote steuert. Bei einer Risikobewertung würde diese Bedrohung als kritisch bewertet. Je nach Angriffsart ist die Risikobewertung unterschiedlich – letztlich geht es jedoch nicht nur um die CVEs, also die Schwachstellen an sich. Vielmehr im Fokus stehen sollten die Bedingungen der Umgebung, unter denen CVEs ausgenutzt werden können.

Zu jedem Asset existiert eine Reihe an Informationsebenen – und in je mehr dieser Ebenen ein Unternehmen Einblick hat, desto besser können der Sicherheitsstatus und das Risiko des Assets analysiert werden. Sicherheitsverantwortliche müssen zudem wissen, wie Assets untereinander kommunizieren. Mit jeder Information, die über ein Asset im Unternehmensnetzwerk vorliegt, steigt die Sicherheit des Unternehmens.

Mit jeder zusätzlichen Information verbessern sich zudem auch die Workflows.

Viele Unternehmen setzen hierbei noch immer auf manuelle Prozesse und haben damit keine gute Quelle für Informationen über ihre Assets – denn werden Geräte etwa in Excel-Listen verwaltet, dann ist es schier unmöglich, diese Listen stets vollständig und auf dem neuesten Stand zu halten.

Die Lösung: Asset Vulnerability Management von Armis

Armis ist der führende Anbieter einer einheitlichen Plattform für Asset Visibility und Sicherheit. Das Unternehmen bietet mit Armis Asset Vulnerability Management (AVM) die einzige Lösung für risikobasiertes Schwachstellenmanagement, die es Unternehmen ermöglicht, Maßnahmen zur Schadensbegrenzung über die gesamte Angriffsfläche von Assets zu priorisieren. Darunter fallen IT, OT, ICS, IoMT, IIoT, Cloud und Mobilfunk-IoT, verwaltet oder nicht verwaltet.

www.armis.com

ARMIS AVM BIETET:

- Eine vollständige, genaue Übersicht über alle Assets und Schwachstellen in der Umgebung, einschließlich verwalteter und nicht verwalteter Assets
- Risikobasierte Priorisierung auf der Grundlage der Kritikalität der Assets und der Schwere der Schwachstellen, um sich auf das Wesentliche zu konzentrieren
- Sicherheitsautomatisierung und -orchestrierung zur Verringerung der Mean Time to Remediation (MTTR)
- Einen vollständigen Lebenszyklus für das Schwachstellenmanagement zur Verfolgung von Maßnahmen zur Schadensbegrenzung im Laufe der Zeit mit sofort einsatzbereiten Berichten und Dashboards

Auch kostengünstige Maßnahmen steigern die Cybersicherheit in kleinen und mittleren Unternehmen effektiv.

MEHR CYBERSICHERHEIT FÜR DAS KLEINE BUDGET

SO SCHÜTZEN SICH MITTELSTÄNDISCHE UNTERNEHMEN VOR CYBERANGRIFFEN

Verantwortliche in kleinen und mittelständischen Unternehmen (KMU) denken oft, dass sie aufgrund ihrer Größe kein lohnendes Ziel für Cyberkriminelle darstellen. Aktuelle Zahlen zeigen jedoch, dass Cyberattacken vor KMU nicht halt machen. Laut der aktuellen Cyberresilienz-Studie von Kaspersky erlebte über ein Viertel (29 Prozent) der befragten Unternehmen in Deutschland zwischen 100 und 500 Mitarbeitern bereits einen Cybervorfall. Die gute Nachricht: Mit einigen einfach umzusetzenden Maßnahmen können KMU ihre Angriffsfläche für Cyberangriffe verkleinern, ohne ihr Budget über Gebühr zu belasten.

Verwenden Sie starke Passwörter

Bei Brut Force-Angriffen versuchen Angreifer Zugang zu digitalen Ressourcen zu erhalten, indem sie viele Passwörter oder Passphrasen testen und hoffen, dass sie dabei zufälligerweise auf die richtige Kombination stoßen. Führen Sie daher eine strenge Passwortpolitik ein, um zu vermeiden, dass Passwörter durch bloßes Ausprobieren geknackt werden. Starke Passwörter bestehen aus mindestens acht Buchstaben, einer Zahl, Groß- und Kleinbuchstaben sowie mindestens einem Sonderzeichen. Mit dem Password Checker von Kaspersky (**password.kaspersky.com**) können Sie ausprobieren, wie lange es dauern würde, ein Passwort zu hacken. Nur eine Runde um den Block oder viermal zum Mond und wieder zurück?

Wenn auch nur der geringste Verdacht besteht, dass ein Passwort geknackt wurde, sollte es sofort geändert werden. Eine Sicherheitslösung mit einem integrierten Password Manager erleichtert es, ein eigenes Passwort für jedes Tool zu verwenden und dabei starke maschinell generierte Passwörter statt leicht zu erratender Eselsbrücken zu nutzen.

Halten Sie Ihre Software up-to-date

Lassen Sie Cyberkriminelle keinen Profit aus Schwachstellen ziehen. Häufig nutzen Angreifer offensichtliche IT-Sicherheitslücken aus. Die aktuelle Studie von Kaspersky ergab, dass 54 Prozent der Cybervorfälle in den befragten KMU weltweit über eine bereits veröffentlichte Schwachstelle in allgemein zugänglichen Anwendungen wie Microsoft Exchange erfolgten. Somit hätte mehr als die Hälfte der Attacken durch ein einfaches Update verhindert werden können. Deshalb gilt: Schieben Sie Software-Updates nicht auf die lange Bank. Aktualisieren Sie Ihr Betriebssystem, Ihre Antiviren-Software, Browser, Treiber und sämtliche Programme, mit denen Sie arbeiten, sobald ein neues Update verfügbar ist. Denn häufig bieten diese nicht nur neue Funktionen oder eine optimierte Nutzerfreundlichkeit, sondern beheben auch potentielle Sicherheitsprobleme.

Sichern Sie Ihre Daten

Ransomware Attacken sind auf dem Vormarsch. Dabei verschlüsseln Angreifer Unternehmensdaten und erpressen Lösegeld. Fast täglich macht ein derartiger Vorfall Schlagzeilen. Erstellen Sie regelmäßig Sicherungskopien der wichtigsten digitalen Informationen in einem Cloud-Service und auf einer alternativen Hardware. So haben Sie auch dann noch eine Kopie zur Verfügung, wenn Ransomware Ihre Daten verschlüsselt. Außerdem sollten Sie die Initiative NO MORE RANSOM kennen. Diese bietet weitere wichtige Tipps und kostenfreie Entschlüsselungstools als letzten Ausweg im Notfall: **nomoreransom.org/de**

Schärfen Sie das Cybersicherheitsbewusstsein

Ob direkt oder indirekt: Weitaus die meisten Cybervorfälle gehen auf menschliche Fehler zurück. Treffen Sie deshalb Vorsorge, dass Mitarbeiter Software nicht selbst installieren können. Die Verwendung von Standardkonten ohne Administratorrechte verhindert, dass Mitarbeiter versehentlich einen Trojaner installieren, der sich als Produktivitätssoftware ausgibt.

Ergreifen Sie außerdem Maßnahmen, das Cybersicherheitsbewusstsein Ihrer Mitarbeiter zu schärfen. Regelmäßige Trainings, die einfach in den Arbeitsalltag integriert werden können – zum Beispiel mittels einer interaktiven Online-Plattform – geben dem Team Gelegenheit, typische Gefahren kennenzulernen und das richtige Verhalten einzuüben. Im Rahmen der Kaspersky Automated Security Awareness Platform können Sie derzeit kostenfrei an einem Online-Kurs rund um den sicheren Umgang mit sozialen Medien und Social Engineering teilnehmen. Sie erreichen diesen unter dem Shortlink: **kas.pr/asap-some**.

Bleiben Sie wachsam

Behalten Sie die Energieeffizienz Ihrer Geräte im Blick. Wenn ein Gerät langsamer wird, überhitzt oder im ungenutzten Zustand viel Lärm macht, könnte das an einer Mining-Malware liegen. Verwenden Sie deshalb eine Sicherheitslösung, die nicht nur Schadprogramme, sondern auch potentiell unerwünschte Installationen erkennt.

Verfolgen Sie die für Ihre Branche relevanten Nachrichten zum Thema Cybersicherheit. So halten Sie sich auf dem Laufenden, auf welche potenziellen Angriffe Ihr Unternehmen gefasst sein sollte. Dieses Hintergrundwissen hilft auch einzuschätzen, ob Ihre Sicherheitslösung ausreichend Schutz bietet. Sie können auch kostenlose Programme verwenden, allerdings ist der Funktionsumfang in der Regel geringer als bei bezahlter Software. Achten Sie bei der Wahl Ihrer Lösung auf Ergebnisse unabhängiger Tests und downloaden Sie die Software stets direkt von der Website des Entwicklers. Da die Zahl erpresserischer Angriffe per Ransomware rasant steigt, sollten Sie bei der Wahl einer Antiviren-Lösung darauf achten, dass diese zu 100 Prozent vor Ransomware schützt, wie beispielsweise Kaspersky Endpoint Security for Business und Kaspersky Small Office Security.

Gut gewappnet mit dem IT-Notfallplan

Ein Cybervorfall ist eine stressige Situation. Klären Sie folgende Fragen im Vorfeld, damit Sie für den Ernstfall vorbereitet sind und schnell reagieren können:

1. Was sind meine geschäftskritischen Daten?

Sorgen Sie für einen ausreichenden Schutz dieser Daten und erstellen Sie regelmäßig Sicherungskopien.

2. Wen muss ich bei einem Zwischenfall schnell erreichen?

Erstellen Sie eine Liste mit den wichtigsten Kontakten, zum Beispiel Partner, Zulieferer, Banken, IT-Anbieter und Incident Response-Services.

3. Was sind Alarmzeichen für einen Cybervorfall?

Zu den möglichen Anzeichen für einen Cybervorfall zählt etwa, dass Computer langsam laufen, häufig abstürzen oder sich sonst ungewöhnlich verhalten. Spätestens, wenn Benutzer nicht mehr auf Konten oder Dokumente zugreifen können oder Nachrichten mit Lösegeldforderungen eingehen, sollten alle Alarmglocken schrillen.

4. Wie bereite ich mich für den Ernstfall vor?

Führen Sie regelmäßig interne Notfallübungen durch. Schalten Sie etwa testweise IT-Systeme ab und versuchen Sie Daten aus Backups wiederherzustellen.

Sorgen Sie dafür, dass Informationen zu Aktionsplänen und zur Kommunikation im Notfall offline verfügbar sind.

Bereiten Sie ein System vor, über das Schlüsselpersonen sofort und sicher kommunizieren können, zum Beispiel einen vom Hauptsystem unabhängigen Messenger-Dienst.

Erstellen Sie Muster für die Krisenkommunikation zur sofortigen Freigabe.

www.kaspersky.de

GOOD TO KNOW

Die neue Cyberresilienz-Studie von Kaspersky mit vielen Tipps, wie KMU ihre Widerstandsfähigkeit gegen Cyberangriffe steigern können, gibt es hier kostenfrei zum Download: **kas.pr/cyberresilienz**

Weitere praktische Handlungsempfehlungen zum Unternehmensschutz ohne zusätzliche Kosten bietet „Kaspersky Cybersecurity on a Budget Hub“: **www.kaspersky.com/blog/budget-cybersecurity**

SCHATTEN-IT

VERBORGENE GEFAHREN IM IT-NETZWERK

Das macmon secure Support Team registriert eine wachsende Zahl an Schatten-IT-Vorfällen. Netzwerkzugangskontrolle ist ein zentraler Baustein für deren Abwehr.

Neben der offiziellen IT-Infrastruktur existiert in Unternehmen der Austausch von unternehmenskritischen Daten ohne das Wissen der IT-Abteilung. Dazu gehört beispielsweise die Verwendung von IT-Services, die von Dienstleistern außerhalb des Unternehmens angeboten werden, wie Webmail-Services oder komplexe Angebote wie Software-as-a-Service oder Cloud Services. Eine starke Zunahme verzeichnet die Einbindung privater Smartphones und Tablet-PCs inklusive der entsprechenden Apps in die Unternehmensnetzwerke, aufgrund von Home-Office-Regelungen.

Diese sogenannten Schatten-IT-Instanzen sind weder technisch noch strategisch in das IT-Service-Management eingebunden, und können nicht kontrolliert werden. In einer Marktstudie aus dem Jahr 2020 schätzten 53 Prozent der IT-Verantwortlichen, dass über die Hälfte der Mitarbeiter Anwendungen ohne das Wissen der IT-Abteilung auf Firmengeräten oder Privatgeräten nutzen. Die unkalkulierbare Gefahr, die sich durch die Schatten-IT ergibt, kann zu signifikanten Schäden wie Datenverlusten, Compliance-Verstößen oder Malware-Intrusion führen.

Komplexe Herausforderung für die Netzwerksicherheit

Folgende Schritte sind notwendig, um Sicherheitsziele zu erreichen, und unbekannte und unerwünschte IT-Prozesse zu bekämpfen.

1. Übersicht

Ein vollständiger Überblick über die angeschlossenen Geräte im Netzwerk ist der erste Schritt zur Netzwerksicherheit. Das bedeutet, dass Administratoren eine Übersicht über alle Geräte und Benutzer im Netzwerk benötigen und diese ständig überwacht, identifiziert und aktualisiert wird.

2. Kontrolle

Im nächsten Schritt sollte eine effektive Zugangskontrolle mit einem einheitlichen und automatischen Regelwerk implementiert werden. Mit diesem Tool werden im Netzwerk nur Geräte zugelassen, die die Erlaubnis der IT-Abteilung haben, ihre Berechtigung nachweisen können, oder erst verifiziert werden müssen. Dabei sollte es möglich sein, auf die Herausforderungen wie dezentrale Organisationsformen, Fusionen und Übernahmen, den Mangel an Fachpersonal und stagnierende IT-Budgets zu reagieren.

3. Compliance

Mit der Compliance ist es möglich, den Zugriff basierend auf dem Sicherheitsstatus der Endgeräte zu kontrollieren (auch nach erfolgreicher Authentifizierung im Netzwerk). Die zunehmende Vielfalt der Bedrohungen und unterschiedlichste Sicherheits-Lösungen und Ansätze führen zur anwachsenden Komplexität bei der Bekämpfung der Risiken.

macmon secure verfügt über eine breite Palette von Lösungen zur Bewältigung der beschriebenen Risiken. Dazu gehört die Erlangung des notwendigen Überblicks über alle Geräte im Unternehmen ebenso, wie die aktive Kontrolle des Zugriffs auf das Netzwerk und die Überprüfung von Compliance-Richtlinien, einschließlich der richtigen Integrationen und Schnittstellen. Das wird durch vielfältige Technologie-Partnerschaften mit führenden IT-Sicherheits-Anbietern realisiert.

Fazit

Schatten-IT wird man im Unternehmen nie komplett verhindern können, aber durch den Einsatz von macmon NAC in Kombination mit weiteren IT-Security-Lösungen ist ein Maximum an Sicherheit zu erzielen. Gleichzeitig sollten Mitarbeiter kontinuierlich auf die Gefahren von Schatten-IT aufmerksam gemacht werden.

Sabine Kuch | www.macmon.com

ÜBERSICHT STATT UNORDNUNG

GEFAHREN FÜR DIE IT-SICHERHEIT BEI FUSIONEN BEWÄLTIGEN

Jede Fusion steht vor der großen Herausforderung, zwei zum Teil völlig verschiedene Betriebe in eine einheitliche Organisationsstruktur überführen zu müssen. Vor allem wenn es ans Getriebe geht – sprich an die zugrundeliegende IT-Infrastruktur – sehen sich die M&A Manager mit einer oftmals undurchsichtigen Situation konfrontiert.

Unterschiedliche Prozesse, verschiedene IT-Lösungen und unzählige neue Endgeräte. Jeder, der schon einmal in seinem Berufsleben eine Fusion mitgemacht hat, kennt das Problem: Die gewohnten Routinen müssen den Abläufen in der neuen Firma weichen. Das E-Mail-System ist ein anderes, die genutzten Dienste und Tools folgen einer völlig anderen Logik und greifen auf ungewohnte Datenbanken zu. Viele On Prem-Prozesse sind beim neuen Arbeitgeber in die Cloud gewandert, statt lokal gespeicherter Dokumente wird vom neuen Arbeitgeber die Nutzung von online Workspaces verlangt.

BEI DER VERSCHMELZUNG ZWEIER UNTERNEHMEN KANN SICH DAS RISIKO EINER SICHERHEITSLÜCKE DURCH KOMPROMITTIERTE ENDGERÄTE DRAMATISCH ERHÖHEN.

Zac Warren, Chief Security Advisor EMEA, Tanium, www.tanium.de

Vor allem der Zustrom unzähliger, teils nicht registrierter Endgeräte stellt eine große Gefahr für die IT-Sicherheit der Fusionspartner dar. PCs, Laptops, Smartphones, Tablets und eine Vielzahl internetfähiger IoT-Geräte verbinden sich jeden Tag mit dem Firmennetz und greifen auf unternehmenskritische Daten zu. In einem solch diversen Umfeld ist es für IT-Sicherheitsverantwortliche nicht immer leicht, die Übersicht zu behalten. Bei der Verschmelzung zweier Unternehmen kann sich das Risiko einer Sicherheitslücke durch kompromittierte Endgeräte dramatisch erhöhen.

Eine Fusion sollte jedoch als Chance gesehen werden, die IT-Sicherheit auf ein neues Level zu heben, Systeme zu modernisieren und Dienste zu konsolidieren.

Die häufigsten Fehler bei Fusionen

Fehlende Sichtbarkeit im Firmennetz: Cyberattacken erfolgen meist über schlecht überwachte oder unsichtbare Teile des Unternehmensnetzwerks. Dazu gehören vor allem unregistrierte Endgeräte. Angreifer konzentrieren sich immer auf das schwächste Glied in der Kette. So ist es für sie ein leichtes, diese Schwachstellen auszunutzen, um weitreichende Zugriffsrechte für laterale Bewegungen im Firmennetz zu erlangen, Firmengeheimnisse zu erbeuten, Ransomware ins System einzuschleusen und großen Schaden beim Opfer anzurichten.

Lösung: Bereits vor der Zusammenlegung der Firmen-IT sollte eine Sicherheitsplattform eingerichtet werden, die in der Lage ist, alle Endgeräte im Netzwerk zu identifizieren.

Zentralisierte Patchverwaltung: Eine der größten Schwachstellen in der klassischen IT-Sicherheit ist die zentrale und starr getaktete Verwaltung von Patches. Wer lediglich am „Patch Tuesday" die Softwareupdates aller Firmenrechner über einen zentralen Server abwickelt, erzeugt nicht nur Datenstaus, sondern läuft auch Gefahr, Zero Day Schwachstellen eine Woche lang mitzuschleppen.
Lösung: Eine agentenbasierte Update- und Sicherheitslösung entlastet die Leitungen und sorgt für einen Echtzeit-Überblick aller Endgeräte und deren Patchstatus.

Isoliertes und inkompatibles Risikomanagement: Wenn heterogene Systeme konsolidiert werden, kommt es häufig zu Kompatibilitätsproblemen. Viele Sicherheitslösungen sind auf einzelne Plattformen zugeschnitten und können nicht auf andere Systeme skaliert werden. Bei Fusionen werden alte Prozesse häufig parallel weitergeführt und erzeugen dadurch blinde Flecken in der IT-Sicherheit.

Lösung: Ein konvergierte IT-Sicherheitsstrategie ist so konzipiert, dass sie maximale Kompatibilität über verschiedene Plattformen hinweg bietet. Auf diese Weise können schwer zu ersetzende Prozesse weitergeführt werden, ohne die IT-Sicherheit zu kompromittieren.

Fazit

Die zentrale Frage bei Übernahmen ist, ob man die IT-Infrastruktur des erworbenen Unternehmens beibehalten will oder nicht. Diese Entscheidung sollte auf Basis einer lückenlosen Bestandsaufnahme durch dedizierte Lösungen erfolgen.

Zac Warren

PHISHING- UND RANSOMWARE-ANGRIFFE VERMEIDEN

E-MAILS VERSENDEN OHNE RISIKO

Wie viele E-Mails haben Sie heute schon verschickt oder empfangen? Wahrscheinlich eine ganze Menge. Das sind auch eine ganze Menge Gründe für Hacker, sich an den Informationen zu bedienen, um daraus Strategien für Cyberattacken zu entwickeln. Umso wichtiger ist es, dass Unternehmen Maßnahmen ergreifen, um die Kommunikation zu schützen. Mit professionellen Secure E-Mail-Lösungen lassen sich der interne und der externe Mailverkehr maximal absichern.

Cyberangriffe wie Ransomware-, Phishing- oder Spear-Phishing-Attacken auf Unternehmen sind mittlerweile eine tägliche Erscheinung geworden. Dabei werden die Tricks von Cyberkriminellen immer professioneller: Mit trügerisch echt aussehenden Mails versuchen sie – beispielsweise im Namen einer Bank –, an wichtige Daten zu gelangen. Einmal an diese Informationen gekommen, können die Hacker damit großen Schaden anrichten. So wird etwa bei Ransomware-Attacken eine Schadsoftware verschickt, die sich automatisch im Unternehmensnetzwerk verbreitet und in der Lage ist, komplette Systeme lahmzulegen. Nicht zuletzt aus diesen Gründen ist ein signierter und für sensible Daten verschlüsselter, DSGVO-konformer E-Mail-Verkehr essenziell. Denn Schäden, die durch diese kriminellen Angriffe entstehen, sind häufig kostenintensiv und rufschädigend.

ANDERS ALS VON VIELEN ANGENOMMEN, IST DIE EINRICHTUNG EINER E-MAIL-VERSCHLÜSSELUNG EINFACH UMSETZBAR UND MIT WENIG AUFWAND SOWIE KOSTEN VERBUNDEN.

Günter Esch, Geschäftsführer SEPPmail, Deutschland GmbH, www.seppmail.com

E-Mails schützen ist nicht schwer!
Anders als von vielen angenommen, ist die Einrichtung einer E-Mail-Verschlüsselung einfach umsetzbar und mit wenig Aufwand sowie Kosten verbunden. Mit Technologien wie S/MIME- oder openPGP-Verschlüsselung lässt sich gewährleisten, dass Daten auf dem Weg vom Absender bis zum Empfänger zu keinem Zeitpunkt unverschlüsselt sind und durch Dritte mitgelesen werden können.

Eine ganzheitliche Secure E-Mail-Lösung sollte nicht nur einfach sein – auch ein rollenbasiertes Rechtesystem ist sinnvoll. Damit lässt sich beispielsweise einstellen, dass Admins Vollzugriff haben, während weiteren Rollen entsprechend andere Rechte zugewiesen werden.

Wichtig ist aber auch, dass die Lösung im Hintergrund läuft und die Mitarbeiter nicht im Arbeitsalltag behindert. Ein zentrales Management hilft dabei, openPGP

Public Keys sowie S/MiME-Zertifikate zu verwalten. Mit der Bereitstellung eines Outlook Add-In lässt sich die Lösung außerdem einfach in den Arbeitsalltag integrieren.

Digitale Signatur

Zusätzlich zur E-Mail-Verschlüsselung eignet sich eine E-Mail-Signatur. Um eine solche Signatur zu erhalten, wird ein validiertes Zertifikat benötigt, das bei einer akkreditierten Zertifizierungsstelle beantragt werden muss. Moderne Signaturlösungen vereinfachen den damit verbundenen administrativen Aufwand deutlich: Wenn ein Nutzer die erste E-Mail versendet, beantragt die Appliance über eine Managed Public Key Infrastructure (MPKI) automatisch die benötigten Zertifikate bei einer der sogenannten Certificate Authorities (CAs). Die CAs bestätigen dann, dass das Zertifikat zu einer bestimmten E-Mail-Adresse gehört. Ist dieser Vorgang abgeschlossen, kann sich der E-Mail-Empfänger über die Identität des Absenders sicher sein. Damit schafft eine professionelle elektronische Signatur Integrität und Authentizität.

E-Mails „mal eben" versenden

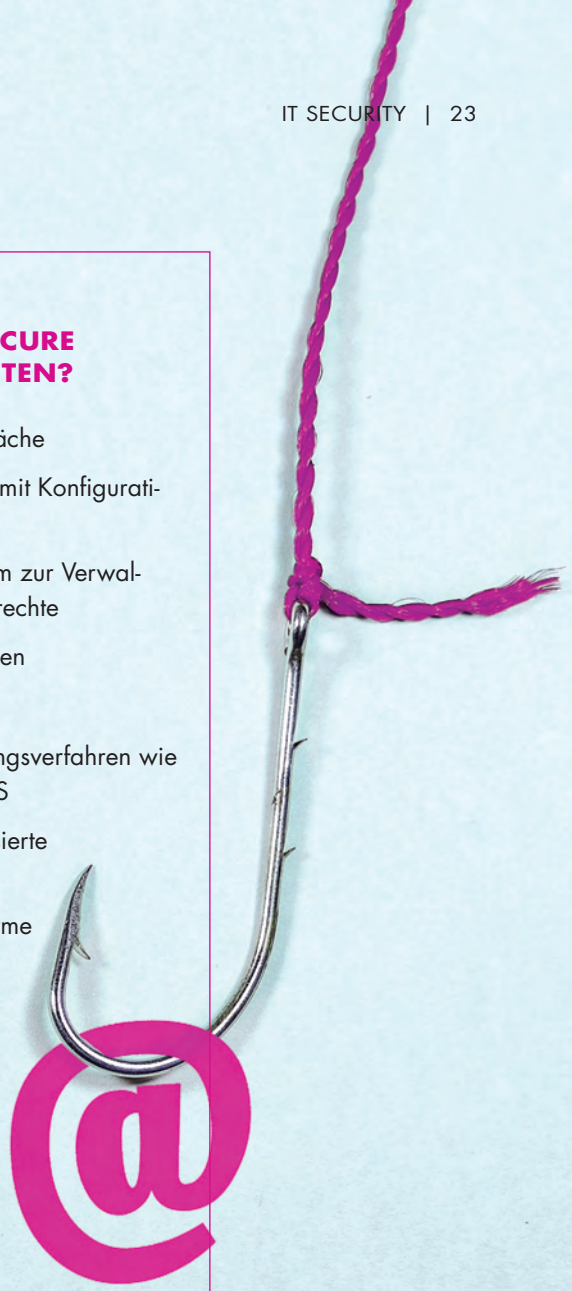
Nicht jedes Unternehmen verfügt über eine eigene Verschlüsselungslösung oder besitzt eigenes Schlüsselmaterial. Viele denken immer noch, dass eine entsprechende Lösung zu umständlich ist und ein gewisses Know-how erfordert. Dies ist aber nicht der Fall – eine professionelle Lösung liefert auch gleich eine nutzerfreundliche, einfache Spontanverschlüsselung mit. Bei dieser Methode werden E-Mails inklusive Anhängen verschlüsselt und mit einer Trägermail ausgeliefert. Die Empfänger können anschließend nach Eingabe eines Passwortes die Mails ganz einfach öffnen und ebenfalls verschlüsselt antworten. Die Bedienung der modernen Lösungen erfolgt intuitiv.

Auf Wolke sicher

Natürlich gibt es nicht nur On-Premises-Lösungen, die Security-Features bieten. Auch professionelle Cloud-Lösungen enthalten, neben einer hochprofessionellen E-Filter-Lösung für Anti Spam, Anti Virus und Anti Malware, auch Funktionen für E-Mail-Verschlüsselung, automatisches Zertifikatsmanagement und digitale Signaturen. Bekannte Verschlüsselungstechnologien wie Spontanverschlüsselungen, S/MIME oder OpenPGP sind ebenfalls vorhanden. Das Zugreifen auf Cloud-Lösungen hat häufig einen ganz simplen Grund: Die Cloud zeichnet sich durch ihre Einfachheit und ihren Komfort aus. Eine gehostete Lösung hat nicht nur den Vorteil, dass eine Installation vor Ort wegfällt, sie spart oft auch Kosten ein. Zudem wird die Cloud-Lösung in hochverfügbaren Rechenzentren betrieben, bei denen es mit hoher Wahrscheinlichkeit nicht mehr zu Ausfällen oder Verzögerungen beim E-Mail-Verkehr kommt.

WAS SOLLTE EINE PROFESSIONELLE SECURE E-MAIL-LÖSUNG BIETEN?

- ✓ Benutzerfreundliche Oberfläche
- ✓ Übersichtliches Dashboard mit Konfigurationsmöglichkeiten
- ✓ Rollenbasiertes Rechtesystem zur Verwaltung verschiedener Zugriffsrechte
- ✓ Erstellung digitaler Signaturen
- ✓ Spontanverschlüsselung
- ✓ Verschiedene Verschlüsselungsverfahren wie S/MIME, OpenPGP und TLS
- ✓ Verfügbarkeit als Cloud-basierte Lösung
- ✓ Sichere und DSGVO-konforme Kommunikation
- ✓ Verfügbarkeit als Outlook Add-In
- ✓ Kompatibilität mit anderen Technologien und Anbietern
- ✓ Zusammenfassung aller Sicherheitsfunktionen als All-in-one-Lösung



E-Mail-Sicherheit kompakt

E-Mail-Sicherheit spielt in Unternehmen nach wie vor eine große und wichtige Rolle. Um die E-Mail-Kommunikation sicher zu gestalten, gibt es verschiedene Möglichkeiten. Eine moderne All-in-one-Lösung, die sowohl digitale Signaturen als auch E-Mail-Verschlüsselung beinhaltet, ist eine gute Möglichkeit, die Sicherheit in jedem Unternehmen zu optimieren und Cyberattacken zu verhindern. Die durchzuführenden Maßnahmen sind dabei einfach umsetzbar und mit wenig Aufwand sowie Kosten verbunden.

Günter Esch

VERTRAULICHE MEETINGS ABSICHERN

MEETING MANAGEMENT SOFTWARE ALS MITTEL DER WAHL

Bei Sitzungen in der Führungsebene werden in der Regel strategisch und operativ wichtige Entscheidungen getroffen oder vorbereitet. Unabhängig davon, ob die Geschäftsführung, die Amtsleitung oder der Vorstand einer Organisation wichtige Meetings vor Ort im persönlichen Kreis oder als Online – beziehungsweise Hybridkonferenz abhält: Es kommt dabei im Vorfeld, während und im Nachgang der Sitzung fast immer zum Austausch von vertraulichen oder gar streng geheimen Informationen. Gelangen hier Daten frühzeitig nach außen, können Markt- und Wettbewerbsvorteile sowie die Rechtssicherheit des Unternehmens bedroht sein. Auch Behörden müssen empfindliche Konsequenzen fürchten, wenn vertrauliche Informationen nach außen gelangen. Aus diesem Grund sollte das Topmanagement mit allen involvierten Akteuren eine Lösung verwenden, die sich für vertrauliche und hochsensible Informationen eignet.

Alles sollte den Compliance-Richtlinien entsprechen und gut abgesichert sein. Einige Meeting-Management-Lösungen sind genau darauf ausgelegt und lassen sich reibungslos in die vorhandene Kommunikationsumgebung einfügen.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 15 Seiten und steht kostenlos zum Download bereit.

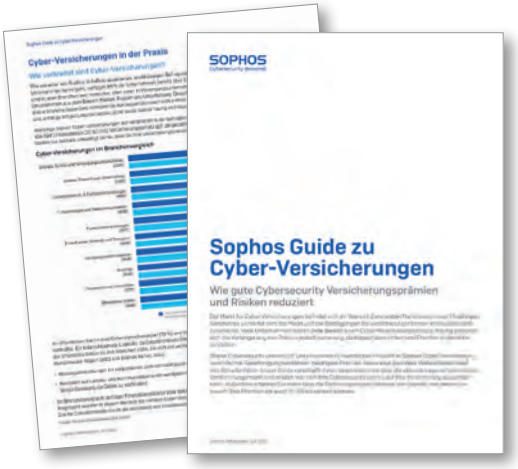
www.it-daily.net/Download

GUIDE ZU CYBER-VERSICHERUNGEN

WIE GUTE CYBERSECURITY VERSICHERUNGS-PRÄMIEN 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.

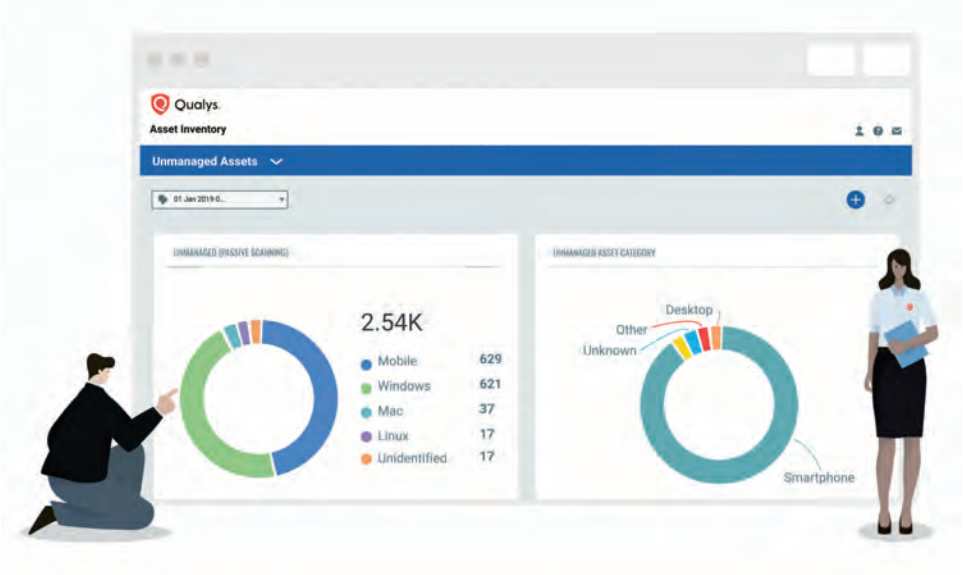
Der Guide verschafft Ihnen einen Überblick über die aktuelle Lage auf dem Cyber-Versicherungsmarkt und erklärt, wie sich Ihre Cybersecurity positiv auf Ihre Versicherung auswirken kann. Außerdem erfahren Sie mehr über die Technologien und Services von Sophos, mit denen Sie sowohl Ihre Prämien als auch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



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 10 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/Download



ZERO-DAY-BEDROHUNGEN

SO ERLEICHTERT QUALYS POLICY COMPLIANCE DIE BEKÄMPFUNG

Qualys Policy Compliance ist eine moderne Lösung, die es ermöglicht, Cyberrisiken laufend zu verringern und interne Richtlinien, Branchenanforderungen und gesetzliche Bestimmungen effektiv einzuhalten. Die Lösung unterstützt Unternehmen jeder Größe bei der Reaktion auf Zero-Day-Bedrohungen.

Risikominderung durch kompensierende Kontrollen

Qualys Policy Compliance (PC) verfügt über eine umfangreiche Bibliothek von Sicherheitskontrollen, um verschiedene Zero-Day-Lücken in unterschiedlichen Technologien und Plattformen abzugleichen. Qualys veröffentlicht kontinuierlich weitere kompensierende Kontrollen für neue Zero-Day-Lücken und beginnt mit der Entwicklung neuer Kontrollen, sobald eine Schwachstelle bekannt wird, für welche noch kein Patch verfügbar ist. Zwar kann sich kein Unternehmen vollständig vor einem Zero-Day-Angriff schützen. Jedoch können Unternehmen neue Zero-Day-Schwachstellen ermitteln und mithilfe dieser Kontrollen von Qualys PC die damit verbundenen Risiken mindern.

Ermittlung kompensierender Kontrollen

Auf der neuen Benutzeroberfläche von der Lösung können Anwender die Konformität mit diesen Kontrollen überprüfen, indem sie sich einfach die CVE ID/ eindeutige Kennung für die Sicherheitslücke ansehen. Wie nachfolgend dargestellt, können sie mit dem QQL-Token control.vulnerability.cveId: leicht nach der CVE suchen und dann ein Dashboard mit den Ergebnissen erzeugen.

Vorteile im Kampf gegen ero-Day-Bedrohungen

Der Hauptvorteil, den Qualys Policy Compliance bietet, ist „Defense in Depth". Unternehmen können ihre Sicherheitsarchitektur verbessern, indem sie Fehlkonfigurationen analysieren und beheben, und dann leicht Patches implementieren, sobald diese verfügbar sind, um das Cyberrisiko des Unternehmens insgesamt zu verringern.

Die anfängliche Analyse gibt den Cybersicherheitsteams Aufschluss darüber, wie es aktuell um ihre Sicherheit bestellt ist. Sie ist eine wichtige Voraussetzung dafür, das Risiko durch Zero-Day-Lücken zu mindern, solange die IT-Umgebung anfällig ist und der Hersteller noch keinen Patch veröffentlicht hat. Unternehmen können jedoch eine weitere Sicherheitsschicht hinzufügen, indem sie mithilfe der Kontrollen von Qualys PC Fehlkonfigurationen ermitteln und entschärfen.

Ausführung von Workarounds

Mit Qualys Custom Assessment and Remediation können Sicherheitsexperten benutzerdefinierte Skripte und Kontrollen schnell erstellen und ausführen und dann unverzüglich handeln, um die bestehenden Probleme direkt zu beheben und Abhilfemaßnahmen anzuwenden. Über Qualys PC können sie die Maßnahmen umsetzen, indem sie ein PowerShell-Skript erstellen und es auf den anfälligen Assets ausführen.

Fazit

Qualys Policy Compliance ist nicht nur führend bei der Bereitstellung von Sicherheitsempfehlungen, die die CIS- und DISA-Standards umfassen, sondern bietet auch Out-of-the-Box-Empfehlungen und kompensierende Kontrollen. Dank dieser Kombination schützt Qualys PC die IT-Infrastruktur von Unternehmen vor veröffentlichten Zero-Day-Lücken, wenn kein Patch verfügbar ist, und reduziert dadurch das Gesamtrisiko jeder Zero-Day-Lücke.

www.qualys.com

DISASTER RECOVERY

KEIN WEG FÜHRT AM ACTIVE DIRECTORY VORBEI

Ob Großbrände, Überflutungen oder Ransomware-Attacken, es gibt viele Großschadenereignisse, welche die IT einer Organisation in ihren Grundfesten erschüttern kann. Sowohl die in den letzten Jahren verstärkt auftretenden Naturkatastrophen als auch die zunehmenden Cyberangriffe können ein Unternehmen in seiner Existenz bedrohen. Allein in Deutschland waren im vergangenen Jahr laut einer kürzlich von Sophos veröffentlichten Studie 67 Prozent der befragten Organisationen mit einer Ransomware-Attacke konfrontiert. Die Verantwortlichen in Unternehmen sollten sich also nicht der Hoffnung hingeben, dass ausgerechnet ihre Organisation verschont bliebe.

Gerade Schadenereignisse, bei denen die Domain-Controller einer Organisation in Mitleidenschaft gezogen werden, stellen IT-Teams regelmäßig vor eine schier unlösbare Herausforderung. Denn in einem solchen Fall ist die komplette Netzwerk- und Mandanten-Verwaltung via Active Directory (AD) betroffen. Ohne entsprechende Vorkehrungen ist es für die IT-Verantwortlichen nahezu un-

möglich, den Geschäftsbetrieb auf absehbare Zeit wiederherzustellen – im wahrsten Sinne eine existenzgefährdende Situation. Denn mit dem AD steht und fällt die gesamte IT-Infrastruktur einer Organisation. Microsoft-Dienste wie Exchange, SharePoint oder SQL-Server, aber auch SAP, Oracle und vieler anderer Anbieter, sind von einem funktionierendem Verzeichnisdienst abhängig. Doch nach wie vor scheint vielen IT-Teams nicht bewusst zu sein, wie gefährlich es ist, Notfallmaßnahmen für das Active Directory außer Acht zu lassen.

Für den Ernstfall gewappnet

Der erste Schritt zur Sicherung des AD besteht darin, dass sich die IT-Verantwortlichen der Risiken bewusstwerden und einen geeigneten Notfallwiederherstellungsplan entwickeln. Dieser muss in der Folge getestet werden. Dazu eignet sich ein (virtuelles) Testlabor, mit dessen Hilfe die Angriffsreaktion überprüft und etwaige Fehlfunktionen erkannt werden können. Hierzu bedarf es eines präzisen Abbildes der AD-Struktur, da ansonsten unvorhergesehene Störungen im Wiederherstellungsprozess drohen, sollte der Fall der Fälle eintreten.

Aufbau eigener Testumgebung ist komplex

IT-Teams sollten den Aufwand für die Einrichtung einer virtuellen Testumgebung nicht unterschätzen. Damit im Rahmen eines Testfelds das AD wiederhergestellt werden kann, bedarf es der Erstellung von Systemen mit übereinstimmenden Servernamen und die Ausführung vom Domain Controller Promoter (DCPromo), sodass ein leerer Forest entsteht. Zudem müssen im Nachgang auch Systemstatus-Backups wiederhergestellt werden. Und dazu müssen die Teams denselben Systemstatus auf derselben Betriebssystemversion, demselben Patch-Level und zuweilen derselben Hardware wiederherstellen. Genau hier kommt es oft zu Schwierigkeiten.

Auch erfordert der Aufbau eines Testlabors ein Abbild der gesamten Verzeichnisumgebung, inklusive aller AD-Nutzer und -Gruppen aus dem produktiven Umfeld. Dieses Abbild muss mit Hilfe von Skripten in der Testumgebung geschaffen werden, was ein tiefergehendes Verständnis des Scriptings erfordert. Dass die Test- und Produktionssysteme nicht in derselben Umgebung laufen, macht den Vorgang umso schwieriger. Hinzukommt, dass trotz gleicher Benennung der Gesamtstruktur, für Domänen, Benutzer und Gruppen unterschiedliche Sicherheitskennungen (SIDs) gelten. Sie verfügen über eine jeweils eindeutige, unveränderliche Kennung, die bei der Vergabe von Berechtigungen auf Dateien, Ordner und andere Windows-Ressourcen zur Anwendung kommt. Daher ist es ausgeschlossen, dass zwei erstellte Forests dieselben SIDs besitzen. Dies hat zur Folge, dass Anwendungsserver nicht in eine Testumgebung verschoben werden können.

Letztlich sind dies nur einige Aspekte, die belegen, wie schwierig und personalintensiv der Aufbau einer eigenen Testumgebung ist. Ein solches Testlabor verliert zudem vergleichsweise schnell seine Aktualität, da Änderungen in der Produktivumgebung darin nicht abgebildet werden.

Abhilfe durch spezielle Tools

Obgleich Unternehmen sich für eine weitgehend manuell eingerichtete Testumgebung entscheiden können, um ihre Notfallpläne für das AD zu testen, spricht das Kosten-Nutzen-Verhältnis eindeutig dagegen, vor allem, da es effiziente Tools in diesem Bereich gibt. Allerdings können IT-Teams beispielsweise mit dem Recovery Manager for Active Directory Disaster Recovery Edition weitgehend automatisiert ein virtuelles Testlabor schaffen, das die tatsächliche Betriebsumgebung abbildet. Auf diese Weise müssen auch keine manuellen Aktualisierungen vorgenommen werden.

Auch an anderer Stelle kommen die Vorzüge eines Wiederherstellungs-Tools zum Tragen. Denn es lassen sich damit Abgleiche des AD sowohl mit der ihm zugeordneten Sicherung als auch verschiedener anderer Sicherungen durchführen und im Anschluss entsprechende Vergleichsberichte exportieren. Eine Wiederherstellung ist damit ebenfalls problemlos umsetzbar, da die schnelle Identifizierung gelöschter oder geänderter Attribute und Objekte dazu beiträgt, nunmehr überflüssige Schritte einzusparen.

Im Falle hybrider Umgebungen, also der gleichzeitigen Nutzung von AD und Azure Active Directory (AAD), können spezialisierte Tools ebenfalls ihre Stärken ausspielen. Hierbei ist sowohl die Verfügbarkeit als auch die Integrität beider Systeme von entscheidender Bedeutung. Mit entsprechenden Tools können IT-Teams auf Basis eines Dashboards zwischen Hybrid- und reinen Cloud-Objekten unterscheiden und direkt Berichte erstellen, die Auskunft über Unterschiede zwischen den Produktivsystemen und ihren Sicherungen geben. Die Wiederherstellung ist in Active Directory ebenso wie in Azure Active Directory jederzeit möglich.

Letzter Ausweg: Bare Metal Recovery

Kommt es zum Worst Case wie beispielsweise einer Ransomware-Attacke oder

einer Naturkatastrophe, bei der auch die Backups in Mitleidenschaft gezogen werden, bleibt den Administratoren oft nur noch eine sogenannte Bare Metal Recovery. Daher sollten Unternehmen bei der Wahl ihrer Backup- und Recovery-Lösung auch an ein solches Schadenereignis denken und sich für eine Lösung entscheiden, die Bare Metal Recovery unterstützt und zudem die Backups auf Malware überprüft. Denn bei einer solchen Lösung sind alle für die Wiederherstellung benötigten Komponenten auf einem bootfähigen Medium gespeichert, sodass die Rücksicherung zeitnah auch von Null an erfolgen kann. Bei dieser Rücksicherung werden folglich nicht nur die Daten wiederhergestellt, sondern auch die jeweilige Betriebssystemversion und alle entsprechenden Komponenten. Dieser Prozess erfordert lediglich funktionsfähige Hardware, also das „nackte Metall", was im Übrigen nach einer umfassenden Ransomware-Attacke ohnehin das einzige ist, über das die IT-Teams noch verfügen.

Abhängig vom Schweregrad und Umfang eines Angriffs beziehungsweise einer Zerstörung durch einen Brand oder eine Überschwemmung kommt auch eine gemischte Wiederherstellungsstrategie in Betracht. Dabei werden nur ausgewählte Systeme auf Basis des Backups komplett wiederhergestellt, bei anderen wird lediglich ein frisches Betriebssystem aufgespielt und das AD darauf wiederhergestellt. Auch hier gilt, dass dies manuell bzw. mit den Bordmitteln der OS-Hersteller ein äußerst zeitraubender und ineffizienter Prozess ist, der angesichts des Zeitdrucks in einer solchen Situation nicht zu empfehlen ist. Die IT-Verantwortlichen müssen jedoch auch bei der Nutzung einer entsprechenden Software-Lösung darauf auchten, dass diese die Automatisierung aller benötigten Wiederherstellungsschritte unterstützt. Dazu zählt die Rekonstruktion der AD-Services, sei es auf Basis der Bare Metal Recovery oder frisch ausgerollter Betriebssysteme, die Bereinigung von Metadaten, die Wiederherstellung der Trusts, die Rücksetzung von Kennwörtern der hochprivilegierten Konten sowie der Neustart der Replikation.

MIT DEM AD STEHT UND FÄLLT DIE GESAMTE IT-INFRASTRUKTUR EINER ORGANISATION.

Ragnar Heil,
EMEA Channel Account Manager,
Quest Software, www.quest.com

Früherkennung trotz Notfallplänen wichtig

Pläne und umsetzbare Maßnahmen für den Notfall in der Schublade zu haben, ist von großer Bedeutung. Ebenso wichtig ist es, eine Ransomware-Attacke frühzeitig zu erkennen. Denn der beste Angriff aus Sicht der Opfer ist zweifelsohne der, der unterbunden wird, bevor Schaden entsteht. Hierzu muss mittels entsprechender Tools sichergestellt werden, dass Anomalien am Domain-Controller automatisiert erkannt und gegebenenfalls Gegenmaßnahmen eingeleitet werden. Auch das Management potenzieller Angriffspfade ist eine wichtige Komponente beim Schutz von AD- und Microsoft 365-Umgebungen vor Angriffen. Hier gilt es durch Priorisierung und Quantifizierung der Angriffspfade Erkenntnisse zu gewinnen, um die Pfade mit dem größten Gefährdungspotenzial zu identifizieren und zu eliminieren.

Schutz des Active Directory wird zunehmend wichtiger

Vielen Verantwortlichen wird erst nach und nach bewusst, wie schnell auch ihr eigenes Unternehmen von einem Großschadenereignis wie einer Ransomware-Attacke oder einer Naturkatastrophe betroffen sein könnte. Umso wichtiger ist es, sich einerseits vor einem Cyberangriff zu schützen und andererseits mittels probater Notfallpläne auch für den Worst Case gerüstet zu sein. Kaum eine IT-Ressource ist so elementar wie das AD oder Azure Active Directory. Daher sollte der Schutz dieser Schlüsselsysteme besser heute als morgen angegangen werden, um im Schadenfall nicht mit leeren Händen dazustehen.

Ragnar Heil

5 WEGE FÜR MOBILE SICHERHEIT

FÜR HOHE SICHERHEIT LOHNT ES SICH, AUF EINE DURCHDACHTE GESAMTLÖSUNG ZU SETZEN

Cyber-Angriffe, die auf Smartphone-Nutzer abzielen, haben in den letzten Jahren zugenommen. Die Attacken durch Hacker, Viren, Malware und Co. stellen für Unternehmen eine ernsthafte Bedrohung dar – zumal mobile Geräte häufig auch privat im Einsatz sind. Für einen möglich lückenlosen Schutz sollte die Sicherheitsstrategie daher an mehreren Stellen ansetzen.

1. Geräteintegrität von Anfang an

Die Grundlage mobiler Sicherheit bildet ein Hardwareschutz auf allen Ebenen. Bei Samsung Mobilgeräten wird dazu bereits ab Werk die mehrschichtige Knox Plattform integriert. Sie bildet ein stabiles Fundament, das die Geräte von innen nach außen in Echtzeit schützen kann. Dazu wird zum Beispiel in einer TrustZone eine manipulationssichere Umgebung geschaffen, die PINs, Passwörter, biometrische Daten und sicherheitskritische Schlüssel physisch vom Rest trennt. Selbst mit Lasern und Power-Glitch-Taktiken können Hacker diese nicht überwinden. Zudem ermöglicht die Plattform durch eine wachsende Anzahl von Schnittstellen (APIs) die granulare Verwaltung der Geräte.

2. Trennung beruflicher und privater Daten

Eine große Herausforderung für Unternehmen kann die private Nutzung der Geräte darstellen. Sinnvoll können daher Funktionen zum Isolieren und Verschlüsseln von Geschäftsanwendungen und -daten in separaten Containern sein. Geht ein Gerät verloren oder verlässt der Mitarbeiter das Unternehmen, kann die Geschäftspartition remote gelöscht werden, während persönliche Inhalte davon unberührt bleiben.

3. Zero Touch Konfiguration

Neben der Hardware spielt auch die Konfiguration der Geräte eine große Rolle für einen sicheren und effizienten Betrieb. Automatisierte Lösungen können nicht nur den Enrollment-Prozess verschlanken, sondern auch menschliche Fehlertoleranz ausgleichen. Schließlich müssen die Geräte nicht händisch eingerichtet werden, sondern lassen sich zentral ohne Endnutzerinteraktion (Zero Touch) konfigurieren.

4. Effiziente Verwaltung

Zum Marktstandard gehört heute auch eine datenschutzkonforme Verwaltung der mobilen Geräteflotte. Die Durchsetzung von Sicherheitsrichtlinien wird über ein Mobile Device Management (MDM) gelöst, mit dem IT-Administratoren die Geräte über eine webbasierte Konsole verwalten können. Entsprechende Lösungen sind benutzerfreundlich und effizient – und können sich so auch für kleine und mittlere Unternehmen lohnen. Für größere Unternehmen bieten bestimmte Geräte zudem die Möglichkeit zur Einbindung in bereits bestehende MDM- oder EEM-Lösungen.

5. Updates und Patches

Veraltete Firmware stellt eine der größten Schwachstellen dar, die zu Malware-Infektionen führen kann. Die Verwaltung des ständigen Patch-Streams kann jedoch eine zusätzliche Belastung für die IT sein. Aber auch hier gibt es Lösungen, die Administratoren helfen können, die richtigen Patches termingerecht bereitzustellen. Zudem lässt sich die Kompatibilität zu bereits genutzter Unternehmenssoftware im Vorfeld prüfen.

Holger Dohrmann
www.samsungknox.com/de

Mit Samsung Knox steht eine Gesamtlösung zur Sicherung, Bereitstellung und Verwaltung Ihrer Samsung Mobilgeräte zur Verfügung.

Mehr dazu erfahren Sie hier:

IDENTIFIZIEREN VOR SCHÜTZEN

RISIKOERKENNUNG UND -BEWERTUNG SIND EINE HOHE KUNST

Zwischen Risikowahrnehmung und tatsächlichen Sicherheitsvorfällen klafft eine große Lücke. Das verrät ein Blick in die Cybersecurity-Studie von COMPUTERWOCHE Research Services in Zusammenarbeit mit Damovo und ist eines der zentralen Ergebnisse. Birgt diese Lücke die Gefahr, zur Schwachstelle im Sicherheitsnetz eines Unternehmens zu werden?

it security sprach mit Edgar Reinke, Security-Experte und Strategic Technology Officer (STO) bei Damovo, über die Notwendigkeit einer strukturierten Sichtweise auf die Risiko- und Sicherheitslage, ganzheitliche Konzepte wie Zero Trust und die Brisanz des Fachkräftemangels im Security-Kontext.

it security: *Herr Reinke, laut Cybersecurity-Studie verzeichneten in diesem Jahr mehr als die Hälfte der befragten Unternehmen Sicherheitsvorfälle durch ehemalige oder aktuelle Beschäftigte. Gleichzeitig halten nur knapp 28 Prozent einen solchen Vorfall für wahrscheinlich. Wie erklären Sie sich diese Diskrepanz?*

Edgar Reinke: Die Diskrepanz spiegelt wider, wie hoch die Kunst der Risikoerkennung und -bewertung ist. Es kommt darauf an, Risiken und digitale Bedrohungen, auch von innen, strukturiert zu betrachten und den Ursachen auf den Grund zu gehen. Passieren Fehler aus der Komplexität von Lösungen und Services heraus? Werden Mitarbeiter deshalb aus Unwissenheit zu Mittätern? Es geht also darum, Risiken sichtbar zu machen und Awareness für potenzielle Gefahren zu schaffen.

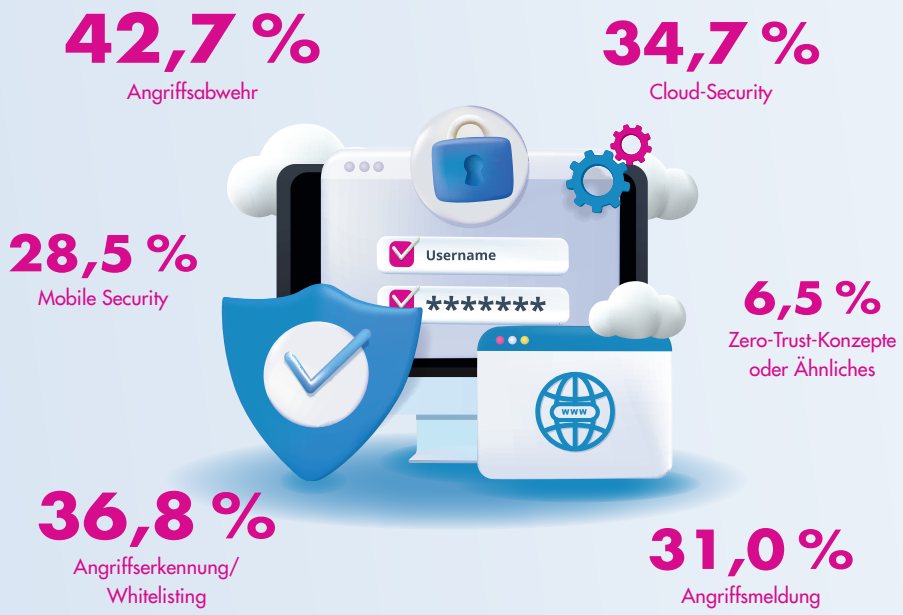
it security: *Das heißt, Prävention vor Reaktion?*

Edgar Reinke: Genaugenommen heißt das: Identifizieren vor Schützen. Ein hundertprozentiger Schutz ist nicht möglich, deshalb ist auch die Angriffserkennung wichtig. Instanzen wie etwa das BSI nehmen Organisationen und Behörden in die Pflicht, Security Events zu erkennen und darauf zu reagieren. Laut Studie liegt die Angriffserkennung mit rund 37 Prozent auf Platz 2 bei den Investitionen in Cybersecurity 2022, direkt hinter der Angriffsabwehr selbst. Die Wichtigkeit der Angriffserkennung haben die Unternehmen offensichtlich erkannt. Es fehlt aber oftmals an Know-how und Ressourcen, um die Angriffserkennung qualifiziert zu erfüllen.

it security: *Laut Studie sehen allerdings nur rund 11 Prozent der befragten Unternehmen die personellen Ressourcen als Security-Herausforderung an.*

Edgar Reinke: Das überrascht mich tatsächlich. Denn komplexe

WO LIEGEN DIE SCHWERPUNKTE IHRER CYBERSECURITY-INVESTITIONEN? (AUSZUG)



Quelle: Cyber Security Studie von COMPUTERWOCHE Research Services in Zusammenarbeit mit Damovo, München 2022

ZIEL EINER SECURITY-STRATEGIE IST ES, EINE NACHHALTIGE CYBER-RESILIENZ AUFZUBAUEN UND SO CYBERANGRIFFE ERFOLGREICH ABZUWEHREN.

Edgar Reinke, Strategic Technology Officer, Damovo, www.damovo.com

Aufgabenstellungen wie Aufbau und Umsetzung von Security-Strategien und -Maßnahmen erfordern Expertie. Ein anderes Bild in puncto Fachkräftemangel zeichnet beispielsweise die „CIO-Agenda 2022" von CIO-Magazin, WHU – Otto Beisheim School of Management und Horváth Digital. Demnach geben immerhin 32 Prozent der CIOs an, dass fehlende Kompetenzen und Fähigkeiten die Umsetzung ihrer strategischen Vorhaben bremsen.

it security: *Auf welche technischen Maßnahmen setzen die Unternehmen, um sich vor Cyberangriffen zu schützen?*

Edgar Reinke: Laut Studie ergreifen die befragten Unternehmen mehrheitlich punktuelle IT-Sicherheitsmaßnahmen und setzen auf einen klassischen Basisschutz aus Firewall, Anti-Virenschutz, Verschlüsselung und weitere. Damit wähnen sie sich vor Cyberangriffen gut geschützt. Eine Scheinsicherheit. Erforderlich sind ganzheitliche Konzepte wie Zero Trust. Dieses gehört aber nicht zu den Top-Investitionsbereichen der Unternehmen. Mit nur 6,5 Prozent rangieren Zero-Trust-Konzepte am Ende der Investitionsliste.

it security: *Woran liegt das?*

Edgar Reinke: Zero-Trust-Konzepte zu entwickeln, ist ein langwieriger, anspruchsvoller Prozess. Es müssen viele verschiedene Blickwinkel und Fragestellungen betrachtet werden. Zwar sind die strategischen und technischen Frameworks klar beschrieben, die Umsetzung jedoch ist eine Herausforderung und meist wieder eine Kompetenz- und Ressourcenfrage. In der Konsequenz setzen Unternehmen Einzelmaßnahmen wie Identity- und Accessmanagement um, betten sie jedoch nicht in ein Gesamtkonzept wie Zero Trust ein. Ein solcher Bottom-up-Ansatz führt zwar mit einer gewissen Geschwindigkeit zu einem pragmatischen Ergebnis, ist aber nicht weitreichend genug.

it security: *Wie sollten Unternehmen idealerweise vorgehen, um sich bestmöglich und umfassend in Sachen Cybersecurity aufzustellen?*

Edgar Reinke: Gefragt ist eine übergeordnete, ganzheitliche Risikomanagement- und Security-Strategie, die von der Bestandsaufnahme und Risikobewertung bis hin zur strategischen Konzeptionierung und Umsetzung geeigneter Security-Maßnahmen führt. Ziel ist es, durch integrierte IT-Sicherheitsmaßnahmen eine nachhaltige Cyber-Resilienz aufzubauen und so Cyberangriffe und andere Bedrohungen, auch von innen, erfolgreich abzuwehren.

it security: *Herr Reinke, vielen Dank für das Gespräch!*

IMPRESSUM

Geschäftsführer und Herausgeber:
Ulrich Parthier (-14)

Chefredaktion:
Silvia Parthier (-26)

Redaktion:
Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Holger Dohrmann, Günter Esch, Ragnar Heil, Jörg von der Heydt, Sabine Kuch, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Michael Veit, Zac Warren

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 30,
gültig ab 1. Oktober 2022.

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

Unternehmen leben länger mit

IT-Security Schutzmaßnahmen

SCAN ME

Mehr Infos dazu im Printmagazin

itsecurity

und online auf **www.it-daily.net**