itmanagement
OKTOBER 2021

INKLUSIVE 48 SEITEN
IT SECURITY

HOMEOFFICE

DER NEUE DAUERBRENNER

Sascha Häckel und Wilko Frenzel, Aagon GmbH

RECHENZENTRUM DER ZUKUNFT

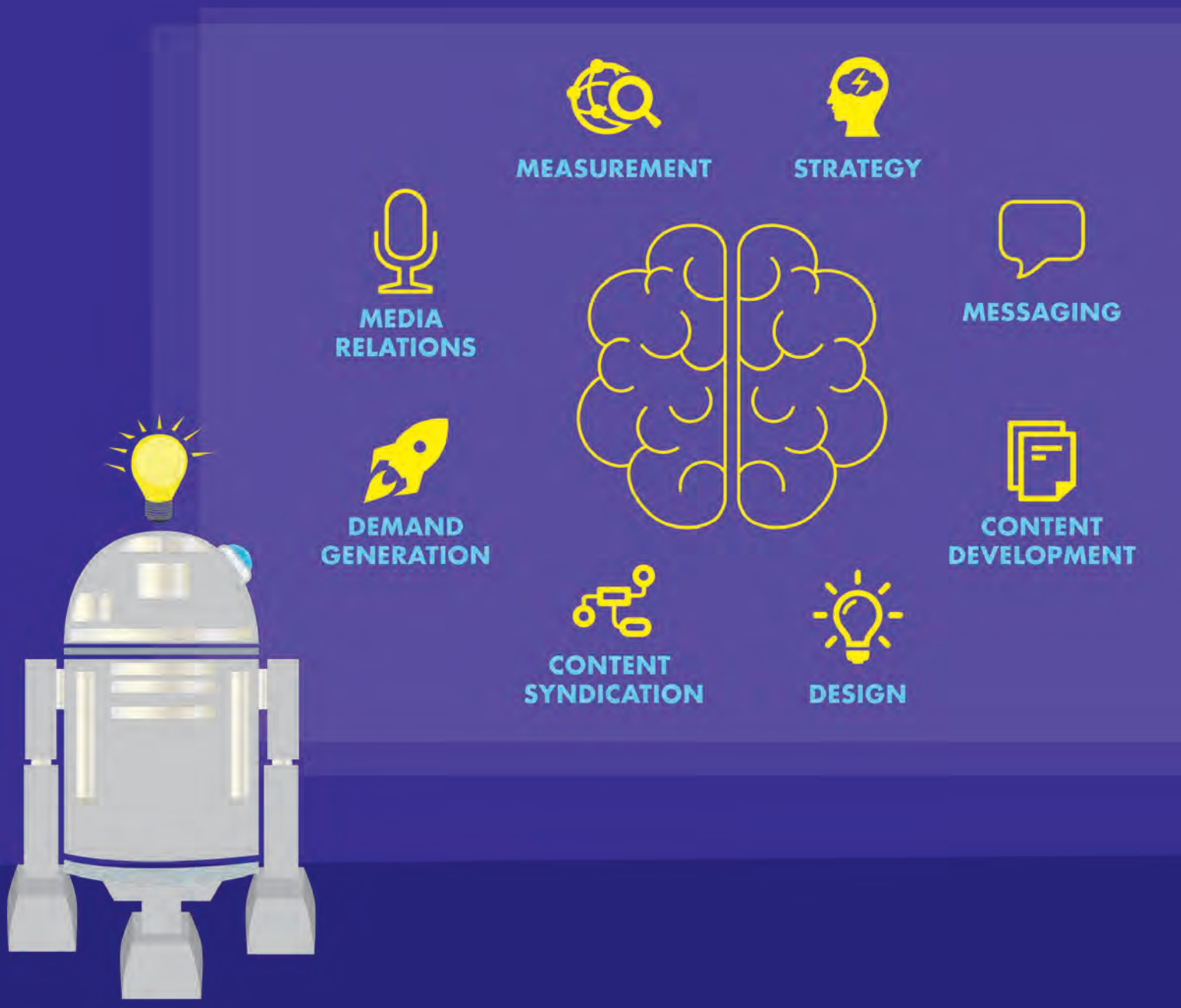
Alleskönner oder kritischer Erfolgsfaktor?

DEVSECOPS PIPELINE

Everything-as-a-code – Anything secure?

www.it-daily.net

Thought Leadership



KÜNSTLICHE INTELLIGENZ
THOUGHT LEADERSHIP

TOTGEGLAUBTE LEBEN LÄNGER

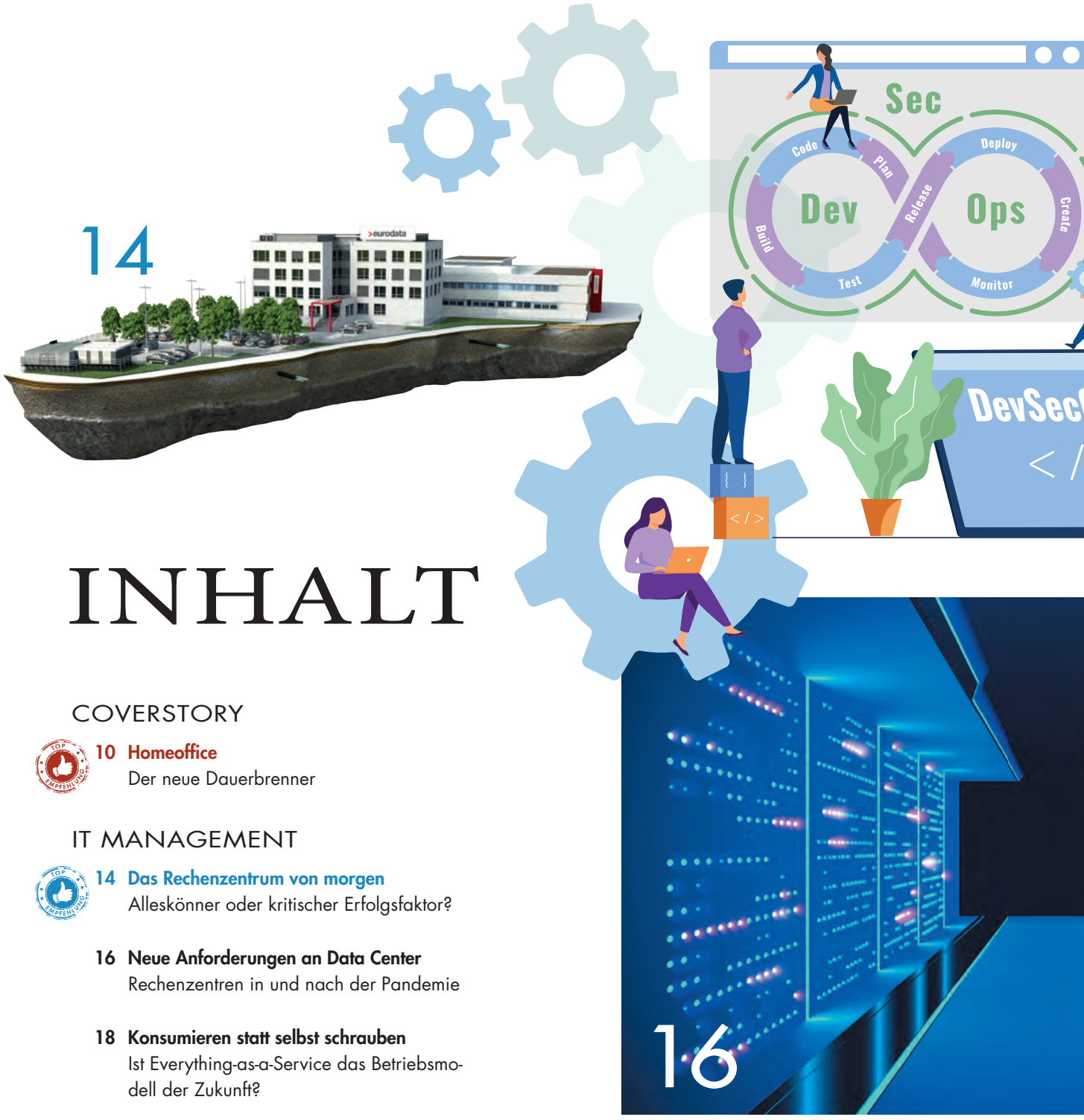
Die it-sa findet wieder statt und das sogar als Präsenzveranstaltung. Jetzt sagen Sie sicher, „Wieso totgeglaubt?“, sie ist im letzten Jahr doch nur wegen der Covid-19-Pandemie abgesagt worden. Sicher! Aber trotzdem wurde es für die großen Messen in der Vergangenheit immer schwerer mit Konzepten und Ideen zu überzeugen – bestes Beispiel wäre da die Cebit. Jahrelanges Ringen brachte die Messe nicht wieder zu ihrer ursprünglichen Größe zurück und letztendlich musste das Konzept begraben werden. Auch die it-sa kämpfte mit schwindenden Ausstellern und Teilnehmern. Doch dann kam Covid-19.

Während der Hochzeit der Pandemie wurde spekuliert, dass ein genereller Trend weg von Präsenzveranstaltungen hin zu Onlinemessen eintreten würde. Diese seien letztendlich kostengünstiger und man erreiche online durchaus mehr Menschen als auf einem Messestand. Trotzdem fehlten die persönlichen Gespräche, die direkten Vergleiche mit dem Mitbewerber oder eben ganz spontane, zufällig Aufeinandertreffen zweier innovativer Ideen, aus denen vielleicht mal etwas ganz Großes werden könnte. Beide Messearten haben also ihre Vor- und Nachteile.

Umso schöner ist es zu sehen, dass sich einige Veranstalter wieder trauen – unter teilweise schwierigen Bedingungen und Hygieneauflagen – Messen als Präsenzveranstaltung stattfinden zu lassen. Viele Unternehmen sind ob der Situation noch vorsichtig, daher verwundert es nicht, dass die it-sa dieses Jahr eher klein ausfällt, aber was noch nicht ist, kann ja nächstes Jahr wieder werden. Nun muss sie nur noch mit neuen Konzepten überzeugen und somit die Zukunft der Messen einläuten.

Lassen wir uns überraschen

Carina Mitzschke | Redakteurin it management



INHALT

26

10

COVERSTORY

Inklusive 48 Seiten

IT SECURITY SPEZIAL

unplugged

22

RANSOMWARE-KRISE

EIN GLOBALER LÖSUNGSANSATZ MUSS HER

Ransomware hat sich mittlerweile zu einem globalen Problem entwickelt. Cyberkriminelle Gruppen operieren von Ländern aus, die ihnen einen sicheren Unterschlupf bieten und es ihnen ermöglichen, sogar raffinierteste Angriffe zu starten. Um eine Eskalation zu verhindern, braucht es eine gemeinsame, weltweite Strategie.

1. Schluss mit Lösegeldzahlungen

Solange Ransomware profitabel ist, fehlt den Angreifern der Anreiz aufzuhören. Jedes Unternehmen, das Teil der Lieferkette einer Bundes-, Landes- oder Kommunalverwaltung ist, sollte sich vertraglich verpflichten, kein Lösegeld zu zahlen.

2. Regulierung der Krypto-Währungsbörsen

Was Ransomware zu einer globalen Krise gemacht hat, ist das Ausmaß, in dem immer wieder Nationalstaaten die Cyberkriminellen ausbilden. Leider fehlt hier bislang jegliche Handhabe. Cyberkriminelle wandeln die Lösegelder in Krypto-Währungsbörsen in harte Währungen um. Die Einführung strengerer Vorschriften würde es Ransomware-Gruppen erschweren, von ihrer Arbeit zu profitieren.

3. IT-Hygiene

Es gibt einige grundlegende IT-Hygienemaßnahmen, die viele Unternehmen immer noch nicht ergreifen: Aufklärung der Mitarbeiter über Spear-Phishing, Einführung von Zwei- und Mehrfaktor-Authentifizierung, ein grundlegender Endpoint-Schutz und die Sicherung von Daten auf netzwerk- und standortfernen Speichern.

Außerdem muss es Standard werden, Sicherheitsvorfälle zu melden, um so die Sensibilisierung voranzutreiben.

www.sophos.com

DIE KOSTEN EINER RANSOMWARE-ATTACKE SIND MEHR ALS „NUR" DAS LÖSEGELD

Dazu kommen Kosten für:

- Ausfallzeiten
- Mitarbeiter
- Geräte
- Netzwerke
- Upgrades der IT-Infrastruktur

AKTUELLE STUDIE

DIGITALISIERUNG BRAUCHT MESSBARKEIT

Schaffen Cloud und Digitalisierung tatsächlich den gewünschten Mehrwert? Wie können Prioritäten für IT-Investitionen gesetzt werden? Komplexe Fragen, für die es vielfach an verlässlichen Daten fehlt.

Kaum ein Unternehmen, dass aktuell nicht mit technologischen Investitionen seine strategischen Weichen neu stellt: Laut der internationalen HBR-Studie haben 82 Prozent der befragten Führungskräfte ihre Digitalisierungsinitiativen intensiviert. 62 Prozent sagen, dass Investitionen in Technologien in nächster Zukunft höchste Priorität haben.

Das ist zunächst nicht allzu überraschend und gehört zum Tagesgeschäft der IT. Spannend wird es bei einem genauen Blick auf andere Zahlen – denn: Für 92 Prozent der Befragten ist der Mehrwert, der aus dem Einsatz von Technologien resultiert, von höchster Bedeutung bei Budgetplanungen.

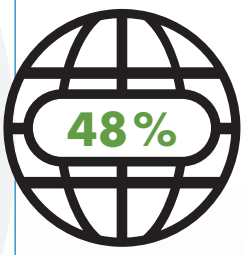
Eine Anforderung, die weit weniger trivial ist, als sie klingt. Denn mit gängigen Bordmitteln in Unternehmen ist, wenn überhaupt, nur vage abschätzbar, welche technologischen Komponenten in einzelnen Geschäftsbereichen zu einem messbaren finanziellen Wertbeitrag führen und welche Aufwendungen dem insgesamt gegenüberstehen. Dafür braucht es ein systematisches IT-Finanzmanagement, das Industriestandard entspricht.

So unterstreicht auch die HBR-Studie, dass nur 62 Prozent den dazu verfügbaren Informationen vertrauen – eine Differenz von 30 Prozent zwischen der Bedeutung der Information und dem Vertrauen in deren Verlässlichkeit.

www.apptio.com

FÜHRUNGSKRÄFTE WISSEN, DASS SIE VERBESSERTE DATEN BENÖTIGEN, UM AGILE ENTSCHEIDUNGEN ZU TREFFEN

Entwicklung von Kennzahlen und datenbasierten Prozessen, um die Geschäftsergebnisse ihrer Technologieinvestitionen zu messen



Bestandsaufnahme der Kompetenzen, die unsere Mitarbeiter zur Umsetzung unserer digitalen Strategie benötigen

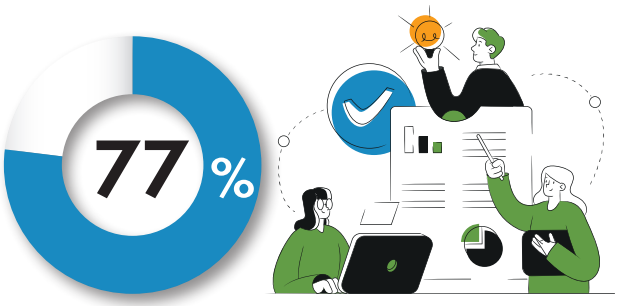
Konsolidierung der Daten, die von IT-, Finanz- und Geschäftsbereichsfunktionen zur Nachverfolgung und Prognose der Technologieausgaben herangezogen werden

DIGITALE ARBEITSPLÄTZE

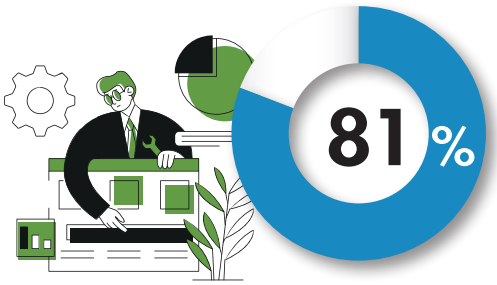
VON TECHNISCHER PERFORMANCE ZUM IT-ERLEBNIS

Nexthink präsentiert die Ergebnisse seiner Studie „Digitale Arbeitsplätze". Sie zeigt: Der bislang eher hemdsärmelige Umgang mit IT-Störungen wird zum Problem für die Innovationsfähigkeit und Produktivität in Unternehmen. Die überwiegende Mehrheit der befragten IT-Experten plant daher Projekte und Investitionen, um Störungen in IT-Infrastrukturen bereits präventiv zu verhindern oder beschleunigt zu lösen.

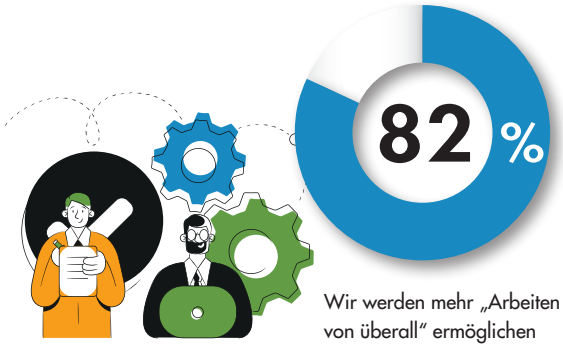
www.nexthink.com



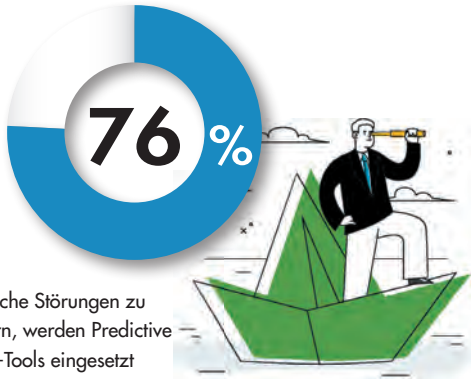
End User Experience Management (EUEM) wird ein Thema mit hoher Priorität werden



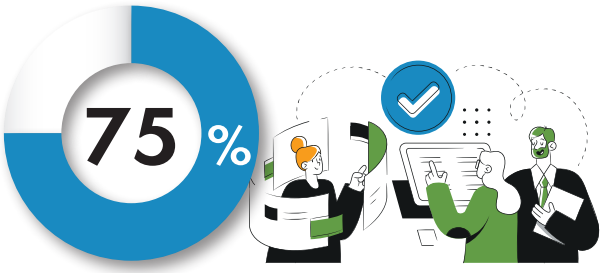
Zu beschleunigten Störungsbehebung werden systematische Prozesse und Werkzeuge mit hohem Automatisierungsgrad eingesetzt



Wir werden mehr „Arbeiten von überall" ermöglichen



um mögliche Störungen zu verhindern, werden Predictive Analytics-Tools eingesetzt



Für IT-Helpdesks wird eine zentrale Management Plattform genutzt, die vom Ticketing über die Benutzerkommunikation bis zur Anleitung zur Fehlerbehebung alles abdeckt

NACHHALTIGKEIT MESSEN UND STEUERN

Immer mehr Unternehmen verpflichten sich zur Nachhaltigkeit. Damit stehen sie vor der Herausforderung, ihre gesamte Wertschöpfungskette auf den Prüfstand zu stellen. T-Systems hat dafür eine web-basierte Lösung entwickelt. Mit „Syrah Sustainability" behalten Unternehmen alle Nachhaltigkeitsindikatoren im Blick. Eine benutzerfreundliche Oberfläche unterstützt sie, die relevanten Daten zu erfassen und auszuwerten. Das Besondere: Die Dashboard-Lösung ist vollständig auf die Agenda 2030 der Vereinten Nationen mit ihren 17 Nachhaltigkeitszielen abgestimmt.

www.telekom.com

RECHENZENTREN

STATUS QUO

Wachsender Kapazitätsbedarf, steigende Anforderungen an die Verfügbarkeit, Lieferengpässe bei kritischen Produkten – die Liste der Herausforderungen, vor denen Rechenzentren weltweit stehen, ist lang. Eine aktuelle Studie des Uptime Institutes zeigt auf, wo die Branche 2021 steht.

„Noch nie stand mehr auf dem Spiel, wenn es um die Vermeidung von Ausfällen, die Umweltverträglichkeit und die Gesamtleistung geht. Deshalb müssen Unternehmen ihre geschäftskritische digitale Infrastruktur und ihren Betrieb weiterhin sorgfältig überprüfen, um das Risiko eines Serviceausfalls zu minimieren und die Ausfallsicherheit zu maximieren“, sagte Andy Lawrence, Executive Director of Research.

www.uptimeinstitute.com

ERKENNTNIS 1
Potenzial für mehr Effizienz beschränkt sich auf IT-Racks

ERKENNTNIS 2
Nachhaltigkeits-controlling ist ausbaufähig

ERKENNTNIS 3
Die Hälfte aller Ausfälle verursacht spürbaren Schaden

ERKENNTNIS 4
Wachsende Kapazitäten setzen Lieferketten unter Druck

ERKENNTNIS 5
Der Fachkräftemangel verschärft sich weiter

HOMEOFFICE

DER NEUE DAUERBRENNER

Wer hätte das zu Beginn der Pandemie gedacht? Das Homeoffice ist die neue Dauerbaustelle der IT. Über Chancen und Risiken sprach Ulrich Parthier, Herausgeber it management, mit den beiden Aagon-Geschäftsführern Sascha Häckel (Entwicklung & Produkt) und Wilko Frenzel (Sales & Marketing).

Ulrich Parthier: *Es wird viel über Chancen geredet, die Risiken werden oft verdrängt. Nun, da sich abzeichnet, dass das Homeoffice für viele Teil unseres künftigen Arbeitslebens sein wird, stellt sich die Frage: Wie gehe ich das Thema strategisch an?*

Sascha Häckel: Angesichts von bis zu 18 Millionen Angestellten, die in Deutschland künftig zumindest teilweise von zu Hause arbeiten werden, liegt es auf der Hand, dass die IT-Abteilungen von Unternehmen eine ganz neue Strategie brauchen. Denn ihre bisherigen Lösungen sind dem nicht mehr gewachsen. Nicht nur, dass sie Rechner nun auch aus der Ferne verwalten, Patches und Updates remote verteilen sowie kritische Einstellungen überwachen müssen – und dass diese Prozesse einen enormen zusätzlichen Zeit- und Personalaufwand bedeuten. Auch das Thema Security gewinnt angesichts massiv angestiegener Cyberangriffe auf Homeoffice-Arbeitsplätze nochmals an Bedeutung.

Wir haben noch vor dem zweiten Lockdown eine Checkliste mit allen Punkten entworfen, die es beim Homeoffice-Betrieb zu beachten gilt. Das fängt bereits bei der Hardware an, die standardisiert an die Angestellten ausgegeben werden muss. Interne Server sind auf verschlüsselte Zugriffe von außen vorzubereiten, standardisierte Software und einheitliche Patch-Stände sicherzustellen, Verteilungsprofile anzulegen und Windows-Updates vollständig zu installieren. Weitere Erfordernisse sind Lizenzschlüssel für alle Homeoffice-Plätze und eine umfassende Antivirenlösung.

Ulrich Parthier: *Die IT-Infrastruktur im Homeoffice war zu Beginn der Pandemie die Schwachstelle, da sie praktisch jeden unvorbereitet traf. Welche Komponenten sind aus Ihrer Sicht essentiell, welche „nice to have"?*

Wilko Frenzel: Definiert man als Ziel einen stets aktuellen und einheitlichen Client-Stand, dann sind einige Komponenten natürlich essenziell: eine stabile, unterbrechungsfreie Remote-Verbindung als Voraussetzung für die jederzeit mögliche Software-Überspielung sowie die initiale, vollständige Inventarisierung und Analyse der gewonnenen Informationen. Kernaufgabe im Endpoint Management ist es dann, Software-Updates und Patches für Windows-Betriebssysteme zu überwachen und automatisch zu installieren.

Auch Echtzeit-Virenschutz etwa mittels Microsoft Defender Antivirus ist alles andere als ein Nice-to-have. Man kann diesen aber, statt ihn über Microsoft-Management-Lösungen wie Intune und SCCM zu konfigurieren, in die einheitliche Oberfläche einer Client-Management- oder Unified-Endpoint-Management-Lösung einbinden. Unsere ACMP-Suite bietet diese Möglichkeit – das ist kein Muss, aber eine deutliche Verbesserung hinsichtlich zentraler Verwaltung. Für Abhilfe und eine zusätzliche Entlastung der Firmeninfrastruktur können FTPS-Repositories sorgen, über die Software-, Betriebssystem- und Windows-Patch-Ressourcen zur Verfügung stehen.

> ACMP VERWALTET ALLE COMPUTER ZENTRAL UND VERTEILT SOFTWARE- UND SICHERHEITS-PATCHES IN- UND AUSSERHALB DES FIRMEN-NETZWERKS – AUCH OHNE WINDOWS SERVER UPDATES SERVICES.
>
> Sascha Häckel, Geschäftsführer, Aagon GmbH, www.aagon.com

Ulrich Parthier: *Kommen wir zu ACMP, Ihre Client-Management-Software. Wie kann sie Unternehmen helfen, im Homeoffice sicher und effizient zu arbeiten?*

Sascha Häckel: Die ACMP-Suite unterstützt beim Patchen und Installieren der eingesetzten Hard- und Software. In wenigen Minuten kann der Administrator eine große Anzahl von Notebooks für den Einsatz im Homeoffice vorbereiten. ACMP verwaltet alle Computer zentral und verteilt Software- und Sicherheits-Patches inner- und außerhalb des Firmennetzwerks – auch ohne Windows Server Updates Services. Dies spart der IT-Abteilung enorm viel Zeit, erhöht die Unternehmenssicherheit und sorgt dafür, dass keine Schatten-IT entsteht. Die Software bildet auch den kompletten Lifecycle ab. So ist ein kontinuierlicher Überblick über alle Firmenrechner und Lizenzen gewährleistet.

Ulrich Parthier: *Sicherheit ist Vertrauenssache. Kann man Ihre Software auch kostenlos testen?*

Wilko Frenzel: Interessenten haben mit der kostenlosen ACMP-Testversion die Möglichkeit, unsere Client-Management-Lösung zur schnellen und einfachen Verwaltung der IT auszuprobieren. Diese erstreckt sich über alle von uns angebotenen Module. Vorab bieten wir Informationen und Unterstützung bei der Einrichtung und Anwendung.

Ulrich Parthier: *Wie lange dauert ein Roll-out der Lösung? Ist er von der Zahl der User abhängig und läuft er automatisiert ab?*

Sascha Häckel: Die Installation von ACMP ist schnell erledigt. Hierzu werden lediglich ein paar administrative Zugänge benötigt, und auf Wunsch wird auch direkt ein SQL Express Server mit installiert. Das anschließende Roll-out der ACMP-Agenten für das Management der Clients und Server kann entweder manuell über unsere Agentendistribution erfolgen oder auch automatisch über die Installationsregeln. Das bedeutet, dass sich der zeitliche Aufwand eines kompletten ACMP-Roll-outs für den Admin sehr gering gestaltet. Alles in allem kann man also innerhalb von ein bis zwei Stunden mit ACMP starten.

> INTERESSENTEN HABEN MIT DER KOSTENLOSEN ACMP-TESTVERSION DIE MÖGLICHKEIT, UNSERE CLIENT-MANAGEMENT-LÖSUNG ZUR SCHNELLEN UND EINFACHEN VERWALTUNG DER IT AUSZUPROBIEREN.
>
> Wilko Frenzel, Geschäftsführer, Aagon GmbH, www.aagon.com

Ulrich Parthier: *Wie sieht das Lizenzmodell aus?*

Wilko Frenzel: Dieses richtet sich nach der Anzahl der zu verwaltenden Clients. Neben dem klassischen Software-Kauf mit entsprechend jährlich anfallender Wartung planen wir, künftig für alle Module auch ein Mietmodell, das sogenannte Pay-per-Use-Modell, anzubieten. Für den Kunden hat dies den Vorteil, dass er die Software nicht erwirbt und die Miete entsprechend einfach als Aufwand verbuchen kann. Auch Änderungen oder Erweiterungen können so sehr flexibel realisiert werden.

Ulrich Parthier: *Was sind häufige Hürden und Herausforderungen, auf die Unternehmen bei der Verwaltung der Homeoffice-IT stoßen? Worauf gilt es besonders zu achten?*

Sascha Häckel: Gerade, wenn viele Beschäftigte remote arbeiten, wird die Verteilung von Software-Aktualisierungen und Patches auf die verteilten Client-Systeme zur Herausforderung. Oft setzen Unternehmen dafür noch zu viele Ressourcen ein und erledigen die Aufgaben teils manuell mit Insellösungen. Mit einer zentralisierten UEM-Lösung lassen sich Update- und Patch-Management wesentlich besser planen und automatisch unternehmensweit einspielen – auch bei Remote-Verbindungen. Solche Systeme prüfen die Verfügbarkeit von Patches selbständig, testen sie auf ihre Kompatibilität mit anderen Software-Anwendungen und installieren sie automatisch. Auch regelmäßige

Scans werden durchgeführt und Berichte auf Basis der Ergebnisse erstellt.

Ulrich Parthier: *Wie sehen Sie die Zukunft des Homeoffice, in welche Richtung werden wir uns hier entwickeln?*

Wilko Frenzel: Nicht alle Office-Worker werden zu 100 Prozent an ihre angestammten Arbeitsplätze zurückkehren. Vielmehr gehört die Zukunft dem Hybrid-Betrieb. Die neuen Anforderungen an das Management werden sich daher weiter verfestigen. Ohne ein Client beziehungsweise Unified Endpoint Management werden Unternehmen die Homeoffice-Situation nicht in den Griff bekommen.

Ulrich Parthier: *Bisher sprachen wir über die Risiken. Wie schaut es mit den Chancen aus? Welche Vorteile sehen Sie für Unternehmen wie für Beschäftigte und: Wie handhaben Sie das selber in Ihrem Unternehmen?*

> Weiterführende Informationen und eine Checkliste mit den wichtigsten Punkten, auf die Unternehmen bei der Einrichtung von Homeoffices achten sollten, gibt es unter ***https://www.aagon.com/workfromhome***

Sascha Häckel: Flexible Arbeitszeitgestaltung und Homeoffice gibt es auch bei Aagon, und dies nicht erst seit Corona. Remote zu arbeiten gehört zu unserer Unternehmens-DNA, und wir schätzen die Vorteile. Neben der genannten Flexibilität ist dies zum Beispiel auch eine Möglichkeit für Arbeitgeber, trotz steigender Beschäftigtenzahl keine zusätzlichen Büroflächen anmieten zu müssen.

Dezentrale Arbeitsplätze sind für uns ferner eine Chance, neue Beschäftigte auch aus Regionen weit weg von der Unternehmenszentrale oder einzelnen Standorten zu gewinnen.

Ulrich Parthier: *Herr Häckel, Herr Frenzel, vielen Dank für das Gespräch.*

GUTEN CONTENT SCHREIBEN

SO PRODUZIEREN SIE MEHRWERT-CONTENT, DER GELESEN WIRD

Dieses Buch ist die pragmatische Anleitung für den perfekten Content. Wer Texte und Bilder für die Produkt- und Unternehmenskommunikation erstellt, sei es auf Websites, Blogs, Landingpages und Social-Media-Plattformen, erhält mit diesem Praxisleitfaden das nötige Know-how. Dr. Beatrice Eiring führt Sie Schritt für Schritt durch den Prozess der Content-Erstellung – beginnend mit der Zielsetzung, die Intention zwischen Ihnen als Sender und Ihrem Leser als Empfänger zu matchen. Mit Tipps zur Keyword-Recherche und zum zielgruppengerechten Schreibstil bis hin zur SEO-Optimierung erfahren Sie, was wirklich guten Content ausmacht. Ergänzt wird dieses konkrete Schreib-Know-how um zahlreiche Tools und Best-Practices für die Social-Media-Plattformen Facebook, Instagram, LinkedIn und Xing. Die Autorin setzt in ihrem Buch den Fokus nicht nur auf Unternehmenskommunikation, sondern darauf, wie Content gefunden wird und vor allem überzeugt.

Guten Content schreiben
– So produzieren Sie Mehrwert-Content, der gelesen wird und wirkt;
Beatrice Eiring; Springer Gabler; 06-2021

OPERATIONAL SERVICES
YOUR ICT PARTNER

Microsoft Partner

Microsoft

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

MICROSOFT 365 & AZURE GERÄUSCHLOS AUSROLLEN UND SICHER BETREIBEN

Zusammenarbeit gelingt ohne Widerspruch zum deutschen Datenschutz

IT und Kommunikation verschmelzen immer stärker - auch mit dem Zuwachs an Home-Office-Arbeitsplätzen und globaler Zusammenarbeit. Microsoft Cloud-Lösungen wie Microsoft 365 und Azure gehören zu den besten Plattformen der Welt.

Allerdings sind die Planung und Einführung komplex. Unsere erfahrenen Solution Architekten begleiten Unternehmen als kompetente Partner für eine nahtlose Integration sämtlicher Module und Plattformen. Dabei beachten wir die hohen Auflagen des deutschen Datenschutzes sehr genau.

Profitieren Sie von unserer Expertise und verlassen Sie sich auf uns als Microsoft Gold Partner.

operational-services.de/microsoft-365

Starten Sie mit uns sichere, cloudbasierte Collaboration

DAS RECHENZENTRUM VON MORGEN

ALLESKÖNNER ODER KRITISCHER ERFOLGSFAKTOR?

Was würden wir nur tun, wenn wir für all die Daten, mit denen wir tagtäglich umgehen, keinen Speicherplatz hätten? Wer kann sich heute noch ein Leben ohne Cloud vorstellen? Wie ist es möglich, dass unsere hybride Arbeitssituation produktiv ist und bleibt? Auch wenn diese Fragen in unterschiedliche Richtungen zielen – eines haben sie gemeinsam: Ohne die Kapazitäten und Technologie moderner Rechenzentren wären diese Fragenstellungen nicht lösbar. Umso wichtiger ist es, sich mit den Herausforderungen und der Zukunft von Rechenzentren zu beschäftigen.

Denn das Einzige was in diesen Zeiten sicher ist, ist der konstante Wandel. Schon allein durch die voranschreitende Digitalisierung ergeben sich permanent neue Anforderungen und Situationen, in deren Mittelpunkt dabei immer die IT-Strukturen und Rechenzentren stehen. Ohne sie wäre dieser Fortschritt nicht möglich. Doch wie steht es um die deutschen Rechenzentren? Was macht sie aus und wo geht die Reise hin?

Grundsätzlich kann man sagen, dass der Großteil der Unternehmen heutzutage bezüglich einer sicheren und rechtskonformen Datenspeicherung sensibilisiert sind. Das gilt nicht nur in Bezug auf den DSGVO-konformen Umgang mit personenbezogenen Daten und den damit verbundenen Problemen bei der Nutzung von Clouddienstanbietern in Drittstaaten, sondern auch das Thema Nachhaltigkeit spielt eine zunehmend wichtige Rolle bei der Auswahl von Dienstleistern. Der Saarbrücker Softwarehersteller eurodata beispielsweise, betreibt seine Cloudlösungen im unternehmenseigenen ISO-zertifizierten Hochleistungsrechenzentrum, das u.a. die „Grüne Hausnummer" für sein nachhaltiges Energiekonzept erhalten hat. Diesen umweltbewussten Umgang wissen viele Kunden sehr zu schätzen – und das nicht erst, seit das Buzzword Nachhaltigkeit Einzug gehalten hat, sondern bereits seit Ende der 90er Jahre.

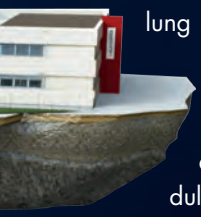
Auch Rechenzentren müssen flexibel sein

Wie aber kann ein Rechenzentrum, die aktuellen Anforderungen und Erwartun-

EURODATA RECHENZENTRUM SAARBRÜCKEN

- Fortlaufende Zertifizierung nach ISO 9001 sowie der ISO 27001 und ISO 22301, inkl. Monitoring und Ressourcen-Vermessung
- IT-Services und Betrieb basieren auf ITIL-Framework
- Deutsche Datenschutzvorgaben sowie EU-Datenschutzgrundverordnung werden erfüllt
- Hochverfügbare und redundante Internet-Anbindungen über multiple 10-Gbit-Anbindungen unterschiedlicher Carrier
- Getrennte Wegführung über redundante Glasfaserstrecken, inkl. räumlich getrennten Gebäudezugängen Public- und Private Cloud verfügbar und mit Hybrid Cloud kombinierbar
- Geschäftsprozesse können in datenschutzkritische sowie -unkritische Arbeitsabläufe unterschieden werden
- Absicherung durch fortschrittliche Gebäude-Techniken und 24/7/365 Überwachung
- Absicherung der Spannungsversorgung durch USV Anlagen und Trafos sowie Notstromdiesel-Technik sowie eine redundante Stromführung
- intelligente Videoüberwachung, restriktive Zugangskontrollen, Brandmeldeanlagen sowie Brandfrüherkennung

gen erfüllen, die einerseits durch einen kontinuierlich steigenden Leistungsbedarf der Kundensysteme und andererseits durch ein immer stärker in den Mittelpunkt der öffentlichen Wahrnehmung tretendes Umweltbewusstsein entstehen? Im konkreten Fall des Saarbrücker Rechenzentrums wird etwa die durch die Kühlung entstehende Wärme in den Gebäudekreislauf zurückgeführt, um die angegliederten Büros zu heizen. Darüber hinaus werden nur energieschonende, modulare Elemente eingesetzt, die so konzipiert sind, dass sich im Falle neuer Entwicklungen, die Rechenzentrums-Hardware sukzessiv austauschen lässt.



Grundvoraussetzung für die ausfallsichere Bereitstellung von Rechenzentrumkapazitäten und Dienstleistungen, die über das Internet als Cloudlösungen angeboten werden, ist eine mehrfach redundante Anbindung des Backbones an unterschiedliche Internetprovider und damit an unterschiedliche DCIX-Knoten.

Hinzukommt, dass die Kapazitäten eines Rechenzentrums skalierbar sein sollten. Das ist gerade vor dem Hintergrund des zunehmenden Einsatzes von Cloudlösungen und des mobilen Arbeitens nicht zu unterschätzen. Vor allem wenn man bedenkt, dass ein Rechenzentrum nie ausfallen darf.

Die doppelte Absicherung ist auch beim eurodata-Rechenzentrum garantiert. Zusätzlich zu einem zweiten, separaten Rechenzentrum in Saarbrücken werden die Backups aller Daten, sogar noch in einem weiteren Rechenzentrum gesichert.

Man muss aber auch bedenken, dass die Anforderungen wie Geschwindigkeit, Skalierbarkeit, Auslastung, Produktivität an Rechenzentren stetig wachsen. Ergo muss es den Betreibern gelingen, ihre Dienstleistung anzupassen und dass, ohne in den Betrieb einzugreifen; ein Kunststück, dass absolute Profis voraussetzt.

CHECKLISTE:

Was muss man bei der Wahl eines Rechenzentrums beachten?

- Es sollte in jedem Fall über eine ISO 27001 Zertifizierung verfügen, mit breitem Geltungsbereich
- Der Standort sollte in Deutschland sein und der Zugriff auf Daten im Supportfall nur aus der EU (DSGVO-konform) erfolgen können
- Die zu hostende Datenmenge sollte flexibel skalierbar sein
- Auf welchen Ebenen (Basisinfrastruktur, Server, Software, Hardware) wird Datenverfügbarkeit garantiert?
- Welche Nachhaltigkeits-Konzepte und Energieeffizienz-Strategien gibt es?

Neue Möglichkeiten dank KI

Spätestens an dieser Stelle kommen die innovativen Möglichkeiten der Künstlichen Intelligenz hinzu. Dieser Aspekt ist so mächtig und weitreichend, dass man ihn inhaltlich kaum zusammenfassen kann. Eines aber ist all den Facetten, die KI für Rechenzentren mit sich bringt gemeinsam: Sie optimieren immerzu und sorgen so an den unterschiedlichsten Stellen für signifikante Vorteile – für den Rechenzentrumsbetreiber, die Kunden und letztlich auch die Umwelt. Ein Beispiel: Zum Speichern werden in den Rechenzentren Maschinen auf Servern platziert. Diese Maschinen haben bestimmte Größenanforderungen und es ist leicht vorstellbar, dass zwischen den einzelnen Maschineninstanzen immer wieder Kapazitäten frei sind, die man mit Speicher bestücken könnte. Diese Lücken lassen sich über KI ermitteln und dann sogar zu Geld machen. Amazon beispielsweise verkauft diesen Platz als „Spot-Instanzen" zu einem günstigeren Preis.

Hier zeigt sich, dass es heute nicht mehr ausreicht, ein Rechenzentrum sorgfältig zu planen und zu betreiben, sondern dass bestehende Prozesse und Prinzipien immer wieder – und zwar in immer kürzeren Zyklen – überdacht werden müssen. Menschen ist es kaum mehr möglich das oben genannte Szenario in einem festen Zeitraum zu überblicken und konsequent zu optimieren. Hier kann man heute schon auf Algorithmen vertrauen und deren Vorteile nutzen. So hilft etwa der von Red Hat mitentwickelte OptaPlaner, den Einsatz von Maschinen bestmöglich zu planen und immer wieder anzupassen: Die KI des OptaPlaners ist in der Lage, innerhalb kürzester Zeit freien Platz zu identifizieren und so für die optimale Auslastung zu sorgen.

Trends 2025

Trotz der intensiv genutzten Möglichkeiten lassen sich neue Trends identifizieren, die in den kommenden Jahren eine wichtige Rolle spielen werden, nicht zuletzt durch die CO^2-Steuer und Edge-Computing, was der Entwicklung der Rechenzentren einen enormen Schub verleihen wird. Zukünftig wird auch der Einsatz regenerativer Energien zunehmen, Wärme noch gezielter genutzt werden und die Etablierung von Stoffkreisläufen an Bedeutung gewinnen.

Dr. Dirk Goldner

> GRUNDSÄTZLICH KANN MAN SAGEN, DASS DER GROSSTEIL DER UNTERNEHMEN HEUTZUTAGE BEZÜGLICH EINER SICHEREN UND RECHTSKONFORMEN DATENSPEICHERUNG SENSIBILISIERT SIND.
>
> Dr. Dirk Goldner, Vorstand eurodata AG, www.eurodata.de

NEUE ANFORDERUNGEN AN DATA CENTER

RECHENZENTREN IN UND NACH DER PANDEMIE

Covid-19 trifft die Weltwirtschaft hart. Glück im Unglück haben Unternehmen, deren IT-Infrastrukturen flexibel und auf Krisen vorbereitet sind. Robuste und skalierbare Cloud- und Data-Center-Infrastrukturen sind hierfür häufig entscheidend und können Unternehmen deutliche Wettbewerbsvorteile bringen. Data-Center-Anbieter sollten sich entsprechend positionieren.

Noch vor 15 Jahren wären die wirtschaftlichen Auswirkungen der Corona-Krise deutlich stärker gewesen. Home-Office-Technologien wie Video-Konferenzen, ganz allgemein Kollaborations- und Kommunikationswerkzeuge und zu Grunde liegende Breitband-Internet-Anschlüsse konnten einen freien Fall der Wirtschaft bislang verhindern. Dabei wird ebenfalls klar: Die größten Herausforderungen der Unternehmens-IT haben sich weg vom Firmennetz in die Cloud und in Rechenzentren verschoben.

On-Premises-IT ist meist anfälliger für Extremsituationen. Vor allem bezüglich Robustheit und Skalierbarkeit kann sie nur selten mit hochgezüchteten Cloud-Plattformen und Rechenzentren mithalten. Dort laufen die immensen Datenmengen aller Firmen zusammen, dort sind Geschwindigkeit und Leistung besonders geschäftskritisch … und Corona hat diese Entwicklung nochmals beschleunigt.

Die Kernfrage für Data-Center-Anbieter: Wie differenziert man sich am besten für die Zeit nach Corona?

Übersicht der Anforderungen

Der Data Center Markt ist stark fragmentiert. Manche Rechenzentren buhlen um Kunden aus bestimmten Branchen oder Regionen (Retail Collocation), andere um Großkunden, Telekommunikationsanbieter oder Systemintegratoren (Wholesale) oder Kunden, die eine besonders hohe Konnektivität wünschen (High-Connectivity). Wieder andere fokussieren sich auf Cloud-Anbieter und Hyperscaler wie Azure, AWS oder Google Cloud. Dazu kommen Edge Data Center, die sich durch besondere Nähe zum Kunden positionieren.

Kernfrage für Data Center ist daher, welche Auswahlkriterien – neben dem Preis – von den verschiedenen Kundensegmenten angelegt werden. Data Center unterscheiden sich hinsichtlich (1) Sicherheit, Zuverlässigkeit und Reputation, (2) Standort, (3) Konnektivität, (4) Stromversorgung und Energieeffizienz sowie (5) Bereitstellungszeit. Für Data Center lohnt sich ein Blick auf diese fünf Kriterien, um die eigene Marktposition zu analysieren und entsprechende Strategien ableiten zu können. Hier ein kurzer Überblick:

1. Sicherheit, Zuverlässigkeit und Reputation

Sicherheit, Zuverlässigkeit und Reputation zählen offensichtlich zu den wichtigsten Aspekten im Rahmen der Evaluierung eines Data Centers – und zwar für alle Kundentypen. Die Bedeutung von Sicherheit zeigt sich unter anderem bei Cloud-Lösungen fürs Home-Office: Mit Telearbeit steigt das Risiko von Datenlecks, Rechenzentren sollten hier kein zusätzliches Risiko darstellen. Die Zu-

verlässigkeit ist generell hoch – die meisten Data Center haben heute eine gute Einstufung laut Uptime Institute („Tier 1-4"), aber ein einzelner Ausfall würde massive Auswirkungen auf Kundenzufriedenheit und Reputation haben. Und aus eben diesem Grund ist Reputation so entscheidend: Es ist schwer, Sicherheit und Zuverlässigkeit abschätzen zu können, Reputation ist meist der beste „Proxy". Die meisten Hyperscaler vertrauen beispielsweise einigen ausgewählten Anbietern mit hoher Reputation.

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

Matthias Hamel, Partner Altman Solon, www.altmansolon.com

2. Standort

Der Standort eines Data Centers ist der entscheidende Faktor für niedrige Latenzzeiten und damit oft für reibungsloses Arbeiten. Anders ausgedrückt: Je näher der Standort, desto geringer die Verzögerungen beim Datentransfer. Eine hohe Latenz wirkt sich vor allem dann negativ aus, wenn viele Datenanfragen schnell beantwortet werden müssen. Im Trend sind vor allem Edge Data Center, die näher / besonders nah beim Kunden positioniert sind. Der Standort ist auch von hoher Bedeutung für Retail-Colocation-Kunden, die eigene Server regelmäßig vor Ort warten müssen / wollen. Eine Fahrzeit von mehreren Stunden ist hier leicht ein Ausschlusskriterium. Entscheidend ist der Standort natürlich bezüglich gesetzlicher Vorschriften (DSGVO) und Compliance-Richtlinien. Bei entsprechenden IT-Anforderungen können sich nationale / lokale Anbieter klar differenzieren.

3. Konnektivität

Eine stabile Konnektivität ist offensichtlich die Voraussetzung, um Applikationen und Services performant, dauerhaft und sicher bereitzustellen. Dies ist besonders wichtig in Verbindung mit Telearbeit und vor allem bei Cloud Services und Remote Storage. Cloud-Anbieter nutzen hierfür voll-redundante Verbindungen, benötigen dafür aber mehrere unabhängige Glasfaseranbindungen zum Data Center. Data Center definieren sich seit langer Zeit gerne als „carrier-neutral", um Anbindung durch mehrere Glasfaseranbieter zu betonen. Für bestimmte IT-Aktivitäten werden Data Center bevorzugt, die durch viele dutzende internationale Telekommunikationsanbieter angebunden sind. Entsprechende „high-connectivity" Data Center genießen seit vielen Jahren eine attraktive Marktposition. Für Edge Data Center ist Konnektivität zu lokalen Internetanbietern natürlich entscheidend.

4. Stromversorgung und Energieeffizienz

Ein regional wenig wichtiger, aber überregional und international umso bedeutenderer Aspekt ist die Stromversorgung, die sicher / stabil, erweiterbar und vor allem günstig sowie zunehmend auch ökologisch sein sollte. Besondere Bedeutung hat dies für leistungshungrige Anwendungen wie High-Performance-Computing (HPC) oder Echtzeitberechnungen (bei denen oft Standort / Nähe ebenfalls entscheidend ist). Rechenzentren in Ländern mit günstigem Strom – vor allem durch Wasserkraft – und niedrigen Temparaturen können sich für Anwendungen, die höhere Latenz vertragen, besonders gut positionieren. Strom aus regenerativen Quellen ist zunehmend von besonderer Bedeutung. Neben der Versorgung spielt auch die Energieeffizienz des Data Centers eine wichtige Rolle. Bei den meisten neuen Rechenzentren liegt diese jedoch hoch, das heißt, es gibt weniger entsprechende Optimierungs- und damit auch Differenzierungspotentiale für Anbieter.

5. Bereitstellungszeit

Time-to-Market – hier ist die Zeit, bis ein Data Center einen Neukunden versorgen kann, gemeint – ist gerade in Zeiten schnell wachsender Cloud-Anbieter von zunehmender Bedeutung. Einige Cloud-Anbieter planen überaschend kurzfristig und suchen oft händeringend nach Data Centern, die sowohl den eigenen Standards entsprechen, die richtigen Anforderungen für den entsprechenden Use Case erfüllen, als auch baldmöglichst die benötigte Kapazität am richtigen Ort zur Verfügung stellen können. Kurze Bereitstellungszeiten – gepaart mit hoher Qualität – sind daher leicht ein Differenzierungsmerkmal für Großaufträge.

Fazit

Corona hat die Bedeutung von digitalen Infrastrukturen für Staaten, Unternehmen und Kunden deutlich erhöht. Für Unternehmen hat die Pandemie konkret offengelegt, wie relevant eine stabile, schnelle und zuverlässige IT-Infrastruktur ist, um am Markt bestehen und sich Wettbewerbsvorteile sichern zu können. Für Data Center Anbieter bedeutet dies höhere Wachstumspotentiale. Um diese Potentiale zu heben, muss sich ein Rechenzentrum möglichst optimal positionieren – am besten entlang der oben kurz vorgestellten fünf Kriterien.

Matthias Hamel

Lesen Sie mehr zum Thema Covid-19 und Remote-Arbeitsplatz unter
it-daily.net

KONSUMIEREN STATT SELBST SCHRAUBEN

IST EVERYTHING-AS-A-SERVICE DAS BETRIEBSMODELL DER ZUKUNFT?

Die IT muss heute schnell und flexibel auf neue geschäftliche Anforderungen reagieren. Das geht am besten, wenn Unternehmen für ihr Rechenzentrum die Einfachheit, Agilität und Wirtschaftlichkeit, die man von der Cloud kennt, mit den Sicherheits- und Leistungsvorteilen einer On-Premises-IT kombinieren.

Agilität und Flexibilität mit dem Ziel, den sich schnell ändernden Marktbedingungen gerecht zu werden, werden heute von Unternehmen als Selbstverständlichkeit angesehen. Sie wollen eine IT, die Ergebnisse liefert und sie dabei unterstützt, all ihre geschäftlichen Herausforderungen zu lösen. Das umfasst das Hoch- und Runterskalieren der Infrastruktur je nach Bedarf, die Auslagerung von Vermögenswerten aus der Bilanz und die Optimierung nicht genutzter IT-Ressourcen. Das traditionelle Investitionsmodell, bei dem alle drei bis fünf Jahre Hard- und Software ausgetauscht werden, ist vor diesem Hintergrund für viele Unternehmen nicht mehr sinnvoll. Realistische Prognosen über die IT-Auslastung über einen solch langen Zeitraum fallen schwer, und die Firmen sehen sich in der Folge mit einer Über- oder Unterdimensionierung bei der Bereitstellung konfrontiert: Kalkulieren sie zu knapp, steigt das Risiko, nicht schnell genug auf Veränderungen am Markt reagieren zu können. Immerhin müssen zunächst einmal Server-, Speicher- und Netzwerkressourcen beschafft und installiert werden. Auf der anderen Seite binden zu groß dimensionierte Reserven unnötig Kapital und verursachen laufende Kosten.

MIT EINEM MODERNEN AS-A-SERVICE-MODELL LASSEN SICH ALLE VORGABEN EINHALTEN UND GLEICHZEITIG DIE VORTEILE DER CLOUD IN PUNKTO FLEXIBILITÄT IM EIGENEN RECHENZENTRUM NUTZEN.

Benjamin Krebs,
General Manager Enterprise Germany,
Dell Technologies,
www.delltechnologies.com

IT as a Service kann die Lösung sein

Die immer schnellere Digitalisierung vieler Geschäftsmodelle sorgt außerdem dafür, dass die Datenmengen etwa durch das Internet der Dinge (IoT) kontinuierlich anwachsen – und damit die Anforderungen an die IT-Infrastruktur. Angesichts dieser Tatsache haben viele Unternehmen Teile ihrer IT in den vergangenen Jahren in die Cloud verlagert: Sie nutzt ein grundlegend anderes Modell, bei dem die IT-Ausgaben auf der Ressourcennutzung basieren, sodass Unternehmen schnell skalieren können und bei der Kapazität nicht auf Prognosen angewiesen sind. Trotz dieser Agilität und Self-Service-Funktionen erkennen mehr und mehr Unternehmen aber die Grenzen gerade der Public Coud. Sicherheit, Kontrolle und Governance sprechen nun einmal dafür, die wichtigen Workloads im eigenen Rechenzentrum vorzuhalten und damit Herr der Daten zu bleiben. Aus diesen Gründen suchen IT-Verantwortliche nach einer einfacheren Lösung: IT-as-a-Service ist ein Betriebsmodell, bei dem eine externe oder interne Organisation einem Unternehmen schlüsselfertige IT-Services bedarfsgerecht und zu transparenten Preisen bereitstellt. Die Akzeptanz für diese Art des IT-Konsums hat in den letzten Jahren deutlich zugenommen. Tatsächlich schätzen die Marktforscher von IDC, dass bis 2024 mehr als die Hälfte der Rechenzentrumsinfrastruktur über solche As-a-Service-Modelle genutzt und betrieben wird.

Moderne Angebote umfassen dabei den kompletten IT-Stack von Storage-, Server- und Networking-Lösungen über hyperkonvergente Infrastrukturen bis hin zu PCs. Everything-as-a-Service ist das Motto, das beispielsweise Dell Technologies unter dem Namen APEX vorantreibt. Die Ressourcen werden dabei vor Ort entweder im eigenen Rechenzentrum, an einem Edge-Standort oder bei einem Colocation-Anbieter installiert und beziehen Cloud-Funktionalitäten ein. Die Infrastruktur wird vom Unternehmen betrieben, aber vom Hersteller verwaltet. Das heißt, die Verantwortlichen müssen sich nicht mehr um Planung, Beschaffung, Wartung, Upgrades, Aktualisierungen oder Überwachung kümmern. Wichtigste Komponente von APEX ist eine zentrale Konsole: Über diese können Unternehmen mit wenigen Klicks die Ausführung

von Workloads anstoßen, ihre IT-Umgebungen verwalten, ihre Kosten in Echtzeit überwachen und benötigte Ressourcen hinzufügen. Neben den Workflows für die Provisionierung enthält dieses Self-Service-Portal auch Funktionalitäten für vorausschauende Analysen. Dadurch sind Unternehmen jederzeit in der Lage, ihre IT flexibel an neue Geschäftsanforderungen anzupassen. Gleichzeitig wird dank der umfassenden Einblicke das Risiko für Sicherheitsprobleme und Compliance-Verstöße minimiert.

Strenge Richtlinien, extreme Lastspitzen

As-a-Service-Modelle spielen ihre Vorteile da aus, wo traditionelle IT-Infrastrukturen an ihre Grenzen stoßen. In vielen Branchen üben beispielsweise neue Akteure mit grundlegend digitalen Businessmodellen einen großen Druck auf seit langem etablierte Unternehmen aus, wenn diese den digitalen Weg nicht schnell genug beschreiten. Gleichzeitig hat sich das Kundenverhalten verändert: Wer mit den Produkten und Dienstleistungen seines Anbieters nicht mehr zufrieden ist, wandert einfach zur Konkurrenz ab. Unternehmen müssen sich deshalb über innovative Angebote differenzieren, die wiederum flexible und skalierbare IT-Systeme voraussetzen. Neben hohen Ansprüchen an Performance und Verfügbarkeit kommt erschwerend hinzu, dass Organisationen etwa aus der Finanz- oder der Gesundheitsbranche einer strengen Regulatorik unterliegen. Rechenzentren, Managementsysteme und Prozesse müssen Audits erfolgreich durchlaufen und umfassend zertifiziert sein. Mit einem modernen As-a-Service-Modell lassen sich alle Vorgaben einhalten und gleichzeitig die Vorteile der Cloud in punkto Flexibilität im eigenen Rechenzentrum nutzen.

Ein anderes Beispiel sind saisonal bedingte Lastspitzen, wie sie etwa im E-Commerce und damit einhergehend in der Logistikbranche oder bei Versicherungsunternehmen Standard sind. Für Web-Shops und Zusteller läuft von Ende Oktober bis Anfang Dezember das Jahresendgeschäft. Zusätzlicher Traffic auf den Webseiten wird durch vertriebliche Rabatt- oder Gutscheinaktionen generiert. In dieser Zeit sind die IT-Systeme besonderen Belastungen ausgesetzt. Nicht anders sieht es bei Versicherungen aus, wenn Lastspitzen bei der Neueinstufung und dem Wechsel von Kfz-Policen zum Jahresende abgefedert werden müssen. Bei einem herkömmlichen Kaufmodell müssten die Unternehmen für diese Spitzenzeiten IT-Ressourcen vorhalten, die den Rest des Jahres weitgehend ungenutzt bleiben. Diese Überplanung führt zu Kosten und Kapitalbindung, ohne dass die Kapazitäten ständig gebraucht werden. Kalkulieren die Retailer, Logistiker oder Versicherer allerdings zu knapp, kommt es bedingt durch fehlende IT-Ressourcen zu Ausfällen und Verzögerungen in der umsatzstärksten Zeit.

Fakt ist, IT-as-a-Service bietet handfeste Vorteile: Unternehmen können sich stärker auf ihr Geschäft konzentrieren und Innovationen beschleunigen, indem sie den IT-Betrieb schnell an neue Geschäftsanforderungen anpassen und zu ihren Bedingungen effizient gestalten. Planung und Beschaffung der IT-Infrastruktur sowie Migrationszyklen werden vereinfacht. Gleichzeitig erfüllen die Unternehmen alle Anforderungen in Bezug auf Datenlokalisierung, behördliche Auflagen und Audits, während sich die IT-Mitarbeiter auf wertschöpfende Aktivitäten konzentrieren können.

Benjamin Krebs

Mehr zum Thema Rechenzentrum finden Sie hier:
it-daily.net

Bild: KIRCHHOFF Automotive

TRANSPARENTER ÜBERBLICK

WELTWEITER ROLL-OUT EINES STANDARDS FÜR DIE RECHNUNGSVERARBEITUNG

Der weltweit tätige Automobilzulieferer KIRCHHOFF Automotive nutzt die xSuite Rechnungsverarbeitungslösung als Werkzeug zur Vereinheitlichung der Prozesse in der Kreditorenbuchhaltung

KIRCHHOFF Automotive ist ein global präsenter Entwicklungspartner der Automobilindustrie und Komplettanbieter für komplexe Metall- und Hybridstrukturen für Rohkarosserie und Fahrwerk sowie Crash-Management-Systeme und Armaturentafelträger. Das seit 1785 bestehende Familienunternehmen gehört zur heutigen KIRCHHOFF Gruppe, die sich aus den Geschäftsbereichen KIRCHHOFF Ecotec, KIRCHHOFF Mobility und WITTE Tools zusammensetzt. Mit 9.000 Beschäftigten und 26 Produktionswerken in elf Ländern stellt KIRCHHOFF Automotive den größten Bereich der KIRCHHOFF Gruppe dar.

Bis vor einigen Jahren regelten die einzelnen Werke in den verschiedenen Ländern ihre Kreditorenbuchhaltung in Eigenregie, die Finanzabteilungen agierten mehr oder weniger autark. Die Unternehmensgruppe wächst stetig und erwirbt dabei neue Werke. Da bleibt es nicht aus, dass jeder Standort seine Rechnungsbearbeitung ein klein wenig anders handhabt, eigene Prozesse und Logiken etabliert. Etwa im Bereich der Transportrechnungen, wo die Prozesskette „Bestellanforderung in SAP generieren – genehmigen – Bestellung und Lieferung – anschließende Rechnung" – teilweise unterschiedlich durchgeführt wurde. Dies kann zu einem Mehraufwand führen, speziell wenn keine SAP-Bestellungen vorhanden sind. Denn dann stellt sich oft die Frage, wer für die Rechnungsfreigabe überhaupt verantwortlich ist. Oft gab jemand Bestellungen per Telefon auf, die sich dann nicht in SAP wiederfanden. Die Folge: Waren wurden angeliefert, die keinen Bestellbezug hatten, und die Suche ging los, zu wem die Rechnung nun gehört.

Gesamtüberblick über wichtige Kennzahlen

„Damit fiel eine Vergleichbarkeit schwer", sagt Martin Jonczyk, Global Consultant für die xSuite-Lösung bei KIRCHHOFF Automotive. „Die Durchlaufzeiten, bis eine Rechnung gebucht und freigegeben

wurde, waren sehr unterschiedlich. Mit Implementierung der Rechnungseingangssoftware wurde daher ein Kennzahlensystem aufgebaut. Hiermit werden jetzt diese Prozesse in den jeweiligen Werken verglichen, mit dem Ziel, Verschwendungen aufzudecken."

Um zu einer Prozessvereinheitlichung zu gelangen, führte das Unternehmen die Lösung zur Eingangsrechnungsverarbeitung der xSuite Group ein. „Besonders gut hat uns daran gefallen, dass die Validierung der Rechnungen innerhalb von SAP stattfindet. Das Preis-Leistungs-Verhältnis war sehr gut und auch der zwischenmenschliche Aspekt stimmte", so Martin Jonczyk.

Neues Financial Shared Service Center

Die Produktentscheidung fiel 2013. Seitdem wird die Software Stück für Stück in den einzelnen Landesgesellschaften ausgerollt, neue Funktionen kommen hinzu. Im Zuge der Implementierung baute KIRCHHOFF Automotive auch ein Financial Shared Service Center nahe Porto in Portugal auf. „Das dortige Werk war best-practice in den Prozessen. Dies konnten wir gut als Blaupause zur Vereinheitlichung verwenden, um künftig Synergie-Effekte zu nutzen", erklärt Martin Jonczyk, der die Implementierung der Rechnungsbearbeitungslösung von Beginn an koordinierte.

75 Prozent der Rechnungen als PDF

Ende 2020 war der Rechnungsworkflow in 13 Buchungskreisen aktiviert. Verarbeitet werden 250.000 Rechnungen pro Jahr weltweit, davon 80 Prozent bestellbezogene aus SAP MM, von denen wiederum 80 Prozent direkt gebucht werden, sofern es keine Preis- oder Mengendifferenzen gibt. 75 Prozent der Rechnungen treffen heute per E-Mail im PDF-Format ein und gehen an ein zentrales Postfach im Shared Service Center. Dort liest die xSuite-Software im ersten Schritt Kopfdaten aus und startet für die Kostenrechnungen aus SAP FI anschließend den Freigabeworkflow. An diesen sind weltweit mittlerweile 2.000 Personen angeschlossen. Sie kontrollieren die Rechnungen über ihren SAP-Account und geben sie anschließend frei. Die Verbuchung übernimmt die Software nach der letzten Freigabe. In einer nächsten Stufe sollen später auch die Positionsdaten ausgelesen werden.

Transparenter Überblick für Accounting-Fachkräfte

Die verbleibenden 25 Prozent in Papierform vorliegenden Rechnungen schicken die Lieferanten an das jeweilige Werk im Land, wo sie gescannt und an das Shared Services Center zur Weiterverarbeitung übermittelt werden. Lokale SAP-FI Key User unterstützen in den Werken die Endbenutzer und treiben wichtige Verbesserungen voran.

Per Mausklick können sich die Accounting-Fachkräfte einen transparenten Überblick verschaffen: Wie viele Rechnungen sind derzeit im Umlauf und wo befinden sie sich? Solche Informationen liegen heute standardisiert innerhalb des SAP Systems vor. Aus diesen vorhandenen Daten wurde ein externes zentrales Kennzahlensystem entwickelt, mit welchem Prozesse teilweise tagesgenau verglichen und analysiert werden können. Skontogewinne spielen durch nun rechtzeitige Zahlungen durchaus eine Rolle bei KIRCHHOFF Automotive, wenngleich sie laut Martin Jonczyk eher ein deutsches Thema sind. Doch auch die Auslandswerke profitieren, denn die Prozesse sind deutlich vereinfacht und Zahlungen erfolgen schneller. Noch viel wertvoller ist deshalb die Information, wieviel Arbeitsaufwand man in die Bearbeitung einer Rechnung stecken muss. Denn je einfacher der Prozess, desto mehr Rechnungen kann eine Person pro Stunde/Tag bearbeiten. Dies ist wichtig vor dem Hintergrund eines stetig wachsenden Rechnungsaufkommens, das KIRCHHOFF Automotive parallel zum wachsenden Geschäftsvolumen seit Jahren verzeichnet.

Ab Anfang 2021 will der Automobilzulieferer auch seine Werke in Mexiko an den Workflow anschließen, danach folgen die Werke in den USA und China. Und auch technisch will KIRCHHOFF Automotive noch stärker auf XML- bzw. EDI-Formate umsteigen. So lässt sich der Automatisierungsgrad nochmals steigern, die Validierung verbessert sich weiter.

Dina Haack | www.xsuite.com

Bild: KIRCHHOFF Automotive | Gene Schilling

MICROSOFT UNPLUGGED

MEHR WERT ODER KEIN MEHRWERT?

ICH VERSTEHE MICH ALS LIZENZOPTIMIERER. DAZU ZÄHLT AUCH, GÜNSTIGE ALTERNATIVEN ZU DEN VON MICROSOFT PROPAGIERTEN STANDARD-LÖSUNGEN AUFZUTUN.

Markus Seirer, Microsoft Licensing Professional, Vendosoft GmbH, www.vendosoft.de

2021 ist das Jahr, in dem Microsoft für Überraschungen sorgt. Entgegen seines Mantras, die Cloud sei die erstrebenswerteste Form der Software-Lizenzierung, bringt der Konzern gleich drei käufliche Lizenzen heraus: den Windows Server 2022, Office 2021 und Windows 11 – alle drei Schwergewichte in der microsoft'schen Produktpalette. Bekanntermaßen betreibt der Hersteller gern den Abgesang auf on-premises und propagiert seine Cloud. Was also hat es mit den Kauflizenzen auf sich? Warum die neuen Versionen? Wie innovativ sind sie wirklich, was ist für Unternehmen anders, gut… oder auch nicht?

Microsoft Windows Server 2022

Wie ein Zugeständnis mutet der Windows Server 2022 an. Denn dass er als on-premises-Variante kommt, muss wohl daran liegen, dass nach wie vor viele Unternehmen ihr Betriebssystem lokal installieren und möglichst wenige Anwendungen mit der Microsoft-Cloud verbinden wollen.

Den Windows Server 2022 wird es nur als LTSC-Version geben. Halbjährliche Channel-Releases sind nicht mehr vorgesehen. Dafür wird er fünf Jahre lang im Mainstream-Support und weitere fünf Jahre im Extended Support unterstützt. Bereitgestellt wird der Server als Standard, Datacenter und Datacenter Azure Edition. Die OEM-Version ist bereits gelauncht. Volumenlizenzen sollen ab Oktober handelbar sein. Alle zwei bis drei Jahre plant Microsoft nach eigener Aussage neue Versionen.

Das Programm basiert auf Windows 10 und bleibt auch optisch daran angelehnt, nicht etwa am neuen Betriebssystem Windows 11. Statt Microsoft Edge kommt in Zukunft Chromium-Edge zum Einsatz.

Die neuen Funktionen bieten vor allem einen verbesserten, mehrschichtigen Schutz gegen Cyber-Bedrohungen, zusätzliche Sicherheitsebenen für die sichere Konnektivität zu geschäftskritischen Ressourcen und die standardmäßig aktivierte Unterstützung für HTTPS und TLS 1.3. Mit Azure Arc kann der Windows Server 2022 vor Ort verwaltet und gesteuert werden. Virtuelle Maschinen können dank neuem Windows Admin Center besser betreut werden. Hier lassen sich auch .NET-Anwendungen mit dem neuen Containerisierungs-Tool aktualisieren. Soll von on-premises nach Azure migriert werden, unterstützt dies der Storage Migration Service. Last but not least sorgen reduzierte Image-Größen der Container-Anwendungen für einen schnelleren Download und eine vereinfachte Implementierung von Netzwerkrichtlinien. Nicht ganz klar ist bisher, ob das Hosting von Hyper-V-Plattformen in virtuellen Maschinen weiterhin in der Standardedition enthalten sein wird oder nur in der Enterprise-Variante. Wer es nutzt, für den wäre das durchaus ein Problem. Denn Hyper-V müsste mit dem Windows Server 2022 über Azure laufen, was zu explodierenden Kosten führen kann.

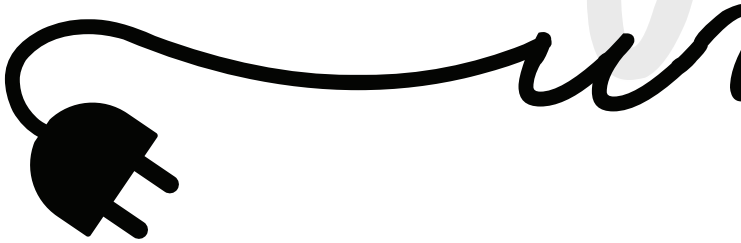
Microsoft Office 2021

Kommen wir zu Office. Auch hier erstaunte zunächst die Ankündigung, dass auf Office 2019 noch weitere on-premises-Versionen folgen. Dass es sie gibt, ist wie beim Windows Server sicher ein Hinweis auf die anhaltend große Nachfrage nach lokal installierten Computerprogrammen.

Microsoft Office 2021 für Unternehmen kommt ab 5. Oktober 2021 in den Editionen Standard und Professional Plus auf den Markt. Beide beinhalten OneNote und Teams, wobei noch nicht klar ist, ob deren Nutzung kostenfrei sein wird. So weit, so gut.

Unschön hingegen, dass Microsoft die Preise der Kauflizenz gegenüber Office 2019 anhebt – im Raum stehen 10 Prozent – und gleichzeitig die Supportlaufzeit von sieben auf fünf Jahre verkürzt. Auch Office 2021 wird es nur als LTSC-Edition geben. Das entspricht im Prinzip einer heutigen Office-Lizenz ohne Software Assurance.

Es scheint, als statte Microsoft das neue on-prem-Office stiefmütterlicher aus als seine Cloud-Pläne. Fragt sich, warum dann



upgraden? Tatsächlich bestünde der nennenswerteste Vorteil im integrierten Teams. Doch für Unternehmen, die dies mit bestehenden Office-Paketen nutzen wollen, gibt es bereits eine kostengünstige Lösung: Die Kombination von Office 2019 ProPlus mit M365 Business Basic, wie es der Microsoft Gold Partner VENDOSOFT vorschlägt. Wer dennoch über ein Upgrade nachdenkt, ist mit Blick auf die Funktionalitäten und Support-Laufzeiten ebenso gut mit Office 2019 und 2016 beraten. Preislich sowieso – denn beide gibt es weit unter dem Neupreis für Office 2021 gebraucht zu kaufen!

Microsoft Windows 11

Lange Zeit hieß es aus der Firmenzentrale in Redmond, eine Nachfolge für Windows 10 sei nicht geplant. Schon deshalb kam die Ankündigung zu Windows 11 überraschend. Nach Startschwierigkeiten im Juni soll das neue Betriebssystem ab Oktober 2021 ausgerollt werden.

In Bezug auf seine Funktionalität ist Windows 11 kein Quantensprung gegenüber dem Vorgänger – eher eine Iteration. Verbessert wurden die Benutzeroberfläche und das Startmenü. Sie muten nun ein wenig Apple-like an, orientieren sich jedenfalls eindeutig am Marktbegleiter. Optisch und/oder funktional neu sind abgerundete Ecken, modernere Icons und ein neuer Widgets-Bereich. Snap-Gruppen und Snap-Layouts bieten mehr Flexibilität und Wahlmöglichkeiten bei der Einrichtung eines Displays mit mehreren Fenstern. Über den neu gestalteten Microsoft Store können neuerdings auch Android-Apps installiert werden. Sie stammen aus dem App Store von Amazon. Das bedeutet zwar mehr Reichweite als bisher. Aber weniger als sie beispielsweise Google Play bietet. Auch ist die Anmeldung auf einem Amazon-Konto notwendig, um die Apps herunterzuladen.

Hardware-seitig benötigt Windows 11 Prozessoren, die ungefähr ab 2016/2017 hergestellt wurden (für Intel-PCs ab 8. Pentium- und Atom-Chips). Microsoft begründet dies mit den Sicherheits-Features, die Prozessoren erst seit diesem Zeitpunkt bieten. Auch eine Unterstützung für TPM (Trusted Platform Module) ist obligatorisch.

Damit sind wir bei den Nachteilen angekommen. Für ältere Geräte ist eine Installation mit Windows 11 uninteressant oder extrem kostspielig. Wie gewohnt wird es regelmäßig Sicherheits-Updates geben. Feature Updates sind jedoch nur noch einmal im Jahr vorgesehen, anstatt wie bisher zweimal jährlich.

Positiv wäre zu bewerten, wenn in das neue Betriebssystem tatsächlich Microsoft Teams eingebacken wurde. Hierzu gibt es jedoch noch keine offiziellen Angaben. Denkbar – und wahrscheinlicher – ist, dass Teams vorkonfiguriert ist, aber nicht im Preis enthalten.

Fragt sich, ob Windows 11 Unternehmen einen echten Mehrwert bietet? Das eher nicht. Microsoft hat keine grundlegenden Änderungen vorgenommen und hätte ebenso gut seine Updates für Windows 10 fortsetzen können. Es geht gar das Gerücht, der Konzern sei von den Microsoft Partnern zu einer neuen Version gedrängt worden. Dahinter steht wohl die Hoffnung, mehr Hardware verkaufen zu können, auf der das neue Betriebssystem installiert wird.

ALS KOMMUNIKATIONSVERANTWORTLICHE HINTERFRAGE ICH DIE SINNHAFTIGKEIT VON SOFTWARE-NEUHEITEN AUS DEM HAUSE MICROSOFT, BEVOR ICH SIE KOMMUNIZIERE.

Angelika Mühleck, Leitung Kommunikation, Vendosoft GmbH, www.vendosoft.de

Fragwürdige Intention

Mit den Kauflizenzen Windows Server 2022, Office 2021 und Windows 11 scheint sich Microsoft am Bedarf derjenigen Unternehmen und Organisationen zu orientieren, die es nicht in die Cloud zieht. Doch meint man zu spüren, dass die neuen On-Prem-Produkte weniger ‚kommod' daherkommen sollen als ihre Pendants aus der Cloud. Kaum oder nur unwesentliche Funktionsverbesserungen zeugen davon. Aber auch eingeschränkte Flexibilitäten und das Entfernen von Bausteinen, die in früheren Versionen enthalten waren. Wer diese weiterhin nutzen will (und darauf meist angewiesen ist), den erwarten kostspielige Workarounds. Ein Schelm, wer Böses dabei denkt…

Markus Seirer, Angelika Mühleck

ZUKUNFTSMUSIK ODER REALITÄT?

STANDARDISIERUNG VON INDUSTRIE-4.0-LÖSUNGEN

NUR, WENN ALLE MASCHINEN SYSTEMÜBERGREIFEND MITEINANDER KOMMUNIZIEREN KÖNNEN, IST EINE ENTSPRECHEND FLEXIBLE PRODUKTION ÜBERHAUPT MÖGLICH.

Frank Schnicke, Expert „Industrie 4.0 System Architectures" am Fraunhofer-Institut für Experimentelles Software Engineering IESE, www.iese.fraunhofer.de

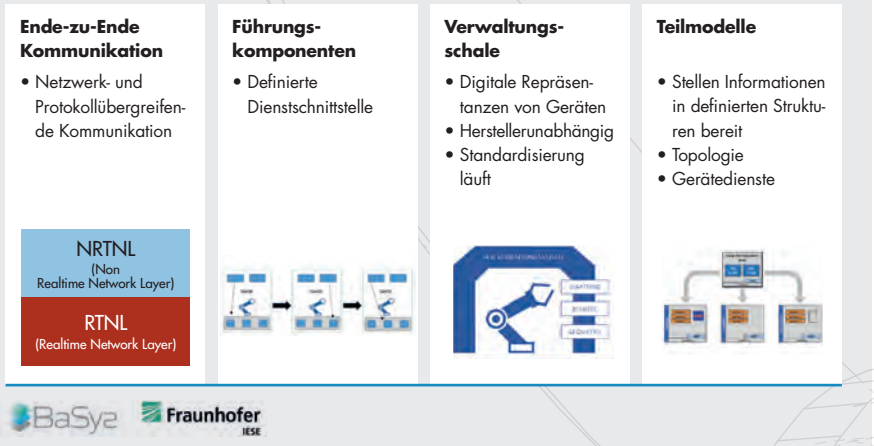
Ohne Standards ist die vierte industrielle Revolution nicht denkbar – davon ist nicht nur Bundesforschungsministerin Anja Karliczek überzeugt. Auch das Fraunhofer-Institut für Experimentelles Software Engineering IESE hat sich schon seit Langem intensiv mit einer standardkonformen Industrie-4.0-Middleware beschäftigt – und in diesem Jahr den Durchbruch geschafft.

Um verstehen zu können, warum die Normierung von Produktions- und Prozessdaten im Kontext rund um Industrie 4.0 von so großer Bedeutung ist, hilft der Vergleich zur Logistikbranche: Nachdem im Januar 1968 erstmals eine ISO-Norm die Abmessungen und Typenbezeichnungen des weltweiten Standard-Seecontainers definiert hatte, trat dieser daraufhin seinen Siegeszug rund um den Globus an. Auch in der digitalen Welt können Standards und Normen dazu beitragen, die Transformation der Wirtschaft wesentlich schneller, sicherer und somit kostengünstiger voranzutreiben.

Ein solcher Katalysator ist auch dringend notwendig, denn: Die Mehrheit der hiesigen Firmen ist noch immer weit von der Industrie-4.0-Ziellinie entfernt. Laut dem aktuellen „Digitalisierungsindex Mittelstand 2020/21" kommen die Industrieunternehmen derzeit nur auf 62 von 100 möglichen Punkten hinsichtlich ihres Digitalisierungsgrades. Berücksichtigt man zudem die Tatsache, dass die vierte industrielle Revolution weit über die bloße digitale Transformation von Produktionsprozessen hinausgeht, würde das Ergebnis sicherlich noch erschreckender ausfallen.

Industrie 4.0 sieht vielmehr vor, eine durchgängige Vernetzung aller Maschinen zu erzielen. Denn nur, wenn alle Maschinen systemübergreifend miteinander kommunizieren können, ist eine entsprechend flexible – und somit wandelbare – Produktion überhaupt möglich. Für diesen Schritt ist es jedoch notwendig, das Vertrauen der Firmeninhaberinnen und -inhaber zu erwerben, sodass diese auch bereit sind, die Transformation einzuleiten.

BaSys 4.0 BAUSTEINE – WORAUS BESTEHT BaSys 4.0?



Meilenstein in der Industrie-4.0-Geschichte

Abhilfe kann hier vor allen Dingen die Standardisierung der entsprechenden IT-Lösungen schaffen – ein Thema, das Expertinnen und Experten schon seit vielen Jahren umtreibt und nun endlich in greifbare Nähe gerückt ist. Die Rede ist vom sogenannten 1.0 Release der Eclipse BaSyx Middleware basierend auf den Spezifikationen der Plattform Industrie 4.0. Zugegeben, der Name klingt abstrakt und lässt sich keineswegs in nur einem Satz erklären. Eines sei an dieser Stelle jedoch schon vorweggenommen: Der Release markiert einen bedeutenden Meilenstein in der Industrie-4.0-Geschichte der Bundesrepublik und könnte die digitale Transformation ab sofort endlich in die Breite tragen.

Zum Hintergrund: Das Bundesministerium für Bildung und Forschung hatte bereits Mitte 2016 gemeinsam mit 14 weiteren Partnern aus Wirtschaft und Forschung das Projekt „Basissystem Industrie 4.0"

(kurz: BaSys 4.0) ins Leben gerufen. Die Konsortialleitung hat seitdem das Fraunhofer-Institut für Experimentelles Software Engineering IESE in Kaiserslautern inne. Ziel des Forschungsprogramms war es, ein Technologiesystem für Produktionsanlagen zu entwickeln, das die effiziente Wandelbarkeit eines Herstellungsprozesses als zentrale Herausforderung der vierteln industriellen Revolution realisiert.

Der Plan wurde inzwischen in die Tat umgesetzt. Mit der „BaSys 4"-Middleware hat das Konsortium eine Referenzarchitektur entwickelt und mit der Referenzimplementierung Eclipse BaSyx einfach umsetzbar gemacht. Dadurch wird die Umstellung der Unternehmen auf eine wandelbare Produktion breitenwirksam ermöglicht. Dafür ist es zunächst notwendig, die Datenmodelle und Protokolle so aufzubereiten, dass sie interoperabel sind – also miteinander „kommunizieren" können.

Überführung in eine einheitliche Sprache

Ein Beispiel: Angenommen eine Firma steht bei der Transformation noch gänzlich am Anfang, so muss beispielsweise zuerst der Shopfloor mit dem Officefloor verknüpft werden. Mit Hilfe des im Rahmen des Forschungsprojekts entwickelten sogenannten Virtual Automation Bus (VAB) wurde eben dafür ein Konzept entwickelt, das eine netzwerk- und protokollübergreifende Peer-to-Peer-Kommunikation zwischen den Produktionsmaschinen und der IT Wirklichkeit werden lässt.

Liegen auf diese Weise sämtliche Daten einer Maschine digital vor, geht es anschließend darum, diese in eine gemeinsame Form „zu gießen". Denn: Eine einheitliche Sprache ist DIE Grundvoraussetzung, um die Produktionsanlagen vernetzen zu können. Für den Sprach-Transfer aller Daten sieht BaSys 4 das Prinzip der Verwaltungsschalen vor.

Hierbei handelt es sich um fest spezifizierte Digitale Zwillinge, die entsprechend einer einheitlichen Struktur aufgebaut sind. Jede Verwaltungsschale enthält Teilmodelle, die sowohl den Zustand eines realen Assets virtuell abbilden als auch bei Bedarf Live-Daten über diese zur Verfügung stellen. Der Clou dabei: Die Verwaltungsschalen können nicht nur an andere Unternehmen weitergegeben werden; die der Standardisierung zugrunde liegenden Spezifikation ist offen und jederzeit einsehbar.

Plant ein Unternehmen nun schließlich, eine effiziente Losgröße-1-Fertigung zu realisieren, hält BaSys 4 das Konzept der Führungskomponenten bereit. Jedes Gerät erhält dadurch eine einheitliche Dienstschnittstelle – nämlich indem die Ausführung von Produktionsprozessen von Produktionsdiensten getrennt wird. Zudem wird jede Fähigkeit einer Maschine ausreichend exakt beschrieben, sodass eine Fertigungsanlage möglichst einfach und effizient auf die Herstellung einer Sonderanfertigung umgestellt werden kann. Damit die „BaSys 4"-Middleware möglichst vielen Unternehmen die digitale Umstellung erleichtern kann, steht die Referenzimplementierung den Firmen Open Source zur Verfügung.

1.0 Release – ein Versprechen

Doch worum handelt es sich nun genau beim 1.0 Release? Dieser enthält ein Versprechen: Die Middleware macht es ab sofort möglich, die im Rahmen der vom Bundeswirtschaftsministerium 2013 gegründeten „Plattform Industrie 4.0" entwickelten Spezifikationen flächendeckend und standardkonform umzusetzen. Als ein Teil der Plattform hat sich hierbei die Arbeitsgruppe „Referenzarchitekturen, Standards und Normung" in den vergangenen Jahren eingehend mit der Entwicklung offener und einheitlicher Standards für die Industrie 4.0 beschäftigt.

Diese sollen sowohl einen fairen Wettbewerb sichern als auch die Investitionsrisiken für Unternehmen senken. Die Standards schließen sämtliche Bereiche einer vernetzten Produktion mit ein: Hard- und Software, Anwender- und Anbieterbranchen sowie Produktdesign bis -recycling. Dank des 1.0 Release sind ab sofort nun auch sämtliche Schnittstellen der Eclipse BaSyx Middleware stabil und die Kompatibilität zu zukünftigen Updates gegeben. Dadurch haben die Unternehmen die Garantie, auch zukünftige Features und Updates ohne Änderungen an bestehendem Code integrieren zu können.

Frank Schnicke

DEVSECOPS PIPELINE

EVERYTHING-AS-CODE – ANYTHING SECURE? QUO VADIS?

Die Softwareentwicklung befindet sich im Umbruch: Beflügelt durch die digitale Transformation erscheinen agile Konzepte und DevOps Ansätze unumgänglich, um mit den Anforderungen eines sich immer schneller verändernden Marktumfeldes Schritt halten zu können. Die aktuelle Corona-Situation hat diesen Trend in den letzten Monaten sogar noch verschärft. Der Druck auf Unternehmen, innerhalb kürzester Zeit flexible digitale Geschäftsmodelle voranzutreiben, steigt und wird zum kritischen Erfolgsfaktor im globalen Wettbewerb.

Gleichzeitig durchdringt Quellcode zunehmend etablierte Systemlandschaften und -architekturen. Der Trend scheint klar: „Everything is code and code is law".

Aus großer Macht folgt große Verantwortung

Mit diesem Bedeutungszuwachs einhergehend wächst jedoch auch die Verantwortung von Softwareentwicklern in Hinblick auf nicht-funktionale (Security-)Anforderungen. Denn auch die Anzahl von Cyber-Attacken und Sicherheitsvorfällen steigt seit Jahren kontinuierlich. Es stellt sich die Frage, wie gut Entwickler von heute in Bezug auf die Schaffung der zukunftsfähigen und sicheren Infrastrukturen von morgen vorbereitet sind.

Ein guter Indikator hierfür ist das Top 10 Projekt der OWASP Foundation, welches die kritischsten Schwachstellen in Web Applikationen in regelmäßigen Abständen dokumentiert.

Der direkte Vergleich des aktuellen Release mit der vorherigen Version des Benchmarks stimmt aus Security Sicht leider nur bedingt optimistisch:

KRITISCHE SCHWACHSTELLEN IN WEB APPLIKATIONEN

OWASP Top 10 – 2013	→	OWASP Top 10 – 2017
A1 – Injection	→	A1:2017 – Injection
A2 – Fehler in Authentifizierung und Session Mgmt	→	A2:2017 – Fehler in der Authentifizierung
A3 – Cross Site Scripting (XSS)	↘	A3:2017 – Verlust der Vertraulichkeit sensibler Daten
A4 – Unsichere direkte Objektreferenzen [mit A7]	U	A4:2017 – XML External Entities (XXE) [NEU]
A5 – Sicherheitsrelevante Fehlkonfiguration	↘	A5:2017 – Fehler in der Zugriffskontrolle [vereint]
A6 – Verlust der Vertraulichkeit sensibler Daten	↗	A6:2017 – Sicherheitsrelevante Fehlkonfiguration
A7 – Fehlerhafte Autorisierung auf Anw.- Ebene [mit A4]	U	A7:2017 – Cross-Site Scripting (XSS)
A8 – Cross Site Request Forgery (CSRF)	☒	A8:2017 – Unsichere Deserialisierung [NEU, Community]
A9 – Nutzung von Komponenten mit bekannten Schwachstellen	→	A9:2017 – Nutzung von Komponenten mit bekannten Schwachstellen
A10 – Ungeprüfte Um- und Weiterleitungen	☒	A10:2017 – Unzureichendes Logging Moniting [NEU, Community]

(Quelle: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf

DIE WICHTIGSTEN SCHRITTE ZUM AUFBAU EINER SICHEREN CI-/CD-PIPELINE SIND UND BLEIBEN DER WISSENSAUFBAU IM BEREICH SECURITY BEI ALLEN INVOLVIERTEN SOFTWAREENTWICKLERN SOWIE DIE SENSIBILISIERUNG FÜR RISIKEN UND SCHWACHSTELLEN.

Jan Sudmeyer, Managing Partner, carmasec GmbH & Co.KG, www.carmasec.com

Auch wenn sich das Risikoprofil in einigen Bereichen verbessert oder zumindest verschoben hat, zählen zum Beispiel Cross-Site Scripting (XSS) und die Nutzung unsicherer (3rd Party) Komponenten noch immer zu den häufigsten Schwachstellen moderner Web Applikationen.

Dies mag einerseits auf fehlende Expertise oder mangelndes Bewusstsein für Sicherheitsaspekte innerhalb der Softwareentwicklung zurückzuführen sein. Andererseits nehmen jedoch auch die Komplexität und technische Abhängigkeiten rasant zu, so dass sich das Gesamtbild teilweise nur noch schwer überblicken lässt. Zudem werden Dienste in modernen Architekturen durch das Zusammenspiel einer Vielzahl von Microservices erbracht, die häufig von verschiedenen Entwicklerteams oder Drittanbietern beigesteuert werden.

Was tun?

Die wichtigsten Schritte zur Bewältigung dieser Herausforderungen sind und bleiben die Sensibilisierung für Risiken und Schwachstellen sowie der Wissensaufbau im Bereich Security bei allen involvierten Softwareentwicklern. Weiterhin sollten Security-Tools möglichst frühzeitig in die CI/CD Pipeline integriert werden („Shift Left").

Die Zusammenstellung eines geeigneten Security-Toolsets gestaltet sich nicht ganz trivial: Zwar existiert schon eine Vielzahl von Lösungen für die verschiedenen Phasen des Entwicklungszyklus, einen groben Überblick der gängigsten Tools bietet beispielsweise die Checkliste zum Thema „Cloud Security DevSecOps Practices" des SANS Institute. Dabei handelt es sich jedoch vielfach um Insellösungen.

Die Auswahl und Integration geeigneter Tools ist häufig schwierig. Dieser Herausforderung stellen wir uns im zweiten Teil dieses Artikels.

Der Use Case

In unserem Lab-Projekt zeigen wir auf, wie sich die Sicherheit von Sourcecode mit einfachsten Mitteln und Open Source Tools erhöhen lässt. Wir erläutern unser Vorgehen dabei Schritt für Schritt, sämtliche Ressourcen stehen als GitLab-Repository zur Verfügung:

https://gitlab.com/carmasec_public/Everything-as-Code-Anything-secure

DIE INTEGRATION EINES BASISSETS VON (OPEN SOURCE) SECURITY-TOOLS MUSS NICHT AUFWÄNDIG SEIN. SIE LÄSST SICH BEREITS MIT EINFACHEN MITTELN IN DER ENTWICKLUNGSPIPELINE REALISIEREN UND LIEFERT DABEI EINEN KLAREN MEHRWERT.

Kevin Kloft, Security Solution Architect, carmasec GmbH & Co.KG, www.carmasec.com

Der Aufbau unserer Lab Umgebung ist dabei wie folgt:

Für unser Demo-Lab verwenden wir exemplarisch ein Sourcecode Management Tool sowie einen Sourcecode Scanner. Wir wählen in diesem Fall die Tools GitLab und SonarQube. GitLab ist in der Community Edition kostenfrei verfügbar und bringt von Haus aus nützliche Funktionalitäten wie zum Beispiel Continuous Integration (CI) ein. Auf diese Weise kann eine YAML-Datei im eigenen Projektordner abgelegt werden.

SonarQube ist in der Community Edition ebenfalls ein frei verwendbares Tool und bietet eine große Diversität unterstützter Programmiersprachen.

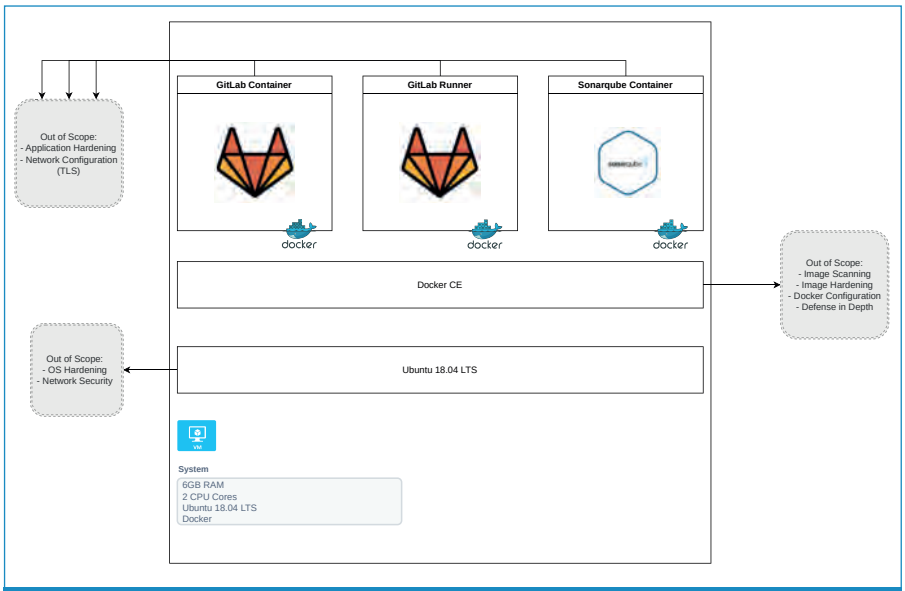


Bild 2: Architekturdiagramm

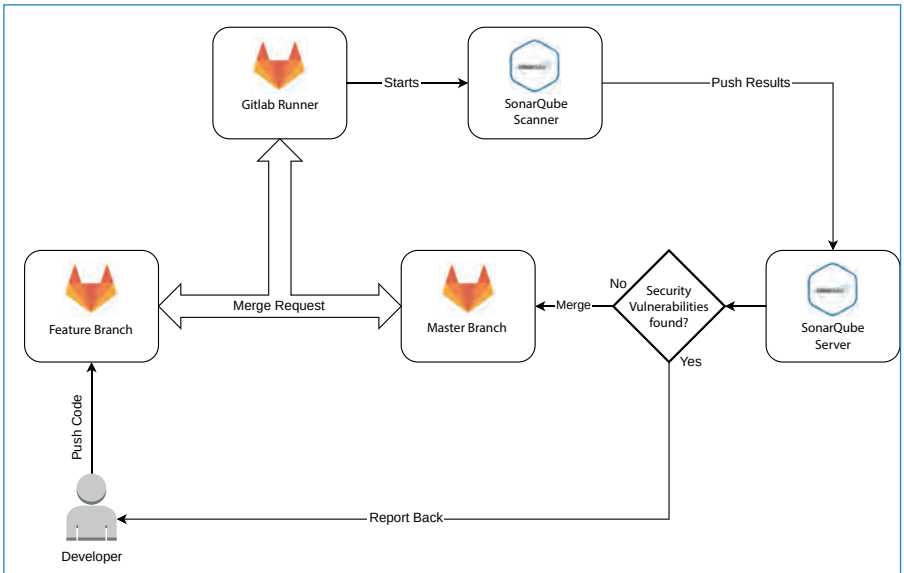


Bild 3: Flussdiagramm

Der Scope

Dieses Lab legt den Fokus sehr stark auf die automatisierte Überprüfung der Sicherheit von Sourcecode. Zur Vereinfachung werden folgende Themen nicht berücksichtigt (siehe auch Architektur-Diagramm):

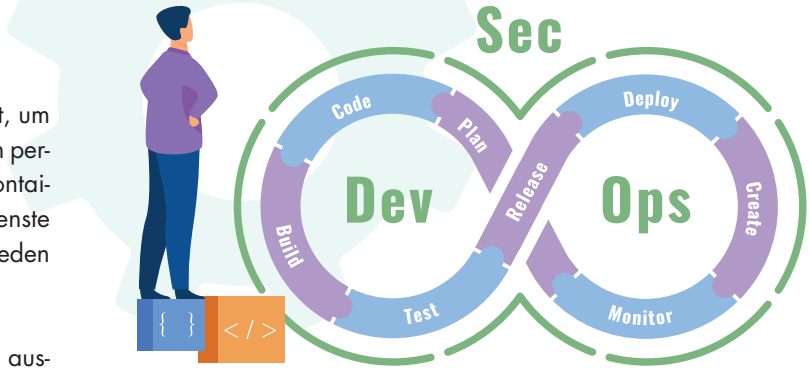
- OS Hardening
- Network Hardening
- Container Security
- Application Security

Das Deployment

Für das Deployment der Artefakte des Labs wird Ansible verwendet. Hierzu wird ein Ansible Playbook erstellt, welches folgende Funktionen erfüllt:

- Updaten des Systems
- Entfernen der vorinstallierten Docker Version
- Installieren der Docker Community Edition
- Anlegen eines Docker Users
- Kopieren von Bash-Scripten auf das Zielsystem
- Ändern der Berechtigung der Bash-Scripte

Die Bash-Scripte erfüllen verschiedene Aufgaben im Zusammenspiel mit den Docker-Containern. Ein Script kopiert die aktuellsten Images, welche für das Lab benötigt werden, von Docker Hub: Dies sind zum einen GitLab, des Weiteren GitLab Runner sowie SonarQube Server. Ein vorheriges manuelles Herunterladen des SonarQube Scanners ist nicht erforderlich, da dies durch die CI-Funktionalität von GitLab automatisch durchgeführt wird.



Die übrigen Scripte werden benötigt, um die Container auszuführen und einen persistenten Speicher innerhalb der Container zuzuweisen, sowie für die Dienste entsprechende Ports zu setzen und jeden Container eindeutig zu benennen.

Zusätzlich wird ein weiteres Script ausgeliefert, welches den GitLab-Runner konfiguriert. Dazu muss zunächst innerhalb von GitLab ein Runner-Token erstellt werden, welches anschließend dem Script weitergegeben und somit der Runner GitLab zugewiesen wird.

Die Besonderheit einer containerisierten GitLab Instanz ist die Portzuweisung. Am Anfang des Projektes traten häufiger Probleme mit git-Befehlen auf der Konsole auf, sofern GitLab nicht der Standard SSH Port 22 zugewiesen wurde. Daher entschließen wir uns, dem Host System einen alternativen SSH Port zuzuweisen und GitLab auf dem Standard SSH Port zu nutzen.

Projekte, Projekte, Projekte

Um ein Repository scannen zu können, muss zunächst ein SonarQube Projekt angelegt und ein Project Key vergeben werden. Anschließend wird ein Token generiert. Dies geschieht durch Vergabe eines Token Namens, zu dem SonarQube einen alphanumerischen String erzeugt.

Als nächstes muss im Projektordner die Konfigurationsdatei sonar-project.properties angelegt werden. Diese enthält insbesondere die Parameter Project.Key und Project.Name. Ohne diese generiert SonarQube eine Fehlermeldung. Weiterhin muss zwingend die Quelle (das heißt der Pfad zum Sourcecode) spezifiziert werden. Zusätzlich können noch weitere Eigenschaften wie Kodierung und Programmiersprache konfiguriert werden, was jedoch in unserem Fall nicht erforderlich ist.

Das Anlegen der Konfigurationsdatei sonar-project.properties ist ebenfalls nicht zwingend notwendig: Alternativ können die Werte Project.Key und Project.Name auch in GitLab selbst hinterlegt und anschließend in der .gitlab-ci.yml zugewiesen werden.

Die .gitlab-ci.yml

Das Herzstück der Automatisierung dieses kleinen Labs bildet die in YAML geschriebene Datei .gitlab-ci.yml. Für diesen Anwendungsfall ist die Komplexität minimal gehalten, alle Anweisungen werden vom GitLab-Runner ausgeführt.

In diesem simplen Fall sucht der GitLab-Runner das Sonar-Scanner-Image auf Dockerhub, sofern es nicht bereits lokal vorliegt. Hier kommt das alphanumerische Token zum Einsatz, welcher an den Scanner übergeben wird. Zusätzlich muss die Host-Adresse von SonarQube angegeben werden, um nach dem Scan die Ergebnisse auf den Server zu pushen. Nachdem dies ausgeführt wurde, beendet sich der Container mit dem Sonar-Scanner wieder automatisch und wird erst dann erneut gestartet, wenn ein neuer Merge-Request auf den Master aufgeführt wird.

Ausblick

Wie oben erwähnt sind einige Security-Best-Practices, wie die Härtung von Betriebssystem und Netzwerk, hier nicht berücksichtigt.

Auch dieser Ausblick fokussiert daher eher den horizontalen Ausbau rechts und links der im Architekturdiagramm skizzierten Lösung. Beginnen wir mit der Betrachtung des „Links“:

Dem Sourcecode Management Tool vorgelagert sitzt im Normalfall der Editor oder die IDE des Entwicklers. Hier können verschiedene Plugins genutzt werden, um zum Beispiel implementierte Kryptographie zu identifizieren und festzustellen, ob die Schlüssellänge richtig gewählt ist. Somit können Sicherheitsmängel sofort behoben werden. Danach erfolgt ein Commit und gegebenenfalls der Merge-Request und ein automatischer SonarQube-Scan.

Dem Lab nachgelagert (gedanklich rechts von unserer Lösung) sind andere Sicherheitsfeatures eingereiht, etwa ein eigenes Image Repository und ein Image Vulnerability Scanner. Somit kann sichergestellt werden, dass die Security-Abteilung diese Images vorab überprüfen kann, bevor Entwickler diese nutzen. Auch hier ist Kommunikation zwischen den Abteilungen sehr wichtig.

Zu guter Letzt sollen weitere nicht-funktionale Tests noch Erwähnung finden: Ebenso wie funktionale- und End-to-End Tests können auch einige Security Tests automatisiert durch Scanner und andere Tools durchgeführt werden. Diese sind nicht nur hilfreich für die Entwickler, sondern auch für die Operatoren, da auch Konfigurationen mit in diese Tests einbezogen werden.

Fazit

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

Wie so oft führen viele Wege zum Ziel und jede Reise beginnt mit dem ersten Schritt.

Jan Sudmeyer, Kevin Kloft

PROJEKTE STARTEN MIT DESIGN THINKING

GUTE VORBEREITUNG IST ALLES

Projekte haben einen Auftraggeber, ein klares Ziel und einen abgegrenzten Umfang („Scope"), ein eindeutiges Start- und Enddatum, ein Budget und ein Team. Es sind einmalige, noch nie dagewesene Vorhaben. Das jedenfalls sagt die Theorie. Aber wie läuft es in der Praxis? Und wie kann Design Thinking helfen? Werfen wir dafür einen Blick auf die Geschichte von Max - eine zugegebenermaßen fiktive Geschichte, die nichtsdestotrotz auf wahren Begebenheiten beruht.

Wie ein Projekt beginnt, bevor es anfängt

Max ist Assistent der Geschäftsführung in einem mittelständischen, global agierenden Industrieunternehmen. Kürzlich hat ihn der Marketingleiter beiseite genommen. Er erzählt Max, dass die meisten Kontakte zu Neukunden inzwischen online geknüpft werden, diese aber nicht immer zufrieden seien mit der User Experience und dem Content der Online-Services. Um das volle Potenzial auszuschöpfen, müssten Länder-Websites, Online-Shop und Backend-Prozesse jetzt dringend überarbeitet werden. Der Marketingleiter eröffnet Max, dass er im anstehenden Strategie-Workshop der Geschäftsführung darauf drängen wird, ein bereichsübergreifendes Projekt für den Relaunch der Online-Services zu initiieren. Er fragt, ob Max das Projekt nicht übernehmen könnte. Max ist sofort Feuer und Flamme. Endlich kann er zeigen, was er in seinem Studium gelernt hat. Um sich auf die neue Aufgabe vorzubereiten, entwirft er umgehend den groben zeitlichen Ablauf des Projekts.

Im Strategie-Workshop steht das Thema Website-Relaunch ganz oben auf der Agenda. Die Webstatistiken, direkte Kundenfeedbacks, aber auch die vermeintlichen Erfolge und Vorsprünge des Wettbewerbs haben die anderen Bereichsleiter ebenfalls für das Thema sensibilisiert. Wie angekündigt schlägt der Marketingleiter Max als Projektleiter vor. Der Geschäftsführer des Unternehmens nickt zustimmend und wendet den Blick erwartungsvoll an Max. Max betont, dass er das Projekt äußerst spannend findet und sich als Assistent der Geschäftsführung gern darum kümmert. Er wirft den Erstentwurf eines Gantt-Diagramms an die Wand und erläutert der Runde, wie er sich die Umsetzungsschritte und die Zusammenarbeit der Bereiche vorstellt. Als Projektlaufzeit schlägt Max einen Zeitraum von sechs Monaten vor.

Die Führungskräfte im Strategie-Workshop zeigen sich beeindruckt, wie weitgehend sich Max bereits in die Planung eingearbeitet hat. Allerdings müsse man jetzt erstmal genau ermitteln, welche Anforderungen umzusetzen sind, und welche Ressourcen für das Projekt eingesetzt werden können. Der IT-Leiter, der mit seinem Team den Online-Shop verantwortet, möchte bei der Gelegenheit eine neue Version der Shop-Software implementieren und einen Einheits-Login einführen. Der Vertrieb mahnt an, dass aktuelle, konsistente Infos zu Produkten und Lieferterminen nur durch einen automatischen Abgleich der Daten im Online-Shop mit der internen Warenwirtschaft sichergestellt werden können. Auch die Personalleiterin meldet sich zu Wort. Sie spricht von „War of Talents" und „Digital Natives" und hält es für äußerst wichtig, im Verlauf des Projekts die Bewerberseiten zu überarbeiten und jetzt endlich mit einem Influencer-Blog zu starten.

Der Geschäftsführer überträgt Max die Projektleitung. Für das Projekt wird ein Lenkungsausschuss gebildet. Um das Projekt klarer in Hinblick auf Ziele, Umfang, Zeit und Kosten zu definieren, wird Max im nächsten Schritt mit allen Entscheidern und ihren Teams Anforderungen und Ressourcen klären. Er erhält vier Wochen Zeit, um einen formalen Projektantrag zu erstellen.

Viele Interessen, wenig Commitment

Der Marketingleiter zeigt Max einige Websites von Wettbewerbern, die ihm gefallen, und bietet Max an, das Gestaltungskonzept gemeinsam mit einem Agenturpartner zu entwickeln. Dabei solle bitte auch das neue Corporate Design berücksichtigt werden. Leider ist das Marketing-Team gerade mit einer großen Industriemesse und einer neuen Imagebroschüre beschäftigt, so dass Max nur auf die Hilfe der Agenturen und der eines Praktikanten zählen kann. Die Berater der Agenturen würden alle gern helfen, benötigen aber zunächst ein genaues Briefing. Der Vertriebsleiter will die Zahl der Online-Vertriebskontakte verdoppeln und die Antwortzeit auf ein Viertel reduzieren. Seine Leute leben von Verkaufsprovisionen und „müssen Geld verdienen", Ressourcen hat er daher keine. Der IT-Leiter verweist Max an einen Software-Entwickler, der ihm eine Excel-Datei mit einer Liste von 20 Wunsch-Features überreicht. Außerdem sollen alle digitalen Anwendungen in Zukunft unbedingt zentral in einem Rechenzentrum gehostet

werden. Der Entwickler freut sich über die Initiative und würde gern mitarbeiten, aber über den Termin müsse man noch mal reden, denn er und sein Team seien die nächsten zwölf Monate mit einem anderen Projekt ausgelastet. Die Personalleiterin zeigt Max ein fertiges Konzept für ein Bewerberportal, das seit zwei Jahren in der Schublade liegt. Ein Werkstudent aus ihrem Team könne gern helfen, es umzusetzen.

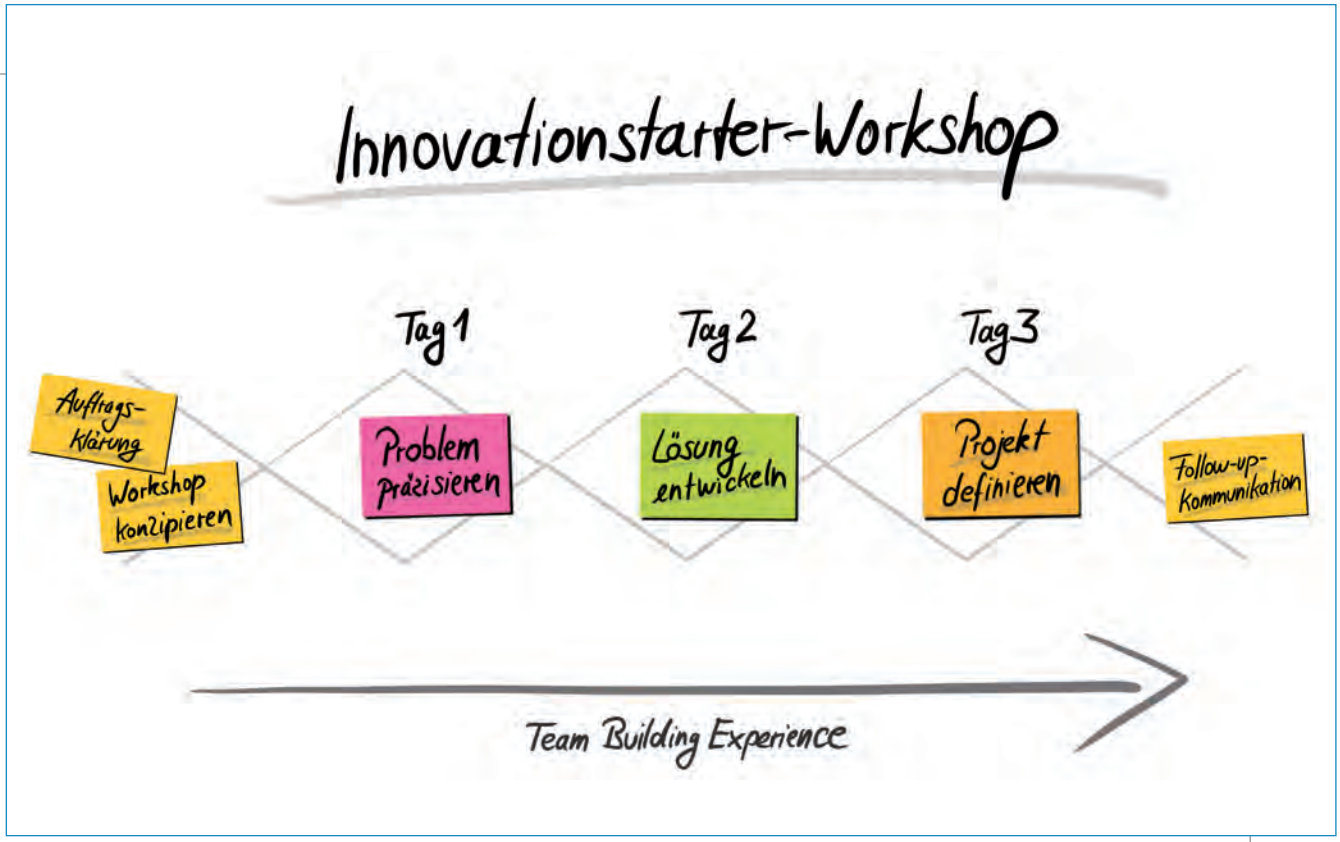
Nach vier Wochen und vielen weiteren Gesprächen ist Max nicht wesentlich weiter. Die Liste der Anforderungen wächst mit jedem Gespräch. Eine Priorisierung ist schwierig, denn jeder Fachbereich verteidigt vehement die eigenen Wünsche. Die Anforderungen sind ungenau formuliert, so dass es unmöglich erscheint, die benötigten Ressourcen zu kalkulieren. Und obwohl alle die Dringlichkeit des Projekts betonen, gibt es nur wenig Commitment zur Mitarbeit. Wie soll Max dieses komplexe Projekt bewältigen, wenn schon der Start so schwer fällt?

Kickoff mit Design Thinking – aber wie?

Ein Kollege aus dem Innovationsteam rät Max zu einem Design Thinking-Workshop. Von Design Thinking, der co-kreativen, nutzerzentrierten Problemlösungsmethode, hatte Max bereits im Studium gehört. Aber wie soll er den Ansatz in einem Kickoff-Workshop umsetzen? Über eine Webrecherche trifft er auf das 3-tägige Workshop-Format „Innovationsstarter". Die zeitliche Staffelung der ersten beiden Workshop-Tage orientiert sich am Design Thinking-Prozess. Hier wird der inhaltliche Umfang - der Scope des Projektes - konkretisiert. Der dritte Tag ist ein typischer Kick-off-Workshop zum Start eines neuen Projekts. Das Projekt wird im Kontext der Organisation betrachtet sowie zeitlich und personell grob definiert.

Max findet online eine genaue Schritt-für-Schritt-Anleitung für den Workshop. Er wirft auch einen Blick in das dazugehörige Arbeitsbuch. Im Workshop kommt es darauf an, die co-kreative Zusammenarbeit zwischen den Fachbereichen zu initiieren, um Silodenken zu überwinden und gemeinsame Entscheidungen zu treffen. Max erfährt, dass er durch die frühzeitige Klärung der sechs Erfolgsfaktoren Purpose, People, Place, Process, Pace und Project die co-kreative Zusammenarbeit begünstigen kann.

Vier Wochen später kann Max zwar noch keinen formalen Projektantrag vorweisen. Doch dafür findet das Konzept des Innovationsstarter-Workshops im Lenkungsausschuss großen Zuspruch. Max nutzt das Meeting als „Workshop für den Workshop", um die Rahmenbedingungen des Innovationstarter entlang der sechs P's Purpose, People, Place, Process, Pace und Project zu klären.



Der Innovationstarter-Workshop teilt sich auf drei Tage auf.
Sorgfältige Auftragsklärung, Vor- und Nachbereitung sichern die erfolgreiche Durchführung.

NUR DIE FRÜHZEITIGE KLÄRUNG DER SECHS P'S PURPOSE, PEOPLE, PLACE, PROCESS, PACE UND PROJECT FÜR CO-KREATIVE ZUSAMMENARBEIT MIT DEN STAKEHOLDERN DES PROJEKTS STELLT SICHER, DASS DESIGN THINKING SEINE WIRKSAMKEIT IN EINEM KICKOFF ENTFALTEN KANN.

Jens Otto lange, Designfacilitator, www.guentherlange.de

Kraftvoller Kickoff mit dem „Innovationstarter"

Wenige Wochen später treffen sich die Führungskräfte der verschiedenen Bereiche und ihre wichtigsten Wissensträger im Innovationstarter-Workshop. Die Moderation übernimmt Max. Innerhalb von drei Tagen klären sie gemeinsam alle Fragen, die Max im Projektantrag beantworten muss. Überdies entfaltet der Innovationstarter-Workshop ein Momentum, das alle Fachbereiche zu Zugeständnissen in Hinblick auf die Ressourcenplanung bewegt. Der Spaß und die Energie der kreativen Zusammenarbeit hat den Zusammenhalt über Abteilungsgrenzen hinaus gestärkt und bei den Teilnehmern Lust auf eine aktive Projektmitarbeit erzeugt, so dass nach Ende des dritten Workshop-Tages bereits weitgehend feststeht, wer zu welchem Anteil im Projektteam mitarbeiten wird.

Nach einem zunächst verzögerten Start hat Max mit dem Innovationstarter-Workshop eine Punktlandung hingelegt. Endlich kommt das Projekt ins Rollen. Zwei Tage nach Workshop-Ende liegt den Mitgliedern des Lenkungsausschusses der detaillierte Projektantrag vor. Die Diskussion ist kurz, denn im Workshop wurden alle wesentlichen Entscheidungen zum Inhalt des Projekts implizit - durch die gemeinsame Arbeit am Prototyp der Lösung - bereits getroffen. Und über das informelle Netzwerk, dass der Workshop zwischen den Beteiligten geknüpft hat, kann Max mit Hilfe seiner Kollegen auch im weiteren Verlauf so manche Hürde umschiffen.

Pünktlich geht die neue Website ans Netz – mit genau den Features und Inhalten, die für die Nutzer am wichtigsten sind - nicht weniger, aber auch nicht mehr.

Sechs Erfolgsfaktoren für Co-Kreation

Und die Moral von der Geschicht'? Gute Vorbereitung ist alles. Nur die frühzeitige Klärung der sechs P's Purpose, People, Place, Process, Pace und Project für co-kreative Zusammenarbeit mit den Stakeholdern des Projekts stellt sicher, dass Design Thinking seine Wirksamkeit in einem Kickoff entfalten kann. Schauen wir sie noch einmal im Detail an:

Purpose: Warum ist der Innovationstarter-Workshop wichtig?

Jeder Design Thinking-Workshop braucht als Handlungsrahmen ein nutzerzentriertes Workshop-Ziel. Diese sogenannte „Design Challenge" sollte vorab mit den Entscheidern formuliert werden. Ein Beispiel: „Gestalte das Online-Erlebnis für unsere Neukunden in einer globalen Welt, in der der Erstkontakt digital erfolgt."

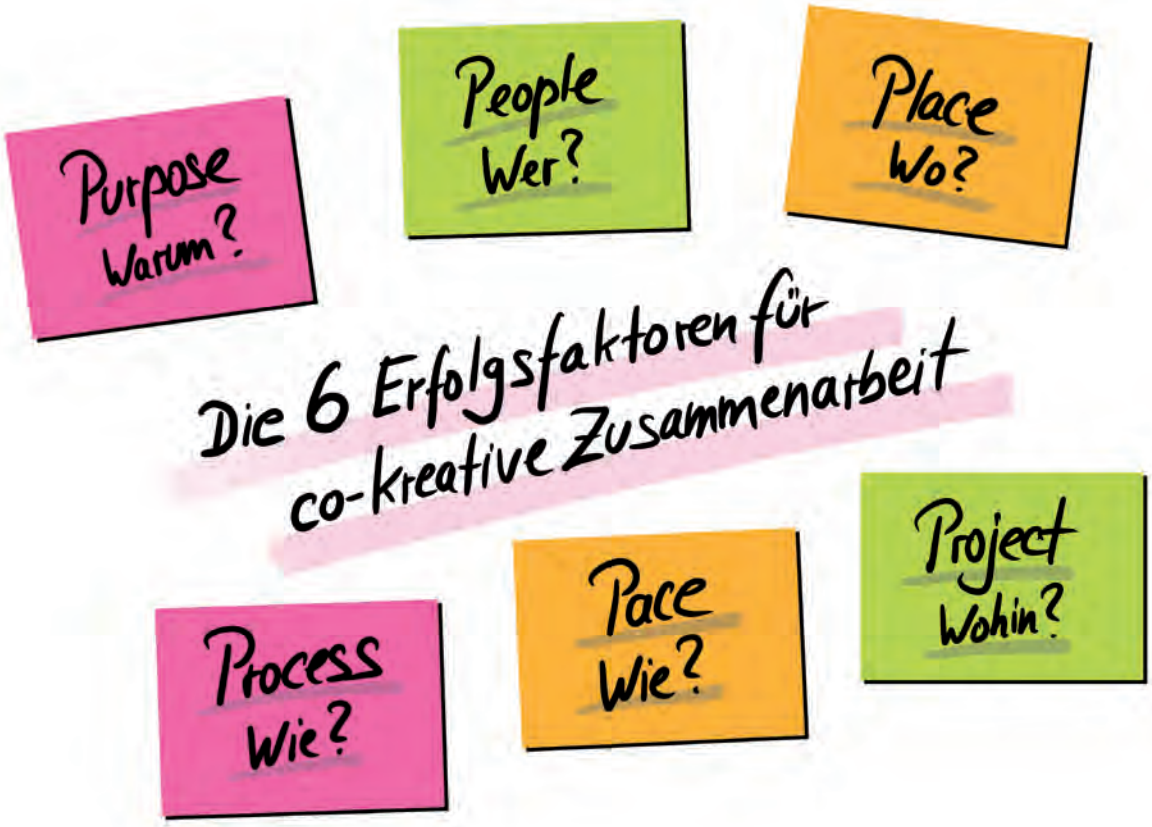
People: Wer ist dabei?

Design Thinking ist ein menschzentrierter Ansatz. Ein Projekt-Kickoff nach diesem

Projekte starten mit Design Thinking – Kreative Konzeptfindung mit System, Jens Otto Lange, Business Village 2020

PROJEKTE STARTEN MIT DESIGN THINKING
Kreative Konzeptfindung mit System

Projektarbeit gehört in vielen Unternehmen zur Tagesordnung. Ob Digitalisierung, Innovationsvorhaben, Change oder neue Produkte und Services, sie haben eins gemein: Sie starten als Projekt. Design Thinking hilft, sie zum Erfolg zu führen. Doch für welche Projektthemen eignet sich Design Thinking? Wie lassen sich cross-funktionale Teams aufstellen? Welche Voraussetzung braucht die Kreativarbeit noch?
Langes Buch gibt Antworten auf diese Fragen. Konkret und anschaulich illustriert es den Einsatz von Design Thinking für den Start und das Scoping von Projekten. Schritt für Schritt zeigt es auf, wie man Design Thinking-Workshops plant, um schnell Konzeptideen für komplexe Fragestellungen zu entwickeln.



Die sechs Erfolgsfaktoren für co-kreative Zusammenarbeit helfen bei der Vorbereitung eines Innovationstarter-Workshops.

Muster braucht daher nicht nur einen klaren Auftraggeber und Teilnehmer aus allen relevanten Fachbereichen, sondern auch den Zugang zu potenziellen Nutzern der Lösung, um Empathie für deren Bedürfnisse aufzubauen.

Place: Wo findet der Workshop statt?

Der Workshop kann remote, onsite oder als Hybrid ausgerichtet werden. Onsite sollte es mindestens 5 qm Fläche pro Teilnehmer sowie ausreichend Materialien für die co-kreative Zusammenarbeit geben. Remote sollten alle Teilnehmer über gleiche Zugangsmöglichkeiten und Fertigkeiten im Umgang mit Online-Tools verfügen.

Process und Pace: Wie läuft der Workshop ab?

Am effektivsten ist ein kompakter Innovationstarter-Workshop über drei Tagen. Alternativ können die Arbeitsphasen als halbtägige Einheiten auf zwei Wochen verteilt werden. Dabei sollte auch die typische Stimmungskurve in Design Thinking-Workshops berücksichtigt werden. Eine sorgfältig formulierte Einladung ist wichtig, um die Teilnehmer frühzeitig einzustimmen.

Project: Wohin soll die Reise gehen?

Auch wenn Details erst im Workshop fixiert werden, macht es Sinn, bereits vorab grob mit den Stakeholdern festzulegen, wann das Projekt starten und enden soll, wer teilnehmen sollte und welches Budget erwartet wird. Diese Infos können am dritten Tag des Innovationstarter weiter detailliert werden.

Projektdesign mit Design Thinking

Design Thinking hilft, schnell und zuverlässig ein von allen Beteiligten verstandenes und akzeptiertes Big Picture des Vorhabens zu entwerfen, das im weiteren Verlauf in ein Projekt gefasst, iterativ verfeinert und in Details ausgearbeitet wird. Das mühselige Zusammentragen von Anforderungen lässt sich mit Design Thinking stark verkürzen. Erste Nutzer-Tests bereits im Workshop minimieren das Risiko, dass die Lösung am Bedarf vorbei entwickelt wird.

Jens Otto Lange

CHECKLISTE

Die Checkliste für die Vorbereitung des Innovationstarter-Workshops: https://www.jensottolange.de/projekte-starten-mit-design-thinking/downloads/

DAS NÄCHSTE

SPEZIAL
itsecurity

ERSCHEINT AM
30. NOVEMBER 2021

WORKING WORLD	Employee Experience im Fokus
RPA-TECHNIKEN	Process Mining leicht gemacht
BANK & FINANCE	Betrügerisches Verhalten ade!

DIE AUSGABE 11/2021 IT MANAGEMENT ERSCHEINT AM 29. OKTOBER 2021.

INSERENTENVERZEICHNIS

WIR WOLLEN IHR FEEDBACK

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

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Carina Mitzschke, Silvia Parthier (-26)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Dr. Dirk Goldner, Dina Haack, Matthias Hamel, Kevin Kloft, Benjamin Krebs, Carina Mitzschke, Angelika Mühleck, Silvia Parthier, Ulrich Parthier, Frank Schnicke, Markus Seirer, Jan Sudmeyer

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 28. Preisliste gültig ab 1. Oktober 2020.

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

Online Campaign Manager:
Vicky Miridakis, Telefon: 08104-6494-2, miridakis@it-verlag.de

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

Erscheinungsweise: 10x pro Jahr

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

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

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

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

NEW WORKING WORLD

Digitalevent | 11.11.2021

„New Work“ steht für viel mehr als Homeoffice, Collaboration-Tools oder das Arbeiten unter Palmen und eines ist klar: „New Work“ verändert die Welt. Lassen Sie uns diese neue Arbeitswelt gemeinsam effizient, sicher und menschlich gestalten.

Highlights aus der Agenda

Unified Communications

Die Unternehmenskommunikation im Wandel – Wie aus einem „Oh, oh“ ein „Yee-haw“ Zustand wird
Martina Yazgan, Marketing Director, Teamwire

Deskless Workforce

MDM plus C: Nutzer mobiler Geräte besser vor Gefahren durch Ablenkung schützen
Matthias Ott, Teamleiter EMM Services, SPIRIT/21

Mobile Arbeitsumgebungen on-demand
Dominik Schleier, DACH Systems Engineer, Jamf

Remote Work / Hybride Arbeitswelten

Raus aus dem Schatten: Warum Schatten-IT bei Messengern große Risiken birgt
Miguel Rodriguez, Head of Sales, Threema

SCAN ME

Jetzt anmelden

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

ES IST WIEDER IT-SA ZEIT UND ES GIBT VIEL NEUES ZU BERICHTEN!

Besuchen Sie uns in
HALLE 7A am **STAND 513**
zu einem persönlichen
Austausch mit unseren
Experten, oder buchen
Sie gleich einen
Termin über
info@seppmail.de.

E-Mail Kommunikation

- E-Mail Verschlüsselung
- E-Mail Signatur - mPKI
- E-Mail Large File Transfer
- E-Mail Disclaimer
- Cloud Data Protection by eperi

E-Mail Filter

- Anti Spam
- Anti Virus
- Anti Phishing
- Anti Malware

SEPPMAIL

SEPPmail – Deutschland GmbH
Ringstraße 1c | D-85649 Brunnthal b. München | Tel.: +49 8104 8999 030
E-Mail: info@seppmail.de | Internet: **www.seppmail.de**

itsecurity
OKTOBER 2021

DAS SPEZIAL

BESTANDTEIL JEDER TRANSFORMATION

ZERO TRUST

Kathrin Redlich, Florian Bäuml, Timo Trunk | Zscaler Germany GmbH

CYBER-RESILIENZ

Unvorhersehbarkeit muss nicht negativ sein

THREAT DETECTION

Transparenz und Echtzeitreaktion

IOT SECURITY

Produktionsnetze zuverlässig schützen

SOFTWARE FOREN LEIPZIG

SAFETY FIRST!

Jedes System hat seine Schwachstellen. Lernen sie ihre kennen, um sie zu verteidigen! Ob Community-Treffen, Konferenz oder spezielles IT-Training: In jedem unserer Formate setzen wir auf intensiven Fachaustausch und Praxisbezug. Lernen Sie aus den Erfahrungen Ihrer Fachkolleg:innen und profitieren Sie von realen Szenarien.

11./12.11.2021

COMMUNITY DAYS
IT-Sicherheit

TRAINING
IT-Sicherheit

18./19.11.2021

COMMUNITY DAYS
Governance, Risk, Compliance

TRAINING
LIVE-Hacking

12./13.05.2022

KONFERENZEN
IT-Sicherheits-management in Versicherungen

TRAINING
Pentest zum Anfassen

COMMUNITYDAYS.DE

LEARNIT.DE

INHALT

COVERSTORY

IT-SA SPECIAL

IT SECURITY

TRANSFORMATION ZU ZERO TRUST

IT-SICHERHEIT MUSS BESTANDTEIL JEDER TRANSFORMATIONSINITIATIVE SEIN

Klassische IT-Sicherheitsmodelle greifen nicht mehr, wenn Anwendungen in die Cloud verlagert werden und Mitarbeiter von überall aus arbeiten. Im Zuge von Transformationsprojekten sollte deshalb auch die Modernisierung der Security auf jeder Agenda stehen. Im Gespräch mit Florian Bäuml, Kathrin Redlich und Timo Trunk von Zscaler wird beleuchtet, wie Cloud-Transformation mit Sicherheits- und Connectivity-Anforderungen in Einklang gebracht wird. Zero Trust tritt an, der traditionellen Hardware-Sicherheit am Perimeter die Vormachtstellung streitig zu machen.

Ulrich Parthier: *Wird Security heute im Rahmen von Transformationsprojekten berücksichtigt?*

Florian Bäuml: Wir sehen zwei Ansätze in unseren Gesprächen. Der eine Teil von Unternehmen agiert nach dem Lift-& Shift-Prinzip und verlagert seine Applikationen in die Cloud, ohne gleichzeitig die Netzwerk- und Sicherheitsinfrastruktur anzupassen. Diese Unternehmen folgen dem tradierten Ansatz und nähern sich ihrer Transformation evolutionär. Das funktioniert zwar, zieht aber weitere Anpassungen nach sich, die zum Beispiel durch unzufriedene Anwender durch Latenz beim Zugriff nötig werden.

Andererseits erleben wir die Unternehmen, die einen ganzheitlichen Transformationsansatz umsetzen. Bei etwa einem Drittel gehen die strategischen Initiativen mit der Nachfrage nach einem Zero Trust-Sicherheitsansatz einher. Hier wird die Cloud-Journey von Netzwerk- und Security-Transformation begleitet, so dass ein echter Strategiewechsel stattfindet.

Ulrich Parthier: *Welche Herausforderungen gehen mit ganzheitlicher Transformation einher?*

Kathrin Redlich: Am erfolgreichsten sind Transformationsprojekte, wenn sie von der Unternehmensspitze mit hoher Priorität vorangetrieben werden, die auch von allen Stakeholdern wahrgenommen wird. Business Units, die die Verlagerung von Apps in die Cloud vorhaben, müssen mit den Netzwerk- und Sicherheitsteams sprechen. In einer 360 Grad-Betrachtung gilt es, den Status Quo einzufangen und Herausforderungen aller Abteilungen zu adressieren. Letztlich muss gemeinsam eine Roadmap für die ganzheitliche Transformation erarbeitet werden.

> EIN ZERO TRUST-ANSATZ KANN NICHT NUR FÜR SICHERHEIT, SONDERN AUCH FÜR DIE NÖTIGE PERFORMANZ SORGEN.
>
> Florian Bäuml, VP EMEA South, Zscaler Germany GmbH, www.zscaler.de

> AM ERFOLGREICHSTEN SIND TRANSFORMATIONSPROJEKTE, WENN SIE VON DER UNTERNEHMENSSPITZE MIT HOHER PRIORITÄT VORANGETRIEBEN WERDEN, DIE AUCH VON ALLEN STAKEHOLDERN WAHRGENOMMEN WIRD.
>
> Kathrin Redlich, Regional Vice President, Zscaler Germany GmbH, www.zscaler.de

Timo Trunk: Wir haben gelernt, dass Unternehmen für die Umsetzung der ganzheitlichen Initiativen einen Katalysator benötigen, der alle Parteien an einen Tisch bringt und auch alle Sorgen mit einbezieht. Wir treten Firmen, die den Sprung in eine moderne Arbeitsumgebung wagen, auf Augenhöhe gegenüber und hören im ersten Schritt zu. Denn oft muss ein Sinneswandel in Gang gesetzt und Ängste überwunden werden, wenn bestehende Infrastrukturen durch neue Technologien abgelöst werden.

Ein Cloud-basierter Zero Trust-Ansatz für IT-Security ersetzt ein Netzwerk-zentriertes Modell, bei dem die Mitarbeiter mit der Administration von Hardware betraut sind. Wir zeigen auf, wie die Cloud nicht nur mit Vorteilen für die Applikationen einhergeht, sondern auch für fortschrittliche Sicherheit sorgt. Eine anfängliche Abwehrhaltung aus Angst vor Veränderungen oder gar Jobverlust lässt sich entkräften durch die Einsicht, dass sich das volle Potenzial der Cloud nur durch eine Veränderung von Netzwerk und Sicherheit herbeiführen lässt. Aufgaben werden verlagert weg von der Administration von Hardware hin zur Erstellung von Richtlinien im Einklang mit der Risikobewertung des Unternehmens.

? **Ulrich Parthier:** *Welche Faktoren führen zu einem Umdenken?*

Timo Trunk: Im schlimmsten Fall erleben Unternehmen durch einen Sicherheitsvorfall, dass ihr Sicherheitskonzept den modernen Angriffsszenarien nicht standhält. Spätestens dann ist die Einsicht für einen Richtungswechsel vorhanden. Ein Umdenken kann aber auch im Vorfeld durch Überzeugungsarbeit herbeigeführt werden. So hilft beispielsweise ein Architektur-Workshop, der mit allen beteiligten Parteien vom Anwendungsbereich über Netzwerk bis zu Sicherheitsteam durchgeführt wird, Alternativen aufzuzeigen. Seit Jahrzehnten bestehende Netzwerkarchitekturen werden nicht leichtherzig durch einen Zero Trust-Ansatz ausgetauscht. Es muss erst Verständnis geweckt werden für moderne Angriffsszenarien und -flächen, die ein Unternehmen in der Cloud ausgesetzt ist.

Kathrin Redlich: Speziell in großen Unternehmen ist es wichtig zunächst die bestehenden – oftmals komplexen – Strukturen und Verantwortungsbereiche der einzelnen Stakeholder zu verstehen und diese mit Expertise abzuholen. Es gibt etablierte Lösungen, die in der Vergangenheit gut funktioniert haben, aber in der heutigen Zeit mit den neuartigen Herausforderungen neu bewertet werden müssen. Für mich ist dabei wichtig, dass wir einen individuellen Lösungsansatz erarbeiten. Dazu muss man erst einmal zuhören können und erst im zweiten Schritt eine Lösungsmöglichkeit präsentieren, die auf die individuelle Zielsetzung und das Tempo des Unternehmens zugeschnitten ist.

? **Ulrich Parthier:** *Ist Sicherheit eine Frage der Unternehmensgröße?*

Florian Bäuml: Es gibt gravierende Unterschiede bei der Schnelligkeit von Transformationsprojekten je nach Größe. Große Unternehmen tun sich aufgrund ihrer Legacy-Thematik und globaler Komplexität deutlich schwerer, denn mit zunehmender Größe steigen in aller Regel die Komplexität der vorhandenen Infrastruktur und damit auch die Veränderungsprozesse. Dennoch haben auch große Konzerne in den letzten 1,5 Jahren vorgeführt, wie schnell globale Transformation umsetzbar ist, um Mitarbeiter

> WIR ZEIGEN AUF, WIE DIE CLOUD NICHT NUR MIT VORTEILEN FÜR DIE APPLIKATIONEN EINHERGEHT, SONDERN AUCH FÜR FORTSCHRITTLICHE SICHERHEIT SORGT.
>
> Timo Trunk, Senior Regional Vice President, Zscaler Germany GmbH, www.zscaler.de

sicher und performant von zu Hause aus arbeiten zu lassen.

Kleinere Unternehmen sind häufig flexibler. Um nicht abgehängt zu werden, setzen gerade die Hidden Champions auf moderne Arbeitswelten und positionieren sich als attraktiver Arbeitgeber. Im gehobenen Mittelstand erleben wir ein großes Momentum, auf die Zeichen der Zeit zu setzen. Nicht nur die Cloud ist angesagt, man tut sich auch leichter, Legacy-Infrastrukturen über Bord zu werfen und neuartige Sicherheits-Konzepte zu implementieren. Entscheidungsprozesse sind beweglicher und die Bereitschaft für Veränderungen ist sehr groß.

? **Ulrich Parthier:** *Wo sollten Unternehmen mit einem Zero Trust Ansatz anfangen?*

Kathrin Redlich: Sie sollten sich über eine konkrete Herausforderung und die Zielsetzung im Klaren sein. Nur dann ist eine konsequente Transformation hin zu Zero Trust möglich. Wir haben auf Basis vieler unterschiedlicher Treiber diesen Weg mit unseren Kunden beschritten. Die jüngsten Ransomware-Attacken lenken das Bewusstsein von Organisationen verstärkt auf das Thema Sicherheit.

Florian Bäuml: Vor Ransomware-Angriffen haben Unternehmen zwar Respekt, aber wir sehen unterschiedlichste Verhaltensmuster: von laxem Umgang bis zu großer Paranoia. Wenn Einsicht für die Anpassung der Infrastruktur vorhanden ist, sollte man bei einem konkreten Problem anfangen, das im Zuge der Transformation entstanden ist. Ist zum Beispiel der Zugang zu Microsoft 365 eine Herausforderung, müssen Hub & Spoke-Netzwerke durch direkte Internet-Übergänge, zum Beispiel mit Hilfe von SD-WAN, abgelöst werden. Damit einhergehend kann ein Zero Trust-Ansatz nicht nur für Sicherheit, sondern auch für die nötige Performanz sorgen. Somit schließt sich der Kreis, dass Cloud-Transformation nicht isoliert betrachtet werden darf.

Timo Trunk: Messbarkeit ist das Zauberwort. Dazu benötigen Unternehmen im ersten Schritt eine Strategie, welche Effekte sie durch die Transformation erzielen wollen. Anhand messbarer Kriterien - das kann die Anzahl der Helpdesk Tickets sein, Einblick in Angriffe auf das Netzwerk oder die Reduktion von Kosten - ergeben sich Ansatzpunkte. Damit die Vorteile der Cloud nicht durch erhöhte Komplexität oder Administration für Hardware abgefedert werden, ergibt sich ein Zero Trust-Modell als logische Folge. Der Mehrwert von erhöhter Sicherheit und reduzierten Kosten schafft schnell Akzeptanz über alle Abteilungen hinweg.

! **Ulrich Parthier:** *Frau Redlich, Herr Bäuml, Herr Trunk, wir danken Ihnen für dieses Gespräch.*

ZERO TRUST-SICHERHEIT

SO GELINGT DIE UMSETZUNG

Dezentrales Arbeiten außerhalb von Büros und der Einsatz von Public Clouds sind in den letzten Jahren zum Alltag in Unternehmen geworden. Durch die Verlagerung von Anwendungen in Multicloud-Umgebungen und Mitarbeiter, die von überall aus produktiv sind, werden neue Sicherheitsansätze nötig. Zero Trust tritt an, die klassische Hardware-basierte Sicherheit abzulösen.

Der durch die Cloud ausgelöste Wandel der Arbeitswelt muss von der IT-Abteilung jedes Unternehmens auch durch einen ganzheitlichen Wechsel in der Infrastruktur begleitet werden. Unternehmen realisieren, dass es im Zuge ihrer Transformation nicht mehr ausreicht, nach dem „Lift-& Shift"-Ansatz Applikationen in die Cloud zu verlagern. Um das volle Potenzial der Cloud zu nutzen, sind radikale Veränderungen im Ökosystem Infrastruktur erforderlich, zu denen neben der Netzwerkarchitektur auch die Modernisierung der IT-Sicherheit zählt.

Für generell performanten Zugriff auf Anwendungen in der Cloud ist es notwendig, auch das Connectivity- und Security-Modell zu überdenken. Anstelle der Weiterführung des klassischen Perimeters mit Netzwerkzugriff und langen Wegen durch das interne Netzwerk bis in die Cloud muss der Zugang zu Anwendungen möglichst auf direktem Weg erfolgen. Unternehmen müssen lernen, dass es zugunsten der Mitarbeiterzufriedenheit in der IT darauf ankommt den schnellen Zugriff zu Applikationen zu gewähren. Hierbei ist der Kontext von Netzwerken nicht mehr wichtig. Entscheidend ist, und hier kommt Zero Trust ins Spiel, dass niemand einen Vertrauensvorschuss für den Zugriff erhält. Aufgrund von Kriterien wird das Vertrauen „erarbeitet" und in einem Zero Trust-Modell mit der Anwenderidentität verknüpft, um Zugriff zu gewähren. Applikationen können sich somit überall befinden, ob im Internet, in der Private Cloud und oder im Rechenzentrum. Für private Applikationen wendet man zusätzlich das Prinzip des ‚Least Privilege' an, also Zugriff auf Basis granularer Regeln und Rollen.

Der Weg zu Zero Trust

Die Grundidee von Zero Trust-Sicherheit basiert auf der Nachvollziehbarkeit der Datenströme aller Mitarbeiter und Geräte zu deren Anwendungen in der Cloud und im Internet, unabhängig von deren Standort. Für die Kontrollfunktion empfiehlt sich eine Cloud-basierte Sicherheitslösung, die mit ihren Filtern und Regeln zwischen dem Anwender und seinen Applikationen sitzt. So sorgt die Zscaler Zero Trust Exchange Plattform dafür, dass für den Zugriff auf jede einzelne Anwendung ein sicherer Microtunnel aufgebaut wird. Dabei definiert die Identität des Anwenders und seine Rolle im Unternehmen, auf welche Internetressourcen, Applikationen in der Cloud oder im Rechenzentrum der Zugriff für die tägliche Arbeit erlaubt wird. Wenn der gesamte Datenverkehr über die Security-Cloud geschickt wird, erhält die IT-Abteilung den Überblick über alle Datenströme zurück und kann diese absichern. Bei einer solchen Security-Transformation helfen die folgenden Überlegungen.

Das Transformationsziel vor Augen haben

Zum Start sollten sich Unternehmen eine klare Zielsetzung definieren, was sie mit der Neuausrichtung ihrer Sicherheitsinfrastruktur erreichen möchten. Geht es um die Kontrolle aller Datenströme, die zum Internet gerichtet sind und den Zugriff der Mitarbeiter auf alle sowie Cloud-basierten Anwendungen, oder auch den sicheren Zugriff unabhängig vom Standort? In komplexen Multicloud-Umgebungen stellt sich darüber hinaus auch die Frage, ob die Cloud-basierten Instanzen korrekt

konfiguriert sind, und welche Workloads miteinander kommunizieren dürfen. Bei all diesen Fragestellungen kann eine Zero Trust-Architektur helfen.

Die Abkehr von der Netzwerksicherheit

Klassischer Perimeterschutz diente dazu, das Netzwerk abzusichern. Wenn die Applikationen in die Cloud verlagert werden und Mitarbeiter von überall aus arbeiten, greift die Hardware am Perimeter ins Leere. Das Backhauling des Datenverkehrs zu zentralen Internet-Gateways aus Gründen der Sicherheitskontrolle muss von direktem Ausbrechen ins Internet abgelöst werden. Die Sicherheitsfilter, die ehemals am Netzwerkperimeter angesiedelt waren, werden dabei über die Security Plattform aus der Cloud bereitgestellt. Da Cloudumgebungen, somit auch die Security aus der Cloud, permanent aktualisiert werden, wird die Verwaltung von Sicherheits-Hardware und das Patchen obsolet.

Zugriff auf Applikationsebene

In der heutigen Remote-Arbeitswelt müssen sich Unternehmen vom Standortdenken lösen, denn von wo aus der Mitarbeiter produktiv ist, spielt keine Rolle mehr. Entscheidend ist, dass jeder User unabhängig von seinem Standort sicher und gleich performant auf seine Anwendungen zugreifen kann, egal ob diese in Multicloud-Umgebungen oder im Rechenzentrum vorgehalten werden. Es gilt also nicht mehr den Anwender ins Netzwerk zu platzieren, um ihm den Remote-Zugriff zu ermöglichen. Eine Zero Trust Architektur brokert den sicheren Zugriff auf Anwendungen auf Ebene der benötigten Applikation und nicht auf Netzwerkebene, wodurch gleichzeitig die aus Sicherheitsgründen angesagte Mikrosegmentierung hergestellt wird.

Kontrolle für höhere Sicherheit

Wenn alle Datenströme über eine hochintegrierte und performante Cloud-basierte Sicherheitsplattform laufen und Zugriff auf Applikationsebene gewährleistet wird, können Unternehmen ihr Sicherheitsniveau an die modernen Anforderungen anpassen. Sie erhalten auf diese Weise eine zentrale Sicht auf die Dinge und damit Einblick in alle Datenströme zurück und können aufbauend Policies definieren, aber auch DLP und CASB-Module implementieren, die über regelbasierte Berechtigungen durch die Cloud gesteuert werden. Für höhere Sicherheit sorgt auch, dass der gesamte Datenverkehr inklusive TLS-verschlüsseltem Traffic auf Malware untersucht werden kann, was häufig für Unternehmen nicht allumfänglich möglich war.

Identität wacht über den Zugriff

Voraussetzung für Zero Trust basierte Sicherheit ist ein Identity-Provider wie Azure ID oder Okta. Da die meisten Unternehmen ihre Mitarbeiter bereits über ein solches System verwalten, ist damit der Grundstock für den Einstieg in die Richtliniendefinition vorhanden. Aufbauend auf der Funktion eines Mitarbeiters werden ihm Rollen zugewiesen und damit Zugriffsrechte auf Applikationen im Identitiy-System vergeben. Die Zero Trust Exchange Plattform sorgt dann für die Umsetzung der Policies und gewährt ausschließlich Zugang zu Applikationen oder Diensten, für die auch die Berechtigung vorliegt.

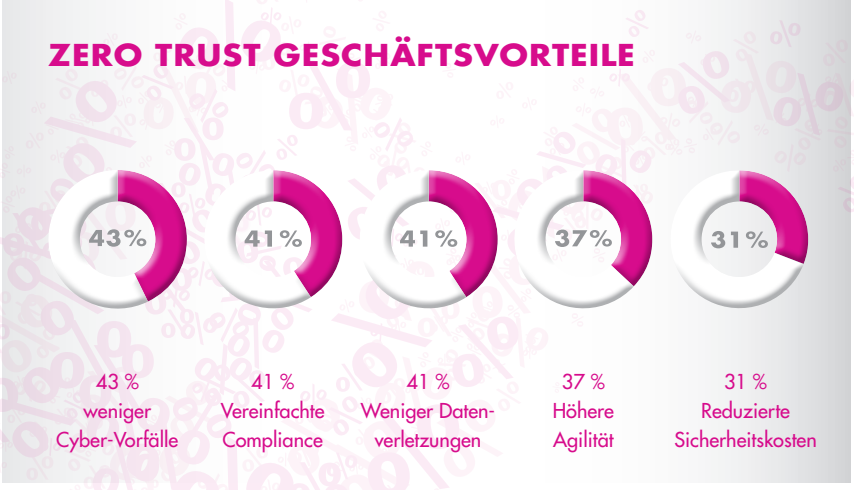
DIE ZSCALER ZERO TRUST EXCHANGE PLATTFORM SORGT DAFÜR, DASS FÜR DEN ZUGRIFF AUF JEDE EINZELNE ANWENDUNG EIN SICHERER MICROTUNNEL AUFGEBAUT WIRD.

Kevin Schwarz, Director, Transformation Strategy EMEA, Zscaler Germany GmbH, www.zscaler.de

Am Anfang steht die Vision

Unternehmen, die nicht nur ihre Applikationslandschaft transformieren, sondern damit einhergehend auch ihre Netzwerkarchitektur und ihre Sicherheit modernisieren wollen, kommen um Zero Trust nicht mehr herum. Um einen konkreten Startpunkt für Zero Trust auszumachen hilft die Vision, was dadurch erzielt werden soll. Unternehmen werden schnell realisieren, dass bereits Ansatzpunkte vorhanden sind, an denen sich konkrete Schritte festmachen lassen, um die Zero Trust-Strategie parallel zu ihrer Digitalisierung voranzutreiben.

Kevin Schwarz



it-sa Spezial

Auf geht's. Vom 12. bis 14. Oktober ist es wieder soweit. Die it-sa findet als Präsenzveranstaltung in Nürnberg statt und wir sind dabei: Halle 7 Stand 401

Bitte umblättern!

HOME OF IT SECURITY

IT-SA 2021 IN NÜRNBERG
WIEDER DIE ZENTRALE DIALOGPLATTFORM
ZUR CYBERSICHERHEIT

Auf 52,5 Milliarden Euro schätzt das Institut der deutschen Wirtschaft die finanziellen Schäden, die im letzten Jahr durch Hackerangriffe auf Mitarbeiter im Homeoffice entstanden. Das ist ein neuer Rekord. Aktuelle Erhebungen des Digitalverbands Bitkom weisen auch einen Anstieg von durch Cybercrime verursachten Schäden insgesamt aus: Deutschen Unternehmen entstanden demnach durch Datendiebstahl, Industriespionage oder Sabotage Schäden von 223,5 Milliarden Euro. Das ist mehr als doppelt so viel wie im letzten Erhebungszeitraum. Als Fachmesse für IT-Sicherheit widmet sich die it-sa vom 12. bis 14. Oktober der professionellen Abwehr von Cyberkriminalität – dieses Jahr wieder wie gewohnt im Messezentrum Nürnberg.

Zentrale Dialogplattform

„Diese Zahlen zeigen: IT-Sicherheit ist wichtiger denn je! Die it-sa bietet Experten und Entscheidern die zentrale Plattform zum fachlichen Austausch rund um den Schutz sensibler Daten, die Sicherheit von IT-Infrastrukturen und aktuelle Bedrohungsszenarien. Wir freuen uns, sie wieder vor Ort im Messezentrum Nürnberg zu begrüßen“, so Frank Venjakob, Director it-sa. TeleTrust-Geschäftsführer Dr. Holger Mühlbauer unterstreicht: „Nach den vielfachen Einschränkungen der letzten Zeit kommt der it-sa als Impulsgeber für den persönlichen Austausch zum Status der Cybersicherheit in Deutschland und darüber hinaus eine besondere Rolle zu. Wir freuen uns sehr, dass die Branche in Nürnberg wieder zusammenkommt. Der Bundesverband IT-Sicherheit (TeleTrusT) unterstützt die it-sa dafür erneut als Premium Partner.“

Umfangreiches Rahmenprogramm

Erstmals findet die it-sa in den Messehallen 7 und 7A und das begleitende Kongressprogramm im modernen NürnbergConvention Center Ost statt, das an die neuen Hallen angrenzt. Die Vorbereitungen dafür sind in vollem Gange. Die Besucher erwartet wie gewohnt ein umfangreiches Foren- und Rahmenprogramm, an dem sich Unternehmen und Partnerorganisationen beteiligen: Vier offene Foren bieten Informationen zu Produkten, Lösungen und Trends im Bereich der Cybersicherheit. Aussteller-Vorträge zu Management und Technik sowie Produktneutrale Beiträge, die als it-sa insights ausgewiesen werden, sind hier frei zugänglich. Zu den Höhepunkten der it-sa 2021 zählt die Verleihung des UP@it-sa Award am dritten Messetag. Bereits zum vierten Mal verleiht die it-sa zusammen mit dem Digital Hub Cybersecurity und dem IT-Sicherheitscluster e.V. diese Auszeichnung für herausragende Leistungen junger IT-Sicherheitsunternehmen aus der DACH-Region. Im Rahmen der it-sa Expo&Congress findet zudem am 12. und 13. Oktober die Veranstaltung „IT Job Kompakt“ statt, eine Kombination aus Fachkonferenz und Recruiting-Messe, die der it-sa Event Partner heise beiträgt.

Internationale Beteiligung und Gemeinschaftsstände

Rund 250 Unternehmen aus 17 Ländern sind derzeit als Aussteller angemeldet. Bestätigt sind Gemeinschaftsstände, aus Österreich, Nordrhein-Westfalen, Baden-Württemberg und Bayern sowie die Beteiligung nationaler und internationaler Verbände und Organisationen. Im englischsprachigen International Forum spricht beispielsweise Luigi Rebuffi, Generalsekretär der European Cyber Security Organisation (ECSO) zu Investment-Potenzial in der Branche. Hier präsentieren sich auch die drei Gewinner des „German-Baltic Business Award“, der an herausragende Anbieter im Bereich der Cybersicherheitsanbieter aus den baltischen Staaten verliehen wurde.

www.it-sa.de

it sa 365
HOME OF IT SECURITY

RANSOMWARE

VERHALTENSBASIERTE SECURITY

Bei einem Ransomware-Angriff handelt es sich nicht um eine „einfache" Infektion durch Malware. Vielmehr ist es eine komplexe Abfolge von Aktionen, bei denen die Erstinfektion nur der erste Schritt ist. Ein erfolgreicher Ransomware-Angriff umfasst fast immer eine Vielzahl von Angriffsvektoren, die häufig durch menschliches Eingreifen gesteuert werden. Die erfolgreiche Abwehr einer derartigen Attacke erfordert eine Lösung, die das gesamte Spektrum der Bedrohungen durch diese Vektoren neutralisieren kann.

Herkömmliche Signatur-basierte Antiviren-Lösungen sind heute unzureichend, um moderne Angriffe abzuwehren. Diese althergebrachten Systeme sind nicht in der Lage, den Kontext eines Angriffs zu analysieren und eine Warnung auszulösen, wenn ein verdächtiges Muster auftaucht. Sowohl bei Cloud-basierten als auch bei On-Premises-Lösungen kann es zu Engpässen und Verzögerungen bei der Auslösung von Alerts kommen, was Angreifern entscheidende Vorteile beim Eindringen ins Netzwerk verschaffen könnte.

Aktiver Schutz vor Ransomware

Die Lösung für das Ransomware-Problem ist eine intelligentere Verteidigung. Durch Berücksichtigung des Verhaltens und nicht der Konformität mit einer Signatur können intelligente Lösungen wie SentinelOne Active EDR Muster erkennen, die von der Systembasis abweichen, sei es durch neue (oder weiterentwickelte) Varianten oder durch Aktivitäten innerhalb des Netzwerks, die nicht der Norm entsprechen. Prozesse, die verdächtige Aktivitäten anzeigen, können beendet oder isoliert werden, bevor sie sich ausbreiten können. Der Einsatz von KI kann so den entscheidenden Vorteil zur schnellen Verteidigung gegen Angreifer ausmachen.

https://de.sentinelone.com/

SentinelOne™

CYBER-ANGRIFFE

ORIENTIERUNG FÜR MEHR SICHERHEIT

Im Hinblick auf die IT-Sicherheit bleibt die Lage in Deutschland weiterhin dynamisch und angespannt, wie aus einem aktuellen Bericht des Bundesamts für Sicherheit in der Informationstechnik hervorgeht. Unter anderem kamen im Jahr 2020 insgesamt rund 117 Millionen neue Schadprogramm-Varianten hinzu. Um sich effektiv gegen die Gefahren zu schützen, brauchen sie eine verlässliche Strategie für die Bedrohungserkennung und -abwehr. Laut einem neuen Report lösen jedoch 91 Prozent aller Angriffe keinen Alarm aus und 53 Prozent der Sicherheitsverletzungen erfolgen unentdeckt.

Welche vier Hürden einer besseren Bedrohungserkennung und -abwehr im Weg stehen, lesen Sie hier:

1. Falsche Herangehensweise beim Thema SIEM

Die meisten Unternehmen führen einfach alle Daten der Sicherheitsüberwachung zusammen und analysieren sie anschließend. Diese sind aber nicht alle relevant und verursachen Mehrarbeit sowie eine Verzögerung der Bedrohungserkennung.

2. Standardkonfigurationen reichen nicht

Viele Standard Logging-Konfigurationen erfüllen die individuellen Anforderungen an die Bedrohungssuche nicht. Das heißt, die konkrete Lage in den einzelnen Unternehmen bleibt unberücksichtigt.

3. Übermaß an Sicherungssystemen

Die meisten Unternehmen verstehen ihr Bedrohungsmodell nicht und sind mit den Technologien überfordert, die sie dann nicht effektiv nutzen.

4. Fehlende echte Priorisierung

Oft unterscheiden sich die Gefahren nicht in der Priorität. Wenn aber alle dieselbe Priorität haben, gibt es für sie keine Rangfolge, die im Umgang mit ihnen als Orientierung dienen kann. Dies erschwert ein gezieltes Vorgehen.

www.kudelskisecurity.com/de

VON GAMING, GANGSTERN UND GUTGLÄUBIGKEIT

WIE MFA UND ZERO TRUST EINE CYBERATTACKE VERHINDERT HÄTTE

Wie man einen der weltgrößten Gaming-Hersteller hackt? Ganz einfach: sich als Mitarbeiter ausgeben, IT-Team per Slack anchatten, vorgeben, sein Smartphone auf einer Party verloren zu haben – und schon erhält man Zugriff auf das Unternehmensnetzwerk. Keine Nachfrage. Keine Aufforderung, sich zu identifizieren. Und das einfach per Chat, ganz ohne Video. Was hier geschildert wird, ist ein realer Cyberangriff auf ein Gaming-Unternehmen der Weltklasse. Die Beute: 780 GB Daten, darunter Quellcode für Spiele sowie Entwicklungstools.

Das Interessante an dem Fall: Der Angriff gelang mit Hilfe eines Sicherheitstokens für ein Benutzerkonto und nicht über ein Passwort. Die Cyberkriminellen setzten ihn ein, um sich zunächst Zugang zum Chat des Unternehmens zu verschaffen. Nach dieser Hürde gaben sie sich als Mitarbeiter aus und erschlichen sich via Social Engineering einen langlebigen Login-Zugangs-Token für das Unternehmensnetzwerk. Im Netzwerk gelang es den Angreifern sich mit lateralen Bewegungen, Zugriff auf kritische Unternehmensdienste zu verschaffen.

EIN KONTINUIERLICHES SOCIAL-ENGINEERING-TRAINING INSBESONDERE FÜR IT- UND SERVICE-DESK-MITARBEITER ERGÄNZT DAS SICHERHEITSNETZ.

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

Tatsächlich sind Social Engineering Angriffe aktuell eine der bevorzugten Methoden von Hackern. Laut dem aktuellen Verizon DBIR Report gingen 2020 etwa 30 Prozent aller Datenverluste weltweit auf das Konto einer erfolgreichen Manipulation von Menschen. In 85 Prozent aller Angriffe waren Menschen direkt involviert und 61 Prozent der Sicherheitsverletzungen wurden durch entwendete oder kompromittierte Berechtigungen initiiert.

Gefahrenquelle Unachtsamkeit

Der Missbrauch von Token hat bei diesem Angriff eine zentrale Rolle gespielt. Zur Klarstellung: Ein Token ist kein Passwort oder Hash-Wert, sondern ein zufälliger, computergenerierter Zeichenfolgenwert, der geheime Informationen enthält. Statische, langlebige Token können Cyberkriminelle ähnlich einem Passwort missbrauchen.

Die „Ironie" bei dem Angriff ist, dass es die IT-Abteilung an Umsicht hat mangeln lassen. Dass ein einfacher Angriff via Chat-Tool gelang, hängt unmittelbar damit zusammen, dass der Service-Desk-Mitarbeiter nicht auf einen Videochat bestand. Die Identifikation des vermeintlichen Kollegen wäre um Einiges einfacher gewesen.

Dass solche Angriffe gelingen, kommt nicht von ungefähr. Der Service-Desk ist aktuell ein beliebtes Ziel für Angreifer, da er oft nicht über die entsprechenden Sicherheitsrichtlinien und -tools verfügt, um die Identitäten der Benutzer ordnungsgemäß zu überprüfen. Die Implementierung einer Multifaktor-Authentifizierung (MFA) verspricht hier ein gewisses Maß an Sicherheit. Jedoch nur dann, wenn sie für den Angreifer schwer oder gar nicht zu überwinden ist. Laut einer aktuellen Studie von Specops Software vertrauen allerdings die meisten Unternehmen, die bereits über Richtlinien zur Benutzerverifizierung verfügen, nur auf eine wissensbasierte Authentifizierung (KBA). Dabei müssen sich Mitarbeiter über die korrekte Beantwortung einfacher Fragen verifizieren – beispielsweise das Geburtsdatum. Die Krux: Es handelt sich hierbei um statische Informationen aus dem Active Directory oder einem HR-System, die sich mit etwas Aufwand von Hackern ermitteln lassen.

Deutlich sicherer ist es, bei der MFA-Implementierung, den Wissensfaktor mit dem Faktor „Besitz" zu ergänzen. Das kann beispielsweise ein FIDO2-Sicherheitsschlüssel sein oder ein Gerät als Identitätsnachweis. Die nächste Stufe ist dann ein starker biometrischer Faktor, wie etwa Gesichtserkennung. Die Kombination der verschiedenen Sicherheitsstufen ist essenziell für eine zuverlässige Gefahrenabwehr.

Ein kontinuierliches Social-Engineering-Training insbesondere für IT- und Service-Desk-Mitarbeiter ergänzt das Sicherheitsnetz. Dazu zählt vor allem, ein Bewusstsein für Phishing-Attacken zu

schaffen, das fest im Arbeitsalltag aller Mitarbeiter integriert sein muss.

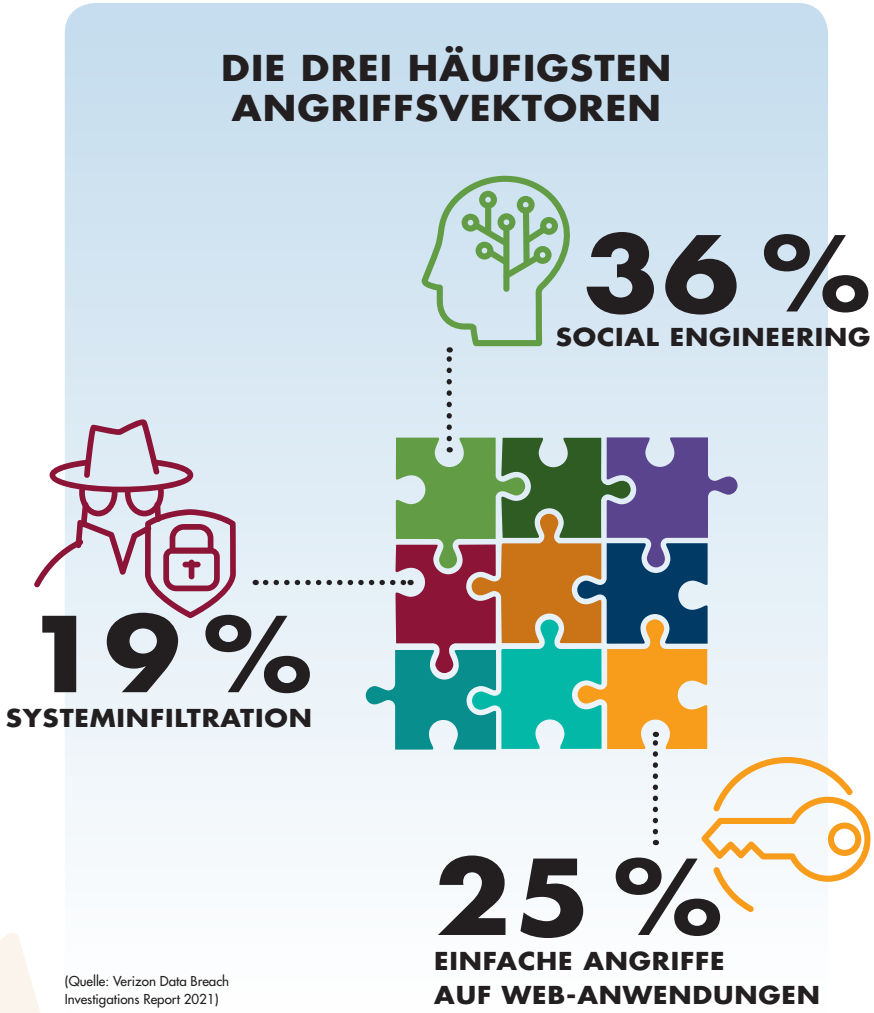
Zero Trust als Mittel der Wahl

Ein Zero-Trust-Sicherheits-Framework hätte diesem Angriff wirksam gegenüberstehen können. Es basiert auf dem Grundsatz: Vertraue niemandem, überprüfe jeden. Dabei spielen drei Kernsätze eine tragende Rolle, um die Angriffsfläche zu verringern:

- Der erste Grundsatz ist die Absicherung des Benutzers mit Zero Sign-On (ZSO). Es eliminiert Benutzerpasswörter und setzt auf stärkere Faktoren wie Besitz und Biometrie in der MFA-Implementierung. Darüber hinaus bietet der erste Grundsatz einen mehrschichtigen Anti-Phishing-Schutz, der die Anmeldedaten des Benutzers einschließlich der Zugriffstoken vor Diebstahl schützt.

- Der zweite Grundsatz besagt, dass der Zustand jedes Geräts überprüft wird. Dieses muss frei von Bedrohungen auf Geräte-, Netzwerk- und App-Ebene sein, bevor eine Verbindung zu Unternehmensressourcen zugelassen wird.

- Der dritte Grundsatz bezieht sich auf die Sicherung des Netzwerk-Gateways mit starken kontextbezogenen Zugriffsregeln. Sie erkennen auffälliges Benutzerverhalten im Netzwerk. On-Demand- und Pro-App-VPNs unterstützen zudem den Zero Trust Network Access (ZTNA)-Ansatz, indem sie nur dem authentifizierten Benutzer, der autorisierten App und dem verwalteten Gerät den Zugriff auf das Secure Access Gateway erlauben. Ein Software-definierter Perimeter (SDP) sichert das Netzwerk und die angeschlossenen Ressourcen weiter ab, da es sowohl die Kontroll- als auch die Datenebene abdeckt. Alle Ressourcen hinter dem Gateway sind für nicht autorisierte Benutzer, Apps und Geräte unsichtbar.



Die Implementierung eines Zero-Trust-Sicherheits-Frameworks hätte den Angriff auf das Gaming-Unternehmen zwar nicht komplett verhindert, aber die Auswirkungen abgeschwächt. Ivanti beispielsweise verfügt über alle Komponenten, welche die drei Grundpfeiler des Zero-Trust-Sicherheits-Frameworks ausmachen. Die Kombination von Endgeräteverwaltung und Technologien wie ZSO, MTD oder Zero-Trust-Access schränkt die Möglichkeiten eines Hackers massiv ein, sich Zugriff auf Daten zu verschaffen. Und die potenzielle Beute rückt plötzlich für Cyberkriminelle in weite Ferne.

All diese Sicherheitsvorkehrungen unterstützen letztlich IT-Mitarbeiter bei der Einschätzung von Risiken. So liefern sie beispielsweise Hinweise darauf, dass sich Aktionen häufen, die ein begründetes Misstrauen auslösen sollten. Das reicht von unüblich hohen Datentransfers, über eine nicht stimmige Geolocation bis hin zu verlorenen Geräten. Ziel ist es zu verhindern, dass der Faktor Mensch versagt.

Gegen Social Engineering anzugehen, ist ein Grundsatz für jedes Unternehmen und leider auch für alle IT-Teams. Das genannte Beispiel zeigt das Dilemma, in dem sich IT-Sec und IT-Ops aktuell befinden. Auf der einen Seite unternehmen IT-Teams alles, um Mitarbeiter im Everywhere Workplace zu unterstützen, produktiv arbeiten zu können – und das bei hoher Arbeitslast. Auf der anderen Seite wird von ihnen ein gesundes Mistrauen gegenüber ihren Kunden erwartet. Dieses Dilemma ist letztlich nur über Schulungen und den Einsatz automatisierter Lösungen auf KI-Basis zu lösen.

Johannes Carl

ZERO TRUST NETWORK

TRAUE NIEMANDEM, DAMIT DIR NICHTS BÖSES WIDERFÄHRT

Den Spruch aus unserer Kindheit kennen wir alle – „Sei vorsichtig, öffne keinem Fremden die Haustür". Was in der realen Welt in unserem Sicherheitsbewusstsein fest verankert ist, wird in der virtuellen Welt jetzt als zentraler Ansatz für die Authentifizierung von Benutzern und Endgeräten diskutiert.

Persönliche Daten gelten als das neue Gold des Internets und die neue Währung der digitalen Welt. Personenbezogene Daten wie Name, E-Mail-Adresse oder Einkommen dienen als wichtige Informationsquelle für gezielte Marketinganstrengungen, ein lukratives Ziel von Cyber-Kriminellen. Durch Diebstahl, Spionage und Sabotage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro. (Quelle: Bitkom, 8/2021)

Datendiebe lauern überall – lokal und in der Cloud

Externe Netzwerkzugriffe auf Unternehmensressourcen sind heutzutage Normalität. Geräte werden weltweit genutzt und können überall und zu jeder Zeit direkt auf Cloud-Dienste, E-Mail-Applikationen und andere potenziell vertrauliche Unternehmensressourcen zugreifen. Kriminelle können somit an unterschiedlichen Stellen ansetzen, um ihre Ransomware zu platzieren. Hier schiebt das Sicherheitskonzept Zero Trust einen Riegel vor. Es fußt auf der Philosophie, weder einem Gerät noch einem Benutzer einen Vertrauensvorschuss zu geben, bevor eine sichere Authentifizierung erfolgt ist. Im Mittelpunkt von Zero Trust stehen die Ressourcen – und nicht die klassische Perimeter-Sicherheit am Übergang zwischen einem Privat- oder Unternehmens-Netz und einem öffentlichen Netz, wie dem Internet. Das Konzept, ein Netzwerk zu errichten und es mit einer Firewall zu schützen, funktioniert nur noch bedingt, da Dienste und Daten nicht mehr lokal verwaltet werden. Die „New Worker" müssen mit allen Endgeräten und Apps auf Tools und Firmendaten zugreifen. Cloud-Dienste außerhalb der Firewall sind Elemente dieser flexiblen Umgebung.

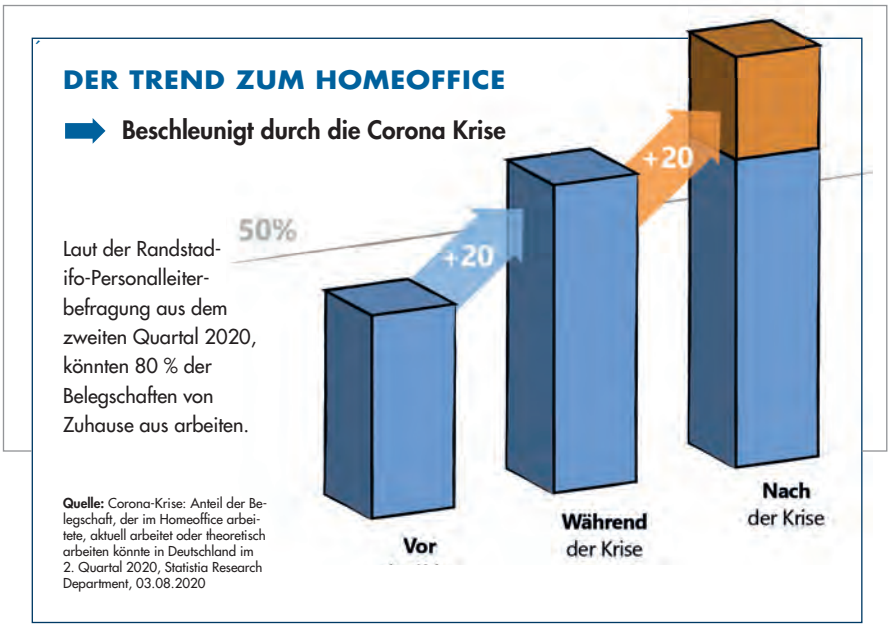
Dazu Christian Bücker, Geschäftsführer macmon secure GmbH: „Mit Zero Trust ist es möglich, die Datensicherheit nachhaltig zu gewährleisten und modernen Anforderungen an die Netzwerksicherheit zu entsprechen. Besonders bedroht fühlen sich mittelständische Unternehmen und Einrichtungen, die im Bereich KRITIS tätig sind, wie beispielsweise Krankenhäuser und Behörden, für die wir branchenspezifische Sicherheitslösungen anbieten."

Viele Unternehmen haben in den letzten Jahren in das Thema IT-Sicherheit investiert, oft jedoch sind die Maßnahmen nicht ausreichend, um einen wirklichen Schutz vor dem Eindringen Unbefugter zu bieten. Dagegen setzt das Zero-Trust-Konzept auf Restriktion und Monitoring. Die Idee dahinter ist über viele Jahre gereift. Bereits seit 2003 trägt macmon secure mit seiner Network-Access-Lösung (NAC) dem Ansatz Rechnung. Dieser erlaubt nur definierten Geräten Zugang zum Netzwerk, ganz gleich, ob iPads, Laptops oder medizintechnische Geräte. IT-Administratoren wissen jederzeit, welche Endgeräte im lokalen Netzwerk angemeldet sind, und können diese dank der kompletten Netzwerk-Übersicht permanent identifizieren und effizient überwachen. Jedes Endgerät, welches im jeweiligen Netzwerk nichts zu suchen hat, erhält von vornherein keinen Zugriff. Die unbefugte Nutzung

VORTEILE VON ZERO TRUST

Entscheider in den Bereichen IT & Security berichten von folgenden Vorteilen während und nach der Einführung von SDP.

ACCESS



der IT-Systeme ist damit nahezu ausgeschlossen.

New Normal erfordert New Security

Security-Experte Bücker ergänzt: „Unternehmen stehen vor der Herausforderung flexible Arbeitsformen in ihre Sicherheitsstrategie integrieren zu müssen. Um den Entwicklungen Rechnung zu tragen, hat macmon secure seine bewährte NAC-Lösung um macmon SDP (Secure Defined Perimeter) ergänzt. Es trägt den Zero-Trust-Network-Access-Gedanken in die mobile Welt und nutzt dabei die langjährigen Erfahrungen mit NAC."

Um die Identität eines Benutzers, seines Geräts und dessen Sicherheitszustand zu prüfen, übernimmt ein sogenannter SDP-Agent die Authentifizierung gegenüber einem SDP-Controller. Dieser arbeitet hochgesichert in einem ISO 27001-zertifizierten Rechenzentrum in Berlin. Ist die Authentifizierung erfolgreich, teilt er dem Agenten mit, ob der jeweilige Nutzer Zugriffsrechte auf die Unternehmensressourcen hat und welche das sind.

Mauern und Tunnel sind nicht mehr ausreichend

Um darüber entscheiden zu können, welcher Security-Ansatz sich für ein Unternehmen am besten eignet, ist eine qualifizierte Beurteilung wichtig. In den vergangenen Jahren standen vor allem perimeterbasierte Sicherheitsvorkehrungen im Vordergrund. Im Unterschied zu klassischen VPNs authentifizieren sich bei SDP sowohl der Benutzer als auch der Agent am Controller. Erst wenn beide als gültig erkannt werden, erfolgt der Zugriff auf das Netzwerk. Dank einer exakten Segmentierung entscheidet das System, wer mit welchem Gerät welche internen Ressourcen erreichen darf und übernimmt zudem die intelligente Steuerung der Kommunikationswege. So werden Bandbreitenengpässe vermieden, und möglichst geringe Latenzen gewährleistet. Jeder einzelne Zugriff auf Unternehmensressourcen – egal ob im Firmennetzwerk oder in der Cloud wird geprüft – es gibt keinen Vertrauensvorschuss.

Sage mir wer Du bist und ich sage Dir was Du darfst

macmon SDP überträgt die ZTNA-Idee auch auf sämtliche Cloud-Dienste und verfolgt einen identitätsbasierten Ansatz. Nach erfolgreicher Authentifizierung erreicht der Nutzer alle erforderlichen Ressourcen – entweder per Single Sign-On bei Cloud-Applikationen, über das SDP Cloud Gateway bei Cloud-Rechenzentren, oder über lokale SDP-Gateways auf die internen Unternehmensressourcen.

Der Ansatz ermöglicht eine granulare Zugriffssteuerung. Es kann bestimmt werden, ob der Zugriff auf eine Unternehmensressource lediglich bei voller, oder auch bei eingeschränkter Konformität der Identitätsmerkmale möglich ist. Weiterer Vorteil gegenüber virtuellen privaten Netzwerken ist die individuelle Festlegung von Richtlinien auf Benutzer- und Geräte-Ebene. Unternehmensnetzwerke sind heute in der Regel vielschichtig. macmon SDP reduziert die Komplexität effektiv, letztlich geht es immer um eine Identität, die Zugriffe benötigt. Die Spielregeln sind klar und werden von den Policies vorgegeben, der Aufwand hält sich im Vergleich zu anderen Ansätzen, die die Zugriffsberechtigung steuern, in Grenzen.

macmon SDP wird als Software as a Service (SaaS) angeboten. Der Pflegeaufwand seitens der Nutzer ist minimal, die Betriebskosten gering. Gleichzeitig ist die Lösung hoch skalierbar und wird in Deutschland in einem ISO-zertifizierten Rechenzentrum gehostet, der Support von einem internen Team in Berlin geleistet.

Sabine Kuch

www.macmon.eu

#WesecureIT

Weitergehende Informationen zu ZTNA erhalten Sie bei der „We Secure IT" Veranstaltung am 28. Oktober: https://www.it-daily.net/wesecureit/

VERSCHLÜSSELUNG IN UNTERNEHMEN

EINE WELTWEITE STUDIE VON ENTRUST GIBT EINBLICKE IN AKTUELLE TRENDS

Für die internationale Studie „Global Encryption Trends" wurden knapp 7.000 IT-Security Experten verschiedener Branchen aus 17 Ländern befragt, darunter Deutschland, Frankreich, das Vereinigte Königreich, Schweden, USA, Hongkong, Japan, Südkorea, Taiwan, Russland und Australien.

Im Rahmen der jährlich durchgeführten Untersuchung werden internationale Trends beim Einsatz von Verschlüsselungslösungen sowie deren Auswirkungen auf die Sicherheitslage von Unternehmen analysiert.

Dabei zeichnet sich bereits seit einigen Jahren eine Vorreiterrolle für Deutschland ab: Deutsche IT-Abteilungen adaptieren Verschlüsselungslösungen schneller als ihre internationalen Kollegen, egal ob On-Premises oder Cloud, egal ob für klassische Anwendungen wie TLS/SSL oder neuere wie Blockchain.

So geben derzeit 71 Prozent der Unternehmen in Deutschland an, dass sie über eine umfassende, konsequent angewandte Verschlüsselungsstrategie verfügen (ein weiterer Anstieg von 5 Prozentpunkten im Vergleich zum letzten Jahr) – weltweit können das nur 50 Prozent von sich behaupten. Für nahezu alle Anwendungen ist die Verschlüsselungsrate hierzulande höher als im weltweiten Durchschnitt: Nach wie vor ganz vorne rangieren Internetkommunikation (wie SSL) und Datenbanken. Backups und Archive sowie Plattformen/Datenspeicher für das Internet der Dinge verzeichnen im letzten Jahr hingegen die größten Wachstumsraten.

Beweggründe und Herausforderungen

Als wichtigen Beweggrund für die Verschlüsselung geben 69 Prozent der Unternehmen in Deutschland den Schutz persönlicher Kundendaten an. Im internationalen Vergleich fällt jedoch auf, dass für deutsche Unternehmen die Einhaltung externer Datenschutzbestimmungen eine besonders dominante Rolle spielt: Für 62 Prozent (gegenüber 45 Prozent weltweit) ist das der wichtigste Treiber für den Einsatz von Verschlüsselungslösungen. Andererseits geben nur 2 Prozent der deutschen Unternehmen an, dass die Vermeidung negativer Publicity nach einem Datenschutzverstoß für sie ein wichtiger Grund ist (hier liegt der weltweite Durchschnitt immerhin bei 16 Prozent).

Befragt nach den größten Herausforderungen bei der Ausführung ihrer Verschlüsselungsstrategie nennen Unternehmen in Deutschland am dringlichsten das Problem der Lokalisierung sensibler Daten. 83 Prozent sehen hierin eine Herausforderung, verglichen mit 65 Prozent weltweit. Obwohl mittlerweile also eine breite Palette von Kunden-, Mitarbeiter-, Finanz- und Gesundheitsdaten verschlüsselt wird, stellt deren Verortung nach wie vor eine der größten Herausforderungen dar. Zudem erschwert der Mangel an qualifiziertem Personal deutschen Unternehmen die Verwaltung ihrer Verschlüsselungskonzepte – 64 Prozent geben dies in Deutschland als große Schwierigkeit an, gegenüber 57 Prozent weltweit.

Großes Vertrauen in Hardware-Sicherheitsmodule (HSMs)

Umso mehr setzen deutsche Unternehmen auf hochsichere Hardware-Sicherheitsmodule (HSMs) für die Verwaltung und den Schutz unternehmenskritischer Schlüssel – sie stellen für 70 Prozent ein zentrales Element ihrer Verschlüsselungsstrategie dar (gegenüber 49 Prozent weltweit). Sei es im Zusammenhang mit PKI oder der Verwaltung von Zertifikaten, bei der Verschlüsselung auf Anwendungsebene oder in der Public Cloud (BYOK), sei es für TLS/SSL, IoT, oder Blockchain-Anwendungen – HSMs werden in Deutschland über nahezu alle Szenarien hinweg häufiger eingesetzt als in den meisten anderen Regionen.

Das Bemühen um die Datensicherheit scheint sich für deutsche Unternehmen auch bezahlt zu machen: Nur 32 Prozent der Unternehmen geben an, in den letzten Jahren eine Datenschutzverletzung erlitten zu haben – der weltweite Durchschnitt lag mit 44 Prozent deutlich höher.

www.entrust.com

DOMAIN-SPOOFING

CYBER THREAT INTELLIGENCE & BRAND PROTECTION

Die Website oder E-Mail-Domain von Unternehmen zu fälschen ist heute so einfach wie noch nie. Kein Wunder, dass Domain-Spoofing daher zu den beliebtesten Phishing-Taktiken zählt. Innerhalb von nur vier Monaten in 2021 fand Digital Shadows rund 360 verdächtige Domains. Aufs Jahr gerechnet muss sich jedes Unternehmen mit rund 1.100 Fake-Domains herumschlagen – und damit mit potenziell 1.100 Fällen von Markenmissbrauch und Reputationsschaden.

Woher kommt dieser Trend? Zum einen unterliegt die Vergabe von Domains keinen strengen Kontrollen. Zum anderen wimmelt es auf Marktplätzen im Darknet von entsprechenden Phishing-Kits, Tutorials und Templates. Basis-Pakete sind bereits ab 50 Dollar erhältlich. Zudem werden die Fake-Domains immer ausgefeilter, hosten Inhalte und besitzen DNS-Einträge.

Für Unternehmen, deren Marke missbraucht wird, ist die Lage schwierig. Nicht jede mögliche Domain-Permutation kann präventiv aufgekauft werden. Um das Sicherheitsrisiko proaktiv zu minimieren, heißt es die Augen offenhalten. Monitoring-Tools wie SearchLight melden automatisch neu registrierte Domainnamen, die dem Unternehmensnamen ähneln, und leiten Takedown-Verfahren ein. Die hochgradig gefilterten, kontextualisierte Alerts liefern detaillierte Informationen sowie eine individuelle Risikoeinstufung, um die Bedrohung besser bewerten zu können. Irrelevante Meldungen lassen sich so bereits im Vorfeld aus dem Threat Intelligence-Feed herausfiltern. Das vereinfacht die Triage für Sicherheitsteams und reduziert den Zeitaufwand beim Management von Domain-Spoofing um bis zu 75 Prozent.

Screenshot SearchLight:
Automatische Alerts bei Domain Spoofing
(Quelle: Digital Shadows)

Robert Blank | www.digitalshadows.de

IOT SECURITY

PRODUKTIONSNETZE ZUVERLÄSSIG SCHÜTZEN

Ist meine Produktion sicher? Diese Frage stellt sich Industrieunternehmen drängender denn je. Denn mit der zunehmenden Automatisierung und Digitalisierung von Produktionsumgebungen steigt auch die Anzahl möglicher Einfallstore für Cyberkriminelle rasant. Unternehmen brauchen ein solides Cyber-Security-Konzept, um sich zu schützen. Eine automatisierte Cyber-Security-Lösung kann hierbei wichtige Dienste leisten und eine umfassende Sicherheit im Produktionsnetz bieten.

Cyber-Attacken nehmen zu. Datenklau, die Manipulation von Anlagen, Erpressungsversuche – die Liste ist lang und wird immer länger. Drei Viertel der Wirtschaft sind mittlerweile betroffen. Nicht nur die großen Unternehmen, auch der Mittelstand steht im Fokus der Cyber-Kriminellen; das Innovationspotential ist hier hoch. Produktion und Fertigung zählen zu den häufigsten Angriffszielen – nicht zuletzt, weil das Sicherheitsniveau in der Operational Technology (OT) im Allgemeinen sowieso geringer ist als in der Information Technology (IT). Als Szenario sehr beliebt: die digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen. Als Folge drohen Arbeitsausfälle und finanzielle Schäden von nicht unerheblicher Natur.

Angriffsvektoren en Masse

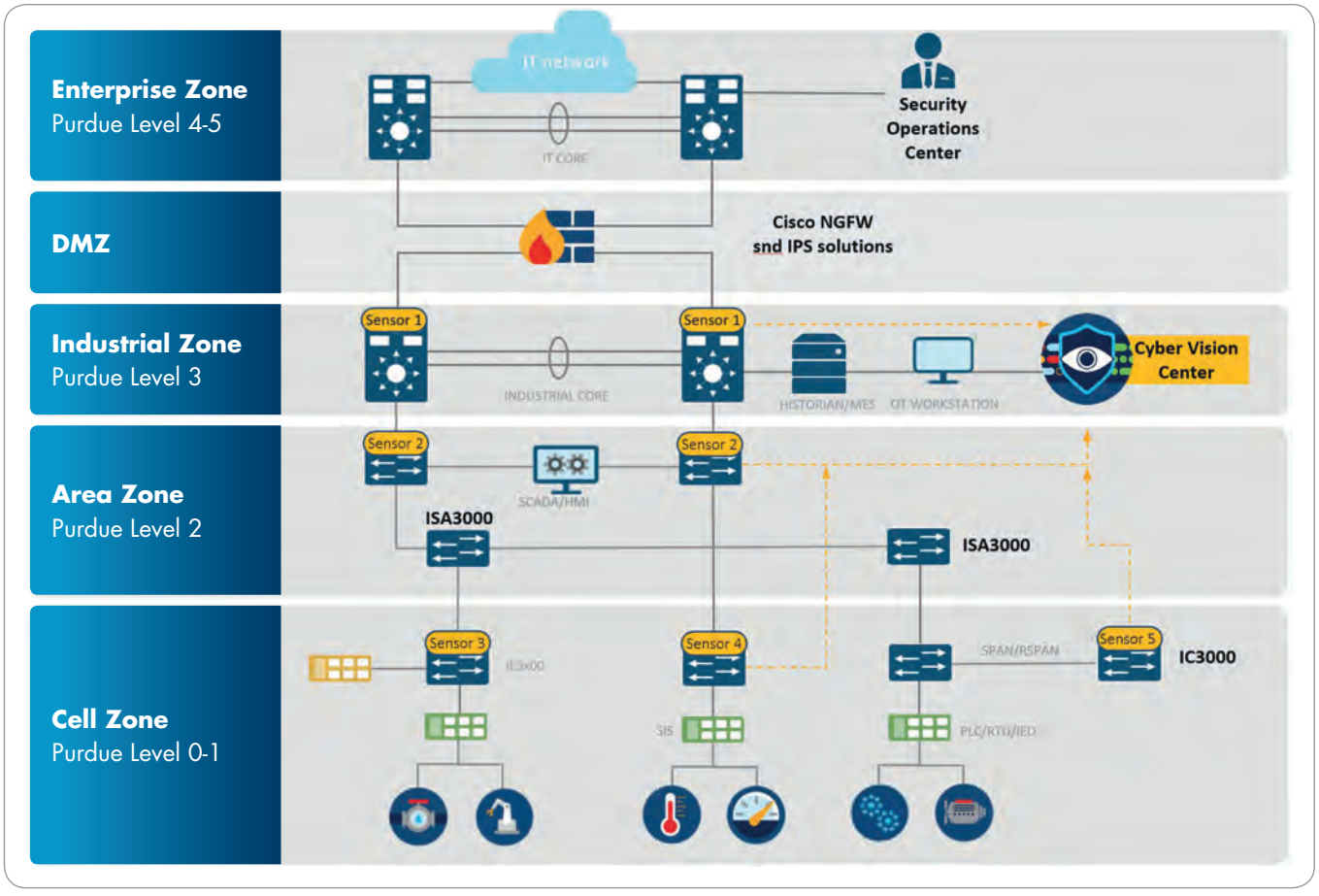
Die Ursachen des Übels sind meist „hausgemacht". Unternehmen, die wettbewerbsfähig bleiben möchten, müssen ihre Produktionsprozesse zunehmend automatisieren; nur so bleiben diese effizient. Als Folge dieser Automatisierung sind industrielle Umgebungen heute stärker vernetzt denn je. Neben Maschinen, Sensoren und Switchen mischen auch Telefone, Tablets, Scanner, Human Device Interfaces und oft viele weitere Unbekannte in der Kommunikation mit. IT und OT stehen dabei allerdings zu selten in einem echten Austausch. Hinzu kommt, dass gerade die OT unter Security-Gesichtspunkten oft (immer noch) zu stiefmütterlich behandelt wird. Die Folge: Die IIoT (Industrial Internet of Things)-Umgebung ist höchst unübersichtlich – und wird zu selten zentral und nicht umfassend genug überwacht. Cyber-Kriminelle frohlocken, bieten diese Umgebungen doch recht einfache Angriffsvektoren. Die Sicherheitsverantwortlichen dagegen müssen immer komplexere Aufgaben bewältigen. Denn für sie ist es zunehmend schwieriger, den Überblick zu behalten, Angriffe zu erkennen, abzuwehren und/oder adäquat auf sie zu reagieren.

Wie sicher ist meine Produktion?

Um derartige Sorgen zu minimieren, müssen sich die Security-Verantwortlichen wichtige Fragen stellen, darunter: Was mache ich, wenn die klassischen Konzepte nicht (mehr) ausreichen? Welche Lösungen sind die richtigen für mich? Was muss ich tun, damit meine Infrastruktur vor Angriffen sicher ist? Wie kann ich Produktionsausfälle vermeiden? Um die richtigen Antworten finden zu können, gilt es zunächst, den IST-Zustand zu ermitteln. Von entscheidender Bedeutung hierbei ist, ob alle Netzwerk-/Kommunikationsteilnehmer und -wege bekannt sind. So können beispielsweise „Altlasten" wie ausgediente Scanner, die unter dem Radar laufen, schnell zu einer Sicherheitslücke werden. Dies geht mit der Frage einher, ob alle Angriffspunkte tatsächlich bekannt sind. Sprich, bekomme ich es überhaupt mit, wenn ich angegriffen werde? Und wie reagiere ich im Zweifelsfall darauf? An dieser Stelle kann es sinnvoll sein, den Status Quo von externen Experten prüfen zu lassen, insbesondere wenn es an internem Know-

DENKT MAN AN CYBER SECURITY, SOLLTE IMMER DER FOKUS AUF EINEM LANGFRISTIGEN LÖSUNGSANSATZ LIEGEN. PFLASTER HELFEN SCHNELL, ABER NICHT LANGE UND HALTEN NUR EINEN BEGRENZTEN ZEITRAUM.

Thomas Kugelmeier, Client Solution Executive, Logicalis GmbH, www.logicalis.de



how und Ressourcen mangelt. So sind die Mitarbeiter im OT-Bereich in puncto Security selten besonders versiert, den IT-Mitarbeitern hingegen mangelt es meist am notwendigen Verständnis für die OT – von ihren längst erreichten Kapazitätsgrenzen einmal ganz abgesehen.

Hand in Hand: IT und OT

Externe Hilfe kann auch vonnöten sein, wenn es nach der Bestandsaufnahme darum geht, die richtige Lösung für – beziehungsweise gegen – die aufgedeckten Sicherheitsproblematiken zu finden. Von Cyber Security über eine OT-Asset-Inventarisierung, die Regulierung von Kommunikation und die Bewertung von Schwachstellen bis hin zu Maßnahmen für die Infrastruktur gilt es hier, einen umfassenden Weg zu beschreiten. Wichtig in diesem Prozess ist vor allem, dass IT und OT zusammenarbeiten; denn eine Security-Lösung muss beiden Seiten gerecht werden und alle Bereiche schützen. Nur dann ist sie wirklich effektiv.

Transparenz von Anlagen und Prozessen

Cyber-Security-Lösungen können einen wichtigen Beitrag für ein ganzheitliches Cyber-Security-Konzept leisten. So wurde beispielsweise Cisco Cyber Vision speziell für die OT entwickelt, um Produktionskontinuität, Widerstandsfähigkeit und Sicherheit zu gewährleisten; notwendige Schnittstellen für eine ganzheitliche IT-OT-Sicherheitsstrategie inklusive. Die Lösung lässt sich nahtlos in den operativen Betrieb integrieren und liefert einen vollständigen Überblick über die IoT-Umgebung. Hierfür überwacht sie passiv die Teilnehmer eines Netzwerks – sprich die Kommunikation von Maschinen und Geräten – und extrahiert daraus Informationen, die Aufschluss über die gesamte Infrastruktur geben. Die Antworten auf wesentliche Fragen rund um mögliche Schwachstellen und Anomalien liefert sie übersichtlich und in Echtzeit; nebst daraus resultierendem Maßnahmenkatalog. Außerdem wichtig: Cisco Cyber Vision bietet die Basis für die Absicherung und Migration industrieller Netzte nach dem „Zones and Conduits" Prinzip der IEC62443 Normierung, bei dem verhindert wird, dass sich einzelne Angriffe auf die gesammte Infrastruktur ausbreiten.

Dem klassischen Aufbau einer Produktionsumgebung entsprechend (siehe Bild) besteht Cisco Cyber Vision aus zwei Architekturstufen. Stufe 1 bilden die Cyber-Vision-Sensoren, die direkt in die Netzwerkstruktur integriert werden und

unmittelbar auf Switchen, Routern oder Compute-Einheiten der unterschiedlichen Produktionszonen laufen. Sie überwachen den Netzwerkverkehr und leiten die Metadaten an das Cyber Vision Center weiter („bottom up"). Dieses sammelt dann in Stufe 2 die von den Sensoren ermittelten Daten und stellt die Logik für Analyse und Auswertung bereit. Auf dieser Basis können Unternehmen (bzw. ihre Security Operations Center, SOC) die richtigen Sicherheitsrichtlinien erstellen und durchsetzen („top down"). Es ist ihnen dabei außerdem möglich, ein konvergentes SOC aufzubauen, das, gespeist mit den Daten beider Welten (IT und OT), extrem schnell auf Sicherheitsvorfälle reagieren kann.

Mikrosegmentierung schafft Sicherheitsbarrieren

Ein wichtiger Ansatz in puncto Sicherheit ist und bleibt aber auch das Thema Mikrosegmentierung. Definierte Bereiche des Netzwerks werden stark in der Kommunikation ihrer Teilnehmer und untereinander reglementiert, damit wirklich nur diejeningen miteinander sprechen, die es auch wirklich müssen. Dies erfolgt in Anlehnung an die IEC62443 Normierung und ermöglicht eine sehr gute Eingrenzung von Angriffen und Schadensregulierung. Angreifer können sich so nicht mehr „frei" im Netzwerk bewegen, sondern scheitern an den jeweils gebauten Barrieren. Nicht betroffene Teile der Produktionsstrecke bleiben damit von Angriffen unberührt und können weiterarbeiten. Wichtig hierbei: Physische und virtuelle Plattformen müssen gleichermaßen bedacht werden. Die Krux: Der Komplexitätsgrad rund um das Thema Mikrosegmentierung ist hoch. Verfügt ein Unternehmen jedoch über ein ganzheitliches Security-Konzept samt Cyber-Security-Lösung, liefert diese die notwendige Datenbasis für eine Mikrosegmentierung quasi direkt mit.

Für welchen Weg auch immer, Unternehmen müssen sich entscheiden – das Motto „Never Change a Running System" ist nicht länger tragbar. Denn klar ist, dass Firmen die Produktion bestmöglich vor Cyber-Angriffen schützen müssen, um Störungen des Ablaufs und kostenintensive Produktionsausfälle zu verhindern. Sprich, mit dem Automatisierungsgrad von Anlagen und Netzwerken muss für Unternehmen auch der Automatisierungsgrad der Security steigen, wollen sie zukunftssicher aufgestellt sein.

Thomas Kugelmeier

DATENSCHUTZ

DIE DSGVO SETZT UNTERNEHMEN UNTER DAUERDRUCK

Ein aufwändiger Prüfprozess vor der Einführung jedes digitalen Tools, regelmäßig neue Entscheidungen der Aufsichtsbehörden und Gerichtsurteile in ganz Europa, die Auswirkungen auf das eigene Unternehmen haben können – die Anforderungen an den Datenschutz setzen Unternehmen in Deutschland unter Dauerdruck.

Zugleich bekommen die Aufsichtsbehörden keine guten Noten für ihre Beratung. Die Hälfte der Unternehmen (50 Prozent) sagt, Deutschland übertreibe es mit dem Datenschutz. Zwei Drittel (66 Prozent) sind der Auffassung, dass der strenge Datenschutz sowie die uneinheitliche Auslegung des Datenschutzes in Deutschland die Digitalisierung erschwert. Das sind Ergebnisse einer repräsentativen Befragung des Bitkom. „Dem Datenschutz kommt in der digitalen Wirtschaft und Gesellschaft eine besondere Bedeutung zu. Den Unternehmen fehlt es aber zunehmend an Planbarkeit und Verlässlichkeit", sagt Susanne Dehmel, Geschäftsleiterin Bitkom. „Unternehmen stehen beim Datenschutz unter permanenten Stress. Sie wollen dem Datenschutz Genüge tun, aber dazu müssen sie nicht nur europaweit Gerichtsurteile verfolgen und die unterschiedliche Auslegung aus den Mitgliedsstaaten kennen, sondern sich zusätzlich mit 18 verschiedenen Lesarten von Datenschutzaufsichten allein in Deutschland auseinandersetzen. Das ist vor allem für kleinere Unternehmen immer schwerer zu stemmen.

Vier von zehn (42 Prozent) Unternehmen geben an, dass sie seit der DSGVO-Einführung mehr Aufwand haben – und dieser auch künftig bestehen bleiben wird. Ein weiteres Drittel (32 Prozent) geht sogar davon aus, dass der Aufwand weiter steigen wird. Nur 19 Prozent erwarten, dass ihr gestiegener Aufwand langsam wieder sinkt.

www.bitkom.org

nevis®

The Nevis experience.
A safe experience.

Lösungen für mehr IT-Sicherheit

Ransomware-Angriffe und Passwort-Leaks sind allgegenwärtig, die Gefährlichkeit der Cyberattacken nimmt zu. Doch wie schätzen User und IT-Entscheider die Lage ein? Und wie lassen sich Login-Informationen und Daten noch besser vor unbefugtem Zugriff schützen? Antworten auf diese und andere Fragen hat Nevis im Sicherheitsbarometer 2021 zusammengefasst. Und zeigt, dass es für ein optimales Kundenerlebnis einen ebenso einfachen wie sicheren Login-Prozess braucht.

Making security an experience.
nevis.net

Jetzt Whitepaper herunterladen

PATCHEN

IMMER, ABER NICHT OHNE TESTEN

In schöner Regelmäßigkeit veröffentlicht Microsoft Updates für Windows Updates und schließt damit Sicherheitslücken. Mit einem simplen „installieren und gut ist's" ist es aber nicht getan: Alle Updates sollten vor einem unternehmensweiten Rollout getestet und nicht direkt produktiv eingesetzt werden. Um das Risiko von Problemen zu minimieren, hat Windows sog. Bereitstellungsringe entwickelt. Aber wie genau funktionieren die eigentlich?

Updatehandling und -kreise

Die Bereitstellungsringe sind eine Methode, um Computer in Gruppen aufzuteilen und diese nacheinander mit dem neuen Updates zu versorgen. Die Ringe müssen in der Regel nur einmal definiert werden. Es liegt jedoch an der IT, die gebildeten Ringe regelmäßig zu überprüfen, um sicherzustellen, dass die Sequenzierung weiterhin korrekt ist.

Gearbeitet wird dabei mit 3 Ringen: Zunächst werden einige wenige Key-User versorgt. Wenn soweit keine Probleme auftauchen, wird in einer ersten Welle eine überschaubare Anzahl an Arbeitsplätzen geupdatet und erst wenn hier keine Probleme auftreten, kommt mit einer zweiten Welle der ganze Rest. Alle Mitarbeiter werden je nach ihrem Tätigkeitsbereich im Unternehmen in die verschiedenen Bereitstellungsringe eingeteilt. Dabei ist es wichtig, zu beachten, dass nicht jeder innerhalb einer Abteilung sich im gleichen Ring befinden sollte. Denn wenn ein Fehlerfall auftritt, wird das gesamte Team lahmgelegt.

Patchmanagement über UEM

Wichtig bei der Umsetzung ist, aus welchen Quellen die teilweise sehr großen Updates an die Geräte verteilt werden, je nachdem ob ein WSUS als lokales Update Repository im Einsatz ist oder nicht. Geräte die selten über das interne Netz erreichbar sind, sollten direkt über die von Microsoft zur Verfügung gestellten Patches versorgt werden. Dadurch wird die VPN Verbindung ins Unternehmensnetzwerk weniger stark belastet und viel Bandbreite gespart.

Um die Auslastung der Netzwerkbandbreite weiter zu verringern, unterstützen Unified Endpoint Management (UEM) Lösungen wie zum Beispiel baramundi die Delivery Optimization von Microsoft. Diese hilft dabei, die Arbeit der Bereitstellung von mehreren Patches untereinander effizient aufzuteilen.

Bildung dynamischer Gruppen

Um besser erkennen zu können, bei welchen Geräten doch noch Handlungsbedarf besteht, empfiehlt es sich dynamische Gruppen zu bilden, um den jeweiligen Patchstand der Clients zu sehen. Dynamische Gruppen sind nichts anderes als Filter, die auf Basis frei konfigurierbarer Kriterien Geräte in Gruppen zusammenfassen. Am Ende können so Updates zuverlässiger, schneller und effizienter verteilt werden.

Durch die Inventarisierung des Windows Security Center wird fortan der Status der Windows-eigenen Schutzmechanismen (Firewall, UAC, Defender) angezeigt. Die Werte sind auch über dynamische Gruppen filterbar, sodass automatisiert auf Sicherheitsvorfälle reagiert werden kann.

Fazit

All diese Elemente können Admins mit Hilfe eines Patchmanagements als Teil einer UEM-Lösung optimal steuern. Damit haben Admins einen guten Überblick über die aktuelle Patch-Situation und auch die notwendigen Werkzeuge, um auf eine akute Bedrohungslage richtig und schnell reagieren zu können. So zum Beispiel die Installation von Patches, Microsoft Anti-Virus Defender Definitions-Updates und dem damit zusammenhängenden Anti-Viren Scan.

Felix Zech | www.baramundi.de

IT-SICHERHEIT

PROTEKT 2021 BIETET KRITIS-BETREIBERN UMFANGREICHES EXPERTENWISSEN

Auf der protekt, die am 10. und 11. November 2021 in der KONGRESSHALLE am Zoo Leipzig stattfindet, erhalten KRITIS-Betreiber umfangreiches Expertenwissen rund um den Bereich IT-Sicherheit. Das Konferenzprogramm widmet sich brandaktuellen Themen, Aussteller präsentieren praxiserprobte Lösungen und der Veranstaltungsrahmen ermöglicht intensives Networking.

Isabel Münch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erklärt, welche Entwicklungen nach dem Inkrafttreten des IT-Sicherheitsgesetzes 2.0 auf kritische Infrastrukturen zukommen. Brandaktuell stellt Thomas Haase, Leiter Certified Security bei T-Systems Multimedia Solutions, eine IST-Analyse zu Krisenmanagement und -kommunikation im Rahmen der Unwetterkatastrophe in Rheinland-Pfalz vom Juli dieses Jahres vor.

Darüber hinaus hält der Track IT-Security zahlreiche weitere spannende Themen bereit, beispielsweise zu integrierten ITSC-/IS-Managementsystemen und sicheren Cloud-Lösungen für Banken und Versicherungen. Die Teilnehmer erwarten außerdem Vorträge zur effizienten Erkennung und Eindämmung von APTs und Ransomware, Erfahrungsberichte zum Umgang mit digitalen Angriffswellen sowie zu An- und Herausforderungen beim Datenschutz in kritischen Infrastrukturen. Ebenfalls behandelt werden die Konzeption und Prüfung von rechtskonformer Künstlicher Intelligenz und ein Prüfer berichtet, auf welche gravierenden Schwachstellen in kritischen Infrastrukturen er im Rahmen seiner Tätigkeit regelmäßig stößt.

Für die Sicherheit aller Beteiligten sorgt das praxiserprobte Hygienekonzept „SafeExpo" der Leipziger Messe.

www.protekt.de

protekt
10. – 11.11.2021
leipzig

DIGITALE FORENSIK

IHRE BEDEUTUNG NIMMT ZU

Das SANS Institute stellt die Ergebnisse seiner Digital Forensics Umfrage 2021 vor. Sie beschäftigt sich mit der Professionalisierung des Berufszweigs und der Bewertung der Fähigkeiten durch die Befragten. Die Umfrage zeigt, dass die meisten der 370 Umfrage-Teilnehmer grundlegende Fähigkeiten und Wissen schätzen und sich auch der Folgen bewusst sind, falls diese nicht vorhanden sind.

Nicht nur im strafrechtlichen als auch im zivilrechtlichen Bereich nimmt die Zahl der Ermittlungen, bei denen die digitale Forensik einbezogen wird, dramatisch zu. Um dieser wachsenden Nachfrage gerecht zu werden, ist auch die Zahl der Organisationen, die digitale forensische Dienstleistungen anbieten, und die Zahl der in der digitalen Forensik tätigen Personen gestiegen. Die digitale Forensik ist als Berufszweig inzwischen etwa drei Jahrzehnte alt und gilt als etablierter Strang der forensischen Wissenschaft, die in der straf- und zivilrechtlichen Praxis weltweit verankert ist.

„Diese Ergebnisse bestätigen, dass Praktiker im Bereich der digitalen Forensik idealerweise über Kompetenzen in den Bereichen Fachwissen und Anwendungsfähigkeiten verfügen sollten, kommentiert Jason Jordaan, Studienautor, SANS-Instructor und leitender forensischer Analytiker bei DFIRLABS. „Besorgniserregend ist jedoch, dass ein kleiner Prozentsatz der Teilnehmer angibt, dass sie die Bedeutung von Fähigkeiten und Kenntnissen, die als grundlegend und wesentlich für die Ausübung der digitalen Forensik gelten, unterschätzen."

11 Prozent der Befragten stuften beispielsweise Software-Engineering als unwichtig ein. Bei den zentralen Nicht-Informatik-Disziplinen, zu denen Kommunikation, Datenanalyse, investigative Recherche, Ethik, Recht, Mathematik und Statistik, Kriminologie und forensische Wissenschaft gehören, gaben ebenso fast 11 Prozent an, dass Ethik eine eher unwichtige Rolle spielt. Sie ist jedoch von entscheidender Bedeutung.

Obwohl die meisten Teilnehmer die grundlegenden Skills und das Fachwissen als wichtig anerkennen, gibt es immer noch erhebliche Lücken bei einigen wichtigen Fähigkeiten. Die Befragten erkannten zwar die Konsequenzen von fehlerhaftem Arbeiten, jedoch nicht , wie wichtig bestimmte Skills sind. Es gilt also, besonders diese Kompetenzen zu stärken und das Bewusstsein für diese speziellen Fähigkeiten zu schärfen.

www.sans.org

DIGITALE FORENSIK

Die grundlegendsten Bereiche sind:

- Computer und Medien Forensik
- Smartphone und mobile Geräte Forensik
- Speicherforensik
- Netzwerkforensik
- Malware-Forensik

RAUS AUS DEM SCHATTEN

WARUM SCHATTEN-IT GROSSE RISIKEN BIRGT UND WIE MAN SIE BEI MESSENGERN VERMEIDET

Als „Schatten-IT" wird Hard- und Software bezeichnet, die Mitarbeiter abseits der offiziellen IT-Infrastruktur eines Unternehmens für geschäftliche Zwecke einsetzen. In einer Umfrage von Forcepoint erklärten fast zwei Drittel aller befragen Arbeitnehmer (63 Prozent), dass sie Inhalte und Dokumente Ihres Unternehmens auch über private Hardware verwalten. Laut einer Studie von Censuswide (2019) gaben 53 Prozent aller IT-Leiter an, mehr als jeder zweite Mitarbeiter nutze Anwendungen jenseits der Kontrolle der IT-Verwaltung.

Bei der Schatten-IT handelt es sich also nicht nur um wenige Einzelfälle, sondern um ein grassierendes Problem. Eine Ursache ist die steigende Anzahl an Cloud-Diensten, Software-as-a-Service-Angeboten und privaten Messenger-Diensten, auf die Angestellte schnell und einfach zugreifen können und deren Handhabung aus dem Privatgebrauch bekannt ist. Sobald Prozesse im beruflichen Alltag nicht reibungslos ablaufen und die Hilfe der IT-Abteilung nicht greifbar ist, suchen Mitarbeiter nach eigenen Wegen zur Lösung ihrer IT-Probleme.

Auch die Arbeit im Homeoffice begünstigt das Aufkommen von Schatten-IT. Privat nutzen Angestellte unter Umständen Software, die hinsichtlich Sicherheit und Datenschutz bedenklich ist. Die Corona-Pandemie hat für eine weitere Zunahme an unkontrollierter IT im Business-Umfeld gesorgt.

Datenschutzrisiko private Messenger

Bei der Verwendung privater Messenger für berufliche Zwecke landen vertrauliche Informationen oft ungeschützt in den Händen privater IT-Dienstleister. Nicht einmal moderate Sicherheitsanforderungen werden so erfüllt, und interne Firmendaten können leicht nach außen gelangen. Außerdem unterliegen viele Chat-Apps dem amerikanischen Datenschutzgesetz, welches nicht mit der Datenschutz-Grundverordnung (DSGVO) vereinbar ist, denn Dienste mit Sitz in den USA müssen den dortigen Geheimdiensten Zugang zu Kundendaten gewähren. Die Nutzung von Chat-Diensten aus den USA stellt daher ein hohes Datenschutzrisiko dar.

Setzen Mitarbeiter WhatsApp für die Kommunikation mit Kunden oder Arbeitskollegen ein, leiten Sie die Kontaktdaten ohne Zustimmung der Beteiligten an den Mutterkonzern Facebook weiter, wo die Informationen zu Marketingzwecken verwendet werden. Auch hinsichtlich der Nutzer-Administration genügen private Messenger-Dienste den Anforderungen von Unternehmen in keiner Weise.

Internen Messenger anbieten

Mit dem Business Messenger Threema Work treten Sie diesen Risiken wirkungsvoll entgegen. Ihre Mitarbeiter finden sich dank der intuitiven Benutzeroberfläche auf Anhieb in der App zurecht und haben aufgrund des breiten Funktionsumfangs keinen Anlass mehr, auf private Chat-Dienste zurückzugreifen. Das Management-Cockpit ermöglicht IT-Administratoren eine bequeme Vorkonfiguration der App und erlaubt, Funktionen nach Bedarf einzuschränken. Die Threema Work-Apps sind Open Source, und der Dienst genügt vollumfänglich den strengen Datenschutzbestimmungen der DSGVO. Kein anderer Messenger bietet ein vergleichbar hohes Mass an Sicherheit und Datenschutz.

threema.ch/work

Threema.Work
Secure enterprise messaging

STRAFEN IN MILLIONENHÖHE DROHEN

Bei Verstößen gegen die DSGVO drohen Geldbußen bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Vorjahresumsatzes. Sanktionen in Millionenhöhe wurden tatsächlich bereits verhängt – insgesamt waren es im Jahr 2020 ca. 160 Millionen Euro. WhatsApp wurde von der irischen Datenschutzbehörde unlängst sogar mit einer Geldstrafe von 225 Millionen Euro wegen eines Verstoßes gegen die DSGVO belegt.

#WesecureIT

We secure IT

Digitalevent

28.10.2021

IT- und Security-Verantwortliche können sich auf der virtuellen Konferenz in Live Vorträgen, Live Demos und Diskussionsrunden über aktuelle Themen der Cybersecurity informieren. Auf zwei Kurzvorträge folgt jeweils eine Q&A-Runde.

Die Konferenz findet live am Donnerstag, 28. Oktober 2021, von 09:00 bis 16:30 Uhr statt. Die Teilnahme ist kostenlos.

Highlights aus der Agenda

Cloud Security

Zero Trust Network Access – Einfach gelebt in einer mobilen Welt
Christian Bücker, CEO, macmon secure GmbH

Endpoint Security MDR & EDR

Machine Learning und Künstliche Intelligenz – die Grundlage gegen immer komplexere Angriffe
Mihai Bapascu, Senior Solution Architect, Bitdefender

Security Management

Cyber Security als Geschäftsprozess
Andreas Nolte, Head of Cyber Security, Arvato Systems

Threat Protection/Detection

Mensch und Maschine im Spannungsfeld der Cybersicherheit
Matthias Canisius, Regional Director, SentinelOne

People Centric Security

Vom Human Risk zur Human Firewall
Charline Kappes, Awareness Specialist, SoSafe GmbH

Mobile Security

MTD, Phishing-Schutz und risikobasierte Schwachstellenanalyse: Effektive Absicherung mobiler Infrastrukturen
Peter Machat, VP Central EMEA, Ivanti

Jetzt anmelden

SCAN ME

www.it-daily.net/wesecureit/

macOS SICHERHEIT IN UNTERNEHMEN SO GEHT'S AUCH KEXTLOS

Apple bietet nativen Schutz der Privatsphäre und der Geräte, aber kein Betriebssystem ist perfekt. Die hohen Anforderungen an Sicherheit erstrecken sich über jedes Betriebssystem, und macOS macht keine Ausnahme. Apple hat viel investiert, um native Datenschutz- und Sicherheitsfunktionen bereitzustellen. Mit zunehmendem Marktanteil von Mac im Unternehmen steigt jedoch auch die Gefahr von schädlicher Software, Sicherheitsverletzungen und Sicherheitslücken. Unternehmen erlauben ihren Mitarbeitern mehr denn je, macOS über Mitarbeiterauswahlprogramme zu nutzen. Dabei stellten sie fest, dass wie bei jeder anderen Plattform zusätzliche Sicherheit und Transparenz erforderlich sind.

Das Whitepaper enthält einen Überblick über den aktuellen Stand der macOS Sicherheit sowie Anleitungen dazu, wie die sicherheitsrelevanten Apple Basiswerte auf effiziente, effektive und benutzerfreundliche Weise verbessert werden können.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 17 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/download

CLOUD MIGRATION

TREND NIMMT TROTZ SICHERHEITSBEDENKEN ZU

45 % der deutschen Unternehmen gaben an, dass sie die Gefahr von Datenlecks und Cyberangriffen infolge der Cloud-Migration als eine der größten Bedrohungen ansehen

39 % In Deutschland stieg der Anteil an Unternehmen, die geschäftskritische Anwendungen in die Cloud verlagern wollen von **17 auf 39 Prozent**

Im Jahr 2020-21 wurde es für Unternehmen noch notwendiger, wettbewerbsfähig zu bleiben und steigende Nutzeranforderungen zu erfüllen. Um diesen Anforderungen gerecht zu werden, planen immer mehr Unternehmen, ihre geschäftskritischen Anwendungen in die Cloud zu verlagern – trotz Bedenken hinsichtlich der Cybersicherheit.

www.equinix.de

73 % der IT-Entscheidungsträger räumen der Migration in die Cloud oberste Priorität ein

ÜBER DEN WOLKEN

CLOUD WORKLOAD SECURITY VERLANGT NACH EINER UMFASSENDEN PLATTFORM

Unternehmen verschieben in schneller Folge produktive Workloads in die Public Cloud. Gleichzeitig sollen mehr Nutzer und Systeme auf die Applikationen, Daten und Ressourcen, die zum Workload gehören, zugreifen. Damit vergrößern sich die Angriffsfläche und die Anzahl der potenziellen Schwachstellen. Cloud-Workload-Sicherheit (CWS) wird zu einer immer komplexeren Aufgabe und erfordert übergreifende Plattformansätze.

Im Gegensatz zu Private Clouds im eigenen Rechenzentrum bewegen sich Public-Cloud-Workloads ständig durch Umgebungen, die von verschiedenen Anbietern verwaltet und geschützt werden. Die Workloads abzusichern, verlangt nach einem völlig anderem Sicherheitskonzept als der Schutz von Prozessen im eigenen Netzwerk. Plattformlösungen bieten einen umfassenden Ansatz zum Schutz von Workloads, die über mehrere Cloudanbieter verteilt sind. Die IT-Sicherheitsverantwortlichen können die Gefahren aber über eine einzige übersichtliche Oberfläche erkennen und erforderliche Abwehrmaßnahmen schnell ergreifen.

Vorteile einer Plattform für Cloud Workload Security

Eine CWS-Plattform, wie Bitdefender GravityZone Security for Containers, verbessert den Schutz von Cloud-Workloads auf verschiedenen Ebenen: Zum einen konsolidiert sie für alle Workloads die Sicherheitswarnungen und das Management der Logs in einem Dashboard. So müssen nicht mehrere verschiedene Sicherheitstechnologien überwacht werden – und die Sichtbarkeit von Workloads in verschiedenen Cloud-Umgebungen wird deutlich verbessert.

Container-Schutz: Cloud-Workload-Sicherheit in der Praxis

Auch der Schutz von Containern ist ein zentrales Element der Cloud-Workload-Sicherheit. Laut den Daten der Bitdefender Labs sind die Angriffe auf Container und Linux-Server dementsprechend in 2021 deutlich gestiegen. 71 Prozent der Malware sind auf die Linux-Schadware Mirai zum Botnetz-Aufbau und auf den Meterpreter-Trojaner zurückzuführen. Diese Ergebnisse belegen, dass die Angreifer zu Multiplattform-Angriffen übergegangen sind und Malware, darunter auch Ransomware, speziell für Linux-Binärdateien entwickeln.

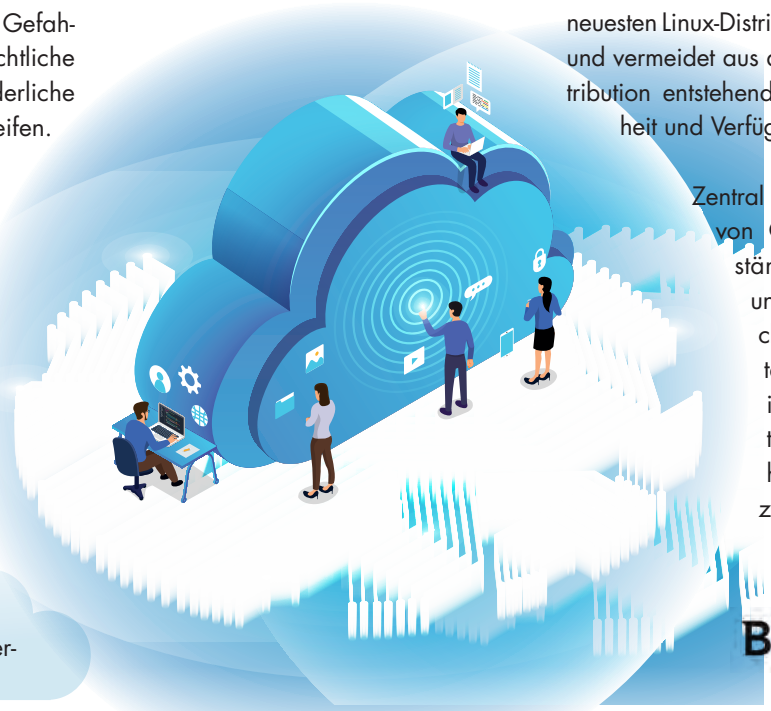
Wirksame Lösungen umfassen die Abwehr von Gefahren sowie Extended Endpoint Detection and Response (XEDR) und schützen Container in Private sowie Public Clouds gegen Exploits. Anwender haben über eine einheitliche Cybersecurity-Plattform Überblick und Kontrolle über die IT-Sicherheit.

Ebenso wichtig ist der Schutz der Container und Cloud-nativer Workloads vor Laufzeitangriffen, Linux-Kernel-, Application-Zero-Day- und bekannten Exploit-Angriffen in Echtzeit. Linux-native Technologien für Prävention und Erkennung identifizieren mögliche Gefahren früher und verkürzen die Verweildauer von Angreifern im Netz. Zugleich identifizieren sie den gesamten Kontext von Vorfällen, einschließlich der beteiligten Container-Images und -Pods.

Wirksamer Containerschutz bietet zudem Sicherheit über mehrere Linux-Distributionen hinweg. Die Probleme mit der Kompatibilität beseitigt ein einziger, kompakten Agent, der auf dem Linux-Kernel aufsitzt. Die Unabhängigkeit vom Linux-Kernel hilft Unternehmen, schnell auf die neuesten Linux-Distributionen umzusteigen und vermeidet aus dem Wechsel der Distribution entstehende Risiken bei Sicherheit und Verfügbarkeit.

Zentral ist auch beim Sichern von Containern die vollständige Transparenz und Kontrolle der Sicherheit über alle Container und Workloads in hybriden oder Multi-Cloud-Umgebungen hinweg mit einer einzigen Oberfläche.

www.bitdefender.de



Bitdefender

CLOUD ODER ON PREMISES?

ENTSCHEIDUNGSGRUNDLAGEN FÜR KMUS

BEI DER ENTSCHEIDUNG FÜR EIN EIGENES RECHENZENTRUM ODER EINE CLOUDLÖSUNG MÜSSEN VIELE FAKTOREN ABGEWOGEN WERDEN.

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

Cloudlösung oder eigenes Rechenzentrum? Um hier die richtige Wahl zu treffen und Fehlinvestitionen vorzubeugen, müssen kleine und mittlere Unternehmen sowohl in finanzieller Hinsicht als auch bei den Anwendungsszenarien genau vorausplanen. Nevis, Spezialist für Identity Access Management und passwortfreie Authentifizierung, gibt einen Überblick zu den wichtigsten Entscheidungskriterien.

Finanzierung und Folgekosten

Unternehmen mit kleineren IT-Teams von unter 50 Mitarbeitern und entsprechend geringen IT-Budgets können die Anfangsinvestitionen schwer stemmen. Neben Ausgaben für Hardware und Softwarelizenzen fallen diverse Projektkosten etwa für Integration und Installation an. SaaS-Lösungen (Software as a Service) sind üblicherweise weit weniger kostspielig, da sie mit relativ geringem Aufwand implementiert werden können; die Zeit bis zur Markteinführung wird so verkürzt und der Return on Investment verbessert.

Hinzu kommt: Da im SaaS-Modell die Instandhaltung durch den Anbieter erfolgt, werden eigene Mitarbeiter entlastet. Vor allem IT-Teams müssen sich fortan nicht um Software-Installationen, Lizenzen, Updates oder Wartungen kümmern. Stattdessen können Ihre Ressourcen auf Aufgaben ausrichten, die ebenso wichtig sind, aber direkt der Wertschöpfung im Unternehmen zugutekommen.

Technischen Vorsprung nutzen

Unternehmen, die ihren Endnutzern die beste User Experience bieten möchten, greifen in der Regel auf SaaS-Lösungen zurück, die von Public-Cloud-Anbietern bereitgestellt werden. Sie können somit modernste Hard- und Software nutzen, die ihre Vorteile überhaupt erst entfalten, weil sie speziell für die Cloud konzipiert wurden. Beispiele hierfür sind spezielle CPUs für künstliche Intelligenz oder verteilte Datenbanksysteme, für die es On Premises keine vergleichbar leistungsfähigen Entsprechungen gibt.

Sicherheit geht vor

Die Cloud-Architektur bietet allen Nutzern dieselben Sicherheitsstandards: Durch die dezentrale Speicherung aller Daten auf einem Cloud-Server führen lokale Hardware- und Software-Probleme seltener zu Datenverlusten. Kleinere Unternehmen genießen somit dieselben Sicherheitsstandards, die auch für größere Firmen gelten.

Das bedeutet aber auch: vertrauliche Firmendaten sind de facto nicht in Unternehmensbesitz, sondern werden auf Betreiberseite gespeichert. Unternehmen müssen daher bei der Auswahl des SaaS-Anbieters besonderes auf Datensicherheit und hohe Standards legen. Seriöse Anbieter garantieren beispielsweise, dass Daten ausschließlich auf Servern innerhalb der EU gespeichert werden und zu keinem Zeitpunkt außereuropäischen Datenzentren umgeleitet werden.

Entwicklungsphase beachten

Die niedrigen Einstiegkosten einer SaaS-Lösung und der schnelle ROI bieten sich gerade für junge Unternehmen an. Doch auch bei etablierten, größeren Firmen setzt mittlerweile ein Umdenken ein: Sie wechseln auf SaaS, da einerseits der Kostendruck auf IT-Abteilungen stetig zunimmt, und andererseits Updates im Cloudsystem erheblich schneller umgesetzt und integriert werden. Da die SaaS-Anbieter diese Arbeiten vollständig übernehmen, sinken auch hier Aufwand und Kosten auf Unternehmensseite.

Stephan Schweizer

NATIVE SECURITY

WIE SIE MEHR AUS OS-SECURITY HERAUSHOLEN

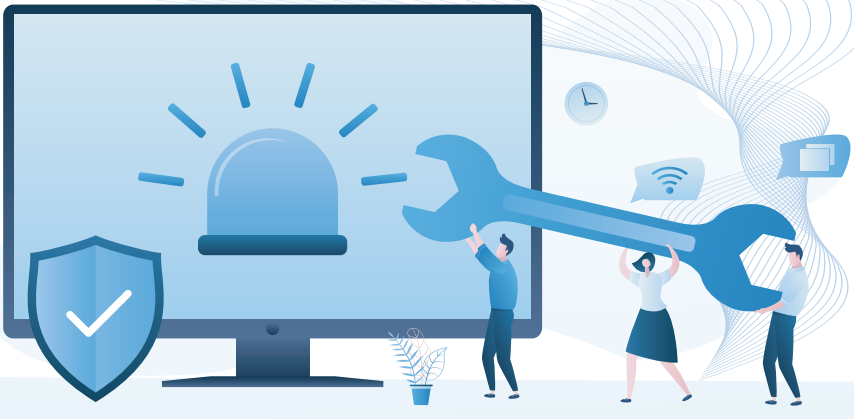
Wer sich mit der Absicherung von Arbeitsplätzen in Organisationen beschäftigt, dem sind viele dieser Lösungen ein Begriff: Microsoft BitLocker, Microsoft Defender, Local Firewall, Management von Benutzern und Gruppen. Analysten fassen diese Lösungen auch kurz unter dem Begriff „Native Security" zusammen, weil sie in das Betriebssystem integriert sind und Lizenznehmern der Betriebssysteme „nativ" zur Verfügung stehen.

In den letzten Jahren haben die Betriebssystemhersteller ihre nativen Sicherheitsfunktionen kontinuierlich verbessert. Die Sicherheitsfunktionen umfassen beispielsweise Funktionen zur Datensicherheit und -verschlüsselung, Authentifizierung, Antivirenschutz, Firewall Management und sicheren Konfiguration. Funktionen wie Antivirenschutz oder Festplattenverschlüsselung können mittlerweile mit Lösungen von Drittanbietern konkurrieren und diese ggf. ersetzen. Das reduziert das Portfolio der Tools, die IT-Sicherheitsverantwortliche managen müssen. IT-Administratoren setzen in der Regel verschiedene Sicherheitstechnologien zur Sicherung ihrer Endpunkte ein, um Angriffsflächen zu reduzieren. Eine Vielzahl an Lösungen geht oft mit operativer Komplexität einher.

Sicherheitsfunktionen zentral verwalten

Der Trend zum Einsatz von Native Security Lösungen ist nachvollziehbar, denn je weniger Einzellösungen genutzt werden, desto einfacher ist die Verwaltung. Laut einer Umfrage von Forrester Research aus dem Jahr 2020 planen 78 Prozent der befragten Entscheidungsträger die Nutzung nativer Sicherheitstools zu erhöhen, 50 Prozent möchten im Gegenzug den Einsatz von Third-Party-Tools begrenzen.

Warum sollten IT-Verantwortliche dennoch Speziallösungen von Drittanbietern in Erwägung ziehen? Der Anbieter DriveLock optimiert beispielsweise die Verwaltung nativer OS Sicherheitsfunktionen und ermöglicht das Einrichten zentraler Sicherheitsrichtlinien. So werden die Lösungen auch der Komplexität großer Unternehmen mit Tausenden von Arbeitsplätzen, Berechtigungen und Profilen gerecht. Dabei verwalten Administratoren die Sicherheitsfunktionen zentral in einer Management Konsole.



DriveLock optimiert nicht nur das Management nativer Security Lösungen, sondern ergänzt sie auch um wichtige Funktionen, wie zum Beispiel bei der Festplattenverschlüsselung mit Microsoft BitLocker: DriveLock ermöglicht eine zentrale, vom Active Directory (AD) unabhängige Konfiguration – auch für Computer ohne AD-Anbindung – und bietet optional eine Pre-Boot Authentication (PBA) an.

Präzisere Analysen

Native Sicherheitsfunktionen generieren zusätzlich nützliche Informationen für die Verhaltensanalyse. Damit können Drittanbieter wie DriveLock ihre Lösung mit Sicherheitsprotokolldaten aus dem Betriebssystem ergänzen. Dies ermöglicht präzisere Analysen und Vorhersagen und trägt signifikant zur Erhöhung der Sicherheit bei.

Die nativen Sicherheitsangebote erfüllen in der Welt der professionellen Cyberattacken wichtige Sicherheitsfunktionen. Mithilfe von Lösungen wie DriveLock können diese Funktionen zentral verwaltet und um wichtige Funktionalitäten ergänzt werden. Die von ihnen erhobenen Daten geben IT-Experten bei entsprechender Weiterverarbeitung mehr Transparenz: Intelligente Software zur Abwehr von Bedrohungen (sogenannte Threat-Intelligence-Lösungen) erweitern die nativen Schutzfunktionen um einen verhaltensbasierten Schutz und bieten somit mehr Sicherheit. Die DriveLock Zero Trust Platform verwaltet und ergänzt Native Security und schützt mit eigenen Modulen wie Device Control und EDR zusammen mit den erhobenen Daten aus den nativen Sicherheitskontrollen Ihre Umgebung vor Cyber-Attacken und weist auf potenziell laufende Angriffe hin.

www.drivelock.de

DriveLock

THREAT DETECTION

TRANSPARENZ UND ECHTZEITREAKTION AUF ANGRIFFE UND SCHWACHSTELLEN

Zeit ist der entscheidende Faktor. Mit den richtigen Tools zur Echtzeitüberwachung können Unternehmen Sicherheitsvorfälle sofort erkennen, um effektive Maßnahmen zu ergreifen. Diese bieten ein intelligentes Real-time-Monitoring für SAP – und kombiniert mit einem Security Dashboard sogar für ganze IT-Sicherheitslandschaften.

Noch 2018 haben nach Untersuchungen des SAP-Securityspezialisten SAST SOLUTIONS Unternehmen durchschnittlich 191 Tage gebraucht, um eine Attacke oder Datenlecks zu entdecken, und im Schnitt noch einmal 66 Tage, bis Bedrohungen neutralisiert wurden. Auch wenn sich inzwischen viele Unternehmen der seit Corona noch verschärften Sicherheitslage bewusst sind und zu handeln beginnen, sprechen allein die jüngsten Vorfälle Bände: Landtage und Landesministerien, das Innenministerium, Universitäten und Krankenhäuser, Städte wie Frankfurt am Main, ganz zu schweigen von Hackern wie REvil, die gerade tausende Unternehmen angriffen. Die Konsequenz: Eine verlässliche Threat Detection ist nun unternehmerisch obligatorisch, für Betreiber systemrelevanter Infrastrukturen (KRITIS) seit diesem Jahr auch gesetzlich vorgeschrieben.

Die Voraussetzungen

Eine seiner ersten und wichtigsten Empfehlungen sei daher stets, so Security-Experte Ralf Kempf, CTO von SAST SOLUTIONS: „Reagieren Sie bei Auffälligkeiten sofort und schieben Sie die Bereinigung nicht auf die lange Bank. Denn Zeit ist der kritische Faktor, sollte es wirklich einmal zu einem relevanten Angriff kommen. Dafür brauchen Sie eine funktionierende Threat Detection." Für eine performante Threat Detection ist die Kombination ganzheitlicher Echtzeitüberwachung mit einem SIEM ideal, benötigt aber einige Vorbereitung: zunächst die Identifikation bestehender Schwachstellen, die klare Zuordnung von Zuständigkeiten und die Vorbereitung und Dokumentation eines Risk Managements. Dann folgt der Schutz der Systeme durch eine umfassende Systemhärtung und ein Awareness-Training der Mitarbeiter. Bevor schließlich eine Threat Detection für das Erkennen von Anomalien und Angriffen und ein kontinuierliches Sicherheitsmanagement implementiert werden kann, ist zu entscheiden, ob man sich gerade im SAP-Bereich, aber auch systemweit der Unterstützung einer spezialisierten Sicherheitslösung samt eines Threat-Detection-Moduls bedient.

JEDES SYSTEM IST ANGREIFBAR. ALLERDINGS LÄSST SICH MIT EINER GUTEN STRATEGIE AUS BERATUNG UND SOFTWARE DIE WAHRSCHEINLICHKEIT EINES ERFOLGREICHEN ANGRIFFS SIGNIFIKANT REDUZIEREN.

Ralf Kempf, CTO SAST SOLUTIONS, akquinet AG, www.sast-solutions.de

Die Umsetzung

Als besondere Herausforderung für Unternehmen angesichts der allgemeinen Bedrohungslage erweist sich die SAP-Security, so Ralf Kempf: „Für SIEM-Tools liegt SAP im toten Winkel. Aufgrund fehlender spezieller SAP-Prüfregeln werden Angriffsmuster meist nicht identifiziert und die Unternehmen wissen nicht einmal, dass es Angriffe gab. In Tests konnten wir oft innerhalb einer Stunde in mehrere Systeme eindringen, ohne dass herkömmliche Monitoring-Tools dies erkannt hätten", führt er aus. „Das Security Radar, als Tool zur Threat Detection Teil unserer Software SAST SUITE, ist hier eine probate Lösung und trägt wesentlich dazu bei, hohen Schaden von Unternehmen abzuwenden." Die Erkennung von Angriffen in SAP-Landschaften durch das SAST Security Radar erfolgt auf Basis von Log-Dateien, deren Auswertung tiefe Kenntnisse über Angriffswege und -muster erfordert. Um sicherheitsrelevante Events herauszufiltern und in den richtigen Kontext zu stellen, ist ein intelligentes Management dieser Informationen notwendig: Das Security Radar bietet dafür eine offene Schnittstelle zur Corporate SIEM-Lösung und analysiert nicht nur SAP-Protokolle, sondern integriert auch Konfigurations- und Rollenanalysen. Es überwacht das System im Minutentakt, wertet Log-Quellen aus, erkennt Bedrohungen durch entsprechende Pattern, kann kritische Systemzustände sowie Konfigurations- und Berechtigungs-Schwachstellen umgehend an das übergreifende SIEM-Tool melden und mit anderen Events korrelieren. Unternehmen erhalten so einen aktuellen und ganzheitlichen Blick auf ihre IT-Sicherheit.

Keine Diskussionen, kein Warten auf den Videobeweis – mit performanter Threat Detection Bedrohungen sofort aus dem Spiel nehmen

Der Aufwand

Die optimale Reaktion auf eine Cyberattacke setzt ein sauber aufgesetztes Risikomanagement voraus, mit definierten Prozessen, um Risikoszenarien zu durchlaufen. „Wir stellen aber gerade beim Thema SAP fest, dass viele Unternehmen eine vollumfängliche Absicherung ihrer Systeme scheuen", so Ralf Kempf. „Denn dafür braucht man ein Projektbudget und dauerhaft personelle Ressourcen. Allerdings: Verglichen mit dem Schaden, den kriminelle Attacken verursachen, ist Aufwand wirklich kein rationales Argument mehr." Zumal, betont Kempf, es auch Varianten der Umsetzung gibt, die sich selbst für mittelständische Unternehmen ohne explizite Sicherheitsabteilung eignen. Für die Echtzeit-Prävention kann eine Managed-Service-Lösung genutzt werden. Hierbei müssen intern keine Ressourcen aufgebaut werden und viele der Services lassen sich pro Arbeitsplatz buchen. Gerade im SAP-Umfeld, wo es viele Patches und ständige Weiterentwicklungen gibt, kann ein Managed Service sofortige Sicherheit bieten. Vorteil ist zudem, dass die Security-Experten einen Erfahrungsschatz mitbringen, der selbst nicht aufzubauen ist. Mit umfangreichen Lösungen wie der SAST SUITE sorgen sie für eine ganzheitliche Absicherung mit Echtzeitüberwachung, die aktuellen Herausforderungen gerecht wird. „Aus unseren Sicherheitstests wissen wir, dass jedes System angreifbar ist", erklärt Kempf. „Allerdings lässt sich mit einer guten Strategie aus Beratung und Software die Wahrscheinlichkeit eines erfolgreichen Angriffs signifikant reduzieren, da sie ihn kompliziert und zeitaufwendig macht – und sollte es doch einmal brenzlig werden, erkennen unsere Kunden dies dank Threat Detection sofort und können unverzüglich handeln."

Das Ergebnis: Transparenz in Echtzeit

Die Antwort auf den Wunsch nach umfassend performanter Threat Detection liegt in der gründlichen Vorbereitung und klugen Kombination von SIEM mit spezialisierten Sicherheitslösungen wie der SAST SUITE. Bei der Erkennung und Minimierung von Bedrohungen ist Geschwindigkeit entscheidend: Threat Detection muss in der Lage sein, Bedrohungen schnell und effizient zu erkennen, damit Angreifern keine Zeit bleibt, Daten zu durchsuchen. Dazu die Empfehlung von Ralf Kempf: „Bindet man zusätzlich ein Security Dashboard ein, das in Echtzeit Schwachstellen über alle Ebenen und über Systemgrenzen hinweg auswerten, bündeln, standardisieren und zielgruppengerecht visualisieren kann, erhält man eine optimale Kombination." Das SAST Security Dashboard ermittelt auf Knopfdruck einen aktuellen Status anhand vordefinierter Risikokennzahlen, zeigt Ursachen für Sicherheitslücken, analysiert und veranschaulicht die historische Entwicklung und bietet jederzeit hochwertige Risiko-Informationen auf einen Blick. So erreicht man ein Maß an Transparenz, das ganzheitliche Echtzeit-Threat-Detection und damit eine qualifizierte und schnelle Reaktion auch auf unvorhergesehene Bedrohungen ermöglicht.

Das SAST Security Radar bietet eine offene Schnittstelle zur Corporate SIEM und prüft nicht nur SAP-Protokolle, sondern integriert auch Konfigurations- und Rollenanalysen

(RETRO)FIT FÜR DEN MASCHINENPARK 4.0

NUTZEN VON RETROFIT

„Industrie 4.0" ist ein Begriff, der in den vergangenen Jahren in fast keiner Debatte um die wirtschaftliche Zukunft der produzierenden Unternehmen in Deutschland fehlte. Die Hoffnungen, die sich damit verbinden, sind enorm, das Potenzial ist gewaltig.

Zumindest kommen zahlreiche Studien zu dem Schluss. In der Praxis – also in den Unternehmen selbst – wird das Thema dagegen etwas zurückhaltender betrachtet. Denn was nutzt die Vision einer Smart Factory, on der sich Cyber-physische Systeme autonom steuern, wenn es aktuell darum geht, die Performance der Maschinen und Anlagen zu steigern, um im immer härter werdenden Wettbewerb zu bestehen?

WHITEPAPER DOWNLOAD

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

AUFBAU EINER SMART FACTORY

SCHRITT FÜR SCHRITT ZUR VERNETZTEN PRODUKTION

eBook DOWNLOAD

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

Der Begriff Industrie 4.0 taucht nahezu täglich in den Medien auf und allzu oft können wir ihn nicht mehr hören! Er verspricht viel, dabei ist den meisten Unternehmen längst klar: Die digitale Vernetzung in der Produktion ist zeit- und kostenintensiv, sie birgt Risiken, erfordert Ressourcen und bedeutet, dass auch neue Kompetenzen geschaffen werden müssen.

Ist der Weg zur Smart Factory, der mit Industrie 4.0 beziehungsweise Industrial Internet of Things eng verbunden ist, wirklich so voller Hürden? Wir sagen „Nein" und möchten Ihnen mit diesem eBook einen Leitfaden an die Hand geben, wie Sie schneller ans Ziel kommen.

NEUE IVANTI-STUDIE

ÜBERMÜDETE IT-TEAMS UND SCHLECHT VORBEREITETE MITARBEITER VERLIEREN DEN KAMPF GEGEN PHISHING

Der Sicherheitsanbieter Ivanti hat die Ergebnisse einer aktuellen Umfrage zu Phishing-Angriffen vorgestellt. Die zentrale Aussage der Studie: Die globale Verlagerung der Arbeit an Remote-Standorte hat sowohl die Zahl der Angriffe, deren Raffinesse und die Auswirkungen von Phishing-Attacken deutlich nach oben getrieben. Fast drei Viertel (74%) der Befragten gaben an, dass ihr Unternehmen im letzten Jahr Opfer eines Phishing-Angriffs geworden ist, wobei alleine 40 Prozent im letzten Monat einen solchen Angriff erlebt haben. Für die Studie befragte Ivanti über 1.000 IT-Experten in Unternehmen in den USA, Deutschland, Großbritannien, Frankreich, Australien und Japan.

Das Volumen von Phishing-Versuchen, so die Untersuchung, hat im letzten Jahr deutlich zugelegt. Acht von zehn Befragten bestätigten, dass die Anzahl der Anläufe zugenommen hat. 85 Prozent stellten darüber hinaus fest, dass diese Versuche immer ausgefeilter werden. Interessant dabei ist die Erkenntnis, dass im letzten Jahr besonders die eigenen IT-Mitarbeiter im Fokus der Cyberkriminellen standen. Fast drei Viertel der Befragten (73%) gaben an, dass speziell IT-Mitarbeiter Ziel von Phishing-Versuchen waren. Noch gravierender: Beinahe die Hälfte dieser Versuche (47%) war erfolgreich.

Mobile Nutzer im Visier der Cyberkriminellen

Zu den neuesten, schnell an Boden gewinnenden Varianten gehören Smishing- und Vishing-Scams, die ganz gezielt mobile Benutzer ins Visier nehmen. Laut einer aktuellen Studie von Aberdeen haben Angriffe auf mobile Endgeräte sogar eine höhere Erfolgsquote als solche auf Server – ein Muster, das sich tendenziell dramatisch verschärft.

Im Everywhere Workplace nutzen Remote-Mitarbeiter mehr denn je mobile Geräte, um auf Unternehmensdaten zuzugreifen. Und Hacker fokussieren sich speziell auf Sicherheitslücken in diesem Umfeld. Das fehlende Gefahrenbewusstsein der

Mitarbeiter wird dabei von 34 Prozent der Befragten als eine der Hauptursachen für erfolgreiche Angriffe erkannt. Als Gegenmaßnahme bietet fast jedes Unternehmen (96%) Cybersecurity-Schulungen an, um die Belegschaft über gängige Angriffe wie Phishing und Ransomware zu informieren. Allerdings mit mäßigem Erfolg: Nicht einmal ein Drittel (30%) der Befragten bestätigten, dass ein Großteil der Mitarbeiter (>80%) diese Schulungen auch absolviert haben.

Phishing als Folge des Personalmangels

Die Ivanti-Studie ergab außerdem, dass der Mangel an IT-Fachkräften die Auswirkungen von Phishing-Angriffen weiter verstärkt. Mehr als die Hälfte der Befragten (52%) bestätigten einen Personalmangel ihres Unternehmens im vergangenen Jahr. Von diesen Befragten wiederum erkannten 64 Prozent fehlendes Personal als Ursache dafür, dass die Behebung von Vorfällen zu lange dauert. Mit weniger Mitarbeitern ist die Fähigkeit der IT-Teams stark eingeschränkt, Sicherheitsprobleme schnell zu beheben. Jede Ausfallzeit, die durch einen Sicherheitsvorfall verursacht wird, kostet eine Organisation Geld und schadet der Produktivität: Fast die Hälfte (46%) ist davon überzeugt, dass vermehrte Phishing-Angriffe eine direkte Folge des Personalmangels sind.

„Jeder, unabhängig von seiner Erfahrung oder seinem Wissen über Cybersicherheit, ist anfällig für einen Phishing-Angriff", erläutert Johannes Carl, Expert Manager PreSales – UEM bei Ivanti. „Um Phishing-Angriffe effektiv zu bekämpfen, müssen Unternehmen eine Zero-Trust-Sicherheitsstrategie implementieren. Nur sie umfasst eine einheitliche Endgeräteverwaltung mit geräteinterner Bedrohungserkennung und Anti-Phishing-Funktionen. Unternehmen sollten auch in Erwägung ziehen, sich von Passwörtern zu lösen. Indem sie die Authentifizierung auf mobilen Geräten mit biometrischem Zugang nutzen, beseitigen sie den primären Gefahrenpunkt bei Phishing-Angriffen."

www.ivanti.de

GEFAHR AUS DEM NETZ

IST IHR UNTERNEHMEN GEGEN CYBERATTACKEN ABGESICHERT?

Laut einer aktuellen Studie von Bitcom beläuft sich der gesamtwirtschaftliche Schaden durch Diebstahl, Erpressung und Sabotage auf die deutsche Wirtschaft auf mehr als 220 Milliarden Euro pro Jahr. Die Schadenssumme hat sich damit im Vergleich zu 2019 mehr als verdoppelt. Zudem waren neun von zehn Unternehmen 2020/2021 von Cyber-Attacken betroffen. Wie kommt es zu dieser hohen Zahl?

Mitarbeitende sind Passwort-müde

Mindestens 12 Zeichen inklusive Zahlen und Sonderzeichen müssen enthalten sein und alle drei Monate gibt es ein neues: Die Anforderungen an sichere Passwörter sind hoch. Da ist es kein Wunder, dass Mitarbeitende zu unsicheren Lösungen greifen. Die Folge sind notierte Passwörter auf Post-its am Bildschirm, „Passw0rt_5" oder gespeicherte Passwörter im Browser.

Unsichere Passwörter = hohes Risiko

Wenn Mitarbeitende unsichere Verwaltungslösungen für Passwörter nutzen, steigt das Risiko für Unternehmen erheblich an. Hacker können über unsichere Zugänge in Systeme eingreifen, wertvolle Informationen stehlen oder sogar Computer und Systeme blockieren, um durch Produktionsstillstand hohe Lösegelder zu erpressen. Die finanziellen Schäden sind in jedem Fall hoch.

Um sensible Zugänge wie das E-Mail-Postfach, das Banking-Portal oder den Messenger gegen Attacken zu schützen, bedarf es einer Passwort-Verwaltungslösung, die Passwörter sicher verwahrt, leicht zu bedienen ist und Mitarbeitende so von ihrer Passwort-Müdigkeit befreit.

Mit Password Safe mehr Sicherheit und Entlastung

Egal, ob auf einen Klick anmelden, Passwörter automatisch austauschen oder sichere Passwörter auf Knopfdruck mit dem Passwort-Generator erstellen: Password Safe von MATESO befreit Mitarbeitende von ihrer Passwort-Müdigkeit, da sie sich keine Passwörter mehr merken müssen! Alle Zugänge werden durch sichere, einzigartige und komplexe Passwörter abgesichert. Ebenso wird durch den Wegfall der manuellen Passwort-Verantwortung die IT von zahlreichen Passwort-Anfragen befreit.

Geteilter Account = geteiltes Wissen?

Häufig werden in Unternehmen Accounts von mehreren Mitarbeitenden genutzt. Die Passwörter zur Anmeldung werden dann im Klartext über E-Mails oder Chat-Programme geteilt. Handlungen wie diese erleichtern es Hackern, Passwörter auszuspähen und Daten abzugreifen. Mit dem Passwort Manager Password Safe können sich Mitarbeitende bei Accounts anmelden, ohne überhaupt das Passwort kennen zu müssen. Dank Sichtschutz kann das Passwort nicht aufgedeckt werden und bleibt somit sicher. Denn das sicherste Passwort ist das, das niemand kennt! Informationen in Password Safe liegen niemals unverschlüsselt vor, sondern werden immer Ende-zu-Ende-verschlüsselt übertragen.

Sicherheit auch bei Fluktuation

Der Administrator hat gekündigt und mit ihm verlassen Passwörter und sensible Informationen das Unternehmen? Nicht mit Password Safe. In Password Safe werden bestimmten Rollen bestimmte Passwörter zugeordnet. Somit hat jeder Mitarbeitender nur seiner Rolle entsprechend Zugriff auf für ihn wichtige Zugänge und Passwörter. Verlässt der Administrator das Unternehmen und somit seine Rolle, hat er automatisch keinen Zugriff mehr auf sensible Informationen und Accounts.

DIE ANFORDERUNGEN AN SICHERE PASSWÖRTER SIND HOCH. DA IST ES KEIN WUNDER, DASS MITARBEITENDE ZU UNSICHEREN LÖSUNGEN GREIFEN.

Sascha Martens, CTO, MATESO GmbH, www.passwordsafe.de

Mit Password Safe können zudem automatisch Berichte erstellt werden, mit denen beispielsweise nach einem Sicherheitsvorfall die Zugriffe auf Kennwörter nachvollzogen werden können. Das Logbuch gibt dabei Aufschluss darüber, welcher Nutzer Zugriff auf welche Passwörter hatte. So behält die IT auch bei Fluktuation stets die Datenkontrolle.

Leichte Bedienbarkeit für jeden Nutzer

Egal ob Ina aus der IT oder Klaus aus der Verwaltung – in Password Safe gibt es für jeden Benutzer die richtige Benutzeroberfläche. Für die meisten Mitarbeitenden sorgt die Light-Ansicht für einen vereinfachten Umgang mit Passwörtern. In der IT hingegen können individuelle Passwort-Richtlinien hinterlegt werden und Zugriffe nachvollziehbar gemacht werden.

Ob über den Browser, die Browser-Erweiterung oder über die gesicherte Password Safe App: Password Safe Nutzer können frei entscheiden, wie sie Passwörter und Zugangsdaten anlegen und darauf zugreifen möchten. Das erleichtert das sichere Arbeiten auch von zu Hause oder unterwegs. Alle Zugangsdaten und Passwörter sind dabei sicher verschlüsselt und stets auf dem aktuellen Stand.

Cyber Security made in Germany

MATESO bietet die IT-Security Software Password Safe in zwei Nutzungsvarianten an. Größere Unternehmen hosten die Lösung selbst. Durch Self-Hosting können Password Safe und alle damit verbundenen Daten auf eigenen Servern vor Ort oder in der Public oder Private Cloud gehostet werden. Für mehr Datenhoheit und -kontrolle: Alle in Password Safe gespeicherten Zugänge, Daten und Passwörter bleiben zu 100 Prozent im eigenen Unternehmen.

KMUs und Start-ups fehlt es häufig an eigenen Servern und IT-Kapazitäten. In diesem Fall bietet sich Password Safe als Managed Service an. Hierbei wird die Software von zertifizierten Partnern im Unternehmen zur Verfügung gestellt, gewartet und die Informationen werden in sicheren Rechenzentren in der DACH-Region gespeichert. So können auch kleine Unternehmen mit Password Safe ihre Zugänge absichern, ohne teure Hardware oder IT-Expertise zur Verfügung zu haben.

Sascha Martens

WHITEPAPER DOWNLOAD

„Die Wahl zwischen Self-Hosting & Outsourcing: Eine Entscheidungshilfe für Unternehmen“ steht zum kostenlosen Download bereit:

www.passwordsafe.de

IT'S (NOT) A KIND OF MAGIC

CYBER SECURITY IST EIN GESCHÄFTSKRITISCHER BUSINESS-PROZESS

Wer kennt sie nicht? Die wohlige Nervosität, wenn man gespannt darauf wartet, ob ein unmöglich erscheinender Zaubertrick gelingen mag. Es gibt nur Weniges, das uns mehr staunen lässt als ein Magier, der seine Tricks scheinbar mühelos beherrscht. Was dabei viele vergessen: Die Show wirkt nur deshalb so perfekt, weil neben dem Zauberer auch alle anderen Helfer optimal vorbereitet sind. Übertragen auf IT-Sicherheit bedeutet das: Damit Security-Lösungen ihre Magie entfalten, müssen Unternehmen zuvor eine Basis schaffen, auf der entsprechende Software wirkungsvoll aufsetzt.

Umdenken dringend erforderlich

Man stelle sich vor, die Arbeiter im Zirkus würden versuchen, ihr komplexes Zelt nicht gleichmäßig an allen, sondern an nur einem einzigen Haken hochzuziehen. Das kann nicht funktionieren. Doch so verhalten sich viele Unternehmen in Sachen IT-Sicherheit: Sie setzen auf einmalige Maßnahmen, schaffen kostspielige Security-Lösungen an und erwarten, dass so ein Höchstmaß an Cyber Security langfristig sichergestellt sei. Das ist mitnichten der Fall. Stattdessen ist IT-Sicherheit als Geschäftsprozess wie jeder andere zu verstehen, der mit Bedacht modelliert, mit Kennzahlen gesteuert, mit Tools überwacht und kontinuierlich optimiert sein will. Am Verständnis, dass Cyber Security das Ergebnis harter Grundlagenarbeit ist, mangelt es vielen Management-Teams. Die Folge: Unternehmen begegnen der Komplexität von Cyber Security nicht angemessen – und riskieren vermeidbare Angriffe, die sie teuer zu stehen kommen.

Aus diesem Grund muss ein Umdenken stattfinden: Damit eine Software ihre „magische" Wirkung entfaltet und bei der Abwehr von Bedrohungen zuverlässig unterstützt, sind Firmen gefordert, etliche Schritte zurückzugehen – ein mitunter steiniger Weg. Wie die Zirkusarbeiter müssen sie zuerst das Zelt aufbauen und sich einen vollständigen Überblick über ihre IT-Infrastruktur verschaffen: Welche Prozesse sind besonders relevant oder geschäftskritisch? Welche Systeme stützen sie? Welche und wie viele Prozesse sind digital abgebildet? Welche Betriebssysteme sind in welcher Abteilung im Einsatz? Welche Abteilungen sind für die Aufrechterhaltung des Geschäftsbetriebs unverzichtbar? Welche Mitarbeiter verantworten welche Prozesse?

Systematische Unterstützung

Natürlich ist die Beschäftigung mit derartigen Fragen äußerst komplex und umfangreich und daher für hauseigene Security-Experten, die ihren Fokus – ähnlich wie Hacker – auf die schlimmsten Schwachstellen legen müssen, kaum zu bewältigen. Daher ist es sinnvoll, einen spezialisierten Dienstleister ins Boot zu holen, der Unternehmen systematisch unterstützt. Mit seiner Hilfe lernen Firmen ihr eigenes Inventar kennen und schaffen damit die Grundlage, um die nächsten prozessualen Schritte zu gehen: Festlegen, welche Systeme gegen Angriffe zu schützen sind; definieren, wie die Ziele zu erreichen sind; und bestimmen, wie die anstehenden Aufgaben zu priorisieren sind.

Wer seine Hausaufgaben macht, hat überzeugende Argumente an der Hand, um selbst den kritischsten Zirkusdirektor zu überzeugen und ihm den Mehrwert von Cyber Security als Business-Prozess zu vermitteln. Magie um der Magie willen funktioniert ebenso wenig wie der Versuch, Sicherheit von der Stange einzukaufen. Dedizierte Security-Lösungen haben nur dann eine magische Wirkung, wenn sie auf einem starken Fundament aufbauen. Darum heißt es: Ärmel hochkrempeln, Zirkuszelt schrittweise aufbauen und dem Zauberer eine optimale Bühne bereiten. Nur dann können Unternehmen von ihrer Security-Lösung behaupten: It´s a kind of magic!

Andreas Nolte

WER SEINE HAUSAUFGABEN MACHT, HAT ÜBERZEUGENDE ARGUMENTE AN DER HAND, UM DEN MEHRWERT VON CYBER SECURITY ALS BUSINESS-PROZESS ZU VERMITTELN.

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

ÜBERGREIFENDE RISIKOANALYSE

EINE GEMEINSAME DATENBASIS IST NICHT GENUG

Es sollte selbstverständlich sein, eine gemeinsame Datenbasis für Grundschutz und BCM zu nutzen. Denn es sind dieselben Stammdaten, die für beide Managementsysteme erhoben werden und es ist dieselbe Infrastruktur, die bei der Strukturanalyse auf Zusammenhänge untersucht wird. Wer noch mit verschiedenen Softwaretools arbeitet, kann zumindest Datenimporte vornehmen oder Schnittstellen einrichten, um Doppelarbeit zu vermeiden und Kosten zu sparen. Bei einem integrierten Managementsystem mit gemeinsamer Datenbasis wie der HiScout GRC Suite muss man sich nicht einmal darum kümmern.

Doch hören die Gemeinsamkeiten zwischen Grundschutz und BCM hier noch nicht auf. Auch bei der Risikoanalyse können Grundschutz und BCM voneinander profitieren. Der BSI-Standard 200-4 gibt zwar nicht die Methode der Risikoanalyse vor, unterstützt und empfiehlt aber ausdrücklich die Nutzung der Risikoanalyse nach BSI-Standard 200-3. Denn im Grundschutz wurden die Risiken für Anwendungen, Systeme, Netze und Standorte bereits sorgfältig bewertet. Der Detaillierungsgrad dieser Risikoanalysen ist eine hervorragende Ausgangsbasis für die weitere Bearbeitung im BCM. Warum sollte man wieder von vorne anfangen?

Zeit- und Kostenersparnis

Der BCM-Verantwortliche kann auf der im Grundschutz erledigten Arbeit aufsetzen und diese fortführen, sobald er über die Business Impact Analyse die zeitkritischen Anwendungen ermittelt hat. Anwendungen, die im Grundschutz als besonders schutzbedürftig eingestuft wurden, sind dort bereits zusätzliche Maßnahmen zugeordnet worden. Diese kann der BCM-Verantwortliche nun einsehen und bei Bedarf für seine Geschäftsfortführungsplanung ergänzen. Umgekehrt kann der Grundschutz-Verantwortliche die vom BCM-Verantwortlichen vorgesehene Absicherung zeitkritischer Anwendungen bei seiner eigenen Maßnahmenplanung berücksichtigen. Wird die Bearbeitung zwischen beiden zeitlich synchronisiert, kann das gemeinsame Maßnahmenpaket gebündelt zur Umsetzung an die Zielobjekt-Verantwortlichen weitergegeben werden. Diese und ihre Mitarbeiter freuen sich über die Zeit- und Kostenersparnis, weil die betroffenen Systemkomponenten nicht zweimal bearbeitet werden müssen.

Gemeinsam arbeiten

In der verwendeten Software sollten Gefährdungen und Maßnahmen idealerweise aus beiden Richtungen zu pflegen sein und direkt am Asset übersichtlich zusammengefasst werden. Die Umsetzungsverantwortlichen der IT können sich dann selbständig einen kompletten Überblick über alle Anforderungen verschaffen und müssen nicht mehr einzeln von den Grundschutz- und BCM-Managern kontaktiert werden. Wo üblicherweise verschiedene Businessbereiche und IT-Abteilungen miteinander ringen, arbeiten nun alle Beteiligten an einem gemeinsamen Ziel. Reibungsverluste zwischen Abteilungen und Personen werden reduziert.

Fazit

Stammdaten und Strukturanalyse können gemeinsam für Grundschutz und BCM genutzt werden. Entsprechende Softwarelösungen sind schon lange am Markt etabliert. Auch bei der Risikoanalyse können die Arbeitsergebnisse von Grundschutz- und BCM-Verantwortlichen in einem Tool zusammenfließen und bis hin zur Umsetzung durch die IT übergreifend koordiniert werden. Das trägt nicht nur zur Zeitersparnis und Kostensenkung, sondern auch zur Verbesserung der Zusammenarbeit zwischen allen Beteiligten bei. HiScout arbeitet an einer übergreifenden Risikoanalyse für Grundschutz, Datenschutz und BCM.

Steffen Voigt | www.hiscout.com

IT-SA
Besuchen Sie uns in Halle 7A,
Stand 7A-627

Bildquelle: ©Elnur – stock.adobe.com

VERTEIDIGUNG GEGEN CYBERANGRIFFE

IM INTEGRIERTEN SECURITY-ECOSYSTEM

Cyberangriffe, etwa Ransomware, sind heute an der Tagesordnung. Und dabei sind es weit mehr als die prominenten Beispiele der Ransomware-Angriffe auf Großunternehmen, Krankenhäuser oder Universitäten, die man aus den Nachrichten kennt.

Schon vor Jahren, zu Zeiten der Locky-Ransomware, waren die Angriffe breit gestreut. Gegen eine Zahlung von relativ geringen Lösegeldsummen von 300 bis 500 Euro bekamen Opfer den Entschlüsselungscode, um Zugriff auf die verschlüsselten Daten zu bekommen. Allerdings sind diese vergleichsweise moderaten Zeiten vorbei.

In der Studie „The State of Ransomware 2021" hat Sophos festgestellt, wie bedrohlich die Lage heute ist: Besonders auffallend ist die Entwicklung der Durchschnittskosten für die Wiederherstellung nach einem Ransomware-Angriff. Diese haben sich in nur einem Jahr mehr als verdoppelt, konkret von rund 630.000 Euro im Jahr 2020 (Deutschland 390.000 Euro) zu 1,53 Millionen Euro in 2021 (Deutschland 970.000 Euro). Auch die durchschnittliche Lösegeldzahlung ist auf ein extremes Niveau gestiegen. Diese beträgt weltweit 140.000 Euro, in Deutschland 115.000 Euro.

Gezielte Angriffe nehmen zu

Speziell für den Bereich des Mittelstands hat die Studie zu Ransomware-Attacken ergeben, dass über die Hälfte der in Deutschland befragten mittelständischen Unternehmen in den letzten zwölf Monaten Opfer von Ransomware waren. Durchschnittlicher Schaden durch den Ausfall oder die Einschränkung des Geschäftsbetriebs: 400.000 Euro. Und Cyberangriffe betreffen Unternehmen und Organisationen aller Branchen und Größen.

Die Sophos-Studie zeigt auch, dass nur acht Prozent der betroffenen Organisationen im Falle einer Zahlung alle Daten wiederbekommen haben. Knapp ein Drittel (29 Prozent) weltweit bekam nicht mehr als die Hälfte der verschlüsselten Daten zurück, was zu schwerwiegenden Folgen für das Business führen kann.

Zwar sank die Zahl der Ransomware-Attacken-Opfer von 51 Prozent (Deutschland 57 Prozent) im Jahr 2020 auf 37 Prozent (Deutschland 46 Prozent) in 2021. Dadurch sank auch die weltweite Anzahl der Unternehmen, die eine Datenverschlüsselung verzeichneten von 54 Prozent in 2021 gegenüber 73 Prozent in 2020. Dieser vermeintliche Rückgang klingt erst einmal nach einer guten Nachricht, wird aber durch die Tatsache beeinträchtigt, dass diese Zahl zumindest teilweise Änderungen im Verhalten der Angreifer widerspiegelt. Denn die Forschungsergebnisse zeigen, dass Angreifer neben groß angelegten, generischen und automatisierten Angriffen zudem zu gezielteren Angriffen übergehen, die auch menschliches Hacking via Tastatur einbeziehen. Das Schadenspotenzial dieser zielgerichteten Angriffe ist weitaus höher.

DAS SOPHOS ADAPTIVE CYBERSECURITY ECOSYSTEM BIETET SYNCHRONISIERTE SICHERHEIT, SECURITY-AUTOMATISIERUNG UND MENSCHLICHES SPEZIALISTEN-WISSEN FÜR EINE KONTINUIERLICHE OPTIMIERUNG DES SCHUTZES GEGEN CYBER-ANGRIFFE.

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

Adaptive Cybersecurity Ecosystem

Es stellt sich die Frage, was Organisationen und Unternehmen tun können (und müssen), um nicht das nächste Opfer zu werden. Außer Frage steht, dass die traditionellen Schutzmaßnahmen wie Firewall und Anti-Virus allein heute keinen ausreichenden Schutz mehr gegen professionelle Angreifer bieten.

Bewährt haben sich sogenannte Endpoint Detection & Response-, abgekürzt EDR-Lösungen. Dies bestätigt auch der Bundesverband IT-Sicherheit e.V. (TeleTrusT) als „Stand der Technik" im Jahr 2020. EDR ist ein ganzheitlicher Ansatz am Endpoint und Server, der neben modernen Schutztechnologien wie Exploit- und Ransomware-Schutz auch die unternehmensweite Erkennung von Hackeraktivität und die Eindämmung von Bedrohungen beinhaltet. Mit EDR können bereits Vorstufen von Angriffen und Ha-

ckeraktivitäten in der Phase erkannt werden, in der sich ein Angreifer im Netzwerk umsieht und ausbreitet. Um EDR jedoch effektiv zu bedienen, wird spezialisiertes Personal benötigt - und zwar rund um die Uhr, am Wochenende wie an Feiertagen. Sophos ergänzt EDR zusätzlich mit XDR (Extended Detection & Response), das die menschliche Kompetenz einbezieht. Damit geht der Schutz über die Endpoint- und Server-Ebene hinaus und ermöglicht der Firewall, der E-Mail-Security und anderen Datenquellen, wichtige Daten an einen Data Lake zu senden. Die Kombination nennt Sophos das Adaptive Cybersecurity Ecosystem. Es nutzt gleichzeitig die Automatisierung und die Kompetenz menschlicher Spezialisten, um Angreifern einen Schritt voraus zu sein. Es lernt und verbessert sich ständig und schafft so einen positiven Kreislauf der Cybersicherheit.

Cybersecurity-Ökosystem

Das Adaptive Cybersecurity Ecosystem basiert auf den gesammelten Bedrohungsdaten der SophosLabs, Sophos Security Operations (menschliche Analysten, die über das Sophos Managed Threat Response-Programm in Tausenden von Kundenumgebungen eingebunden sind) und der Künstlichen Intelligenz (KI) von Sophos. Ein einziger, integrierter Data Lake fasst Informationen aus allen Lösungen und Threat Intelligence-Quellen zusammen. Echtzeit-Analysen ermöglichen es Verteidigern, Einbrüche zu verhindern, indem sie verdächtige Signale finden. Parallel dazu ermöglichen offene APIs Kunden, Partnern und Entwickler, Tools und Lösungen zu entwickeln, die mit dem System interagieren. Alles wird zentral verwaltet über die Sophos Central Management-Plattform.

Fünf Kernelemente – bestehend aus Threat Intelligence, Next-Gen-Technologien, Data Lake, APIs und zentraler Verwaltung – arbeiten zusammen, um ein anpassungsfähiges Cybersecurity-Ökosystem zu schaffen, das ständig dazulernt und sich verbessert.

Das Sophos Adaptive Cybersecurity Ecosystem kann von Sicherheitsexperten von jedem beliebigen Standort aus verwaltet werden und gibt Unternehmen die Möglichkeit, die besten Sicherheitsexperten weltweit zu finden. Alternativ können auch die Experten von Sophos die Erkennung von und Reaktion auf Bedrohungen als Service übernehmen.

Das Adaptive Cybersecurity Ecosystem wurde entwickelt, um der neuen Realität, der von Menschen verursachten und kontrollierten Attacken zu begegnen und gleichzeitig die vernetzte, digitale Welt von heute zu unterstützen. Das Ökosystem ist sehr umfassend und leistungsfähig und es kann aus vielen einzelnen Elementen individuell gewählt werden. Viele Kunden beginnen mit dem Sophos Endpoint-Schutz oder einer Firewall und erweitern ihr System entsprechend ihren Anforderungen.

Offen für alle

In einer vernetzten Welt ist es von entscheidender Bedeutung, dass Cybersecurity in das gesamte Geschäftsumfeld integriert werden kann. Sophos ACE ist eine offene Plattform mit leistungsstarken Integrationen und zahlreichen Programmierschnittstellen (APIs).

Sophos ACE unterstützt ein breites Spektrum an Sicherheitsanforderungen, darunter Managed Security Service Provider (MSSPs), Channel-Partner, Internet Service Provider (ISPs) sowie kleine und mittelständische Unternehmen. Das Sophos Cybersecurity Ecosystem ist sehr flexibel und der Einstieg ist so einfach wie der Einsatz eines der Sophos Security-Lösungen oder -dienste. Unternehmen profitieren umgehend von der kombinierten Threat Intelligence-Expertise von Sophos AI, SophosLabs und Sophos Security Operations. Und sie können das Ecosystem jederzeit und entsprechend der sich verändernden Anforderungen im Unternehmen erweitern.

Michael Veit

CYBER-RESILIENZ

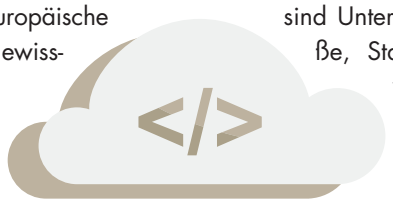
DER QBE UNPREDICTABILITY INDEX – UNVORHERSEHBARE EREIGNISSE SIND NICHT ZWINGEND NEGATIV

Im Oktober 2019 veröffentlichte das australische Versicherungsunternehmen QBE erstmalig den Unpredictability Index. Seine Leitfrage: Ist die Welt heute unvorhersehbarer geworden?

Für die Studie identifizierte QBE fünf Schlüsselbereiche der Unvorhersehbarkeit, in deren Rahmen die Unbeständigkeit der letzten drei Jahrzehnte beleuchtet wurde. Diese umfassen den wirtschaftlichen, unternehmerischen, gesellschaftlichen und politischen Wandel sowie Veränderungen in der Natur. Der technologische Wandel gilt als Charakteristikum jeder der fünf Komponenten. Für die Datenerhebung wurden mithilfe einer Online-Umfrage 1.314 internationale Entscheidungsträger befragt.

Unsicherheit in 30 Jahren

Der Ansatz der Studie: Für die Einschätzung der Unsicherheit betrachteten die Autoren eine Zeitleiste von 1987 bis 2019. QBE folgert, dass die Relation vorrangig Ereignisse der fünf Bereiche Wirtschaft, Unternehmen, Gesellschaft, Politik und Natur betrifft. Exemplarisch waren die unvorhersehbarsten Jahre, 2010 und 2015, besonders von wirtschaftlichen und politischen Entwicklungen geprägt. Das Jahr 2010 war deshalb unvorhersehbar, weil sich die Wirtschaft noch von der Großen Rezession, die 2007 begann, erholte. 2015 sorgte die europäische Flüchtlingskrise für Ungewissheit.

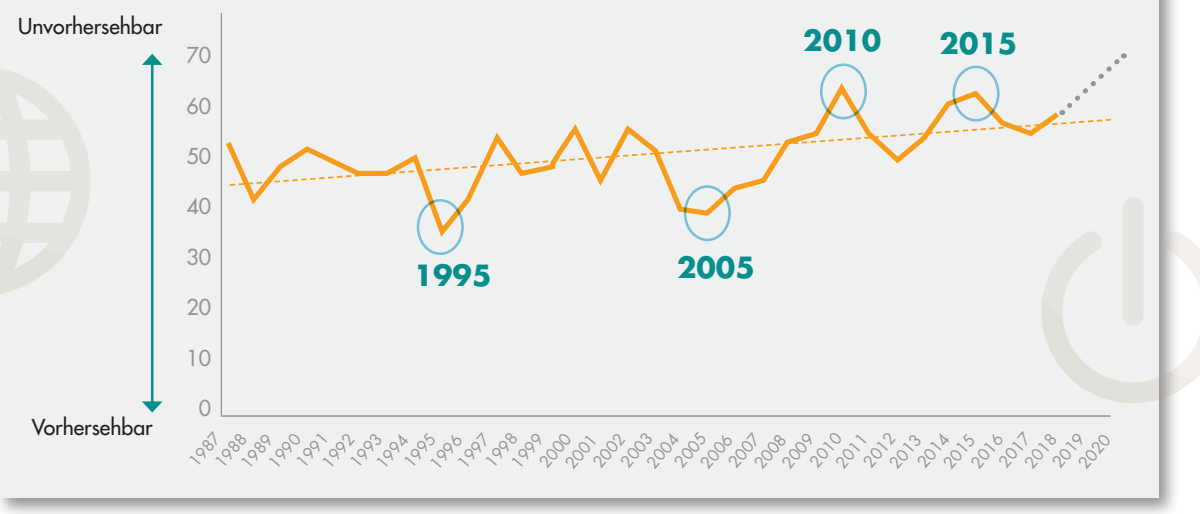


Das Platzen der Dotcom-Blase, die Terroranschläge am 11. September, Unsicherheit am Arbeitsmarkt, Brexit und politische Wahlen – vor allem in den USA – sind weitere Beispiele, welche die Vorhersehbarkeit erschwerten. Erstaunlicherweise charakterisierte QBE schon vor den ersten Nachrichten über Covid-19 das Jahr 2020 als eines der unvorhersehbarsten. Diesen Schluss zogen sie aus der Feststellung eines 5-Jahres-Zyklus der Unvorhersehbarkeit, welcher mit den Jahren 2010 und 2015 begann.

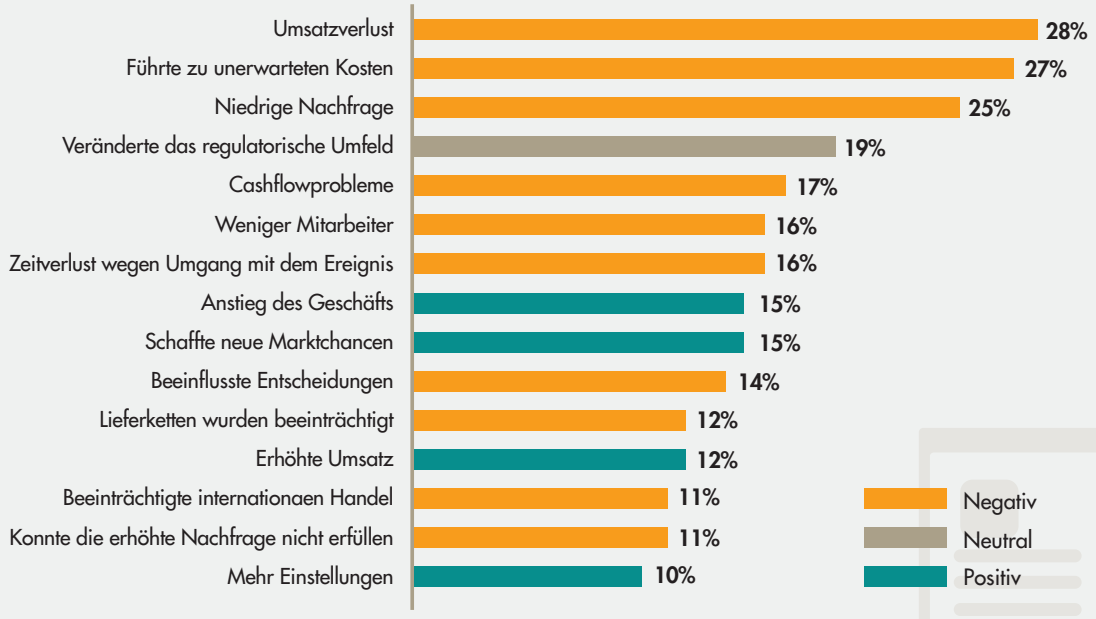
Branchenabhängigkeit bei Cyber-Risiken

Auswirkungen von unvorhersehbaren Ereignissen betreffen meistens den Umsatz, die Kosten oder die Nachfrage. Dabei sind Unternehmen je nach Größe, Standort oder Branche verschieden anfällig. Aus der Studie geht hervor, dass in den letzten zehn Jahren vier von fünf Unternehmen durch Unvorhersehbarkeit beeinträchtigt wurden. Von den kleinen Unternehmen gaben aber 47 Prozent der Einzelunternehmen und 34 Prozent der Mikrounternehmen an, dass sie durch keine der fünf Bereiche der Unvorhersehbarkeit behindert wurden.

DER ‚UNPREDICTABILITY INDEX'



AUSWIRKUNGEN AUF UNVORHERSEHBARE EREIGNISSE



QBE erklärt dies damit, dass solche Unternehmen meist erst vor Kurzem gegründet wurden und somit weniger disruptive Ereignisse miterlebt haben. Dagegen berichten neun von zehn großen Unternehmen, dass mindestens einer der Bereiche betroffen war. Während Produktionsunternehmen und Einzelhändler anfällig für Störungen des Handels und der Lieferketten sind, sind Dienstleistungsträger hauptsächlich durch Regulierungen und Gefahren für die Cybersicherheit beeinträchtigt.

IN UNPLANBAREN ZEITEN IST CYBER-RESILIENZ DER ENTSCHEIDENDE WETTBEWERBSVORTEIL.

Jan Sudmeyer, Managing Partner, carmasec GmbH & Co.KG, www.carmasec.com

„Unvorhersehbare Ereignisse sind ihrer bloßen Natur nach nicht unbedingt negativ", so Andrea Brock, Geschäftsführerin von QBE, „oft geht es um die Art und Weise, wie Unternehmen vorbereitet sind". Eines von sieben Unternehmen konnte sein Geschäft und seinen Umsatz auf Grund unvorhergesehener Ereignisse sogar steigern. Dabei gaben IT- und Computerfirmen die höchste Wahrscheinlichkeit an, trotz Unvorhersehbarkeit Chancen am Markt schaffen zu können.

Empfehlung Risikomanagement

Aus der Beobachtung der bisherigen 30 Jahre vermutet das Research-Team von QBE, dass sich die Zeiten der Stabilität verkürzen und sich die instabilen Phasen verlängern werden. Da so noch kein Ende der Unvorhersehbarkeit zu erkennen ist, empfiehlt QBE, auf ein Risikomanagement zu setzen. Zum Zeitpunkt der Befragung erklärten sich drei von vier Unternehmen in der Handhabung von unvorhergesehenen Ereignissen als vorbereitet. Jedoch hatten nur 29 Prozent einen formalen Risikomanagementplan. „Obwohl ich froh bin zu sehen, dass die Unternehmen insgesamt optimistisch sind", erläutert Brock, „so mache ich mir dennoch Sorgen, dass viele auf den Ansatz ‚Es wird schon alles gut gehen' setzen". Die Corona-Krise bestätigt die Hypothese, dass Unternehmen mit einer sehr guten Vorbereitung in unvorhergesehenen Situationen am besten überleben. Das Ganze gilt natürlich auch für die IT und hier besonders das Feld der IT-Sicherheit.

Jan Sudmeyer

Mehr zum Unvorhersehbarkeitsindex:

it-daily.net

MODERNE SICHERHEITSINFRASTRUKTUR

CYBERATTACKEN IN DER WIRTSCHAFT BEKÄMPFEN

Seit dem globalen Ausbruch der Corona-Pandemie feiern Cyberkriminelle auf der ganzen Welt Hochkonjunktur. Berichten zufolge ist die Anzahl der Angriffe allein in Deutschland um 150 Prozent gestiegen. In anderen Ländern wie den USA ist die Lage sogar noch um einiges schlimmer. Tatsache ist jedoch auch, dass die digitale Transformation dort bereits seit vielen Jahren kontinuierlich vorangetrieben wird, während Deutschland im Vergleich deutlich hinterherhinkt.

Bundeskanzlerin Angela Merkel nahm diese negative Entwicklung zum Anlass, um auf dem Digitalgipfel 2021 eine Transformation der föderalen und staatlichen Infrastrukturen in Deutschland zu fordern, um das eigentlich solide Fundament in Punkto Digitalisierung nicht zum Wanken zu bringen. Das sollte auch Unternehmen aufhorchen lassen, denn nicht nur die weiterhin steigenden Zahlen der Cyberattacken sind auffallend. Auch deren Ausmaß hat extrem an Breitenwirkung zugenommen, wie die Fälle von Unternehmen wie SolarWinds, Microsoft Exchange und zuletzt Colonial Pipeline beweisen. Sie haben der Wirtschaft einmal mehr vor Augen geführt, wie fragil digitale Strukturen sein können und wie wichtig es ist, dass alle Systeme und Prozesse wie ein Uhrwerk harmonisch ineinandergreifen. Nur so lassen sich etwaige Sicherheitslücken bereits im Vorfeld ausschließen – vor allem, wenn es darum geht, mit Kunden und Stakeholdern in Kontakt zu treten.

Dringender Wandel erforderlich

Fakt ist: Technischer Fortschritt kann nur dann stattfinden, wenn auch ein kultureller Wandel vollzogen wird. Das bedeutet, nur weil das Fax-Gerät lange Zeit als nützliches Kommunikationsmittel galt, dies auch heute oder morgen noch der Fall sein muss. Um sich die notwendige Flexibilität zu bewahren, müssen Unternehmen stets auf dem Laufenden bleiben. Das wird auch durch den Fall des bereits genannten, US-amerikanischen Unternehmens SolarWinds untermauert, der

als der bis dato größte und raffinierteste Cyberangriff aller Zeiten Schlagzeilen machte. Er kompromittierte nicht nur den privaten Sektor, sondern betraf auch viele Organisationen der US-Regierung, darunter wichtige Bundesbehörden wie das Finanz-, Justiz- und Handelsministerium. Anfang des Jahres wurde dieser jedoch sogar übertroffen: Im Rahmen einer Attacke auf Microsoft Exchange wurden E-Mail-Adressen von über 30.000 staatlichen als auch kommerziellen US-Organisationen offengelegt. Obwohl über das tatsächliche Ausmaß des Schadens noch nichts bekannt ist, bezeichnen Experten ihn bereits jetzt als noch deutlich gravierender.

Jede dieser Cyberattacken ist für sich genommen schon verhängnisvoll genug. Wirklich alarmierend für Unternehmen ist jedoch, dass die Häufigkeit solch tiefgreifender Attacken konstant steigt. Bei näherer Betrachtung zeigt sich, dass es einige gravierende Fallstricke gibt, deren vermeidbarer Risiken sich Unternehmen mehr oder weniger freiwillig aussetzen und diese Art von Angriffen wahrscheinlicher und damit auch gefährlicher machen.

Die drei Säulen einer modernen Infrastruktur

Die Bandbreite der einzelnen ist völlig unterschiedlich und erstreckt sich von der Lieferkette über die Datenspeicherung bis hin zur Ransomware. Dennoch weisen sie alle auf einige konkrete Schwachpunkte hin, die aus sicherheitstechnischer Perspektive maßgebend sind. Alle Unternehmen weltweit, nicht nur die amerikanischen, sollten aus diesem Grund eine neue, auf Sicherheit ausgerichtete Infrastruktur aufbauen, um zukünftige Angriffe abzuschrecken und die möglichen Konsequenzen eines erfolgreichen Einbruchs zu minimieren. Dieses neue System fußt auf drei Säulen:

1. Zero Trust als Grundgerüst

Dieses Sicherheits-Fundament gibt es schon seit einiger Zeit, aber es gewinnt bei der Implementierung erst jetzt an Bedeutung. Ein Grund dafür ist die ausdrückliche Nennung in der neuen Executive Order der US-Regierung, mit der Präsident Joe Biden einen höheren Cybersecurity-Standard der Vereinigten Staaten anstrebt.

Zero Trust ist eine Methodik, die davon ausgeht, dass alle Daten, Geräte, Apps und Benutzer innerhalb oder außerhalb des Unternehmensnetzwerks von Natur aus unsicher sind und vor jedem Zugriff authentifiziert und verifiziert werden müssen. Entscheidend ist, dass es sich um eine ganzheitliche Strategie handelt. Sie umfasst sowohl technische Protokolle wie Multi-Faktor-Authentifizierung und Identitätszugriffsmanagement als auch eine übergreifende dynamische und äußerst wachsame Denkweise, die in die Arbeitsprozesse einer Organisation integriert ist und proaktiv gegen Cyber-Bedrohungen schützt. Dieser Ansatz erfordert einen Strategiewechsel auf allen Ebenen, da er davon ausgeht, dass jede Schwachstelle, selbst auf der Ebene des einzelnen Mitarbeiters, erheblichen Schaden anrichten kann.

2. Ende-zu-Ende-Verschlüsselung (E2EE)

Da Cyberangriffe sich derzeit häufen, nimmt auch die Bedeutung der Ende-zu-Ende-Verschlüsselung stetig zu. Viele Plattformen weisen Sicherheitslücken auf, weshalb Unternehmen zunehmend E2EE als grundlegendes Sicherheitsmerkmal fordern. Einige beliebte Kollaborations- und E-Mail-Plattformen haben jedoch weder konkrete Pläne für den Einsatz von E2EE erstellt oder bemühen sich erst jetzt um die Integration grundlegender Sicherheitsprotokolle, nachdem sie jahrelang ohne diese gearbeitet haben. Die Definition der „Ende-zu-Ende-Verschlüsselung" ist zudem durch die inflationäre Verwendung des Begriffs im Marketing abgenutzt worden: Bei einer echten Ende-zu-Ende-Verschlüsselung werden die Daten auf dem System oder Gerät des Absenders verschlüsselt und nur der Empfänger kann sie entschlüsseln. Es wurden sogar schon einige Plattformen ertappt, die falsche Angaben gemacht haben oder nur eine schwache Form von E2EE einsetzen. Daher ist es entscheidend, nicht nur die richtige E2EE-

Form zu wählen, sondern diese auch völlig transparent zu kommunizieren.

Eine dezentrale Lösung auf Basis von Double-Ratchet-E2EE ermöglicht beispielsweise, dass jeder einzelne Anruf, jede Nachricht und jede Datei auf jedem Gerät separat verschlüsselt wird, wobei die Schlüssel vom Gerät selbst und nicht von einem zentralen Server generiert werden. Dies hat den Vorteil, dass die Informationen bis zur kleinstmöglichen Einheit geschützt werden, und es entsteht ein System, das mit jeder Nachricht für Hacker komplexer wird und Angriffe daher weniger wirtschaftlich macht.

3. Datenspeicherung dezentralisieren

Anstatt Datenbestände in einem unsicheren, zentralen Speicher abzulegen, schützt die Dezentralisierung sie direkt vor Ort. Damit haben Unternehmen die Kontrolle über ihre Daten selbst in der Hand und sind nicht mehr den Risiken ausgesetzt, die sich aus der Entscheidung eines Anbieters über die Speicherung seiner Daten ergeben können. Lösungen, die von der Edge aus schützen, vermeiden eine einzelne große „Nutzlast" und haben damit eine viel bessere Chance, Daten vor Cyberkriminellen zu schützen.

Im Fall von Microsoft ergab das Fehlen einer Ende-zu-Ende-Verschlüsselung in Verbindung mit der zentralen Datenspeicherung eine gefährliche Kombination. Denn wie viele andere E-Mail-Anbieter speichert auch Microsoft Daten im Klartext auf seinen Servern. Prinzipiell ist es ressourcenschonender, wenn Anbieter einfach eine Perimeter-Verteidigung um ihren zentralen Hub herum aufbauen und die Unternehmen die Verantwortung für diesen Schutz wiederum ihren Anbietern überlassen. Der große Nachteil dieses Ansatzes ist jedoch, dass mutwillige Angreifer, die diese Perimeter-Verteidigung überwinden und sich Zugang zu diesen Servern verschaffen, mit einem Schlag Zugriff auf alle Daten in diesem zentralen Hub erhalten – was bei Microsoft dazu geführt hat, dass die E-Mails von über 30.000 Unternehmen offengelegt wurden. Die Entscheidung für eine on-premises- oder Hybrid-Lösung kann daher das entscheidende Zünglein an der Waage sein, wenn es um das Thema Sicherheit geht. Denn eines ist klar: Wenn eine solche Infrastruktur weiterhin mit zentraler Datenspeicherung und -sicherung sowie veralteten Sicherheitsprotokollen vorherrscht, werden wir mit ziemlicher Sicherheit einen erneuten Anstieg dieser Art von Cyberattacken erleben.

Für eine sichere Zukunft

Genauso, wie wir den Klimawandel nicht mit einer öl- und kohlebetriebenen Energieinfrastruktur bewältigen können, werden wir die aktuellen Sicherheitsherausforderungen nicht lösen, indem wir uns auf Architekturen aus den 1970er Jahren verlassen. Zwar gibt es bereits einige Tools und Plattformen wie Protonmail und Tresorit, die auf diese neue Sicherheitsinfrastruktur setzen – und das ist ein guter Anfang. Wenn Unternehmen jedoch zukunftssicher sein und sich gegen die wachsende Bedrohung durch Cyberangriffe verteidigen wollen, muss ein viel größerer und grundlegenderer Wandel stattfinden. Dieser umfasst nicht nur den Einsatz moderner Technologien und Tools – auch ein unternehmensweiter kultureller Wandel muss stattfinden, der den tatsächlichen Ernst der Lage verdeutlicht. Deutsche Unternehmen tun daher gut daran, dem Beispiel der US-Regierung zu folgen, um jahrelange Sicherheitsmängel endlich zu beheben. Nur wenn sich Unternehmen weltweit diese schwierigen Lektionen über Zero Trust, Verschlüsselung und Daten-Compliance zu Herzen nehmen, kann die digitale Infrastruktur für alle Beteiligten sicherer werden und fatale Angriffe wie die von SolarWinds und Co. gehören endlich der Vergangenheit an.

Morten Brøgger

WENN UNTERNEHMEN ZUKUNFTSSICHER SEIN UND SICH GEGEN DIE WACHSENDE BEDROHUNG DURCH CYBERANGRIFFE VERTEIDIGEN WOLLEN, MUSS EIN VIEL GRÖSSERER UND GRUNDLEGENDERER WANDEL STATTFINDEN.

Morten Brøgger, CEO,
Wire, www.wire.com

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Robert Blank, Morten Brøgger, Johannes Karl, Ralf Kempf, Sabine Kuch, Thomas Kugelmeier, Sascha Martens, Carina Mitzschke, Andreas Nolte, Silvia Parthier, Ulrich Parthier, Kevin Schwarz, Stephan Schweizer, Jan Sudmeyer, Michael Veit, Steffen Voigt, Felix Zech

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 Veröff entlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 28.
Preisliste gültig ab 1. Oktober 2020.

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

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

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

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

Erscheinungsweise:
10x pro Jahr

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

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

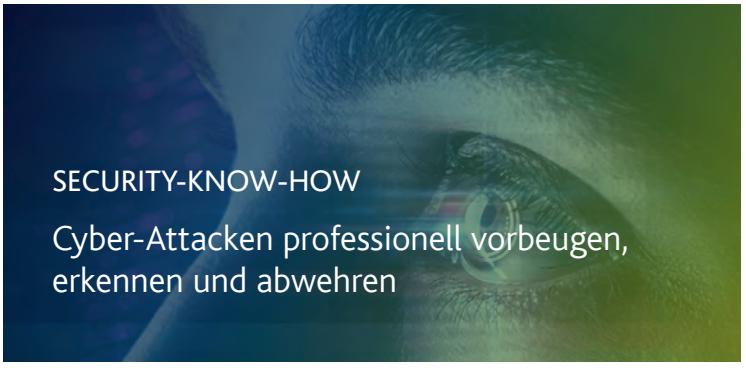
Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

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

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

Womit können wir Sie heute begeistern?

Künstliche Intelligenz | IT-Security | Cloud



Branchenwissen, Cloud-Expertise, KI-Kompetenz, Security-Know-how.

Erleben Sie Arvato Systems. ⟶ arvato-systems.de

brandeins /thema 2021 Heft 17 Beste IT-Dienstleister

top EMPLOYER DEUTSCHLAND GERMANY 2021 CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

arvato BERTELSMANN Arvato Systems

Arvato Systems | Reinhard-Mohn-Straße 200 | 33333 Gütersloh | info@arvato-systems.de

Empowering Digital Leaders.