itmanagement

JULI/AUGUST 2021

INKLUSIVE 32 SEITEN
IT SECURITY

INTERIM PROJEKT-MANAGEMENT

Auftrag erledigt – next please!

CUSTOMER DATA OPERATIONS

Consumer Capitalism

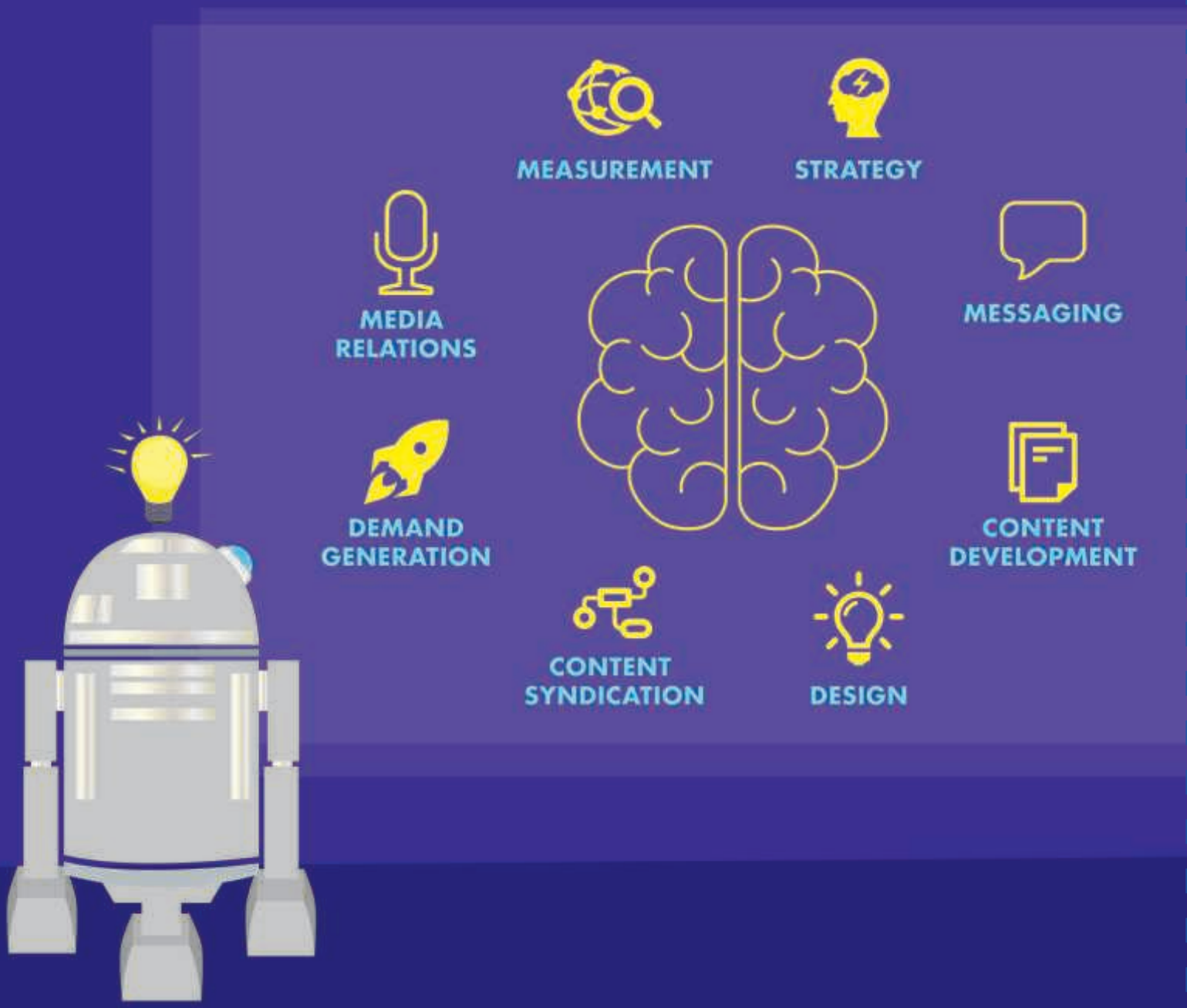
SAP-SECURITY

WARUM SIEM AUF DIESEM OHR TAUB IST

Ralf Kempf, SAST SOLUTIONS

www.it-daily.net

Thought Leadership



KÜNSTLICHE INTELLIGENZ
THOUGHT LEADERSHIP

DIGITALISIERUNG FÜR ALLE!

Vor kurzem landete eine Pressemitteilung mit dem Titel „Aktionstag für digitale Teilhabe gestartet“ in meinem Posteingang. Beim Überfliegen der Schlagzeile dachte ich, ich hab mich verlesen. Laut der repräsentativen Studie im Auftrag von „Digital für alle“ empfinden tatsächlich mehr als ein Siebtel der Deutschen die Digitalisierung als zu schnell voranschreitend. Nicht wirklich überraschend, fühlen sich 37 Prozent der über 75jährigen von der Digitalisierung überrannt. (Quelle: www.digitaltag.eu)

Auf der anderen Seite stehen allerdings 54 Prozent, denen der Fortschritt zu langsam vorangeht. Dieser Gruppe fühle ich mich zugehörig. Natürlich möchte ich die Vorteile der Digitalisierung nutzen und anwenden, Technologien erlernen, die mir Dinge abnehmen oder erleichtern, schneller und einfacher Zugang zu bestimmten Informationen erhalten. Grundvoraussetzung dafür ist aber der Zugang zur digitalen Welt und die Möglichkeit mich darin auch zurechtzufinden. Eine Grundvoraussetzung, die genau die Generation 70+ oft nicht hat. Gerade in Zeiten, in denen Behördengänge, Arzttermine und ähnliches digital erledigt werden könnten, hakt es einfach. So toll der Fortschritt und die sich ergebenden Möglichkeiten auch sind, es nützt nichts, wenn man bestimmte Bevölkerungsgruppen einfach vergisst. Denn nur, wenn „Digitalisierung greifbar und erlebbar ist, kann die ganze Gesellschaft den technologischen Wandel gestalten und davon profitieren.“

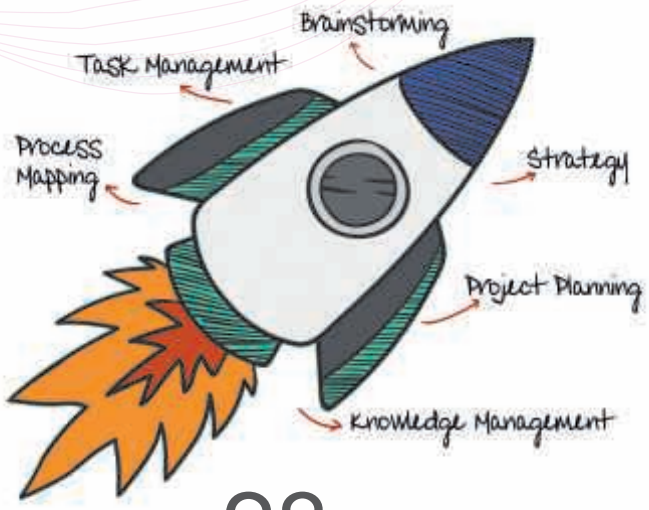
In diesem Sinne

Carina Mitzschke | Redakteurin it management

25

10

INHALT

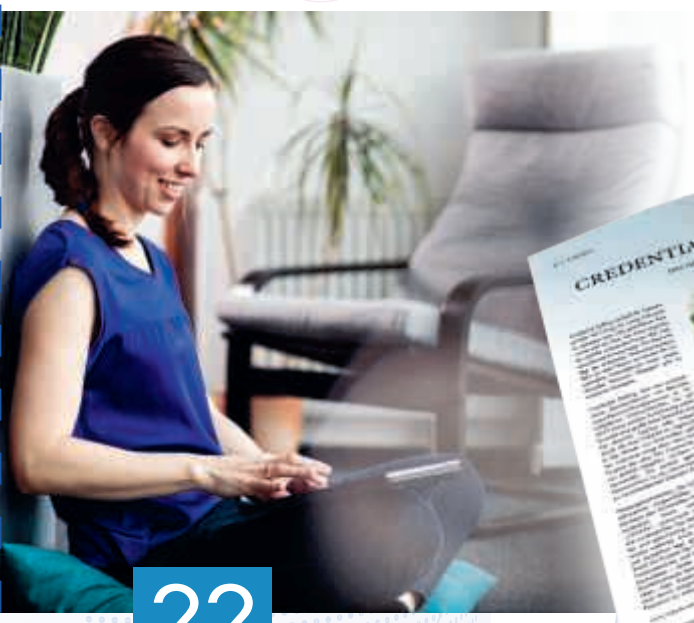


28

COVERSTORY

IT MANAGEMENT

IT INFRASTRUKTUR



Inklusive 32 Seiten

IT SECURITY SPEZIAL

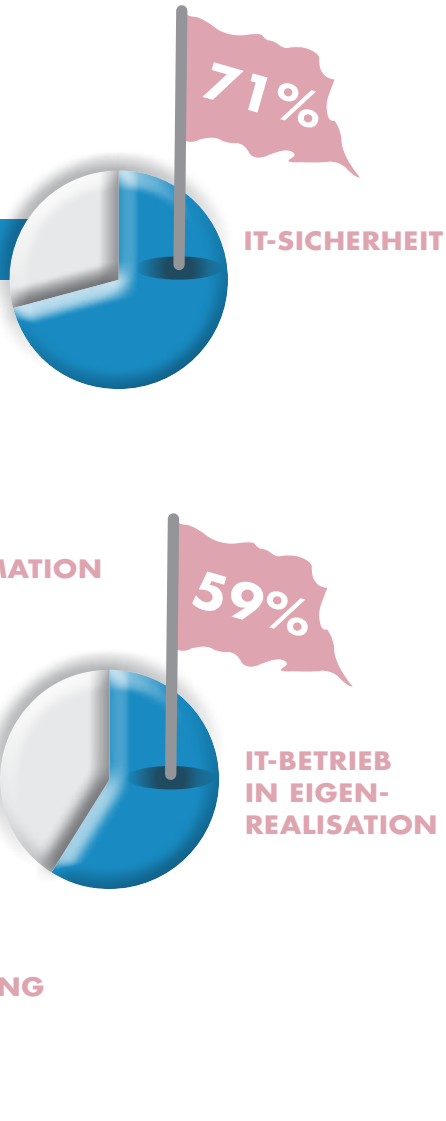
AKTUELLE STUDIE

IT-TRENDS IM MITTELSTAND

Die T-Systems Tochter operational services hat die IT-Trends im Mittelstand 2021 untersucht. Die Themen: digitale Transformation, IT-Sicherheit, Eigen- und Fremdrealisation des IT-Betriebes, Cloud und Prozessautomatisierung/KI.

Mehr als die Hälfte der Unternehmen ergänzen herkömmliche IT-Sicherheit demnach um proaktiven Schutz – ein Paradigmen-Wechsel. Zu den neuen Maßnahmen zählen Vulnerability Scanning oder Managed Detection Services. Ein Drittel der Unternehmen sehen sich als digitale Vorreiter, die Hälfte als digitale Follower. Alle übrigen Befragten ordnen sich den digitalen Nachzüglern zu.

www.operational-services.de



HANDLUNGSEMPFEHLUNGEN FÜR DIGITALE PROJEKTE

1. IT-Kompetenz stärken und digitale Transformation zur Chefsache machen
2. Benchmarks identifizieren und sich an digitalen Vorreitern orientieren
3. IT-Sicherheit abdecken und um proaktives Schwachstellenmanagement ergänzen
4. Den Digitalisierungserfolg in kleinen, schnellen Schritten sicherstellen
5. Die IT strategischer ausrichten, Eigenrealisation kritisch hinterfragen
6. Einsatz von Cloud-Anwendungen forcieren, um Flexibilität sicherzustellen

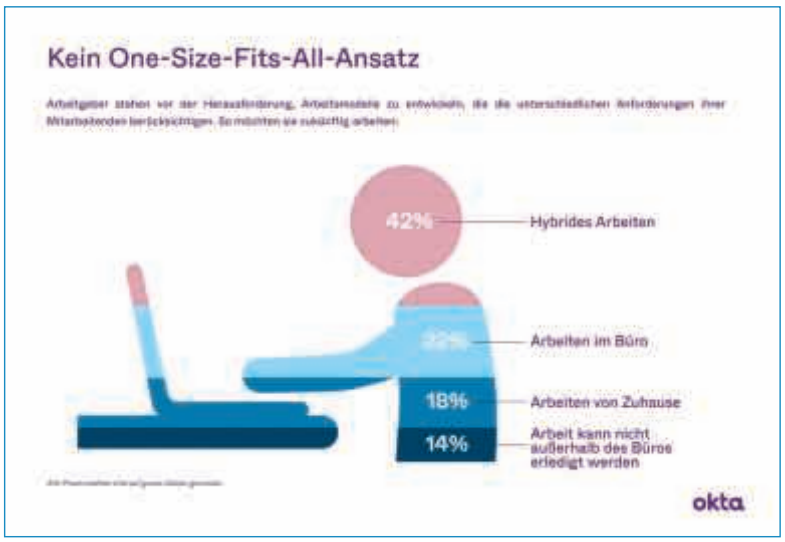
REMOTE WORK

PRO ODER CONTRA BÜROZWANG?

Mehr als ein Jahr nach dem Beginn des ersten bundesweiten Lockdowns möchten viele Arbeitnehmer nicht mehr zu ihrer früheren Arbeitsweise zurückkehren. Das ergab eine neue Studie von Okta und Censuswide.

Drei Viertel (75 %) der Befragten in Deutschland wären mit Gesetzesänderungen einverstanden, die es Unternehmen verbietet, sie zu zwingen, vor Ort im Büro zu arbeiten. 43 % wünscht sich Ausnahmeregelungen und ein Drittel (33 %) ist der Meinung, dass ein Vorschreiben des Arbeitsortes in allen Fällen gegen das Gesetz verstoßen sollte.

22 % der Büroangestellten in Deutschland möchten fünf Tage pro Woche im Büro arbeiten. In einer vergleichbaren Umfrage, die Okta im Mai 2020 durchführte, gaben noch 30 % der Arbeitnehmer an, dass sie wieder Vollzeit ins Büro zurückkehren möchten. Obwohl in Deutschland im europäischen Ländervergleich der Wunsch, Vollzeit im Büro zu arbeiten noch immer am stärksten ausgeprägt ist, geht der Trend hin zu dynamischeren Arbeitsmodellen.



www.okta.com/de

PROZESSANALYTIK

WIRTSCHAFTLICHER MEHRWERT

Mit der Global Process Mining Survey 2021 bewertet Deloitte erstmals die aktuelle Verbreitung von Process Mining (PM) und liefert Einblicke, wie mit der Technologie nachhaltig Mehrwerte erzeugt werden können. Ziel der Umfrage ist die Identifizierung von Trends und Fallstricken in Process Mining-Projekten, um Anwender bei einem langfristig erfolgreichen Einsatz von PM zu unterstützen und ihnen zu ermöglichen, in ihren Initiativen und Projekten messbare Verbesserungen und damit echte Mehrwerte zu generieren.

Vor allem Softwareanbieter schüren hohe Erwartungen und vermarkten die unbegrenzten Möglichkeiten von Process Mining. Einer der wesentlichsten Punkte ist der Vorteil, dass sie alles in einem Paket liefern kann – ein Grund, warum Process Mining oft als Allround-Talent verstanden wird.

www.deloitte.de

63% **... DER STUDIENTEILNEHMER HABEN BEREITS MIT DER IMPLEMENTIERUNG VON PM BEGONNEN**

87% **... PLANEN EIN PILOTPROJEKT ODER EINEN PROOF-OF-CONCEPT**

83% **... DER UNTERNEHMEN, DIE PM BEREITS ANWENDEN, PLANEN EINE AUSWEITUNG IHRER INITIATIVEN**

DIE ROLE CONVERSION IST KEIN KINDERSPIEL

WIE MAN S/4HANA-BERECHTIGUNGSPROJEKTE DENNOCH SICHER UND ZÜGIG MEISTERT

Eine Umfrage im Rahmen des ITOK-Expert-Talks zu den größten Herausforderungen für SAP-Security ergab im März, dass gut die Hälfte der Befragten diese im Umfeld von Rollen und Berechtigungen sehen. Die Einbettung des Berechtigungskonzeptes stellt also eine der Kernaufgaben bei der S/4HANA-Einführung dar und ist ein häufiger Grund dafür, dass diese als Ganzes scheitert. Wie aber ist mit Konflikten wie Ressourcenengpässen, Prioritätenverschiebungen bei Teilprojekten, Änderungen bei Tasks und Tests umzugehen? Warum neben Ansatz und Projektmanagement das richtige Berechtigungskonzept über Erfolg und Dynamik der Transformation entscheidet, erklärt Roozbeh Noori-Amoli, Deputy Head SAST CONSULTING, im Interview im it management-Herausgeber Ulrich Parthier.

Ulrich Parthier: *Herr Noori-Amoli, Sie haben gerade erfolgreich eine globale Role Conversion mit PUMA SE abgeschlossen. Was sind die wichtigsten Überlegungen, die man vor der S/4HANA-Migration anstellen sollte?*

Roozbeh Noori-Amoli: Zuerst natürlich, welcher Ansatz dem Projekt gerecht wird, also etwa Green-, Brown- oder Bluefield. Beim Vorgehen muss zwischen klassischem und agilem Projektmanagement entschieden werden. Und dann folgt schon die Frage: Wie sieht mein Berechtigungskonzept aus? Richtet es sich wie häufig nach dem einzigen Vorschlag eines Beraters oder einem Best-Practice-Ansatz ohne Bezug auf das Unternehmen und die projektspezifischen Bedürfnisse? Dann ist das schon der eigentliche Kardinalfehler: Denn man muss sich die Vor- und Nachteile der verschiedenen Konzepte vorher bewusst machen, die ja alle je nach Situation ihre Daseinsberechtigung haben. Hat man die falsche Wahl getroffen, erkennt man das häufig erst nach etlichen Tagen, die bereits für die Implementierung aufgewendet wurden, oder schlimmer noch, erst später im Alltag. Die nach-

> DIE WAHL DES BERECHTIGUNGSKONZEPTS IST EINE ABWÄGUNG ZWISCHEN DEM BEDÜRFNIS NACH HOHER SICHERHEIT UND DEM WUNSCH NACH MINIMALEM ADMINISTRATIONSAUFWAND.
>
> Roozbeh Noori-Amoli, Deputy Head Consulting, SAST SOLUTIONS, https://sast-solutions.de

trägliche Korrektur kann dann hohe Aufwände und Kosten bedeuten.

Ulrich Parthier: *Aber wie lässt sich angesichts der Vielfalt das richtige Berechtigungskonzept finden?*

Roozbeh Noori-Amoli: Dafür müssen von Beginn an die wichtigsten Fragen geklärt werden: Wie ist der tatsächliche Unternehmensbedarf, was sind die Projektziele und wie hoch ist das Sicherheitsbedürfnis? Wie sind Budget sowie zeitliche und personelle Ressourcen bemessen? Limitierende Faktoren wie die bestehenden organisatorischen Strukturen und Prozesse, die Anzahl der SAP-User sowie grundsätzlich die Art und Architektur des Systems geben bereits einen festen Rahmen vor. Die Priorisierung der Ziele wird dann von der jeweiligen IT-Strategie bestimmt. Die Wahl des Berechtigungskonzepts ist so letztlich eine Abwägung zwischen dem Bedürfnis nach hoher Sicherheit mit passgenauen Berechtigungen und dem Wunsch nach minimalem Administrationsaufwand. Als Zielkonflikt könnte man die minimale Vergabe von Berechtigungen vs. die Vereinheitlichung von Prozessen formulieren.

Ulrich Parthier: *Können Sie uns ein paar Szenarien nennen, wann welches Konzept Sinn macht?*

Roozbeh Noori-Amoli: Also, bei einer internationalen Organisation mit vielen gleichen Unternehmensteilen und wiederkehrenden Prozessen funktioniert zum Beispiel der Template-Rollenansatz mit Ableitungen nach organisatorischen Einheiten oder das Menu/Value-Rollenkonzept. Bei einem sehr hohen Sicherheitsbedürfnis und dem Wunsch nach präziser Vergabe der Berechtigungen und gleichzeitig einer niedrigen Anzahl verwendeter Transaktionen je User und einem System mit wenigen, aber unterschiedlichen Prozessen empfiehlt sich stattdessen das Konzept 1 Transaktion – 1 Rolle.

Ulrich Parthier: *Gibt es konkrete Beispiele aus Ihrer Erfahrung für eine richtige und eine schlechtere Wahl?*

Roozbeh Noori-Amoli: Gerne, das lässt sich gut anhand der durchdachten und einer weniger durchdachten Entscheidung für dasselbe Berechtigungskonzept zeigen. Der Kunde PUMA mit rund 14.000 Mitarbeitern in 50 Ländern hatte viele länderspezifische Eigenentwicklungen und Schnittstellen sowie hohe Compliance-Anforderungen. Das Projekt beinhaltete den Start der Migration mit 4 Ländern und unterschiedlichen SAP ERP-Systemen auf S/4HANA. Wegen vieler Organisationseinheiten, verteilter Prozesse, kritischer Länderspezifika ergab sich die Herausforderung, ein globales Berechtigungskonzept zu erstellen, das anschließend auf Länderebene in die Tiefe ausgerollt werden sollte. Wir haben uns mit PUMA schließlich für prozessuale Einzelrollen mit funktionalen Arbeitsplatz-Sammelrollen entschieden, weil es viele Einheiten gibt, die ähnlich sind, zentral verwaltet, mit zentraler Revision und einem einheitlichen Konzept mit Sonderrollen sowie Ableitungen über Organisationsebenen. Der Kunde ist damit heute hochzufrieden, zumal wir das Ganze mit einem agilen Projektmanagement-Ansatz sehr zügig, dynamisch und flexibel umgesetzt haben.

Ulrich Parthier: *Und die schlechtere Entscheidung?*

Roozbeh Noori-Amoli: Dass dasselbe Konzept aber längst nicht für jeden die richtige Wahl ist, wurde bei einem anderen Projekt deutlich: Hier war auf dringlichen Wunsch des Kunden und ohne vorhergehende Beratung ebenfalls genau dieses Berechtigungskonzept umzusetzen. Dabei wurde jedoch in den Workshops mit den Fachbereichen schnell klar, dass es nur bedingt möglich war, Benutzer in homogene Gruppen zu separieren und eine klare Trennung der einzelnen Prozesse zu implementieren. Letztlich konnten wir den Kunden deshalb überzeugen, ein hybrides Berechtigungskonzept vorzuziehen, um besser auf die Gegebenheiten der Länder- und Abteilungsspezifika eingehen zu können.

Ulrich Parthier: *Welche Learnings können Sie für eine gelungene Role Conversion mit auf den Weg geben?*

Roozbeh Noori-Amoli: Wichtig ist, von Beginn an Zeit für das Testing einzuplanen und zwischen dem Test-, dem Schulungsmanagement und dem Berechtigungsteam eine detaillierte Abstimmung sicherzustellen. Ein agiles Projektmanagement birgt hier große Vorteile: Integrations-, Regressions- und Berechtigungstests werden dabei nicht separat betrachtet, sondern parallel durchgeführt. Die gesamte Thematik muss frühzeitig gemeinsam mit den Fachbereichen angegangen werden, schließlich gilt es, fachbereichsübergreifende Entscheidungen hinsichtlich der Rollen-Inhalte zu treffen und kundeneigene Kataloge und Gruppen zu erstellen, um nicht auf den überladenen SAP-Standard zurückgreifen zu müssen. Eine weitere Erkenntnis: Weg vom Berechtigungsteam, hin zu je einem Verantwortlichen in den Fachabteilungen. Sinnvoll ist eine passgenaue Tool-Unterstützung, benötigt werden Standard-Templates für Vorschlags-Rollen zum Testen sowie saubere und SoD-freie Rollen. Berechtigungen dürfen nicht nur auf Funktionalität getestet werden, sondern es müssen auch Negativ-Tests stattfinden. Ein unterbrechungsfreies Tagesgeschäft sollte unbedingt durch einen Safe-go-live-Ansatz gewährleistet bleiben. Wichtig ist schlussendlich, ausreichend Zeit und Ressourcen einzuplanen, das Thema kann nicht einfach neben dem Tagesgeschäft umgesetzt werden.

Ulrich Parthier: *Herr Noori-Amoli, wir danken für dieses Gespräch.*

SAP-SECURITY

WARUM SIEM AUF DIESEM OHR TAUB IST UND WIE MAN SAP-INCIDENTS DENNOCH GEHÖR VERSCHAFFT

Für die SAP-Sicherheit greift die übliche SIEM-Überwachung oft zu kurz, da die speziellen SAP-Protokolle und -Auswertungen nicht verstanden und folglich keine Angriffsmuster ausgemacht und erkannt werden können. Warum dies so ist, was Unternehmen tun können, um SAP dennoch in ihr Monitoring zu integrieren, und warum diese ganzheitliche Absicherung sogar zusätzliche Vorteile mit sich bringen kann, lesen Sie im folgenden Beitrag.

SIEM (Security Information and Event Management) dient der Sicherheit der IT-Umgebungen von Unternehmen und Organisationen und kombiniert Security Information Management (SIM) und Security Event Management (SEM), um Echtzeitanalysen von Sicherheitsalarmen zu erstellen. Durch das Sammeln, Korrelieren und Auswerten von Logdaten, Meldungen, Alarmen und Logfiles werden Angriffe, außergewöhnliche Muster oder gefährliche Trends erkannt. Damit bietet SIEM einen Überblick über sicherheitsrelevante Ereignisse in IT-Umgebungen und hilft, gesetzliche Vorgaben, Richtlinien und Compliance-Regularien der IT-Sicherheit zu erfüllen. Die wesentlichen Aufgaben: Berichte über sicherheitsrelevante Vorfälle wie erfolgreiche oder fehlgeschlagene Anmeldungen, aber auch Malware- und andere mögliche schädigende Aktivitäten bereitzustellen und Benachrichtigungen zu senden, wenn die Analyse ergibt, dass eine Aktivität gegen vorgegebene Regelsätze verstößt und somit auf ein mögliches Sicherheitsproblem hinweist.

Die Funktionsweise von SIEM

Kritische Aktivitäten können durch die Bündelung von Daten an einer zentralen Stelle, durch Analysemuster und Trends frühzeitig erkannt werden. Das Sammeln und die Interpretation der Daten erfolgen in Echtzeit und die gewonnenen Informationen werden unveränderbar gespeichert. Gängige Quellen für SIEM sind etwa Server, Firewalls, Router, IPS und IDS. Deren Daten werden an eine zentrale Station weitergeleitet, die sie für die Speicherung sichert, normalisiert, strukturiert und auswertet. Die Analysen nutzen Regeln, Korrelationsmodelle, maschinelles Lernen und künstliche Intelligenz, um Beziehungen zwischen den Einträgen zu generieren und Auffälligkeiten zu erkennen. Ein Angriff wird im Gegensatz zu anderen Security-Maßnahmen also nicht im Vorfeld abgewehrt, dessen Auswirkungen und Ausweitung können aber zum Beispiel durch Alarmierungen reduziert werden. Zudem erlauben diese und auch automatisierte Berichte Reaktionen auf unterschiedliche Bedrohungen in Echtzeit und nachträgliche Nachweise von Sicherheitsereignissen. Leider funktioniert dieses Prinzip kaum bei SAP-Systemen.

Parallelwelten: SAP und SIEM

Dass SIEM und SAP sich sozusagen auf Anhieb missverstehen, hat eine ganze Reihe von Gründen: So hat das SIEM seinen Ursprung in der klassischen Netzwerktechnik, aus Zeiten unter DOS und Ethernet mit großen eigenständigen Mainframe-Applikationen für Rechnungswesen, Controlling, Finanzwirtschaft, alle voneinander abgekoppelt. Als dann der IT-Kosmos immer vernetzter wurde, begann man mit SIEM zu überwachen, was auf dem Netzwerk-Layer passiert, mit den Fragestellungen, woher eigentlich eine Information stammt, wer darauf zugreift, was man bereits kennt oder was eben aus der Reihe fällt. Wichtig sind also Rule Sets, mit denen man prüft, was auf dem Netzwerk passiert, und daraus Schlüsse für die Sicherheit zieht. Klassische SIEM-Tools betrachten daher nicht

einzelne Applikationen, sondern IT-Infrastrukturen. In den letzten Jahren wurde immer deutlicher, dass man auch Applikationen einbeziehen muss, ob Microsoft Dynamics, ein Produktplanungstool oder ein SPS in der Produktion. Bezüglich SAP folgt nun jedoch das große Aber: Es unterscheidet sich gravierend von anderen Applikationen und ist quasi ein Netzwerk für sich, mit SAP kann ich sehr viele verschiedene Dinge tun, sowohl mit Rollen und Berechtigungen als auch hinsichtlich Security. Viele Mechanismen sind zwar der IT sehr ähnlich, aber SAP differiert bereits hinsichtlich Nomenklatur und Rule Sets. Für die Netzwerktechnik und den Rest der IT ist SAP also quasi eine fremde Welt mit einer anderen Sprache und eigener Diktion. Deswegen findet sich in den Firmen auch noch oft die Trennung SAP und Rest der IT.

SAP stößt bei SIEM auf taube Ohren – müsste es aber nicht

Klassische SIEM-Tools konzentrieren sich auf die Erkennung ungewöhnlichen Verhaltens innerhalb von Infrastrukturen. SAP-Systeme werden dabei oft nicht gehört. Schafft man keinen Zugang zu SAP, erkennt SIEM wenig mehr als ein Art Grundrauschen von Logs mit Millionen Einträgen, die am Ende kaum jemand deuten kann oder will. Anders gesagt: Für SIEM-Tools liegen SAP-Systeme im toten Winkel, denn sie haben keine speziellen SAP-Prüfregeln. Aufgrund fehlender Angriffsmuster werden Bedrohungen und auch Prüf-Attacken von Security-Teams daher meist nicht identifiziert. Exceptions in SAP können auf Netzwerkebene unauffällig scheinen und sind nur erkennbar, wenn man die Applikation selbst betrachtet. Diese Verständnisprobleme führen dazu, dass viele das Thema SAP gar nicht oder als Letztes anfassen, weil man ja lieber das angeht, was man versteht. Darum wird SAP oft stiefmütterlich behandelt und daher geschieht es häufig, dass selbst Unternehmen, die hochprofessionell IT-Security betreiben, die SIEM im Einsatz haben und alle Non-SAP-Bereiche par excellence beherrschen, SAP unwissentlich oder gar wissentlich ausblenden. Weil sie etwa hoffen, dass ihre SAP-Mitarbeiter dies irgendwie selbst kontrollieren, dass das unvollständige SIEM schon ausreichen wird oder weil man vielleicht nicht einmal weiß, dass es die Möglichkeit gibt, diese Lücke zu schließen. Hier muss sich wohl so mancher CISO, die SIEM bereits im Einsatz hat, fragen lassen: Seid Ihr sicher, dass Ihr SAP auch ausreichend betrachtet? Falls nicht – führt beide Welten zusammen, denn dies macht einfach Sinn.

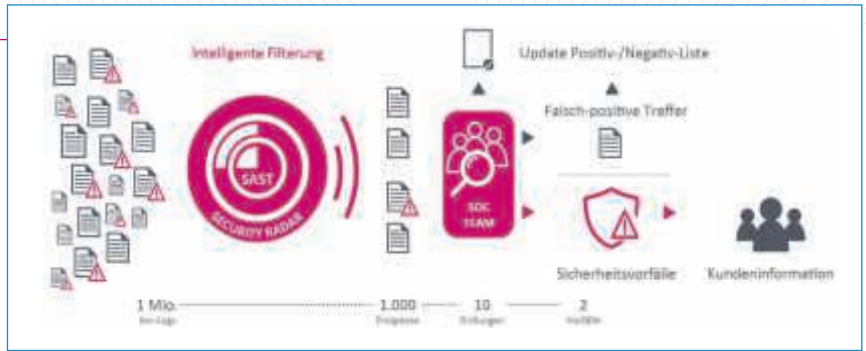
Das Beste aus beiden Welten

Da die Netzwerker effiziente Tools zur Übersicht geschaffen, dabei aber häufig vergessen haben, dass es um sie herum noch andere Welten gibt, gilt es im Rahmen ganzheitlicher Absicherung nun, beide Welten zum Vorteil des Unternehmens zusammenzuführen. Und hier kommt Software wie die SAST SUITE ins Spiel, die Events aus dem Applikationslayer herauszieht und so transportiert und übersetzt, dass die SIEM-Netzwerker damit etwas anfangen können. Die Erkennung von Angriffen auf Basis von Log-Dateien und die Auswertung von Netzwerkverkehr erfordert tiefe Kenntnisse über Angriffswege und -muster. Um diese Security-Daten auswerten zu können, ist ein intelligentes Management aller Informationen notwendig. Die sicherheitsrelevanten Events müssen aus der Fülle der Daten herausgefiltert und in den richtigen Kontext gestellt werden. Der SAST Security Radar analysiert zur Gefahrenerkennung daher nicht nur SAP-Protokolle, sondern integriert auch Konfigurations- und Rollenanalysen. Die SAST SUITE speist diese Informationen aus SAP „out of the box" in bestehende SIEM-Systeme aller Couleur ein und macht sie auswertbar. Das funktioniert vom kleinen bis zu den weltgrößten SAP-Systemen unserer Kunden, teilweise für über 1.000 Systeme. Ein weiterer Vorteil ist das Security Dashboard: Durch die Integration mit einem übergreifenden SIEM-Tool können alle sicherheitsrelevanten Vorfälle von SAP ERP- und S/4HANA Systemen mit anderen relevanten IT-Systemen konsolidiert werden. So findet SAP im SIEM Gehör und Unternehmen erhalten auf Knopfdruck eine bewertete Dashboard-basierte Darstellung ihres gesamten Sicherheitsstatus.

Ralf Kempf

BEI DER AUSWAHL EINES SIEM-TOOLS IST ES WICHTIG, DARAUF ZU ACHTEN, DASS ES IN DER LAGE IST, ALLE RELEVANTEN DATENQUELLEN IN DER UNTERNEHMENS-INFRASTRUKTUR ZU INTEGRIEREN – INSBESONDERE SAP.

Ralf Kempf, CTO, SAST SOLUTIONS, https://sast-solutions.de



Intelligente Filterung kritischer Ereignisse durch die SAST SUITE

Quelle: Getty Images

SITZUNGEN – DIGITAL ABER SICHER

DIE MEETINGSUITE VON BRAINLOOP SCHAFFT VERTRAUEN

Seit über einem Jahr müssen wir mit der Pandemie zurechtkommen und Home Office sowie Kontaktbeschränkungen werden uns sicherlich auch noch eine Weile begleiten. Damit stehen auch digitale Meetings weiter auf der Tagesordnung. Dennoch werden diese oft noch mit improvisierten Lösungen durchgeführt. Das kann besonders auf Führungsebene zu einem Sicherheitsrisiko werden. Unternehmen sollten daher auf professionelle Tools zur Durchführung ihrer digitalen Gremien-Meetings setzen.

Wie sollen Aufsichtsräte und Vorstände in der jetzigen Situation effiziente und sichere Meetings abhalten? Diese Frage stellen sich nicht nur die Mitglieder der Gremien, sondern auch Mitarbeiter, die für die Vor- und Nachbereitung der Sitzungen zuständig sind. Zunächst müssen die Sitzungsmappen zu den Mitgliedern gelangen. E-Mails sind schon der Größe der Dateien wegen keine praktikable Lösung – von der Sicherheit ganz zu schweigen. Auch die Nutzung allgemein bekannter File-Sharing-Dienste verbietet sich aus Sicherheits- und Compliance-Gründung. Muss man daher ganz auf die Digitalisierung dieser Dokumente verzichten?

Mehr Sicherheit durch die richtige Digitalisierung

Viele Unternehmen verschicken in der Tat ausgedruckte Sitzungsmappen mit der Post an Vorstands- oder Aufsichtsratsmitglieder. Damit umgehen sie zwar die Gefahren unsicherer digitaler Kommunikationskanäle, schaffen aber auch neue Risiken. Auch auf dem Postweg können Sendungen verloren gehen oder in falsche Hände geraten. Das kann ebenso mit nicht mehr benötigten aber bereits gedruckten Unterlagen passieren – schließlich hat nicht jeder einen Aktenvernichter zuhause.

Die Lösung ist also nicht einen Schritt zurück ins analoge Zeitalter zu machen, sondern auf sichere digitale Lösungen zu setzen. Damit eine Lösung für den Dokumentenaustausch als sicher gelten kann, sollten Unternehmen darauf achten, dass sie folgende Punkte erfüllt:

Hosting der Daten in zertifizierten Rechenzentren im Inland oder im EU-Rechtsraum – das ist unter anderem wichtig, um die Vorgaben der DSGVO zu erfüllen.

- Durchgehende Verschlüsselung der Datenbanken.
- Betreiberabschirmung, die gewähr-

leistet, dass nur das Unternehmen selbst Zugriff auf die eigenen Datenräume hat.
- Trennung der Administrations- und Datenebene, was bedeutet, dass die IT-Abteilung zwar die Lösung verwaltet, selbst aber keinen Zugriff auf die in den sicheren Datenräumen abgelegten Daten besitzt.
- Möglichkeiten der sicheren Authentifizierung.
- Nachvollziehbarkeit aller Aktionen dank durchgängiger Protokollierung (Audit-Trail).

Effizienz und Sicherheit müssen kein Widerspruch sein

Hohe Sicherheitsanforderungen verbinden viele noch immer mit Komplexität in der Anwendung. Das muss aber nicht sein. Zwar beruht auch eine Lösung wie die MeetingSuite von Brainloop auf komplexen Sicherheitstechnologien, doch davon bekommen die Anwender so gut wie nichts mit. Sie werden lediglich bei der Anmeldung zu einer Zweifaktor-Authentifizierung aufgefordert, die aber auch in Sekundenschnelle erledigt ist. Um die Technologie hinter den Sicherheitsfeatures und um die Compliance mit den entsprechenden Regularien, kümmert sich der Lösungsanbieter. Durch die abgeschlossene Datenraumarchitektur wird sichergestellt, dass dabei nicht einmal Brainloop als Lösungsanbieter und -Betreiber Zugriff auf die Unternehmensdaten hat.

Der gesamte Ansatz von Brainloop lässt sich als Security by Design zusammenfassen, das heißt, Sicherheit wird von Beginn der Entwicklung aller Lösungen als Toppriorität betrachtet. Dazu gehört auch die Verpflichtung, alle Daten von Unternehmen im Inland zu speichern und eine aktuelle Zertifizierung nach gängigen Zertifikaten anzustreben. Die Einhaltung aller relevanten Richtlinien wird zudem durch regelmäßige Sicherheitsaudits überprüft.

Vor diesem Hintergrund können Gremienmitglieder unbesorgt mit bereitgestellten Dokumenten arbeiten, die sie auch online kommentieren können. In die Brainloop-Lösung ist ebenfalls ein Tool zur Online-Beschlussfassung integriert, das Abstimmungen vereinfacht. Doch nicht nur Mitglieder profitieren von der innovativen Lösung, sondern auch ihre Assistenzen, die die Meetings vorbereiten. Sie werden beispielsweise bei der Erstellung der digitalen Sitzungsmappen im Vorfeld unterstützt, ebenso wie bei der Nachbereitung und der Erstellung von Sitzungsprotokollen. Umfangreiche Automatisierungsmöglichkeiten entlasten die Teams und helfen dabei, menschliche Fehler zu vermeiden.

Sicher unterwegs – auf allen Geräten

Die sich immer wieder und kurzfristig ändernden Rahmenbedingungen während der Corona-Pandemie zeigen wieder einmal, wie wichtig es für Führungsgremien ist, kurzfristig Entscheidungen treffen zu können. Gerade Ausnahmesituationen lassen oft keine Zeit, um ein Meeting im gewohnten Rahmen einzuberufen. Dann müssen Entscheidungen ad hoc getroffen werden. Fundiert sollen sie dennoch sein, was bedeutet, dass Führungskräfte Zugriff auf wichtige Daten als Entscheidungsgrundlage haben müssen, wo auch immer sie sich gerade befinden. Das setzt natürlich die Nutzung mobiler Geräte voraus.

Doch mit jedem mobilen Gerät steigt auch das Risiko für Datenverstöße, -verluste, Diebstahl oder andere Unwägbarkeiten. Das kann unmittelbare Folgen haben, durch Diebstahl von Geschäftsgeheimnissen aber auch juristische Folgen, wegen Nichteinhaltung von Datenschutzrichtlinien. Deshalb ist es bei mobilen Geräten umso wichtiger darauf zu achten, auf welchen Wegen Daten übertragen werden und wo sie gespeichert sind. Am besten werden sensible Unterlagen nämlich gar nicht auf das jeweilige Mobilgerät übertragen und dort gespeichert, sondern verbleiben im sicheren Datenraum, wo sie der Mobilnutzer lediglich einsehen kann – nach gelungener Authentifizierung, versteht sich.

VIRTUELLE ODER HYBRIDE SITZUNGEN WERDEN AUCH IN NAHER ZUKUNFT FESTER BESTANDTEIL VON EFFIZIENTER GREMIENARBEIT SEIN.

Kevin Heinloth,
Modern Governance Solution Advisor,
Brainloop AG, www.brainloop.de

Ein Blick in die Zukunft

Die Pandemiebekämpfung macht immer mehr Fortschritte und es wird langsam absehbar, dass wir demnächst zu einem normaleren Leben zurückkehren können. Doch auch wenn Schulen, Restaurants und Geschäfte wieder wie gewohnt öffnen werden, heißt das nicht, dass dann auch alle Mitarbeiter wieder in gleicher Zahl ins Büro strömen werden. Das Konzept Homeoffice wird die aktuelle Krisensituation sicherlich überleben. Zwar nicht im heutigen Umfang, aber wir werden wesentlich mehr hybride Arbeitsmodelle sehen.

Außerdem versuchen immer mehr Unternehmen, an ihrer Klimabilanz zu arbeiten und auf unnötige Reisen zu verzichten. Virtuelle oder hybride Sitzungen werden daher auch in Zukunft fester Bestandteil von effizienter Gremienarbeit sein. Es lohnt sich daher umso mehr, jetzt in sichere digitale Kollaborationslösungen zu investieren.

Kevin Heinloth

Mehr zur MeetingSuite finden Sie hier:
https://bit.ly/3fGQLlm

CONSUMER CAPITALISM

WIE UNTERNEHMEN CUSTOMER DATA OPERATIONS SINNVOLL NUTZEN

Mitte der 1970er Jahre wurde der Fokus auf den Shareholder Value für einige Jahrzehnte zu einem zentralen Ansatz in der Unternehmenssteuerung. Das Ziel: Aktionäre durch die Maximierung der Rendite zufriedenstellen. Doch darum geht es heute schon lange nicht mehr. Unternehmen wie Shopify, Amazon, TikTok oder Netflix zeigen, wie Erfolg gelingt, indem sie den Kundennutzen in den Mittelpunkt rücken und so das Konzept „Consumer Capitalism" vorleben. Diesen kundenzentrieren Ansatz können Firmen in ihren Strukturen etablieren, wenn sie die Möglichkeiten der digitalen Transformation konsequent für sich nutzen und Informationen als wertvolles Instrument wahrnehmen sowie einsetzen.

Customer Data Operations

Die „digitalen Fußspuren" von Kunden sind häufig in Kalendern, Posteingängen und Dateiablagen der Unternehmen versteckt oder wurden teilweise in eine ERP- oder Buchhaltungslösung eingepflegt. Den Weg in das Customer-Relationship-Management-System (CRM) finden sie jedoch selten. Hier kommt Customer Data Operations – auch „Data Ops" genannt – ins Spiel. Diese Methode ermöglicht es Unternehmen, ihre Informationen von deren Speicherort loszulösen. So lassen sich essenzielle Kundendaten aus diversen Quellen auslesen, kategorisieren und Zusammenhänge automatisch erschließen sowie verknüpfen. Diese neu aufbereiteten Informationen können dann unter Berücksichtigung aller Datenschutz- und Sicherheitsvorschriften an die jeweiligen Mitarbeiter zurückgespielt werden, sodass diese jederzeit alle wesentlichen Kundendaten schnell überblicken und nachhaltig eine positive Customer Experience aufbauen können.

Smarte, sichere, skalierbare Datenintegration

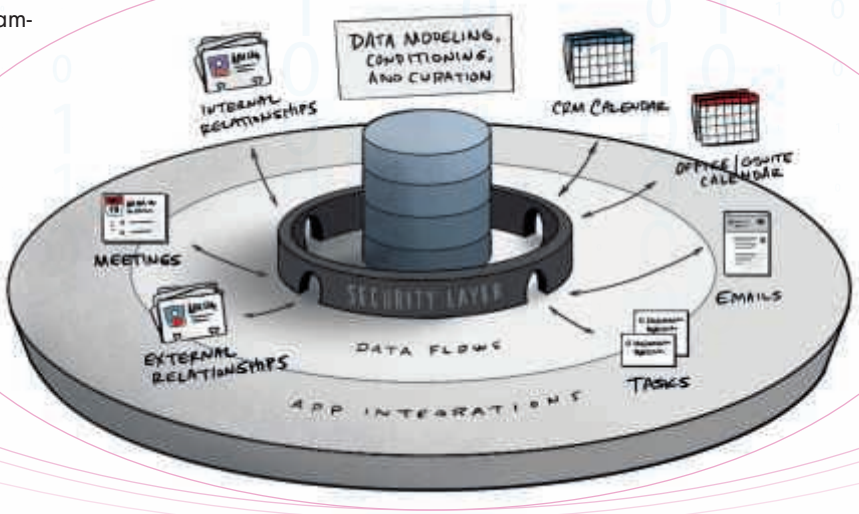
Konkret legen Data Ops Informationen aus unterschiedlichsten Anwendungen offen, indem sie die Workflows und Nutzungsbeschränkungen beseitigen. Allerdings gilt es hier, bei der Wahl eines Technologiepartners dessen Erfahrung und Sensibilität für Datenschutzthemen zu prüfen, um alle Sicherheits- und Compliance-Regelungen einzuhalten. Sogenannte Pass-Through-Technologien entkoppeln die Informationen von den Software-Anwendungen, in denen sie ursprünglich erfasst und gespeichert wurden, und entfalten so ihr volles Potential.

Die Datenintegration erfolgt im Hintergrund und die Teams erhalten automatisch ein vollständigeres, aktuelleres Bild von jedem einzelnen Kunden. Wenn ein Nutzer anruft, kann der verantwortliche Mitarbeiter dessen Erwartungen und Anforderungen viel konkreter antizipieren und gezielter auf die individuellen Bedürfnisse eingehen, weil Data Ops ihm automatisch genau die richtigen Informationen zur Verfügung stellt. Diese Technologie unterstützt auch das Management, weil sie mittels strukturierter, vollständiger Daten bessere Entscheidungsgrundlagen liefert.

Eine neue Ebene im Technologie-Stack

Mit der zunehmenden Entwicklung in Richtung Consumer Capitalism haben Unternehmen sowohl die wachsende Bedeutung eines kundenzentrierten Ansatzes als auch die Beschränkungen der Software-Applikationen erkannt. Data-Ops-Plattformen, wie beispielsweise die Riva Relationship Engine, konzentrieren sich gezielt auf die sichere, effiziente Datenintegration. Unternehmen haben so die Chance, die wertvollen Informationen ihrer Kunden zu nutzen, um ihnen maßgeschneiderte Produkte und Dienstleistungen anzubieten, die auf deren individuelle Anforderungen abgestimmt sind. Mit diesem Mehrwert hat sich Customer Data Operations als neue Ebene im Technologie-Stack etabliert.

Aldo Zanoni, Stéphane Zanoni
www.rivaengine.com



OPERATIONAL SERVICES
YOUR ICT PARTNER

DATA CENTER KONSOLIDIEREN CLOUD SERVICES INTEGRIEREN

ICT Transformation sicher, verlässlich und stabil umsetzen

Die Anforderungen an IT-Services haben sich gewandelt. Immer mehr Business-Prozesse werden digitalisiert, Cloud Services spielen eine zunehmend wichtige Rolle und auch ein optimiertes eigenes Rechenzentrum ist für viele Organisationen wertvoll. Marktveränderungen sowie Kunden erfordern vor allem eines: Flexibilität. Mit konsolidierten Data Centern und ausgewählten Anwendungen und Services aus der Cloud erreichen Sie genau das.

Planung und Umsetzung einer solchen ICT-Transformation sind komplex, vor allem, wenn man bedenkt, dass Zukunftssicherheit und Stabilität höchste Priorität haben. Unsere erfahrenen IT-Architekten und Projektleiter begleiten Unternehmen als kompetente Partner für eine nahtlose Migration zu hybriden Szenarien und bei der Integration von Cloud Services. Dabei bringen wir Sie revisionssicher und unterbrechungsfrei in Ihr zukünftiges Betriebsmodell.

Profitieren Sie von unserer Expertise und verlassen Sie sich auf uns als Ihr Partner für ICT-Transformationen.

operational-services.de/transition-transformation

Starten Sie mit uns sichere Data-Center- und Cloud-Szenarien

DIGITALE TRANSFORMATION MIT SAP S/4HANA

ZUKUNFTSSICHERHEIT DURCH END-TO-END-PROZESSE

In Zeiten digitalisierter Prozesse, Predictive Analytics und unbegrenzter Mobilität müssen die Systeme von Unternehmen immer größere Datenmengen bewältigen. Die Anforderungen an die Geschäftsprozesse steigen dadurch zunehmend. Doch was nützen unzählige Daten, wenn Ihr System diese nur schleppend analysieren und auswerten kann? Als Antwort darauf hat SAP die neue Business-Suite S/4HANA mit der zugehörigen Datenbank SAP HANA entwickelt und zugleich angekündigt, dass bis 2027 der technische Support für alle älteren Versionen eingestellt werden soll. Theoretisch führt daher kein Weg mehr am Wechsel auf S/4HANA vorbei.

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

WHITEPAPER DOWNLOAD

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

STAMMDATENMANAGEMENT

STRATEGISCHE UNTERNEHMENSFÜHRUNG

Steigende Beschwerde- oder Retourenquoten, höhere Absprungraten, eine sinkende Conversion Rate – bei diesen Vorkommnissen schrillen die Alarmglocken. Unternehmen fragen sich, was schiefläuft und suchen nach den Ursachen. Oft stellen sie fest, dass qualitativ schlechte Stammdaten der Auslöser sind. Damit sind nicht nur die von Produkten gemeint, sondern ebenso die der Kunden. Werden diese Daten nicht gepflegt beziehungsweise innerhalb eines Master-Data-Management-Systems organisiert, hat das negative Folgen, die in vielen Fällen nicht rückgängig gemacht werden können. Denn Stammdaten sind ein unschätzbar wertvolles Asset. Akkurat gepflegt erleichtern sie die Automatisierung von Sales- und Marketingprozessen und sind für den Unternehmenserfolg und für weiteres Wachstum essenziell.

Dieses Whitepaper erläutert Ihnen, wie Sie mit einer hohen Stammdatenqualität die Customer Journey entlang aller Touch Points verbessern, die Herausforderungen meistern, Ihren Mitarbeitern stets valide Adressen zur Verfügung stellen und wie Sie das Stammdatenmanagement als strategisches Führungsinstrument erfolgreich umsetzen können.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 14 Seiten und steht kostenlos zum Download bereit. ***www.it-daily.net/download***

DIGITALE SOUVERÄNITÄT

MIT GEBRAUCHTSOFTWARE DIE SOUVERÄNITÄT FÖRDERN UND GLEICHZEITIG KOSTEN SPAREN

Die Corona-Krise treibt die Digitalisierung in Unternehmen weiter voran. Doch gerade jetzt müssen IT-Verantwortliche kostenbewusster denn je planen. Der Einsatz von Gebrauchtsoftware kann dabei helfen, Kosten einzusparen und zudem gefährlichen Abhängigkeitsverhältnissen zu US-Cloud-Anbietern vorzubeugen.

Die Corona-Pandemie stellt Unternehmen vor neue Herausforderungen. IT-Verantwortlichen obliegt es dabei, die schwierige Gratwanderung zwischen IT-Investitionen, die die Digitalisierung im Unternehmen fördern, einerseits und Kostendruck durch wirtschaftliche Einbußen andererseits zu meistern. Die Cloud erfreut sich daher besonderer Beliebtheit, denn sie verspricht (vermeintlich) maximale Flexibilität bei minimalen Kosten. Doch der Wechsel in die Cloud bringt erhebliche Risiken mit sich, die nicht einmal eine krisenbedingte Zwischenlösung rechtfertigen.

UNTERNEHMEN KÖNNEN VIEL GELD SPAREN, WENN SIE AKTUELLE STANDARD-SOFTWARE-VERSIONEN NICHT DIREKT BEIM HERSTELLER, SONDERN AUF DEM GEBRAUCHTMARKT GEGEN EINMALZAHLUNG ERWERBEN.

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

Die Gefahren der Cloud

Ein schneller Wechsel in die Cloud scheint auf den ersten Blick ein Retter in der Pandemie zu sein. Doch der Markt ist stark von US-Software-Giganten dominiert. Vergleichbare europäische Lösungen, die hier Schritt halten können, gibt es kaum. Damit fällt die Wahl oftmals auf die Cloud-Angebote der US-Hersteller, wodurch trotz erheblicher Datenschutzbedenken infolge des Wegfalls des EU-US PrivacyShield der typische Lock-In Effekt aufgrund der beim jeweiligen Anbieter liegenden Kundendaten zum Tragen kommt. Aus Mangel an Alternativen muss der Kunde dann unter Umständen sämtliche Vorgaben und Änderungen wie Preiserhöhungen des Anbieters hinnehmen.

Dies zeigt sich exemplarisch in der Änderung der Microsoft-Lizenzbestimmungen „fromSA" im vergangenen Jahr. Die Regelung untersagt Kunden fortan, während der Nutzung einer bestimmten rabattierten Cloud-Version, ihre nicht mehr benötigten Kauf-Softwarelizenzen weiter zu veräußern. Dies widerspricht nicht nur den Grundsätzen des Europäischen Gerichtshof, sondern gibt auch einen Vorgeschmack darauf, was in der Cloud droht: Der Kunde und damit ganz Europa setzen sich der Willkür und den Interessen der Hersteller aus, ohne jedwede Handlungsalternative und unter Aufgabe ihrer digitalen Souveränität – auch auf Datenebene. Gebrauchtsoftware kann hier mögliche Risiken zumindest abmildern, breitere Handlungsspielräume wahren und zusätzliche Bedenkzeit ermöglichen.

IT-Etat aufbessern

Darüber hinaus lassen sich mit Gebrauchtsoftware Kosten reduzieren und das knappe IT-Budget aufpolstern. Das – oftmals kurzfristig gedachte – Kostenargument der Cloud-Software kommt hier also in geringeren Maßen zum Tragen. Bis zu 50 Prozent können Unternehmen einsparen, wenn sie aktuelle Standard-Software-Versionen nicht direkt beim Hersteller, sondern auf dem Gebrauchtmarkt gegen Einmalzahlung erwerben. Noch größere Einsparungen sind bei Vorgängerversionen möglich. Zudem sollten Verantwortliche überprüfen, welche Software-Lizenzen im eigenen Unternehmen nicht mehr gebraucht werden – etwa durch Restrukturierungen, Unternehmenszukäufe oder die Migration in die Cloud. Denn überschüssige On-Premises-Lizenzen lassen sich oftmals gewinnbringend weiterverkaufen.

In beiden Fällen, ob bei An- oder Verkauf von Gebrauchtsoftware, ist es empfehlenswert, sich an einen erfahrenen Händler zu wenden, der sich mit den komplexen Lizenzbestimmungen der Hersteller auskennt. Durch das Wissen der Experten können sich Kunden zu jeder Zeit sicher sein, dass Transaktionen rechtssicher abgewickelt werden.

Andreas E. Thyen

PREDICTIVE MAINTENANCE

BESSERE ENTSCHEIDUNGEN UND NEUE GESCHÄFTSMODELLE

Die Erfahrung zeigt, dass Unternehmen gut beraten sind, auf vertraute Technologien zu setzen. Einzelne Prozessschritte sollten nicht nur digitalisiert werden um der Digitalisierung Willen, sondern vielmehr, um die Werte aus den Daten zu entschlüsseln. Sein sollten nicht nur zu smarten Daten gemacht werden, sondern auch zu wertvollen, denn nur so glänzt das Gold des 21. Jahrhunderts auch und steigt im Wert. Bleiben Sie offen und lassen Sie sich nicht einschränken! Das sollte sich zum einen auf Ihr persönliches Mindset beziehen, zum anderen aber auch auf die Lock-in-Falle oder wenn es um das Thema Standards geht. Seien Sie offen dafür, die bestmögliche Lösungen für Ihr Unternehmen zu finden und zu integrieren.

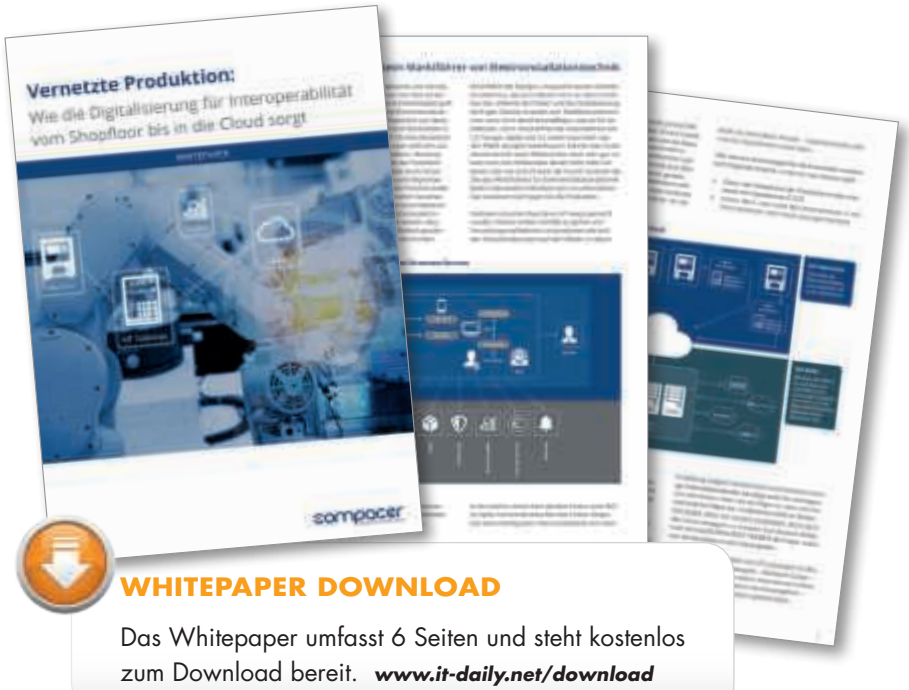
Wenn Digitalisierungsprojekte scheitern dann liegt es nur selten an der Technologie. Was aber sind die Ursachen und wie lassen sie sich beheben? Mit den möglichen Gründen für das Scheitern beschäftigt sich dieses Whitepaper. Es zeigt Ihnen aber auch diverse Möglichkeiten und Lösungen auf, mit denen sich IoT-Projekte erfolgreich umsetzen lassen.

WHITEPAPER DOWNLOAD

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

VERNETZTE PRODUKTION

WIE DIE DIGITALISIERUNG FÜR INTEROPERABILITÄT SORGT



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 6 Seiten und steht kostenlos zum Download bereit. ***www.it-daily.net/download***

Die vergangenen Jahre haben uns aufgezeigt, dass eine maßvolle digitale Transformation keine Schönwetterstrategie ist, sondern vielmehr auf eine langfristige Ausrichtung abzielt. So müssen Unternehmen heute beispielsweise auf neue Anbieter, Kunden, Lieferanten, Ersatzprodukte, aber auch auf neue Regularien beziehungsweise Gesetzgebungen reagieren – schlimmstenfalls sogar auf einen pandemiebedingten Lockdown. Meistens verbergen sich dahinter Chancen, auch wenn sie mir Herausforderungen verbunden sind. Das alles führt zu einem Wandel, der nicht zwangsläufig das gesamte Unternehmen umkrempeln muss, sondern vielmehr einzelne Change Management Maßnahmen mit sich bringt. Diese finden meistens in den drei großen Bereichen Fertigung, Produkte und Vertrieb statt.

ROLLE RÜCKWÄRTS

MICROSOFT RUDERT BEI LIZENZBESTIMMUNGEN „FROM SA“ ZURÜCK

Im Mai 2020 verkündete Microsoft eine Änderung in den AGBs für sogenannte “from SA”-Lizenzen. Seither sind Unternehmen verunsichert, ob sie ihre einst käuflich erworbenen Microsoft-Lizenzen beim Gang in die Cloud wieder veräußern können oder nicht. Zum 1. Juni 2021 dann die große Überraschung: Microsoft ruderte zurück. Ohne große Ankündigung freilich, doch mit großer Wirkung für seine Kunden – und für die Käufer gebrauchter Software.

‚Für Kunden, die sich für den Erwerb von ‚From SA‘-Lizenzen entscheiden, haben wir die Anforderung aufgehoben, dass der Kunde die entsprechenden Qualifizierenden Lizenzen während des gesamten Abonnementzeitraums der ‚From SA‘-Lizenz behält.‘ So lautet seit 1. Juni 2021 der entscheidende Absatz in den Lizenzbestimmungen von Microsoft. Klingt unspektakulär. Tatsächlich bedeutet dies jedoch eine große Erleichterung für alle Beteiligten. Denn Unternehmen können die Migration in die Microsoft Cloud nun wieder gegenfinanzieren – mit einem von Microsoft gewährten Rabatt für ‚From SA‘-Kunden und mit dem Verkauf der nicht mehr benötigten Altlizenzen an Softwarehändler wie die VENDOSOFT GmbH.

Was das konkret bedeutet und dass sich der Verkauf gebrauchter Software wirklich lohnt, zeigt ein Kundenbeispiel: Die Stuttgarter Unternehmensgruppe Glöckle migrierte 2019 in die Microsoft Cloud und veräußerte in diesem Zuge ihre gebrauchten Microsoft Server aus SA-Verträgen, Zugriffslizenzen sowie Office-2019-Pakete. VENDOSOFT nahm die etwa 250 Lizenzen für rund 100.000 Euro in Zahlung. Der Glöckle Gruppe ermöglichte das so freigesetzte Kapital eine nahezu kostenneutrale Umsetzung ihres Cloud-Projekts.

Die Pflicht, überschüssige Lizenzen zu verkaufen

Aus Gründen wie diesen sieht es Rechtsanwalt Dr. Daniel Taraz geradezu als „Pflicht“ eines jeden IT-Verantwortlichen, unnütz gewordene Software zu veräußern und in liquide Mittel zu wandeln. Der Jurist von der renommierten Kanzlei JENTZSCH IT ist u.a. auf die komplexen Lizenzbestimmungen von Microsoft spezialisiert und berät Unternehmen in Belangen des IT- und Lizenzrechts. „Von leitenden Mitarbeitern wird betriebswirtschaftliches Denken erwartet“, so Taraz. Dazu zählt seiner Ansicht nach auch die Kenntnis, welch hohe Vermögenswerte in Softwarelizenzen gebunden sind. „Werden sie nicht mehr benötigt, beispielsweise, weil ein Unternehmen in die Cloud migriert, sollten diese Werte im Sinne des Unternehmens nicht einfach brach liegen.“

ES IST FAST DIE PFLICHT EINES JEDEN IT-VERANTWORTLICHEN, UNNÜTZ GEWORDENE SOFTWARE ZU VERÄUSSERN UND IN LIQUIDE MITTEL ZU WANDELN.

Dr. Daniel Taraz, Rechtsanwalt, www.jentzsch-it.de

Auch im Sinne der Nachhaltigkeit besteht eine Verantwortung, überschüssige IT Assets dem Zweitmarkt zuzuführen. So sieht es VENDOSOFT-Geschäftsführer Björn Orth. Seit 2014 kauft der Reseller und Microsoft Gold Partner gebrauchte Microsoft-Lizenzen aus gewerblicher Nutzung auf und stellt sie Behörden und Unternehmen als Gebrauchtsoftware zur Verfügung. Von diesem Kreislauf profitieren alle – Erstbesitzer wie die Glöckle Gruppe, die ihre IT-Budgets aufstocken, genauso wie die Zweiterwerber. Die sparen nicht nur eine Menge Geld, sondern können auf dem Gebrauchtsoftware-Markt Lizenzen erwerben, die es neu gar nicht mehr gibt.

Rechtsanwalt Dr. Taraz und VENDOSOFT-Geschäftsführer Orth bewerten es denn auch positiv, dass Microsoft dem nun keinen Riegel mehr vorschiebt. Damit endet die einjährige Verunsicherung unter Microsoft-Kunden, ihre Kauf-Lizenzen aus SA-Verträgen zu rekapitalisieren.

Über den lohnenswerten Verkauf gebrauchter Software bietet VENDOSOFT eine kostenlose Beratung durch Microsoft Licensing Professionals an. Wer wie die mittelständische Glöckle Gruppe brach liegende Lizenzen monetarisieren will, findet hier Auskunft: **www.vendosoft.de/gebrauchte-software-verkaufen.**

Angelika Mühleck

NEW WORK

DIE CHANCE FÜR DEN MITTELSTAND

New Work und Mittelstand klingt beim ersten Hören nach Kontrast: Auf der einen Seite urbane Coworking Orte und auf der anderen Seite das traditionelle Büro mit festen Präsenzzeiten. New Work war bisher nicht das klassische Mittelstandsthema. Es wird eher bei Startups verortet oder in großen Konzernen mit umfangreichen HR-Strategien.

Auch wenn einigen Mittelständlern mit diesen Vorurteilen sicherlich Unrecht getan wird, war die Corona-Pandemie des letzten Jahres doch für einen großen Teil der mittelständischen Unternehmen der Anstoß, sich über das Thema Homeoffice dem Trend New Work zu nähern. Eng verwoben ist damit zudem die Digitalisierung, welche die Voraussetzung für eine erfolgreiche Umsetzung des Homeoffice darstellt. Neben Zweifeln über die Produktivität von MitarbeiterInnen zuhause, stellten Defizite in der Digitalisierung häufig die zweite große Hürde vor Veränderungen der Arbeit in Richtung New Work dar.

Glücksfall für den Mittelstand

Der Zwang zum Homeoffice, der für die meisten Unternehmen mit der Pandemie einher ging, stellt sich in dieser Hinsicht als Glücksfall heraus. Einerseits war der bei der Digitalisierung bisher zögerliche Mittelstand nun gezwungen, Bedenken oder Trägheit auszuräumen und digitale Defizite aktiv zu beseitigen. Für viele war das beispielsweise der Zeitpunkt, nun wirklich den Wechsel in die Cloud zu vollziehen, den man vorher vielleicht gemieden hatte. Digitale Infrastruktur wurde erneuert oder erstmalig aufgebaut und auch die digitalen Kompetenzen der MitarbeiterInnen rückten nun vielerorts erstmals in den Fokus. Zumindest eine Grundkenntnis über digitale Anwendungen zu haben, ist nun für die meisten MitarbeiterInnen Pflicht. Vor allem für ältere ArbeitnehmerInnen öffnete sich noch einmal die Tür zur digitalen Welt und damit zu einer Entwicklung, die sie bisher verpasst hatten und für ihre Arbeit nicht zwangsläufig brauchten – es ihnen nun aber erlaubt, beruflich wie privat wieder Anschluss zu finden.

Nach diesen ersten Schritten in Bezug auf Digitalisierung und New Work ist es nun aber wichtig, dass jetzt nicht nur ein Minimum digitalisiert wird, sondern ein Ruck durch die Unternehmen geht, hin zu einer echten digitalen Transformation. Mit digitalen Mitteln sollten nicht alte Arbeitsweisen nachgebildet werden, sondern die Möglichkeiten neuer Zusammenarbeit und Produktivität genutzt werden.

Eine Frage der Balance

Auch wenn die Corona-Zahlen jetzt zurück gehen und so mancher schon wieder von einem Zurück zur alten Normalität träumt, wird uns doch einiges aus der Pandemie-Zeit erhalten bleiben. In Bezug auf Homeoffice haben misstrauische CheflInnen gelernt, dass es ja doch „geht", dass zuhause produktiv gearbeitet werden kann. Auf der anderen Seite haben die ArbeitnehmerInnen gemerkt, wie wertvoll auch die Zeit im Büro ist, dass man sich den direkten und menschlichen Austausch, der für die Arbeit so wichtig ist, nicht einfach sparen kann.

Den Post-Pandemie Umgang mit dem Thema New Work muss nun wohl jedes Unternehmen für sich finden. Für die meisten ist es eine Balance-Frage zwischen pu-

rem Homeoffice aus dem Lockdown des letzten Jahres und einer Arbeit mit Präsenzfokus, wie wir sie von der Zeit davor kannten. Je nach Branche, Tätigkeit und Unternehmenskultur wird die Antwort darauf und die Umsetzung von New Work in der Zukunft unterschiedlich ausfallen.

> NEW WORK BEDEUTET AUCH EINEN GROSSEN WANDEL WEG VON PRÄSENZKONTROLLE HIN ZU ERGEBNISBEWERTUNGEN UND ZIELVEREINBARUNGEN.
>
> Lisa Ehrentraut,
> Teamleiterin Operations, Bundesverband IT-Mittelstand e.V. (BITMi),
> www.bitmi.de

Dabei ist es wichtig, New Work über das Thema Homeoffice hinaus zu denken. Wie so oft bei Trendwörtern wird selten darüber gesprochen, was damit genau gemeint ist. So wird New Work aktuell häufig einfach gleichgesetzt mit Homeoffice. Das liegt nah, ist es doch gerade die spürbarste Veränderung unserer Arbeitswelt. Dabei ist New Work viel mehr als Homeoffice und seine Schwerpunkte Kollaboration und Ortsungebundenheit. Ein ganz zentraler Punkt, der anfangs vielleicht eher unterschwellig mitschwingt, ist eine Veränderung in der Bewertung von Arbeit. Denn wenn ArbeitnehmerInnen nicht mehr durch ihre bloße Anwesenheit im Büro signalisieren können, dass sie arbeiten, was vor Ort von den Vorgesetzten überprüft werden kann, muss Arbeit langfristig anders gemessen und bewertet werden. Eine Übertragung dieser traditionellen Bewertung von Präsenzarbeit ins Homeoffice ist nur durch drastische digitale Überwachung möglich, was in den meisten Fällen weder von Arbeitgebern noch von Arbeitnehmern als erstrebenswert angesehen wird.

Anstoß zur Modernisierung

Stattdessen bedeutet New Work auch einen großen Wandel weg von Präsenzkontrolle hin zu Ergebnisbewertungen und Zielvereinbarungen. Dieser Wandel wird in manchen Fällen nicht oder erst später offen angesprochen, während ihn einige Unternehmen in der Umsetzung von New Work Elementen im eigenen Unternehmen ganz offensiv angehen. Und auch ohne Homeoffice oder Pandemie haben viele Unternehmen diese Veränderung in der Wahrnehmung von Arbeit für sich schon vollzogen. So betont Frank Lehmann, Geschäftsführer von das-handwerk.net, der als IT-Mittelständler selbst diesen Wandel schon vollzogen hat und nun seine Kunden dabei unterstützt: „Anwesenheit an einem bestimmten Ort wird nicht mehr entscheidend sein. Freies, selbstbestimmtes Arbeiten ist die Zukunft. Kontrolle im weiteren Sinne erfolgt dann über Zielvereinbarungen."

New Work ist damit nicht nur ein Wechsel des Arbeitsorts, sondern stellt meist auch einen Wandel der Arbeits- und Unternehmenskultur dar. Für den Mittelstand bringt dieser Trend damit gleich den Anstoß für zwei Herausforderungen und Chancen mit sich: tiefgreifend zu digitalisieren und die eigene Arbeitskultur zu modernisieren.

Lisa Ehrentraut

MIT NEW WORK GEGEN DEN FACHKRÄFTEMANGEL

Ein Dauerbrenner für den Mittelstand ist das Thema Fachkräftemangel. Vor allem im Bereich IT hat die Corona-Pandemie die Situation eher verschlechtert. IT-Unternehmen selbst suchen immer noch händeringend nach Personal, während auch alle anderen Branchen nun noch dringender Unterstützung bei der Digitalisierung brauchen und dafür eigene Stellen besetzen möchten. So zeigt eine Umfrage unter BITMi Mitgliedern vom letzten Jahr, dass viele IT-Mittelständler gerade während der Pandemie viele neue Projektanfragen erhielten und eher noch mehr zu tun hatten als zuvor. Dank des umfangreichen Lockdown-Homeoffice ist kollaboratives Arbeiten nun alltäglich geworden. Vor allem der Mittelstand, der vom Fachkräftemangel stärker betroffen ist als die großen Unternehmen und der bisher oftmals noch nicht die richtige IT-Infrastruktur besaß, um MitarbeiterInnen im großen Stil im Homeoffice arbeiten zu lassen, sollte die Situation jetzt nutzen, um den Fachkräftemangel aktiv anzugehen. Gerade für Unternehmen mit Standorten, die auf ArbeitnehmerInnen wenig attraktiv wirken, eröffnet sich hier die Chance, MitarbeiterInnen zu gewinnen, die planmäßig größtenteils im Homeoffice arbeiten. Das Modell ist nun erprobt, Bedenken sind ausgeräumt – einer erfolgreichen Rekrutierung von neuem Personal steht damit nichts mehr im Wege.

bitmi
Bundesverband
IT-Mittelstand e.V.

FOREVER REMOTE?

FLEXIBEL UND EIGENVERANTWORTLICH ARBEITEN

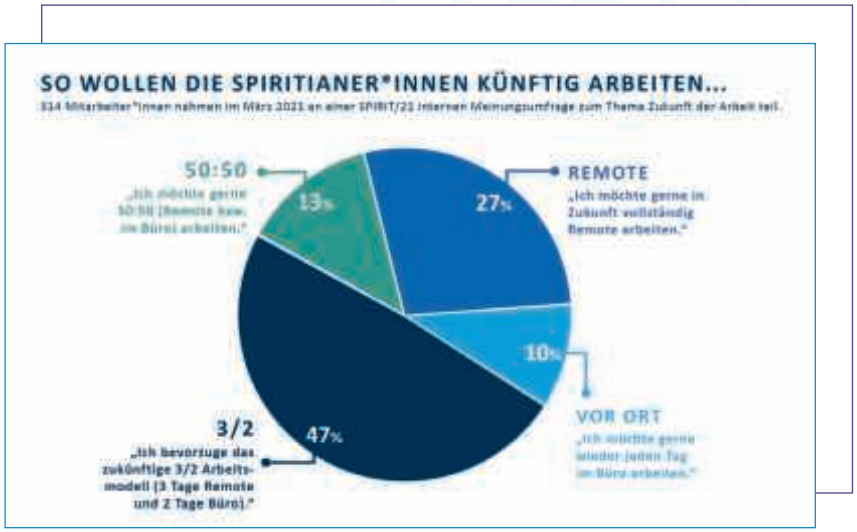
Mobiles Arbeiten ist in den vergangenen 15 Monaten zur neuen Normalität geworden. Aber bleibt dieser Trend auch nach der Pandemie?

Bis vor gut einem Jahr pendelten die meisten ArbeitnehmerInnen in Deutschland täglich ins Büro. Nur eine kleine Minderheit wählte sich remote – also per Fernzugriff – ein. Dann kam Corona und mobiles Arbeiten wurde zum neuen Standard. Auch SPIRIT/21 schickte im Frühjahr 2020 nach einer kurzen Testphase die gesamte Belegschaft – knapp 500 Mitarbeiterinnen und Mitarbeiter - nach Hause, lange bevor die Bundesregierung die Homeoffice-Pflicht einführte.

Technisch war die Umsetzung recht einfach, denn mobile Arbeitsgeräte wie Firmen-Laptops, Mobiltelefone und Collaboration Tools gehören seit Jahren zur Standardausstattung. Dass die technische Infrastruktur allein jedoch nicht ausreichen würde, um in Remote-Teams erfolgreich zusammenzuarbeiten, war der Geschäftsleitung des Böblinger IT-Dienstleisters schnell klar. Ihr kam es vielmehr darauf an, die Mitarbeitenden durch eine völlig neue Art und Intensität der Kommunikation aktiv in den Veränderungsprozess mit einzubeziehen und die verringerten sozialen Kontakte im Unternehmen über eine Reihe virtueller After Work Events zu intensivieren. So wurde erreicht, dass der Lockdown weder Arbeitsmotivation noch Ergebnisse beeinträchtigte, sondern im Gegenteil: Die Effizienz stieg sogar vielfach an.

Aktive Einbindung aller Beteiligten ist das A und O

Auf Basis dieser Erfahrungen machte sich SPIRIT/21 bereits Mitte letzten Jahres Gedanken, wie die Erkenntnisse aus der Pandemiezeit in das künftige Arbeitsmodell integriert werden könnten. Herausgekommen ist ein Konzept, das ein „Sharing" der Büroarbeitsplätze vorsieht und auch nach Corona die Möglichkeit bietet, regelmäßig remote zu arbeiten. „Uns war dabei besonders wichtig, die Flexibilität und Eigenverantwortung zu stärken und Vereinsamungseffekten entgegenzuwirken", erläutert Unternehmenschef Markus Sieber. „Innerhalb unseres hybriden 3/2-Modells kann jeder an drei Tagen pro Woche selbst entscheiden wann, wo und wie sie oder er arbeiten will, und an den beiden Büro-Tagen die Kontakte in der Firma persönlich pflegen."



Flexibel arbeiten – auch nach der Pandemie

Ob und in welchem Ausmaß Remote-Work auch nach der Pandemie funktionieren wird, hängt von verschiedenen Faktoren ab: von der Branche, der Arbeitskultur, der technischen Infrastruktur und der Fähigkeit des Unternehmens, ein attraktives Arbeitsumfeld zu schaffen, das über passende Change Management-Prozesse nicht nur die Mitarbeitenden, sondern auch deren privates Umfeld zuverlässig einbezieht. Die Auswirkungen auf Produktivität, Kosten, Sozialkontakte, Arbeitssicherheit oder die Gestaltung von Büroflächen werden die Suche nach dem perfekten Mix zwischen mobilem Arbeiten und der Anwesenheit im Büro zusätzlich beeinflussen. Wie digitale Veränderungsprojekte unter Berücksichtigung dieser und ähnlicher Faktoren professionell zu realisieren sind, hat SPIRIT/21 bereits in vielen verschiedenen Projekten gezeigt.

www.spirit21.com

RAUS AUS DEM NEBEL – REIN IN DIE CLOUD

WIE LEGACY-TRANSFORMATION WIRKLICH GELINGT!

Viele Unternehmen haben sich bei Legacy-Systemen für eine Cloud First Strategie entschieden. Auf diesen Bestandssystemen laufen geschäftskritische Prozesse. Sie funktionieren seit Jahrzehnten und verarbeiten unglaubliche Mengen an Transaktionen zuverlässig und performant.

Doch die Transformation dieser Systeme bei gleichzeitig hohen Businessanforderungen an Stabilität, Business Continuity & Performance gleicht der Quadratur des Kreises: Denn es fehlt in der Regel das Wissen um die Struktur und Details in den Bestandssystemen, um eine realisierbare Transformationsstrategie festzulegen und konsequent umzusetzen.

Das Gemeine an dieser Situation ist, dass sie sich täglich durch die Verrentung bisheriger Knowhowträger verschlimmert. Dem Unternehmen droht der Stillstand, daher ist nichts tun heute keine Option mehr.

Die drängenden Fragen der IT-Entscheider sind offensichtlich:

- Wie erhalte ich Transparenz und Kontrolle über die Ist-Situation?
- Welche Transformationsstrategie soll ich am besten einschlagen?
- Woher bekomme ich valide Entscheidungsgrundlagen?

Die Transformation von Legacy-Systemen stellt einen grundlegenden Change in der Herzkammer des Unternehmens dar. Neben fachlichen, technischen und betrieblichen Gesichtspunkten sind Aspekte des Risiko-, des Finanz- und des Change Managements zu berücksichtigen.

Vor Beginn der Transformation ist die sorgfältige Bestimmung der Ausgangssituation unerlässlich. Ein zielgerichtetes 360°-Assessment deckt alle relevanten Aspekte ab (siehe Bild).

360° Transformation

PKS hat seit über 30 Jahren sehr große Erfahrung in der Analyse und Transformation von IBM-basierten Legacy-Systemen. Außerdem verfügt PKS über ein stabiles Partnernetzwerk.

eXplain – der Schlüssel zum Erfolg

Zur Herstellung von Transparenz sowohl im Assessment als auch bei der Transformation setzt PKS auf das Analysetool eXplain. Mit eXplain werden nicht nur technische Codestrukturen der Applikationen transparent, sondern diese mit den fachlichen Domänen und Subdomänen in Beziehung gesetzt. Erst durch dieses Beziehungswissen entsteht die notwendige Transparenz für den anstehenden Transformationsprozess.

Die Vorteile liegen auf der Hand:

- kurzfristige Einsparpotenziale von bis zu 50 Prozent durch Hebung von Quick-Wins und Eliminierung technischer Schulden
- Sicherheit im Transformationsprozess und im Betrieb durch Nutzung von eXplain
- Entlastung der Inhouse-Ressourcen durch erfahrenen Partner
- Steigerung der Innovationskraft des Unternehmens: Moderne Technologien und agile Arbeitsweisen sichern die Attraktivität des Unternehmens für junge Mitarbeiter sowie Kunden

www.pks.de

PKS
people knowing software.

ENTERPRISE SERVICE MANAGEMENT

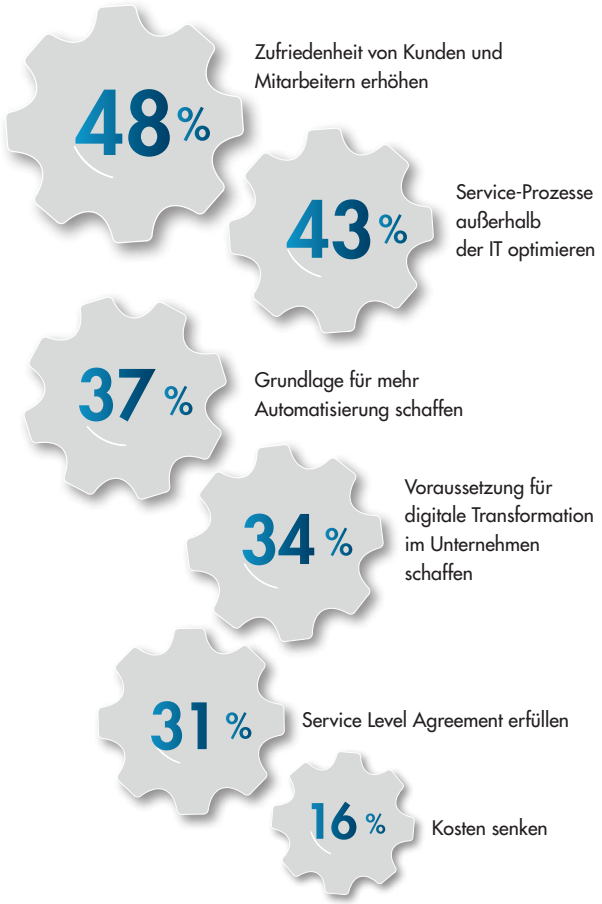
ES IST NOCH LUFT NACH OBEN

IT-Service-Management-Tools gehören zum Hygienearsenal einer funktionierenden IT-Administration. Unternehmen haben in den letzten Monaten massiv in ITSM-Lösungen investiert. Und auch die Übertragung von Service-Management-Prozessen auf Nicht-IT-Betriebe – kurz Enterprise Service Management (ESM) – steht auf der Wunschliste vieler Unternehmensleiter. Doch so richtig flügge ist ESM noch nicht. Das ist das Ergebnis der Studie „IT Service Management 2021".

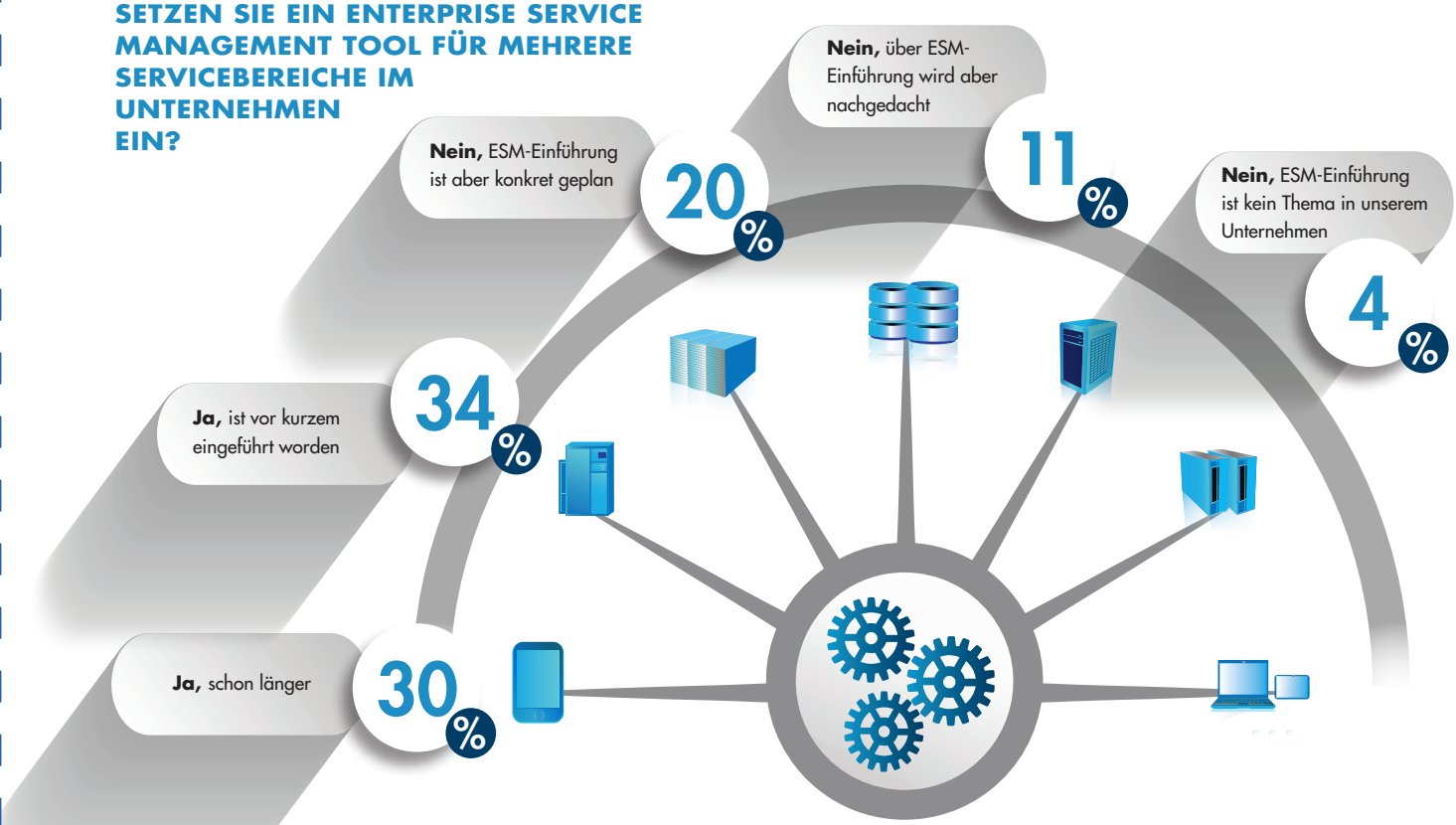
48 Prozent der Unternehmen wollen durch die Implementierung einer ESM-Lösung die Zufriedenheit von Kunden und Mitarbeitern erhöhen. Dementsprechend steigt die Nutzung von ESM-Software kontinuierlich: Bereits 64 Prozent der befragten Unternehmen haben ein solches Tool eingeführt – ein Anstieg um sechs Prozentpunkte im Vergleich zum Vorjahr. Allerdings ist noch Luft nach oben, denn es fehlt an der nötigen Umsetzung.

www.ivanti.de

WAS SIND DIE HAUPTSÄCHLICHEN ZIELSETZUNGEN IHRES UNTERNEHMENS FÜR DIE EINFÜHRUNG IHRER AKTUELLEN ESM-TOOLS?



SETZEN SIE EIN ENTERPRISE SERVICE MANAGEMENT TOOL FÜR MEHRERE SERVICEBEREICHE IM UNTERNEHMEN EIN?



DER ZUKUNFT VORAUS

DIE ARBEITSWELT VON MORGEN SCHON HEUTE IM BLICK

Die Corona-Krise erweist sich als ein Trendbeschleuniger für New Work. Noch zeigt sich der damit voraussichtlich verbundene Umbruch vor allem in der gestiegenen Anzahl an Menschen, die in den eigenen vier Wänden arbeiten. Nicht nur das Homeoffice wird sich auf Dauer etablieren, vielmehr flexibilisiert sich die gesamte Arbeitswelt – zeitlich und räumlich. Gefragt sind daher technologische Lösungen, die das kreative Miteinander vor Ort, die Zusammenarbeit über Grenzen hinweg und einen produktiven Workflow im Homeoffice unterstützen.

Co-Creation und Co-Working

Einzelbüros scheinen von gestern, ein Büro der Zukunft soll Treffpunkt und Begegnungsstätte, Kreativraum und Ideenschmiede sein. Die Mitarbeitenden finden dafür perfekte räumliche Gegebenheiten vor: Open Spaces, Rückzugsräume sowie repräsentative Besprechungsräume.

Doch das allein reicht nicht. Wichtig ist auch die technische Ausstattung. So bieten interaktive Flipcharts wie das Flip 2 von Samsung kreative Spielräume für den Austausch von Knowhow, das gemeinsame Brainstorming und den Feinschliff von Konzepten. Notizen können dafür in unterschiedlichen Farben und Stilen auf verschiedenen Hintergründen verfasst werden. Daneben lassen sich Bilder zuschneiden und bearbeiten sowie Inhalte auf dem Display spiegeln. Die Ergebnisse können nach der Besprechung bequem per Mail geteilt werden.

Kollaboratives Arbeiten

Hybride Office-Szenarien, bei denen ein Teil der Belegschaft zu Hause, der andere im Büro sitzt, könnten zukünftig breite Resonanz finden. Auch Dienstreisen lassen sich oft durch Videokonferenzen ersetzen. Für beide Szenarien braucht es stabile Bild- und Tonübertragungen. Samsung hat dafür gemeinsam mit Cisco eine Lösung für die reibungslose Integration von Videokonferenzsystemen in Besprechungsräumen über Smart Signage Geräte entwickelt. Mit Webex on Flip wurde ein Tool geschaffen, mit dem das ortsunabhängige, kollaborative Arbeiten mit dem Flip 2 einfach gelingt: Unabhängig davon, wo sich die einzelnen Teammitglieder befinden, können sie auf die Oberfläche des smarten Displays zugreifen, Beiträge verfassen und Inhalte teilen.

Um Remote Work in hoher Bild- und Ton-Qualität zu ermöglichen, arbeitet Samsung außerdem mit Logitech zusammen. Moderne Display-Technologien treffen hierbei auf ausgefeilte Kamera- und Tonsysteme – egal ob für das Homeoffice, den kleinen Besprechungsraum oder den Konferenzsaal in der Vorstandsetage.

Homeoffice – gekommen, um zu bleiben

Viele haben in den vergangenen Monaten die Vorteile des Homeoffice schätzen gelernt, weswegen auch in Zukunft manche Teammitglieder den heimischen Arbeitsplatz dem Büro vorziehen werden. Für derartige langfristige Lösungen müssen häufig erst noch die Grundlagen geschaffen werden. So klagt mehr als jeder Dritte laut einer Dekra-Erhebung über gesundheitliche Probleme aufgrund eines schlecht ausgestatteten Arbeitsplatzes zu Hause. Ein Grund: Viele sitzen mit krummen Rücken vor einem kleinen Laptop. Für ein flexibles Arbeiten hat Samsung jüngst ein neues Business-Monitor-Lineup auf den Markt gebracht. Die zehn Modelle der S- und SU-Reihe lassen sich flexibel an den Arbeitsplatz und die Körpergröße anpassen. Sie besitzen darüber hinaus vom TÜV Rheinland branchenweit erstmalig mit dem „Intelligent Eye Care"-Zertifikat ausgezeichnete Features.

Fakt ist: Vieles deutet darauf hin, dass wir in Zukunft ein flexibleres Verständnis von Arbeit haben werden. Unternehmen können mit technologischer Unterstützung schon jetzt Umgebungen schaffen, die Produktivität und Zufriedenheit im Team fördern.

Michael Vorberger

UNTERNEHMEN KÖNNEN MIT TECHNOLOGISCHER UNTERSTÜTZUNG SCHON JETZT UMGEBUNGEN SCHAFFEN, DIE PRODUKTIVITÄT UND ZUFRIEDENHEIT IM TEAM FÖRDERN.

Michael Vorberger, Head of B2B & B2C Sales, Professional Display Solutions & Consumer Displays, Samsung Electronics GmbH, www.samsung.de

ERFOLGREICHES UP- UND

IN NEUN SCHRITTEN BESTENS AUF NEW WORK VORBEREITET

> UP- UND RESKILLING BESCHREIBEN DEN PROZESS DES KONTINUIERLICHEN ERLERNENS NEUER FÄHIGKEITEN, DER MENSCHEN EFFEKTIV FÜR NEUE UND AUFSTREBENDE BERUFLICHE ROLLEN WEITERENTWICKELT.
>
> Elton Schwerzel, Managing Director DACH, Talentsoft, www.talentsoft.de

Die Veränderungen in der Arbeitswelt stellen Unternehmen vor große Herausforderungen – beginnend mit dem Ausbruch der Corona-Pandemie im vergangenen Jahr, dem damit einhergehenden virtuellen Arbeiten, neuen Arten der Teamführung oder der zunehmenden Automatisierung. Um also heute schon erfolgreich und den eigenen Wettbewerbern einen entscheidenden Schritt voraus zu sein, benötigen Unternehmen Mitarbeiter mit den richtigen Fähigkeiten.

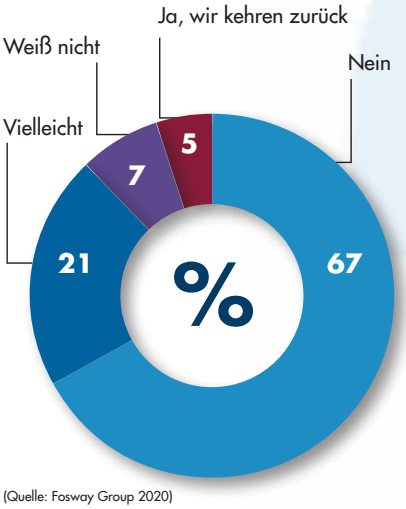
Dabei sind die Qualifizierung und Umschulung der Belegschaft unerlässlich. Denn so werden nicht nur Soft Skills und Fähigkeiten für technologische Aufgaben entwickelt, sondern auch gleichzeitig die Zufriedenheit der Mitarbeiter und die Unternehmens-Performance gesteigert. Damit dieses Vorhaben von Erfolg gekrönt ist, kommt es auf ein gezieltes Up- und Reskilling an.

Was bedeuten Upskilling und Reskilling?

Up- und Reskilling beschreiben den Prozess des kontinuierlichen Erlernens neuer Fähigkeiten, der Menschen effektiv für neue und aufstrebende berufliche Rollen weiterentwickelt. Diese Kultur des kontinuierlichen Lernens ist aktuell wichtiger denn je: So ergab eine neue Studie des McKinsey Global Institute (MGI), dass sich rund 6,5 Millionen Erwerbstätige in Deutschland bis 2030 erhebliche neue Fähigkeiten und Qualifikationen aneignen oder eine Umschulung machen müssen. Weitere vier Millionen Menschen müssen sich sogar mit einem Berufswechsel anfreunden. Insgesamt sind in den kommenden zehn Jahren in Deutschland also rund 10,5 Millionen Berufstätige betroffen – 900.000 mehr als noch vor Ausbruch der Pandemie.

Eine Studie der Fosway Group zusammen mit Talentsoft macht ebenfalls die Auswirkungen der Corona-Pandemie deutlich: So gaben 99 Prozent der befragten Unternehmen an, dass COVID-19 einen enormen Einfluss genommen hat und damit auch auf den Bereich Lernen und Weiterentwicklung. 59 Prozent stufen nun die Entwicklung neuer Fähigkeiten als sehr wichtig ein, weitere 56 Prozent treiben ihre eigene Up- und Reskilling-Strategie sogar entschiedener voran.

Glauben Sie, dass ihre Trainingsstrategie, Investitionen und Ressourcen auf das Niveau von vor der Pandemie zurückkehren werden?



(Quelle: Fosway Group 2020)

Zu den entscheidenden Fähigkeiten zählen dabei unter anderem:

- Analytisches Denken und Innovation
- Aktives Lernen und Lernstrategien
- Kreativität, Originalität und Eigeninitiative
- Technologiedesign und -programmierung
- Kritisches Denken und Analysieren
- Komplexe Problemlösung
- Führung und sozialer Einfluss
- Emotionale Intelligenz

Erfolgreiches Up- und Reskilling

1. Verstehen, welche Fähigkeiten den entscheidenden Mehrwert liefern

Gerade in der Vergangenheit war es häufig ein langwieriger Prozess, die für das eigene Unternehmen notwendigen Fähigkeiten zu definieren und diese Liste vor allem aktuell zu halten. Künstliche Intelligenz und intelligente Datenverarbeitung sorgen nun dafür, dass dieser Prozess innerhalb weniger Tage oder sogar Stunden vonstattengeht. Auf diese Weise ist es auch in neuen oder herausfordernden Situationen möglich, den Überblick zu behalten, welche Fähigkeiten benötigt werden und welche Mitarbeiter über sie verfügen.

2. Silos einreißen

Wenn Unternehmen die Fähigkeiten ihrer Mitarbeiter effizient (weiter-

RESKILLING

59% hielten die Einführung digitalen Lernens in ihrer Organisation für nicht ausgereift

94% der L&D-Verantwortlichen berichten von einer Anpassung ihrer Trainingsstrategie als Antwort auf die Corona-Pandemie

entwickeln möchten, müssen sie die verschiedenen HR-Bereiche – angefangen beim Recruiting über Lernen und Weiterentwicklung bis hin zum Performance-Management ¬– als großes Ganzes betrachten. Nur so ist es möglich, den Bedarf, die Ziele und die Kompetenzen der Mitarbeiter kennenzulernen, diese gezielt dabei zu unterstützen, ihre Karriere voranzutreiben und so effektiv zur Team- und Unternehmensleistung beizutragen.

3. Mit Blick in die Zukunft handeln

Gerade mit Blick auf das digitale Zeitalter könnte man meinen, dass technologische und analytische Fähigkeiten in Zukunft entscheidend sind und gefördert werden sollten. Mindestens genauso bedeutend sind jedoch Teamfähigkeit, Teamführung, Projektmanagement sowie die Fähigkeit, sich schnell an neue Gegebenheiten anzupassen.

4. Skills konsistent über alle Personalsysteme hinweg abbilden

Auf die richtige Technologie kommt es an: Unternehmen haben hier verschiedene Optionen – wie beispielsweise eine Talent Suite, HCM-Lösungen oder spezielle Tools für das Skills-Management. Generell gilt: Die Wahl der geeigneten Lösung erfordert eine sorgfältige Analyse der bestehenden HR-Tech-Architektur, der Bedürfnisse der Zielgruppe, der Ziele und des Budgets.

5. Mitarbeiter in alle Entscheidungen miteinbeziehen

Jeder Mitarbeiter hat spezielle Talente und individuelle Fähigkeiten, die er fördern möchte oder den Wunsch, sich neuen Herausforderungen zu stellen. Unternehmen sollten daher auf jeden Einzelnen konkret eingehen und ihn bei seiner Weiterentwicklung zur Seite stehen. Die Mitarbeiter zu involvieren, ist dabei das A und O ebenso wie das gemeinsame Erstellen von Lern- und Weiterentwicklungsplänen.

6. Kontinuierliches Lernen und Weiterentwickeln mit Möglichkeiten belohnen

Belohnung und Wertschätzung sind ein wirksames Mittel, um die Motivation der Mitarbeiter zu steigern, ihre Leistungsbereitschaft zu erhöhen und die Loyalität zum Arbeitgeber zu steigern. Damit diese die gewünschte Wirkung erzielen, müssen sie zum jeweiligen Mitarbeiter passen. So empfehlen sich für den einen beispielsweise die Teilnahme an einem Projekt, durch das er seine Stärken im Rahmen von Teamarbeit einbringen kann, oder für den anderen eine Fortbildung zu einem bislang unbekannten Aufgaben- oder Wissensbereich.

7. KPI-Messung

Natürlich ist es wichtig, die Auswirkungen neuer Fähigkeiten auf das gesamte Unternehmen im Auge zu behalten und diesen Mehrwert konkret zu messen. Unternehmen sollten hier auf eine entsprechende HR-Analytics-Software setzen, die in der Lage ist, alle relevanten Daten abzubilden. Sie unterstützt Personalverantwortliche und Führungskräfte so im nächsten Schritt beim Treffen klarer Entscheidungen und Erstellen von zukunftsorientierten Entwicklungsplänen.

8. Die richtigen Technologien einsetzen

Um Up- und Reskilling zu unterstützen, bieten sich verschiedene Technologien an. So setzen laut der Studie der Fosway Group 90 Prozent der befragten Unternehmen auf Performance-Management-Lösungen, 87 Prozent auf E-Learning Tools und 21 Prozent auf Software zur Karriereplanung. Über interne Talentmarktplätze verfügen lediglich sechs Prozent der befragten Unternehmen. Hier gilt es, auszuprobieren, was am besten für das eigene Unternehmen geeignet ist.

9. Kontinuierliches Lernen und Ausprobieren

Der Prozess des kontinuierlichen Lernens und Ausprobieren ist unerlässlich, um Mitarbeiter fit für die Arbeitswelt der Zukunft zu machen und so den eigenen Unternehmenserfolg zu sichern. Für Unternehmen steht hier auch die Aufgabe im Fokus, die Ansätze für Lernen, Weiterbildung und Kompetenzentwicklung regelmäßig zu überdenken und zu optimieren.

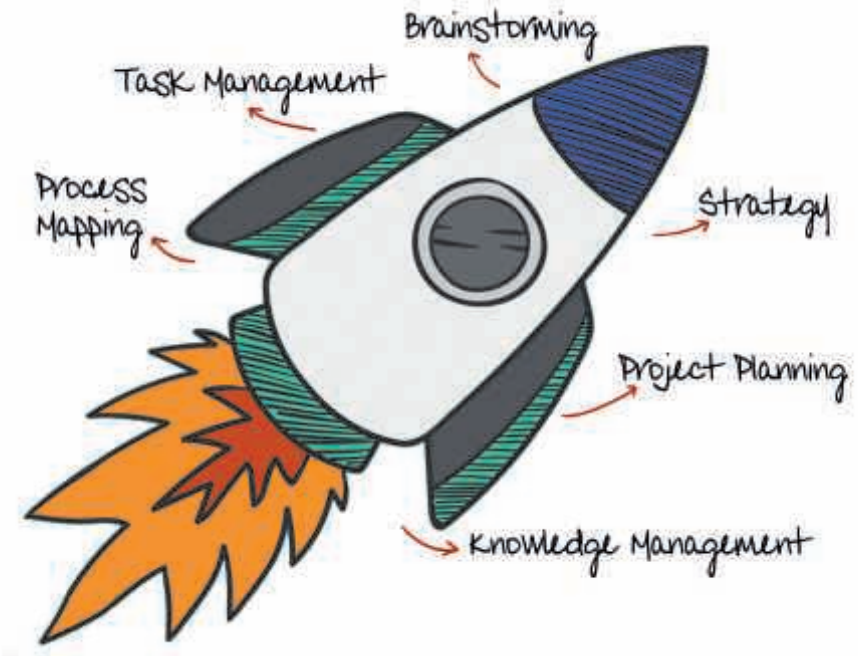
Fazit

Mitarbeiter sind das wertvollste Kapital eines Unternehmens. Indem Führungskräfte in die Fähigkeiten ihrer Belegschaft investieren, investieren sie gleichzeitig in ihr Unternehmen. Entsprechende Up- und Reskilling-Strategien und -Programme müssen dabei individuell auf die Anforderungen des jeweiligen Unternehmens zugeschnitten sein, um langfristig zum Erfolg zu führen.

Elton Schwerzel

IT´S NO ROCKET-SCIENCE

MEHR TRANSPARENZ MIT VISUELLER PROJEKTPLANUNG



Die Planungsphase eines Projekts ist elementarer Bestandteil und Erfolgsfaktor zugleich. Laut einer Untersuchung des „Harvard Business Review" überschritten IT-Projekte ihr Budget im Schnitt um 27 Prozent. Noch erschreckender: Bei mindestens einem von sechs IT-Projekten waren sogar Kostenüberschreitungen von 200 Prozent und Terminüberschreitungen von 70 Prozent zu beobachten. Allerhöchste Zeit zu fragen, was man besser machen kann.

Zur Verbesserung und Optimierung der Projektplanung gibt es unterschiedliche Strategien. Verschiedene Visualisierungs- und Diagrammtechniken, zum Beispiel Starbursting-, Ursache-Wirkungs- oder Affinitätsdiagramme und Mindmaps, um nur einige zu nennen, unterstützen die Projektplanung auf ganz neue Art und Weise. Vorteilhaft ist, dass sie helfen, den Überblick zu behalten und komplexe Probleme zu lösen. Visuelle Projektplanungstechniken tragen mit ihrer klaren und verständlichen Kommunikation dazu bei, dass Stakeholder und Teammitglieder auf demselben Stand bleiben und dabei Budget- und Ressourcenbeschränkungen eingehalten werden.

Noch vielversprechender ist die Tatsache, dass diese visuellen Methoden nicht nur die Projektplanung erleichtern, sondern auch während der Umsetzung helfen, Probleme zu lösen, Risiken zu minimieren und agile Anpassungen vornehmen zu können.

Im Mittelpunkt steht das zu lösende Problem

Ausgangssituation von Projekten ist in der Regel ein bestimmtes Problem, das es zu lösen gilt. Deshalb ist es wichtig sich von Anfang an, auf die Problemstellung zu fokussieren. Dabei können verschiedene Herangehensweisen helfen.

1. Denkhüte von De Bono

Die „Denkhüte" von Edward de Bono sind ein Modell, mit dessen Hilfe komplexe Situationen oder Herausforderungen aus unterschiedlichen Perspektiven betrachtet werden. Die Teammitglieder tragen dabei jeweils einen „Denkhut" und schlüpfen damit in verschiedene Rollen beziehungsweise Perspektiven, was unterschiedliche Blickwinkel erlaubt, welche bei der Lösungsfindung helfen.

DIE VORTEILE DER VISUELLEN PROJEKTPLANUNG

- ✚ Effektive Vorausplanung jeder Projektphase
- ✚ Unmittelbares Erkennen und Lösen komplexer Probleme
- ✚ Klare Kommunikation von Stakeholdern und dem Projektteam
- ✚ visuelle Projektpläne erleichtern die Fehlerbehebung
- ✚ übersichtliche Darstellung des Projektziels sowie der für die Zielerreichung erforderlichen Schritte

2. Starbursting

Oft lässt sich die Tendenz eines übereilten Handelns erkennen, noch bevor das Problem überhaupt verstanden wurde. Starbursting hilft, indem immer und immer wieder bis ins Detail nachgefragt wird, anstatt sofort nach Antworten zu suchen.

3. Five-Why-Methode

Die Five-Why-Methode wird zur Qualitätssteigerung eingesetzt. Hier wird ein Problem mit der Six-Sigma-Methode DMAIC (Define, Measure, Analyze, Improve, Control) gründlich untersucht. Durch Wiederholung der Frage „War-

um" wird bis zum Kern des Problems vorgedrungen.

Ein Bild sagt mehr als tausend Worte

Ist die Problemstellung präzise herausgearbeitet, kann man mit dem Brainstorming loslegen. Ziel ist es einerseits möglichst unbefangen Ideen zu sammeln, andererseits aber durchaus den Fokus nicht aus den Augen zu verlieren. Vier visuell geprägte Methoden bieten in dieser Projektphase hilfreiche Anknüpfungspunkte.

1. Reverse Brainstorming

Anstatt wie üblich einfach nach der Problemlösung zu suchen, werden beim reversen Brainstorming erst einmal mögliche Ursachen ermittelt, damit im Anschluss vorbeugende Maßnahmen abgeleitet werden können. Ein Beispiel für reverses Brainstorming ist das Ursache-Wirkungs-Diagramm. Es ist optimal geeignet, ein Problem zu erfassen und dann alle potenziellen Ursachen zu ermitteln.

2. Mindmapping

Mit Mindmaps lässt sich der Ideenfluss erfassen und strukturieren – schnell und übersichtlich. Die Mindmapping-Methode hilft, die Beziehung zwischen verschiedenen Ideen zu verstehen und sie bietet eine solide Grundlage für eine tiefergehende Analyse.

3. Affinitätsdiagramme

Brainstorming generiert oft unermesslich viele Informationen, die gegebenenfalls unübersichtlich sind und es schwer machen, Lösungen zu erkennen, prüfen und zu priorisieren. Ähnlich wie mit Mindmaps lassen sich auch mit Affinitätsdiagrammen Ideen gruppieren, so dass durch die Visualisierung die Analyse erleichtert wird.

4. Konzept-Maps

Konzept-Maps illustrieren die Beziehungen zwischen Ideen oder Konzepten. Gedanken, die während einer Brainstorming-Session diskutiert und innerhalb eines Konzepts platziert werden, können Zusammenhänge aufzeigen und Erkenntnisse hervorbringen, die ein besseres Verständnis des Problems beziehungsweise Finden einer potenziellen Lösung ermöglichen.

ES LOHNT SICH, MUTIG ZU SEIN UND AUF VISUELLE TOOLS ZU VERTRAUEN.

André Kreß, MindManager Director Sales DACH & Eastern Europe, Corel, www.corel.com

Gewusst wie

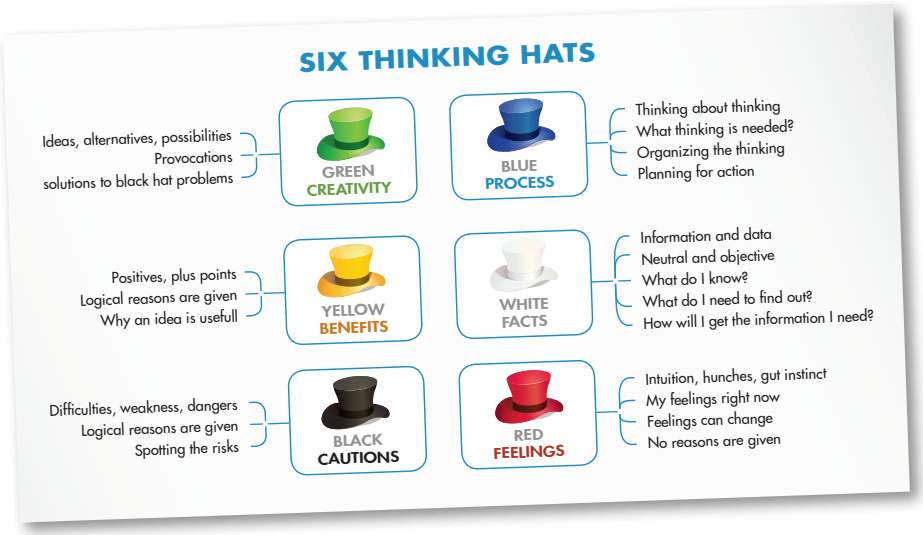
Jetzt geht es darum, Lösungen zu potenziellen Projekten zu priorisieren. Eine Handlungsprioritäten-Matrix ist eine leistungsstarke Methode, um Ergebnisse von Brainstorming-Sessions auszuwerten. Eine solche Matrix hilft, bestehende Optionen zu verfeinern und den Fokus auf die vielversprechendsten Aufgaben auszurichten, damit sich Zeit, Ressourcen und Chancen optimal nutzen lassen. Priorisieren kann man nach Kategorien wie Quick-Wins, Major Projects, Fill in Projects oder Thankless Tasks.

Nun müssen der Projektumfang und der Projektauftrag definiert werden. Dieser Schritt lässt sich gut in Form einer Mindmap visualisieren, etwa indem man unterschiedliche Äste und Zweige anlegt mit Aspekten wie Anforderungen, Meilensteinen oder Risiken. Dann steht die Ressourcenplanung an, für die sich das Format des Organigramms am besten eignet, denn es zeigt auf einen Blick Verantwortlichkeiten, Hierarchien und Abhängigkeiten. Hilfreich ist auch eine Work Breakdown Structure, um die nötige Granularität zu erreichen. Diese werden in der Regel in Form von Gantt-Diagrammen oder Workflow-Diagrammen visualisiert.

Fazit

Gerade zu Beginn eines Projektes, in der Planungsphase, sind die zahlreichen Visualisierungsmethoden und -tools hilfreich. Sie sorgen dafür, dass sich die notwendige Kreativität zur Lösungsfindung entfalten kann, der erforderliche Überblick auch bei komplexen Themen nicht verloren geht und durch die detaillierte Dokumentation der Projektverlauf nachvollziehbar ist und bleibt. Auch wenn diese Methoden heute noch nicht zum üblichen Projekt-Standard gehören – es lohnt sich, mutig zu sein und auf visuelle Tools zu vertrauen. Wer es einmal ausprobiert hat, wird es nicht mehr lassen, denn er hat erlebt, wie viel mächtiger und zielführender diese Methoden sind.

André Kreß



INTERIM PROJEKTMANAGEMENT

VON PROJEKT ZU PROJEKT, AUFTRAG ERLEDIGEN UND WEITER

Das Szenario, dass wichtige Projekte bevorstehen und intern niemand ruft, dass er zu wenig Arbeit hat, ist nicht außergewöhnlich. Manchmal gibt es auch einfach keine verfügbare Person, die über die benötigten Qualifikationen verfügt. Diese Lücke schließt ein Interim Projektmanager.

Fehlende Ressourcen

Projekte sind oft dynamisch und auch der Bedarf an benötigten und verfügbaren Experten sowie der generelle Bedarf an Projekten kann sich dynamisch verändern. Die Chance auf den richtigen Experten zur richtigen Zeit kann die Flexibilität der Unternehmen deutlich erhöhen. Dies betrifft die Möglichkeiten, im Kerngeschäft mehr Aufträge und Umsätze zu generieren und auch, notwendige interne Initiativen nach vorne zu treiben.

Warum sollten Unternehmen wichtige Projekte bei Kunden absagen oder zumindest verschieben, nur weil an einer oder an mehreren Positionen kein interner Mitarbeiter zur Verfügung steht? Warum sollte ein internes Veränderungsprojekt und damit die Wettbewerbsfähigkeit der Organisation verschoben werden, weil keine passende Ressource gefunden wird? Beide Konstellationen führen zu einer gesteigerten Konkurrenzsituation um interne Ressourcen. Im Ergebnis werden unnötigerweise Projekte verschoben oder abgesagt.

Wenn Projekte nicht besetzt werden können, wird die dadurch geplante Investitionsrendite in Form von neuen oder erweiterten Geschäftsmodellen, Umsätzen und Deckungsbeiträgen aus Kundenprojekten, einer notwendigen internen Kostenreduzierung oder der Vermeidung von Geschäftsrisiken nicht erzielt. Der Ausgleich des Mangels an fehlenden oder individuell passenden Ressourcen wird durch Interim Projektmanager ermöglicht. Gerade bei einem wechselhaft hohen Bedarf ist dies eine praktikable Lösung.

Projektmanagement als Dienstleistung

Projekte stellen Organisationen nicht nur vor inhaltliche Herausforderungen. Die Verfügbarkeit und die Auswahl der personellen Besetzung hat entscheidenden Einfluss auf den Projekt- und den Projektmanagementerfolg.

Nicht jeder interne Kandidat mit der richtigen Qualifikation ist politisch durchsetzbar und nicht jeder persönlich passende Kandidat hat die notwendige Qualifikation. Weiterhin warten intern gut passende Projektmanager nicht unbedingt auf ein neues Projekt und sind direkt verfügbar. An dieser Stelle kommt die „externe Lösung“ ins Gespräch.

Interim Projektmanagement kann über verschiedene Anbieter eingekauft werden. Zum einen sind das große und mittlere Dienstleistungsunternehmen. Zum anderen gibt es auch kleine Anbieter und spezialisierte Freiberufler. Da es sich um eine persönliche Dienstleistung handelt, sollte der Projektmanager selbst und seine Kompetenz und nicht das anbietende Unternehmen im Fokus stehen. Die globalen Referenzen des Unternehmens, die

von anderen Personen erreicht wurden, sind an dieser Stelle sekundär.

Vor- und Nachteile

Wie so oft, gibt es auch beim Interim Projektmanagement zwei Seiten einer Medaille. Einer Vielzahl von Argumenten dafür stehen auch Einwände gegenüber. Eine allgemeingültige Bewertung ist nicht möglich. Sie ist individuell, wie Projekte es auch sind. Ein genauerer Blick auf Vorteile und Nachteile zeigt dies. Situationsbedingt können sich die Vorzeichen auch umkehren und aus einem vermeintlichen Nachteil wird ein Vorteil.

Projekts ausgewählt werden. Er bietet zudem weitere Vorteile. Dies sind zum Beispiel die Einbringung seiner externen Erfahrungen und eine unvoreingenommene Neutralität. Das könnte ihm in Konfliktsituationen einen Vertrauensvorschuss bringen. Ein politisch durchsetzbarer Kandidat kann sich schon allein durch die Verringerung von Widerständen rentieren. Ein externer Kandidat hat in den meisten Fällen keine internen Interessen und kann durch diese Eigenschaft, sowie Unvoreingenommenheit und Neutralität auch kritische Stakeholder eher überzeugen. Das Einbringen von einem externen Blickwinkel ohne eine bereits gewachsene Meinung, ergibt sich ein anderer Blickwinkel und vielleicht auch ein neues Bild. Das kann nicht nur dem Projekt helfen, sondern sich nachhaltig auf die Organisation und deren Reifegrad im Projektmanagement auswirken.

Das Phänomen „Die externe Meinung“

Die „externe Meinung“ hat in Projekten teilweise größeres Gewicht bei Führungskräften und Mitarbeitern. Dies liegt unter anderem daran, dass gewürdigt wird, dass „der Externe“ viele verschiedene Situationen bei anderen Kunden gesehen hat. Die Fehler, die an anderer Stelle schon gemacht wurden, brauchen hier nicht noch einmal gemacht werden und die Erfolge von anderer Stelle können eingebracht und vielleicht wiederholt werden. Auch eine unabhängige Bestätigung des vorhandenen Vorgehens kann helfen.

Einsatzmöglichkeiten für Interim Projektmanager im operativen Projektmanagement werden durch Beratungsmöglichkeiten ergänzt.

Projektleiter	Übernahme einer Projektleitung auf Zeit zur Abdeckung von fehlenden Ressourcen oder Schaffung einer neutralen Projektleitung.	Beratung	Beratung für Unternehmen bei Optimierung von Projektmanagement-strukturen und Methoden auf Basis von Best Practices.
Projekt Management Office (PMO)	Aufbau und Betrieb einer aggregierten Steuerung von Projekten auf Zeit.	Coaching	Methodische und persönliche Unterstützung von Fachkräften im Projekt.
Projekt Portfolio Management (PPM)	Schaffung einer Übersicht der Unternehmensprojekte und Sicherstellung, dass die richtigen Projekte zur richtigen Zeit durchgeführt werden.	Schulungen	Weiterbildung von Projektmitarbeitern in Methoden und Werkzeugen.
Projektsicherung	Sicherung von Projektzielen und Qualität des Projektmanagements zum Beispiel für den Lenkungsausschuss.	Mediation	Hilfe bei der Lösung von Konflikten durch neutrale Mediation.

Als Hindernisse oder Nachteile kann man fehlende Kenntnisse des Unternehmens und keine Einbindung in die Unternehmensorganisation anführen. Damit fehlt auch eine emotionale Verbundenheit und nach Durchführung der Projektaufgabe verlässt mit der Interim Lösung Wissen das Unternehmen. Schlussendlich geht mit dem externen Projektmanager auch eine Rechnung einher, die sich erst einmal rentieren muss.

Dem gegenüber steht das Argument, dass eine Interim Lösung eine passgenaue Verfügbarkeit ermöglicht. Das bedeutet, dass hier Spitzen oder nicht stetig benötigte Skills abgedeckt werden können, die nicht über einen längeren Zeitraum bezahlt werden müssen, sondern nur, wenn sie tatsächlich benötigt werden.

Der externe Projektmanager kann nach dem individuellen Anforderungsprofil des kel und Best Practice Ansätze aus vielen anderen Projekten außerhalb der Unternehmensorganisation kann nicht nur das Projekt, sondern auch die Organisation weiterbringen.

Ein weiterer entscheidender Punkt ist die Unabhängigkeit von der Organisation. Damit kann er befreiter handeln, da er keine Nachteile in einer späteren Linienarbeit befürchten muss, anders als ein interner Kollege, wenn er Projektteilnehmer in der täglichen Arbeit wiedertrifft, die eventuell dort sogar hierarchisch höher angesiedelt sind. Weniger persönliche Betroffenheit erleichtert, Entscheidungen ohne Emotionen zu treffen.

Beispiele aus der Praxis

Der unvoreingenommene Blick

Schaut man auf ein neues Umfeld, eine neue Organisation und deren Arbeitsweise ohne eine bereits gewachsene Meinung, ergibt sich ein anderer Blickwinkel und vielleicht auch ein neues Bild. Das kann nicht nur dem Projekt helfen, sondern sich nachhaltig auf die Organisation und deren Reifegrad im Projektmanagement auswirken.

Konflikte im Projekt

In Projekten gibt es aus unterschiedlichsten Motivationen Meinungsverschiedenheiten. Das können zum Beispiel Interessen- und Zielkonflikte sein oder sich aus

einer Kunden-/Lieferantenbeziehung ergeben. Hier kann der Interim Projektmanager seine Stellung und seine Unabhängigkeit nutzen. Seine Unvoreingenommenheit und mangelnden internen Interessen sind authentischer. Er kann teilweise auch als Mediator auftreten.

Voraussetzungen: Grundlagen, Erfahrung und Persönlichkeit

Gute Informatiker oder andere Fachexperten sind nicht zwangsläufig durch ihre exzellenten Fachkenntnisse auch für das Projektmanagement qualifiziert. Oft wollen sie das auch gar nicht. Verdiente Berater, IT-Auditoren und Wirtschaftsprüfer mit Know-how in ihren Disziplinen werden nicht zu Projektexperten nur weil sie gerade über den Projektflur laufen oder in der Cafeteria/Kantine den richtigen Platz haben. Für diese Aufgabe sollten fundierte Kenntnisse und entsprechende Erfahrungen in den Disziplinen des Projektmanagements vorliegen. Wissen auf Überschriftenebene ist hier nicht ausreichend.

Die Aus- und Weiterbildung im ausgeübten Beruf macht unabhängig von der Art des Berufes Sinn. Für Interim Aufgaben ist dies aus diversen Gründen auch so. Wenn jemand bereit ist, nicht nur Geld zu nehmen, sondern auch wieder in seinen Beruf zu investieren, zeigt dies die Bedeutung, die er seinem Beruf gibt. Das Wissen, was er sich aneignet, kommt den Unternehmen zugute, die ihn beauftragen. Schnelles Onboarding in Projekten wird ermöglicht, wenn zum Beispiel die angeeignete Projektmanagementmethode dort verwendet wird. So sprechen alle schon mal eine „Methodensprache". Generell hilft es natürlich auch, einen Methodenbaukasten im Projekt parat zu haben. Der externe Kandidat kann durch Methodenkompetenz Mehrwerte einbringen. In Summe sind dies auch gute Argumente für geforderte und angemessene Stundensätze. Gerade bei der Inflation von

WENN PROJEKTE NICHT BESETZT WERDEN KÖNNEN, WIRD DIE DADURCH GEPLANTE INVESTITIONSRENDITE NICHT ERZIELT.

Martin Besemann, Berater und zertifizierter Projektmanager (PMP, Prince2 Practitioner/ Agile, Senior Project Manager IPMA Level B), www.conpromas.de

Worten wie Projekt und Projektmanagement können Zertifizierungen einen ersten Eindruck geben, wie der Interim Projektmanager aufgestellt ist.

In Prince2 wird als Grundprinzip „Lernen aus Erfahrung" genannt und beschrieben. Wie ein Unternehmen profitiert auch der Interim Projektmanager von diesem Grundprinzip. Ein entscheidendes Kriterium für die Auswahl eines Anbieters sind seine Erfahrungen und das, was sich daraus auch in anderen Themenfeldern entwickeln lässt.

Die eigene Persönlichkeit ist ein entscheidender Erfolgsfaktor. Als Leader eines Projektes muss die Person über die entsprechenden Eigenschaften verfügen. Nur ein Titel reicht nicht, um die notwendige Kompetenz zu verkörpern. Die Person muss allen Stakeholdern, Projektteilnehmern wie Projektbetroffenen, auf Augenhöhe begegnen, weil er oder sie als Leader und nicht als Support engagiert ist.

Interim Projektmanager sollten sich der Aufgabe bewusst sein und auch damit leben können, dass sie auch mal schlechte Nachrichten überbringen oder nicht der Liebling des Projekts sind. Ihre Aufgabe ist, das Projektmanagement zum Erfolg zu bringen und dazu gehören auch unpopu-

Was spricht für einen Interim Projektmanager?

Verfügbarkeit

- Zeitlich verfügbare Ressourcen nach Bedarf
- Benötigtes Fachwissen ohne Ausbildungskosten bei Bedarf verfügbar
- Individuelle Auswahl passend zum Projekt

Kosten

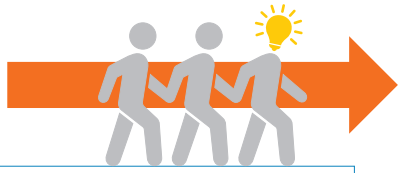
- Variable Kosten statt Fixkosten
- Cash out nur bei speziellem Bedarf und dedizierter Rendite
- Fertige Ressourcen ohne Zusatzkosten für Ausbildung

Erfahrung

- Unvoreingenommener Blickwinkel und Innovation
- Neues Wissen (Best Practices) kommt ins Unternehmen
- Erfahrungen können implementiert werden und bleiben im Unternehmen

Position

- Neutralität durch fehlende Organisationseinbindung
- Keine persönliche Betroffenheit erleichtert unabhängige Entscheidungen
- Unabhängige Meinung / Möglichkeiten zur Mediation



Auswahlkriterien für einen Interim Projektmanager

- Best Practice Kenntnisse und umfangreiche Erfahrung steigern den Wert für den Kunden.
- Methodenkenntnisse erleichtern das Onboarding und die Durchführung des Projekts.
- Die Persönlichkeit ist ein Erfolgsfaktor um den Stakeholdern auf Augenhöhe zu begegnen.

Der Projektmanager sollte zunächst sein PM Handwerk verstehen, denn er soll das Projekt führen und nicht alle fachliche Arbeit selber machen.

läre Aktivitäten. Eine extrovertierte Persönlichkeit und Kommunikationsstärke auf allen Ebenen ist allgemein im Projektmanagement hilfreich. Man sollte sich als Führungskraft darstellen und nicht die Arbeitsweise diktieren lassen. Die Interim Lösung ist unabhängig von der Unternehmensorganisation und sollte auch so handeln und behandelt werden.

Ein guter Interim Projektmanager geht den Konflikten nicht aus dem Weg, sondern versucht, sie zu lösen. Ein reines „Kopf runter" um nicht in die Gefahr zu kommen die Umsatzeingänge zu gefährden, ist keine Lösung im Sinne des Projekterfolgs.

Generell muss ein Projektmanager, der in ein neues Projekt kommt, vielleicht sogar in einem ganz neuen Umfeld, immer damit rechnen, dass er nicht auf eine „Rund um sorglos Kreuzfahrt" geht, sondern zunächst in ein anspruchsvolles Fahrwasser. Wenn er dafür nicht geeignet ist, muss generell über den Beruf nachgedacht werden.

Bevor es zu einer Übernahme des Projektes kommt, sollte beiderseitig geprüft werden, ob nicht nur der Interim Kandidat zum Projekt passt, sondern auch umgekehrt das Projekt für den Interim Manager. Eine kurzfristige Sichtweise, das heißt auf der einen Seite nur einen „billigen" Einkaufspreis zu erzielen oder auch auf der anderen Seite nur den angepeilten Umsatz zu erreichen, wird keiner Seite mittelfristig einen Vorteil bringen. Man kann auch mal ein Projekt beziehungsweise einen vorteilhaft wirkenden Preis ablehnen. Bietet sich ein Interim Projektmanager zu einem zu günstigen Preis an, ist es lohnend zu fragen, warum das so ist. Es macht auch für den Kunden keinen Sinn, wenn der Anbieter nach einiger Zeit das Projekt sitzen lässt, weil er attraktivere Aufträge gefunden hat. Eine Win-Win Situation ist nicht nur im beiderseitigen Sinn, sondern vor allem auch für das Projekt ein Gewinn.

Fazit

Interim Projektmanagement bietet sowohl für den Kunden wie auch für den Projektmanager ein spannendes Arbeitsfeld. Der Projektmanager hat immer neue Umfelder und Herausforderungen, wovon er in seiner Entwicklung profitiert. Das beauftragende Unternehmen profitiert von diesem Erfahrungsschatz. Damit profitieren beide gegenseitig von sich. Eine gute Grundlage für eine Geschäftsbeziehung.

Den richtigen Interim Projektmanager zu finden, ist erfolgskritisch. Im Gesamtkontext des Projekteinsatzes ist ein gewisser Unterschied im Honorar nicht ausschlaggebend. Die Frage ist an dieser Stelle, was brauche ich, was setze ich ein und was bekomme ich dafür?

Martin Besemann

Ist Interim Projektmanagement eine Alternative? Einige Fragen...

Verfügbarkeit

- Werden Projekte verschoben, weil kein interner Projektmanager verfügbar ist?
- Werden Projekte verschoben, weil verfügbare Projektmanager nicht passen?
- Mussten Personen Projekte übernehmen, die das eigentlich nicht wollten?

Wirtschaftliche Aspekte

- Wurden benötigte Projektergebnisse mangels Ressourcen verpasst?
- Gab es eine Unter- oder Überdeckung interner Ressourcen?
- Gab es eine ausreichende und lohnende Weiterbildung der Mitarbeiter?

Wissen

- Sind die Fachkenntnisse im Projektmanagement ausreichend?
- Kann das Projektmanagement Impulse gebrauchen?
- Wurde Personal mit Know-how durch Fluktuation verloren?

Position

- Gab es in Projekten Unstimmigkeiten bei der Auswahl des Projektleiters?
- Gibt es genug Abstand zu den Projekten und den Projektgegenständen?
- Kann Unabhängigkeit und Neutralität in Projekten helfen?

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
30. SEPTEMBER 2021

CLOUD COMPUTING

Agil, flexibel und sicher?

MODERN ACCOUNTING

Unabhängig und schnell einsatzbereit

GAMECHANGER: MINDSET

Lernende IT-Organisationen sind notwendig

DIE AUSGABE 09/2021 VON IT MANAGEMENT ERSCHEINT AM 31. AUGUST 2021.

INSERENTENVERZEICHNIS

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Carina Mitzschke, Silvia Parthier (-26)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Martin Besemann, Lisa Ehrentraut, Kevin Heinloth, Ralf Kempf, André Kreß, Carina Mitzschke, Angelika Mühleck, Silvia Parthier, Ulrich Parthier, Elton Schwerzel, Andreas E. Thyen, Michael Vorberger, Aldo Zanoni, Stéphane Zanoni

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: 08104-6494-21
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

SIE TUN ALLES FÜR IHR UNTERNEHMEN. WIR AUCH.

Unsere Dell Technologies Experten entwickeln mit Ihnen individuelle Technologielösungen, ganz gleich ob Sie beabsichtigen, Ihren Kundenstamm auszubauen oder Ihr Team zu vergrößern. So können Sie sich ganz Ihren Kunden widmen.

Kontaktieren Sie einen Dell Technologies Experten unter **0800-724 49 07*** oder **Dell.de/KMU-Beratung**

DELL Technologies

XPS 13

Windows 10

Erledigen Sie mehr mit einem modernen Windows 10 Pro Gerät

itsecurity
JULI/AUGUST 2021

DAS SPEZIAL

ZERO TRUST NETWORK ACCESS

SICHERHEIT IN DER MOBILEN WELT

Christian Bücker, macmon secure

SECURITY-KONSOLIDIERUNG
THOUGHT LEADERSHIP

CREDENTIAL STUFFING

Strategien, die Unternehmen wirklich helfen

CYBER-ATTACKEN

Die Basis für eine fortlaufende Optimierung

SECURITY BY DEFAULT

Stärkung für das Internet of Things (IoT)

#WesecureIT

We secure IT

IT Security 2021

Digitalevent

28.10.21

SCAN ME

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

13

28

INHALT

4 COVERSTORY

COVERSTORY

THOUGHT LEADERSHIP

IT SECURITY

24

ZERO TRUST NETWORK ACCESS

SO FUNKTIONIERT ER IN DER MOBILEN WELT

Zero Trust ist derzeit das Modewort in der IT-Security Welt. Passt, wackelt und hat Luft. Werfen wir einen Blick hinter die Kulissen mit Christian Bücker, CEO beim Berliner Security-Spezialisten macmon secure.

Ulrich Parthier: *Würden Sie mir zustimmen, wenn wir Zero Trust als den Hypebegriff unserer Zeit bezeichnen und wie lautet ihre Definition?*

Christian Bücker: Zero Trust Network Access (ZTNA) gewinnt tatsächlich immer mehr an Bedeutung. ZTNA fußt auf der Philosophie, weder einem Gerät noch einem Benutzer vor einer sicheren Authentifizierung einen Vertrauensvorschuss zu geben. Der rasante Wandel der Arbeitswelt sorgt für neue Anforderungen an die IT-Sicherheit. Mobiles Arbeiten, das „New Normal", die fortschreitende Digitalisierung führen verstärkt zu einer Auslagerung verschiedener Dienste in die Cloud. Daraus resultiert, dass ZTNA auch in Zukunft ein wichtiger Bestandteil integrativer IT-Security-Lösungen sein muss, also kein kurzfristiger Hype, sondern ein neuer und langfristiger Ansatz.

Ulrich Parthier: *Historisch gesehen kommen Sie ja aus dem NAC-Umfeld. Ist Zero Trust Network Access die logische Weiterentwicklung von NAC?*

Christian Bücker: Mit unserem macmon NAC Lösungsportfolio konzentrieren wir uns weiterhin auf physische Netzwerke, mit macmon SDP (Secure Defined Perimeter) sind wir den logischen Schritt in die Cloud gegangen, um für die aktuellen und zukünftigen Rahmenbedingungen und Sicherheitsanforderungen ein zuverlässiges Angebot bieten zu können. Das sichert langfristig unsere Marktposition als zentraler Bestandteil eines IT-Sicherheitskonzepts, und gleichzeitig eröffnen wir unseren Marktpartnern im Channel interessante Vertriebsmöglichkeiten. NAC ist ein Teil von ZTNA und SDP ein weiterer Teil – insofern ist es vor Allem eine Erweiterung.

Ulrich Parthier: *Kernstück des ZTNA-Ansatzes ist ja der SDP-Agent. Könnten Sie kurz das Prinzip erklären, das dahintersteckt?*

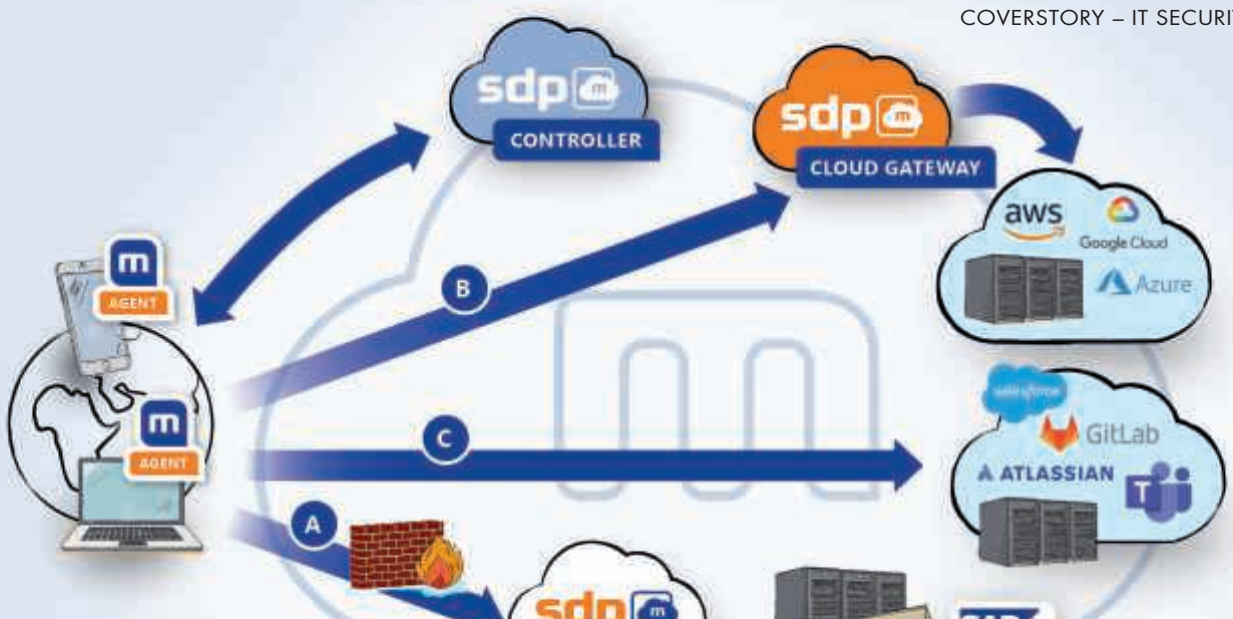
Christian Bücker: Die Funktionsweise und vor allem die Nutzung von macmon Secure Defined Perimeter ist denkbar einfach. Der macmon SDP-Agent übernimmt transparent eine hochsichere Authentifizierung gegenüber dem macmon SDP-Controller, um die Identität des Benutzers sowie des Gerätes und dessen Sicherheitszustand zu prüfen. Der SDP-Controller befindet sich in einer ISO 27001 zertifizierten deutschen Cloud in Berlin und liefert über die verschlüsselte Verbindung nach erfolgreicher Authentifizierung die definierte Policy zurück an den Agenten. Die Policy enthält alle Information über die Erreichbarkeit der Unternehmensressourcen, für die dem Benutzer, unter den entsprechenden Bedingungen, der Zugriff gewährt wird.

Ulrich Parthier: *Sicherheit bedeutet ja heute nicht nur On-Premises im Unternehmensnetzwerk, sondern es heißt auch Cloud. Wie gewährleisten Sie die Sicherheit in beiden Welten?*

Christian Bücker: Sicherheit im lokalen Netzwerk erzielen wir weiterhin durch unser erprobtes NAC-Portfolio. Die Ver-

MIT BLICK AUF DIE SICHERHEIT KOMMEN ALLE BISHERIGEN KONZEPTE UND ARCHITEKTUREN AN IHRE GRENZEN, SO DASS NEUE LÖSUNGEN NOTWENDIG SIND, UM DER KOMPLEXITÄT HERR ZU WERDEN.

Christian Bücker, CEO, macmon secure, www.macmon.eu



DAS SDP-FUNKTIONSPRINZIP

A traditionelle lokale Ressourcen im Firmennetzwerk
B Ressourcen in der private cloud
C Ressourcen in der public cloud

bindung zur Cloud stellen wir über macmon SDP her. Nach erfolgreicher Authentifizierung erreicht der Nutzer alle erforderlichen Ressourcen. Entweder direkt per Single Sign-on bei Cloud-Applikationen oder über das macmon SDP-Cloud-Gateway bei Ressourcen in Private Clouds. Darüber hinaus können auch lokale Ressourcen im Firmennetzwerk über eine direkte Verbindung durch ein lokales SDP-Gateway erreicht werden. Zur Absicherung der Kommunikation bestehen jeweils verschlüsselte Tunnel, die je nach Konfiguration nur gezielt Ressourcen erreichbar machen. So werden sämtliche Cloud-Strategien, wie auch „Hybrid Cloud" flexibel unterstützt, und Unternehmen können ihre Roadmaps zur Migration von Services bedenkenlos verfolgen.

Ulrich Parthier: *Heutzutage nutzen die Anwender viele Geräte: im Büro, Home-Office und mobil. Wie managen sie die Zugriffssteuerung?*

Christian Bücker: Mit macmon NAC wissen unsere Anwender jederzeit, welche Geräte sich im lokalen Netzwerk befinden und haben somit den Überblick über die Geräte, deren Aktivitäten dann auch erst kontrolliert werden können. Alle eingesetzten Geräte können permanent identifiziert und effizient überwacht werden, um unbefugte Zugriffe zu verhindern. Die Kombination von macmon NAC mit bestehenden Identitätsquellen – CMDBs, Asset Management, AD/LDAP oder auch Mobile Device Management (MDM) – führt zu einer zentralen und vollständigen Sicht. Ergänzt um unsere neue Lösung macmon SDP erweitern wir die Zugriffsteuerung nun effizient über die Netzwerkgrenzen des Unternehmens hinweg, und decken das Home-Office, genauso wie mobile Zugriffe aus dem Hotel oder vom Strand aus, ab.

Ulrich Parthier: *SDP konkurriert ja in Bezug auf Sicherheit direkt mit VPN-Anschlüssen. Gibt es für die Anwender Mehrwerte in puncto Sicherheit gegenüber einem Virtual Private Network?*

Christian Bücker: Es gibt diverse Unterschiede und SDP wird ja auch oft als „next generation VPN" bezeichnet. Zum einen ist ein Grundprinzip, dass nicht nur der Benutzer authentifiziert wird, sondern auch das Endgerät selbst, sowie dessen Sicherheitsstatus. SDP sorgt dafür, dass nur definierte Benutzer mit definierten Geräten den Zugang zu definierten Ressourcen bekommen. Und da liegt auch der zweite große Unterschied – SDP bietet die Möglichkeit mehrere Tunnel aufzubauen um Ressourcen an verschiedenen Standorten, lokal im Netzwerk oder auch in Cloud-Rechenzentren direkt zu erreichen, ohne den aufwändigen Umweg über ein VPN-Gateway am Hauptstandort. In Summe also mehr Flexibilität bei umfangreicherer Kontrolle und Sicherheit.

Ulrich Parthier: *Kommen wir noch einmal zurück zum Thema Zero Trust. Wie sehen die IT-Entscheider die Argumente für Zero Trust?*

Christian Bücker: Mit Blick auf die Sicherheit kommen alle bisherigen Konzepte und Architekturen an ihre Grenzen, so dass neue Lösungen notwendig sind, um der Komplexität Herr zu werden. Strategisch muss in der Zukunft die Verwaltung all dieser Anforderungen auf Basis von Identitäten erfolgen, denn es dreht sich immer um eine Identität die Zugriffe benötigt. Zero Trust setzt genau da an, in dem Identitäten von Benutzern und deren Endgeräte, sowie deren Sicherheitsstatus in alle Entscheidungen einbezogen werden. In Gesprächen mit IT-Ent-

scheidern ernten wir massives Verständnis und Bestätigung für diesen Ansatz. Es geht damit weniger darum, ob Zero Trust eingeführt wird, als vielmehr darum wann dies geschieht.

Ulrich Parthier: *Wo sehen sie die Vorteile von macmon SDP als deutschem Produkt?*

Christian Bücker: In Deutschland gibt es keine Alternative zu macmon SDP – unsere Daten befinden sich sicher in einem deutschen Rechenzentrum, DSGVO konform, ein wichtiger Vertrauensfaktor für uns, im Gegensatz zu Angeboten von amerikanischen Marktpartnern. Außerdem sind wir auch mit unserem Support vor Ort in Berlin. Unsere Kundenumfragen ergeben immer wieder, dass dies von unseren Kunden, insbesondere in Deutschland, Österreich und der Schweiz, sehr geschätzt wird. Zudem ist SDP hochskalierbar für jede Anzahl an Nutzern und bietet eine globale Verfügbarkeit, ein weiterer interessanter Faktor für den Exportweltmeister Deutschland

Ulrich Parthier: *Wie vertragen sich macmon NAC und macmon SDP?*

Christian Bücker: Beide vertragen sich ausgezeichnet. Wir sind überzeugt, dass

> ZTNA WIRD AUCH IN ZUKUNFT EIN WICHTIGER BESTANDTEIL INTEGRATIVER IT-SECURITY-LÖSUNGEN SEIN.
>
> Christian Bücker, CEO, macmon secure, www.macmon.eu

wir mit macmon SDP einen wichtigen strategischen Schritt gehen und unsere Marktposition – zusätzlich zu unserer NAC Kompetenz - deutlich stärken werden. Wir dehnen unseren bewährten und geprüften Schutz auf sämtliche Unternehmensressourcen in der Cloud aus und bieten Unternehmen damit einen ganzheitlichen und umfassenden Schutz für all ihre Ressourcen. Ergänzend haben wir noch diverse Ideen, wie das Zusammenspiel der beiden Produkte zukünftig noch ganz neue Möglichkeiten bieten kann, wie zum Beispiel die tunnelbasierte Anbindung von kryptographisch authentifizierten IOT-Devices. Die nötigen Technologien haben wir nun bereits. Unsere Kernaussage: Wir sind innovativer und einziger Anbieter von NAC plus SDP mit Identity Access Management aus Deutschland, gehostet in Deutschland.

Ulrich Parthier: *Thema Partner und Kooperationen. Wie hat sich Ihre Landschaft hier entwickelt?*

Christian Bücker: Wir konnten in den letzten Jahren viele interessante Partnerschaften mit führenden Anbietern von Sicherheitslösungen eingehen und durch die nahtlosen Integrationen unseren Kunden echte Mehrwerte bieten. Unser Fokus auf die Kontrolle der Zugänge bietet eine hohe Spezialisierung, während die Integrationen unseren Kunden die Macht in die Hand gibt, jederzeit mit höchster Effektivität durch Know-how Kombinationen auf Vorfälle und Sicherheitsverstöße zu reagieren. Zusammenfassend hat sich unsere Technologiepartner-Strategie sehr gut entwickelt und alle Anzeichen stehen darauf, dass es auch genauso erfolgreich weiter geht!

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

SECURITY-KONSOLIDIERUNG

TEIL 2

WELCHE BEDEUTUNG DAS THEMA HOMEOFFICE EINMAL HABEN WÜRDE, AHNTE VOR ÜBER EINEM JAHR NOCH KEINER – DASS DIESES DANN ABER UMSO MEHR GESCHÜTZT WERDEN MUSS, WAR SCHNELL KLAR

DER PANDEMIE EINEN ENTSCHEIDENDEN SCHRITT VORAUS

MULTIFAKTOR-AUTHENTIFIZIERUNG AUS DER CLOUD EBNET REMOTE-ARBEIT DEN WEG

Die 1966 gegründete Yamaha Music Europe GmbH mit Sitz in Rellingen ist als Vertriebsgesellschaft für das gesamte Europa-Geschäft der Yamaha Corporation Group zuständig, deren Name fest mit der internationalen Geschichte der Musikinstrumenteherstellung verknüpft ist.

Quelle: Yamaha Music Europe GmbH

AUTHPOINT BRACHTE UNS VIEL MEHR MÖGLICHKEITEN BEI DER DEFINITION VON ZUGRIFFSBERECHTIGUNGEN, DENN EINSTELLUNGEN KÖNNEN DARÜBER DEUTLICH GRANULARER VORGENOMMEN WERDEN.

Christian Schulz, IT-Administrator, Yamaha Music Europe GmbH
www.yamaha.de
(Quelle: Yamaha Music Europe GmbH)

Der Schutz der digitalen Unternehmensressourcen genießt bei Yamaha Music – weltweit bekannt für das Angebot eines breiten Spektrums an Musikinstrumenten, Elektronik- und Hi-Fi-Produkten sowie zahlreichen damit verknüpften Dienstleistungen – schon immer besondere Aufmerksamkeit. Bereits seit vielen Jahren gilt beispielsweise die konzernweite Vorgabe zur Zwei-Faktor-Authentifizierung, um VPN-Zugriffe auf das Firmennetz abzusichern. Ein 2019 separat initiiertes Projekt am Standort Rellingen führte in dem Zusammenhang nicht nur zu einem zusätzlichen Effizienzschub im Hinblick auf interne Administrationsprozesse. Im Gegensatz zu vielen anderen Unternehmen hatte die Yamaha Music Europe GmbH darüber hinaus einen klaren Vorsprung, als im März 2020 von jetzt auf gleich auf Homeoffice-Betrieb umgestellt werden musste.

Für Christian Schulz, der bereits seit über 20 Jahren in der IT-Abteilung der Europa-Zentrale von Yamaha Music in Rellingen tätig ist, hätte das Timing für die Umstellung auf eigene Strukturen zur Multifaktor-Authentifizierung kaum besser sein können. Er erinnert sich: „Ursprünglich ging es bei der Einführung einer ‚europäischen Lösung' zur Multifaktor-Authentifizierung vor allem um mehr Flexibilität und Kosteneinsparungen in unseren eigenen Reihen." Bisher zeichnete das Headquarter in Japan für den Remote-Zugang aller europäischen Mitarbeiter auf die IT-Systeme in Europa sowie Japan verantwortlich. Dieses Zepter wollten die Rellinger nun selbst in die Hand nehmen. „Wir sind als Vertriebs- und Servicegesellschaft für alle Lokationen in Europa IT-seitig verantwortlich und betreiben das europäische Re-

chenzentrum, über das zum einen alle hiesigen Aktivitäten laufen und zum anderen auch die Brücke zu den zentralen Systemen in Japan geschlagen wird. In logischer Konsequenz sollten wir auch bei der Absicherung der Logins selbst an vorderster Front stehen – nicht zuletzt, um deutlich schneller auf unvorhergesehene Ereignisse reagieren zu können", so Schulz.

Homeoffice vor Corona kaum ein Thema

Welches Ausmaß der VPN-Zugriff innerhalb weniger Monate annehmen würde, ahnte bei Start des Projekts noch keiner. „Unsere Vertriebsmitarbeiter waren logischerweise schon immer viel unterwegs im Einsatz. Auch die Abteilungsleiter hatten bereits die Möglichkeit zum mobilen Arbeiten. Aber der Rest der rund 300 Mitarbeiter am Standort Rellingen war vor Ausbruch der Pandemie eigentlich stets im Büro, um von hier aus der täglichen Arbeit nachzugehen. In den anderen europäischen Ländern gestaltete sich die Situation ähnlich", wie der IT-Administrator berichtet. Die Einführung einer Multifaktor-Authentifizierungslösung zur Absicherung des VPN-Zugangs auf europäischem Boden war in dem Moment also eher die Kür und vor allem ein Schritt zu mehr Unabhängigkeit im Tagesgeschäft der Rellinger IT.

Drei Argumente bei der Lösungsauswahl

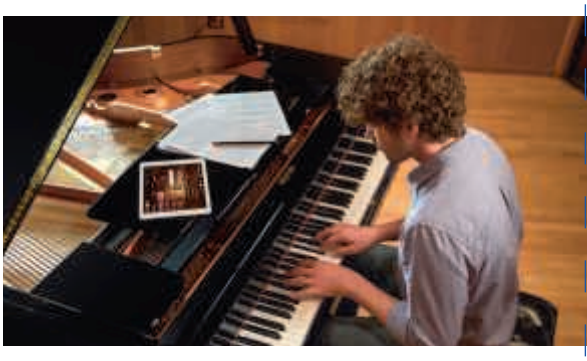
Ein Produkt schaffte es schnell auf die Wunschliste des Projektteams: AuthPoint von WatchGuard. Schließlich vertraute die Yamaha Music Europe GmbH im Rahmen des Netzwerkschutzes bereits seit vielen Jahren auf die Lösungen des US-amerikanischen IT-Security-Anbieters. Die Absicherung des Perimeters nach außen gestaltete sich mit den jeweiligen Produktgenerationen der Firewalls und UTM-Appliances stets reibungslos. Heute befinden sich insgesamt 15 der roten Boxen in unterschiedlicher Größenordnung an den 14 Standorten europaweit im Einsatz, um den Internetverkehr aller Niederlassungen und über 800 Mitarbeiter von Yamaha Music Europe auf ein verlässliches Fundament zu stellen.

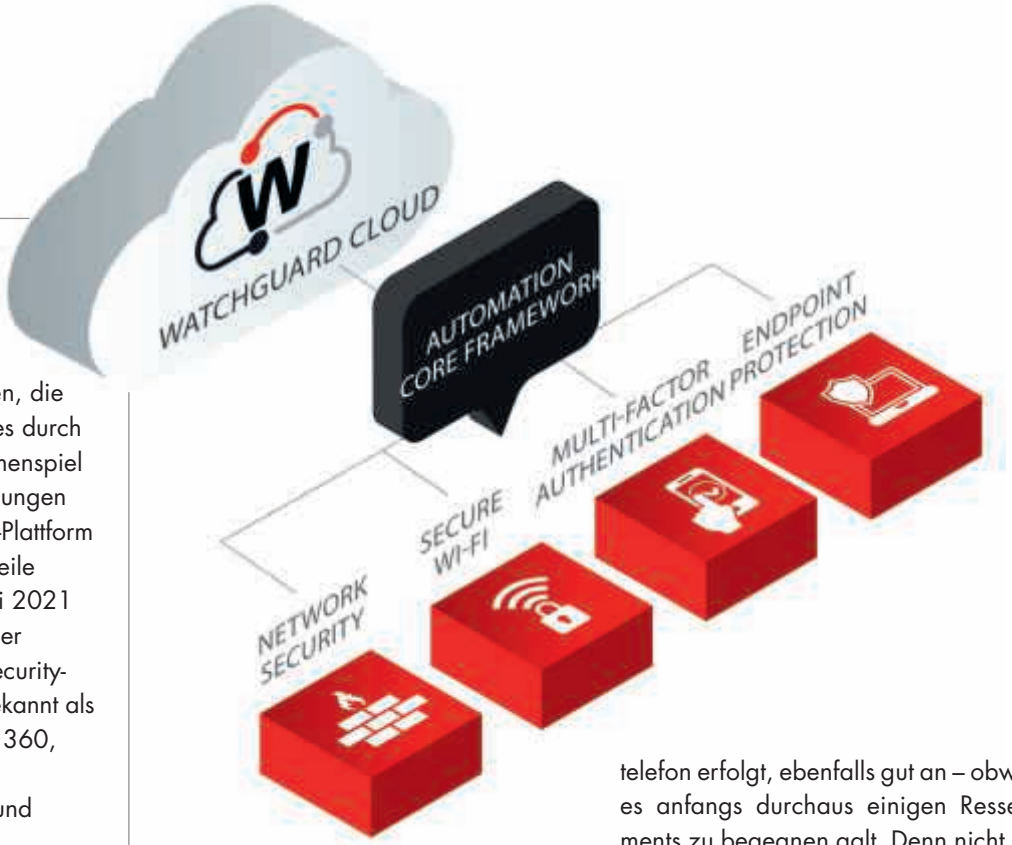
„Die leistungsstärksten Appliances stehen als HA-Cluster bei uns in Rellingen. Die Hardwareauswahl an allen anderen Orten passt zur Größe der jeweiligen Lokation – von der kleinen Tabletop-Firebox T80 bis zur M370 ist alles dabei. Hinsichtlich der Funktionalität gibt es allerdings keine Unterschiede", wie Schulz betont. Auf allen Geräten gewährleistet die „Total Security Suite" umfangreichen Schutz – als Komplettpaket, das neben traditionellen Security Services wie IPS, Antivirus, URL-Filterung, Application Control, Spam-Schutz und Reputations-Suche mittlerweile auch fortschrittliche Technologien für KI-basierten Malware-Schutz, erweiterte Netzwerkvisualisierungsfunktionen, Cloud-Sandboxing oder DNS-Filter umfasst.

Neben den bisherigen Erfahrungen beim Netzwerkschutz spielten bei der Entscheidung im Rahmen des neuen MFA-Projekts zwei weitere Aspekte eine nicht unerhebliche Rolle. „Die cloudbasierte AuthPoint-Lösung brachte umfangreiche und moderne Features mit sich, die gewiss auch ohne bisherige Berührung zum Anbieter überzeugen. Aber die Tatsache, dass sich die Multifaktor-Authentifizierung und alle anderen Funktionalitäten zum Netzwerkschutz über die gleiche intuitiv aufgebaute Oberfläche verwalten lassen und dadurch weiteren Synergien Weg gebahnt wird, erhöhte den Reiz für das Team nochmal deutlich. Schließlich ist der Umgang mit den WatchGuard-Produkten bei allen mittlerweile in Fleisch und Blut übergegangen." Zudem erübrigte sich für Schulz auf diese Weise auch die Verantwortlichkeitsfrage. „Je mehr Hersteller im Rahmen von Security-Konzepten im Boot sind, desto höher ist auch das Risiko, dass im Fall der Fälle einer auf den anderen zeigt und sich dadurch die eigentliche Lösungsfindung verzögert. Sollte bei uns wirklich mal was haken, sind wir direkt an der richtigen Adresse." Diese Effizienzthematik ist seines Erachtens gerade für ein personell limitiertes IT-Team von enormer Bedeutung.

Souverän und schnell zum Ziel

Auf Basis der Cloud konnte mit der Umsetzung des MFA-Konzepts sofort gestartet werden, die Konfiguration war in kürzester Zeit implementiert und die Unter-





UMFASSENDE SICHERHEIT AUS EINEM GUSS

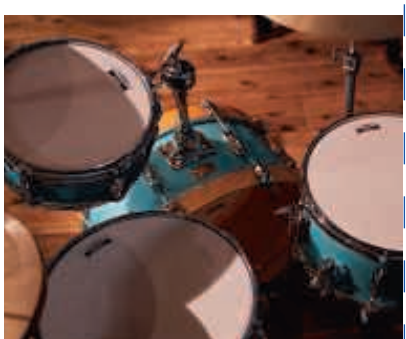
Die Synergiemöglichkeiten, die WatchGuard Technologies durch das abgestimmte Zusammenspiel einzelner IT-Sicherheitslösungen über eine zentrale Cloud-Plattform eröffnet, wurden mittlerweile gezielt erweitert. Seit Juni 2021 sind auch alle Produkte der WatchGuard Endpoint-Security-Produktfamilie – bisher bekannt als Panda Adaptive Defense 360, Adaptive Defense, Endpoint Protection Plus und Endpoint Protection – in WatchGuard Cloud integriert. Die vor einem Jahr erfolgte Akquise von Panda Security als Spezialist für den Schutz von Endpunkten ist damit auch technologisch abgerundet. Kunden wie Partner profitieren von der einfachen Bereitstellung weitreichender IT-Security-Funktionalitäten, die vom Netzwerkschutz über Multifaktor-Authentifizierung bis hin zur Absicherung der Endpunkte reichen.

www.watchguard.de

schiede zum vorangegangenen Lösungsszenario zeigten sich schnell, wie Schulz präzisiert: „AuthPoint brachte uns viel mehr Möglichkeiten bei der Definition von Zugriffsberechtigungen, denn Einstellungen können darüber deutlich granularer vorgenommen werden. Zudem müssen wir bei Anpassungswünschen oder Optimierungen nicht mehr über Japan und den von der Zentrale beauftragten Dienstleister gehen, was jedes Mal zusätzliche Kosten bedeutete. Ich sehe nach wie vor nur Vorteile: Wir haben selbst eine viel bessere Kontrolle, gewährleisten ein hohes Maß an Sicherheit und können dabei auch noch Geld sparen."

Hoher Komfort für Anwender

Auf Anwenderseite kommt die Lösung, bei der die Authentifizierung über Mobiltelefon erfolgt, ebenfalls gut an – obwohl es anfangs durchaus einigen Ressentiments zu begegnen galt. Denn nicht alle Mitarbeiter verfügen über ein Firmenhandy und die Einbindung von Privatgeräten war nicht gleich jedermanns Sache. Diese Bedenken konnten jedoch schnell zerstreut werden. Wie Schulz berichtet, ist inzwischen selbst dem größten Kritiker klar, dass es sich nur um ein Mittel zum Zweck handelt. Bequemer könnte es schließlich kaum sein. Sobald der Mitarbeiter oder die Mitarbeiterin per VPN auf das Firmennetz der Yamaha Music Europe zugreifen möchte, müssen nur der Username und das Passwort eingegeben werden. Dadurch wird automatisch der weitere Authentifizierungsprozess in Gang gesetzt und eine Push Notification ans zugeordnete Mobiltelefon gesendet, die einfach bestätigt werden kann, ohne irgendeine zusätzliche Eingabe zu erfordern.



Minerva Studio / Shutterstock.com

Von null auf hundert in Rekordzeit

Wie wertvoll dieses Projekt tatsächlich war, zeigte sich jedoch erst und gerade in der Pandemie. „Wir sind im Sommer 2019 mit wenigen Lizenzen gestartet. Mittlerweile liegen wir bei knapp 700 Nutzern in ganz Europa, da im Zuge von Kontaktbeschränkungen und Homeoffice sozusagen über Nacht fast die gesamte Belegschaft auf den VPN-Zugang angewiesen war, um überhaupt noch geschäftlich agieren zu können. Spätestens an dieser Stelle wäre uns das Konstrukt mit dem japanischen Dienstleister wahrscheinlich um die Ohren geflogen, nicht nur hinsichtlich der Reaktionszeiten, sondern insbesondere kostenseitig", so Schulz.

Bis auf wenige Ausnahmen – beispielsweise beim Lagerpersonal, den Klavierstimmern oder den Kollegen, die zuhause keinerlei Homeoffice-Möglichkeit realisieren konnten – war im Lockdown kaum noch jemand von der Belegschaft in der Firma, um von hier unter dem Schutz des eigentlichen Netzwerkperimeters zu arbeiten. Der Wechsel ins Homeoffice gestaltete sich insbesondere hardwareseitig als Herausforderung. Christian Schulz: „Laptops waren kaum kurzfristig zu beschaffen, viele der Mitarbeiter nahmen daher ihre Desktop-PCs aus dem Büro mit." Im Vergleich dazu stellte die Absicherung der neuen Arbeitssphären keinerlei Problem dar. Es reichte ein Telefonanruf, um weitere Lizenzen für den verlässlichen VPN-Zugang zu ordern, die bereits am nächsten Tag einsatzbereit waren. Das Einspielen des Clients auf dem Mobiltelefon des Anwenders dauerte meist länger als die Administration an sich. Der Rollout der AuthPoint-App erfolgte per Mail. Sobald der User im System angelegt war, ging die entsprechende Einladung mit dem Download-Hinweis für iOS oder Android automatisch raus. Der Rest war selbst auf die Entfernung ein Kinderspiel.

Vorsicht statt Nachsicht

In dieser Ausnahmesituation hatte Yamaha Music Europe mit der cloudbasierten Authentifizierungslösung natürlich einen eklatanten Vorteil. Schulz ist sich sicher: „Auch wenn hinsichtlich des Zeitpunkts der Fertigstellung eine enorme Portion Glück im Spiel war, trägt gewiss auch das Selbstverständnis unserer japanischen Konzernmutter dazu bei, dass es im Hinblick auf IT-Security bisher kein Szenario gab, bei dem wir Federn lassen mussten". In der Organisation wird seit jeher enorm viel Wert daraufgelegt, sich in keiner Hinsicht abhängen zu lassen – egal ob bei der Produktentwicklung, Kundenansprache oder auch im Rahmen der internen Abläufe. Es gilt, rechtzeitig die nötigen Voraussetzungen zu schaffen, um erst gar nicht angreifbar zu werden. Schlagzeilen wie sie beispielsweise Sony vor einigen Jahren hinnehmen musste, als Hacker ins Firmennetz eindrangen, soll proaktiv vorgebeugt werden. Daher packt Yamaha Music neue sicherheitsrelevante Fragestellungen in der Regel frühzeitig an.

Harmonisch abgestimmt

Christian Schulz ist zufrieden. Die cloudbasierte Lösung, die Netzwerkschutz und MFA in Symbiose verbindet, läuft verlässlich. Das Team hat stets die Kontrolle über alle damit verbundenen Vorgänge. So wird beispielsweise täglich geprüft, ob es irgendwelche Auffälligkeiten gibt, die eine Reaktion erfordern. „Das ist total intuitiv. Solange alles grün ist, müssen wir uns keine Sorgen machen. Und sollte doch mal was aufploppen, sind wir selbst beziehungsweise unser IT-Partner sofort zur Stelle. Meist können wir das Problem intern lösen, nur in Einzelfällen ziehen wir die Silpion IT Service Management GmbH als externen Dienstleister zurate." Im Zuge des MFA-Projekts gab es beispielsweise bisher nur drei minimale Zwischenfälle, dass zum Beispiel ein Anwender keine Push-Benachrichtigung erhalten hat. Die Ursache war dann immer schnell gefunden.

Nachdem die Multifaktor-Authentifizierung bei den eigenen Mitarbeitern so reibungslos angenommen wurde, gibt es bereits erste Überlegungen, künftig auch externen Partnern den auf diese Weise zusätzlich geschützten VPN-Zugang zu ermöglichen – für eine noch effizientere Zusammenarbeit bei gleichzeitigem Sicherheitsgewinn.

Rebecca Horn

CYBER-ATTACKEN STRATEGISCH ANGEHEN

DIE BASIS FÜR EINE FORTLAUFENDE OPTIMIERUNG VON RISIKOMANAGEMENT- UND ENTSCHEIDUNGSPROZESSEN

IT-Security ist ein hohes Gut. Obwohl für viele Unternehmen der Schutz ihrer IT-Infrastruktur, Systeme, Workplaces und Daten oberste Priorität hat, ist ein großer Teil für einen Angriff nicht gewappnet. Das ist fahrlässig und hochriskant zugleich. Von Cyber-Attacken sind Unternehmen jeglicher Größe betroffen. Umso wichtiger ist es, entsprechende Security-Vorkehrungen zu treffen (Prevention) und im Angriffsfall mit den richtigen Erkennungs-, Abwehr- und Bereinigungsmaßnahmen zu reagieren (Detection und Response).

Investitionen in Cyber Security sind sinnvoll

Hacker-Angriffe nehmen seit Jahren rasant zu. Die Motive für solche Attacken sind vielfältig: von Industriespionage bis hin zu erpresserischen Absichten und damit verbundenen Schutzgeldforderungen. Um dem vorzubeugen, haben die meisten Unternehmen definierte IT-Krisenprozesse. Häufig eignen sie sich aber nicht, um einen wirklich ausgefeilten Angriff abzuwehren. Angriffsmethoden, die bisher nur von APTs (Advanced Persistent Threats) bekannt waren, sind nun auch bei gewöhnlichen Cyber-Kriminellen zu beobachten. Die Lage hat sich verschärft – und darauf müssen Unternehmen vorbereitet sein. Denn kommt es zum „Security-Incident", müssen sie ansonsten je nach Art des Vorfalls in kurzer Zeit Maßnahmen einleiten, die oft jahrelang niemand angepackt hat. Im Zweifel ist ihre über Jahre gewachsene IT-Infrastruktur innerhalb weniger Wochen komplett neu zu organisieren. Darum ist es wichtig, nicht erst dann zu reagieren, wenn ein akuter Sicherheitsvorfall dazu zwingt.

Vorbereitung ist alles

Cyber Security ist das Ergebnis eines fortlaufenden Prozesses und darum höchstindividuell. Soll das Security Level langfristig hochgehalten werden, ist Situation Awareness entscheidend. Um auf akute Bedrohungen reagieren zu können, sollten Maßnahmenpakete für verschiedene Angriffs-Szenarien vorab definiert werden. In solchen Plänen sind das Ziel einer Maßnahme, die erforderliche Vorgehensweise und die notwendigen Skills, Rollen und Unternehmensbereiche beschrieben. Auch ein Incident-Response-Kommunikationsplan darf nicht fehlen. Nur so ist es möglich, schnell zu reagieren und die Situation wieder in den Griff bekommen.

Schwachstellen erkennen

Hackern sollte es so schwer wie möglich gemacht werden. Aus beispielsweise Systemdaten eines Unternehmens kann ein Scoring erstellt werden, das Aufschluss über die Kritikalität und etwaige Schwachstellen gibt (Vulnerability Management). Doch auch wenn mögliche Angriffspunkte bekannt sind, gibt es natürlich keine absolute Sicherheit. So ist der umfangreiche Schutz gegen Zero Day Exploit Attacks und APTs sehr aufwändig und nie zu 100 Prozent möglich. Es macht daher Sinn, den ersten Fokus auf einfacher abzuwehrende Bedrohungen zu legen und sich in diesem Kontext gegen groß angelegte Angriffe abzusichern.

Besonders schützenswerte Bereiche definieren

Es ist nicht möglich, ein Fort Knox um die IT zu bauen. Stattdessen müssen sich Unternehmen auf ihre Crown Jewels fokussieren, also auf jene Infrastrukturen, Daten und Systeme, die besonders schützenswert sind. Mit dem MITRE ATT&CK erfährt man, wie man am wahrscheinlichsten angegriffen wird. Es listet alle bekannten Angriffstechniken tagesaktuell auf und erklärt, wie man sie erkennt und mögliche Angriffe behebt. Außerdem ist es wichtig, sich mit der Bedrohungslage in der eigenen Branche zu beschäftigen. Hacker sind zumeist auf bestimmte Branchen und Angriffstechniken spezialisiert. Mit einer Heatmap, die zeigt, welche Technologie wo besonders häufig angewendet wird, können Crown Jewels gezielt geschützt werden.

> INVESTITIONEN IN CYBER SECURITY LOHNEN SICH, WEIL SIE DAS RISIKO EINES KRITISCHEN SECURITY INCIDENTS NACHWEISLICH REDUZIEREN.

Arne Wöhler, Head of Business Consulting and Development Cyber Security, Arvato Systems, www.arvato-systems.de/security

Daten korrelieren

Um einen drohenden Hacker-Angriff zu erkennen, ist Detektivarbeit gefragt. Mit einem EDR-Tool werden Ereignisse auf Endgeräten wie PCs, Notebooks, Tablets und Smartphones aufgezeichnet, zum Beispiel eine Nutzeranmeldung, das Öffnen einer Datei, aufgebaute Netzwerkverbindungen und ähnliches. Laufen diese Meldungen, Alarme und Logfiles verschiedener Geräte, Netzkomponenten, Anwendungen und Security-Systeme in ein SIEM-System, können diese in Echtzeit korreliert und ausgewertet werden. Erkannte Anomalien sind wichtige Indizien für eine akute Bedrohung.

Auf Teamwork setzen

Incident Response funktioniert wie ein Mannschaftssport, bei dem die Spieler ihre Stärken nach abgestimmten Playbooks einbringen. Hier braucht es einen ausgewogenen Mix aus Erfahrung und Fachwissen. Diese Fähigkeiten intern aufzubauen, verursacht großen Aufwand. Einen Dienstleister heranzuziehen, der Managed Security als Service bietet, kann insbesondere für mittelständische Unternehmen eine Überlegung wert sein. Aber auch große Konzerne profitieren von einer derartigen Zusammenarbeit. Falls deren eigenes Team zum Beispiel zu den üblichen Geschäftszeiten monitort, übernimmt der Dienstleister in der Nacht, am Wochenende und an Feiertagen. Oder er leitet die nötigen Response-Maßnahmen ein, wenn Mitarbeiter einen Angriff bemerken. Dabei ist Vertrauen sehr wichtig. Schließlich greift der Dienstleister im Zweifel auf hochsensible Daten zu. Ganz gleich, wie ein Security Team zusammenstellt ist, sind regelmäßige Trainings unverzichtbar, um eine hohe Reaktionsfähigkeit sicherzustellen. Denn bei einem Angriff ist das ganze Security-Team gefragt.

Einrichtung eines SOC

Im Zentrum steht dabei zunächst das Security Operations Center (SOC). Die Mitarbeiter in einem SOC überwachen alle eingehenden Notables beziehungsweise Alarme und bewerten das Gefahrenpotenzial: Handelt es sich tatsächlich um einen kritischen Incident? Oder um ein False Positive? Bei der forensischen Untersuchung des vermeintlichen Vorfalls ermitteln die Experten, wie der Angreifer in die Infrastruktur eindringen konnte, welche Ziele er verfolgt, wie tief er eingedrungen ist und welche technischen Methoden er angewendet hat. Dafür ziehen sie neben Logging-Daten auch Informationen aus dem EDR-System und dem Netzwerk-Monitoring heran und analysieren auffällige Systeme bis in die Tiefe. Meistens liegt das Augenmerk dabei auf dem Active Directory, den besonders schützenswerten Bereichen und dem DMZ.

Schnell und richtig reagieren

Es ist sehr wichtig, dass das SOC bei der Bewertung des Angriffs mit dem Incident Response Team zusammenarbeitet. Handelt es sich um einen massiven Vorfall koordiniert das Incident Response Team die Eindämmungs- und Bereinigungsaktivitäten und führt sie durch. Dabei ist zu entscheiden, welche Handlungen ad hoc vorzunehmen (Containment) und welche vordefinierten Maßnahmenpakete anzuwenden sind. Wichtig ist, die Komplexität des Angriffs, den Aufbau der jeweiligen Infrastruktur, die Monitoring-Fähigkeiten auf Endpoints und Netzwerkverkehr sowie die verfügbaren Analyse-Skills zu berücksichtigen. Schließlich müssen die Abwehr-Maßnahmen den Methoden und Techniken des Angreifers entsprechen.

Angriffe im Nachhinein analysieren

Nach dem Angriff ist vor dem Angriff. Darum ist es unverzichtbar, dass Cyber-Attacken nachbereitet werden. Denn jeder Angriff ist anders, man lernt immer etwas Neues dazu. Nur wenn aus einem Vorkommnis strategische Maßnahmen abgeleitet werden, können Unternehmen eine bessere Reaktionsfähigkeit und Resilienz entwickeln. Übertragen auf den Fußball, geht es um Fragen wie: Passten Spielaufbau und Organisation? Haben die Spieler auf den richtigen Positionen gespielt? Hat die Kommunikation im Team funktioniert? War die Mannschaft mit der nötigen Intensität bei der Sache? War die Visibilität über das Spielgeschehen ausreichend? Diese Fragen immer wieder aufs Neue zu beantworten, bildet die Basis für eine fortlaufende Optimierung von Risikomanagement- und Entscheidungsprozessen.

Arne Wöhler

NACHHALTIGE IT-SICHERHEIT

SECURITY BRAUCHT MEHRERE EBENEN

Eine gute Cyber-Abwehr benötigt jeder. Und mit der richtigen Hilfe kann sich auch jeder angemessen verteidigen. Eine intelligente Endpoint Detection and Response (EDR) beobachtet und bekämpft intelligent und damit handhabbar auch komplexe Attacken. Dazu kommen Rat und Tat durch die Managed-Detection-and-Response-(MDR) Sicherheitsexperten.

Nichts ändert sich so schnell wie die IT-Gefahrenlage. Neue Ransomware und komplexe Angriffe treffen früher oder später jeden. Denn unabhängig von ihrer Größe beherbergen Unternehmen genügend Informationen und intellektuelles Kapital, um ein lohnendes Ziel zu sein. Alternativ werden ihre Systeme Einfallstore für den Sprung der Hacker in die Netze größerer Unternehmen. Eine klassische Prävention kann inzwischen mit den neuen Angriffen nicht mehr Schritt halten.

Zugleich leidet die Abwehr unter Ressourcenmangel. Viele IT-Teams sehen zwar die eingehenden Alarme der Prävention, können aber nicht alle Meldungen mit der notwendigen Geschwindigkeit bearbeiten. Oft wissen sie auch nicht, welche Effekte die Malware hat und welche Maßnahmen sie ergreifen sollen. Denn nicht jeder Administrator ist ein Sicherheitsspezialist.

Intelligente Entscheidungshilfen

Viele Verantwortliche benötigen daher effiziente Hilfe wie EDR. Eine Endpoint Detection and Response ist laut Gartner ein Bündel von Werkzeugen, die sich darauf konzentrieren, verdächtige Aktivitäten und deren Spuren auf Hosts und Endpunkten zu entdecken und zu untersuchen. Sie unterstützt IT- und Sicherheitsteams dabei, gezielte Angriffe zu erkennen und abzuwehren. Zudem schafft sie Transparenz über das Geschehene und seine Auswirkungen – vor, während und nach einer Attacke.

EDR setzt als Stand-Alone-Lösung auf den installierten Präventions- und Endpunktsicherheitstechnologien auf. Sie nutzt zudem sowohl die Daten aus der Telemetrie des Unternehmens als auch die globale Datenbasis eines EDR-Anbieters. So erkennt sie mit Hilfe Künstlicher Intelligenz und Machine Learning Angriffsmuster sowie Verdachtsmomente aus jeder Phase der Kill-Chain eines Angriffs.

Wo ist der Unterschied? Eine reine Endpoint-Security würde etwa einen Workload, der mit anderen Workloads im gleichen Netzwerk kommuniziert, kaum als verdächtig einstufen. Eine EDR warnt aber, dass beide bisher nicht miteinander kommuniziert haben. Sie erkennt außerdem auch verdächtige Aktivitäten im Netz.

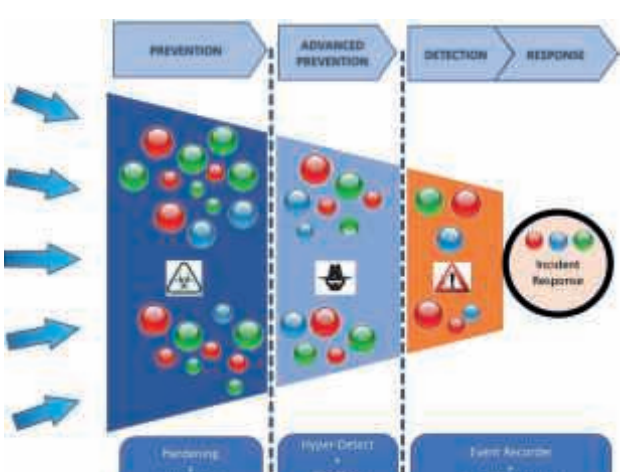
Handlungskompetenz

EDR liefert den Sicherheitsverantwortlichem gefilterte und relevante Informationen. Statt falscher Alarme erhalten IT-Teams visuell verständliche Details samt einschlägiger Ratschläge. In einer Sandbox wird, wenn gewünscht, das zukünftige Verhalten einer Malware simuliert. In der Konsequenz können Administratoren verdächtige Dateien oder Prozesse blockieren, abbrechen und Endpunkte oder Netzbereiche isolieren. Das schneidet lateralen Bewegungen der Angreifer den Weg ab und verhindert auch den Abfluss von Daten.

Nachhaltiger Schutz

Viele Hacker steuern ihre gezielten Angriffe manuell. Dagegen benötigt auch

> OHNE PRÄVENTION FUNKTIONIERT KEINE IT-SICHERHEIT. DOCH OHNE ZUSÄTZLICHE TECHNOLOGIE UND EXPERTISE BLEIBEN DIESE WERKZEUGE WIRKUNGSLOS.
>
> Bogdan Botezatu, Director Threat Research and Reporting, Bitdefender, www.bitdefender.de



Ein integrierter EDR-Ansatz baut auf einer Prävention auf, die die Mehrzahl der Bedrohungen bereits herausfiltert. So bleibt nur noch eine sehr kleine Menge an Ereignissen übrig, die genauer untersucht werden muss.

ein angegriffenes Unternehmen die helfende Hand der Sicherheitsanalysten einer Managed Detection and Response. Im Rahmen eines langfristigen Services analysieren die IT-Abteilung und der Dienstleister zunächst die gesamte IT und erstellen ein individuelles Risikoprofil für das Unternehmen. Sie definieren die normalen Abläufe in einer Organisation. Die Abwehrspezialisten suchen ab dann bei Abweichungen, ob eine böswillige Ursache zugrunde liegt. Ebenso vereinbaren sie, welche Notfallmaßnahmen die Dienstleister ohne Absprache mit der Unternehmens-IT durchführen können.

Zudem bieten erfahrene Sicherheitsanalysten das nötige Maß an Intuition, um die neuen Risiken schneller zu erkennen und zu bekämpfen. Um Fileless Malware oder Living-of-the-Land-Angreifer abzuwehren, denken sich gute Analysten in den Angreifer hinein. So können sie deren Strategie besser nachvollziehen und die nächsten Schritte des Gegners leichter verhindern.

Zukunftssicherheit

Ohne Prävention funktioniert keine IT-Sicherheit. Doch ohne zusätzliche Technologie und Expertise bleiben diese Werkzeuge wirkungslos. EDR und MDR bieten intelligente Hilfe oder den notwendigen menschlichen Expertenrat. Und seine Stand-Alone-EDR kann ein Unternehmen bei einer Migration in die Cloud jederzeit mitnehmen.

Bogdan Botezatu

IT-SECURITY

HACKER MACHEN KEINE PAUSE – SECURITY-INNOVATIONEN ABER AUCH NICHT

Das gilt auch in COVID19-Zeiten. Neben der stetigen Weiterentwicklung bestehender Lösungen ist das Innovationstempo auch in Sachen neuer Produkte ungebrochen.

Beispiele hierfür sind etwa das Security Framework von Build38, das eHealth-Apps sicherer macht oder fraud0, welches in real-time den Ad-Betrug im Online-Marketing verhindert. Beide Made in Germany!

Das eBook bietet 12 Artikel zu allen wesentlichen aktuellen Themen der IT-Security.

Highlights aus dem eBook:

➜ QR-Codes: klein, gemein, hinterhältig

Quick Response, kurz QR, der anderen, unerwünschten Art. Fünf Tipps für den sicheren Umgang, um Schadcode zu vermeiden.

➜ Social Engineering & Awareness-Kampagnen

Bei Assessments fallen neun von zehn Firmen durch. Was hilft gegen die Profi-Attacken der neuen Generation und wie setzt man Kampagnen schnell und effektiv auf?

➜ Reifegradmodelle für die Cybersicherheit

Ein „Cybersecurity Maturity Model" hilft bei der Sicherstellung der Produktivität und Qualität des Unternehmens sowie der Einhaltung der Budget- und Zeitplanung.

Das eBook umfasst 50 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/download

SECURITY BY DEFAULT

STÄRKUNG FÜR DAS INTERNET DER DINGE

Digitalisierung der eigenen Prozesse hat Priorität, sei es in kleinen und mittleren Unternehmen (KMU), bei Konzernen, Global Playern oder Behörden. Für die bessere Kommunikation und Automatisierung von Abläufen setzen viele IT-Abteilungen bereits auf das Internet der Dinge (Internet of Things, IoT). Es erlaubt die Kommunikation zwischen Geräten sowie die digitale Vernetzung und Verarbeitung von Daten. Das kann beispielsweise für schnellere Produktionsabläufe sorgen, oder dabei helfen, wichtige Prozesse selbstständig überwachen zu lassen.

Mit dem breiteren und häufigeren Einsatz von IoT-Geräten vergrößert sich jedoch auch der Sicherheitsanspruch dieser Geräte, genau wie ihre Rolle in der Absicherung des kompletten Unternehmensnetzwerks. Hinzu kommt: Mit der hohen Verfügbarkeit von 5G-Netzwerktechnologie wird diese Entwicklung beschleunigt, da damit noch mehr Datenverkehr in weniger Zeit abgewickelt werden kann. Cyberkriminelle haben bereits reagiert und zielen vermehrt auf Schwachstellen in IoT-Geräten, um Zugang zu Netzwerken zu erlangen. Entsprechend gilt es, frühzeitig zu reagieren und die Sicherheit der IoT-Geräte zu erhöhen.

Charter of Trust fördert Security by Default

Die Mitglieder der Charter of Trust, einer Initiative von Siemens, der Münchner Sicherheitskonferenz und globalen Unternehmen, haben zehn Prinzipien und Basisanforderungen für IT-Sicherheit erarbeitet, um diese in allen Bereichen zu etablieren. ‚Security by Default', also die Absicherung von Produkten ab Werk durch entsprechende Konzeption und Herstellung, spielt dabei eine zentrale Rolle, besonders im Zusammenhang mit IoT. Dabei soll inhärente Absicherung durch Standards, Best Practices und objektive Überprüfungen zu einem Kern-Element von IoT-Geräten werden. Zusätzlich sollen allgemeingültige Standards entwickelt werden, die Sicherheit global prüf- und verifizierbar machen. Voraussetzung dafür ist es, kritische Anforderungen zu definieren, um sichere Produkte, Prozesse, Dienstleistungen und Geschäftsmodelle, in Übereinstimmung mit den entsprechenden Standards und Best Practices, zu bauen.

Der Weg zu ‚Security by Default' beinhaltet drei zentrale Aspekte:

- **Aspekt 1:** Produkte, Funktionalitäten und Technologie.
- **Aspekt 2:** Prozesse, Abläufe und Architektur.
- **Aspekt 3:** Gemeinsame Nutzung von Best Practices.

Dabei reicht es allerdings nicht, das Prinzip nur auf der Ebene der Produkte oder Technologie umzusetzen. Es gilt, einen umfassenden Ansatz zu verfolgen, der Prozesse, Abläufe und Infrastrukturen hinter Produkt und Technologie einbezieht. Die 17 Mitgliedsunternehmen der Charter of Trust haben sich verpflichtet, das Prinzip ‚Security by Default' in ihrer eigenen Organisation zu etablieren und mit gutem Beispiel voranzugehen.

Normen und Standards erhöhen Sicherheit

Steigende Anzahl von Homeoffice-Arbeitsplätzen, dezentrale Unternehmenskonzepte und ein hoher Grad an Automatisierung: Das geht Hand-in-Hand mit den steigenden Anforderungen an die Sicherheit von IoT-Geräten. Standards und Best-Practices, die schon bei der Konzeption von Produkten und Geräten beachtet werden, helfen dabei, Sicherheit „ab Werk" zu gewährleisten und die potenzielle Angriffsfläche für Hacker signifikant zu verringern. Einheitliche Standards und Normen innerhalb der Europäischen Union würden ebenfalls wesentlich zu mehr Sicherheit beitragen. Auf dieser Basis können unabhängige Prüforganisationen dann Zertifikate erteilen, die als Gütesiegel fungieren und somit für mehr Transparenz im Markt sorgen.

Sudhir Ethiraj

EINHEITLICHE STANDARDS UND NORMEN INNERHALB DER EUROPÄISCHEN UNION WÜRDEN WESENTLICH ZU MEHR SICHERHEIT BEITRAGEN.

Sudhir Ethiraj,
Global Head of Cybersecurity Office (CSO),
TÜV SÜD, www.tuvsud.de

SECURITY AWARENESS

TRAININGS ALS SAAS-LÖSUNG

Security Awareness Trainings anbieten ohne eigenes Fachpersonal? Der MSSP und Systemhauspartner Network Box sensibilisiert Mitarbeiter für den richtigen Umgang mit E-Mails und vertraulichen Daten und entwickelt ganzheitliche und nachhaltige IT-Sicherheitskonzepte als SaaS-Lösung für jede Unternehmensgröße.

Phishing Simulation
In Absprache mit dem Kunden versendet Network Box Werbe-Emails und auf Wunsch individuell gestaltete E-Mails (CEO-Fraud) mit gefälschten Inhalten an die Mitarbeiter. Im Anschluss erstellt der IT-Sicherheitsexperte anonymisierte Auswertungen mit den Ergebnissen und gibt Handlungsempfehlungen.

eLearnings
Die eigens entwickelte eLearning-Plattform bietet Schulungsvideos und interaktive Awareness Präsentationen zu aktuellen Bedrohungen und Themen wie Sicherheit am Arbeitsplatz, Home Office Awareness, Social Engineering und Passwortschutz. Teilnahmezertifikate dienen als Nachweis im Rahmen der DSGVO und anderen Zertifizierungsstandards wie ISO27001 oder ISMS.

Awareness-Newsletter
Der monatliche Awareness-Newsletter informiert die Mitarbeiter über aktuelle Bedrohungslagen und Themen zur Informationssicherheit und gibt wertvolle Tipps zu IT-Sicherheit und Datenschutz. Abgerundet wird das Konzept durch Materialien am Arbeitsplatz.

Security Awareness Konzept
Network Box entwickelt individuelle Strategien zur nachhaltigen IT-Sicherheit. Die ganzheitlich gemanagten Security Awareness Trainings sind als einmalige Kampagne oder monatlich kündbare Pakete buchbar.

NETWORK BOX

www.network-box.eu

VERTRAUEN ALS SICHERHEITSRISIKO

ZERO TRUST FÜR MENSCHLICHE UND MASCHINELLE IDENTITÄTEN

Durch die verstärkte Remote-Arbeit sind IT-Administratoren, Sicherheitsteams und reguläre Mitarbeiter aktuell in hohem Maße auf den Fernzugriff auf Unternehmenssysteme, DevOps-Umgebungen und Anwendungen angewiesen. Hierdurch steht Bedrohungsakteuren eine wesentlich größere Angriffsfläche zur Verfügung.

Digitale Identitäten haben sich dabei als die Waffe der Wahl für Cyberkriminelle herausgestellt. Verwenden privilegierte Benutzer eines Unternehmens routinemäßig gemeinsam genutzte privilegierte Konten für den Zugriff – insbesondere aus der Ferne über ein VPN – hat jeder Angreifer, der diese Anmeldedaten kompromittiert, im schlimmsten Fall weitreichenden Zugang zu unternehmenskritischen Daten und Ressourcen. Überdies sind nicht nur privilegierte Benutzer gefährdet. Viele Cyberangriffe zielen auf reguläre Mitarbeiterkonten ab, um sie als Ausgangspunkt zur Auskundschaftung des Netzwerks zu nutzen.

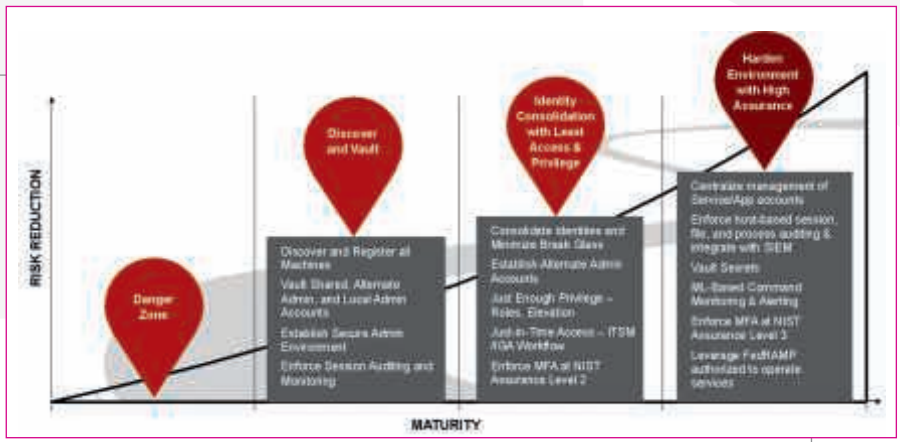
Vor diesem Hintergrund sollten Unternehmen die Auswirkungen einer dezentralen Belegschaft, externen Auftragnehmern und der wachsenden Angriffsfläche durch eine stark verteilte IT-Infrastruktur überprüfen und die Implementierung neuer Zero-Trust-Strategien in Erwägung ziehen, um besser auf diese neue Dynamik reagieren zu können.

Zero-Trust-Strategie

Beim Zero-Trust-Modell wird keinem Akteur, der Zugriff auf sensible Daten, Anwendungen oder Infrastrukturen des Unternehmens anfordert, von vornherein vertraut. Die Sicherheitsmaßnahmen sollten jedoch nicht bei Identitäten menschlicher Benutzer aufhören. Nicht-menschliche Identitäten und Service-Accounts für Maschinen, Anwendungen und andere Workloads stellen in vielen Unternehmen zunehmend die Mehrheit der „Benutzer" dar. Dies gilt insbesondere in Cloud- und DevOps-Umgebungen, in denen Entwickler-Tools, containerisierte Anwendungen, Microservices und elastische Workloads – die alle Identitäten benötigen, um miteinander zu kommunizieren – eine dominante Rolle spielen. Um ihre identitätsbasierte Sicherheitsposition zu verbessern, sollten Unternehmen deshalb auf das Management privilegierter Zugriffsberechtigungen, basierend auf einem Zero-Trust-Ansatz konzentrieren.

Zero-Trust-Sicherheit durch PAM

Der traditionelle Netzwerkperimeter löst sich auf, da Benutzer und IT-Ressourcen immer mehr örtlich verteilt sind. Daher ist es nicht mehr praktikabel, Zugriffsentscheidungen auf simplen Konzepten wie „vertrauenswürdige Benutzer befinden sich innerhalb des Perimeters und nicht vertrauenswürdige Benutzer außerhalb" zu fällen und IP-Adressen für diese Unterscheidung zu verwenden. Unternehmen müssen davon ausgehen, dass sich Bedrohungsakteure bereits innerhalb ihrer Systeme befinden. Aus dem veralteten „Vertraue, aber überprüfe"-Ansatz muss „Vertraue nie, überprüfe immer" werden.



Das Zero Trust PAM Maturity Modell

„Vertraue nie" bedeutet, dass legitime Administratoren keinen Freibrief mehr für den Zugriff auf privilegierte Konten haben. Das heißt, anstatt freigegebene privilegierte Konten wie Root und Lokaler Administrator nach Belieben zu nutzen, verwenden Admins ihr von der Personalabteilung geprüftes Unternehmenskonto, das über grundlegende Rechte verfügt. Dies verhindert schwerwiegende Fehler und reduziert die Auswirkungen, falls ein Angreifer dieses Konto kompromittiert. Die PAM-Sicherheitskontrollen können dann selektiv erhöhte Privilegien gewähren, wenn es die Situation erfordert, ba-

sierend auf zentralisierten Rollen und Richtlinien. Anstatt dass Identitäten ständig über umfassende Berechtigungen verfügen, reduziert dieser Least-Privilege-Ansatz das Sicherheitsrisiko, während er es legitimen Administratoren weiterhin ermöglicht, ihre Arbeit zu erledigen, indem sie gerade genug Privilegien anfordern, just-in-time und für eine begrenzten Zeitraum. Um einen effektiven Schutz sicherzustellen, müssen Unternehmen diesen Ansatz konsequent auf alle IT-Ressourcen anwenden, egal ob im Rechenzentrum, in der Demilitarisierten Zone (DMZ), der Virtual Private Cloud oder in Multi-Cloud-Umgebungen.

> DIE STEIGENDE ZAHL ERFOLGREICHER CYBERANGRIFFE ZEIGT, DASS TRADITIONELLE PERIMETERBASIERTE SICHERHEITSKONZEPTE NICHT MEHR AUSREICHEN.
>
> Özkan Topal, Sales Director, ThycoticCentrify, www.centrify.com

Durch die Implementierung dieses Zero-Trust-Ansatzes für PAM mittels Least-Privilege-Zugriffskontrollen minimieren Unternehmen ihre Angriffsfläche, verbessern die Audit- und Compliance-Transparenz und reduzieren Risiken, Komplexität und Kosten.

Erste wichtige Schritte

PAM ist eine vielschichtige Technologie, jedoch können Unternehmen bereits mit einigen wenigen Grundlagen erhebliche Sicherheitsfortschritte erzielen und ihren Zero-Trust-Reifegrad kontinuierlich verbessern, indem sie sukzessive fortgeschrittenere Funktionen implementieren. Erste wichtige Schritte sind eine verbesserte Passworthygiene, die Sicherung gemeinsam genutzter privilegierter Konten und die Durchsetzung von Multi-Faktor-Authentifizierung (MFA) für Administratoren.

1. Gute Passwort-Hygiene für menschliche und maschinelle Identitäten

Ein einziges kompromittiertes Passwort kann potenziell das gesamte Unternehmen schädigen. Passwörter mit hoher Entropie, die schwer zu knacken sind, sind daher unerlässlich. Häufige Passwort-Rotationen reduzieren zudem das Zeitfenster für potenzielle Angreifer. Dies ist auch für die nicht-menschlichen Konten wichtig. Sie werden selten gewechselt, aus Angst, eine Anwendung oder einen Dienst zu beschädigen. Mithilfe von PAM können diese Konten zentral verwaltet und eine häufige Rotationsrichtlinie angewendet werden. Dabei können diese Lösungen eine Multiplexed-Account-Funktion nutzen, um sicherzustellen, dass das Passwort vor der Rotation auf allen abhängigen Computern synchronisiert wird, um das Risiko eines Anwendungsausfalls zu mindern.

Da der Mensch immer noch das schwächste Glied in der Sicherheitskette ist und deshalb eines der Hauptziele für Angreifer darstellt, sollten kontinuierliche Sicherheitsschulungen für alle Benutzer obligatorisch sein, nicht nur für Administratoren.

2. Multi-Faktor-Authentifizierung für Administratoren

Ein weiterer konkreter Schritt, um die Identitätssicherheit zu stärken, ist die Implementierung von Multi-Faktor-Authentifizierung für alle Administratoren. Auch für Angreifer ist Zeit Geld. Daher können zusätzliche Sicherheitshürden wie MFA einen Angreifer dazu veranlassen, einfach zum nächsten potenziellen Opfer weiterzuziehen.

Die Verwendung eines physischen Authentifikators (YubiKey, Push-Benachrichtigung oder integrierte biometrische Daten wie Apple Touch ID) als zweiten Faktor stellt eine sehr hohe Hürde für Angreifer dar. Diese Maßnahme stoppt auch Bots oder Malware. Eine konsequente Anwendung von MFA an mehreren Zugangspunkten ist unerlässlich.

3. Passwort-Vaulting

Identitäten mit permanenten Berechtigungen bergen ein erhebliches Sicherheitsrisiko. Insbesondere Linux-Systeme sind eine große Quelle für lokale privilegierte Konten. Die beste Methode ist, so viele dieser Konten wie möglich zu eliminieren. Die Konten, die ein Unternehmen nicht eliminieren kann, sollten in einem Passwort-Vault aufbewahrt und der Zugriff darauf nur auf Notfälle beschränkt werden. Diese beiden Maßnahmen reduzieren die Angriffsfläche bereits erheblich. Im nächsten Schritt sollten Administratoren nur die Berechtigungen erhalten, die sie auch benötigen, und zwar just-in-time, wenn sie sie brauchen.

Die steigende Zahl erfolgreicher Cyberangriffe zeigt, dass traditionelle perimeterbasierte Sicherheitskonzepte nicht mehr ausreichen. Denn ist dieser Schutzwall erst einmal überwunden, haben Kriminelle zumeist leichtes Spiel. Unternehmen müssen davon ausgehen, dass sich Angreifer bereits in ihren Netzwerken befinden, und ihre Sicherheitsmaßnahmen auf dieser Annahme aufbauen. Nur so können alle Assets und sensiblen Daten eines Unternehmens geschützt und Schäden durch externe Angriffe und Insider-Bedrohungen minimiert werden.

Özkan Topal

IM FOKUS DES CYBERCRIMES

NEUE STUDIE ZUR SAP-SICHERHEIT

Geschäftskritische SAP-Systeme geraten zunehmend ins Visier von Cyberkriminellen mit tiefem SAP-Know-how. Dies haben der Cybersicherheitsanbieter Onapsis und SAP bei einer globalen Bedrohungsanalyse festgestellt.

Die Angreifer gezielt anzulocken und dann zu beobachten, welche Techniken und Verfahren sie nutzen, um Zugriff auf ein SAP-System zu erhalten: Dies war das Ziel des gemeinsamen „Threat Intelligence Reports" von Onapsis und SAP. Dazu wurden mehrere weltweit verteilte SAP-Systeme absichtlich mit Schwachstellen versehen und im Internet zugänglich gemacht. Diese wurden mehrere Monate lang rund um die Uhr beobachtet wobei sich alarmierende Erkenntnisse zur aktuellen SAP-Bedrohungslage heraus kristallisierten.

Insgesamt wurden mehr als 300 erfolgreiche Angriffe registriert, die sich ungepatchte SAP-Sicherheitslücken und fehlerhafte Systemeinstellungen zunutze machten. Vielfach ließ das Vorgehen der Täter eindeutig auf umfassendes SAP-Wissen schließen. So gelang es einigen Angreifern, vorhandene SAP-Schwachstellen auszunutzen, ohne dass bereits ein zugehöriger Public Exploit verfügbar war. Manche Angreifer legten ein erschreckendes Tempo vor. So gab es Fälle, in denen das Zeitfenster zwischen der Veröffentlichung eines SAP-Sicherheitspatches und der Ausnutzung der zugehörigen Schwachstelle gerade einmal 72 Stunden betrug.

Den Threat Intelligence Report kann hier kostenlos heruntergeladen werden:

https://bit.ly/3p8isHW

Angesichts der wachsenden SAP-Bedrohungslage raten die Onapsis- und SAP-Sicherheitsexperten den Unternehmen dringend zu folgenden Schutzmaßnahmen:

- Systematisches SAP-Patchmanagement
- Automatische Gefährdungsanalysen
- Zeitnahe SAP-Sicherheitskontrollen

www.onapsis.com

APPLIKATIONSKONTROLLE

WHITELISTING ALS EFFEKTIVSTER SCHUTZ

Die Anwendungskontrolle ist ein wesentlicher Bestandteil der Endgerätesicherheit und Herausforderung, bei der die Sicherheitsrichtlinien auf der einen und Benutzeranforderungen in einer Büroumgebung auf der anderen Seite normalerweise nicht harmonieren. Zur Vermeidung von Konflikten in Bezug auf Lizenzierung und Regelkonformität sowie aus Sicherheitsgründen blockieren einige IT-Abteilungen die Endgeräte für die Installation neuer Software oder Updates vollständig. Dies kann für die Benutzer sehr ärgerlich sein, da unkritische, aber nützliche Tools unter Umständen nicht installiert werden und somit ein effizientes Arbeiten behindern. Darüber hinaus können zahlreiche Anfragen für die Installation bestimmter Anwendungen schnell zu einer Überlastung des IT-Supports führen. Dasselbe gilt im industriellen Umfeld für zeitkritische Updates. Eine vollständige Sperrung ist daher in vielen Fällen ineffizient, so dass geeignete flexible Verfahren mit Ausnahmebehandlungsmechanismen gefunden werden müssen.

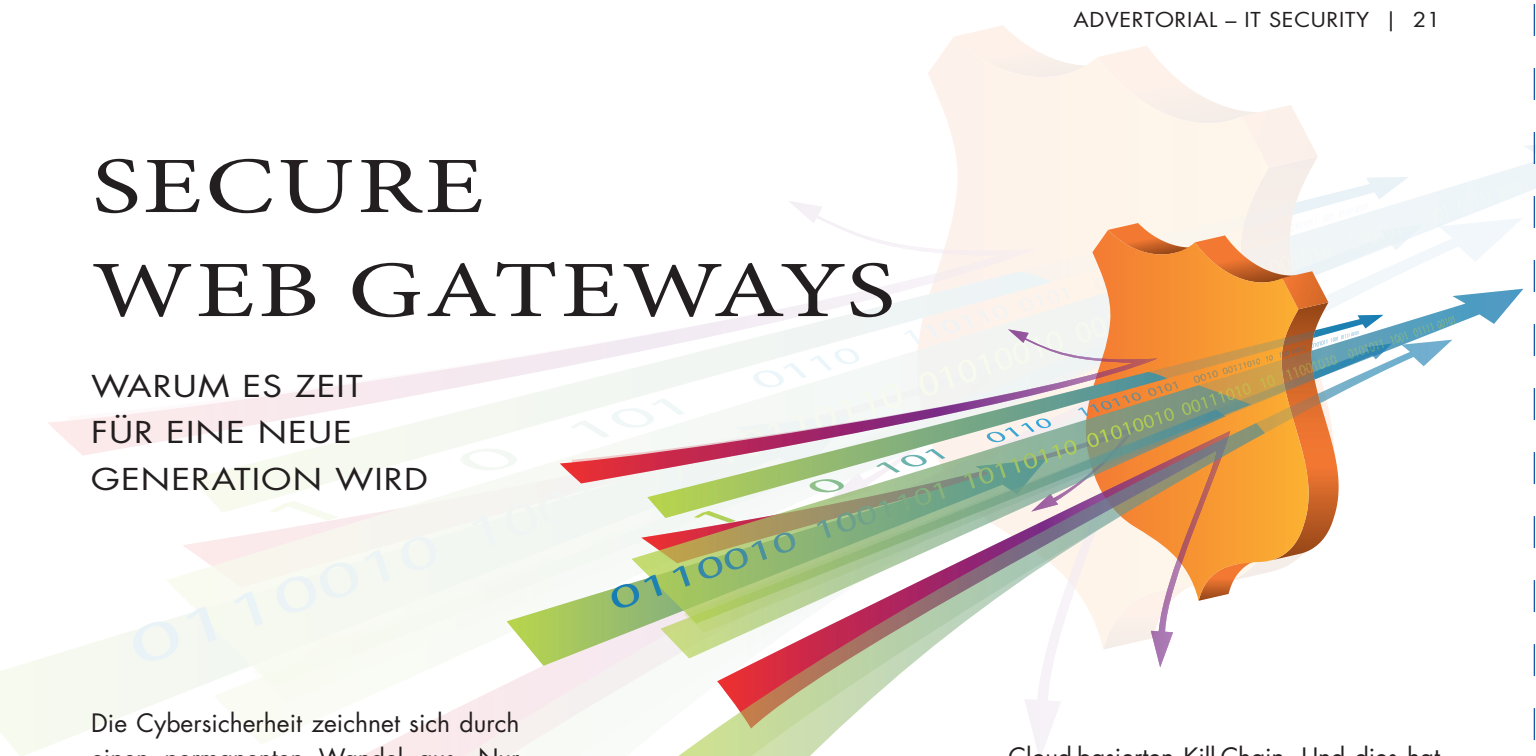
WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 13 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/download

SECURE WEB GATEWAYS

WARUM ES ZEIT FÜR EINE NEUE GENERATION WIRD



Die Cybersicherheit zeichnet sich durch einen permanenten Wandel aus. Nur wer seine Security-Strategie ständig hinterfragt und gegebenenfalls anpasst, kann die Sicherheit seiner Systeme, Daten und Nutzer sicherstellen. Noch vor wenigen Jahren galten Secure Web Gateways (SWG) mit ihren regionalen Web-Filterlisten, dem Einsatz von ICAP zum Schutz von Dateien vor Bedrohungen, Caching von Web-Objekten und Scripting-Richtlinien zum Herausfiltern unerwünschter Web-Objekte als State-of-the-Art-Lösung für den Web-Traffic. Doch die Zeiten haben sich – nicht zuletzt aufgrund der zunehmenden Verbreitung und Nutzung der Cloud – geändert.

Dies gilt insbesondere für den Web-Traffic: Heute entfallen mehr als die Hälfte der Verbindungen auf Apps und Cloud-Dienste. Der Netskope Cloud & Threat Report hat gezeigt, dass knapp 90 Prozent der Nutzer täglich in der Cloud arbeiten. Zudem hat sich die durchschnittliche Anzahl der in Unternehmen genutzten Apps von 1.295 im Jahr 2019 auf 2.415 im Jahr 2020 fast verdoppelt. Der Webverkehr besteht also längst nicht mehr nur aus der Nutzung von Websites. Berücksichtigt man noch die zunehmende Arbeit von zu Hause aus, die Nutzung von Collaboration-Tools und den projektübergreifenden Austausch von Daten zwischen Mitarbeitern, Partnern und Kunden, wird deutlich, dass der Web- und Cloud-Verkehr mittlerweile ein fließender Datenstrom ist.

Single-Pass-Cloud-Security-Edge

Die Umstellung von traditionellen SWG-Appliances auf Cloud-basierte SWG-Lösungen ermöglicht Vorteile bei der Netzwerk- und Sicherheitstransformation, Kosteneinsparungen und eine geringere Komplexität. Diese Verlagerung löst jedoch nicht die Schatten-IT-Risiken und lässt sowohl App- als auch Datentransformationen in die Cloud außer Acht. Die Bewältigung dieser Herausforderungen erfordert eine neue Generation von SWGs: einen Single-Pass-Cloud-Security-Edge, der den kompletten Web- und Cloud-Datenverkehr analysiert, einschließlich Schatten-IT-Apps, Datenrisiken und Cloud-basierten Bedrohungen.

Herkömmliche Cloud-basierte SWGs bieten zwar fortschrittliche Funktionen für Sandboxing, neue ML-basierte Modelle für die Erkennung von Bedrohungen und Remote Browser Isolation (RBI) für nicht kategorisierte und gefährliche Websites. Allerdings sind sie blind gegenüber Cloud-Phishing, der Bereitstellung von Cloud-Malware sowie der gesamten Cloud-basierten Kill-Chain. Und dies hat gravierende Folgen: In den Phishing Trend Reports der Anti-Phishing Working Group belegen Angriffe auf SaaS/Webmail seit Jahren den ersten Platz. Und gemäß dem aktuellen Cloud & Threat Report stammen 63 Prozent der Malware aus der Cloud. Cloud-Apps sind mittlerweile das Ziel von jeder dritten (36 %) Phishing-Kampagne. Während die Mehrzahl der Phishing-Köder noch auf herkömmlichen Websites gehostet wird, nutzen Angreifer jedoch zunehmend Cloud-Apps, um in Unternehmen Fuß zu fassen. Es ist offensichtlich, das herkömmliche SWGs viele Lücken in Bezug auf Transparenz und Kontrolle aufweisen. Und diese Lücken werden größer, je mehr Unternehmen auf die Cloud setzen oder gar eine Cloud-First-Umgebung einführen.

Die nächste Generation von SWGs muss also ein Secure Web und Cloud Gateway sein, das in der Lage ist, sämtlichen Traffic zu erkennen und zu analysieren, egal ob der Zugriff auf Cloud-Dienste, Websites oder private Anwendungen erfolgt. Die Bedrohungen haben sich gewandelt. Höchste Zeit, dass sich die Sicherheitsansätze der Unternehmen hieran anpassen.

www.netskope.com

netskope

IT-SICHERHEIT

COVID-19 UND DIE DEUTSCHEN KMU

Hat die Pandemie durch Homeoffice, Videokonferenzen und unsicher Netze die IT-Sicherheit beeinträchtigt? Oder haben deutsche KMU notgedrungen massiv in IT-Security investiert?

Eine aktuelle Studie von Capterra liefert einige Antworten.
www.capterra.com.de

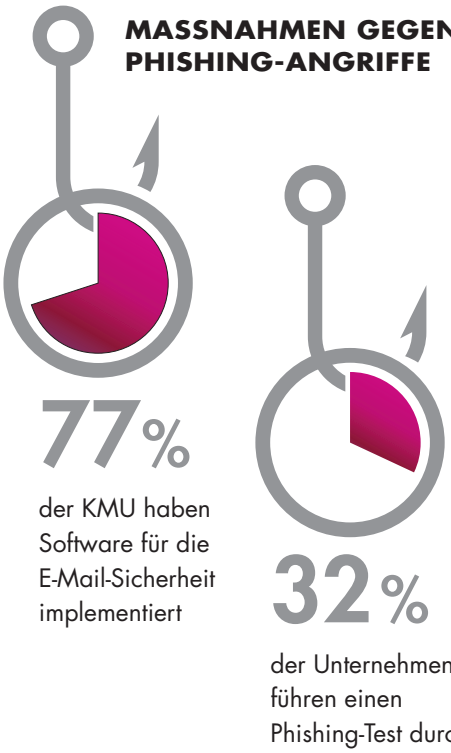
COVID-19 UND DIE IT-SICHERHEIT

44 % der Unternehmen haben während der Krise mehr Phishing-E-Mails als gewöhnlich erhalten

44 % der Unternehmen waren bereits Opfer eines Cyberangriffs

47 % investieren aufgrund von Covid-19 mehr in IT-Sicherheit

MASSNAHMEN GEGEN PHISHING-ANGRIFFE



77 % der KMU haben Software für die E-Mail-Sicherheit implementiert

32 % der Unternehmen führen einen Phishing-Test durch

DIE GRÖSSTEN IT-BEDROHUNGEN 2020

56 % E-Mail-Phishing

39 % Leichtsinn von Endnutzern

38 % Attacken mit Erpresser-Software

„IT SECURITY MADE EASY“

MEHR SCHUB FÜR NATIVE SECURITY-TOOLS

BitLocker Festplattenverschlüsselung, Defender Antivirus und die klassische Firewall gehören zu einem Set an nativen Security Lösungen, die Microsoft seinen Kunden kostenfrei zur Verfügung stellt. Für viele Unternehmen sind diese fester Bestandteil ihrer IT Sicherheitsstrategie: Jede weitere Sicherheitslösung bedeutet eine Hürde mehr, die ein Angreifer nehmen muss. Ziel ist es, Cyberkriminellen ihre Arbeit so schwer wie möglich zu machen.

Mit der Zunahme an Security Tools steigt die Komplexität für Administratoren und Sicherheitsverantwortliche: Sicherheitsrichtlinien, Profile und Berechtigungen müssen verwaltet werden. Anders gesagt: Je mehr Tools, Endgeräte und User desto komplizierter wird es.

Unter der Devise „IT Security made easy“ hat sich der Endpoint Security Spezialist DriveLock zum Ziel gesetzt, mehr aus den nativen Security-Tools herauszuholen. Der Anbieter optimiert deren Verwaltung 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 aber nicht nur das Management der nativen Security Lösungen, sondern ergänzt sie auch um wichtige Funktionen, so zum Beispiel die BitLocker Festplattenverschlüsselung: DriveLock ermöglicht eine zentrale, vom Active Directory (AD) unabhängige Konfiguration – auch für Rechner ohne AD-Anbindung und bietet eine eigene BitLocker Pre-Boot Authentication.

Mit DriveLock verleihen Sie Ihren Microsoft Security Tools den richtigen Schub! Erfahren Sie mehr unter ***www.drivelock.de/native-security-management***

DIGITALE TRANSFORMATION

ERFOLGREICH VERNETZTE MITARBEITER SICHERN WETTBEWERBSVORTEILE

2020 hat gezeigt, wie dringend die digitale Transformation im Bereich gewerblicher Mitarbeitender ist. Und dass sie über die richtigen Werkzeuge verfügen müssen, um ihre Arbeit bestmöglich zu erledigen. Diese Mitarbeitergruppe konnte nicht ins sichere Homeoffice und litt weiterhin unter schlechter Vernetzung. Die Folge waren uninformierte, demotivierte oder gar verängstigte Beschäftigte. Der zu erwartende Aufschwung im Jahr 2021 ermutigt Firmenleitungen jetzt dazu, entsprechende Maßnahmen zu ergreifen. Doch die meisten wissen noch nicht, wie sie ihre Belegschaft auf dem Weg der Digitalisierung mitnehmen können.

Das Buch „Digitale Transformation der Frontline“ zeichnet für Führungskräfte eine klare Roadmap zur Verbesserung ihrer Betriebsabläufe. Sie finden zudem Beispiele und Ratschläge, die bei der Umstrukturierung traditioneller Ansätze für Effizienz, Digitalisierung und Mitarbeitereinbindung helfen. Cristian Grossmann schildert Fallstudien, Beispiele und Erkenntnisse aus der Praxis, um wichtige Themen der Digitalisierung anzusprechen.

Digitale Transformation der Frontline: Wie Sie Ihre Mitarbeiter in Service und Produktion zum größten Wettbewerbsvorteil machen; Independently published; 05-2021

IDENTITY ACCESS MANAGEMENT AGIL

VON DER MIDDLEWARE ZUM ERFOLGSGARANTEN – IAM-SYSTEME IM WANDEL

Die Domänen Identity and Access Management (IAM) und Identity and Access Governance (IAG) in modernen Unternehmen unterliegen einem stetigen Wandel. IAM/IAG-Systeme werden klassischerweise hauptsächlich als Middleware eingesetzt, die eine technische Synchronisation von Identitäts- und Berechtigungsdaten aller relevanten Systeme erlauben und eine zentrale Administrationsoberfläche für die Verwaltung bieten. Jedoch steigen im heutigen agilen Geschäftsumfeld die Anforderungen an solche Systeme. IAM wird von Unternehmen nicht mehr nur als Disziplin wahrgenommen, mithilfe derer klassische Joiner-/Mover-/Leaver Prozesse realisiert und Richtlinien und Regeln ohne große Nutzerinteraktion umgesetzt. Vielmehr wird IAM als One-Stop-Shop für alle Anwender einer Organisation verstanden, um Ihnen verschiedenste Möglichkeiten zu bieten in den Prozessen mitzuwirken. Die technische Basis ist weiterhin die Grundvoraussetzung für erfolgreiches IAM. Die Weiterentwicklung von Governance-Strukturen innerhalb der Unternehmen, die Verankerung der Verantwortlichkeit über Daten innerhalb von Fachbereichen und die stärker geforderte aktive Mitarbeit der Business Units an der Berechtigungsvergabe stellen aber neue und andere Anforderungen an das IAM. Während der Anwenderkreis des IAMs sich früher hauptsächlich auf IT und IT-affine Anwender fokussierte, sind heute fast alle Mitarbeiter eines Unternehmens zur aktiven Beteiligung und Verantwortungsübernahme im Identitäts- und Berechtigungsmanagement gefordert. Abteilungsleiter sollen neue externe Kollegen über das IAM onboarden, Geschäftsrollenverantwortliche ihre Rollenzusammenstellungen prüfen und Anwendungssystemverantwortliche die Zuweisung von kritischen Berechtigungen ihres Systems genehmigen. Meist kommt erschwerend hinzu, dass IAM als Disziplin wahrgenommen wird, die nur von einer zentralen und meist monolithischen Lösung zu meistern ist. Insbesondere bei größeren Unternehmen treten Performance- und Flexibilitätsprobleme zusammen mit hohen Kosten auf, wenn neue Anforderungen innerhalb dieses Kosmos realisiert werden sollen. In den letzten Jahren zeigt sich aber, dass IAM als Gesamtheit eher aus einzelnen, zielgerichteten und leicht anpassbaren Modulen besteht, die möglichst flexibel und dynamisch zusammenarbeiten müssen, um das Portfolio an Diensten schnell und einfach bereitzustellen.

NEBEN DER TECHNISCHEN UMSETZUNG IST DER ORGANISATORISCHE WANDEL UND DIE AUSRICHTUNG DES IAM-TEAMS EIN WICHTIGER ERFOLGSFAKTOR, UM VON DEN BENEFITS EINER DEZENTRALEN IAM-STRUKTUR ZU PROFITIEREN.

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

IAM-Self-Services – Development Kit als Voraussetzung

Insbesondere die Bereitstellung von Self-Services für Fachbereiche und Endanwender gewinnt an stetiger Bedeutung und wird als Aushängeschild eines modernen IAM wahrgenommen. Einen Self-Service charakterisiert hierbei, dass er eine isolierte und reduzierte IAM-Funktionalität für einen gewissen Personenkreis zur Verfügung stellt. Beispiele solcher Services sind u.a. Berechtigungs- und Geschäftsrollenanträge durch den Empfänger, Rollenveränderungsanträge innerhalb des bestehenden Geschäftsrollenmodells oder die selbst-initiierte Rezertifizierung durch Verantwortliche. Neben den Services bedingt die immer stärker notwendige Mitarbeit des Fachbereichs auch deutlich gestiegene Herausforderungen an die Transparenz der im IAM verankerten Informationen, um dem Endanwender immer die individuell korrekten und notwendigen Daten anzuzeigen.

Um diesen Anforderungen agile Lösungen für einzelne solcher Endbenutzer und deren Interaktionswünsche zu präsentieren, bieten IAM-Tools verschiedene Lösungsansätze. Der erfolgversprechendste Lösungsansatz zeigt sich in der Einfüh-

rung und Bereitstellung eines IAM Development Kits, das verschiedenste Werkzeuge für den schnellen Aufbau und Einsatz von IAM- Services bietet. Ein solches Development Kit, wie es beispielsweise die Identity Analytics & Governance Plattform NEXIS 4 bietet, besteht typischerweise aus den folgenden Komponenten:

1. Konfigurierbare UI/UX:

Das Frontend als wichtigste Interaktionskomponente für die Zielgruppe muss schnell und leicht anpassbar sein. Klassische Ansätze, die Interfaces per HTML oder webbasierten Entwicklungsmethoden zu erstellen, erweisen sich als zu langsam, um mit den erforderlichen Fachbereichsanforderungen Schritt zu halten. Ein Baukastensystem, das eine individuelle, schnelle und rein konfigurative Aufbereitung des Interfaces für den Fachbereich erlaubt, ist hier unabdingbar. Ein modernes Development Kit bringt eine Vielzahl an konfigurierbaren UI-Elementen mit, die trotzdem Best-Practices folgen und standardisiert einzusetzen sind.

2. Dynamisches Formularmanagement:

Formulare und Anträge stellen eine bedeutende Basis für viele Self-Services dar. Anwender müssen Formulare mit Informationen aus bestehenden Live-Daten in ihrem jeweiligen Kontext bestücken können. So muss beispielsweise ein Rollenverantwortlicher, der die Stammdaten seiner Rolle editieren möchte, ein Formular zu seiner Rolle einsehen dürfen das nur für ihn relevante Daten enthält und eine fehlerfreie Bearbeitung zulässt. Gültige Wertelisten für Attribute der Rolle sowie Referenzen auf andere Objekte, etwa um Genehmiger festzulegen, müssen schnell und einfach in der Formularkonfiguration zur Verfügung gestellt werden können. Über die Formulare werden wichtige Kontextinformationen für alle weiteren Workflow-Schritte erhoben, die von verschiedenen Stakeholdern durchlaufen werden müssen.

3. Moderne IAM-Workflow-Engine:

Eine template-basierte Workflow-Engine, die eine Vielzahl typischer IAM-relevanter Konfigurationen erlaubt, ist unabdingbar für den schnellen Einsatz von IAM-Services. Beispielsweise darf keine aufwändige Programmierung notwendig sein, um das 4-Augen-Prinzip in einem Workflow zu erzwingen, um SOD-Prüfungen bei Anträgen vollautomatisiert im Hintergrund durchzuführen, oder um Best-Practice-Delegationsketten (an den Vorgesetzten oder den Dateneigentümer) zu realisieren. Traditionelle IAM-Workflow-Engines erfordern meist tiefes technisches Verständnis und Programmierarbeit, so dass meist nur ein recht kleiner Personenkreis Änderungsanforderungen umsetzen kann.

4. Individuelle Stakeholder-Konfiguration:

Services für Endanwender müssen den verschiedenen Stakeholdern individuell präsentiert werden. Innerhalb der Services müssen Daten dynamisch und kontextbasiert geladen und angezeigt werden. Rollenverantwortliche dürfen beispielsweise nur die von ihnen verantworteten Rollen einsehen und Änderungsanträge für diese Rollen starten. Die Individualisierung von Services bedingt bei klassischen IAM-Systemen schwerfällige und oft programmatische Anpassungsarbeiten. Ein IAM-Service Development Kit stellt im Auslieferungszustand bereits Templates nach dem Baukastenprinzip und leicht konfigurierbare Möglichkeiten zur Verfügung.

Rapid Prototyping von IAM-Services

Die Projekterfahrung zeigt, dass insbesondere die Bereitstellung der genannten Self-Services im IAM durch Unterstützung von agilen Entwicklungsmethoden gut umzusetzen ist. Unter Zuhilfenahme eines template-basierten und leicht bedienbaren Development Kits, können gemeinsam mit dem Fachbereich in iterativen Entwicklungszyklen und ohne viel IT-Know-how neue IAM-Services angeboten werden. Ein typischer Entwicklungsprozess eines solchen IAM-Services sieht wie in Bild 1 aus.

Zunächst formuliert der Fachbereich beziehungsweise Adressat des Services

Bild 1: Prozess zur Entwicklung von IAM-Services

seine Anforderung in Form von User Stories, die gemeinsam mit dem IAM-Team diskutiert und konkretisiert werden. Das IAM-Team erstellt auf dieser Basis innerhalb kürzester Zeit einen Prototypen des Services anhand dessen die Anforderungsumsetzung erprobt werden kann. Im Falle kleiner Änderungen können diese live und gemeinsam mit dem Fachbereich in Workshops umgesetzt werden. Der Service kann dann als isolierte Komponente über das klassische IAM-Staging in die Produktion übernommen werden. Die zugrundeliegende Prämisse des Entwicklungsprozesses ist es, dass Anpassungen gemeinsam mit den Fachexperten und ohne Wechselwirkungen auf bestehende IAM-Funktionalitäten erfolgen. Dies gewährleistet einerseits die erwartete Funktionalität, erlaubt es aber auch, weiche Faktoren (wie die Usability oder die Endbenutzer-Akzeptanz) schon durch die Ausgestaltung des Entwicklungsprozesses zu beachten.

Beispiel Rollenerstellung

In einem vollwertigen IAM stellen Geschäftsrollen einen integralen Bestandteil der Berechtigungsvergabe dar. Die Bündelung von Berechtigungen in anwendungsunabhängige Geschäftsrollen erlaubt die flexible und (teil-)automatisierte Vergabe von Berechtigungen an Mitarbeiter. Während der Aufbau eines Geschäftsrollenmodells mittlerweile bereits von vielen Unternehmen realisiert ist, ist die operative Administration des Rollenmodells weiterhin ein oft manueller und ad-hoc getriebener Prozess. Der Fachbereich stellt häufig die Anforderung an die Funktionalität von Geschäftsrollen, während sich die IAM-Zentrale oder Rollenkoordinationsstelle darum kümmert, dass neue oder veränderte Geschäftsrollen dem unternehmensweiten Rollenmodell folgen. Im Markt ist eine Verlagerung dieses Prozesses zur individuell gewünschten Rollenerstellung durch Fachbereiche beobachtbar. Da jedoch häufig das Know-how im Fachbereich fehlt, stellt dieser Schritt eine Herausforderung dar. Ein strukturierter IAM-Service, der vordefinierten Rahmenbedingungen unterliegt, schafft hier Abhilfe. Im folgenden Beispiel wird die Zielsetzung und der Erstellungsprozess eines solchen IAM-Services illustriert:

Typischerweise entsteht der Bedarf für die selbstständige Anlage neuer Geschäftsrollen aus dem Umstand, dass Fachbereiche neue Applikationen einführen, Tätigkeitsfelder sich verändern, oder bisher ungenutzte Funktionalitäten von bestehenden Anwendungssystemen verwendet werden sollen. Klassischerweise kommuniziert der Fachbereich eine textuelle Beschreibung der neuen Anforderung an das IAM-Team und in aufwändiger und intensiver Zusammenarbeit erstellt das Rollenmodellierungsteam eine neue, für den Fachbereich passende, Geschäftsrolle. Anhand eines von den Modellierungsteams in der IT für den Fachbereich maßgeschneiderten Rollenerstellungs-Self-Service, kann dieser Prozess signifikant verschlankt und beschleunigt werden.

Die Erstellung eines solchen Services mithilfe eines modernen Development Kits wie NEXIS 4 läuft typischerweise wie folgt ab:

- Das IAM-Team definiert für den Fachbereich ein Formular, das die verständliche Erstellung einer neuen Geschäftsrolle ermöglicht. Dabei kann das IAM-Team bei der Konfiguration schon sicherstellen, dass Richtlinien des Geschäftsrollenmodells eingehalten werden, etwa der Rollenname und die Beschreibung vorgegebenen Konventionen folgen, und dass Pflichtattribute ausgefüllt werden.

- Eine Selektionskomponente für Berechtigungen der Geschäftsrollen wird so vorkonfiguriert, dass nur genau die Berechtigungen zur Verfügung gestellt wer-

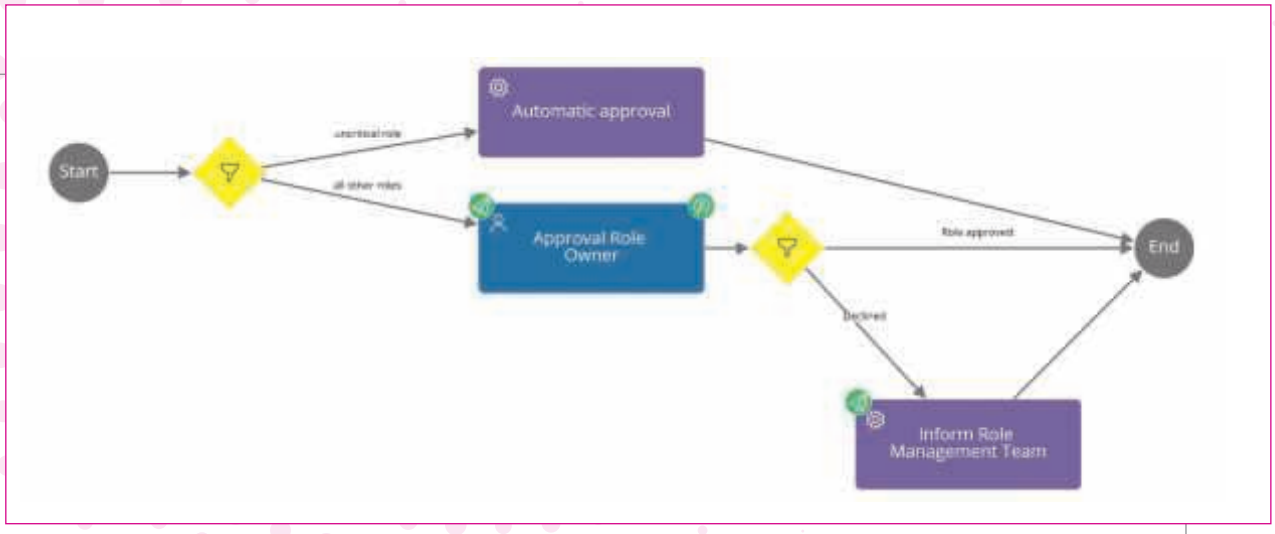


Bild 2: IAM-Service in der Workflow-Ansicht des Development Kits von NEXIS 4

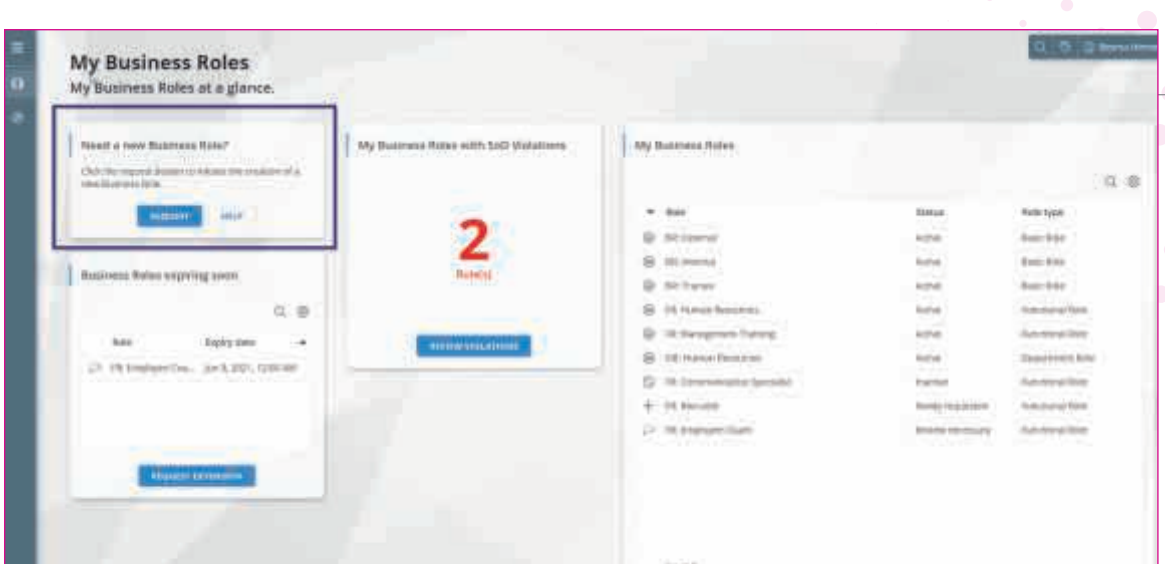


Bild 3: Dashboard in NEXIS 4 mit publiziertem IAM-Service zur Rollenerstellung

den, die tatsächlich für die Rollenaufnahme in Frage kommen. Von Unternehmen wird vor allem als Vereinfachung wahrgenommen, dass nicht aus einer sehr großen Menge an schwer verständlichen Berechtigungen ausgewählt werden muss, sondern dass dem Endanwender fachlich verständliche Gruppierungen von Berechtigungen samt Zusatzinformationen bereitgestellt werden.

➤ Nach der Definition des Formulars und der Funktionen zur Berechtigungsergänzung, wird der gewünschte nachgelagerte Workflow konfiguriert. In einem interaktiven und grafischen Workflow-Editor kann für den Fachbereich transparent das 4-Augen-Prinzip zur Erstellung und Genehmigung des Antrags durch Verantwortliche konfiguriert werden. Ein qualitätssichernder Schritt durch die Rollenkoordinationsstelle ist empfehlenswert und kann über weitere Knoten im Workflow realisiert werden. Eskalationsschritte, die den Prozess bei Nichtbearbeitung durch Stakeholder vorantreiben sollen, können ebenfalls hinterlegt werden.

➤ Abschließend wird der Service in einem benutzerfreundlichen Dashboard für den Fachbereich eingebettet und bereitgestellt.

Während in klassischen Systemen die Schritte der Formularerstellung, Workflow-Konfiguration und Anwenderkonfiguration zeitintensive und isolierte Tätigkeiten sind, kann – durch moderne IAM Development Kits wie NEXIS4 – die Erstellung eines solchen Services interaktiv, gemeinsam und für den Fachbereich verständlich vollzogen werden. Dies sichert einerseits die Integration von Stakeholder-Anforderungen und andererseits schafft es Verständnis für die Funktionsweise des produktiven Service. Nachdem der Service durch Pilot-Anwender getestet wurde, kann er auf der Produktiv-Umgebung aktiviert werden.

Trend zur De-Zentralisierung des IAM

Viele Compliance-Anforderungen verlangen die klare Verankerung der Verantwortlichkeit und damit die Mitwirkung von verantwortlichen Personen in den verschiedensten Berechtigungsprozessen. Weiterhin wird der Trend, außenwirksam und endanwenderfreundlich Teilfunktionen in die Fachbereiche zu verlagern, durch das größere Einsatzspektrum und die Bedeutungszunahme von IAM-Systemen verstärkt. Dies drängt IAM-Teams dazu, immer schneller auf sich wechselnde Anforderungen zu reagieren, was mithilfe der klassischerweise zur Verfügung stehenden Techniken kaum möglich ist. Es zeigt sich, dass schnell einsetzbare und leicht konfigurierbare IAM Tools eingesetzt werden müssen, um mit diesen Entwicklungen Schritt zu halten. NEXIS 4 als IAG-Plattform wird entwickelt, um diese Dezentralisierung von IAM-Funktionalitäten innerhalb von Unternehmen erfolgreich weiterzutreiben.

Neben der technischen Umsetzung ist der organisatorische Wandel und die Ausrichtung des IAM-Teams ein wichtiger Erfolgsfaktor, um von den Benefits einer dezentralen IAM-Struktur zu profitieren. Klassische Tätigkeiten wie die operative Vergabe und die Administration von Berechtigungsstrukturen sowie die Umsetzung von Hintergrundprozessen werden zukünftig eine untergeordnete Rolle für IAM-Teams spielen. Vielmehr müssen sie sich selbst als Dienstleister für den Fachbereich verstehen, der flexibel und dynamisch auf neue Anforderungen reagieren kann.

Dr. Michael Kunz

CREDENTIAL STUFFING

DAS HILFT WIRKLICH

Credential Stuffing verheißt für Cyberkriminelle viel Ertrag mit wenig Aufwand: Es genügen eine Liste gestohlener Passwörter und ein Tool, das diese Login-Daten mithilfe rotierender Proxys über mehrere Dienste hinweg testet. Den Rest erledigt die statistische Wahrscheinlichkeit, denn zu viele Nutzer verwenden für verschiedene Onlinedienste immer wieder dasselbe Passwort. Dagegen gibt es wirksame Strategien.

Credential Stuffing, also das automatisierte „Durchprobieren" von Benutzername-Passwort-Kombinationen in verschiedenen Online-Diensten, hat seit 2019 einen starken Aufschwung erlebt: Ursache sind große Data Breaches etwa bei Marriott, Equifax oder LinkedIn, durch die eine Vielzahl an Login-Daten in die Hände von Kriminellen gelangten. Schwerer wiegt aber, dass rund 52 Prozent der User ihre Passwörter nicht nur einmal vergeben, sondern wiederverwenden. Ein einmal gestohlenes Passwort kann so als „Generalschlüssel" zu verschiedensten Diensten fungieren.

Nutzergewohnheiten, die sich teils über Jahrzehnte eingeschliffen haben, erleichtern den Kriminellen ihr Handwerk zusätzlich. Noch immer bilden „123456", „password" und „abc123" die unrühmlichen Top drei der beliebtesten und gleichzeitig unsichersten Passwörter weltweit. Auch, wer mehr Wert auf Sicherheit legt, greift oft daneben: Rund 32 Prozent der User vertrauen auf Fantasiewörter und 21 Prozent auf Geburtsdaten – leider sind gerade diese Kombinationen besonders leicht zu knacken. Den Expertenrat, ganze Sätze und damit möglichst viele Zeichen als Passwort zu nutzen, beherzigen mit gerade einmal elf Prozent viel zu wenige Menschen.

VERALTETE PASSWORT-VERFAHREN LEISTEN DEM MISSBRAUCH DURCH DATENDIEBE VORSCHUB – DIE PASSWORTLOSE AUTHENTIFIZIERUNG ERMÖGLICHT GEGEN-STRATEGIEN.

Stephan Schweizer, CEO, Nevis Security GmbH, www.necis.net

Welche Goldgräberstimmung unter Cyberkriminellen herrscht, lässt sich auch mit einem Blick auf die Zahl der erfolgreichen Cyberattacken 2020 ermessen: Über 80 Prozent erfolgten mittels gestohlener Login-Daten oder Brute Force; bevorzugtes Angriffsziel waren mit mehr als 90 Prozent Web-Applikationen. Tiefere Technik- oder Programmierkenntnisse müssen die Täter dabei nicht mitbringen: Geleakte Passwortlisten sind teils frei zugänglich oder lassen sich im Darknet käuflich erwerben. Ebenso einfach gestaltet sich der Zugang zu Tools fürs Credential Stuffing.

Credential Stuffing im Detail

Einschlägige Toolsets bringen bereits alles mit, um mit geringem Aufwand große Schaden anzurichten. Optimierte Voreinstellungen für unterschiedliche Angriffsziele ermöglichen einen automatisierten Angriff auf Knopfdruck – dabei können Bankkonten, Cloudspeicher oder E-Commerce-Accounts ebenso das Ziel sein wie die Websites von Airlines und Hotels, Datingportalen oder Gaming- und Gambling-Anbietern.

Ob und wo ein Login mit den gestohlenen oder gekauften Anmeldedaten möglich ist, testen die Kriminellen mit Hilfe eines rotierenden Proxys, der Hunderttausende von Anmelde-Informationen über mehrere Dienste hinweg ansteuert. Der zeitliche Aufwand liegt selbst für eine groß angelegte Attacke bei wenigen Minuten – das unterstreicht die Gefahr, die von Credential Stuffing ausgeht.

Eine Modellrechnung zeigt das Ausmaß möglicher Schäden: Bereits bei einer durchschnittlichen Größe von einer Million gestohlener Logindaten und der konservativ geschätzten Erfolgsquote von 0,5 bis drei Prozent ergeben sich 5.000 bis 30.000 Accounts, auf die sich die Kriminellen im Verlauf einer einzigen Credential-Stuffing-Attacke Zugriff verschaffen können.

Die Hürden für Endanwender

Keine Frage: Der Gebrauch unsicherer Passwörter und ihre Mehrfachnutzung sind ein schwerwiegendes Problem. Doch den Nutzern die alleinige Schuld an der Passwort-Misere zuzuschieben, führt in die Irre. Warum aber agieren Anwender immer wieder so scheinbar sicherheitsvergessen?

- Die Zahl der Anbieter von Waren und Dienstleistungen im Netz ist seit den Anfängen des Internets exponentiell gewachsen. Mittlerweile verfügt ein Anwender über bis zu 130 digitale Benutzerkonten. Für jedes ein individuelles Passwort zu vergeben – und es sich sicher zu merken! – ist für viele schlicht nicht praktikabel.

- Schon jetzt verbringen Anwender statistisch zwölf Tage ihres Lebens mit der Suche nach Benutzernamen und Passwörtern.

- Weltweit wird eine von drei Online-Transaktionen aufgrund fehlender Benutzernamen und Passwörter abgebrochen.

Benutzername und Passwort sind also gerade deshalb ein Sicherheitsrisiko, weil sie beim Endanwender ein nicht zu unterschätzendes Frustpotenzial entfalten – das schließlich in einer gefährlichen Lethargie in Sicherheitsfragen mündet. Das Security and Privacy Institute (CyLab) der Carnegie Mellon University hat das daraus resultierende Nutzerverhalten nach einer Datenpanne analysiert. Die Ergebnisse sind alarmierend: Nur 33 Prozent der Nutzer änderten tatsächlich ihre Passwörter, nachdem sie über eine Datenschutzverletzung informiert wurden, und das jeweils nur für die jeweilige Plattform oder den betroffenen Account. Die Wahrscheinlichkeit, dass diese Nutzer ihr Passwort für alle Konten mit denselben Anmeldedaten ändern, dürfte noch weitaus geringer ausfallen.

Klar ist: Die meisten Nutzer wünschen sich bequeme Alternativen zum konventionellen Passwort, die gleichzeitig hohe Sicherheitsstandards erfüllen. Aber welche Verfahren bieten sich hier an? Eines ganz sicher nicht: die beliebte SMS-TAN.

Die SMS-Falle

Die SMS als Teil einer Zweifaktor-Authentifizierung wird noch immer häufig eingesetzt. Wie schnell sich dieses System aushebeln lässt, hat jüngst ein Test mit der Software Sakari durch die Website Motherboard ergeben: Das eigentlich fürs Unternehmensmarketing gedachte Tool ermöglicht den massenhaften SMS-Versand. Dabei lassen sich jedoch beliebige Mobilfunknummern hinterlegen – und sogar die an diese Nummern gerichteten SMS empfangen. Hacker können das nutzen, um die SMS eines Zweifaktor-Systems abzufangen, ohne dass der eigentliche Adressat dies bemerkt.

Der Grundfehler des Systems liegt damit offen zutage: De facto existieren keine Standards und Sicherheitsprotokolle für das (Re-)Routing von SMS. Eine weitere Nutzung im Rahmen von Zweifaktor-Authentifizierungen sollte unbedingt vermieden werden.

Passwörter abschaffen: So geht's

Dabei existiert mittlerweile ein Verfahren, das Passwörter vollständig durch eine biometrische Authentisierung ersetzt und sowohl die Benutzerfreundlichkeit als auch die Sicherheit verbessert: die sogenannte passwortfreie Authentisierung.

Dreh- und Angelpunkt sind die biometrischen Sensoren, die in modernen Smartphones verbaut sind und die eine eindeutige Authentifizierung des Nutzers anhand seiner Gesichtszüge oder Fingerabdrücke ermöglichen – ohne dass sensible Daten jemals das Gerät verlassen.

Beispiel Face ID

Biometrische Merkmale bieten prinzipbedingt eine große Sicherheit. Beispiel Face ID: Bei der Einrichtung scannt das Gerät das Gesicht des Nutzers und erstellt eine Art „Landkarte" der Physiognomie mit ihren einzigartigen physiologischen Merkmalen. Diese unverwechselbaren Kennzeichen werden als Datenpunkte in Form eines verschlüsselten 3D-Bildes direkt auf dem Mobilgerät gespeichert. Sobald diese einzigartigen Identifizierungsmerkmale im Speicher abgelegt sind, erkennt das Smartphone den Nutzer sofort, wenn er einen Blick auf das Display wirft.

Face ID registriert darüber hinaus potenzielle Veränderungen der Gesichtszüge, die im Laufe der Zeit auftreten können – wie Falten oder Tränensäcke unter den Augen – und „erlernt" diese leicht veränderten biometrischen Merkmale mittels Machine Learning. Auch ein paar schlaflose Nächte machen den Nutzer also nicht für das System unkenntlich.

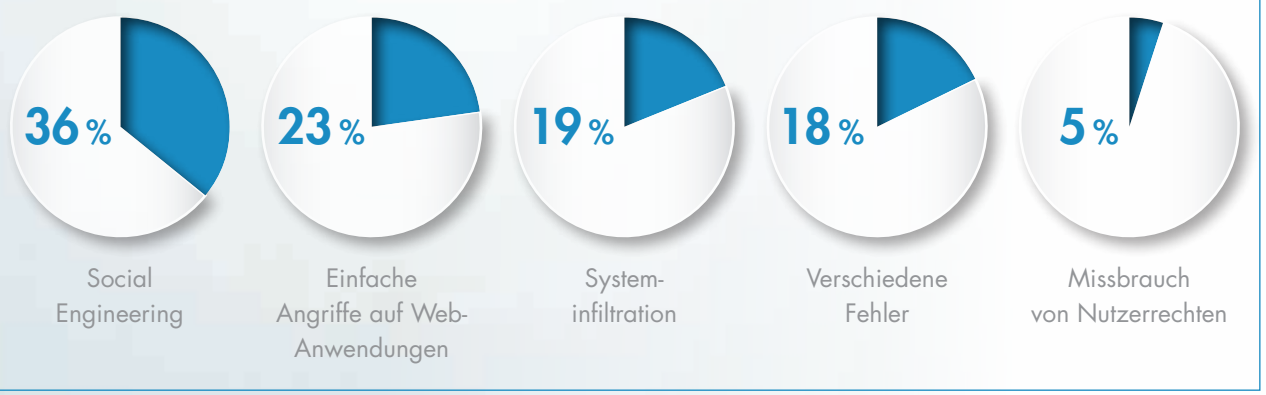
Passwortfrei per App

Die passwortfreie Zweifaktor-Authentifizierung per App nutzt den hohen Sicherheitsstandard der biometrischen Daten: Das verwendete FIDO UAF Protokoll basiert auf asymmetrischer Verschlüsselung, wobei der private Schlüssel immer auf dem Endgerät des Benutzers verbleibt und in einem speziell abgesicherten Chip-Set, der Secure Enclave, abgespeichert wird. Die biometrischen Merkmale wie Gesicht und Fingerabdruck werden lediglich zur Entsperrung des privaten Schlüssels verwendet und verbleiben daher ebenfalls immer auf dem Endgerät. Dieser Ansatz ermöglicht sehr hohe Sicherheit und zudem die Wahrung der Privatsphäre des Benutzers.

Insgesamt verspricht die Nutzung der passwortfreien Authentifizierung einen gewaltigen Sprung in der End-to-End-Sicherheit bei gleichzeitiger Verbesserung des Kundenerfahrung. Eine flächendeckende Durchsetzung des Verfahrens wird entscheidend dazu beitragen, großangelegte Betrugsmanöver wie das Credential Stuffing in Zukunft wirksam auszubremsen.

Stephan Schweizer

HÄUFIGKEIT DER SICHERHEITSVERLETZUNGEN



(Quelle: Verizon Data Breach Investigations Report 2021)

EFFEKTIVE ABSICHERUNG

KRITISCHE INFRASTRUKTUREN SCHÜTZEN

Immer mehr Branchen und Unternehmen mit Kritischen Infrastrukturen (KRITIS) – selbst jene, von denen man es auf den ersten Blick nicht erwarten würde – sind von Informationssystemen abhängig, um den Betrieb und somit auch die Gesellschaft aufrechtzuhalten. Mit zunehmender Digitalisierung und Vernetzung machen sie sich jedoch auch angreifbarer für Cyber-Kriminelle.

Mit folgenden drei Maßnahmen können Organisationen und Unternehmen wesentlich zur Verbesserung ihrer Sicherheit beitragen.

1. Security by Design

Es ist wichtig, bereits vor Installation der IT-Umgebung Hersteller und Anbieter zu wählen, die den Sicherheitsaspekt von Anfang an und während des gesamten Entwicklungsprozesses berücksichtigen. Durch diesen „Security-by-Design"-Ansatz erhalten KRITIS Gerätschaften oder Systeme an die Hand, die vorkonfiguriert und sicher einsatzbereit sind.

2. Mehrschichtige Strategie

Sollte doch erst im Nachhinein, also nach Installation, für Sicherheitsmaßnahmen gesorgt werden müssen, bedarf es technischer Lösungen, die den Betrieb bereits bestehender Kritischer Infrastrukturen nicht gefährden und gleichzeitig ganzheitlich schützen. Um die gesamte IT-Umgebung KRITIS nachhaltig und effektiv zu schützen, braucht es eine mehrschichtige und ganzheitliche Sicherheitsstrategie.

3. Cyber-Sicherheitsverbände

Unternehmen mit Kritischen Infrastrukturen können von einer Mitgliedschaft in Verbänden oder Kooperationen maßgeblich profitieren. So konzentriert sich zum Beispiel der öffentlich-private Umsetzungsplan (UP) KRITIS vornehmlich auf KRITIS und fördert den Austausch. Zentrale Ziele des UP KRITIS sind die Kommunikation über Cyber-Vorfälle und die Sensibilisierung und Aufklärung der aktuellen Bedrohungslage.

www.mcafee.com/de

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Bogdan Botezatu, Sudhir Ethiraj, Rebecca Horn, Dr. Michael Kunz, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Stephan Schweizer, Özkan Topal, Arne Wöhler

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 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


NCP
SECURE COMMUNICATIONS
Auffallend flexibel
Richten Sie Ihr Unternehmen jetzt produktiv und sicher für die Zukunft aus!
Ermöglichen Sie Homeoffice und mobiles Arbeiten – mit skalierbaren VPN-Lösungen und Lizenzmodellen für jeden Bedarf.
Wie flexibel sind Sie?
www.ncp-e.com
NCP
my access
SecurITy
made in Germany