itmanagement
DEZEMBER 2019

www.it-daily.net

INKLUSIVE 32 SEITEN
IT SECURITY SPEZIAL

WORKPLACE 4.0

Mit Transparenz zum Erfolg

ASSET MANAGEMENT

Stets alles im Überblick

DIGITALISIERUNG IM PROJEKTMANAGEMENT

VOM BUZZWORD ZUR MISSION POSSIBLE

Thomas Brunschede, Le Bihan Consulting

jamf
MDM für Apple-Geräte
ab Seite 16

www.it-daily.net

OPERATIONAL SERVICES
YOUR ICT PARTNER

BACKBONE OF DIGITAL TRANSFORMATION

Keine Digitalisierung ohne hybride IT-Servicemodelle

Die digitale Transformation beschäftigt alle Unternehmen, unabhängig von Größe, Branche oder Geschäftszweck. Dennoch muss jeder Betrieb seine eigene Digitalisierung individuell gestalten. Das gelingt mit einem hybriden IT-Servicemodell, in dem einige IT-Funktionen an externe Spezialisten ausgelagert werden und andere im Unternehmen bleiben. Neben hybriden Cloud-Infrastrukturen gehören Managed ICT Services aus dem Data Center oder sogar 24/7 Remote sowie On Premise Services dazu. Unternehmen gewinnen so einen Wettbewerbsvorsprung, sparen Zeit sowie Ressourcen ein, nutzen die Kompetenzen ausgewiesener Digitalisierungsspezialisten und profitieren von höchsten Sicherheitsstandards.

www.operational-services.de

DAS ZEITALTER DER BUZZWÖRTER!

Digitalisierung, Robotic Process Automation, Industrie 4.0, Künstliche Intelligenz, Workplace 4.0 – alles Buzzwörter für das „intelligente Zeitalter" – diese Aufzählung könnte noch beliebig erweitert werden!

Der „gut gebildete Mensch" wirft ja gern und dann auch täglich mit irgendwelchen Schlagwörtern um sich, dabei ist nicht einmal das Problem, dass viele gar nicht oder nur in etwa wissen, was die einzelnen Termini eigentlich bedeuten, sondern, dass oft ein unterschiedliches Verständnis darüber herrscht! Also habe ich mir mal den Spaß gemacht und „intelligentes Zeitalter" zur Begriffsklärung in meine liebste Suchmaschine eingegeben!

Das war mehr oder weniger aufschlussreich. Die erste Kernaussage war: Wir müssen für das Roboter-Zeitalter lernen! Bedeutet, wir müssen uns auf intelligente Maschinen vorbereiten und uns dann zurechtfinden. Die zweite Aussage war: Wir verschwinden, Maschinen ersetzen uns!

Gut, diese Diskussion ist nicht neu und es gibt immer die Befürworter und die „Ängstlicheren/Bedenkenträger" unter uns. Wenn man sich aber wirklich tiefgründig mit der Thematik beschäftigt, sollte ein gutes Mittelmaß aus Pro- und Contrawissen rauskommen und dann darf man auch gern mit Buzzwörtern um sich werfen!

Übrigens, Workplace 4.0, Internet of Things oder Robotic Process Automation sind auch Themen dieser Ausgabe und wo wir gerade bei Buzzwörtern sind: In unserem Supplement it security finden Sie noch mehr davon: Künstliche Intelligenz, Industrie 4.0 oder Hacking!

Viele Spaß beim Weiterbilden!

Herzlichst!

Carina Mitzschke

INHALT

IT MANAGEMENT

8

COVERSTORY

28

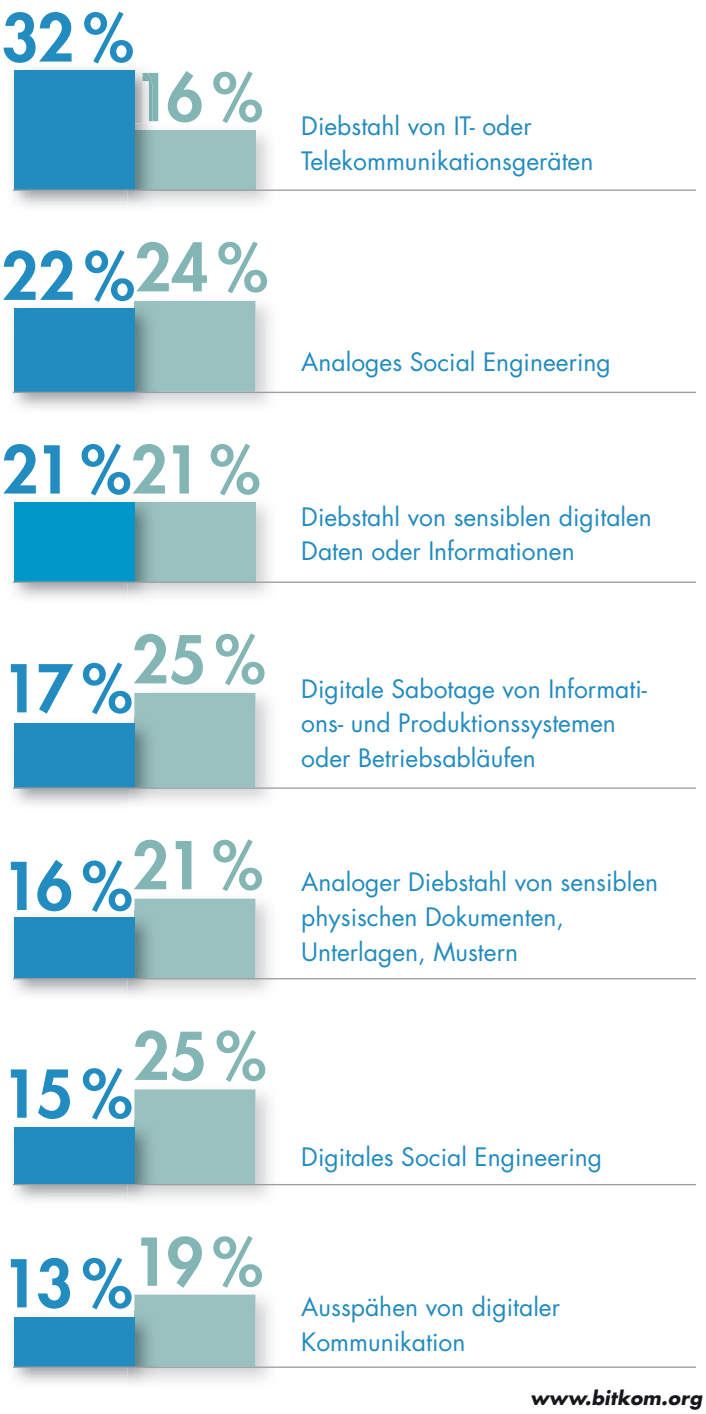
Inklusive
32 Seiten

IT SECURITY SPEZIAL

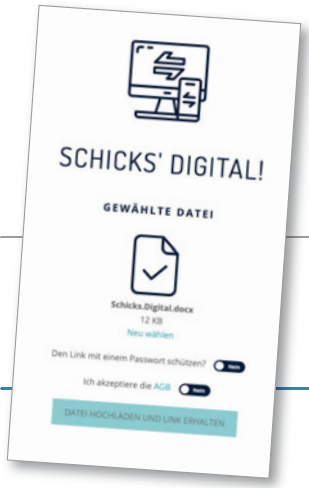
IT INFRASTRUKTUR

ANGRIFFSZIEL DEUTSCHE WIRTSCHAFT

Von welchen der folgenden digitalen oder analogen Arten von Datendiebstahl, Industriespionage oder Sabotage war Ihr Unternehmen innerhalb der letzten zwei Jahre betroffen/vermutlich betroffen?



www.bitkom.org



SCHICK'S DIGITAL

DIE VERSCHLÜSSELTE WETRANSFER-ALTERNATIVE

Wer große oder vertrauliche Dateien online versenden will, kann ab sofort die neue Plattform Schicks.Digital nutzen. Im Gegensatz zu anderen Datenaustausch-Diensten garantiert die Lösung durch eine Ende-zu-Ende Verschlüsselung, dass die Dokumente vertraulich bleiben. Sender haben die Möglichkeit, Dateigrößen bis 3GB DSGVO-konform hochzuladen und zu verschicken – schnell, unkompliziert und sicher. Die Übertragung wird schon vor dem Upload verschlüsselt, um die Unterlagen vor Datendiebstahl zu schützen. Der Empfänger erhält die Daten als einfachen Download-Link über E-Mail, WhatsApp, Telegramm und beliebige andere Messenger oder über die neue vertrauliche „Briefkasten"-Funktion von Schicks.Digital. Übertragene Dokumente stehen 14 Tage zur Verfügung und werden anschließend automatisch vom Server gelöscht. Über die Briefkasten-Funktion kann der Nutzer anonyme Adressen generieren. Damit können ihm andere Personen vertrauliche Dokumente in den verschlüsselten Briefkasten legen. Das Online-Tool kann kostenlos und ohne Login genutzt werden.

Die Server stehen in Deutschland und werden vom Unternehmen Uniki gehostet.

www.uniki.ce

ZUKUNFT DER ARBEIT

TECHNOLOGIEN, DIE VORANTREIBEN

1. **Kollaborative KI:**
KI wird für Zusammenarbeit konzipiert sein. Maschinen werden kontinuierlich ihr Verständnis des Menschen ausbauen und dadurch ihre Fähigkeit zur Zusammenarbeit verbessern und die Produktivität steigern.

2. **Multimodale Schnittstellen:**
Haptisches 3D-Feedback, Gestenerkennung und sogar Geruch werden in Schnittstellensystemen verwendet, um vielfältigere und zugänglichere Möglichkeiten der Interaktion mit Daten und Anwendungen zu bieten.

3. **Erweiterte Realität (XR):**
XR, die angereicherte Realität (AR), virtuelle Realität (VR) und gemischte Realität (MR) umfasst, kombiniert reale und virtuelle Umgebungen, damit Nutzer abstrakte Informationen in reichhaltige, interaktive Erfahrungen umwandeln können.

4. **Sichere verteilte Ledger:**
Sichere verteilte Ledger wie Blockchains stellen einen unveränderlichen, transparenten Datenspeichermechanismus bereit, der Arbeitsprozesse wie die Zahlungsabwicklung in Echtzeit nach Abschluss einer Arbeitsaufgabe automatisieren kann.

www.delltechnologies.com

DIGITALISIERUNG IM

VOM BUZZWORD ZUR MISSION POSSIBLE

Die digitale Transformation wird das Projektmanagement in den kommenden Jahren verändern. Viele Unternehmen unterschätzen das und sind nicht ausreichend vorbereitet. Der Projektmanagement-Experte Thomas Brunschede, Geschäftsführer bei Le Bihan Consulting, stellt sich den Fragen von Ulrich Parthier, Herausgeber it management.

? **Ulrich Parthier:** *Digitalisierung ist Buzzword, Hype und Realität zugleich. Wie würden Sie diesen Begriff definieren?*

Thomas Brunschede: Die Digitalisierung ist ja nicht neu. Wir erleben eine Digitalisierung seit den 1970er Jahren. Damals und in den Jahrzehnten danach ging es um eine Automatisierung auf Basis von Elektronik und EDV. Heute steht die Informatisierung im Vordergrund. Dabei wird uns zunehmend Künstliche Intelligenz (KI) zur Verfügung stehen. Das bringt tiefgreifende Veränderungen in der Arbeitswelt und letztlich in der Gesellschaft mit sich.

? **Ulrich Parthier:** *Die Digitalisierung eröffnet auch im Projektmanagement völlig neue Möglichkeiten. Welchen Einfluss hat dieser Trend aktuell?*

Thomas Brunschede: Zunächst einmal glaube ich nicht, dass es sich bei der Digitalisierung um einen Trend handelt. Eher um einen Umbruch, der dauerhafte Veränderungen mit sich bringt. Genau deshalb sind die Auswirkungen auf das Projektmanagement auch so stark.

Ich bin davon überzeugt, dass die Verzahnung des Projektmanagements mit anderen Disziplinen deutlich zunehmen wird. Dem Benutzer kann es künftig gleichgültig sein, welche Disziplin und welches System ihm bei seinem Problem weiterhilft oder Informationen zur Verfügung stellt. Die Grenzen zwischen PM, BI, ERP – und was immer Ihnen an sonstigen Abkürzungen aus diesem Umfeld einfällt – werden immer weiter aufgelöst.

PROJEKTMANAGEMENT

Diese Verzahnung ist heute bereits in Ansätzen zu beobachten und wird sich in den kommenden Jahren weiter durchsetzen. Die Systeme und Disziplinen werden quasi nahtlos ineinander übergehen.

Einen weiteren Effekt der Digitalisierung auf das Projektmanagement werden wir beim Thema „Führung" erleben. Verantwortung wird zukünftig dezentraler verteilt sein. Das klassische Command and Control wird kleinen, selbstbestimmten Teams weichen. Auch dieser Prozess hat längst begonnen, wird sich aber noch weiter verstärken.

? **Ulrich Parthier:** *Neben den bereits beschriebenen Veränderungen stehen auch Wechsel bei den Prozessen, in der Kommunikation und Organisation an. Was sind hierfür die Gründe?*

Thomas Brunschede: Für den wesentlichen Treiber halte ich zunehmende Komplexität. Die erleben wir in allen Arbeitsbereichen. Wir haben uns in den letzten Jahrzehnten so weit entwickelt, dass wir an die Grenzen dessen geraten, was wir noch mit „Bordmitteln", also unserem eigenen Hirn, lösen können.

Dabei geht es nicht nur um die Menge an Daten und Informationen. Heute könnten wir unsere Aufgaben auch mit viel Zeit nicht mehr angemessen lösen, weil die Daten- und Informationslage zu unübersichtlich geworden ist. Alles hängt irgendwie mit allem zusammen, der Überblick droht verlorenzugehen. Die Digitalisierung hilft uns dabei, diese Datenverflechtung zu managen.

Zwischen Digitalisierung und Komplexität besteht dabei eine kaskadierende Wechselwirkung: Weil wir durch zunehmende IT-Unterstützung komplexere Aufgabenstellungen lösen können, machen wir das natürlich auch. Dadurch nimmt die Komplexität weiter zu.

? **Ulrich Parthier:** *Was ändert sich im Projektalltag und wie können Unternehmen sich dafür wappnen?*

Thomas Brunschede: Die Dynamik wird zunehmen, und darauf sind viele Unternehmen unzureichend vorbereitet. Wir empfehlen unseren Kunden, ihre Organisation zu einem „dynamikrobusten System" umzubauen. Das bedeutet: Es gibt Bereiche und Aufgabenstellungen, die sich gut in Prozessen beschreiben und durch Regeln managen lassen – der wissensbasierte, eher statische Bereich. Und es gibt andere Bereiche, in denen benötigen Sie Ideen, Kreativität und den hierfür notwendigen Freiraum. Hier herrscht eine solche Dynamik, dass heute definierte Prozesse morgen schon wieder angepasst werden müssten. Hier führen Sie auch weniger durch Regeln, sondern eher auf Basis von Prinzipien.

Wenn Sie nun einen Brückenschlag zwischen der statischen und der dynamischen Welt hinbekommen, haben Sie ein dynamikrobustes System geschaffen. Ein System, das mit Dynamik umgehen kann, ohne im Chaos zu versinken. Das wird eine Herausforderung für viele Unternehmen: Wo man sich darauf einlässt, verändert es die DNA eines Unternehmens.

Das hat zur Folge, dass Themen wie Verantwortung, Führung und Kommunikation neu gedacht werden müssen. Wir werden zukünftig noch viel agiler und flexibler arbeiten als heute. Aber wir müssen lernen, dass gerade an den Nahtstellen zwischen Statik und Dynamik die Kommunikation gut funktionieren muss. Das hat Auswirkungen sowohl auf Mitarbeiter als auch auf die Führung.

> DIE DIGITALISIERUNG IST EINE HERAUSFORDERUNG, DIE NICHT ERST KOMMEN WIRD, SONDERN LÄNGST ANGEFANGEN HAT.
>
> Thomas Brunschede,
> Geschäftsführer,
> Le Bihan Consulting,
> www.lebihan.de

? **Ulrich Parthier:** *Es gibt eine neue Generation von Mitarbeitern, die mit sozialen Medien arbeitet, neue Kommunikationsplattformen wie Slack, Wickr Pro oder Circuit nutzt. Wie verändert das die Kommunikation?*

Thomas Brunschede: Eine der integrativen Aufgaben der Projektleitung wird darin bestehen, einen Kommunikationsmix zu schaffen, der die unterschiedlichen digitalen Reifegrade der Teammitglieder berücksichtigt. Dazu gehört, die Motivationen zu hinterfragen, die zu bestimmten Formen der Kommunikation führen. An dieser Stelle ist Führung gefragt. Es muss verbindliche und vor allem verlässliche Vereinbarungen geben.

Digitalisierung ist eben nicht nur ein technisches Thema, sondern auch eine Frage der Kultur und ihrer Veränderung. Und wenn hier das Top-Management nicht mit an Bord ist, wird es nicht unbedingt einfacher.

? **Ulrich Parthier:** *Sehen Sie die Digitalisierung als klassisches Projekt mit Anfang und Ende oder eher als iterativen Prozess?*

Thomas Brunschede: Der Begriff „Digitalisierung" charakterisiert rein sprachlich keinen Zustand, sondern den Weg dorthin. Damit werden Aspekte, Aufgaben und Herausforderungen umfasst, die wir teilweise noch gar nicht kennen. Wir werden es beispielsweise mit Disruption zu tun bekommen, können die aber gegenwärtig weder genau beziffern noch eindeutig eingrenzen. Digitalisierung hat also in jedem Fall einen iterativen Charakter.

? **Ulrich Parthier:** *Im Projektalltag gibt es einen enormen Wandel in der Geschwindigkeit, etwa durch die neuen digitalen Kommunikationsmittel: Skype, Hangouts, Messenger- oder Cloud Service-Dienste.*

Thomas Brunschede: Ich würde nicht sagen, dass die neuen Kommunikationsmöglichkeiten in erster Linie Geschwindigkeitstreiber sind. Diese wird eher durch die schnellere Verfügbarkeit von Informationen befördert. Und das wird sich noch steigern: Mithilfe von KI wird es möglich sein, passgenaue Informationen in sehr kurzer Zeit aufbereitet zu bekommen. Die persönliche Kommunikation wird sich durch KI reduzieren, wodurch sie indirekt wieder schneller wird.

? **Ulrich Parthier:** *Parallel dazu werden neue Methoden wie das Design Thinking oder agile Verfahren wie Scrum immer populärer. Sind da klassische PM-Tools nicht ein Auslaufmodell?*

Thomas Brunschede: Ein Aspekt unserer Arbeit bei Le Bihan besteht ja darin, dass wir in Kooperation mit dem Projektmagazin als Ratingagentur für PM-Software tätig sind. Durch die Assessments, die wir mit den Herstellern machen, bekommen wir einen ganz guten Einblick in den Markt der PM-Tools. Die meisten Hersteller passen sich ständig an neue Methoden und Verfahren an.

Ich glaube, dass die Kombination aus traditionellem und agilem Projektmanagement uns noch eine ganze Weile begleiten wird. Und dieser hybride Ansatz ergibt auch Sinn. Es wird auch in Zukunft Projekte geben, die Sie nicht wirklich agil managen können. In einem Softwareprojekt können Sie auftretende Fehler mit dem nächsten Bugfix beheben. Im Bau sieht das anders aus. Wenn Sie einen Planungsfehler bemerken, der Beton aber schon hart ist, haben Sie ein Problem.

? **Ulrich Parthier:** *Auch die Art der Projekte ändert sich. Das PM gestaltet sich mehr in Richtung cross-funktional. Kann das klassische Projektmanagement hier überhaupt noch greifen?*

> WIR WERDEN ZUKÜNFTIG NOCH VIEL AGILER UND FLEXIBLER ARBEITEN ALS HEUTE. ABER WIR MÜSSEN LERNEN, DASS GERADE AN DEN NAHTSTELLEN ZWISCHEN STATIK UND DYNAMIK DIE KOMMUNIKATION GUT FUNKTIONIEREN MUSS.
>
> Thomas Brunschede

Thomas Brunschede: Grundcharakter des Projektmanagements ist von je her eine interdisziplinäre Ausrichtung. Das heißt: Es würde diesem Grundgedanken regelrecht widersprechen, wenn eine solche übergreifende Art der Zusammenarbeit nicht möglich wäre. Das klassische Projektmanagement wird sich sicherlich verändern müssen, um eine firmenübergreifende Zusammenarbeit auch in der Praxis zu unterstützen, etwa durch einheitliche Standards. Aber es muss sich nicht neu erfinden.

? **Ulrich Parthier:** *Klassisches Projektmanagement wird in Etappen und Zeitumfängen geplant. Je komplexer die Projekte, desto schwieriger das Ziel. Ist es da sinnvoll, mehrere Entscheider zu definieren und dezentrale Strukturen zu schaffen, um Verantwortung zu delegieren?*

Thomas Brunschede: Unbedingt! Wir benötigen dezentrale, autarke Teams, die mit der notwendigen Entscheidungskompetenz ausgestattet sind. Diese Delegation von Verantwortung und letztendlich auch Macht wird meines Erachtens nach eine der großen Herausforderungen der Digitalisierung werden.

Beim Stichwort „keine starren Ziele" muss man zwischen Gesamt- und Teilzielen unterscheiden. Gesamtziele, die idealerweise ja auch stark mit der Unternehmensstrategie synchronisiert sein sollten, sind sicherlich starrer als Teilziele, die zur Erreichung des Gesamtziels definiert werden und einer ständigen Überprüfung und Anpassung unterliegen. Genauso wie Strategie, Gesamt- und Teilziele synchronisiert werden müssen, sollten auch die verschiedenen Entscheidungsebenen und -träger gut abgestimmt sein.

? **Ulrich Parthier:** *Qualität und Qualitätskontrolle waren schon immer ein schwieriges Umfeld im Projektmanagement. Wie kann man Feedback und Kontrollen im Projektmanagment-Service digitalisieren?*

Thomas Brunschede: Die bessere und durchgängigere Verfügbarkeit von Daten und Informationen hat natürlich auch einen positiven Effekt auf das Qualitätsmanagement. Die Möglichkeiten der Überprüfung von Lieferobjekten sollten sich durch verzahnte Workflows verbessern.

Gleichzeitig wird hier auch eine zunehmende Automatisierung stattfinden. Es ist auch denkbar, dass dem Qualitätsaspekt im Zuge der Digitalisierung eine größere Bedeutung zukommt. Wenn Qualität vom Verbraucher entsprechend honoriert wird, bedeutet das für Unternehmen, hier investieren zu können.

? **Ulrich Parthier:** *Die Kommunikation war immer ein zentrales Thema im Projektmanagement. Durch den massiven Wandel der Technik spielen räumliche Faktoren heute eine eher untergeordnete Rolle. Was für Regeln empfehlen Sie für die digitale Kommunikation?*

Thomas Brunschede: Ich war vor kurzem im Büro eines traditionell kommunizierenden Managers. Bei dem klingelte permanent das Telefon. In diesem Moment ist mir klar geworden, wie selten das heute nur noch passiert. Wir haben mittlerweile einen guten Teil dessen, was früher am Telefon besprochen wurde, auf andere Kommunikationswege ausgelagert. Das erzeugt zunächst einmal eine Fülle von Daten und Informationen.

Es ist für die Kommunikation grundsätzlich eine Herausforderung, die wichtigen Informationen aus der Flut von Daten herauszufiltern. Zukünftig wird KI uns dabei unterstützen, indem sie uns Informationen auf Zuruf aufbereitet und zur Verfügung stellt.

Wir empfehlen unseren Kunden, gemeinsam mit dem Team eine Kommunikationsstrategie zu entwickeln. Gemeinsam deshalb, weil man Kommunikation nur bedingt Top-down einführen kann. Und weil individuelle digitale Reifegrade berücksichtigt werden müssen. Das Ergebnis enthält dann verschiedene Kommunikationskanäle: vom persönlichen Gespräch oder Telefonat bei komplexen Sachverhalten über Chats für flüchtige Informationen bis hin zu Informationssystemen wie etwa einer digitalen Projektakte, in die auch Mails integriert werden.

? **Ulrich Parthier:** *Welche drei Handlungsempfehlungen geben Sie Unternehmen zum Schluss mit auf den Weg?*

Thomas Brunschede: Erstens: Die Digitalisierung als eine Herausforderung annehmen, die nicht erst kommen wird, sondern längst angefangen hat. Bei der man aktiv und gestaltend teilnimmt, statt nur vom Spielfeldrand zuzuschauen.

Zweitens: Das eigene Unternehmen kulturell, prozessual und methodisch fit für die Zukunft machen. Konkret: Ein ausreichend dynamisches Umfeld schaffen, in dem Verantwortung dezentral verteilt ist und in dem eine pathologische Politik nicht alle erfolgsversprechenden Veränderungsansätze bereits im Keim erstickt.

Drittens: Das Unternehmen technisch fit für die Zukunft machen. Derzeit wird das Thema Digitalisierung oft auf technische Aspekte reduziert. Erfolgreich werden aber vor allem die Unternehmen sein, bei denen Technik, Organisation, Menschen, Prozesse und Methoden gut aufeinander abgestimmt sind.

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

WORKPLACE 4.0

NEW WORK BASIERT AUF TRANSPARENTEN PROZESSEN

Die inhaltliche Bandbreite dessen, was gemeinhin mit Begrifflichkeiten wie New Work, Modern Workplace oder Arbeiten 4.0 assoziiert wird, ist enorm. Für viele Unternehmensverantwortliche sind die dahinterstehenden Konzepte weder greifbar noch definierbar. Doch unabhängig vom jeweiligen Verständnis dienen bei genauerem Hinsehen immer durchgängige und transparente Softwarelösungen als Basis für jedwede Form des modernen Arbeitens. Sie sorgen für bessere Kommunikation, schlankere Prozesse und stärken den Service-Gedanken.

Mobiles Arbeiten ist laut öffentlicher Wahrnehmung eine der am häufigsten praktizierten Formen von New Work. Die Standortunabhängigkeit gewährt den einzelnen Mitarbeitern mehr individuellen Freiraum und zielt darauf ab, ihre Produktivität in einem für sie passenden Arbeitsumfeld ohne starre Anwesenheitspflicht zu erhöhen. Individualität und Freiraum entfalten ihre produktivitätssteigernde Wirkung jedoch nur, wenn die zugrundeliegenden Prozesse auf leistungsfähigen, zentralen IT-Architekturen ablaufen. Dabei müssen sie vor allem durchgängig, transparent und nachvollziehbar sein. Die Annahme liegt nahe, dass alle diese Attribute generell die Grundlage für die neuen Modelle des Arbeitens bilden.

Dies vorausgesetzt, beginnt die Wandlung zu New Work in Bereichen, wo man sie nicht direkt vermuten würde. Wenn beispielsweise sehr alltägliche, bislang jedoch zeitraubende Abläufe wie das Management von Anfragen, Aufgaben, Freigaben und Genehmigungen mit modernen Tools zentral verwaltet wird, lassen sich sogar Partner und Kunden in ausgewählte Prozesse einbinden. Somit sparen nicht nur die eigenen Mitarbeiter Zeit und arbeiten produktiver, auch Kundenanfragen können gezielter und schneller bearbeitet werden, was den Service-Gedanken stärkt und damit die Kundenzufriedenheit erhöht: Neues Arbeiten als Synonym für Öffnung und Transparenz und letztlich mehr Kundenorientierung.

Drehscheibe für alle Anfragen und Freigaben

Ein solches unternehmensweites Anfragemanagement-System hat das Beratungs- und Softwarehaus ams.Solution mit dem Software-Modul ams.taskmanager entwickelt. Alle Mitarbeiter und auch berechtigte Externe haben die Möglichkeit, sich im System anzumelden und Tasks einzustellen. Prädestiniert ist das Tool für interne Änderungs- und Helpdesk-Anfragen, für Service-Anfragen von Kunden oder auch für Freigabeprozesse wie Angebots- und Urlaubsgenehmigungen. Die Software greift nicht unmittelbar in die ERP-Prozesse ein, dennoch können die Nutzer dank nahtloser Integration in ams.erp Verknüpfungen zu jedem Geschäftsobjekt herstellen und auch Listen von verknüpften Tasks anlegen, sodass alle mit einem Angebot verbundenen Aufgaben direkt bereitstehen.

Mit dem Anfragemanagement-System verfügen die Anwender nun über eine zentrale Kommunikationsplattform, die mit ihren definierten Workflows bislang zumeist unstrukturierte Anfrage- und Freigabeprozesse ablöst und damit Zeit, Aufwand und Kosten reduziert. In erster Linie werden langwierige E-Mail-Konversationen vermieden, was für sich alleine genommen bereits eine modernere Form des Arbeitens darstellt. Mit dem Kollaborations-Tool können die Mitarbeiter alle anfallenden Aufgaben strukturiert und historisiert verwalten und austauschen, außerdem lassen sich automatisierte, dynamische Prozesse für die im System befindlichen Tasks hinterlegen.

Der Ersteller einer Task priorisiert diese durch die Angabe der Dringlichkeit seines Anliegens. In einem drohenden

> NEUES ARBEITEN STEHT ZUNEHMEND FÜR DIE VERNETZUNG ALLER UNTERNEHMENSBEREICHE, DIE IN MODERNEN PROZESSLANDSCHAFTEN NICHT MEHR TRENNBAR SIND.
>
> Eckhard Ulmer, Vorstand, ams.Solution AG, www.ams-erp.com

Schadensfall kann zum Beispiel angegeben werden, wann ein Schaden eintreten könnte und wie hoch er voraussichtlich ausfallen wird. Auch Kundenanfragen lassen sich auf diese Weise nach ihrer Wichtigkeit und möglichen Eskalationsstufe einordnen, wobei immer gewährleistet ist, dass sie tatsächlich bearbeitet werden. Darüber hinaus kann der Priorisierungsgrad des jeweiligen Anfragetypen festgelegt werden. Wird aus einer Anfrage eine Task, ist definiert, wer primär zuständig ist und welche weiteren Prozessschritte folgen. Das System gibt dann beispielsweise vor, dass bei einer Angebotsänderungsanfrage zunächst immer der Vertriebsinnendienst aktiv wird, bevor der Sachverhalt an den jeweiligen Projektleiter übergeben wird.

Grundsätzlich ist das System beliebig konfigurierbar, was es einerseits äußerst flexibel und anpassbar macht, gleichzeitig aber auch voraussetzt, dass die abzuwickelnden Anfragefälle zunächst definiert werden. Sind die entsprechenden Workflows festgelegt, werden die Änderungen an einem Task lückenlos dokumentiert: Es ist immer klar, wer zu welchem Zeitpunkt welche Änderungen vorgenommen hat.

Einbindung aller Unternehmensbereiche

An einer anderen Stelle wird deutlich, dass sich hinter dem Begriff New Work mehr verbirgt als die Schaffung mehr individuellen Freiraums für die einzelnen Mitarbeiter. Die angesprochene Durchgängigkeit und Transparenz geht über die Firmengrenzen hinaus. Über eine definierte Schnittstelle erlaubt der ams.taskmanager die Anbindung von Fremdsoftware und damit auch von Maschinen und Produktionsanlagen. Schlägt der Wärmesensor einer vernetzten Maschine aufgrund zu hoher Temperatur Alarm, kann die betroffene Anlage über die Programmierschnittstelle (API) automatisch eine Task anlegen, um einen Mitarbeiter zu benachrichtigen oder um einen Service-Prozess auszulösen – ein prototypischer Fall von Industrie 4.0.

Die Beispiele zeigen: Neues Arbeiten steht zunehmend für die Vernetzung aller Unternehmensbereiche, die in modernen Prozesslandschaften nicht mehr trennbar sind. Vielmehr fließen sie ineinander, was sich an der Einbindung von Industrie-4.0-Komponenten gut ablesen lässt. New Work setzt transparente und durchgängige Prozessketten voraus, die zum einen die internen Abläufe in den Unternehmen beschleunigen und zum anderen den Blick auf Kunden und Partner schärfen. Für beides ist ein zentrales Software-System zur schnellen und konsistenten Bearbeitung von Tasks geradezu prädestiniert.

Eckhard Ulmer

„DIGITAL WORKPLACE“ IM

VOM WUNSCH ZUR WIRKLICHKEIT

Neue Technologien ändern maßgeblich die Art und Weise, wie Menschen arbeiten, kommunizieren und lernen. Auf diese äußeren Veränderungen müssen Organisationen schnell reagieren, um nicht mehr nur wettbewerbsfähig, sondern vielmehr zukunftsfähig zu bleiben. Schließlich ist gerade der Megatrend zum „Digital Workplace“ zu einem absoluten Schlüsselfaktor geworden, und zwar nicht nur im Hinblick auf die operative Arbeit, sondern auch und noch viel mehr hinsichtlich der Attraktivität des Unternehmens für Mitarbeiterinnen und Mitarbeiter – und vor allem für junge Fachkräfte.

DIE MEHRHEIT DER EUROPÄISCHEN ARBEITGEBER BLICKT OPTIMISTISCH AUF DIE VERÄNDERUNGEN, DIE DIE EINFÜHRUNG NEUER TECHNOLOGIEN AM ARBEITSPLATZ FÜR SIE BEDEUTEN.

Niculae Cantuniar, CEO, Ricoh Deutschland, www.ricoh.de

In vielen großen Unternehmen und Konzernen gehört dieser Digital Workplace und mit ihm die digitale Kommunikation und Zusammenarbeit bereits zum Alltag und ist organisatorisch fest verankert. Doch auch der Mittelstand hat unlängst die Notwendigkeit erkannt, sich auf den Wandel einzulassen und entwickelt flexible Strategien und Lösungen, um auf die Bedürfnisse ihrer Mitarbeiterinnen und Mitarbeiter einzugehen und die Voraussetzungen für eine langfristig erfolgreiche, moderne Arbeit zu schaffen. Denn mehr als die Hälfte der Entscheidungsträger in kleinen und mittelständischen Unternehmen befürchten, dass ihr Geschäft nicht überleben wird, wenn sie nicht innerhalb der nächsten fünf Jahre in neue Arbeitsplatztechnologien investieren. Das ergab eine Studie, die Ricoh zusammen mit IDC durchgeführt hat.

Trotzdem fällt vielen der Einstieg in die Digitalisierung schwer, denn das Thema ist bei Mittelständlern nach wie vor Chefsache. Dort steht, nachvollziehbar, das operative Tagesgeschäft im Vordergrund. Da bleibt wenig Zeit, um sich konkreter mit diesem Thema auseinanderzusetzen. Dies ist aber zwingend notwendig – denn die Digitalisierungsstrategie gibt es nicht von der Stange. Es ist wichtig, sich bei diesem Thema auf einen Technologiepartner verlassen zu können, der bei der Konzeption und Umsetzung nachhaltig berät und unterstützt. Nur so gelingt der Einstieg effektiv und die damit einhergehende Veränderung, insbesondere im Hinblick auf Prozesse und Arbeitsweisen, zeigt die gewünschten Effekte.

Enabler für die Digitalisierung

Für den Mittelstand gilt ganz klar: Der effektivste Schritt auf dem Weg zum Digital Workplace ist eng mit der Digitalisierung von papierbasierten Geschäftsprozessen verknüpft. Hier gibt es vor allem bei KMU ein großes Digitalisierungspotenzial: Laut einer aktuellen IDC-Studie schätzen zwar 84 Prozent der befragten Unternehmen, dass beispielsweise die Prüfung von Verträgen und Angeboten in ein bis zwei Jahren ausschließlich digital ablaufen wird. Aktuell ist das allerdings erst bei rund der Hälfte aller Unternehmen so. Bei ihnen ist das Druck- und Dokumentenmanagement, beziehungsweise Konzepte für Managed Document Services (MDS) und Managed Print Services (MPS), noch immer einer der effektivsten Enabler für die Digitalisierung: Neun von zehn Unternehmen bestätigen, dass eben dieses Thema eine signifikante Rolle bei der Digitalisierung ihrer Prozesse spielt. MDS-Konzepte sind mehr denn je zu einem echten Treiber für die Digitalisierung im Mittelstand avanciert und kreisen umso mehr um die Anforderungen, die sich Unternehmen durch die Zunahme digitaler und mobiler Arbeitsweisen stellen. Die Schlüsselrolle nehmen hierbei die Multifunktionssysteme als zentrale Digitalisierungs-Hubs ein. Mehr als die klassischen Print- und Output-Funktionen stehen heute vor allem die Input- und Throughput-Funktionen der Systeme im Vordergrund, vor allem wegen der direkten Anbindung an Cloud-Services und ECM-Systeme, wie etwa DocuWare.

Immer mehr ECM-Systeme in der Cloud

Laut der neuen Bitkom-Studie „Digital Office im Mittelstand“ verwenden aktuell bereits 86 Prozent der befragten Großunternehmen unternehmensweite Enterprise-Content-Management-Systeme und Plattformen für Content Services, also die Software an der Schnittstelle zwischen MFP und Dokumentenmanagement beziehungsweise Workflow. Hier hinkt der Mittelstand noch hinterher: Nur 19 Prozent der KMU verfügen über eine unter-

MITTELSTAND

Mit der A3-Funktionalität des IM C3000 können in-house Broschüren und Banner produziert werden.

nehmensweite ECM-Lösung. Aber immerhin nutzt inzwischen knapp die Hälfte (47%) der befragten mittelständischen Unternehmen eine Standard-Software für die digitale Dokumentenverwaltung.

Bei der Betriebsart dieser Lösungen hat sich inzwischen längst ein Paradigmenwechsel vollzogen: War der Betrieb von ECM-Software in der Cloud in der Vergangenheit vor allem im deutschen Markt mehr oder weniger verpönt, so hat der Großteil der Unternehmen inzwischen die Vorteile von Cloud-basierten Lösungen erkannt. Für immer mehr Unternehmen lautet das Mantra deshalb inzwischen: „Cloud first!" Vor allem der Mittelstand profitiert davon, da IT-Ressourcen hier meist knapp bemessen sind. Laut Bitkom betreiben 2019 deutlich über die Hälfte der Unternehmen ECM-Lösungen in der Cloud. Das Private-Cloud-Modell ist dabei besonders beliebt: Rund die Hälfte der mittelständischen Unternehmen setzt beim Thema ECM auf eben dieses Betriebsmodell.

Eine ECM-Lösung, die vor allem im Mittelstand aktuell sehr stark nachgefragt wird, ist DocuWare. Dort schlägt sich der Cloud-first-Trend deutlich in den stark wachsenden Umsatzerlösen nieder. So stieg im letzten Geschäftsjahr der Umsatz mit der Cloud-Variante der Lösung um über 90 Prozent im Vergleich zum Vorjahr an. Den größten Teil machten dabei Neukunden aus dem Mittelstand aus. Klassische Beispiele für den Einsatz von DocuWare, das inzwischen bei Ricoh zu den eigenen Bordmitteln gehört, sind die Rechnungsverarbeitung, Buchhaltung und das Personalmanagement. Die „Smart Integration"-Technologie von Ricoh wiederum ermöglicht die schnelle und nahtlose Anbindung der Multifunktionssysteme an DocuWare sowie an viele weitere Cloud-Dienste.

Technologien zur Verbesserung der Arbeit

Der „Digital Workplace" unterstützt Menschen dabei, möglichst effizient und flexibel zu arbeiten. Neue Technologien fördern die mobile und digitale Kommunikation und Zusammenarbeit, Innovationen im Bereich der KI und RPA entlasten Menschen bei Routineaufgaben und der Prozessarbeit und ermöglichen ein produktiveres und kreativeres Arbeiten. Konzepte wie Managed Document Services haben in diesem Zusammenhang eine immense Hebelwirkung und können überdies intelligent mit weiteren Technologien, etwa mit Interactive Whiteboards, verknüpft werden, was den Nutzen und Mehrwert der implementierten Lösung weiter steigert.

Davon profitieren Unternehmen – und auch die Mitarbeiterinnen und Mitarbeiter selbst erwarten zunehmend, dass sich die Arbeit im Zuge des technologischen Wandels und der Automatisierung von Arbeitsabläufen verändert. Eine gute Nachricht, vor allem für den Mittelstand: Die Mehrheit der europäischen Arbeitgeber (61 %) blickt optimistisch auf die Veränderungen, welche die Einführung neuer Technologien am Arbeitsplatz für sie bedeuten. Das ergab die neue „Future of Work"-Studie von Ricoh. Mehr als drei Viertel (77 %) sind außerdem zuversichtlich, dass sie heute schon die notwendigen Fähigkeiten besitzen, um ihren derzeitigen Job auch in den nächsten zehn Jahren ausführen zu können. Dennoch sollten Mitarbeiter bei der Umstellung nicht alleine gelassen werden. Wichtig ist ein strategisches Change Management, das alle Mitarbeiter einbezieht und beim Veränderungsprozess unterstützt. Auch das zeigt die Future of Work-Studie: Vier von fünf befragten Arbeitnehmer bestätigen, dass sie von ihren Arbeitgebern Hilfsmittel und Schulungen für die Weiterbildung erwarten. So können auch kleine und mittelständische Unternehmen die Herausforderungen meistern, die neue Technologien und Automatisierung mit sich bringen.

Niculae Cantuniar

MOBILE DEVICE MANAGE

MIT JAMF PRO APPLE-GERÄTE PROFESSIONELL VERWALTEN

MDM-Lösungen für ein zentrales Endgeräte-Management für Apple-Geräte sind Mangelware. Jamf Pro, die Verwaltungslösung speziell für Unternehmen sowie Organisationen im Bildungs- und Gesundheitswesen, hilft, die Sicherheitslücken in der Apple-Welt in den Griff zu bekommen. Oliver Hillegaart, Regional Sales Manager D/A/CH bei Jamf im Gespräch mit it management-Herausgeber Ulrich Parthier.

Ulrich Parthier: *Die Jamf Produktfamilie besteht mittlerweile aus Jamf Pro, Jamf Now und Jamf Connect. Wie grenzen sich diese voneinander ab?*

Oliver Hillegaart: Jamf Now ist unsere Lösung für Kleinunternehmen und Privatanwender. Mit ihr können bis zu drei Geräte kostenlos verwaltet werden und das ganz ohne technische Vorkenntnisse. Jamf Pro hingegen ist unser Tool für Großunternehmen und verwaltet eine unbegrenzte Zahl an Apple-Geräten in komplexeren Ökosystemen. Mit Jamf Connect haben wir auf die Nachfrage nach einer applespezifischen Lösung für Identitäts- und Zugriffsmanagement reagiert. Die Lösung basiert auf der Software NoMAD des Herstellers Orchard & Grove, die wir im Herbst 2018 akquiriert haben.

Ulrich Parthier: *Sie haben im Juli die Übernahme von Digita Security, einem Entwickler von Endpoint-Protection-Lösungen speziell für Apple-Geräte, bekannt gegeben. Was war der Hintergrund?*

Oliver Hillegaart: Mit der Übernahme haben wir unsere Management-, Authentifizierungs- und Account-Management-Lösungen um eine spezielle Sicherheitslösung für Unternehmen erweitert. Die Anwender profitieren damit künftig von noch besseren Schutzfunktionen gegen Cyberangriffe und Bedrohungen, die speziell auf Apple-Geräte abzielen.

Ulrich Parthier: *War es denn noch zeitgemäß eine neue, spezielle Apple-Lösung zu entwickeln?*

Oliver Hillegaart: Es gibt aktuell viele hervorragende Sicherheitslösungen auf dem Markt. Doch keine dieser Lösungen hat den Fokus auf die besonderen Sicherheitsbedürfnisse von Mac-Geräten. Auch was die Erwartungen der IT- oder Security-Abteilungen und der Anwender in Unternehmen betrifft, fehlt dieser Fokus meist.

Das war der Grund warum Digita Security diese neue Enterprise-Endpoint-Protection-Lösung exklusiv für Apple-Geräte entwickelt hat, basierend auf dem bestehenden Security Framework von Apple.

Mit diesem engen Fokus verfolgten sie den Ansatz, bestehende und neueste Sicherheitsfunktionen für macOS voll auszuschöpfen und zu erweitern. Genau wie Jamf hat sich Digita Security ausschließlich auf Apple-Produkte spezialisiert. Daher kann ein Day-Zero Support bei neuen macOS-Releases gewährleistet werden. Dies ermöglicht IT-Abteilungen einen besseren Einblick in Sicherheitsschwachstellen und damit eine optimierte Nutzung neuer Sicherheitsfunktionen. Zudem sind für Endnutzer stets die neuesten macOS-Funktionen verfügbar.

Ulrich Parthier: *Also handelt es sich um komplementäre Produkte, die sich sinnvoll ergänzen?*

Oliver Hillegaart: Das ist bei unserer gesamten Produktfamilie der Fall. Die neue Sicherheitslösung wird übrigens unter dem Namen „Jamf Protect" ab 2020 auch in Deutschland erhältlich sein. Momentan ist diese nur in den USA verfügbar.

> ES GIBT AKTUELL VIELE HERVORRAGENDE SICHERHEITSLÖSUNGEN AUF DEM MARKT. DOCH KEINE DIESER LÖSUNGEN HAT DEN FOKUS AUF DIE BESONDEREN SICHERHEITSBEDÜRFNISSE VON MAC-GERÄTEN. IN DIESE LÜCKE STÖSST JAMF MIT SEINEM PRODUKTPORTFOLIO.
>
> Oliver Hillegaart, Regional Sales Manager D/A/CH, Jamf, www.jamf.com

MENT FÜR APPLE-GERÄTE

jamf

Ulrich Parthier: *Von Apple-Sicherheitslücken hört man relativ wenig. Was soll das neue Security Framework von Apple leisten?*

Oliver Hillegaart: Zum besseren Verständnis folgendes. Eine gängige Komponente von (vielen) Sicherheitswerkzeugen ist ein Process and File Monitor. Wie der Name schon sagt, überwachen diese Monitore verschiedene Prozess- und Datei-Ereignisse, etwa das Erstellen, Öffnen, Löschen von Dateien. Solche Monitore extrahieren oft „Metainformationen" wie den Prozess-/Dateipfad, Prozessargumente und Prozesscode-Signaturinformationen. Ausgestattet mit einem Process and File Monitor können Sicherheitstools ungewöhnliche oder schädliche Aktivitäten finden.

Bisher war es in früheren Versionen von macOS ziemlich schwierig, einen Process and File Monitor umfassend und akkurat zu erstellen. Der einfachste Weg, diese Aktionen durchzuführen, war innerhalb des Kernels. Da Apple sich schnell bemüht, Kernel-Erweiterungen von Drittanbietern (einschließlich solcher, die von externen Sicherheitsanbietern erstellt wurden) zu verwerfen, war eine andere Lösung erforderlich.

Ulrich Parthier: *Und was hat sich nun grundlegend verändert?*

Oliver Hillegaart: Zum Glück hat Apple mit der Veröffentlichung von macOS 10.15 (Catalina) ein neues User-Mode Framework namens „Endpoint Security" eingeführt. Mit der Einführung dieser neuen Funktion erkennt Apple sowohl den Bedarf an zusätzlichen Sicherheitsmechanismen (also einer umfassenden Verteidigung) als auch die Unterstützung von Drittanbietern an, die diese Rolle übernehmen.

Obwohl Apples Endpoint Security System und Framework sich noch in der Beta-Phase befindet, haben wir das Potenzial erkannt und für Jamfs Day-Zero macOS-Sicherheitstools entworfen. Wir entwickeln bereits intern umfassende Process and File Monitors, die ausschließlich auf dem neuen Endpoint Security Framework von Apple basieren. Solche Monitore werden nahtlos in unser zukünftiges macOS-Sicherheitstool integriert, das in Kürze veröffentlicht wird.

Ulrich Parthier: *MDM-Lösungen für Apple-Devices haben Seltenheitswert. Wie arbeitet Jamf in heterogenen Umgebungen, also wenn Anwender beispielsweise Windows-basierte Systeme einsetzen?*

Oliver Hillegaart: Seltenheitswert würde ich nicht sagen, aber fast alle anderen Lösungen kommen von einem Multiplattformansatz. Das bedeutet, dass oft der kleinste gemeinsame Nenner bestehen bleibt. Wir verfolgen den Ansatz der Ökosysteme, das heißt wir wollen für alle Endbenutzer, dass die Apple User Experience sich auch mit einem MDM-System voll umfänglich entfaltet. Daher fokussieren wir uns ausschließlich auf Apple Betriebssysteme, um das native Apple MDM-Frame für macOS, iOS, iPadOS und tvOS auszuschöpfen. Für macOS bieten wir sogar einen eigenen Agent an. Daher empfehlen wir in heterogenen Umgebungen jeweils im Ökosystem zu bleiben: Microsoft für Windows und Jamf für das Apple Ökosystem. Auf diese Weise können die Vorteile jedes Ökosystems vollkommen ausgeschöpft werden. Beide Ökosysteme lassen sich über unsere AAD (Azure Active Directory) Integration und MS Conditional Access hervorragend miteinander verbinden.

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

DIGITALER DOKUMENTEN

OFFICEMASTER SUITE 7DX – NEUES MAJOR RELEASE VON FERRARI ELECTRONIC

Die Digitalisierung ist eines der Kernthemen in Wirtschaft, Politik und Gesellschaft und zugleich eine der größten Chancenträger und Herausforderungen unserer Zeit. Sich als Unternehmen dieser Entwicklung zu verweigern, ist durchaus fahrlässig. Dennoch sind Skepsis und Unwissenheit, was die Implementierung digitaler Kommunikationslösungen im eigenen Unternehmen betrifft, weit verbreitet. Dabei lässt sich die bereits vorhandene Infrastruktur unter Einsatz intelligenter Dokumentenmanagementsysteme kosteneffizient, unkompliziert und sanft in die digitale Welt migrieren.

„Früher wurde gesagt, die Großen schlucken die Kleinen. Dann: die Schnellen fressen die Langsamen. Aktuell heißt es: die Digitalen fressen die Analogen". Dieses Zitat der Autoren Gerhard Feiler und Gernot Krickl könnte passender nicht sein. Die Digitalisierung schreitet rasend schnell voran und mit demselben Tempo verändern sich auch die Anforderungen, denen Unternehmen, Institutionen und Behörden gegenüberstehen. Von Letzteren wird ein deutliches Mehr an digitalem Service gefordert, der digitale Dialog miteingeschlossen. Gesetzliche Beschlüsse wie das Digitale Versorgung-Gesetz (DVG) reformieren das Gesundheitswesen und ab 2020 sind Unternehmer europaweit zur elektronischen Rechnungstellung für öffentliche Aufträge verpflichtet.

Konzerne setzen auf digitale Agenda

Der digitale Aufbruch ist allgegenwärtig und längst in den Konzernen angekommen. Tatsächlich ist kaum mehr ein großes Unternehmen zu finden, das sich die digitale Transformation nicht auf die Fahne geschrieben hat. Das zeigt auch eine im Juli 2019 veröffentlichte Studie des IT-Beratungs- und Dienstleistungsunternehmens DXC Technology: 71 Prozent der befragten Unternehmen aus Deutschland, Österreich und der Schweiz verfügen über eine digitale Agenda, um sich auf die neuen Anforderungen einzustellen – das ist ein Plus von 22 Prozent im Vergleich zum Vorjahr. Weitere elf Prozent planen, innerhalb des nächsten Jahres eine Strategie für die digitale Reise konkret zu beschließen. Die Aussicht auf positive Umsatzimpulse sind nach den Erfahrungen der Digitalpioniere ebenfalls gegeben: 56 Prozent der Manager zeigen sich mit den Ergebnissen ihrer digita-

AUSTAUSCH – ABER SICHER!

MIT NGDX GEBEN WIR UNSEREN KUNDEN EINE LÖSUNG AN DIE HAND, DIE ES IHNEN ERMÖGLICHT, DAS VOLLE POTENZIAL BEIM RECHTSSICHEREN AUSTAUSCH VON DOKUMENTEN IN IP-UMGEBUNGEN AUSZUSCHÖPFEN.

Stephan Leschke, Vorstandsvorsitzender, Ferrari electronic AG, https://ngdx.ferrari-electronic.de

len Projekte zufrieden und berichten von ersten messbaren Erfolgen.

Digitalisierung im Mittelstand

Es steht außer Frage: Für den Erhalt der Wettbewerbsfähigkeit ist die digitale Transformation unumgänglich und für die effiziente Gestaltung des Arbeitsalltags ein wahrer Segen. Doch längst nicht alle Betriebe können sich mit der Selbstverständlichkeit eines Großkonzerns in das Abenteuer Digitalisierung stürzen. Gerade im Mittelstand dominiert mitunter eine große Unsicherheit, entsprechend zurückhaltend geht er mit Investitionen in diesem Bereich um: Nur jedes fünfte Unternehmen in der EU möchte mehr als fünf Prozent seiner Einlagen für die digitale Transformation aufwenden, verglichen mit 35 Prozent in technologisch weiter fortgeschrittenen Teilen Europas wie Skandinavien. Das zeigt der European Private Business Survey 2019 von PricewaterhouseCoopers.

Dokumentenaustausch – wichtige Stellschraube

In welchem Bereich eines Unternehmens soll die digitale Transformation also ihren Anfang nehmen? Idealerweise in der Kommunikation, denn ein zuverlässiger Austausch – sowohl intern als auch mit externen Partnern – ist der Grundpfeiler jedes erfolgreichen Unternehmens. Hinzu kommt die branchenübergreifende Pflicht, sensible Dokumente auf digitalem Wege rechts- und manipulationssicher auszutauschen.

Genau das ermöglicht die seit Mitte Oktober verfügbare OfficeMaster Suite 7DX des UC-Herstellers Ferrari electronic. Unternehmen verbinden mit dem neuen Major Release ihr E-Mail-System mit den Kommunikationswegen NGDX, Fax, SMS und Voicemail zu einer echten Unified-Communications-Lösung.

Next Generation Document Exchange

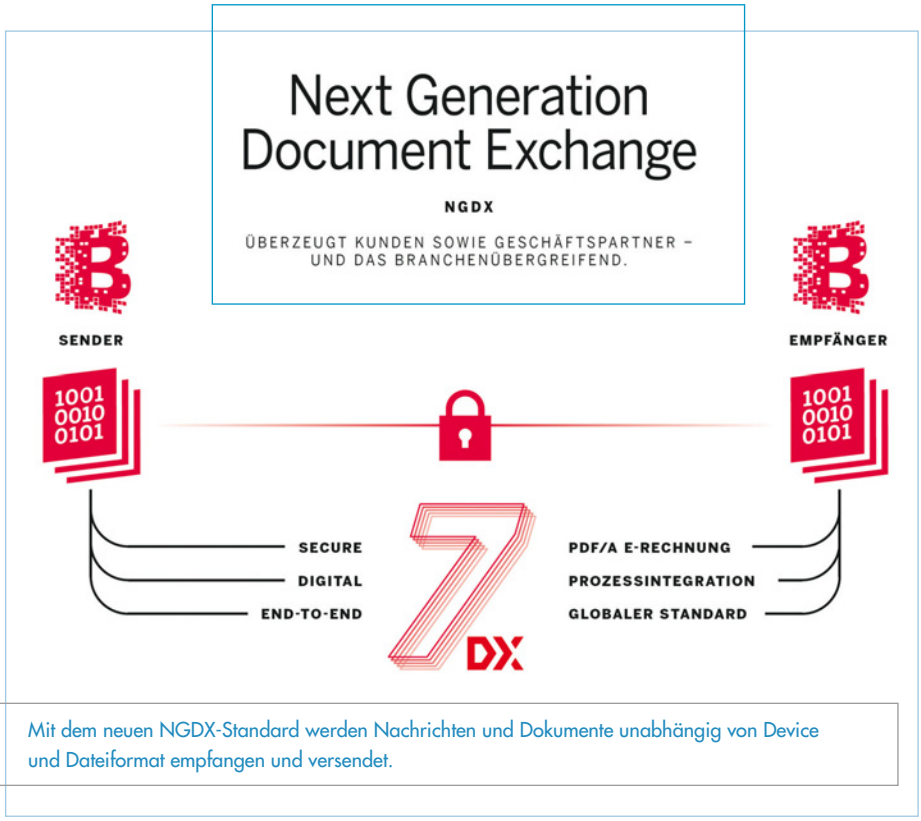
„Next Generation Document Exchange" (NGDX) für den rechts- und manipulationssicheren Dokumentenaustausch in IP-Umgebungen ist die markanteste Neuerung der OfficeMaster Suite 7DX. Ferrari electronic macht damit den Weg frei für die Übermittlung hybrider – von Mensch und Maschine lesbarer – Dokumente wie PDF/A oder das Rechnungsdatenformat ZUGFeRD 2.0. Letzteres ist Voraussetzung für die in absehbarer Zeit gesetzlich verpflichtende elektronische Rechnungsstellung (e-Rechung). NGDX basiert auf modernen ITU-Standards und ist abwärtskompatibel zum etablierten Fax-Protokoll, was den Dokumentenempfang der Gegenstelle sicherstellt, unabhängig von Device und Übertragungstechnologie. Damit stellt NGDX die erste rechtssichere Alternative zur E-Mail dar.

NGDX übermittelt die Dokumente im Original, verlustfrei und End-to-End als PDF an den Empfänger. Formatierungen, Farben und selbst hohe Auflösungen bleiben erhalten. Potenziell schädliche, aktive Inhalte wie Hyperlinks oder Applikationen sind hingegen vom Transfer ausgeschlossen. Die erfolgreiche Übertragung wird mit einem qualifizierten Sendebericht rechtssicher quittiert. Der Dokumentenversand mit NGDX erfolgt dabei in sehr hoher Geschwindigkeit: Bei reiner IP-Übertragung können Dokumente bis zu hundertfach schneller als per Fax übertragen werden – selbst ohne NGDX-Gegenstelle.

Revisionssicherer Datenaustausch dank Blockchain

Kommt es zum digitalen Austausch unternehmenskritischer oder sensibler Daten, sind die Sicherheitsbedenken verständlicherweise groß. Nicht ohne Grund, denn seitdem die Telefonie und das Fax über IP-Strecken geführt werden, ist das Abfangen und Mitlesen von Dokumenten deutlich einfacher geworden. Die Verschlüsselung des Übertragungsweges ist ebenfalls schwierig, da diese beim Passieren von Gateways oder Carriern immer wieder aufgebrochen wird. Unter Einsatz von NGDX sind diese Bedenken allerdings unbegründet – der Sicherheitsaspekt steht an erster Stelle: Sämtliche mit NGDX übertragenen Dokumente werden End-to-End, rechtssicher und verschlüsselt versendet, empfangen und archiviert.

Durch den optionalen Einsatz der Blockchain-Technologie besteht darüber hinaus die Möglichkeit des revisionssicheren Dokumentenaustausches. Indem jedem Geschäftsprozess ein eindeutiger Hashwert zugeordnet und in der Blockchain hinterlegt wird, können die einzelnen Schritte der unendlich vielen Datentrans-



Mit dem neuen NGDX-Standard werden Nachrichten und Dokumente unabhängig von Device und Dateiformat empfangen und versendet.

aktionen transparent und manipulationssicher nachvollzogen werden. So lässt sich jederzeit überprüfen, ob beispielsweise die angegebenen Kunden und Zahlungsziele korrekt sind, welcher Vertragsentwurf final ist oder ob die vorliegende Version auch ursprünglich so unterzeichnet wurde. Für geschäftskritische Dokumente besteht die Möglichkeit eines „digitalen Einschreibens mit Rückschein". Zusätzlich errechnet die OfficeMaster Suite 7DX während des Dokumentenversands eigene Hashwerte und verfügt damit über ein weiteres, in die Software integriertes Sicherheits-Feature.

Wird NGDX in Business-Process-Management-Systeme (BPM) integriert, können die Dateien in Sekundenschnelle digital ausgetauscht und verarbeitet werden. Der gesamte Prozess des Austauschs erfolgt dabei medienbruchfrei, automatisiert und in einem einheitlichen, standardisierten Format. Zeitintensive Routineaufgaben wie die Erfassung und Überprüfung von Rechnungen oder die Dokumentenablage, lassen sich stark vereinfachen.

Im Unternehmen kann dieser Prozess wie folgt aussehen: Der Vertrieb übermittelt die Rechnungsdaten via NGDX vollständig digital, fehlerfrei und maschinenlesbar an die Buchhaltung; eine manuelle Erfassung ist nicht mehr notwendig. Anschließend gehen die Daten zur weiteren Bearbeitung in das BPM über, welches das Sortieren von Dokumenten nach Kunden- oder Versicherungsnummern ermöglicht oder diese automatisch dem richtigen Projektordner zuweist.

Erleichterte Archivierungspflicht

Interessant ist die Möglichkeit der Prozessautomatisierung insbesondere für Unternehmen, die der Archivierungspflicht unterliegen. Sie erfüllen diese oft mithilfe umständlich dokumentierter Prozesse und teurer WORM-Speichersysteme (Write-once-read-many). Ein Nachteil dieser Prozesse ist, dass sich der erfolgreiche Austausch der Dokumente nicht belegen lässt. Anders bei NGDX: Entsprechend des OK-Vermerks eines Fax, sendet das Empfangsgerät nach Erhalt eine Bestätigung über die erfolgreiche Transaktion, die selbst vor Gericht Bestand hat. Dank dieses qualifizierten Sendeberichts lässt sich jederzeit rechtssicher nachvollziehen und belegen, welche Dokumente versendet und empfangen wurden.

Durch die bereits in die OfficeMaster Suite 7DX integrierte Funktion DirectSIP können Dokumente direkt und ohne Einsatz von Telefonanlagen, Routern oder Faxkarten an einen SIP-Trunk oder eine IP-Telefonanlage übertragen werden. Dieser direkte Übertragungsweg ist wesentlich stabiler und zuverlässiger als die bisherigen, zur Verfügung stehenden heterogenen Lösungen. Darüber hinaus lässt sich die Lösung in der DMZ und damit auch ohne Internet- oder Cloud-Anbindung betreiben und ist kompatibel mit allen E-Mail- und Web-Clients sowie Microsoft Exchange 2019 und Notes.

Insbesondere für Microsoft Exchange 2019 – das keine eigene Voicemail-Lösung im Programm hat – ist das Tool die optimale Ergänzung: es verfügt ab Werk über eine Voicemail-Lösung, die sich in zahlreiche Messaging-Systeme integrieren lässt und mit dem neuen Major Release eine erweiterte Sicherheitsfunktion bietet. Um den Serviceaufwand im Unternehmen zu minimieren, ist die OfficeMaster Suite 7DX mit einem Monitoring-Tool für den Versand von Admin Alerts und Update Notifications ausgestattet.

Sanfte Migration in die digitale Zukunft

Die OfficeMaster Suite 7DX ist ohne zusätzliches Anwenderprogramm nach Einrichtung der Telefonverbindung sofort funktionsfähig und lässt sich einfach in ITK-Umgebungen sowie in komplexe Szenarien mit mehreren SIP-Trunks und verschiedensten Groupware-Systemen integrieren. Eine Kopplung an mobile Endgeräte ist ebenfalls möglich. Mit der Kombination dieser Features setzt sie neue Maßstäbe für die professionelle Unternehmenskommunikation und ermöglicht einen manipulations- und rechtssicheren Dokumentenaustausch in IP-Umgebungen.

Stephan Leschke

GEBRAUCHTSOFTWARE-MARKT BOOMT

SO SPAREN CLEVERE IT-VERANTWORTLICHE

Der Markt für Gebrauchtsoftware wächst weiter rasant. Kein Wunder, denn Lizenzen aus zweiter Hand bringen Unternehmen eine Reihe von Vorteilen. In der Regel können sie dadurch 20 bis 50 Prozent im Vergleich zum Neukauf beim Hersteller sparen. Ein weiterer Pluspunkt: Auf dem Sekundärmarkt sind auch Vorgängerversionen erhältlich, die Unternehmen noch mehr Einsparpotenzial bieten. Beim Hersteller ist hingegen immer nur die aktuellste Programmversion verfügbar. Das bedeutet: Kunden, für die beispielsweise aus Kompatibilitätsgründen durchaus eine Vorgängerversion in Frage kommt, müssen beim Hersteller die aktuelle Software kaufen und dann auf die gewünschte Version downgraden. Sie bezahlen also für eine Version, die sie gar nicht nutzen. Hinzu kommt, dass viele Unternehmen die neuesten Features, etwa von Office 2019, auch gar nicht benötigen und mit einer erprobten Vorgängerversion besser bedient sind.

Clevere IT-Verantwortliche prüfen zudem den eigenen Lizenzbestand und verkaufen nicht mehr benötigte Software. Überzählige beziehungsweise ungenutzte Lizenzen entstehen zum Beispiel bei Restrukturierungen und Unternehmenszukäufen oder wenn Anwendungen in die Cloud verlagert wurden. Durch den Verkauf lässt sich der IT-Etat zusätzlich aufstocken, sodass mehr Budget für andere IT-Projekte zur Verfügung steht.

Absolut legal

Die rechtlichen Rahmenbedingungen für den Handel mit Gebrauchtsoftware sind dabei schon seit Langem durch höchstrichterliche Urteile genau abgesteckt. Rechtliche Grundlage ist der sogenannte Erschöpfungsgrundsatz des Urheberrechtsgesetzes. Dieser besagt: Sobald ein Hersteller eine Lizenz erstmalig verkauft hat, ist sein Verbreitungsrecht erschöpft. Der neue Eigentümer darf sie also weiterverkaufen – sofern diese einige Voraussetzung erfüllt: So muss die Lizenz ursprünglich mit Zustimmung des Herstellers im Gebiet der EU oder eines anderen Vertragsstaats des europäischen Wirtschaftsraums in den Handel gebracht worden sein. Außerdem muss der Erst-Käufer für die Software ein Entgelt gezahlt haben, das es dem Rechteinhaber ermöglichen soll, eine angemessene Vergütung zu erzielen. Der Erst-Käufer muss zudem ein unbefristetes Nutzungsrecht inklusive etwaiger Verbesserungen und Aktualisierungen erworben haben. Zudem muss er eventuelle Kopien unbrauchbar machen und darf die Software nicht weiter nutzen.

Erfahrene Händler unbedingt erforderlich

Obwohl der Handel mit Gebrauchtsoftware rechtlich eindeutig geregelt ist, sollten Unternehmen die Umsetzung gemeinsam mit einem erfahrenen Gebrauchtsoftware-Händler abwickeln. Grund hierfür sind unter anderem die komplexen Lizenzbestimmungen der Software-Hersteller und verschachtelte Lizenzhistorien. Zu ermitteln, ob eine Lizenz alle rechtlichen Bedingungen für einen Weiterverkauf erfüllt, ist daher selbst für einen erfahrenen Experten oftmals äußert aufwendig und zeitintensiv.

Ein leistungsstarker Händler greift hier auf umfassendes Know-how sowie lange Erfahrung zurück. Gestützt durch ausgeklügelte Prozesse und Tools, kann er Historien und Rechtssicherheit der gehandelten Lizenzen exakt nachvollziehen und dokumentieren. Kundenorientierte Gebrauchtsoftware-Händler bieten darüber hinaus eine Haftungsfreistellung und unterstreichen so nochmals die volle Verantwortung für den Lizenz-Transfer. Durch eine Vermögensschadenhaftpflicht und vorgangsbezogene Testate von Wirtschaftsprüfern gewähren sie darüber hinaus zusätzliche Sicherheit.

Andreas E. Thyen

> OBWOHL DER HANDEL MIT GEBRAUCHTSOFTWARE RECHTLICH EINDEUTIG GEREGELT IST, SOLLTEN UNTERNEHMEN DIE UMSETZUNG GEMEINSAM MIT EINEM ERFAHRENEN GEBRAUCHTSOFTWARE-HÄNDLER ABWICKELN.
>
> Andreas E. Thyen, Präsident des Verwaltungsrats, LizenzDirekt AG, www.lizenzdirekt.com

WAS MACHT EINEN GUTEN

WICHTIGE SKILLS, MIT DENEN SIE IHR LIZENZMANAGEMENT LANGFRISTIG STÄRKEN

Die Lizensierung von Software und deren Dokumentation steht in zahlreichen IT-Abteilungen nicht an der Tagesordnung. Viele Unternehmen scheitern bereits an der Hürde, einen Verantwortlichen für das Lizenzmanagement zu benennen. Dabei ist ein Lizenzmanager unabdingbar, wenn Sie hohe Kosten für Nach- oder Überlizensierung beziehungsweise rechtliche Konsequenzen vermeiden wollen. Doch was sind eigentlich die Aufgaben eines Lizenzmanagers und welche Eigenschaften runden das Jobprofil ab? In vielen Stellenbeschreibungen herrscht kein Konsens über die entsprechenden Qualifikationen, da es keine konkrete Ausbildung zum Lizenzmanager gibt. Umso wichtiger ist es, sich Gedanken über eine Jobbeschreibung zu machen, sodass Ihre Unternehmenstechnologie inklusive Softwarelizenzen stets sicher und effizient verwaltet wird.

Das Berufsbild des Lizenzmanagers war in der Wirtschaft lange Zeit nicht existent. In vielen KMUs ist das heute noch immer der Fall, da in diesen für das Lizenzmanagement in der Regel der IT-Administrator verantwortlich ist. Dies führt jedoch häufig zu einer Vernachlässigung des Themas, wodurch wiederum finanzielle und rechtliche Konsequenzen drohen. Erster Schritt für Führungskräfte ist es demnach, einen Lizenzverantwortlichen zu benennen. Der zweite Schritt ist eine klare Aufgabendefinition und die Bereitstellung der richtigen Werkzeuge wie einem ganzheitlichen SAM-Tool, sodass der jeweilige Mitarbeiter nicht sämtliche Release-Stände der eingesetzten Programme in einer Excel-Liste überblicken muss.

Aufgaben eines Lizenzmanagers

Ein Lizenzmanager verwaltet die Lizenzen der im Unternehmen eingesetzten Software? Richtig, doch die tatsächlichen Aufgaben eines Lizenzverantwortlichen gehen weit darüber hinaus. Um seinen Verantwortungsbereich adäquat auszufüllen, muss ein Lizenzmanager die Softwarelizenzen nicht nur führen und prüfen, sondern auch optimieren und planen. Dazu gehören unter anderem die Abstimmung und Beratung mit den Mitarbeitern aus sämtlichen unternehmensinternen Fachabteilungen. Auch Preis- und Vertragsverhandlungen im Rahmen der Softwarebeschaffung stehen auf dem Plan eines Lizenzmanagers. Darüber hinaus ist er für das Management zahlreicher Daten verantwortlich, die zum Softwareeinkauf, zur Software-Konsolidierung und Lizensierung herangezogen werden. Auch die zentrale wie auch sichere Aufbewahrung der Lizenznachweise und die klare Definition von Lizensierungsregeln fallen in den Verantwortlichkeitsbereich eines Lizenzmanagers.

Organisations- und Kommunikationstalent

Die klare Definition des Aufgabenbereichs eines Lizenzmanagers ist die halbe Miete. Damit jedoch die passenden Kandidaten für die Stelle ausgewählt werden, ist es von Vorteil, sich auch die nötigen Qualifikationen beziehungsweise Softskills eines Lizenzmanagers bewusst zu machen. Orientiert man sich an dem zuvor beschriebenen Jobprofil, kristallisieren sich klare Kriterien und Stärken heraus. Ein guter Lizenzmanager benötigt dementsprechend:

EIN GUTER LIZENZMANAGER MUSS WIRTSCHAFTLICH, STRATEGISCH, KOMMUNIKATIV UND TECHNISCH HANDELN. IDEALERWEISE ARBEITEN LIZENZMANAGER UND IT-ADMINISTRATOR ENG ZUSAMMEN.

Benedikt Gasch, CTO, DeskCenter Solutions AG, www.deskcenter.com

1. Software- und IT-Know-how

Für die Position im Lizenzmanagement ist ein gewisses Software- und IT-Verständnis unumgänglich. Sicher können Lizenzmanagementposten auch von Mitarbeitern mit kaufmännischem Hintergrund besetzt werden, jedoch sollten diese stets über ein Basiswissen in Sachen Softwareinstallationen, Softwareverträge, Softwareinventarisierung und IT-Strukturierung inklusive Workplaces, Server, Cloud-Technologien und mobile Devices verfügen.

2. Organisationstalent

Ein Lizenzmanager muss nicht nur Lizenzen überblicken oder Rechnungs- und Zugangsdaten managen, auch die Softwarerecherche, die Einhaltung der Lizensierungsregeln und die Kommunikation mit der Managementebene fällt in seinen Verantwortungsbereich. Das erfordert ein gewisses Maß an Organisation, um stets die Kontrolle und die Qualität über die eigenen Aufgaben sicherzustellen.

LIZENZMANAGER AUS?

3. Strategisches Denken

Braucht das Unternehmen diese oder jene Software wirklich? Welche Programme lassen sich zum Beispiel durch andere kompensieren, wie viele Lizenzen müssen zukünftig nachgekauft und welche Bereiche können kostensparend in die Cloud verschoben werden? Diese sowie viele weitere Fragen machen das strategische Ausmaß des Lizenzmanagements deutlich. Als Lizenzmanager gilt es, mit Hilfe von Übersichten und wissensbasierten Systemen den Einsatz und die Nutzungsrechte von Software zu optimieren, zu planen und langfristig den Unternehmensbetrieb zu stärken.

4. Fundierte Kenntnisse über den Unternehmensbetrieb

Welche Software ist wo im Einsatz und welcher Kollege benötigt ein besonderes Programm zum Arbeiten? Ein guter Lizenzmanager kennt das Unternehmen, für das er arbeitet und ist sich der alltäglichen Aufgaben der einzelnen Fachabteilungen bewusst. Nur so kann er bedarfsgerecht Software einkaufen und strategisch den Workflow im Unternehmen sicherstellen.

5. Wirtschaftliche Kompetenzen

Beim Lizenzein- beziehungsweise -nachkauf ist es wichtig den besten Preis zu den besten Konditionen zu finden beziehungsweise herauszuschlagen. Einfach und schnell Softwarelizenzen zu kaufen, kann sich später mitunter teuer rächen. Dementsprechend ist für die Aufgaben des Lizenzmanagers wirtschaftliches Geschick gefragt, um die Kosten für die Softwarelizenzen, den Installationsaufwand und die Organisation der Datenträger und Lizenzschlüssel gegeneinander abzuwägen und das bestmögliche Preis-Leistungsverhältnis zu generieren.

6. Kenntnisse im Vertragsmanagement

Ein guter Lizenzmanager ist nicht nur im IT-, sondern auch im Vertragsmanagement zu Hause. Letzten Endes obliegt es seiner Verantwortung, die rechtlichen Risiken von Lizensierungen zu minimieren und hohe Kosten wegen Verletzung von Lizenzrichtlinien zu verhindern. Darüber hinaus muss er Lizenznachweise und Datenträger sicher und zentral aufbewahren, idealerweise nicht nur in einem feuerfesten Aktenschrank, sondern auch digital in einer Cloud.

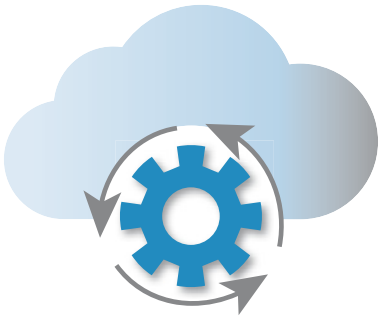
7. Kommunikationsstärke

Die Koordination mit anderen Fachabteilungen, die Preis- und Vertragsverhandlungen oder die Abstimmung mit der Managementebene: Als Lizenzmanager gibt es eine Menge zu besprechen. Dabei muss der Spagat zwischen der strategischen Ausrichtung des Unternehmens und dem Schubladendenken der einzelnen Fachabteilungen gelingen. Für diese Hürde sind hohe kommunikative Fähigkeiten essenziell, sodass einer reibungslosen Lizenzplanung und -verwaltung im Sinne aller nichts mehr im Weg steht.

Hand in Hand

Idealerweise arbeiten Lizenzmanager und IT-Administrator eng zusammen. Auf diese Weise können Inventarisierung, Softwareverteilung und Lizenzmanagement aufeinander abgestimmt und ein ganzheitliches IT-Asset-Management realisiert werden. Ein guter Lizenzmanager tauscht sich daher regelmäßig mit seinen Kollegen aus der IT-Abteilung aus. Nicht selten sind Lizenzmanager und IT-Administrator sogar ein und dieselbe Person. Dies funktioniert allerdings nur, wenn Prozesse und Regeln mit Hilfe einer Software-Asset-Management-Lösung automatisiert werden. Als Folge stehen Lizenzmetriken, Lizenztypen und der aktuelle Softwarebestand auf Knopfdruck bereit, anhand welcher die nächsten Investitionen und Strategien ausgearbeitet werden können.

Benedikt Gasch



WILLKOMMENER NEBENEFFEKT

WIE GEBRAUCHTE SOFTWARE DIE CLOUD-MIGRATION FINANZIERT

Wollen Unternehmen ihre vorhandene IT-Infrastruktur zukünftig als Cloud-Modell betreiben, kann dies kostengünstig umgesetzt werden. So suggerieren es viele Cloud-Anbieter. Tatsächlich aber entstehen Initialkosten, die ein solches Projekt zu einer ausgewachsenen Investition machen. Da passt das Angebot der Firma VENDOSOFT in die Zeit. Der Software-Händler stattet Unternehmen mit Lizenzen von Microsoft und Adobe aus. Nicht mehr benötigte Software – wie sie beim Umstieg auf Mietmodelle entsteht – kauft er zurück. Das finanziert wechselwilligen Firmen einen erheblichen Teil der Cloud-Kosten.

Migration erfordert Investitionen – trotz Mietmodell

Ein Werbeversprechen von Cloud-Anbietern wie Microsoft ist der schnelle und kostengünstige Wechsel für Unternehmen. Richtig ist, dass „in der Cloud" keine hohen Investitionen für Infrastrukturen, Plattformen und Services notwendig sind. Dank Abo-Modell zahlt ein Unternehmen nur, was es an Software tatsächlich nutzt. Auch die Migration ließe sich theoretisch innerhalb von Stunden oder Tagen vornehmen, denn ein virtueller Firmenserver ist in wenigen Minuten eingerichtet. Der gesamte Umzug aber erfordert eine strategische und organisatorische Vorbereitung – das braucht Vorlauf.

Und spätestens damit ist klar: Kostenlos ist so ein Umstieg nicht! Er kostet Ressourcen. Prozesse müssen angepasst oder neu entwickelt werden, Architekturen verändert und Change Management betrieben werden (schließlich wollen die Veränderungen nachhaltig und maximal effizient im Unternehmen verankert werden). Üblicherweise werden Ausgaben dieser Dimension über Kredite oder Kapitalerhöhungen finanziert.

Die Alternative zur Finanzierung der Cloud

An dieser Stelle tritt die VENDOSOFT GmbH auf den Plan. Bezieht ein Unternehmen seine Microsoft Cloud über den oberbayrischen Software-Anbieter, gewinnt es in vielfacher Hinsicht: Es erhält die Cloud-Lösungen zu besonders günstigen Konditionen. Zertifizierte Microsoft Licensing Professionals begleiten das gesamte Projekt bis zur Migration. Und VENDOSOFT-Cloud-Kunden profitieren vom Kerngeschäft des Resellers: dem Handel mit gebrauchten Softwarelizenzen.

KOSTENLOS IST EINE MIGRATION NICHT! SIE KOSTET RESSOURCEN. PROZESSE MÜSSEN ANGEPASST ODER NEU ENTWICKELT WERDEN, ARCHITEKTUREN VERÄNDERT UND CHANGE MANAGEMENT BETRIEBEN WERDEN.

Björn Orth, Geschäftsführer, VENDOSOFT GmbH, www.vendosoft.de/cloud

Ein beachtlicher Teil der finanziellen Mittel, die der Wechsel in die Cloud verschlingt, steckt in den firmeneigenen On Premises Assets. Also in Microsoft Servern, Büroanwendungen und Zugriffslizenzen, die nach der Umstellung auf Miet-Software nicht länger benötigt werden. Verkauft das wechselwillige Unternehmen diese Lizenzen als gebrauchte Software, generiert es die benötigten liquiden Mittel quasi aus sich selbst heraus.

VENDOSOFT monetarisiert also überschüssige Computerprogramme und finanziert Unternehmen so den Umstieg in die Cloud. Ein Service, den selbstredend jede Firma, Behörde, jeder Verein und Gewerbetreibende in Anspruch kann, bei der oder dem ungenutzte Software Assets schlummern. Diese entstehen nicht nur bei der Migration in die Cloud, sondern über die Jahre in fast jedem Unternehmen. Beispielsweise durch die Zusammenlegung von Abteilungen, durch Outsourcing oder Insolvenzen.

Der Verkauf solcher nicht mehr benötigter Gebrauchtsoftware hat für Unternehmen genau genommen zwei Vorteile: Es schafft liquide Mittel und verringert den Aufwand, den die Verwaltung der Lizenzen mit sich bringt. Ein verschlanktes Software Asset Management ist also ein willkommener Nebeneffekt zur Aufstockung der IT-Budgets!

Björn Orth

CYBERSICHERHEIT

WENN APIs DAS NIVEAU ANHEBEN

In einer überwiegend digitalen Welt wird die zunehmende Vernetzung oft als Gefahr für die Cybersicherheit wahrgenommen. Kann letztere durch APIs erhöht werden?

Stellen Sie sich folgendes Szenario vor: Nach dem Informationsaustausch zwischen der Firewall und der SIEM-Konsole wird eine Maschine, die Schadprogrammen ausgesetzt ist, ohne menschlichen Eingriff unter Quarantäne gestellt. Das ist das Versprechen der APIs („Application Programming Interfaces") im Cybersicherheits-Umfeld. Sie sind in der Lage, einen Dialog zwischen Fehlererkennungslösungen und anderen Systemen herzustellen, die geeignete Gegenmaßnahmen ergreifen können.

Die Python-API von Stormshield

Stormshields Python-API ermöglicht es Anwendungen und Produkten von Dritten, sich direkt mit den Stormshield-Network-Security-Firewalls (SNS) zu verbinden, damit Befehle erteilt werden, ohne dafür auf die klassische Benutzerschnittstelle zurückgreifen zu müssen. „Das ist der Grundstein für zukünftige intelligente Systeme", erklärt Uwe Gries, Country Manager DACH bei Stormshield.

Ein weiteres Beispiel ist „Stormshield Data Security" (SDS): Ein mithilfe der Stormshield-SDS-Connector-API gesteuertes Programm kann Dateien verschlüsseln, die von einer Data-Loss-Prevention-Software Dritter als sensibel gekennzeichnet wurden.

Wenn APIs im Dienst der Sicherheit stehen

Neben der Sicherstellung, dass Warnmeldungen von den dafür bestens geeigneten Sicherheitssystemen verarbeitet werden, können APIs auch für Orchestrierungszwecke sehr nützlich sein. Bei der Installation einer virtuellen Maschine oder einer neuen Anwendung kann ein Orchestrierungswerkzeug wie Ansible die API nutzen, um sowohl die Grundkonfiguration der Firewall als auch spezifische Einstellungen basierend auf vordefinierten Optionen automatisch vorzunehmen. Dadurch werden die Sicherheitsregeln ebenfalls automatisch mitkonfiguriert.

Die Schattenseiten der APIs

Ungeachtet der Versprechen der APIs, darf die für deren Integration erforderliche Investition nicht unterschätzt werden. „Diese Vernetzungsprojekte sind komplex, kostspielig und benötigen eine lange Umsetzungszeit, da sie eines hohen Maßes an Dienstleistungen und technischer Unterstützung bedürfen", warnt Gries. „Nicht zuletzt muss auch die Zeit für die Schulung des Personals, insbesondere der Entwickler, mitberücksichtigt werden", denn eine tiefgehende Vorbereitung im Vorfeld ist unerlässlich, um die Personalressourcen optimal zu nutzen. Gleichzeitig sollten Hersteller die Tatsache berücksichtigen, dass Entwickler und Produkte aus verschiedenen Bereichen in der Lage sein müssen, zusammenzuwirken.

Der Aspekt „Cybersecurity by Design" ist zudem von entscheidender Bedeutung. Da diese Art der Vernetzung direkten Einfluss auf die Funktionsweise von Sicherheitslösungen nimmt, müssen Vertraulichkeit und Integrität der ausgetauschten Informationen gewährleistet sein. Dies macht die Sicherheit der APIs selbst zu einem zentralen Anliegen.

Fazit

Wenn die Sicherheitsregeln während der Designphase eingehalten werden, können APIs die Gesamteffizienz von Cybersicherheitslösungen erhöhen. Durch den privilegierten Informationsaustausch erleichtern APIs die Implementierung von Sicherheitslösungen, verbessern die Leistung des Sicherheitssystems und minimieren menschliche Fehler im Alltag. Die Vorteile solcher offenen, automatisierten Lösungen sind bei Notfällen besonders begrüßenswert.

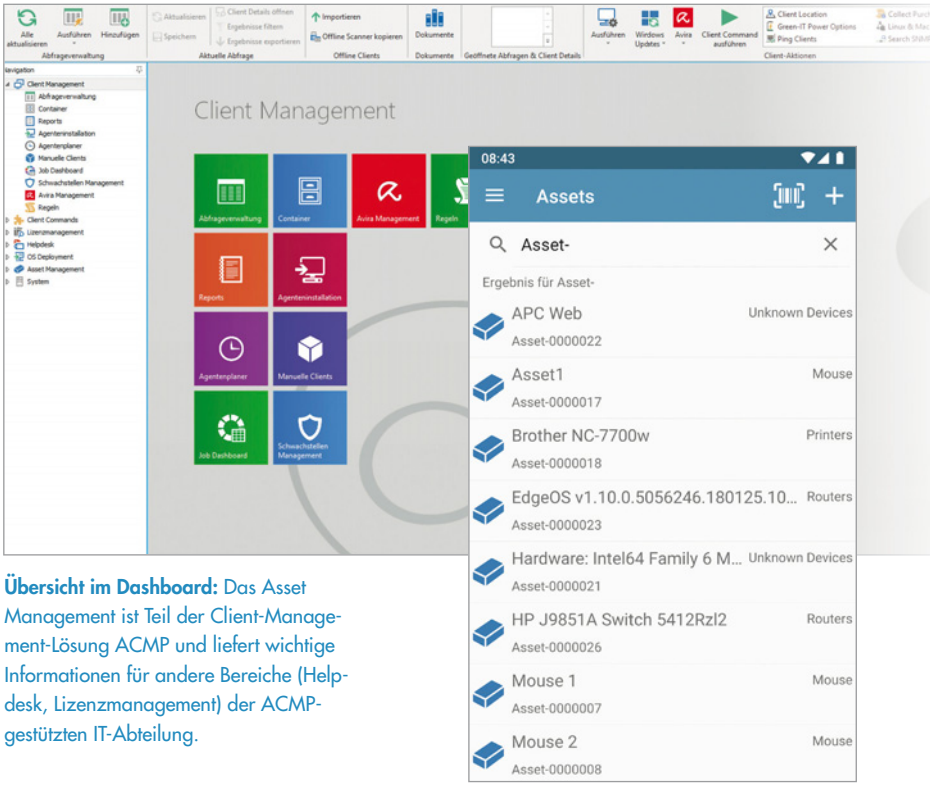
www.stormshield.com

ASSET MANAGEMENT À LA

STETS ALLES IM ÜBERBLICK

Ein leistungsstarkes Asset Management liefert sowohl dem IT-Verantwortlichen als auch dem Controlling einen schnellen und kompletten Überblick über die Anlage- und Sachgüter eines Unternehmens. Die ACMP-Suite von Aagon geht noch einen Schritt weiter, denn im Gegensatz zu anderen Tools erfasst und verwaltet es nicht nur das komplette IT-Equipment wie Computer, Tastaturen, Mäuse, Software, Monitore und Mobilgeräte, sondern auch die zum Arbeitsplatz gehörenden Tische und Stühle: ein unschätzbarer Vorteil sowohl für den IT-Verantwortlichen als auch für das Controlling. Die Suche nach im Unternehmen „verschollenen" Druckern, Bürostühlen und sonstigem Equipment gehört somit ab sofort der Vergangenheit an.

Jeder IT- und Kostenverantwortliche kennt das Problem, wenn eine Übersicht über alle aktuellen Assets – also IT-Equipment, Büromöbel und andere Sachgüter – anzufertigen ist: Im Allgemeinen setzt dies einen aufwändigen Suchprozess in Gang, bei dem zahllose Ordner, Dateien und sogar auch Lager oder Arbeitsplätze vor Ort zu überprüfen sind. Abhilfe schafft das Asset-Management-Modul der ACMP-Suite, das speziell auf die Bedürfnisse des IT-Administrators sowie des Controllings zugeschnitten wurde: Es ordnet und verwaltet alle Anlagegüter des Unternehmens, gruppiert die einzelnen Objekte, weist diese definierten Personen, Kostenstellen und Abteilungen zu und lässt sich überdies konkurrenzlos einfach bedienen.



Übersicht im Dashboard: Das Asset Management ist Teil der Client-Management-Lösung ACMP und liefert wichtige Informationen für andere Bereiche (Helpdesk, Lizenzmanagement) der ACMP-gestützten IT-Abteilung.

Mobile Lösung: Das ACMP Asset Management ist auch als App verfügbar. So haben Nutzer mobil jederzeit Zugriff auf die wichtigsten Informationen und Funktionen der gespeicherten Daten.

Mit dem Asset Management hat die Geschäftsführung stets einen vollständigen Überblick über alle verfügbaren Assets, kann Geräte nach Kostenstellen, Benutzern und Standorten sortieren und zudem Abschreibungssummen, Anschaffungskosten sowie Garantiedaten berechnen. Richtig eingesetzt, verknüpft die Lösung die Abläufe des IT- mit dem Business-Bereich, bildet den Lebenszyklus der Assets von der Beschaffung bis zur Entsorgung ab und liefert Entscheidern eine wertvolle Planungsgrundlage für Neuanschaffungen beziehungsweise optimalen Einsatz der Assets. Bei der Entwicklung dieses Tools hat das Aagon-Team die Anforderungen der IT-Administratoren exakt umgesetzt.

Die wichtigsten Vorteile im Überblick

Umfangreiches Rechtemanagement und unterschiedliche Benutzergruppen: Die Lösung ist mit einem umfangreichen Rechtemanagement ausgestattet, über das sich definieren lässt, welcher Anwender welche Assets einse-

AAGON

hen kann und in wessen Händen die der Verwaltung der Sachgüter liegt. So sieht jeder Anwender nur diejenigen Sachgüter, die für seine Arbeit erforderlich sind. Beispielsweise haben der Facility Manager und der Empfang nur Einsicht in die gespeicherten Firmenfahrzeuge, das Controlling und die Geschäftsleitung dagegen können die Komplettübersicht abrufen.

Lifecycle: Ebenfalls komfortabel verwalten lassen sich Details zur Anschaffung, dem Betrieb, der Nutzungsdauer und der Ausmusterung von Anlagegütern. Hilfreich ist dieses Feature unter anderem für Behörden, die hier im Handumdrehen abrufen können, wofür ein bestimmtes IT-Budget investiert wurde und wie lange oder wo die einzelnen Assets im Einsatz sind.

Integrierte Report-Engine: Auch diese Funktion erweist sich als äußerst hilfreich im Arbeitsalltag. Sie erstellt etwa für jeden neuen Mitarbeiter einen Ausgabezettel mit allen Assets (Laptop, Smartphone, Stuhl, Beamer), die zum Arbeitsplatz gehören. Scheidet der Mitarbeiter aus, so lässt sich blitzschnell überprüfen, ob die Gegenstände vollständig sind. Zudem druckt die Report-Engine etwa für Tische und andere Komponenten Barcode-Aufkleber aus, in denen alle erforderlichen Daten hinterlegt sind.

Logische Zusammenfassung von Assets: Das Tool ermöglicht eine gemeinsame Verwaltung von Büroausstattungen (Drucker / Schnittstelle oder Beamer / Tasche / Fernbedienung), so dass diese Assets bei einer Weitergabe an eine andere Abteilung immer als zusammengehörende Einheit behandelt und verwaltet werden. Hier kann der Empfänger auf einen Blick feststellen, ob alle Komponenten vorhanden sind. Ähnlich funktioniert der Verleih-Prozess: Die Asset-Collection erkennt, ob alle erfassten Assets, wie Firmenwagen plus Fahrtenbuch, Schlüssel und Tankkarte gemeinsam weitergeben werden.

Ein weiteres wichtiges Merkmal von ACMP Asset Management ist seine einfache und komfortable Bedienung sowie seine flexible Erweiterbarkeit. Je nach Bedarf lassen sich beliebig viele Tabellen und Felder definieren – feste Formatvorgaben kennt das Programm nicht.

Die Vorteile auf einen Blick

- Flexibel erweiterbar durch beliebig viele individuelle Tabellen und Felder – losgelöst von festen Formatvorgaben
- Einfacher Import bestehender Datensätze
- Zuordnung von Standorten, Kostenstellen, Kontakten
- Unterschiedliche Benutzergruppen, das heißt Sichtbarkeiten, Zugriffs- und Editierbeschränkungen
- Garantiedatenerfassung
- Gruppierung von Assets / Bildung von Sets
- Integrierte Report-Engine für Berichte für unterschiedlicher Fragesteller im Unternehmen
- Status- und Nutzungsänderungen nachvollziehbar (Historie)
- Zentrales Dokumentenmanagement (Verträge, Rechnungen, Anleitungen, Scans etc.)
- Verleihverwaltung
- Plausibilitätsprüfung
- Logische Zusammenfassung von Assets – individuell anpassbar
- Lifecycle: Anschaffung – Betrieb – Ausmusterung von Assets
- Planungs- und Entscheidungssicherheit

Das ACMP Asset Management ist nicht nur als weiteres Modul vollständig in die ACMP-Suite integriert, sondern liefert auch einen völlig neuen Ansatz im Bereich IT Asset Management. Die Schwerpunkte liegen in einer problemlosen und effizienten Erfassung der IT-Sachgüter, hoher Flexibilität sowie einfacher Handhabung.

Besonderes Feedback für das Asset Management von Aagon gab es jüngst beim „Professional User Rating 2020" des Marktforschungsunternehmens techconsult im Bereich IT-Operations. Hier gab es eine überdeutliche Erstplatzierung für ACMP, das vor allem durch Spitzenwerte bei Benutzerfreundlichkeit, Funktionsumfang und Innovation überzeugen konnte.

Die neueste Entwicklung für das ACMP Asset Management ist eine App, über die sich Hardware, Anlage- und Sachgüter mobil inventarisieren und verwalten lassen. Das Anlegen, Bearbeiten und Löschen sowie das Zusammenfassen in Asset Collections gehören zu den Grundfunktionen der App. So haben Anwender auch mobil jederzeit Zugriff auf die relevanten Informationen der Anlage- und Sachgüter des Unternehmens. Ein integrierter Barcode-Scanner zum Einlesen von QR-Codes beschleunigt und erleichtert die Inventarisierung, Zuordnung und Integration der Assets.

Alexander Stühl | www.aagon.de

Foto: stock.adobe.com | maxoidos

LAGERHALTUNG DER ZUKUNFT

ERP GESTÜTZTE INVENTUR

Egal ob Händler oder Produktionsbetrieb: Korrekte Bestände sind ein elementarer Baustein für einen reibungslosen Prozessablauf, die Einhaltung der Liefertermintreue und somit Grundlage für eine hohe Kundenzufriedenheit. Die Basis ist, neben einer einwandfreien Bestandsführung, die Inventur. Der folgende Überblick beschäftigt sich mit der Durchführung einer Inventur mit ERP-Unterstützung und den damit verbundenen Vorteilen.

Die sicherlich geläufigste und am häufigsten genutzte Methode ist die Stichtagsinventur. Bei dieser Art der Inventur werden die Bestände zu einem vorher definierten Stichtag gezählt (Istwerte) und die Ergebnisse mit den Sollwerten aus dem ERP-System abgeglichen.

Die Erfassung der Bestände kann mittels vorgefertigter Inventurlisten (Zähllisten) durchgeführt werden. Das ERP-System erzeugt dabei Listen der bestandsgeführten Artikel, zum Beispiel abgegrenzt nach Lagerort oder Artikelgruppe, sodass die zu bearbeitenden Bereiche für das Inventurpersonal etwa möglichst zusammenhängend definiert sind. Je nach Funktionsumfang des ERP-/Warenwirtschaftssystems können diese Listen um verschiedene Sollwerte ergänzt werden. Ein nachgelagerter Abgleich dieser Sollwerte mit den Istwerten ermöglicht die Erstellung von Differenzlisten, um etwa dramatische Ausreißer zu identifizieren und im besten Falle die Ursache dafür zu ermitteln sowie diese zu beheben. Eine andere Möglichkeit, die Eingabe zu vereinfachen, ist die direkte Eingabe der ermittelten Realwerte in die Maske des ERP-Systems oder das Einlesen dieser über eine Schnittstelle, wenn mangels verfügbarer Datenfernübertragung nicht auf das ERP-System zugegriffen werden kann und die Erfassung erfolgt.

Optimierung der Prozesseffizienz

Eine präzisere und weniger fehleranfällige Verfahrensweise stellt die Erfassung per Barcode dar. Das bedeutet zunächst einen hohen, jedoch einmaligen, Aufwand bei der Einführung des Systems. Dieser relativiert sich durch eine hohe Zeitersparnis bei der Erfassung, da die Materialnummer und der Lagerplatz nicht manuell eingegeben werden müssen. Dies führt wiederum zu einer reduzierten Fehleranfälligkeit bei der Eingabe sowie zu einer Optimierungen der Prozesseffizienz.

Neben der Unterstützung bei der eigentlichen Erfassung bietet ein ERP-System auch bei vor- und nachbereitenden Schritten hilfreiche Features. So können bei der Planung und Organisation verschiedene Funktionalitäten einer integrierten Lagerverwaltung die Durchführung der Inventur erleichtern.

Einen weiteren Aspekt, der ab einer gewissen Unternehmensgröße kaum mehr manuell zu bewältigen ist, stellt die anschließende Bestandsbewertung dar. Nicht zuletzt, weil die Qualität und Transparenz dieser Bewertung maßgeblich für eine reibungslose Steuerprüfung sind. Durch lückenlos protokollierte Vorgänge, die sich im ERP-System nachvollziehen lassen, können mit vergleichsweise wenig Aufwand jederzeit solche Bestandsbewertungen durchgeführt werden. Aus den gesammelten Informationen lässt sich zudem die aktuelle Gesamtsituation sowie die Entwicklung einzelner Artikel erkennen, sodass bestenfalls eine Sortimentsoptimierung daraus hervorgeht.

Korrekt und schnell

Abschließend bleibt festzustellen, dass eine ERP-basierte Inventur im Ergebnis korrekte Lagerbestände ermittelt, eine optimale Bedarfsplanung ermöglicht und so zu geringeren Lagerkosten und einer höheren Liefertermintreue sowie zur Reduzierung der Lieferzeit beiträgt. Dies gilt auch für die nicht näher betrachteten Inventurverfahren, wie die permanente Inventur und die Stichprobeninventur, da sich diese statistischer Methoden bedient.

Philipp Wodan, Christine Schuhmacher
www.caniaserp.de

IT GEHT IN FÜHRUNG

IT ENTSCHEIDERTREFF: DILK, DIE 2.

Zum zweiten Mal trafen sich über 1.400 IT-Verantwortliche zum Deutschen IT-Leiter-Kongress in Düsseldorf. Mit vor Ort waren Michael Gloss, Initiator des DILK und Geschäftsführer bei der Wolters Kluwer Deutschland GmbH und Ulrich Parthier, Publisher it management.

Ulrich Parthier: *Herr Gloss, der DILK 2019 ist nun schon Geschichte. Wie zufrieden sind sie mit der Veranstaltung?*

Michael Gloss: Wichtig ist uns, dass die Teilnehmer/innen begeistert sind. Aus den Gesprächen haben wir mitgenommen, dass sowohl Teilnehmer, Partner und Referenten sehr zufrieden sind. Dafür spricht insbesondere die hohe Wiederanmeldequote. Dies führt zu einem kontinuierlichen Wachstum des Kongresses. Mit diesem Ergebnis sind wir als Veranstalter sehr zufrieden.

Ulrich Parthier: *Das Motto der Veranstaltung lautete „IT geht in Führung". Was verbirgt sich hinter dem Motto?*

Michael Gloss: Die IT ist Innovationstreiber, sie steht für Progressivität und für Zukunftsthemen. Neben den aktuellen Fragestellungen zeigen wir Trends auf, klären in welche Richtung es gehen wird und welches Handwerkszeug dafür notwendig ist. Die Vermittlung von Führungs-, Management und Technologiekompetenz ist hierbei die Erfolgsformel.

Ulrich Parthier: *Welche Highlights können die Teilnehmer 2020 erwarten?*

Michael Gloss: Das Programm steht bereits in weiten Teilen, aber natürlich lebt das Programm und wir reagieren kurzfristig auf aktuelle Entwicklungen. Grundsätzlich bietet unser Programm einen spannenden Mix aus rund 80 hochkarätigen Fachreferenten, Überraschungsspeakern und Prominenten, wie zum Beispiel:

Felix Thönnessen, Deutschlands erfolgreichster Unternehmer- & Gründercoach mit dem Vortrag: „Vom IT-Leiter zum Innovation Rockstar! – So digitalisieren Sie Ihr Business",

Dr. Julian Hosp, internationaler Blockchain-Guru: „Blockchain – Hit oder Hype? – Was jetzt für Ihr Unternehmen möglich ist und wovor Sie sich in Acht nehmen müssen",

Prof. Dr. Dr. Ayad Al-Ani, Zukunfts- & Organisationsforscher: „CIOs als Zukunftsstrategen?! – Warum IT die Souveränität und Überlebensfähigkeit deutscher Unternehmen sichert" oder

Dr. Mai Thi Nguyen-Kim, Deutschlands bekannte Wissenschaftlerin & Quarks-Moderatorin: "Dumm durch Overload – Wie Digitalisierung Bildung gefährdet und was Sie als IT-Entscheider dagegen tun können."

DIE IT IST INNOVATIONSTREIBER, SIE STEHT FÜR PROGRESSIVITÄT UND FÜR ZUKUNFTSTHEMEN. NEBEN DEN AKTUELLEN FRAGESTELLUNGEN ZEIGEN WIR TRENDS AUF, KLÄREN IN WELCHE RICHTUNG ES GEHEN WIRD UND WELCHES HANDWERKSZEUG DAFÜR NOTWENDIG IST.

Michael Gloss, Geschäftsführer, Wolters Kluwer Deutschland GmbH, www.wolterskluwer.de, www.deutscher-it-leiterkongress.de

Ulrich Parthier: *Welche Themen stehen aktuell auf der Agenda der IT-Leiter in den kommenden 12 Monaten bis zum nächsten DILK?*

Michael Gloss: Laut einer aktuellen Umfrage von Oxford Economics antworteten 63 Prozent der IT-Entscheider auf die Frage, worauf es denn aus ihrer Sicht bei ihrem Job besonders ankomme, dass „Geschäfts-, Management- und Führungsqualitäten inzwischen wichtiger sind, als reines Technologieverständnis. Darauf müsse sich ein erfolgreicher CIO konzentrieren!". Ansonsten sind natürlich weiterhin Themen wie Cloud Management, Cybersecurity und Big Data top aktuell. Ebenso die Digitale Transformation und was es für die IT und die Geschäftsmodelle bedeutet. Künftig werden auch alle Aspekte rund um die Künstliche Intelligenz und Augmented Reality eine stärkere Rolle spielen.

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

BUSINESS NETWORKS

NEUES BUZZWORD ODER ZUKUNFTSTECHNOLOGIE?

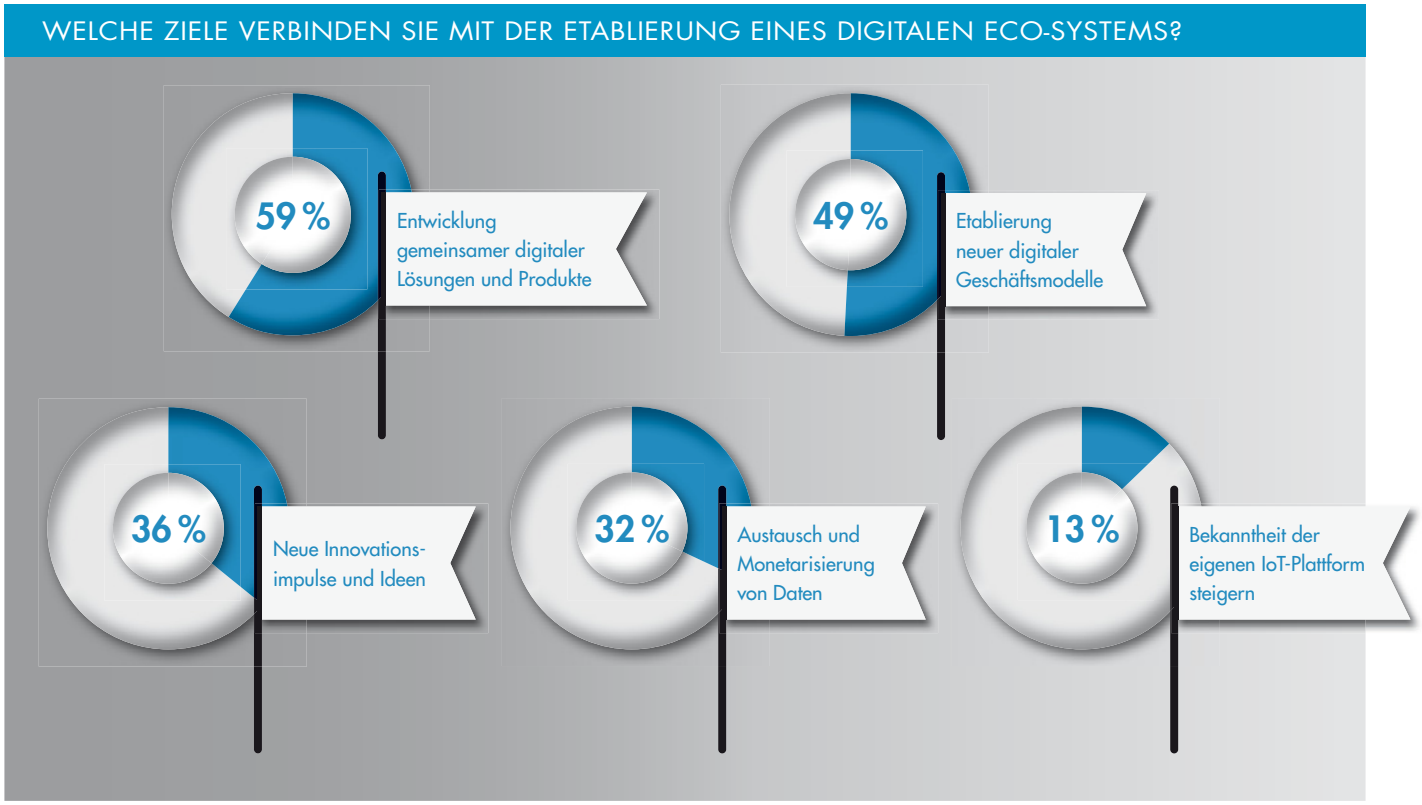
Bereits mehr als ein Drittel der deutschen Unternehmen hat inzwischen konkrete Erfahrungen mit der Umsetzung von IoT-Projekten, besagt eine aktuelle Studie von Crisp Research. Allerdings gibt es nur wenig Übung mit deren Betrieb, denn lediglich 15 Prozent der Unternehmen nutzen IoT-Lösungen im operativen Geschäft. Dabei ist diese Technologie wesentlicher Bestandteil moderner Ecosysteme und ein Erfolgsfaktor von morgen.

So wundert es kaum, dass 32 Prozent der Unternehmen digitale Ecosysteme als strategischen Erfolgsgaranten einstufen und 59 Prozent sogar schon gemeinsam mit Partnern entsprechende Lösungen entwickeln. Die damit verbundenen technologischen Herausforderungen, wie zum Beispiel Schnittstellen, sind schon lange kein Thema mehr und auch die grundlegende technische Infrastruktur hat man im Griff. Aber an einer Stelle hapert es noch: Den Kunden beziehungsweise Anwendern im B2B-Umfeld ist der Mehrwert digitaler Ecosysteme nur schwer zu vermitteln, was daran liegt, dass die Vorteile im B2B-Bereich nicht so schnell spürbar sind wie im B2C-Sektor.

Es geht also darum, den Kunden die Win-Win-Situation aufzuzeigen, sprich Unternehmen, die den Auf- und Ausbau eines Ecosystems planen, sollten bei ihren Überlegungen den Kunden und seine Bedürfnisse in den Mittelpunkt stellen. Nur wer sich „customer centric" aufstellt, wird langfristig in der Lage sein, aus einem Ecosystem ein erfolgreiches Business-Netzwerk zu entwickeln.

Bedarfsgerechte Plattformen schaffen

Was heißt das? Der zentrale Antriebsfaktor für ein Ecosystem ist letztendlich dessen Nutzung. Ein Beispiel: Wenn ein Autohersteller eine Serviceplattform entwickelt, um Autofahrer, Werkstätten oder Zulieferer miteinander zu vernetzen, der Autofahrer aber letztlich kein Interesse daran hat, weil ihm die vorhandenen Informationen und Meldungen direkt vom Auto ausreichen, wird die Serviceplattform nicht funktionieren. Hätte der Autohersteller aber im Vorfeld seine Kunden eingebunden, wäre ihm schnell klar geworden, welche Erwartungen der Kunde an eine Serviceplattform hat. Ergo ist es wichtig, zu allererst den Bedarf zu ermitteln, bevor man sich für den Aufbau eines Ecosystems entscheidet.



Quelle: Crisp Research AG, Erfolgreiche Geschäftsmodelle mit IoT-Plattformen und Eco-Systemen, Seite 49

NUR WER SICH „CUSTOMER CENTRIC" AUFSTELLT, WIRD LANGFRISTIG IN DER LAGE SEIN, AUS EINEM ECOSYSTEM EIN ERFOLGREICHES BUSINESS-NETZWERK ZU ENTWICKELN.

Lumir Boureanu,
Geschäftsführer compacer GmbH,
www.compacer.com

Darüber hinaus sollte man bedenken, dass es ja auch bereits Ecosysteme gibt und es eventuell mehr Sinn macht, sich solch einem System anzuschließen, als ein eigenes zu entwickeln. Betrachtet man allein den internationalen Status Quo bestehender Ecosysteme wird deutlich, dass der amerikanische Markt mit Microsoft, Apple, Alphabet, Amazon, Salesforce & Co. mit Abstand führend ist. Lediglich Unternehmen aus dem asiatischen Raum wie Samsung, Alibaba und Tencent können noch mithalten – europäische Ecosysteme dagegen gibt es so gut wie keine – SAP einmal ausgenommen. All diese Konzerne positionieren sich als Ecosystem-Anbieter: Sie verstehen sich als Knotenpunkte in Netzwerken von Kunden, Lieferanten und Produzenten komplementärer Dienstleistungen. Sie haben es geschafft, sich von den herkömmlichen Geschäftsmodellen zu lösen, neue Wege einzuschlagen und sich die Vorteile innovativer Technologien zu eigen zu machen. Es ist ihnen gelungen, durch Netzwerk-Effekte ganz andere Businessmodelle zu entwickeln und zu etablieren, als es früher der Fall war.

MVP - Klein, aber fein

Damit der Umstieg auf zukunftsweisende Ecosysteme gelingt, sollten Unternehmen mit Funktionen starten, die wesentliche Mehrwerte liefern. Es lohnt sich durchaus mit einem Minimum Viable Product (MVP) zu beginnen. Der Grundgedanke dieser Vorgehensweise ist, mit einer Minimalversion des angedachten Produkts zu starten, um dann schrittweise, in Interaktion mit den Kunden, Mehrwerte für beide Seiten zu entwickeln. Das hat mehrere Vorteile, zum einen sind die Einstiegshürden und -kosten für das Unternehmen nicht so hoch und zum anderen können Marktimpulse und -veränderungen schnell und agil bei der Produktentwicklung aufgegriffen werden. Kurz gesagt: Nicht einmal der große Riese „Amazon" hat als eine globale Plattform gestartet, sondern sich durch sukzessive MVP-Einsätze zu einem Business Network entwickelt. Doch auch bei dieser Methode ist und bleibt es eine große Herausforderung, ein System zu etablieren, das die Anforderungen der digitalen sowie der physischen Welt zusammenbringt.

Ein Beispiel: eScooter können inzwischen in vielen Großstädten ausgeliehen werden. Die Abwicklung dieses physischen Ausleihprozesses wird letztlich über eine digitale Plattform gesteuert und abgewickelt. Denkbar wäre, diese Plattform und deren Kunden mit weiteren Services zu bedienen, etwa mit Informationen zu Veranstaltungen in der jeweiligen Stadt oder auch mit der Möglichkeit, Tickets für den ÖPVN zu buchen. Gleichzeitig könnte man den Nutzern des ÖPNV proaktiv das Ausleihen von eScootern anbieten. So könnte sich das MVP eScooter zu einem regionalen Ecosystem entwickeln oder dazu beitragen.

Dieses kleine Beispiel zeigt, wie vielseitig und reichweitenstark sich Businessideen unter Zuhilfenahme von IoT und digitalen Netzwerken entwickeln können. Dass es sich bei digitalen Ecosystemen um einen ernstzunehmenden Zukunftstrend handelt, zeigt nicht zuletzt die Tatsache, dass Branchenbeobachter und Regulierungsbehörden diese Veränderungen sorgsam beobachten. Ihnen ist klar, dass sich hier vollkommen neue Konstellationen entwickeln, die die internationale Wirtschaft grundlegend verändern: herkömmliche Sichtweisen zur Wertschöpfung durch die Unternehmen haben ausgedient und es geht darum Standards, Prozesse und Rahmenbedingungen für international vernetzte Ecosysteme festzulegen.

Was bringt die Zukunft

Die Bedeutung digitaler Ecosysteme beziehungsweise Business Netzwerke wird zunehmen, denn die Wirtschaft wird zukünftig noch stärker von Netzwerkeffekten angetrieben, als das heute schon der Fall ist. Demnächst werden deshalb nicht mehr einzelne Unternehmen, sondern ganze Ecosysteme im Wettbewerb stehen. Schon heute zählen Konzerne wie Google zu den wichtigsten, größten und wegweisendsten Unternehmen weltweit. Ihr Geschäftsmodell basiert bereits seit Jahren auf der Vernetzung von Systemen, wobei immer der Kunde und seine Bedürfnisse im Vordergrund ihres Handels stehen.

Folglich sind einerseits die Lösungen genau das, was die Menschen haben wollen und zum anderen bekommt das Unternehmen auch das, was es will: Daten. Auf Basis der transparenten, unternehmensübergreifenden Prozesse entstehen so in der Interaktion zwischen Unternehmen, Lieferanten und Kunden ganz neue Geschäftsmodelle und Business Networks, die die Basis zukünftiger Wirtschaftssysteme bilden.

Lumir Boureanu

RPA RICHTIG EINSETZEN

(TEIL 2)

SOFTWARE-ROBOTER SIND DIE LÖSUNG! ODER ETWA DOCH NICHT?

RPA als Teil einer Gesamtstrategie muss nicht unbedingt etwas Schlechtes sein. So kann eine RPA-Lösung auch aus taktischen Gründen in ein bald zu ersetzendes System implementiert werden, um kurzfristig Effizienzsteigerung oder andere Vorteile zu realisieren.

Wie fast jede im Gartner Hype Cycle analysierte Technologie ist auch RPA kein Allheilmittel. Sie ist vielmehr ein Hilfsmittel, das unter den richtigen Umständen dabei helfen kann, die Vorteile und Einschränkungen von RPA besser zu verstehen. Im Folgenden haben wir einige Leitlinien zusammengefasst, die dabei helfen sollen, von RPA zu profitieren:

DER SELBSTVERSTÄNDLICHE UMGANG VON KUNDEN UND MITARBEITERN MIT DIGITALISIERUNG TRÄGT LANGFRISTIG ZU EINEM GESÜNDEREN UNTERNEHMEN BEI.

Mike Mason, Global Head of Technology, ThoughtWorks, www.thoughtworks.com

Die perfekte Formel für den richtigen Einsatz von RPA

1. Verwenden Sie nach Möglichkeit eine zugrunde liegende API. Wenn Sie eine bestimmte Anwendung mittels RPA automatisieren möchten, erkundigen Sie sich vorab beim Anwendungswartungsteam, ob eine Nicht-GUI-Schnittstelle erstellt werden könnte und wie hoch die Kosten dafür wären. In den meisten Anwendungen steuert die GUI-Schicht eine zugrunde liegende Geschäftslogikschicht, und es könnte weniger aufwendig sein, als Sie denken, diese Geschäftslogik direkt bereitzustellen. Sie können trotzdem eine RPA-Lösung einsetzen, um zwischen den Anwendungen hin und her zu wechseln. Durch Umgehen der Schnittstelle gewinnt Ihr System aber an Stabilität und Geschwindigkeit. Einige Unternehmen setzen RPA als Vorstufe zur Implementierung einer API ein – durch die Arbeit mit einer RPA-basierten Schnittstelle machen sie sich mit den Funktionen vertraut, die sie benötigen, wenn sie die RPA letztlich durch eine API ersetzen.

2. Fangen Sie klein an – versuchen Sie nicht sofort, die ganze Welt zu automatisieren. Viele Unternehmen versuchen, komplexe, langwierige Prozesse zu bewältigen, und stoßen schnell auf Probleme. Zerbrechen Sie sich darüber nicht den Kopf und folgen Sie ihrem eigenen Tempo, indem Sie zunächst klein anfangen – selbst ein einfacher Prozess, der effektiv von einem Roboter gesteuert wird, kann mit der Zeit zu enormen Vorteilen führen.

3. Ermitteln Sie anhand der „Regel der Fünf" Automatisierungsmöglichkeiten in Prozessen, die sich nicht sehr schnell entwickeln, die nicht besonders komplex sind und in die Menschen viel Arbeit investieren, die aber nur einen sehr geringen Mehrwert schaffen. Der Forrester-Autor Craig Le Clair prägte den Begriff „Regel der Fünf" – maximal fünf Anwendungen, zwischen denen man hin und her wechselt, maximal fünf Entscheidungen während des Prozesses und maximal fünfhundert benötigte Klicks.

4. Erweitern Sie Ihre RPA-Lösung und verwenden Sie dabei Einsatzanalysen („where used") oder RPA-Monitoring-Analysen. So können Sie genau erkennen, welche Bots auf welche IT-Anwendungsschnittstellen, APIs und Infrastrukturkomponenten zugreifen, sodass Sie immer nachvollziehen können, welche Bots nach dem Anpassen einer IT-Komponente geändert werden müssen.

5. Setzen Sie RPA als Lösungskonzept in Ihrem Toolkit zur Modernisierung Ihrer Altsysteme ein, und stellen Sie sicher, dass in Ihrer strategischen Roadmap alle von Ihnen geplanten Modernisierungsansätze berücksichtigt werden. Es ist oftmals wenig sinnvoll, RPA zur Automatisierung eines Prozesses zu verwenden, der in sechs Monaten ohnehin abgeschafft und durch einen völlig neuen Prozess oder ein System ersetzt wird.

6. Seien Sie bei Ihren Schätzungen hinsichtlich der Kosteneinsparungen durch einen neuen RPA-Ansatz vorsichtig, insbesondere wenn Sie bisher noch keine Anwendung beziehungsweise keinen Anwendungsbereich automatisiert haben. Wie wir bereits erwähnt haben, erfordern viele RPA-Implementierungen einen höheren Arbeitsaufwand und mehr laufende Unterstützung als ursprünglich angenommen.

7. Gehen Sie von einem höheren Testbedarf für Ihre Anwendungen aus. Durch Implementieren einer RPA-Lösung zum Betreiben von GUI-Anwendungen werden diese miteinander verknüpft. Das ist nicht notwendigerweise eine schlechte Sache – durch Verknüpfungen können die verschiedensten Aufgaben erledigt werden –, aber zu starke oder unerwünschte Verbindungen können problematisch sein. Wenn Sie für den Betrieb einer GUI-Anwendung RPA einsetzen, stellen Sie sicher, dass dem Team, das die Anwendung unterstützt, der neue „Roboterbenutzer" in der Software bekannt ist. Sorgen Sie außerdem dafür, dass Robotertests Teil des Softwarefreigabeprozesses sind.

8. Fahren Sie mit der Neugestaltung Ihrer Geschäftsprozesse fort und nutzen Sie RPA als Überbrückungsmaßnahme. Der selbstverständliche Umgang von Kunden und Mitarbeitern mit Digitalisierung trägt langfristig zu einem gesünderen Unternehmen bei. Unzureichende Geschäftsprozesse können Sie zwar oberflächlich mit einer RPA-Lösung verdecken, das zugrunde liegende Problem wird dadurch aber nicht beseitigt. Durch RPA lassen sich nicht nur bestimmte Anwendungen, sondern Ihre gesamten Geschäftsprozesse schwerer anpassen.

Mit diesen Leitlinien für den RPA-Einsatz verbessern Sie die Effizienz, insbesondere bei hochgradig manuellen Geschäftsprozessen, in denen Menschen nur einen geringen Mehrwert schaffen. Wenn die Arbeit von sehr vielen Menschen ausgeführt wird, kann sich bereits ein geringer Automatisierungsanteil auszahlen. Die RPA sollte jedoch nur ein Teil Ihrer Strategie sein, nur ein Werkzeug in Ihrem Instrumentarium, und in Verbindung mit einem langfristigen Ansatz und einer ganzheitlichen Technologiestrategie im Unternehmen eingesetzt werden.

Fazit

RPA kann ein Bestandteil vieler Initiativen zur digitalen Transformation sein, da sie Kosteneinsparungen verspricht, ohne dass sofort alle zugrunde liegenden Architekturen und Systeme modernisiert werden müssen. Es ist sinnvoll, die eingesparten Kosten dann für eine echte Modernisierung einzusetzen.

Da Modernisierungsmaßnahmen allerdings mehrere Jahre in Anspruch nehmen können, und ein Unternehmen es sich in der Regel nicht leisten kann, auf Effizienzsteigerungen zu warten, ist RPA eine geeignete Möglichkeit, kurzfristige Verbesserungen zu erzielen. Unternehmen müssen aber auch an die Konsequenzen denken: Durch RPA verbundene Systeme lassen sich nicht mehr so einfach modifizieren. Die Weiterentwicklung dieser Systeme bedeutet mehr Aufwand und birgt das Risiko, dass funktionierende RPA-basierte Integrationen unbrauchbar werden.

Wir meinen, dass Unternehmen sich im Rahmen einer ganzheitlichen Modernisierungsstrategie aktiv mit RPA auseinandersetzen müssen. Richtig durchdacht kann eine RPA kurzfristige Gewinne bringen, solange Unternehmen bei der Planung nicht die auf lange Sicht zu erwartenden Einschränkungen aus den Augen verlieren.

WIR MEINEN, DASS UNTERNEHMEN SICH IM RAHMEN EINER GANZHEITLICHEN MODERNISIERUNGSSTRATEGIE AKTIV MIT RPA AUSEINANDERSETZEN MÜSSEN.

George Earle, Global Director, ThoughtWorks, www.thoughtworks.com

Mike Mason, George Earle

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
28. FEBRUAR 2020

BLOCKCHAIN-EINSATZGEBIETE

Geeignete Anwendungen für Unternehmen

ROBOTIC PROCESS AUTOMATION

Wettbewerbsvorteile erzielen

KÜNSTLICHE INTELLIGENZ

Optimale Infrastruktur für Data Scientists

DIE AUSGABE 01/02 2020 VON IT MANAGEMENT ERSCHEINT AM 31. JANUAR 2020.

INSERENTENVERZEICHNIS

Dieser Ausgabe liegt eine Beilage der Wolters Kluwer Deutschland GmbH bei.

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Lumir Boureanu, Niculae Cantuniar, George Earle, Günter Esch, Andreas Fuchs, Benedikt Gasch, Thomas Gertler, Kai Grunwitz, Oliver Keizers, Michael Klatte, Stephan Leschke, Mike Mason, Peter Meivers, Carina Mitzschke, Heiko Mock, Annette Neth, Björn Orth, Silvia Parthier, Ulrich Parthier, Joe Payne, Terry Ray, Christine Schuhmacher, Alexander Stühl, Andreas E. Thyen, Donja Torabian, Eckhard Ulmer, Stefan Vollmer, Philipp Wodan

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH,
Rudolf-Diesel-Ring 21, D-82054 Sauerlach
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. 27.
Preisliste gültig ab 1. Oktober 2019.

Mediaberatung & Content Marketing-Lösungen it management | it security | it daily.net:
Kerstin Berthmann
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

Das E-3 Magazin

Information und Bildungsarbeit von und für die SAP-Community

Überfordert?

Wir bieten Information und Bildungsarbeit von und für die SAP-Community

e-3.de | e3zine.com

ZEIT FÜR ECHTE INTELLIGENZ!

Mit der neuen IM-C-Serie bringt Ricoh ab sofort echte Intelligenz in Ihr Büro. Denn dank der innovativen Always Current Technology™ sind die Systeme nicht nur immer auf dem neuesten Stand, sondern lassen sich außerdem im Handumdrehen mit neuen Funktionen und Features erweitern – ganz einfach über die Cloud. Das alles und noch viel mehr nennen wir Dynamic Workplace Intelligence. **www.ricoh.de/dwi**

RICOH
imagine. change.

itsecurity
DEZEMBER 2019

DAS SPEZIAL

VERSICHERUNGSSCHUTZ FÜR UNTERNEHMEN

RISIKO CYBERKRIMINALITÄT

Tobias von Mäßenhausen, AXA Konzern AG

FÜHRUNGSKRÄFTE & IT SICHERHEIT

Mangelnde Unterstützung

ZERO TRUST-PLATTFORM

Never Trust, always verify

IIOT-SCHWACH-STELLEN

Unterstützung für IT und OT

ab Seite 20

IAM CONNECT 2020

Die Brücke zu neuen Geschäftsmodellen

16. bis 18. März 2020
Berlin Marriott Hotel – Inge-Beisheim-Platz

www.iamconnect.de

Save the Date!

Eine Veranstaltung von itmanagement & itsecurity

4
COVERSTORY

INHALT

WIR BIETEN UNTERNEHMEN EIN VERSICHERUNGSKONZEPT AN, DAS DANK EINES MODULAREN BAUSTEINPRINZIPS GENAU DER ERFORDERLICHEN VERSICHERUNGSLEISTUNG ENTSPRICHT.

Tobias von Mäßenhausen,
Leiter Technische und Cyber-Versicherungen,
AXA Konzern AG, www.axa.de

RISIKO CYBERKRIMINALITÄT

VERSICHERUNGSSCHUTZ FÜR UNTERNEHMEN

Unternehmen sind zunehmend Bedrohungen und Risiken aus Cyberspace und durch IT ausgesetzt. Dabei kann Cyberkriminalität jedes Unternehmen teuer zu stehen kommen. Mit einer Cyber-Versicherung kann das finanzielle Risiko reduziert werden. Was aber, wenn trotzdem etwas passiert? Darüber sprach Ulrich Parthier, Herausgeber it-security, mit Tobias von Mäßenhausen, Leiter Technische und Cyber-Versicherungen bei AXA.

? **Ulrich Parthier:** Ein Unternehmen ist Opfer eines Cyberangriffs geworden und nicht mehr handlungsfähig. AXA kann hier Abhilfe schaffen?

Tobias von Mäßenhausen: Ja, genau hier tritt AXA auf den Plan. Im Falle eines Cyberangriffes ist sehr schnell das gesamte IT-System betroffen, wodurch der unternehmerische Schaden enorm sein kann.

Als Versicherung ist unser Kerngeschäft die Sicherheit. Das bedeutet nicht, dass wir nur eine „Zahlstelle" sind, wenn es zum Schaden gekommen ist, sondern dass wir unsere Kunden in diesen kritischen Momenten begleiten. Es geht darum, kurzfristig Maßnahmen zu ergreifen und einen Schaden zu verhindern oder zu begrenzen. Hierfür haben wir ein Netz aus Dienstleistern und Kooperationspartnern aufgebaut, mit denen wir schnelle Unterstützung und Beratung bei der Wiederherstellung des Betriebes leisten können.

? **Ulrich Parthier:** Jeder Cyberangriff ist unterschiedlich - woher kann ein Unternehmen im Vorfeld wissen, wogegen es sich absichern muss?

Tobias von Mäßenhausen: Hierbei gilt es, drei wichtige Aspekte zu betrachten:

1. Woraus können die größten Schäden resultieren? Sprich, welche Cybergefahren sind für mein Unternehmen am wahrscheinlichsten.

2. Wo werden die größten Auswirkungen erwartet? Die letzten Jahre zeigen, dass dies insbesondere im Bereich der Betriebsunterbrechung und der Datenwiederherstellung der Fall ist.

3. Wie teuer wird es, den Schaden und seine Auswirkungen zu beheben?

Hieraus ergibt sich, welche Maßnahmen für Unternehmen sinnvoll sind. AXA bietet Unternehmen ein individuelles Versicherungskonzept an, das dank eines modularen Bausteinprinzips so individu-

ell zusammengestellt werden kann, dass es genau der erforderlichen Versicherungsleistung entspricht.

Somit können Schäden durch Cyber-Angriffe zwar nicht vollständig verhindert werden, im Schadensfall erhalten versicherte Unternehmen jedoch schnelle und individuelle Unterstützung.

? **Ulrich Parthier:** Sind präventive Schutzmaßnahmen im Zweifel nicht sinnvoller, als die Absicherung eines eventuellen Schadenfalls?

Tobias von Mäßenhausen: Das eine schließt das andere nicht aus. Ich trage als Unternehmer immer die Verantwortung für die Sicherheit in meinem Unternehmen, aber gegen alle Cyber-Risiken kann man sich nun mal nicht schützen. Es gilt abzuwägen, welche Absicherung für ein Unternehmen sinnvoll ist und welche eher nicht.

Man sollte ganz konkret schauen, welche Kosten in Abhängigkeit vom Risiko entstehen können und dann entscheiden, ob und in welcher Höhe eine Investition in eine Cyber-Versicherung betriebswirtschaftlich Sinn ergibt.

? **Ulrich Parthier:** Und gibt es Möglichkeiten, durch entsprechende Schutzmaßnahmen Einfluss auf den letztendlichen Versicherungsbeitrag zu nehmen?

Tobias von Mäßenhausen: Wir honorieren, wenn Kunden proaktiv mit ihren Risiken umgehen und mitwirken. Kunden, die sich allein auf ihre Versicherung verlassen möchten, werden vorher geprüft und nicht ohne Weiteres versichert. Wir legen Wert auf ein hohes und homogenes Sicherheitsniveau unserer Versichertengemeinschaft, sodass ein Ausgleich des guten Vertrags für den schlechten Vertrag nicht in Frage kommt.

Wir setzen zudem bei allen unseren Kunden grundlegende Maßnahmen zur IT-Sicherheit voraus. Dazu gehören sowohl technische als auch organisatorische Maßnahmen, wie beispielsweise eine Firewall und Antivirensoftware, ein Patchmanagement-System zur Schließung von Sicherheitslücken sowie – besonders wichtig – regelmäßige Back-Ups der Daten.

? **Ulrich Parthier:** Worauf kommt es also beim Risikomanagement an?

Tobias von Mäßenhausen: Das Wichtigste ist erstmal das Bewusstsein innerhalb des Unternehmens – insbesondere der Geschäftsleitung – dass IT-Sicherheit ein wichtiges Thema ist. Denn ein effektiver Schutz gegen Hackerangriffe und vergleichbare Attacken kann in der Regel nur durch das Unternehmen selbst gewährleistet werden.

Risikomanagement ist am Anfang erstmal ganz losgelöst von der Versicherung, sondern fängt mit anderen Dingen an – beispielsweise:

1. Wie wir der Datenschutz sichergestellt?
2. Wie ist meine Internetseite dargestellt?
3. Wie erfolgen Back-Ups?
4. Und vor allem: Ist Budget für Cyber-Risikomanagement vorhanden?

Wir sehen allerdings, dass dieses Bewusstsein in kleineren Unternehmen deutlich abnimmt, wobei gerade hier die Attacken am erfolgreichsten sind.

? **Ulrich Parthier:** Wenn aber trotz aller Sicherheitsvorkehrungen der Schadenfall eintritt - das Unternehmen also nicht mehr arbeitsfähig ist. Wie kann AXA hier ganz konkret unterstützen?

Tobias von Mäßenhausen: Wir bieten eine 24/7 Hotline an, mit der unser Kunde mit einem IT-Dienstleister die Situation direkt analysieren und umgehend Maßnahmen einleiten kann.

Oft ist es leider so: Der Kunde wird gehackt und versucht direkt mit seinem Back-Up zu retten, was zu retten ist. Wenn er jetzt die Back-Up-Festplatte an das infizierte System anschließt, ist das Back-Up befallen und nicht mehr nutzbar. Deswegen ist es wichtig, im ersten Schritt schnelle professionelle Hilfe und einen Expertenrat einzuholen, um Bedienungsfehler und eine Ausweitung des Schadens zu verhindern und die richtigen Maßnahmen anzustoßen.

Im zweiten Schritt erfolgt dann die Sicherung und Wiederherstellung der Daten – dies wird dann häufig vor Ort vorgenommen.

Alternativ haben unsere Kunden auch die Möglichkeit, direkt mit ihrem eigenen IT-Dienstleister zu arbeiten und Sofortmaßnahmen ohne vorherige Absprache mit uns einzuleiten. Da der eigene Dienstleister die Kunden-IT bereits kennt, kann damit das Schadenausmaß häufig schnell und effektiv reduziert werden.

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

RISIKEN DER DIGITALISIERUNG

KÖNNEN CYBER-VERSICHERUNGEN ABHILFE SCHAFFEN?

Der digitale Wandel vollzieht sich immer rasanter und das Verlangen nach Effizienzsteigerung treibt konsequent Veränderungen voran. Auch Unternehmen bekommen diesen Wandel zu spüren: Um wettbewerbsfähig zu bleiben, werden Prozesse digitalisiert und automatisiert, Abteilungen vernetzt und Geschäftsinformationen in der Cloud gesichert. Neben massiven Vorteilen bringt diese Entwicklung auch große Gefahren mit sich.

Die Schattenseiten des digitalen Zeitalters

Cyber-Kriminalität ist auf dem Vormarsch. Cyber-Attacken richten sich dabei nicht unbedingt direkt gegen ein bestimmtes Unternehmen. Oft führen nicht zielgerichtete Angriffe auf eine Vielzahl von Unternehmen ebenfalls zum Ziel. So steigt die Zahl der sich im Umlauf befindlichen Schadprogramme seit Jahren kontinuierlich an und lag im Jahr 2018 bereits bei circa 800 Millionen – 200 Millionen mehr als ein Jahr zuvor. Tagtäglich registrieren IT-Sicherheitsunternehmen viele Hunderttausende Cyber-Attacken. Wo früher nur das Betriebssystem oder der Browser angreifbar waren, ergeben sich heute weitreichende Möglichkeiten. Informationen zu Überwachungskameras, Smart Homes oder IoT-Geräten können schnell und unkompliziert online erbeutet werden – der Hack ist meist nur noch einen Mausklick entfernt. Laut einer Umfrage des BSI waren bereits 70 Prozent der deutschen Unternehmen Opfer von Cyber-Angriffen – hierbei konnte sich jeder zweite Angreifer Zugriff auf IT-Systeme verschaffen, jeder vierte führte zu teilweise verheerenden und kostspieligen Produktions- und Betriebsausfällen sowie weiteren Kosten für die Wiederherstellung der IT, Imageschäden oder Drittansprüchen.

Auch der Netzwerkausrüster Cisco kommt in einer Studie mit Teilnehmern aus 26 Ländern zu dem Ergebnis, dass mehr als die Hälfte der mittelständischen Unternehmen im Jahr 2018 eine Datenpanne erlitten hatten, insbesondere durch Phishing, also betrügerische Angriffe auf Mitarbeiter, aber auch durch Malware und DDos-Attacken. Nicht selten bekommen Angreifer erst über die ungewollte Mitwirkung von Mitarbeitern Zugang zur geschützten Infrastruktur eines Unternehmens. Das BSI rät derzeit erneut vor der „weltweit gefährlichsten Schadsoftware Emotet", die Nutzer dazu bringt, infizierte E-Mail-Anhänge zu öffnen und hierdurch Malware zu installieren. Erst kürzlich sorgte eine neue Angriffswelle binnen weniger Tage für erhebliche Schäden in der deutschen Wirtschaft, bei Behörden und Organisationen. Für Unternehmen stellt sich daher nicht die Frage, ob sondern wann sie Opfer einer Cyber-Attacke sein wird.

Wie kann sich ein Unternehmen schützen?

Unternehmen werden sich des Risikos immer bewusster, der Markt um IT-Experten boomt. Gezielte Maßnahmen können das Risiko eines Cyber-Angriffs bereits wesentlich einschränken. Durch das Verwenden von professionellen Firewalls und Antivirenprogrammen erlangt das Unternehmen einen Grundschutz. Sicherheitslücken sollten durch regelmäßige Softwareaktualisierungen geschlossen werden. Tägliche Datensicherungen und regelmäßige Wiederherstellungstests können vor großen Datenverlusten schützen. Ein Berechtigungsmanagement verwehrt unbefugten Personen Zugang zu kritischen Geschäftsprozessen und kann die Reichweite des Angriffs einschränken. Auch der Faktor Mensch sollte nicht zu kurz kommen. Regelmäßige Schulungen zur IT Sicherheit sensibilisieren Mitarbeiter und können Fehlentscheidungen minimieren. Genaue Handlungsanweisungen und Notfallmaßnahmen sollten für Worst-Case-Szenarien bereits vorab in einem Notfallplan klar definiert sein, um Chaos im Krisenfall zu vermeiden.

Cyber-Versicherung als Ergänzung zur IT-Sicherheit

Leider bietet keine Maßnahme einen allumfassenden Schutz gegen Cyber-Kriminalität, ein Restrisiko verbleibt. Dies haben auch die Versicherer erkannt und in den letzten Jahren zunehmend neue Versicherungsprodukte auf den Markt gebracht. Zwar gibt es Unterschiede in Bedingungen und Deckungsumfang, im Kern haben sie jedoch dasselbe Ziel: Eine Cyber-Versicherung soll Unternehmen vor Vermögensschäden als Folge von Hacker-Angriffen oder sonstigen Akten der Cyber-Kriminalität schützen. Hierbei werden sowohl Eigen- als auch Drittschäden versichert, darunter fallen zum Beispiel Daten-, Betriebsunterbrechungs- und Haftpflichtschäden.

Die Deckungsinhalte sind umfangreich, unter anderem werden folgende Kosten ersetzt:

- Betriebsunterbrechungsschäden, insbesondere Ertragsausfälle und Mehrkosten. Einige Anbieter übernehmen

ebenfalls Rückwirkungsschäden durch Ausfall eines Clouddienstleisters

- IT-Forensikkosten zur Schadenermittlung und Schadensuche

- Kosten für die Wiederherstellung von Daten und Programmen in den früheren, betriebsfertigen Zustand. Hierunter fallen die Wiederbeschaffung und Wiedereingabe von Daten oder die Beseitigung von Schadsoftware

- Kosten eines Krisenmanagements, rechtliche Beratungen oder externe Kommunikation durch Pressearbeit zur Abwendung oder Minderung eines Reputationsschadens

- Aufwendungen, die durch gesetzlich geforderte Maßnahmen anfallen, insbesondere auch Kosten eines behördlichen Meldeverfahrens oder die Einrichtung eines Call-Centers für Betroffene bei Datenschutzvorfällen

- Kosten für die Abwehr von Haftpflichtansprüchen Dritter z.B. aus Datenschutzverletzungen, aufgrund eines Hacker-Angriffs oder aus unberechtigter Verbreitung von Daten und Programmen

- Kosten, die durch Schäden eines Identitätsdiebstahls oder Manipulation entstehen können

Eine schnelle Reaktionsfähigkeit kann im Krisenfall in vielerlei Hinsicht den Schaden drastisch minimieren. Daher bieten Cyber-Versicherer zusätzlich zum Deckungsumfang wichtige Serviceleistungen an. So besteht die Möglichkeit als Versicherungsnehmer rund um die Uhr über eine Notfallhotline an fachkompetente IT-Dienstleister zu gelangen, die im Krisenfall Soforthilfe leisten. Insbesondere kleine und mittelständische Unternehmen schätzen diesen Service sehr. Ein weiterer Service wird im Rahmen der Präventionsmaßnahmen angeboten. So können Mitarbeiter durch kostenfreie Awareness-Schulungen sensibilisiert werden und Unterstützung beim Ausbau der IT-Sicherheit kann, etwa durch Mithilfe bei der Erstellung eines Notfallplans, angefragt werden.

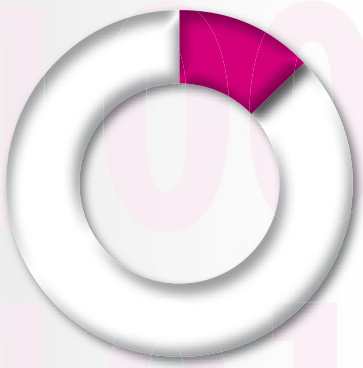
Der Nutzen einer Cyber-Versicherung ist für Unternehmen immens, insbesondere vor dem Hintergrund, dass die vielfältige finanzielle Absicherung und die angebotenen Serviceleistungen bereits für wenige Hundert Euro im Jahr erhältlich sind. Als Grundvoraussetzung für den Abschluss einer Versicherung verlangen die Versicherer einen gewissen Reifegrad der bereits umgesetzten technischen, organisatorischen und prozessualen Maßnahmen. Da die Geschäftsführung oft mit der Bewältigung von IT-Risiken überfordert ist, sollte der IT-Leiter im Rahmen des Risikomanagementprozesses mit der Geschäftsführung Risiken identifizieren und zu ergreifende Bewältigungsmaßnahmen auswählen. Es sollte geklärt werden, welche Informationen und Unternehmensdaten besonders schützenswert und auf welche Art und Weise diese bereits abgesichert sind. Im letzten Schritt kann dann entschieden werden, ob das verbleibende finanzielle Restrisiko eines Cyber-Vorfalls durch das Unternehmen selbst getragen werden soll oder durch den Abschluss einer Cyber-Versicherung auslagert wird.

Donja Torabian, www.axa.de

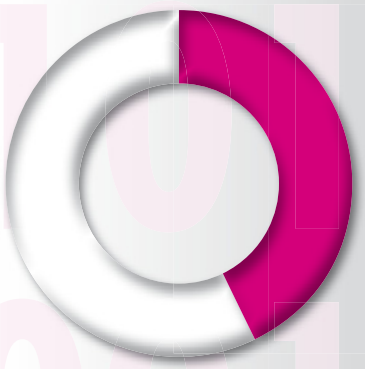
BYTE PROTECT 5.0 VON AXA

- **sichert Cyber-Risiken wirkungsvoll ab**
- **versichert Eigenschäden und Drittschäden**
- **ist durch das flexible Bausteinprinzip individuell an Unternehmensbedürfnisse anpassbar**
- **ist für jede Unternehmensbranche und -größe geeignet**
- **bietet sowohl die freie Wahl des IT-Dienstleisters im Krisenfall, als auch die Möglichkeit der Nutzung einer 24/7 Notfallhotline**

RISIKOMANAGEMENT IM UNTERNEHMEN



13 %
der Unternehmen erklären, dass derzeit ein Risikomanagement implementiert wird



43 %
der Unternehmen betreiben aktuell kein gezieltes Risikomanagement

(Quelle: AXA Konzern AG)

IIOT-SCHWACHSTELLEN MANAGEMENT

UNTERSTÜTZUNG FÜR IT UND OT BEI DER EINFÜHRUNG EINER GEMEINSAMEN SPRACHE

Es ist höchste Zeit, dass sich IT- und OT-Profis beim Schwachstellenmanagement in der Industrie 4.0 auf eine gemeinsame Sprache verständigen, um ihre Systeme zu schützen.

IT- und Produktions-Betriebstechnik (OT) Teams sind sich der Hemmnisse bewusst, die es im Bereich Cybersecurity zu überwinden gilt, um eine erfolgreiche Implementierung des Industrial Internet of Things (IIoT) zu erreichen. Trotzdem gehen in vielen Fällen die einzelnen Abteilungen an diese Bedrohungen mit sehr unterschiedlichen Prioritäten heran.

Für IT-Teams erfordert das Endpunktmanagement ein sehr Detailorientiertes Arbeiten. Denn in der IT besteht das Ziel darin, autorisierten Netzwerkbenutzer sicheren und zuverlässigen Dateizugriff zu ermöglichen. Auf der anderen Seite ist für die OT-Teams die oberste Priorität eine stabile Produktionslinie aufrechtzuerhalten. Aus diesem Grund ist bei den OT-Teams eher die Mentalität verbreitet: „Wenn es nicht kaputt ist, lass die Finger davon". Ein Beispiel für diesen Zwiespalt ist die Kohleindustrie, wo es einfach keine „schnellen Lösungen" für Sensoren, Maschinen und Steuerungssysteme gibt. Änderungen können hier das gesamte System zum Stillstand bringen, wodurch die gesamte Produktionslinie ins Stocken kommen kann.

In einem aktuellen Bericht der Beratungsgruppe McKinsey & Co. haben sich Unterschiede auf der „letzten Meile" in der IT/OT als große Hürde für Unternehmen erwiesen, die versuchen, IIoT-Programme aus der Pilotphase in eine unternehmensweite Implementierungen umzusetzen. Hier besteht die Herausforderung darin, den beiden Teams zu helfen, die Sprache des jeweils anderen zu verstehen und gleichzeitig das für ihre Arbeitsumgebung passende Verfahren für Schwachstellenmanagement anzuwenden.

Probleme (zu) patchen

Innerhalb des Bereichs Patch-Management sind die deutlichsten Unterschiede in der Sprache des IIoT für IT- und OT-Pro-

WHILE PILOTS ARE COMMON, COMPANY-WIDE WOLL OUT IS STILL RAE.
Percent of solutions by type at each stage of development

Quelle: McKinsey Industry 4.0 Global Expert Survey 2018

> ES IST HÖCHSTE ZEIT, DASS IT- UND OT-MITARBEITER SICH DURCH GEMEINSAM GESTALTETE VERFAHREN UND RICHTLINIEN DEM THEMA IIOT-SCHWACHSTELLENMANAGEMENT ANNEHMEN.
>
> Peter Meivers, Senior Product Manager
> baramundi software AG, www.baramundi.de

fis zu finden. Der Sinn eines Patches ist es, Sicherheitslücken zu schließen, Fehler zu beheben und Funktionen sowie die Funktionalität von Systemen zu erweitern. Insgesamt wird so die Sicherheit innerhalb eines Netzwerks erhöht. Prinzipiell ist das ein guter Ausgangspunkt, um die Kluft in den Vorgehensweisen von IT und OT zu überwinden.

IT-Profis betreiben das Patch-Management mit großem Nachdruck. Dies zeigt sich zum Beispiel am „Patch Tuesday", wenn regelmäßig jede Woche die Funktionalität und Sicherheit der Systeme erweitert und verbessert wird. Mit einer automatisierten Software, wie einem Unified Endpoint Management (UEM)-System, können Patches vorkonfiguriert und getestet werden, die dann über Nacht bereitgestellt werden, wobei die Systeme in dieser Zeit automatisch hochgefahren, konfiguriert, neu gestartet und heruntergefahren werden, bevor die Benutzer am nächsten Morgen ankommen. Endpunktnutzer werden dadurch kaum bis gar nicht gestört, während die regelmäßigen neuen Updates verhindern, das Angreifer bekannte Schwachstellen ausnutzen, um sich illegalen Zugriff auf die Geräte zu verschaffen. Dieses Vorgehen hat sich als äußerst effektiver Schutz erwiesen, um der kontinuierlichen Bedrohung von Cyberangriffen zu begegnen.

Im Vergleich dazu stehen OT-Profis mit Patch-Management vor einer großen Herausforderung. Angriffe auf industrielle Steuerungssysteme nehmen von Jahr zu Jahr zu, meist mit dem Ziel, die Produktion zu stören oder Industriespionage zu betreiben. Obwohl die Bedrohung klar ist und den OT-Mitarbeitern die Notwendigkeit regelmäßiger Patches bewusst ist, schränken die im Dauerbetrieb befindlichen, komplexen Multi-Vendor-Umgebungen ihre Reaktionsfähigkeit empfindlich ein. Tatsächlich verfügt eine durchschnittliche, mittelgroße Industrieanlage über mehr als 200 Geräte von Lieferanten mit unterschiedlichen Konfigurationen und Protokollen. Daher können die OT-Mitarbeiter die Steuerungssysteme nicht routinemäßig für Patches und Neustarts offline nehmen, da dies die Produktion unverhältnismäßig stark beeinträchtigen würde.

Eine aktuelle SANS-Studie hat ermittelt, dass für 56 Prozent des befragten OT-Personals die Einschränkungen beim Patchen als eine ihrer größten Herausforderungen für die Sicherheit der Produktion ansehen. Weiterhin gaben nur 40 Prozent der Befragten an, regelmäßig Patches zu installieren. Die anderen gingen lieber das Risiko ein, auf vollständigere Software-Updates zu warten, um Dienstunterbrechungen rechtfertigen zu können. Dies führt dazu, dass „Patch Tuesday" für OT-Mitarbeiter eher wie „Patch Q3" oder „Patch November" aussieht, da Einsätze weit im Voraus geplant, getestet und bereitgestellt werden müssen.

Überwindung der Spaltung

Wie viele Analysten, darunter IDC und Gartner, vorgeschlagen haben, müssen Unternehmen bei IT- und OT- innerhalb von IIoT einheitlichere, richtlinienbasierte Verfahren entwickeln, um eine belastbare Verteidigung gegen die Gefahren von Cyberangriffen aufzubauen. Ein Ansatz dies zu erreichen, besteht darin, die Sprachbarriere zu überwinden. Ein Beispiel dafür sind Geräte in der industriellen Produktion: Diese müssen als Endgeräte in ähnlicher Weise erkannt werden wie PCs und Smartphones. Tatsächlich sind bereits viele OT-Geräte mit PC-ähnlichen Rechnern ausgestattet und bieten Unternehmen damit eine große Chance, einheitliche Sicherheitsverfahren zu nutzen, um Schwachstellen frühzeitig zu erkennen.

Hier wird das Patch-Management Teil eines breiteren Vorgehens gegen Schwachstellen im System. So können beispielsweise OT- und IT-Experten innerhalb von IIoT mit Hilfe eines UEM-Systems potenzielle Schwachstellen schnell identifizieren, indem sie alle netzwerkfähigen Endpunkte registrieren, zuordnen und inventarisieren. Darauffolgend können dann geeignete Patches zur Bereitstellung entwickelt werden, die sich an den Anforderungen der jeweiligen Arbeitsumgebung und der Schwere des Risikos orientieren, um Störungen der Produktion zu minimieren.

Es ist höchste Zeit, dass IT- und OT-Mitarbeiter sich durch gemeinsam gestaltete Verfahren und Richtlinien dem Thema IIoT-Schwachstellenmanagement annehmen. Nur so können sie optimale Sicherheit gewährleisten und wichtige Updates in ihren Systemen ermöglichen.

Peter Meivers

DER MENSCH & DIE CYBER-SICHERHEIT

VON INDICATORS OF COMPROMISE (IOC) HIN ZU INDICATORS OF BEHAVIOR (IOB)

> DER MENSCH IST DIE KONSTANTE IN EINER SICH STÄNDIG WANDELNDEN BEDROHUNGSLANDSCHAFT. IM FOKUS SOLLTE ALSO DER VERTRAULICHE, SICHERE UMGANG MIT DATEN IM UNTERNEHMEN STEHEN.
>
> Nicolas Fischbach, CTO, Forcepoint, www.forcepoint.com

Das menschliche Verhalten als Schlüssel zu moderner Cyber-Sicherheit war eines der Top-Themen auf der it-sa 2019. Klassische Lösungen fokussieren sich nach wie vor stark auf die Erkennung von Schadcode. Wie aber kann ein Risikopotenzial identifiziert werden, das aus den eigenen Reihen hervorgeht und gänzlich ohne Schadcode agiert? Die gewichtigsten Schadereignisse in Bezug auf schützenswerte Daten und Informationen erfolgen nicht durch Malware, sondern durch Menschen.

„Die IT-Security muss sich weg von Indicators of Compromise (IOC) hin zu Indicators of Behavior (IOB) bewegen", betonte Nicolas Fischbach, CTO von Forcepoint. „Der Mensch ist die Konstante in einer sich ständig wandelnden Bedrohungslandschaft. Im Fokus sollte also der vertrauliche, sichere Umgang mit Daten im Unternehmen stehen: Wo befinden sich meine Daten? Um welche Art von Daten handelt es sich und wie interagieren Menschen und Maschinen mit diesen?"

Dynamic Data Protection

Forcepoint zeigt wie die Analyse menschlichen Verhaltens dabei helfen kann und die Cyber Security in den nächsten Jahren verändern wird. Der Schlüssel dazu sind risikoadaptive Lösungen für Prävention, Erkennung und Reaktion auf hochentwickelte Cyber-Bedrohungen – unter anderem Dynamic Data Protection (DDP).

Im Gegensatz zu herkömmlichen Data Loss Prevention (DLP)-Systemen lassen sich damit interne Sicherheitsrichtlinien adaptiv an alle Endpunkte oder -geräte anpassen, ohne dass ein Administrator eingreifen muss. Dadurch können Unternehmen die Sicherheit von Nutzern und Daten problemlos mit Anforderungen hinsichtlich Produktivität und Effizienz in Einklang bringen. Die DDP-Lösung prüft sämtliche Risiken kontinuierlich und passt das Sicherheitslevel automatisch sowie situativ an die jeweiligen Anforderungen an. Dadurch wird wirkungsvoll verhindert, dass sensible Daten aus dem Unternehmen abfließen können. Hierbei unterstützen moderne Analysemethoden, die den Umgang von Entities mit kritischen Daten und geistigem Eigentum fokussieren. Wichtige Kontextinformationen wie sich ändernde Risiken in Unternehmensnetzwerken werden so auf intelligente Weise in die Sicherheitsstrategie miteinbezogen.

Der DDP-Ansatz von Forcepoint verbindet quasi intelligente Algorithmen zur Bedrohungserkennung mit modernen Methoden der Verhaltensforschung. Somit lässt sich das individuelle und sich stets wandelnde Verhalten von Menschen und Maschinen umfassend verstehen und ein weitreichender, adaptiver Schutz vor verschiedensten Risiken für das Unternehmensnetzwerk realisieren.

DIGITAL TRANSFORMATION DESIGN

33 PRINZIPIEN, WIE SIE ORGANISATIONEN INS INTELLIGENTE ZEITALTER FÜHREN

Die Digitalisierung hat schon viele Branchen umgekrempelt, manche sogar vernichtet. Und sie wird nicht als Hype vorüberziehen. Vielmehr wird sie eher noch schneller und noch radikaler unser Leben verändern. Denn das, was wir bisher erlebt haben, war erst der Anfang.

Aber wie bereitet man sich auf die bevorstehenden Umbrüche vor? Wie setzt man die digitale Transformation im Unternehmen in Gang? Welche Werkzeuge sind für die digitale Transformation hilfreich? Wie steuert man diese Transformation? Und vor allem: Was bedeutet digitale Transformation wirklich?

Das neue Buch von Prof. Dr. Dennis Lotter gibt Antworten auf genau diese Fragen. Es liefert 33 fundamentale Prinzipien und Tools, mit denen sich die digitale Transformation gestalten lässt. Mit diesem Playbook lassen sich zukunftsrelevante Fähigkeiten identifizieren und die eigene Roadmap zur digitalen Transformation entwickeln. Denn erst wer die Mechanismen der digitalen Transformation verstanden hat, kann sie gestalten.

Digital Transformation Design

33 Prinzipien, wie Sie Organisationen ins intelligente Zeitalter führen

Dennis Lotter, BusinessVillage 2019

BEDROHUNGEN VON INNEN

CODE42s DATA EXPOSURE REPORT 2019

UNTERNEHMEN IGNORIEREN DIE GRÖSSTE BEDROHUNG FÜR DIE SICHERHEIT IHRER DATEN: IHRE EIGENEN MITARBEITER. WÄHREND DEN MEISTEN SICHERHEITSVERANTWORTLICHEN DAS PROBLEM WAHRSCHEINLICH BEKANNT IST, IST IHNEN MÖGLICHERWEISE DAS IMMENSE AUSMASS DES PHÄNOMENS NICHT BEWUSST.

Joe Payne, President und CEO, Code42, www.code42.com

Keine schöne Vorstellung, und doch eine Tatsache: Die eigenen Mitarbeiter bedrohen die Datensicherheit im Unternehmen. Nicht notwendigerweise immer aus böswilligen Motiven, sondern ebenso häufig aus Unkenntnis, Nachlässigkeit oder sogar in der besten Absicht. Code42 hat dieses Phänomen in seinem alljährlichen globalen Data Exposure Report 2019 untersucht. Die Studie ergab, dass Insider Threats – verursacht durch die bestehende Belegschaft wie auch durch scheidende Mitarbeiter – Unternehmen einem hohen Risiko für Datenpannen aussetzen und Firmendaten gefährden.

Gegenwärtig sind 79 Prozent der Entscheider im Bereich Informationssicherheit der Meinung, dass die eigenen Mitarbeiter eine effektive erste Verteidigungslinie gegen Datenpannen bilden. Diese Ansicht wird jedoch vom diesjährigen Data Exposure Report widerlegt. Firmen setzen vermehrt auf Strategien zur Zusammenarbeit und möchten den Informationsaustausch so einfach und reibungslos wie möglich gestalten. Das erfordert allerdings auch angemessene Kontrollen, um Probleme in puncto Datensicherheit zu erkennen und darauf reagieren zu können. Das unterbleibt jedoch oft, und die Organisationen verlassen sich darauf, dass ihre Mitarbeiter die Daten vertraulich behandeln. Dieses Vertrauen wird häufig missbraucht: Die Studie zeigte, dass Mitarbeiter mit den Daten weitaus nachlässiger umgehen, als die Arbeitgeber annehmen, und dass die Unternehmen somit einer ernstzunehmenden Bedrohung von innen ausgesetzt sind.

Sonderfall Mitarbeiterfluktuation

Obwohl die meisten Mitarbeiter sich im Guten von ihrem Unternehmen verabschieden möchten, besteht dennoch die Möglichkeit, dass sie bei ihrem Austritt mehr als nur Erinnerungen mitnehmen – nämlich geschützte Daten. Das führt zu Problemen am „anderen Ende", wenn neue Mitarbeiter die Daten ihrer ehemaligen Arbeitgeber mitbringen und unkontrolliert ins System des neuen Arbeitgebers einspielen. Dass das gar nicht mal so selten vorkommt, belegt der Report: Beinahe zwei Drittel (63 Prozent) der Befragten geben zu, Daten von ehemaligen Arbeitgebern mit an ihre neue Arbeitsstelle genommen zu haben. Denn die meisten Mitarbeiter (72 Prozent) sind der Meinung, persönliche Eigentumsansprüche an ihrer Arbeit zu haben.

Sicherheitsverantwortliche wissen in der Regel, dass ihre Daten Gefahren ausgesetzt sind. Zwar sind herkömmliche Präventionslösungen weit verbreitet, jedoch können sie Insider Threats für wertvolle Daten, wie beispielsweise Kundenlisten oder Quellcodes, nicht wirkungsvoll abwehren. Laut des Reports gaben mehr als zwei Drittel (69 Prozent) der Unternehmen an, eine Datenpanne aufgrund einer internen Bedrohung erlitten zu haben und bestätigen, dass zum Zeitpunkt des Vorfalls eine Präventionslösung implementiert war. Auch die Konsequenz aus diesem Befund ist den meisten durchaus klar: Mehr als drei Viertel (78 Prozent) der Entscheider im Bereich Informationssicherheit – darunter jene mit einer herkömmlichen DLP-Lösung – sind der Meinung, dass Schutzstrategien und -lösungen nicht ausreichen, um interne Bedrohungen abzuwenden.

Joe Payne

Kostenloser Download des Data Exposure Reports 2019: https://bit.ly/2NiBURa

INDUSTRIE 4.0

MEHR SICHERHEIT FÜR KONVERGIERENDE NETZWERKE

Cyber-Attacken bedrohen die Wirtschaft mehr denn je: Laut einer aktuellen Studie von Deloitte sehen sich inzwischen 85 Prozent aller mittleren und großen Unternehmen in Deutschland mit Angriffen konfrontiert. 28 Prozent davon berichten von täglichen Attacken, weitere 19 Prozent registrieren Vorfälle mindestens einmal pro Woche. Im Vergleich zum Vorjahr haben die Frequenz und Intensität der Angriffe weiter zugenommen.

Eine der größten Herausforderungen für die Industrie stellen konvergierende Netzwerke dar: Mit zunehmender Vernetzung von IT und Operational Technology (OT) steigt die Zahl der potenziellen Angriffspunkte für Hacker. Vor allem im Bereich Anlagenmanagement, Supply Chain, Fernwartung oder Patch-Management ist dies der Fall. Operational Technology ist Hardware und Software, die die Leistung physischer Geräte überwachen und kontrollieren. Um die Gefahr einzudämmen, wäre eine nahtlose Zusammenarbeit von IT und OT-Security-Abteilungen notwendig, was in der Praxis jedoch bislang nur schwer umsetzbar ist.

Sicherheit wird nur zur Hälfte bedacht

Die ersten Hürden entstehen bereits durch unzureichende Investitionen in einen umfassenden Schutz, da oftmals nicht genügend finanzielle und personelle Ressourcen verfügbar sind. Obgleich viele Unternehmen die Sicherheit ihrer IT-Netze bereits verstärkt haben, lässt die OT-Sicherheit nach wie vor zahlreiche Fragen offen – nicht zuletzt wegen mangelnder Best Practices und praktikabler Lösungen. Gängige Maßnahmen aus der IT-Security, wie Schwachstellenscans oder das Einspielen von Patches, sind in den meisten Fällen nicht auf OT-Umgebungen anwendbar.

OBGLEICH VIELE UNTERNEHMEN DIE SICHERHEIT IHRER IT-NETZE BEREITS VERSTÄRKT HABEN, LÄSST DIE OT-SICHERHEIT NACH WIE VOR ZAHLREICHE FRAGEN OFFEN.

Stefan Vollmer, Chief Technology Officer, TÜV SÜD Sec-IT, www.tuev-sued.de

Hinzu kommt, dass OT-Netzwerke vielfach aus veralteten Geräten und Technologien bestehen, die trotz Sicherheitsmängel weiter betrieben werden. Die Vernetzung mit der IT verschärft das Problem, indem beispielsweise Verbindungen zur Datenübertragung zwischen IT und OT nicht ausreichend gesichert sind. Sind IT-Systeme über solche unsicheren Netzwerke mit OT-Systemen verbunden, die wiederum mit überholten Betriebssystemen laufen, haben Angreifer leichtes Spiel: Komponenten, Systeme und Prozesse lassen sich unbemerkt ausspionieren und manipulieren.

Verbindliche Normen

Initiativen, um Lösungsansätze aus der IT für den OT-Security-Bereich weiterzuentwickeln und zu definieren, sind bereits angelaufen. Die IEC 62443, die als zentrale Normreihe für die Industrie 4.0 gilt und den Aufbau eines Managementsystems für IT- und OT-Security fordert, hat hier bereits einen wichtigen Grundstein gelegt. Auch die Charter of Trust, eine Allianz global tätiger Unternehmen für mehr Cybersicherheit, in der sich auch TÜV SÜD engagiert, arbeitet in diese Richtung: Sie fordert verbindliche Regeln und Standards für angemessenes Niveau an Cybersicherheit.

Neue Ansätze und praktikable Lösungen

Während die Grenzen zwischen IT und OT im Zuge der Digitalisierung immer mehr verschwimmen, findet bei Sicherheitsfragen nach wie vor eine getrennte Verarbeitung statt. Ein vereinheitlichtes IT-OT-Sicherheitsmanagement ist jedoch dringend notwendig, um die Herausforderungen des Internet of Things effizient anzugehen. Unternehmen benötigen neue Ansätze, um das Sicherheitsmanagement beider Bereiche zusammenzuführen. Bestehende Ansätze und Initiativen müssen in den nächsten Jahren verstärkt und ausgebaut werden – hier sind Staat und Wirtschaftsakteure gleichermaßen gefragt.

Stefan Vollmer

UTOPIE ODER BEREITS WIRKLICHKEIT?

CYBERKRIMINELLE NUTZEN KI

Immer mehr Unternehmen investieren in KI-basierte Sicherheitslösungen. Mit dem Volumen an verarbeiteten Daten wächst auch der Wert der KI: Sie befähigt Unternehmen, große Mengen an Informationen aufzunehmen und Muster darin zu erkennen – das tägliche ToDo der Cybersicherheit.

Wie aber steht es mit der Gegenseite? Den Hackern? Nutzen auch diese bereits KI, um die Verteidigung der IT-Systeme erneut ins Wanken zu bringen? Das Positive vorweg: Aktuell ist die Cybersicherheit noch im Vorteil – Unternehmen investieren weit mehr in KI als die Hacker. Das gibt der Branche Zeit, sich vor KI-fähigen Cyberkriminellen zu wappnen.

Erfolgsrezept KI für Cyberangriffe

KI befähigt Unternehmen, riesige Datenmengen zu clustern und Sicherheit zu automatisieren. Große Mengen scheinbar unzusammenhängender Daten können so in kürzester Zeit auf wenige verwertbare Vorfälle oder Ergebnisse reduziert werden. Unternehmen erkennen potenzielle Bedrohungen in Sekunden und können entsprechend reagieren.

> UNTERNEHMEN MÜSSEN JETZT IN EINE EFFEKTIVE VERTEIDIGUNG INVESTIEREN, UM DAS RISIKO EINES ANGRIFFS ZU MINIMIEREN.
>
> Terry Ray, Senior Vice President & Fellow, Imperva, www.imperva.com

Cybersicherheitsteams werden diese Fähigkeit in den kommenden Jahren brauchen, denn die KI könnte zu ihrem Feind werden. Im Gegensatz zu Malware, die rein automatisiert ist, beginnt die KI, Menschen mit beunruhigender Genauigkeit nachzuahmen. Somit kann sie theoretisch auch menschliche Hacking-Taktiken industrialisieren: das Durchforsten von Systemen, das Beobachten des Benutzerverhaltens und das Finden oder Installieren von Hintertüren. Diese Hacks sind von den Sicherheitsteams meist nicht zu erkennen.

Mit KI lässt sich also ein unabhängiger, intelligenter und zielgerichteter Angreifer aufbauen, der wartet und beobachtet – sozusagen ein automatisiertes Advanced Persistence Threat (APT). APTs wären für Unternehmen weitaus schwieriger zu verteidigen als automatisierte „Splash"-Taktiken. Zudem könnten seine Angriffe in sehr großem Umfang ausgeführt oder industrialisiert werden.

Auch Cyberkriminelle können KI nutzen

Noch sind automatisierte APTs Zukunftsmusik, denn KI ist kompliziert und benötigt Zeit zu Lernen. Ein KI-Algorithmus ist nicht benutzerfreundlich konzipiert; das Hacking-Tool muss fortlaufend angepasst werden. Das erfordert KI-Expertise, die in der Hackersphäre noch viel seltener als in der Cybersicherheitsbranche ist. Zuallererst werden sich daher staatliche Hacker KI zunutze machen, um Einrichtungen von nationalem Interesse anzugreifen. Dadurch könnte ein Land mehrere Terabyte Datenmaterial aus den Bereichen Gesundheit, Personal, Bundeshintergrundprüfung und Auftragnehmer erhalten. Ein KI-Programm wiederum könnte Daten wie Familienzugehörigkeiten, Gesundheitsprobleme, Benutzernamen sowie Bundesprojekte pro Kopf clustern und in Beziehung zueinander setzen, um attraktive Zielpersonen für einen zukünftigen Angriff herauszufiltern.

Die Zukunft: KI-Phishing

Phishing-Mails sind immer noch eine der häufigsten Formen von Cyberangriffen.

Aktuell lassen sie sich noch leicht erkennen, da sie häufig voller Tippfehler sind und individuelle Spear-Phishing-Botschaften nur mühsam manuell durchführbar sind. KI hingegen könnte diese Schwachpunkte eliminieren. Die Texte lassen sich von einer menschlichen nicht mehr unterscheiden. Mit KI ist Phishing viel schneller und automatisiert durchführbar. Die Integration von Phishing in automatisierte Systeme wird es erleichtern, monetarisierbare Ziele zu identifizieren und E-Mails um ein Vielfaches gezielter zu gestalten. Damit lässt sich die Erfolgsrate erhöhen, der menschliche Einsatz jedoch halbieren. Das macht KI auch für Hacker interessant.

Lösung: Sofortiger Aufbau einer effektiven Verteidigung

Unternehmen müssen also jetzt in eine effektive Verteidigung investieren, um das Risiko eines Angriffs zu minimieren. Sie benötigen dazu geschulte Cyberspezialisten und KI-basierte Analysetools. Damit können sie verdächtige Verhaltensmuster herausfiltern. Ein rollenbasiertes Identitäts- und Accessmanagement hilft zusätzlich, Attacken von außen zu verringern.

Zudem sollten Unternehmen herausfinden, wo sich kritische Ressourcen befinden und wie sich diese sichern lassen. Im digitalen Zeitalter sind das meist die Datenbanken, auf die es letztendlich auch die Hacker abgesehen haben. Unternehmen sollten also jederzeit abgleichen können, wer und wie auf die internen Daten zugegriffen hat, auf was jemand zugegriffen hat und ob dieser dazu berechtigt war. KI-basierte Analysetools sind eine der wichtigsten Cybersicherheitsinvestitionen für die kommenden Monate, damit der Sicherheitsvorsprung auf Seiten der Unternehmen bleibt.

Terry Ray

SECURITY FÜR LINUX

SICHER GEGEN MALWARE GEWAPPNET

Der Mythos, Linux zähle zu einem der unangreifbaren Betriebssysteme, hält sich genauso hartnäckig wie die Legende, dass Spinat besonders viel Eisen enthält. Die immer noch weit verbreitete These vom „Nerd-Image" führt außerdem zum Trugschluss, dass Linux ein ziemlich unattraktives Ziel für Cyberkriminelle sei. Gemessen am Marktanteil (rund 1,7 Prozent) für Desktop-PCs mag dies stimmen, doch bei Servern liegt er um ein Vielfaches höher und im Laufe der Zeit hat sich Linux wohl ein Monopol in puncto Supercomputer erobert.

Mehrere Tausend Malware-Samples im Umlauf

Jede Suchanfrage bei Google, jede Verbindung bei Fritzbox – alles läuft über Linux-Server. Sie bilden in Unternehmen in der Regel den ersten Zugangspunkt „nach dem Internet". Durch die Einsatzzwecke als Gateways, File-, Mail- und Webserver, die in den verschiedensten Rollen rund um die Uhr laufen, wächst die Angriffsfläche um ein Vielfaches.

Malware-Autoren müssen womöglich kreativer sein als bei Windows, aber über 8.000 Malware-Samples zeigen, dass die Utopie der „uneinnehmbaren Festung Linux" längst der Vergangenheit angehört. Erst kürzlich hat der CERT BUND vor den Schwachstellen in Apache http Server gewarnt, weil Datenmanipulation und Cross-Site Scripting oder Denial of Service Angriffe denkbar waren. Darüber hinaus wurden im Vergleich 2018 die meisten Sicherheitslücken bei Linux entdeckt – weitaus mehr als beim häufig kritisierten Windows 10, nur hat Linux sie schneller behoben.

ESET File Security für Linux

Letztlich reicht eine einzige Schwachstelle, um großen Schaden in Unternehmen anzurichten. Umso entscheidender ist es, eine Sicherheitslösung wie ESET File Security für Linux einzusetzen: Sie erkennt effektiv getarnte Mal- und Spyware und warnt vor verdächtigen Aktivitäten. Mit der komplett neu entwickelten Security-Software, jetzt in der Version 7.0, bietet ESET erweiterten Schutz für eingesetzte Linux-Server in Unternehmen. Die Lösung basiert auf der neuesten ESET LiveGrid-Technologie und beseitigt alle Arten von Bedrohungen, einschließlich Viren, Rootkits, Würmern und Spyware.

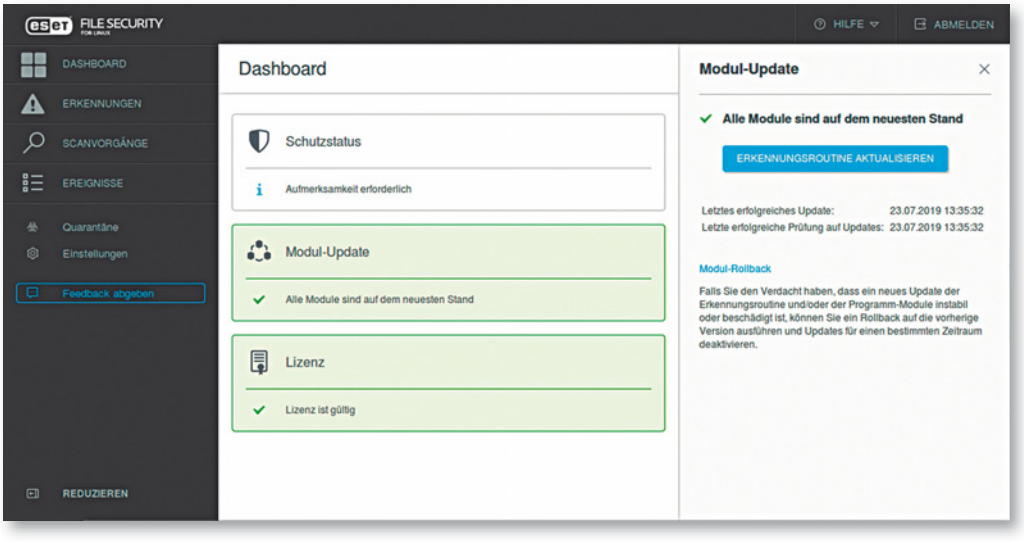
Die neueste Version bietet eine Vielzahl von erweiterten Funktionen, darunter Echtzeit-Dateisystemschutz und eine grafische Echtzeit-Web-Benutzeroberfläche (GUI). Administratoren profitieren neben der stärkeren Bekämpfung von Linux-, Windows- und Mac-Malware von der nativen 64-Bit Scanengine, Performanceverbesserungen und automatischem Software Deployment. Darüber hinaus kann EFSL dank der ICAP-Fähigkeit als Remote-Scanner fungieren. ICAP-kompatible Anwendungen, Appliances oder Dienste können eine verdächtige Datei automatisch einreichen, überprüfen und bewerten lassen. ESFL ist somit in der Lage, auch Netzwerkspeicher (NAS) zu checken.

Michael Klatte | www.eset.de

AUSGEWÄHLTE NEUERUNGEN IM ÜBERBLICK:

- Neue Architektur (Native 64-Bit Scanengine, mehr Performance, Stabilität, Sicherheit)
- Neuer Echtzeitdateischutz (Unterstützung der neuesten LiveGrid-Technologie)
- Neue Kommandozeilen-Tools
- Echtzeit Web-Oberfläche
- Remote Scanning (NAS-Scan über ICAP-Protokoll)

www.eset.com/de/business/file-security-linux



RAUS AUS DEN SILOS!

INTEGRIERTE ANSÄTZE SIND GEFRAGT

Immer mehr Unternehmen vertrauen bei der IT-Sicherheit externen Dienstleistern. 2019 werden laut Marktforschungsinstitut IDC in Deutschland mit Hardware, Software und Services für IT-Sicherheit 4,4 Milliarden Euro umgesetzt, ein erneutes Wachstum von neun Prozent im Vergleich zum Vorjahr. Als Konsequenz dieser Ausgaben nehmen die Kompetenz und die Sensibilisierung zur Prävention gegen Cyberattacken unternehmensseitig deutlich zu.

Die Präventionsaufgabe endet aber nicht bei der IT-Abteilung. Der Unternehmenskommunikation kommt eine vergleichbar bedeutende Rolle zu. Die Kernfrage, die sich ein Unternehmen bei Cyberattacken stellen muss, lautet: Erfüllen wir die Voraussetzungen, um im Krisenfall schnell, transparent und glaubwürdig zu kommunizieren? Hier besteht Handlungsbedarf: Die IT-Angriffe auf die Online-Bank N26 etwa haben gezeigt, dass die Reputation des Gesamtunternehmens im Feuer steht – und das mitten in einer neuen Finanzierungsrunde. Nichts passte da dem Start-up-Star schlechter in den Plan, als Medienberichte über massiv geschädigte Kunden und das unzulängliche Krisenmanagement der Bank.

Drei Stufen für mehr Sicherheit

Immer mehr Firmen digitalisieren ihre Geschäftsabläufe, beispielsweise Versicherungen mit Predicitve Analytics, oder verfolgen ein ausschließlich digitales Geschäftsmodell, wie Uber, Airbnb oder FinTechs. Somit sind Cyberattacken niemals nur ein Angriff auf die Sicherheit der IT-Infrastruktur von Unternehmen. Sie bedrohen immer auch sein Geschäftsmodell, seine Reputation und im schlimmsten Fall die Existenz. Die heutigen Cyber-Bedrohungen erfordern daher einen Schulterschluss von IT-Security-Verantwortlichen, dem Risikomanagement und der Kommunikationsabteilung.

„Aus unserer Erfahrung lässt sich die Zusammenarbeit der verschiedenen Abteilungen in drei Stufen abbilden: die Risikoanalyse, die Krisenprävention und das Handeln im akuten Krisenfall", erklärt Alexander Fink von der Full-Service-Kommunikationsberatung Akima Media, zu deren Kunden namhafte IT-Security-Anbieter gehören.

1. In der Risikoanalyse wird die Selbsteinschätzung zur Krisenbereitschaft des Unternehmens abgefragt und die Ergebnisse mit externen Experten abgestimmt. Zu ihr gehören außerdem ein Audit der Information-Management-Systeme, eine Prüfung vorhandener Krisendokumente, Interviews mit den Mitarbeitern des Krisenteams sowie ein Test der Infrastruktur und der Prozesse. Die Ergebnisse werden in einem Risikoreport zusammengefasst.

2. Die Krisenprävention umfasst dann vor allem die Entwicklung und Zertifizierung der Informationssysteme, die Beratung zur Informationssicherheit sowie Penetration Tests und Kommunikationstrainings. Bestenfalls wird auch der Ernstfall unter realen Bedingungen geprobt, um Schwachstellen aufzudecken.

3. Integrierte Maßnahmen im Krisenfall sind schließlich der Aufbau einer 24/7-Notfall-Hotline mit garantierten Antwortzeiten, das komplette Krisenmanagement über einen zentralen Krisenstab, forensische Analysen und natürlich die laufende Krisenkommunikation mit Medien, Influencern und der Öffentlichkeit.

NUR DER INTEGRIERTE ANSATZ ERHÖHT DEN SCHUTZ DES UNTERNEHMENS UND DIE SCHLAGKRAFT IM ERNSTFALL.

Alexander Fink, Akima Media, www.akima.net

Akima-Krisenexperte Alexander Fink ist sich sicher: „Nur der integrierte Ansatz, bei dem die IT-Sicherheit, das Risikomanagement und die Kommunikation bei Cyberattacken eng zusammenwirken, erhöht den Schutz des Unternehmens und die Schlagkraft im Ernstfall."

HÖHLEN FÜHRUNGSKRÄFTE

VIELE MANAGER IGNORIEREN SICHERHEITSREGELN UND ENTHALTEN

Zwei Fragen: Wer hat die meisten Informationen in einem Unternehmen, die weitesten Rechte zum Datenzugriff und wird deshalb bevorzugt gehackt? Klar, das Topmanagement. Wer sollte sich daher konsequent schützen und schützen lassen? Eben. Doch Sicherheit kann unbequem sein. Neue Untersuchungen zeigen einen gefährlichen Trend: Viele leitende Angestellte weichen Cybersicherheits-Richtlinien auf oder ignorieren sie einfach.

44 Prozent der in einer Studie befragten IT-Security-Experten aus Deutschland sagen, dass leitende Angestellte in ihrem Unternehmen Cybersicherheits-Richtlinien aufweichen oder ignorieren. Zugleich sagen 12 Prozent der Befragten, dass diese Gruppe am stärksten dem Risiko eines Hacks ausgesetzt ist. Dies ist eines der brisantesten Ergebnisse der im Oktober 2019 von Bitdefender veröffentlichten Studie „Hacked Off".

Für die Studie wurden im Rahmen einer internationalen Umfrage unter mehr als 6.000 IT-Security-Experten in acht Ländern auch 515 in Deutschland tätige Security-Spezialisten befragt. Ziel war es, herauszufinden, was ihnen Druck macht, wie sich dieser auf die Wirksamkeit von Sicherheitsmaßnahmen auswirkt, und was die Befragten als die besten Strategien zur Gewährleistung der Sicherheit von Unternehmen ansehen.

Über die Hälfte der Unternehmen seit 2017 gehackt

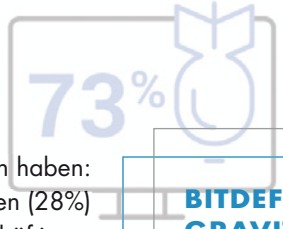
Die Antworten der IT-Security-Experten aus Deutschland zeigen, dass 51 Prozent der Befragten sich Sorgen machen um die Fähigkeit ihrer Organisation im Umgang mit einem global angelegten Cyberangriff in der Größenordnung von WannaCry. Und das nicht ohne Anlass: Über die Hälfte der deutschen Unternehmen (54%) sind in den Jahren 2017 bis 2019 erfolgreich gehackt worden – fast ein Viertel der Unternehmen (24%) wurden alleine in den ersten sieben Monaten des laufenden Jahres Opfer eines solchen Angriffs. Darüber hinaus halten es über ein Viertel der IT-Security-Profis (26%), deren Arbeitgeber nicht bekanntermaßen Opfer eines Cyberangriffs geworden sind, für wahrscheinlich, dass doch insgeheim derzeit ein solcher Angriff läuft, ohne dass die Firma davon Kenntnis hat. Dies könnte darauf hindeuten, dass 2019 ein Rekordjahr für Datenverstöße wird. Im Jahr 2018 lag der Anteil der Unternehmen, die Datenverstöße festgestellt haben, noch bei 35 Prozent.

Die Ergebnisse zeigen die Notwendigkeit auf, die Reaktionsgeschwindigkeit zu erhöhen: Fast jeder dritte deutsche IT-Sicherheits-Profi (32%) gibt an, dass es eine Woche oder länger dauern würde, einen ausgefeilten Cyberangriff zu erkennen. Es gibt auch einen Haken bei der Identifizierung von Datenvorfällen: Nur vier von hundert Befragten vermuten, dass sie mit ihren derzeitigen Security-Werkzeugen jedwede Advanced Attack effizient erkennen und isolieren können. Drei von zehn Befragten (30%) glauben hingegen, dass sie weniger als die Hälfte solch fortschrittlicher Attacken identifizieren und eindämmen könnten. Wenn es darum geht, in effektivere Methoden zur Erkennung von Cyber-Bedrohungen zu investieren, stehen Netzwerkverkehrsanalyse (Network Traffic Security Analysis) mit 43 Prozent und Antimalware mit 42 Prozent an erster Stelle. Die Frage, ob EDR (Endpoint Detection&Response) hilft, zukünftige Angriffe zu verhindern, bejahen über zwei Drittel (68%).

Laut der Bitdefender-Studie „Hacked Off" beklagen international 57 Prozent der Security-Experten, dass das Top-Management Regeln missachtet – in Deutschland sind es 44 Prozent.

DIE IT-SICHERHEIT AUS?

IHREN SPEZIALISTEN WICHTIGE WERKZEUGE VOR



Die Notwendigkeit einer schnellen Erkennung und Reaktion auf Bedrohungen wird auch durch die handfesten Folgen deutlich, denen Unternehmen ausgesetzt sind, wenn ihre Cybersicherheit nicht auf dem neuesten Stand ist: Die Konsequenzen, wenn man einen anhaltenden Sicherheitsverstoß nicht bemerkt, wären laut den deutschen Befragten eine Betriebsunterbrechung (48%), ein Reputationsverlust (37%) und ein Umsatzverlust (39%). Das Schlimmste aus Sicht der IT-Sicherheits-Profis ist jedoch der drohende Verlust des Kundenvertrauens. Mehr als vier von zehn (43%) sagen, dass dies ihre größte Sorge ist.

Darüber hinaus leiden die deutschen Befragten an „Breach Fatigue", also Ermüdungserscheinungen, weil sie zu vielen potenziellen Datenverstößen nachzugehen haben. Im Durchschnitt seien die Hälfte (50%) der Warnungen von EDR-Systemen Fehlalarme. 38 Prozent der Fachleute sagen, dass ihr Team sowohl unter zu vielen Warnungen als auch unter der Arbeit mit zu vielen unterschiedlichen Software-Agenten für die IT-Sicherheit leidet („Alert Fatigue" und „Agent Fatigue"). 69 Prozent von ihnen glauben, dass ihre Organisation wegen mangelnder finanzieller und personeller Ressourcen stärker durch Cyberangriffe bedroht ist.

Nur vier Prozent haben die nötigen Werkzeuge

Vor dem Hintergrund einer immer komplexeren Bedrohungslandschaft sind sich die deutschen Fachleute der Risiken ihrer Organisationen sehr bewusst. Ein Drittel (34%) gibt an, dass ihnen die Sorge um die Cybersicherheit nachts den Schlaf raubt. Erschwerend kommt hinzu, dass es nicht nur die Bedrohung von außen ist, mit der die Experten zu kämpfen haben: Mehr als ein Viertel der Befragten (28%) gibt an, dass es bei den Beschäftigten am Verständnis für Cybersicherheit mangelt.

Es gibt insbesondere ein Problem an der Spitze von Organisationen. Zahlreiche Führungskräfte, leitende Angestellte und Topmanager gehen nicht etwa mit bestem Beispiel voran. Sie höhlen im Gegenteil die IT-Sicherheit ihrer Unternehmen von innen her aus und enthalten IT-Sicherheitsverantwortlichen die Werkzeuge vor, die aus fachlicher Sicht notwendig sind, um für umfassenden Schutz zu sorgen: Gerade einmal vier von hundert deutschen Befragten der „Hacked Off" Studie vermuten, dass sie mit ihren derzeitigen Security-Werkzeugen alle Advanced Attacks effizient erkennen und isolieren können.

Liviu Arsene, Global Cybersecurity Researcher bei Bitdefender, resümiert: „Mangelhafte Cybersicherheit ist heute unbestreitbar eine Bedrohung für Unternehmen mit gravierenden Auswirkungen - die laut der Befragung vom Verlust des Kundenvertrauens bis hin zu Umsatzverlusten reichen. IT-Sicherheits-Profis haben das im Blick und wollen die Lage in den Griff bekommen. Sie wissen, dass die Haupttreiber für die Stärkung der Cybersicherheit ihrer Unternehmen die Verbesserung der Datensicherheit und eine schnellere Erkennung und Reaktionsfähigkeit sind."

www.bitdefender.de

BITDEFENDER GRAVITYZONE ULTRA

Bitdefender GravityZone Ultra bietet eine vollständig integriert Plattform, die drei Dinge verbindet:

- Umfassende Endpoint Protection Platform (für PCs, mobile Endgeräte, Server, virtuelle Maschinen und hybride Umgebungen)
- Mehrschichtige Next Generation Sicherheitslösung (mit Machine Learning, Sandboxing, Memory Protection und Process Monitoring)
- Einfach nutzbares EDR (Alarming, Forensik, Visualisierung und Response Workflows)

Die Lösung bietet Prevention, Detection und Response aus einem Guss. Mit einer einzigen Konsole erhalten Administratoren den Überblick über alle physischen und virtuellen Endgeräte, alle Informationen zu verdächtigen Aktivitäten und die Möglichkeit, Probleme mit einem Klick zu lösen.

www.bitdefender.de/ultra

Der Bericht der Studie „Hacked Off" ist kostenlos erhältlich unter www.bitdefender.com/hackedoff

DIGITALE TRANSFORMATION

UMDENKEN ZWINGEND ERFORDERLICH

Entscheidend für den Erfolg der digitalen Transformation sind die Mitarbeiter. Ihre umfassende Einbindung in die Transformationsprozesse erfordert in den meisten Unternehmen eine Anpassung von Kultur und Führungsstil.

Die digitale Transformation ist allgegenwärtig. Sie treibt den Wandel der Städte zu Smart Cities voran, ermöglicht Verbesserungen in der klinischen Versorgung und wird von manchem Politiker sogar als der Heilige Gral für den sozialen und wirtschaftlichen Fortschritt gepriesen. Allerdings bringt sie auch Risiken mit sich, etwa für Unternehmensmitarbeiter, deren Kenntnisse und Fähigkeiten vermeintlich nicht mehr benötigt werden. Sie fürchten daher verständlicherweise die Folgen der Digitalisierung. Für Führungskräfte ergeben sich dadurch konkrete Herausforderungen. Sie müssen die berechtigten Bedenken der Mitarbeiter aufgreifen und dahingehend die Unternehmensstruktur und auch ihren Führungsstil anpassen.

Der Mitarbeiter-Fokus

Die Mitarbeiter sind die wichtigste Komponente für eine erfolgreiche digitale Transformation. Die Führungsebene muss sich daher fragen: Was muss geändert werden, um alle Mitarbeiter für die digitale Reise abzuholen? Klar ist, dass die Digitalisierung neue Wege der Zusammenarbeit und einen gänzlich veränderten Geschäftsbetrieb erfordert. Das bedeutet, dass die Überprüfung und Infragestellung traditioneller Strukturen und Kulturen unvermeidlich ist. Vor allem muss berücksichtigt werden, dass sich die Bedürfnisse heutiger Mitarbeiter stark verändert haben: Zum einen streben sie nach mehr Selbstständigkeit und -organisation und zum anderen nach einer verstärkten agilen Zusammenarbeit im Team. Moderne Unternehmen wie Google, Amazon oder Tesla sind heute Vorbilder für eine solch kollaborative Kultur. Sie nehmen damit eine Vorbildfunktion ein, wie es vor einigen Jahrzehnten vielleicht bei HP der Fall war.

Die große Aufgabe für das Management ist somit die Etablierung einer Unternehmenskultur und eines Führungsstils, die Autonomie und aktives Engagement fördern. Es ist allerdings keineswegs ausreichend, in innovative Technologien für die Forcierung der digitalen Transformation zu investieren. Vielmehr ist die „People first"-Maxime wichtiger als jemals zuvor, um eine von Motivation und Kreativität geprägte Arbeitsumgebung zu schaffen.

DIE DREI ZENTRALEN ECKPUNKTE EINES ERFOLGREICHEN WANDELS VON UNTERNEHMENSKULTUR UND FÜHRUNGSSTIL LAUTEN: VERTRAUEN, HANDLUNGSFÄHIGKEIT UND VERANTWORTLICHKEIT.

Kai Grunwitz, Geschäftsführer, NTT Ltd. Deutschland, hello.global.ntt

Die digitale Führung

Die drei zentralen Eckpunkte eines erfolgreichen Wandels von Unternehmenskultur und Führungsstil lauten: Vertrauen, Handlungsfähigkeit und Verantwortlichkeit. Wenn ein Unternehmen alle drei Komponenten berücksichtigt, hat es eine große Chance, eine Kultur der Autonomie, Kreativität und Selbstmotivation zu schaffen. In vielen Unternehmen dominiert allerdings nach wie vor eine traditionelle hierarchische Struktur, in der ein Mikromanagement gang und gäbe ist und Mitarbeiter kontrolliert werden, anstatt dass man ihnen vertraut.

Wenn ein Manager etwa eine Aufgabe delegiert und dann mit dem Mikromanagement beginnt, wird Frustration beim Mitarbeiter unweigerlich die Folge sein. Er wird sich Fragen stellen wie: Vertraut mir mein Vorgesetzter nicht? Warum hat er mir diese Aufgabe gegeben, wenn ich nicht in der Lage bin, meinen Job richtig zu machen? Dies kann zum Verlust wichtiger Mitarbeiter führen, die essenziell für die digitale Transformation sind.

Das Manager-Profil

Führungskräfte müssen unter Umständen auch akzeptieren, brillante Mitarbeiter um sich herum zu haben, die oft sogar eine größere Kompetenz besitzen. Führungskräfte sollten folglich eher als Trai-

(Quelle: NTT Ltd.)

ner statt als Spieler agieren und ihre Aufgabe darin sehen, das richtige Team zusammenzustellen. Ebenso wichtig ist allerdings, dass sie ihren Teams eine klare Vision und Strategie an die Hand geben – und sie realistisch an die Zukunft heranführen: die Jobanforderungen und -beschreibungen werden sich kontinuierlich ändern. Darin besteht eine große Chance für Mitarbeiter und Führungskräfte, ständig zu lernen und sich weiterzuentwickeln. Digital Natives, Innovatoren und Change Agents wollen mit Menschen zusammenarbeiten, die sich für die Zukunft begeistern. Das bedeutet auch, dass Manager das vorleben müssen, was sie vorgeben – sie müssen auf jeden Fall authentisch bleiben und ihre eigene Flexibilität zeigen. Die digitale Führungskraft ist Teil der Transformation und die Speerspitze der Teams. Kurz gesagt: Ihr Stellenprofil hat sich geändert. Der Wert einer Führungskraft wird nicht mehr an der Anzahl der Personen in der direkten Berichtslinie bemessen, sondern an der Fähigkeit, das Überleben des Unternehmens im digitalen Zeitalter zu sichern.

Die digitalen Skills

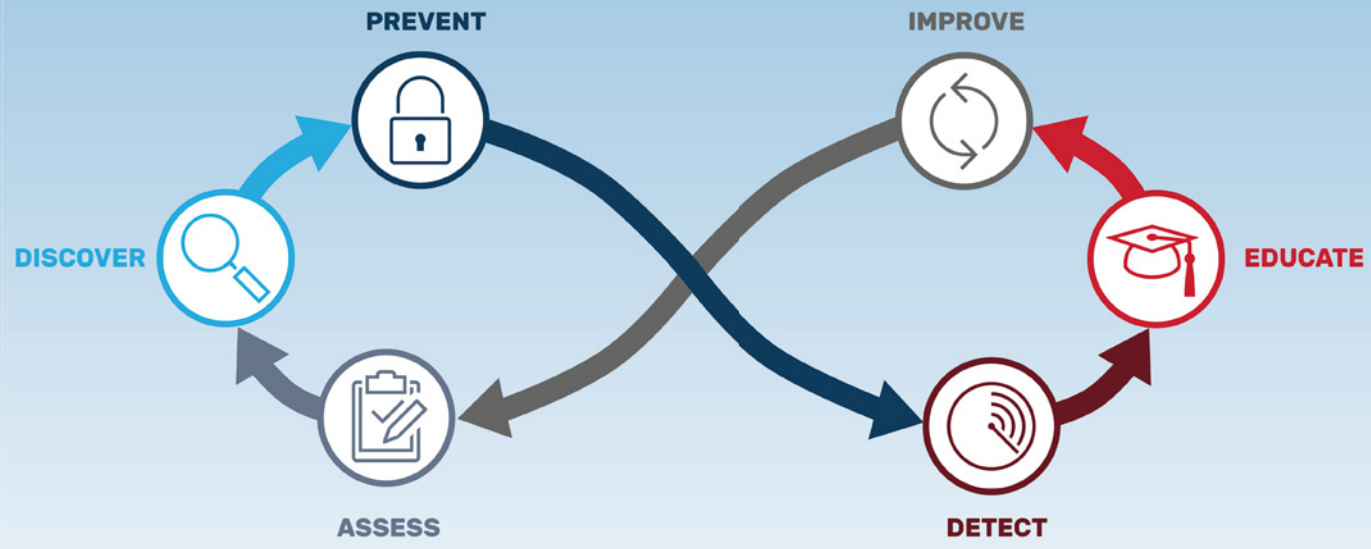
Das wichtigste Kapital auf dem Weg der digitalen Transformation ist die Kompetenz der Mitarbeiter. Der richtige Führungsansatz und die adäquate Unternehmensstruktur werden sicherlich dazu beitragen, die Mitarbeiter zu motivieren und Widerstände gegen den digitalen Wandel zu beseitigen. Allerdings erfordert die Weiterentwicklung digitaler Skills auf Mitarbeiterseite auch einen proaktiveren Ansatz von Führungskräften und Bildungseinrichtungen als in der Vergangenheit.

Zum einem sind Fortbildungen und Umschulungen ein wichtiger Weg, um das Potenzial der Mitarbeiter auszuschöpfen. Sie können nicht nur ein sehr kosteneffizienter Ansatz sein, um Talente in wachsenden Geschäftsbereichen des Unternehmens einzusetzen, sondern sie fördern auch die Loyalität der Mitarbeiter. Zum anderen müssen aber auch Schulen und Universitäten ihre Bildungsprogramme für Digital Natives anpassen, damit die nächste Generation, die in den Arbeitsmarkt eintritt, entsprechend qualifiziert ist.

Gleichzeitig gilt es, die menschlichen Fähigkeiten wieder in den Vordergrund zu stellen, die, gemäß der aktuellen Arbeitsmarktstudie der Royal Bank of Canada „Humans Wanted", gerade im Zeitalter der Technologisierung immer wichtiger werden. Als Voraussetzung für die Jobs von morgen werden aktives Zuhören, Reden und kritisches Denken in dieser Studie jeweils mit rund 50 Prozent deutlich höher bewertet als das reine Monitoring, das nur für 28 Prozent der Befragten vorrangig ist.

Herausragende Technologien mögen die Schlagzeilen beherrschen, aber wenn es um eine erfolgreiche digitale Transformation geht, läuft alles auf Investitionen in Menschen hinaus. Je schneller Führungskräfte dies erkennen, desto eher können sie einen nachhaltigen Erfolg erzielen.

Kai Grunwitz



NEVER TRUST, ALWAYS VERIFY

IN SECHS SCHRITTEN ZUR ZERO TRUST PLATTFORM

Grafik:
Zero Trust Lifecycle

Die zunehmende Digitalisierung und immer raffiniertere Cyberbedrohungen haben eine höchst komplexe IT-Sicherheitslage für Unternehmen und Organisationen zur Folge. Nur ein modernes Sicherheitskonzept nach der Maxime „Zero Trust – nie vertrauen, immer überprüfen", liefert maximalen Schutz vor Zero Day Exploits, gezielten Cyberangriffen oder Social Engineering. Mit diesen sechs Schritten kann Zero Trust – und damit ein umfassender Schutz unternehmenskritischer Daten – in der eigenen Organisation umgesetzt werden:

1. Assessment

Im ersten Schritt ist es wichtig, den organisatorischen Rahmen festzulegen. Dafür muss eine Reihe von Fragen möglichst präzise beantwortet werden:

- Was soll weshalb geschützt werden?
- Wo befinden sich diese digitalen und physikalischen Assets?
- Welche Daten sind als öffentlich klassifiziert und welche sind hochsensibel?
- Wie sehen die Touchpoints mit Mitarbeitern, Partnern, Zulieferern oder Endkunden aus?
- Wie, von wo und über welches Medium erfolgt der Zugriff? Neben Desktops und Laptops erweitern unter anderem mobile Endgeräte, Virtual Environments und Virtual Desktop Infrastructures die Netzwerkgrenzen.

Firmenrichtlinien für Sicherheit und Geräte spielen eine bedeutende Rolle. Erlaubt das Unternehmen „BYOD", sind die Sicherheitsrisiken potentiell höher. Dürfen nur firmeneigene Geräte verwendet werden, sind die Mitarbeiter stärker eingeschränkt. Auch für Wechseldatenträger können ähnliche Restriktionen gelten, zum Beispiel indem Schreibrechte verweigert werden oder die Nutzung sogar gänzlich verwehrt wird. Bestimmte Anwender, wie Wartungsmitarbeiter für Produktionsanlagen, können auch erweiterte Rechte erhalten, etwa um eigene USB-Sticks für einen Datentransfer anzuschließen.

Grundsätzlich sollte der Sicherheitsverantwortliche wissen, wie die Prozesse im Unternehmen aussehen und welche Geräte, Applikationen, Dienste und Workloads verwendet werden. Für eine erfolgreiche Einführung von Zero Trust ist es entscheidend, alle betroffenen Personen im Unternehmen einzubeziehen.

2. Discovery & Inventory

Als nächstes werden alle Daten in einer Bestandsaufnahme visualisiert, um weitere sicherheitsrelevante Aspekte und potentielle Schwachstellen zu ermitteln. Die Inventur umfasst die gesamte angeschlossene Hardware sowie Software und Betriebssysteme. Wurden alle Updates und Patches aufgespielt? Gibt es noch Support vom Hersteller oder ist das System bereits veraltet? Diese Fragen sind äußerst kritisch für die IT-Sicherheit. So hat sich Microsoft nach den verheerenden Folgen des Trojaners WannaCry entschieden, für das veraltete Windows XP noch einen Patch zu liefern.

Lösungen für automatisiertes Schwachstellen- und Patch-Management erleichtern Security-Teams die Arbeit erheblich.

Ein Überblick über das Security Posture, also den Zustand und die aktuellen Einstellungen aller Endpunkte, leitet den nächsten Schritt ein.

3. Präventionsmaßnahmen

Die möglichen Maßnahmen, um Cybergefahren von vornherein zu eliminieren und Datenintegrität zu gewährleisten, sind zahlreich. Das Bundesamt für Sicherheit in der Informationstechnik oder das Center of Information Security bieten umfassende Leitfäden. Zu den wichtigsten Werkzeugen gehören:

- Festplatten- und File & Folder-Verschlüsselung: Festplatten und Dateien sollten immer verschlüsselt werden, egal ob sie auf mobilen Datenträgern, lokalen Servern oder in der Cloud liegen. Richtlinien für Datenverschlüsselung auf Wechseldatenträgern schützen gegen Verlust, Diebstahl und Industriespionage.
- Device Control: Schnittstellenkontrolle ist enorm wichtig, denn USB-Sticks sind nach wie vor ein Einfallstor für Schadsoftware und Datenklau. Richtlinien müssen klären, wer was mit welchen Geräten machen darf.
- Application Control mit Whitelisting: Nur vertrauenswürdige und erlaubte Anwendungen, die auf der Whitelist stehen, werden vom System ausgeführt. Das gewährleistet bestmöglichen Schutz vor Zero Day Exploits, also noch unbekannten oder nicht-gepatchten Sicherheitslücken, und neuer Malware. AV-Test registriert pro Tag 350.000 neue Malware-Programme. Ein zusätzliches Sicherheitsnetz zu Firewalls und Antivirus ist daher essentiell. Dank Application Control wird Schadsoftware, die es doch ins System schafft, nicht ausgeführt. Zudem sollte es keine lokalen Administrationsrechte geben, damit Anwendungen nicht ungeprüft heruntergeladen und installiert werden können.
- Identity & Access Management: Zugriffskontrolle ist eine weitere kritische Sicherheitsmaßnahme. 2-Faktor- oder Multi-Faktor-Authentifizierung, zum Beispiel mittels Smartcard, schützt besonders dort vor den Folgen von Social Engineering, wo schwache Passwörter verwendet werden. Potenzielle Angreifer erhalten so trotz erbeuteter Login-Daten keinen Zugriff auf Daten und Systeme.

4. Detection & Response

Detection Tools erkennen bestimmte Aktionen, Muster oder Applikationen und ordnen sie ein. So ermitteln sie Anomalien und potentiell gefährliche Verhaltensmuster. Wenn etwa unverhältnismäßig viele Dateien auf einen Wechseldatenträger kopiert werden, könnte das auf Industriespionage hindeuten.

Bei unbekannten Anwendungen helfen File Reputation Services, um die richtige Response-Maßnahme, beispielsweise Blacklisting, zu treffen. Diese Listen sammeln alle Informationen zu Applikationen und stellen sie öffentlich zur Verfügung, denn nicht alles Unbekannte muss zwangsläufig auch gefährlich sein. Bei Bedarf können Geräte auch abgeschaltet, vom Netz genommen oder unter Quarantäne gestellt, Prozesse abgebrochen und Schwachstellen geschlossen werden.

Analyse- und Forensik-Funktionen können schließlich ermitteln, wie die Malware in das System gelangt ist. Aus diesen Erkenntnissen können Security-Teams weitere Response-Maßnahmen ableiten. Indem das Team die Daten in eine Security Information and Event Management (SIEM)-Lösung wie Splunk oder LogRhythm einspeist, profitiert es von zusätzlichen Funktionen wie Alerting und automatisierter Priorisierung.

5. Continuous Improvement Process

Schließlich sollte der gesamte Zero Trust Prozess immer wieder von vorne anfangen, um das Sicherheitslevel in der Organisation stets auf dem höchsten Stand zu halten.

ZERO TRUST IST EIN ZUSAMMENSPIEL VON MEHREREN, SICH ERGÄNZENDEN SICHERHEITSMASSNAHMEN MIT DEM STRATEGISCHEN ZIEL, DATENINTEGRITÄT ZU GEWÄHRLEISTEN UND DATENSCHUTZVERLETZUNGEN ZU VERHINDERN.

Andreas Fuchs, Vice President Products, DriveLock SE, www.drivelock.de

6. Security Education

All diese Sicherheitsmaßnahmen greifen erst dann optimal, wenn die gesamte Belegschaft mitzieht. Natürlich können die Einschränkungen durch die Sicherheitsmaßnahmen Mitarbeiter frustrieren. Denn heutzutage sind sie im Zuge des Mobile-Trends gewohnt, selbstbestimmt zu arbeiten. Aber Unternehmen müssen ihren Mitarbeitern verdeutlichen, dass sie ein wichtiger Teil der Sicherheitsstrategie sind. Gleichzeitig müssen sie eine hohe Produktivität gewährleisten. Hier könnten privilegierte User in einem streng geregelten Self-Service-Prozess Anwendungen selbst freigeben. Darüber hinaus schaffen Schulungen und Kommunikationsmaßnahmen das nötige Sicherheitsbewusstsein und verhindern Frustration.

Zero Trust ist ein Zusammenspiel von mehreren, sich ergänzenden Sicherheitsmaßnahmen mit dem strategischen Ziel, Datenintegrität zu gewährleisten und Datenschutzverletzungen zu verhindern. Das Zero Trust Konzept erreicht dieses Höchstmaß an IT-Sicherheit, indem es so viele Hürden und Einschränkungen wie möglich errichtet und alle Assets, Anwender und Aktionen im System überprüft.

Andreas Fuchs

VERTRAUEN ALLEIN REICHT NICHT

E-MAIL-KOMMUNIKATION IN DER CLOUD

Immer mehr Unternehmen verlagern ihre Prozesse und Anwendungen in die Cloud. Dabei macht sich jedoch nur ein Bruchteil davon Gedanken darüber, ob die Sicherheitsvorkehrungen der Cloud-Anbieter überhaupt ausreichend sind. Sie legen sensible Daten in die Hände von internationalen Konzernen und vertrauen ihnen blind; und das in Zeiten, in denen der Datenschutz eine immer größere Rolle spielt oder besser gesagt durch die Europäische Datenschutz-Grundverordnung (EU-DSGVO) sogar gesetzlich vorgeschrieben ist. Unternehmen, die ihre Anwendungen in die Cloud verlagern, sollten unbedingt ergänzende Verschlüsselungslösungen verwenden. Dies gilt vor allem auch für E-Mails.

Die E-Mail ist inzwischen 35 Jahre alt und wird in nahezu jedem Unternehmen tagtäglich genutzt. Bei all den Vorteilen, die die Kommunikation via E-Mail mit sich bringt, birgt sie natürlich auch einige Sicherheitsrisiken. Ein Großteil der Cyberattacken geht von E-Mails aus, die im Vergleich zu anderen Szenarien eine immense Angriffsfläche bieten, da die „Schwachstelle Mensch" eine wesentliche Rolle spielt. Aus diesem Grund ist es umso wichtiger, gute Vorsorge zu treffen. Werden die Daten – inklusive der Daten der E-Mail-Kommunikation – in der Cloud abgelegt, steigt das Sicherheitsrisiko nochmals um ein Vielfaches. Natürlich versuchen die Cloud-Anbieter glaubwürdig zu vermitteln, die Daten seien gut bei ihnen aufgehoben, und stellen Methoden zur Verschlüsselung bereit. Doch hier gilt die Devise: Wer verschlüsselt, hat auch den Klartext. Auf diese Weise können die Cloud-Provider die E-Mails mitlesen und gelangen an sensible Unternehmensinformationen. Gehen die Daten verloren, kann dies einen immensen wirtschaftlichen Schaden verursachen und einen Betrieb schlimmstenfalls in den Ruin treiben. Die Annahme, die Sicherheitsmaßnahmen der Cloud-Anbieter für E-Mails würden genügen, stellt sich damit als Trugschluss heraus. Gefordert sind daher zusätzliche Lösungen, die den deutschen Sicherheitsstandards entsprechen und den E-Mail-Verkehr in der Cloud ausreichend absichern.

Risikofaktoren minimieren

Schaut man sich die internen und externen Kommunikationsprozesse in Unternehmen an, so ist es erstaunlich, wie viele vertrauliche Informationen noch immer ungeschützt per E-Mail verschickt werden. Dies trifft auch auf E-Mails zu,

die in der Cloud abgelegt werden, denn die dort integrierten Sicherheitsvorkehrungen schließen längst nicht alle Hintertüren. Hier weiß man also letzten Endes nie genau, wer wirklich auf die Daten zugreifen kann und wofür diese genutzt werden.

Doch selbst wenn Unternehmen sich über dieses Risiko bewusst sind, hat die Absicherung ihres wichtigsten Kommunikationsmittels häufig keine Priorität. Geht es darum, eine umfassende Verschlüsselungslösung einzuführen, sehen die Verantwortlichen keine Veranlassung dafür, da die Investition nicht direkt zum Umsatz beiträgt. Auf den ersten Blick mag dies vielleicht sogar stimmen. Aber was ist, wenn der Ernstfall eintritt und der Datendiebstahl die Existenz des Betriebes bedroht? Viele Firmen investieren in den Objektschutz und bauen Zäune auf oder installieren Videokameras. Bei Sicherheitsmaßnahmen für das zentrale Kommunikationstool wird dann aber der Rotstift angesetzt. Dabei muss man sich nur einmal die Frage stellen, für welche sensiblen Bereiche E-Mails Verwendung finden: angefangen bei Mitarbeiterinformationen bis hin zu Konstruktionszeichnungen, Verträgen, Produktinnovationen. Im Falle des Verlustes solcher Daten ist es sogar denkbar, dass Verantwortliche mit ihrem Privatvermögen haften müssen. Dieser Gefahr sind sich zahlreiche Geschäftsführer nicht im Geringsten bewusst. Abgesehen von der Schutzfunktion, die eine professionelle Verschlüsselungslösung übernimmt, hat sie den positiven Nebeneffekt, das Vertrauen zu den Kunden und Partnern zu erhöhen. Für den Erfolg muss die verwendete Lösung allerdings einige Anforderungen erfüllen.

Sicherheitslücken schließen

Damit Dritten erst gar keine Chance gelassen wird, vertrauliche Unternehmensinformationen abzugreifen, ist die Nutzung einer professionellen E-Mail-Verschlüsselungslösung Pflicht. Diese Lösung sollte in erster Linie benutzerfreundlich sein und sich problemlos in den gewöhnlichen Versandprozess integrieren lassen. Sie darf keinesfalls die E-Mail-Kommunikation stören oder Mehraufwand für den Anwender verursachen. Als All-In-One-Lösung ist es wichtig, dass sie alle gängigen Verschlüsselungsstandards wie S/MIME, OpenPGP, TLS und Domainverschlüsselung unterstützt und bei jedem Versand zunächst prüft, ob der Empfänger bereits über eigenes Schlüsselmaterial verfügt. Wenn ja, sollte die jeweils beste Methode vollautomatisch zum Einsatz kommen. Um eine uneingeschränkte Kommunikation zu gewährleisten, ist es zudem wichtig, dass die Lösung die verschlüsselte Spontankommunikation mit Adressaten erlaubt, die selbst noch keine Verschlüsselungslösung im Einsatz haben. Auch übergroße Dateien sollten sich problemlos verschlüsselt verschicken lassen. Zur Sicherstellung von Authentizität und Integrität ist außerdem die Anbringung einer digitalen Signatur erforderlich. Alle genannten Punkte sollten auf einer zentralen Administrationsoberfläche bedienbar und für den Nutzer möglichst transparent sein beziehungsweise sich mit nur minimalem Aufwand bewerkstelligen lassen.

UM EINE DURCHGÄNGIGE ENDE-ZU-ENDE-SICHERHEIT ZU ERREICHEN, GILT ES, SÄMTLICHE SENSIBLE INHALTE ZU SCHÜTZEN – EGAL OB MAN SIE ÜBER E-MAILS MIT EXTERNEN PARTNERN AUSTAUSCHT ODER INFORMATIONEN IN DIE CLOUD SENDET.

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

Ganzheitliche Verschlüsselung

Um eine durchgängige Ende-zu-Ende-Sicherheit zu erreichen, gilt es, sämtliche sensible Inhalte zu schützen – egal ob man sie über E-Mails mit externen Partnern austauscht oder Informationen in die Cloud sendet. Deshalb sollte eine geeignete Verschlüsselungslösung alle Daten verschlüsseln, die außerhalb des Unternehmens abgelegt werden. Diese Daten werden derart unleserlich gemacht und sind für Cyberkriminelle wertlos. Dabei sollten die Client-Funktionen wie Suche und Sortierung für den Benutzer erhalten bleiben. Zum anderen muss der Informationsfluss abgesichert werden, sodass die Daten, die sich auf dem Transportweg befinden, geschützt sind. So ist der Austausch von Inhalten und Dateianhängen zu jedem Zeitpunkt verschlüsselt und für Angreifer unbrauchbar – auch wenn die Daten bei Cloud-Providern liegen.

Fazit

Die aktuellen Entwicklungen hinsichtlich des verschärften Datenschutzes und der zunehmenden Hackerangriffe bringen Unternehmen in Zugzwang. Sie haben mittlerweile gar keine Wahl mehr, überhaupt darüber nachzudenken, eine angemessene Verschlüsselungslösung für den unternehmensübergreifenden elektronischen Informationsaustausch einzusetzen. Stattdessen sind sie gefordert, eine geeignete Lösung zu finden, die ihren Ansprüchen entspricht. Im Zuge der steigenden Tendenz zum Einsatz von Cloud-Anwendungen müssen moderne Verschlüsselungslösungen die Anforderungen dieser Technologieplattformen ebenfalls berücksichtigen. Nur so ist eine ganzheitlich gesicherte Kommunikation möglich.

Günter Esch

IAM FÜR MEHR TRANS

ERLEICHTERTER EINSTIEG DANK VORGEFERTIGTER FUNKTIONSBAUSTEINE

Die Gefahr, einer Cyberattacke zum Opfer zu fallen, steigt. Unternehmen sind daher gefordert, Einfallstore, über die sich Hacker Zugriff verschaffen könnten, zu schließen. Die Kontrolle von Zugriffsberechtigungen wird dabei häufig vernachlässigt. Erst im Sommer hatten einige Krankenhäuser und DRK-Einrichtungen in Rheinland-Pfalz und im Saarland mit Malware zu kämpfen. Die Ursache: ein altes Dienstkonto. Wie das Beispiel zeigt, sollten Betriebe immer wissen, welcher Mitarbeiter welche Zugriffsrechte besitzt. Geht dieser Überblick verloren, sind Sicherheitslücken vorprogrammiert.

Im Interview mit it security-Publisher Ulrich Parthier spricht Thomas Gertler, Geschäftsführer von G+H Systems, darüber, warum es einer Softwarelösung bedarf, die Ordnung in das Zugriffsrechtechaos eines Unternehmens bringt, und was diese können sollte.

? **Ulrich Parthier:** *Den Begriff IAM hört man spätestens seit der Einführung der Europäischen Datenschutz-Grundverordnung immer wieder. Doch was hat es damit auf sich?*

Thomas Gertler: IAM behandelt das Thema Bereitstellung, Verwaltung und Kontrolle von Identitäten und deren Zugriffe auf IT-Ressourcen. Verlässt ein Mitarbeiter ein Unternehmen, muss ihm der IT-Verantwortliche die Zugriffsrechte entziehen. Neue Beschäftigte hingegen sollten ihre Berechtigungen schnellstmöglich erhalten. Ohne eine zentrale Softwarelösung ist nur schwer nachvollziehbar, worauf der ehemalige Arbeitnehmer zugreifen konnte, beziehungsweise welche Berechtigungen ein neuer Mitarbeiter benötigt. Um Zugangsdaten sowie Zugriffsberechtigungen strukturiert zu verwalten, ist der Einsatz einer solchen Lösung also anzuraten. Sie unterstützt dabei, Personen in unterschiedlichen Abteilungen bestimmte Rollen zuzuordnen und auf Basis dieser Festlegungen, Berechtigungen und Zugänge automatisch zu vergeben oder zu entziehen. Außerdem ermöglicht eine derartige Lösung, Berechtigungsvorlagen zu erstellen, die auf zukünftige Mitarbeiter übertragbar sind. So lässt sich langfristig sicherstellen, dass die jeweiligen Personen das richtige Maß an Berechtigungen besitzen. Zusammengefasst sorgt eine IAM-Lösung für mehr IT-Sicherheit im Unternehmen und hilft bei der Einhaltung gesetzlicher Anforderungen.

? **Ulrich Parthier:** *Wie schätzen Sie die aktuelle Umsetzung in Unternehmen ein?*

Thomas Gertler: In vielen großen Betrieben spielt das Thema IAM bereits eine tragende Rolle, doch in kleinen und mittelständischen Unternehmen wird es oft vernachlässigt. Dabei ist es selbst für kleine Firmen schwierig, bei der Vielzahl ihrer Systeme und Anwendungen nicht „im Zugriffsrechtechaos zu versinken". Ein Unternehmen mit zehn Mitarbeitern in fünf Zielsystemen verwaltet bereits bis zu 50 Benutzerkonten, und eines mit 30 Mitarbeitern in 15 Zielsystemen sogar stolze 450. Treten bei dieser Menge erst einmal fehlerhafte Berechtigungskonstellationen auf, sind die eigene IT-Sicherheit sowie sensible Daten in Gefahr. Nur eine softwarebasierte Lösung verschafft Transparenz über die Rechtestrukturen und minimiert unbefugte Datenzugriffe.

? **Ulrich Parthier:** *Was sollte eine geeignete IAM-Lösung mit sich bringen?*

Thomas Gertler: Wichtig ist es, eine herstellerunabhängige Lösung einzusetzen, mit der sich alle Systeme in der IT-Landschaft auslesen lassen. Um sich direkt ans Zielsystem anzubinden, bedarf es spezieller Konnektoren. Sofern dies nicht möglich ist, sollten Exportdateien wie CSV und XML verwendbar sein. Hierdurch wird Transparenz über die komplette IT-Landschaft geschaffen. Die Software sollte zudem den Mitarbeiterstamm eines Unternehmens importieren und Zielsysteme auslesen können. Dies bringt Daten in einen Zusammenhang und legt dar, wo und in welchem System ein Mitarbeiter Zugriffsberechtigungen hat. Zusätzlich ist es notwendig, Berechtigungen zertifizieren zu können. Derart lässt sich festlegen, ob und über welchen Zeitraum ein Mitarbeiter gewisse Berechtigungen haben darf. So wird verhindert, dass ein ehemaliger Angestellter noch nach Jahren auf Unternehmensdaten zugreifen kann. Darüber hinaus ist es sinnvoll, dass die Lösung ein Bereinigungstool integriert. Wird im Zuge der Zugriffsüberwachung ein Missstand deutlich, können darüber ein Löschantrag getriggert und Probleme zügig behoben werden. Grundsätzlich gilt es, bei der Wahl der Software zu bedenken, woher der Anbieter stammt. Es empfiehlt sich, auf Lösungen deutscher Hersteller zu vertrauen, die keine Schwachstellen aufweisen.

? **Ulrich Parthier:** *Wie haben Sie als Hersteller sich auf die Marktsituation vorbereitet?*

Thomas Gertler: Um auf die Anforderungen unserer Kunden individuell einzugehen, haben wir unsere Software daccord

PARENZ

> UM ZUGANGSDATEN SOWIE ZUGRIFFSBERECHTIGUNGEN STRUKTURIERT ZU VERWALTEN, IST DER EINSATZ EINER IDENTITY & ACCESS-LÖSUNG ANZURATEN.
>
> Thomas Gertler, Geschäftsführer, G+H Systems, www.guh-systems.de

weiterentwickelt und bieten drei Editions an. Die Access Governance Edition dient zur globalen Auswertung und Zertifizierung von Berechtigungen in beliebigen Zielsystemen. Sie eignet sich für Unternehmen, die IT-Sicherheitsrichtlinien nach gesetzlichen Vorgaben erfüllen müssen und einen Einstieg in das IAM anstreben. Mit der Microsoft Edition haben wir auf Kundenanfragen reagiert, die sich zentrale Auswertungsmöglichkeiten für ihre Microsoft-Umgebungen wünschen. Diese Edition ermöglicht die Analyse und Überwachung der Berechtigungen im Active Directory und NTFS-Filesystem. Die Advanced Edition ist für Unternehmen geeignet, die ein komplettes IAM-System mit umfangreichen Funktionalitäten einführen möchten.

? **Ulrich Parthier:** *Welchen Vorteil bietet ein vollständiges IAM-System?*

Thomas Gertler: Gerade großen Unternehmen reicht eine reine Access-Governance-Lösung oftmals nicht aus. Sie benötigen ein umfassendes und skalierbares Identity and Access Management System. Damit die Verantwortlichen nicht ins kalte Wasser geworfen werden und überfragt sind, wo sie überhaupt beginnen sollen, gibt es vorkonfigurierte, praxisgeprüfte Funktionsbausteine.

? **Ulrich Parthier:** *Vorgefertigte Bausteine – das klingt interessant. Wie kann man sich diese vorstellen? Welche Funktionen können damit abgedeckt werden? Und lassen sie sich auch individualisieren?*

Thomas Gertler: Unsere Erfahrung mit IAM-Systemen bei Kunden hat uns gezeigt, dass bestimmte Prozesse oft ähnlich ablaufen. Daher sind vorgefertigte Funktionsbausteine sehr gefragt. Uns ist aufgefallen, dass die Unternehmen es dadurch einfacher haben, ein IAM-System zu etablieren. Denn viele haben Respekt davor, auf einer „grünen Wiese" zu starten und jeden Prozess neu zu definieren. Aus diesem Grund sträuben sie sich davor, den ersten Schritt in ein umfassendes IAM zu gehen. Mit unserer daccord Advanced Edition können wir zum Beispiel Beantragungs- und Genehmigungsprozesse vorkonfigurieren oder standardisierte Anbindungen an Quell- und Zielsysteme integrieren. Dennoch sind wir in der Lage, die Module an spezifische Kundenwünsche anzupassen. So bieten wir maximale Flexibilität.

! **Ulrich Parthier:** *Herr Gertler, wir bedanken uns für das informative Gespräch!*

NETZWERKSEGMENTIERUNG

JETZT AUCH IM SECURITY-BEREICH

„MAN KANN NICHT SEGMENTIEREN, WAS MAN NICHT SIEHT!" EINE EINFACHE REGEL.

Oliver Keizers, Regional Director, DACH, illumio, www. illumio.com

Den Begriff der Netzwerksegmentierung gibt es schon lange, er stammt aus der Notwendigkeit, performante Netze zu unterteilen, um Broadcast Zeiten zu verringern. Irgendwann kam das Konzept der Segmentierung zu Sicherheitszwecken dazu und die Geschichte nahm ihren Lauf. Unternehmen setzen heute traditionelle Netzwerkarchitektur ein, um die Sicherheit im Rechenzentrum zu erhöhen und es Angreifern zu erschweren, sich weiter im Netz zu bewegen.

Hieraus entsteht Reibung und Interessenskonflikte, weil die traditionellen Netzwerktechnologien darauf optimiert sind, Leistung und Funktion zu erbringen, sie wollen offen und performant sein. Die Anforderungen der Sicherheit jedoch stehen dem entgegen, hier geht es um Kontrolle und Isolation, man will eben geschlossen sein. Diese widerstrebenden Interessenslagen sorgen für Probleme, die sich mit den Anforderungen moderner IT an Agilität, Cloud oder Container nicht vereinbaren lassen.

Gehen wir mal einen Schritt zurück: Warum setzen Unternehmen Segmentierungsprojekte auf die Tagesordnung? Hier sind einige dieser Gründe zu finden:

1. Regulatorische Anforderungen und Compliance
2. Schutz von Kronjuwelen und kritischen Applikationen
3. Fusionen und Akquisitionen
4. Einbruchsschutz und Schadensbegrenzung
5. Cloud-Migrationen
6. Firewall-Aktualisierungen
7. Transport-Verschlüsselung im RZ

All diese Themenbereiche stehen im Konflikt mit der oben genannten Problematik der widerstrebenden Interessenslagen in der traditionellen Segmentierung. Aber muss das so sein? Und was benötigt ein Unternehmen, um diese initialen Treiber zu erfüllen?

Abhängigkeit von IP Adressen

Fragt man einen erfahrenen Netzwerkarchitekten, ob er ein Netz ohne Anforderungen aus der Security anders bauen und konfigurieren würde, bekommt man immer dieselbe Antwort: Auf jeden Fall. Die größte Herausforderung vor der Network Security Engineers stehen, ist die Abhängigkeit von IP Adressen und die damit verbundene fehlende Flexibilität. Kleine Änderungen werden damit zu großen Aufwänden, die meist gescheut werden. Segmentierung ist somit ein recht ungeliebtes Thema geworden.

Visibilität in die Datenflüsse

Es erscheint offensichtlich, dass man nur das segmentieren, also unterteilen kann, was man kennt und versteht. Wer schon einmal versucht hat, den Datenverkehr in einem RZ zu analysieren und zu dokumentieren, wird nachvollziehen können, dass die Forderung an Transparenz leicht gestellt und schwer erfüllt wird. Technologien wie Cloud und Container erschweren die Erledigung dieser Anforderung noch ungemein. Jeder technisch versierte Administrator wird Tools wie Wireshark kennen und nutzen, dann aber feststellen, dass eine Echtzeitbetrachtung des gesamten Datenverkehrs in einem RZ und auch in Richtung der neueren RZ Technologien damit unmöglich ist. Die erste Forderung an ein Segmentierungsprojekt muss also lauten, Visibilität zu erzeugen.

Zentral gemanagte Enforcement Punkte

Solange man sich innerhalb eines abgeschlossenen RZ befindet, scheint es logisch durch Einsatz von Firewalls abgeschlossene Segmente zu produzieren. Erstreckt sich ein Unternehmen und dessen Applikationen über mehrere RZs, wird dies schon erheblich schwieriger und nahezu unmöglich, wenn man Cloud Infrastruktur Services wie Azure oder AWS verwendet.

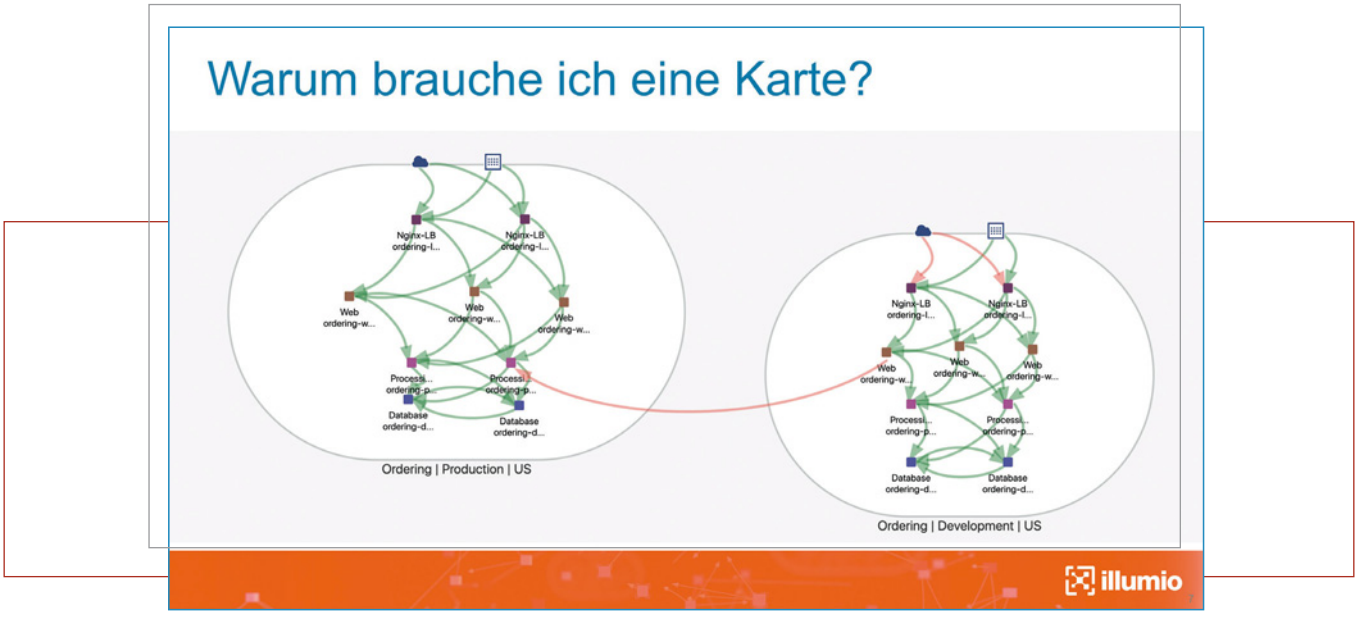
Hier hat der Einzelne keine Kontrolle mehr über die Datenflüsse und Enforcement Punkte, sondern muss sich auf diverse Komponenten verlassen. Hier sind unterschiedliche Firewall Hersteller, Security Groups, Security Tags, VLANs genannt, die ebenfalls nicht zentral verwaltet werden können, durch ihre Unterschiedlichkeit zu administrativen Bürden werden und somit zu Fehlkonfigurationen führen.

Nimmt man nur diese drei Punkte alleine, erklärt sich gut, dass traditionelle Segmentierung durch die Netzwerk-Architektur an einem Ende angekommen ist und es neuer Wege bedarf. Eine ähnliche Situation haben wir bereits schon einmal erlebt. OS Virtualisierung folgte demselben Muster. Es erschien unglaublich, ein Betriebssystem, eine Applikation von der Hardware zu trennen. Mittlerweile trennt man sogar die Komponenten einer Applikation selber auf und Virtualisierung ist Mainstream.

Um Segmentierung erfolgreich, agil und schlussendlich kostengünstig gestalten zu können benötigt man also ein paar Voraussetzungen:

1. Eine Unabhängigkeit von IP-Adressen
2. Eine Landkarte der Verkehrsflüsse
3. Einen zentralen, einheitlichen Prozess

Jedes Unternehmen verfügt über mehr oder weniger gute Informationen über die eingesetzten Systeme und Server, meist im Rahmen einer CMDB, einer As-



set-DB oder anderem. Diese Quellen enthalten beschreibende Informationen über die Systeme, die sich meist in Form von Labeln darstellen. Wo steht ein Server, was für eine Applikation unterstützt der Server, zu welcher Umgebung (Test, Dev, Prod) gehört der Server und oftmals auch, welche Rolle nimmt der Server ein, also Web-, Application- oder DB-Server.

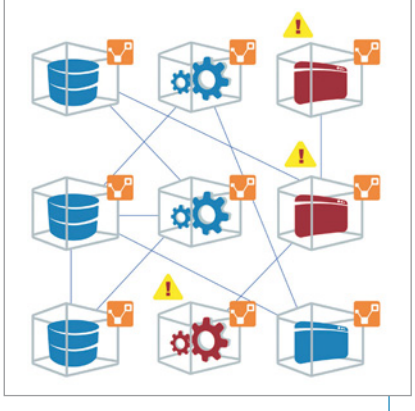
Mit Hilfe dieser Daten ist es ein leichtes, Regeln zu schreiben, die im Klartext und verständlich sind: „Der Webserver der CRM Applikation in der produktiven Umgebung in Deutschland darf nur mit den Processing-Server der produktiven Umgebung in Deutschland sprechen" oder noch einfacher: „Systeme in der Dev Umgebung dürfen nur mit Systemen in Dev sprechen". Die Abwesenheit von IP-Adresse, die Abstrahierung über Label ermöglicht vollkommen neue Segmentierungsregeln.

„Man kann nicht segmentieren, was man nicht sieht!" Eine einfache Regel. Es wird also eine Darstellung der Kommunikation zwischen den einzelnen Servern benötigt. Wer spricht mit wem, grafisch aufbereitet. So erkennt man sofort Fehlkonfigurationen, kann Systemgrenzen festlegen und die Kommunikation innerhalb einer Applikation analysieren und verstehen.

Eine Landkarte, ähnlich Google Maps, in der die Systeme wie Orte sind, die Kommunikation wie Straßen sind und Verkehrsflüsse dargestellt werden, das ist die Grundlage einer erfolgreichen Segmentierungsstrategie und das Kernelement von guten Lösungen. Aus dem Wissen über die faktisch vorhandene Kommunikation kann man dann Regeln ableiten und Systeme schützen.

Das schwächste Glied der Kette

Jeder Firewall Admin kennt die Situation nur zu gut, man hat eine neue Regel implementiert und es beginnt der Moment der gespannten Erwartung. Wird das Telefon klingeln? Habe ich einen Fehler gemacht? Geht alles gut? Die Komplexität von Firewall Regeln ist nicht für Segmentierungsregeln gemacht worden, jedes System hat seine eigenen Logiken, jeder Cloud Service seinen eigenen Gesetze. Man benötigt also ein zentrales System, das die vorhandenen Firewalls der jeweiligen Server kennt und administrieren kann.



Applikationsabhängigkeiten in einer Live Karte

Diesem System zugrunde muss ein Prozess liegen, in welchem man die vorhandenen Verbindungen darstellen kann, auf Basis derer dann Regeln gebaut und diese sicher getestet werden können. Der Test implementiert bereits die erstellten Regeln, fügt aber ein Sicherheitsnetz ein, über welches unerkannte Flows gemeldet und dann bewertet werden können. Erst danach werden diese Regeln scharf geschaltet und die Systeme von der restlichen Umgebung abgetrennt.

Durch diese quasi Virtualisierung der Segmentierung wird sie nutzbar und ermöglicht Unternehmen die eingangs erwähnten Anforderungen auch zu erfüllen.

Oliver Keizers

USER VS. HACKER

WIE WERDEN MITARBEITER FIT GEGEN PHISHING & CO.?

it security sprach mit Alexander Held, Teamleiter Vertrieb Network and Security beim IT-Dienstleister netlogix, über die Sensibilisierung von Usern gegen professionelle Phishing-Angriffe.

it security: *Wie kommt es zu Passwortverlust und welche Folgen entstehen daraus?*

Alexander Held: Hacker nutzen immer ausgereiftere Strategien, um an Passwörter zu kommen. Meist haben sie dann nicht nur Zugriff auf einen Account, denn oft verwenden User Anmeldedaten mehrfach. Neben dem finanziellen Schaden durch den Diebstahl von geistigem Eigentum ist auch Imageverlust ein großes Problem.

it security: *Was können User gegen Passwortverlust tun?*

Alexander Held: Starke Passwörter sind Pflicht! Da niemand sich 20-stellige Kombinationen merken kann, ist eine einfach nutzbare Lösung zur Passwortverwaltung entscheidend. Darüber hinaus müssen User ein Bewusstsein dafür entwickeln, nicht jeden E-Mail-Anhang zu öffnen oder Daten unverschlüsselt preiszugeben.

it security: *Wie können sich Unternehmen gegen Angriffe wappnen?*

Alexander Held: Mit einem durchdachten Konzept zur Sensibilisierung kann man User als häufige Schwachstelle beim Thema Passwortverlust adressieren, ohne diese an den Pranger zu stellen. Denn für Laien ist es nahezu unmöglich, Phishing-Versuche zu erkennen. Umso wichtiger ist es, Anwender für Gefahren aus dem Internet zu sensibilisieren. Eine nachhaltige Strategie umfasst daher, neben einer geeigneten Lösung zur Passwortverwaltung, auch die Komponenten Angriffssimulation zur kontinuierlichen Schulung der Mitarbeiter und regelmäßige Prüfung auf bereits kompromittierte Accounts, um aktiv gegensteuern zu können.

Sinnvoll ist es auch, sich von einem Experten beraten zu lassen. Denn wer die Gefährdungslage kennt, kann durch Optimierung vorhandener Strukturen schnell und günstig die unternehmensweite Sicherheit verbessern.

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

www.netlogix.de


noris network
RZ-SICHERHEIT?
WIR ÜBERTREIBEN
GERNE!
FREIE RECHENZENTRUMSFLÄCHEN
MÜNCHEN | NÜRNBERG | HOF
noris.de/unsere-rechenzentren