itmanagement

MAI/JUNI 2020

INKLUSIVE 24 SEITEN

IT SECURITY SPEZIAL

ERFOLGSFAKTOR CYBER SECURITY

DIGITALISIERUNG IM MITTELSTAND

Dirk Lieder, CONET

DIGITAL PROCESS AUTOMATION

The Next Step

DIGITAL TRANSFORMATION

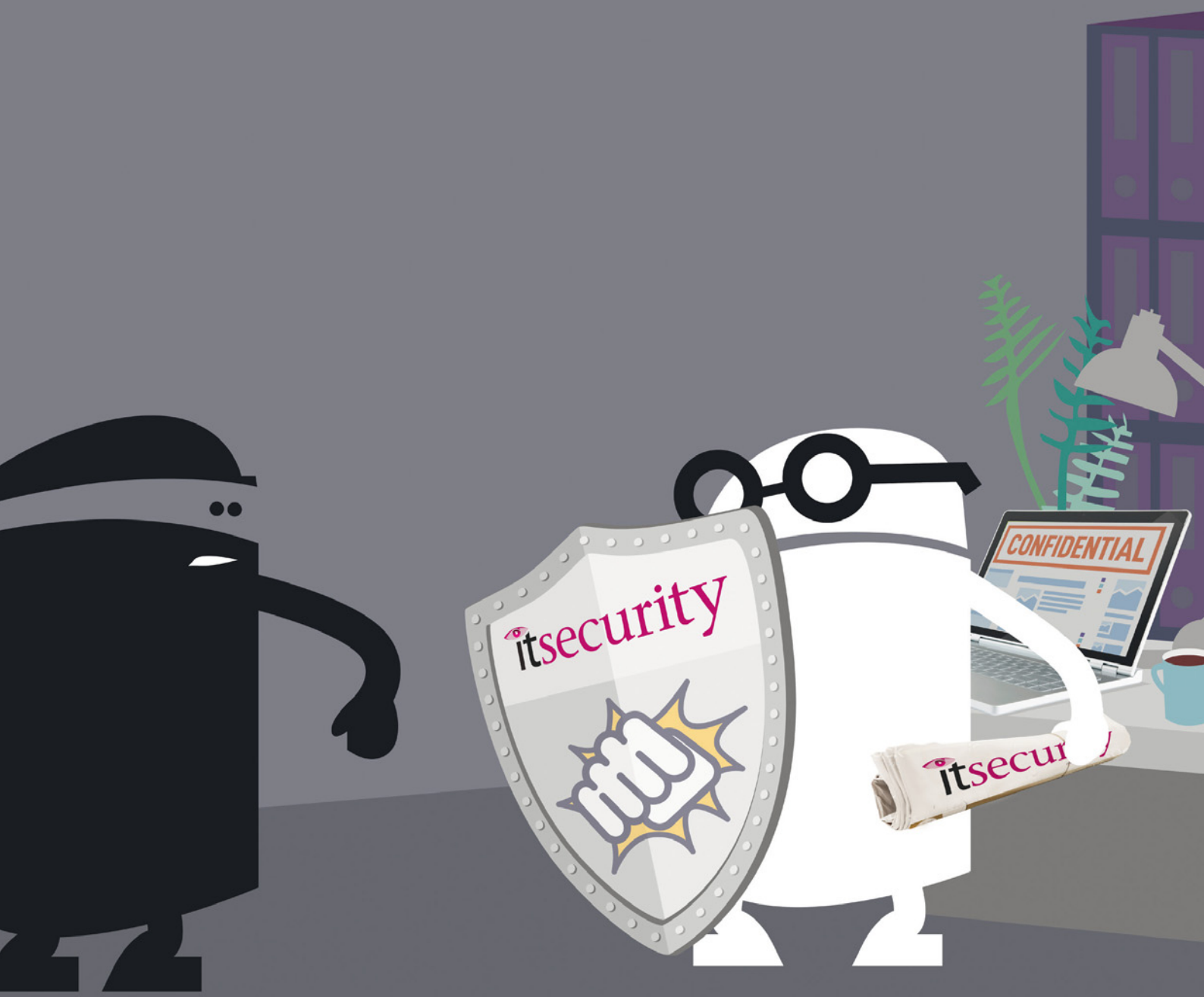
Die größten Hindernisse

WISSENSDATEN-BANKEN

Bessere Servicequalität

www.it-daily.net

Wer viel weiß, weiß sich zu wehren.



Der nächste Angriff kommt bestimmt.

Gut vorbereitet mit itsecurity

www.it-daily.net

DAS LEBEN GEHT WEITER!

Kein Zweifel, das Corona-Virus hat unser aller Leben verändert. Aus meiner Sicht allerdings positiv. Positiv in dem Sinne, dass man Arbeit, feste Strukturen, Kollegen, soziale Nähe jetzt besser zu würdigen weiß, als vor der Krise.

Was mich wirklich bestürzt, ist das Totalversagen des Staates: Es liegt ein Kollektivversagen von Staat und Politik vor. Ähnlich wie bei allen Problemen und Zukunftsaufgaben wie der Digitalisierung inklusive 5G, der Energiewende, dem Fachkräftemangel, der Rentenreform, der Wahlrechtreform, der Länderreform lautet mein Fazit: Danke für NICHTS!

Von den Luschen der Politik und den Cuncatoren der Verwaltung können wir also in Zukunft nichts erwarten. Das ist aber auch das Einzige worauf Sie sich verlassen können. Was hilft, ist nur die Eigeninitiative: In China und anderen Ländern sind aus der Not heraus neue Jobs beispielsweise in der Logistik entstanden, Take aways und Internetplattformen haben Konjunktur.

Auch das stationäre Leben wird nicht mehr lange auf sich warten lassen, wenn auch zunächst auf kleinerer Flamme. Deshalb ist es jetzt um so wichtiger nicht auf den Lockdown zu starren, alten Zeiten nachzutrauern und nach Subventionen zu schreien, auch wenn Überbrückungskredite in vielen Fällen wichtig und notwendig sind, sondern sich auf den Boost vorzubereiten, denn es wird mit Sicherheit in vielen Bereichen auch einen enormen kurzfristigen Nachholbedarf geben.

Mein Tipp: Fragen Sie sich, ob ihr Angebot noch zeitgemäß ist. Sind sie personell richtig aufgestellt? Denken Sie jetzt über Veränderungen und Anpassungen nach. Was ziehen sie für Lehren aus dem Lockdown? Wie verfahren Sie bei einem erneuten Shutdown, wenn eine andere, erneute Krise im Anmarsch ist? Seien Sie bereit: Treffen Sie jetzt die Vorbereitungen und Entscheidungen für morgen!

Herzlichst

Ulrich Parthier

INHALT

10

COVERSTORY

26

30

Inklusive 24 Seiten

IT SECURITY SPEZIAL

IT INFRASTRUKTUR

FABRIK DER ZUKUNFT

ALLES IST MÖGLICH

Die Digitalisierung ist eine mögliche Antwort auf fehlende Planungssicherheit und Restrukturierung. Doch das bedeutet Investitionen in Zeiten sinkender Umsätze. Unternehmen sind derzeit nur bereit zu investieren, wenn die Innovation rasch ihre Wirkung entfaltet.

Drei Bereiche bieten hier besonders gute Ansatzpunkte:

1. **Neuartige Dienstleistungen – der Wert der Daten**
Immer mehr Maschinen sind vernetzt und haben gelernt zu sprechen. Sie liefern permanent eine Fülle von Daten. Daraus lassen sich wertvolle Informationen gewinnen. Unternehmen können diese Daten zusätzlich zum eigenen Produkt verkaufen.

2. **Eng vermaschte Wertschöpfungsketten**
Mit der Digitalisierung rücken Lieferanten, Hersteller und Kunden enger zusammen. Dies macht Prozesse transparenter, schneller und damit effizienter.

3. **Mensch-Maschine-Schnittstelle**
Augmented Reality und Geodatendienste helfen Fehler zu vermeiden und Zeit einzusparen. Virtual Reality unterstützt bei der Wissensvermittlung. Und Benutzerschnittstellen sind besonders dann hilfreich, wenn sie sich auf die jeweilige Umgebung einstellen.

www.telekom.com

SICHERES COWORKING

SIND COWORKING-MÖGLICHKEITEN VORHANDEN?

NEIN

Auswahl und Implementierung

Dinge , auf die Sie nun achten müssen:

- Auswahl der richtigen Produkte/Lösungen
- Geeignete Skalierung
- Lizenzen und Vertragslaufzeiten
- Implementierungsaufwand
- Information der Mitarbeiter
- Sicherheitsaspekte und Risiken
- Eventueller Rückbau der Lösung

JA

Ausbau und Verwendung

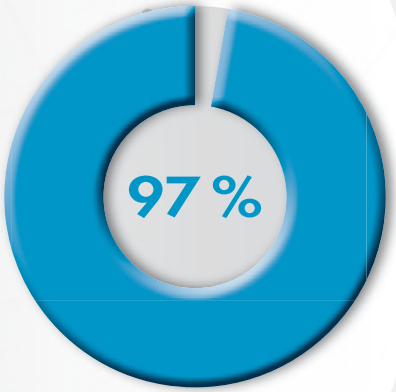
Dinge, auf die Sie nun achten müssen:

- Systemressourcen
- Beschränkungen
- Lizenzen
- Information der Mitarbeiter
- Einhaltung der Richtlinien
- Sicherheitsrisiken durch Last

www.pwc.de

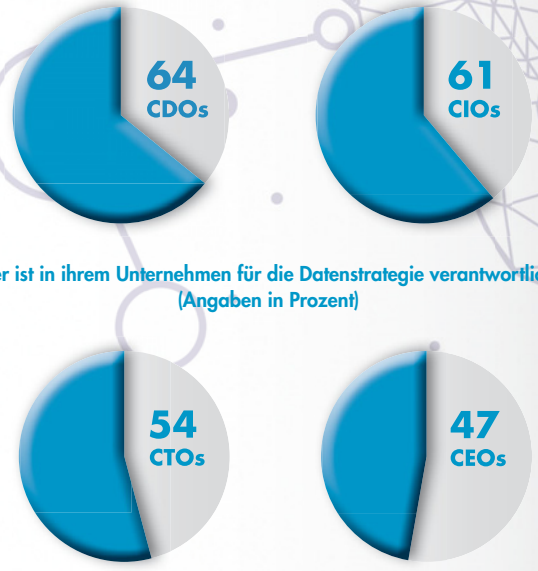
DATENSTRATEGIE

WER IST VERANTWORTLICH?



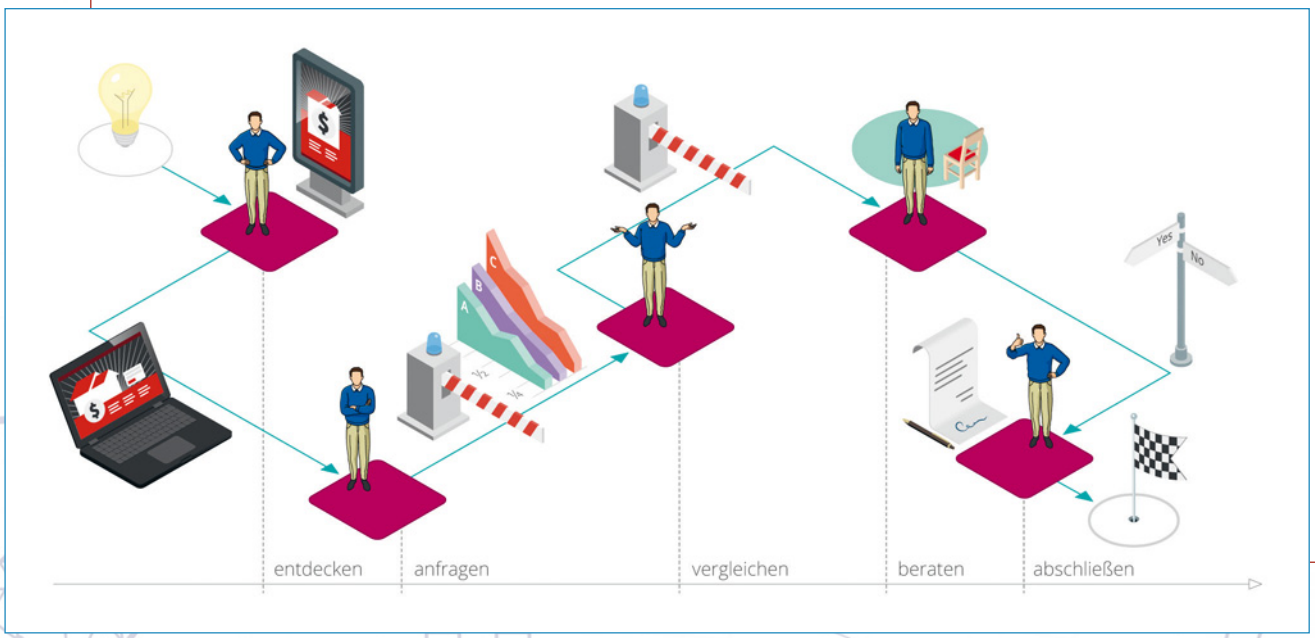
... der deutschen Unternehmen haben nach eigenen Angaben bereits eine Datenstrategie definiert

davon



Wer ist in ihrem Unternehmen für die Datenstrategie verantwortlich? (Angaben in Prozent)

www.exasol.com



FÜNF SCHRITTE

KUNDENZENTRIERTES PROZESSMANAGEMENT

Customer Journey Mapping ist eine effektive Methode, um das Kundenerlebnis zu visualisieren und mit den unternehmenseigenen Prozessen zu verbinden. Signavio zeigt, wie Unternehmen in fünf einfachen Schritten eine Customer Journey Map erstellen und damit ein kundenzentriertes Prozessmanagement umsetzen können.

1. Definition einer Persona

Vor der Modellierung einer Customer Journey muss der Kunde besser verstanden werden. Um aus abstrakten qualitativen Daten ein schemenhaftes Bild von Kunden zu generieren, werden Personas generiert, also fiktive Personen, die eine bestimmte Zielgruppe repräsentieren. Da die Eigenschaften der Personas auch die Customer Journeys definieren, sollte jede Customer Journey Map genau auf eine Persona zugeschnitten sein.

2. Abbildung des Ist-Zustands einer Customer Journey

Jede Customer Journey ist eine Abfolge von Kernelementen wie Schritten, Kontaktpunkten und Momenten der Wahrheit.

Schritte sind durch einfache Linien verbunden und zeigen detailliert die Abfolge einzelner Ereignisse. Kontaktpunkte stehen für alle Schritte, bei denen die Kunden mit dem Unternehmen in Berührung kommen. Jeder Kontaktpunkt bezieht sich auf mindestens einen Kernprozess, eine Rolle oder ein IT-System. Momente der Wahrheit sind wichtige Entscheidungspunkte, die die Chance auf einen Erfolg bei den Kunden steigern oder mindern können.

3. Integration der Customer Journey in die Prozesslandschaft

Um zu verstehen, wie die Customer Experience und die alltäglichen Abläufe im Unternehmen verknüpft sind, muss ein Abgleich der Customer Journey mit den einzelnen Prozessen erfolgen. Deshalb muss ein Unternehmen im nächsten Schritt die neu erstellte Customer Journey Map in seine Prozesslandschaft integrieren. Das Ziel muss sein, alle Kontaktpunkte eindeutig zu modellieren.

4. Anpassung der Customer Journey Map zur Optimierung der Customer Experience

Der Ist-Zustand einer Customer Journey Map zeigt eindeutig auf, welche Schwachstellen die Prozesse für die Kunden aufweisen. Darauf aufbauend können interne Verbesserungsinitiativen gestartet und Customer Journey Maps neu modelliert werden.

5. Bestimmung der zukünftigen Prozesslandschaft

Die für eine ideale Customer Journey Map identifizierten Kontaktpunkte der Kunden mit den internen Prozessen kann ein Unternehmen dann mit denjenigen der aktuellen Customer Journey vergleichen. Basierend hierauf besteht dann die Möglichkeit, die nötigen Schritte zur Optimierung der internen Prozesse entlang der Customer Journey umzusetzen.

www.signavio.com/customerjourney/de/

EDGE COMPUTING

VIER VORTEILE FÜR DAS INTERNET OF THINGS

IoT-Anwendungen stellen anspruchsvolle Anforderungen an die IT-Infrastruktur. Sie benötigen geringste Latenzzeiten bei gleichzeitig höchster Skalierbarkeit, Ausfallsicherheit und Verfügbarkeit. Das erklärt die Tatsache, dass sich Edge Computing zu einer besonderen und zunehmend wichtigen Disziplin innerhalb einer Netzwerk-Infrastruktur entwickelt hat.

Für den Schutz kritischer Infrastrukturen, zeichnet sich Edge Computing im IoT-Umfeld gegenüber Cloud- und Datacenter-zentrierten Ansätzen vor allem durch diese vier Vorteile aus:

1. **Geschwindigkeit**
2. **Sicherheit**
3. **Kosten**
4. **Skalierbarkeit**

www.opengear.com

CYBER SECURITY

DIGITALISIERUNG IM MITTELSTAND

Digitalisierung, Cloud, Künstliche Intelligenz, Cyber Security. Alle diese Themen sind miteinander verwoben. Der CONET-Geschäftsführer Dirk Lieder im Gespräch mit Ulrich Parthier, Herausgeber it management.

Ulrich Parthier: *CONET ist bereits seit über 30 Jahren am Markt. Wie groß muss man sich das Unternehmen vorstellen?*

Dirk Lieder: Zusammen mit der jüngsten Verstärkung unserer Unternehmensgruppe – der Münchner PROCON IT AG – erwarten wir mit mehr als 1.000 Mitarbeitern an 13 Standorten in Deutschland und Österreich einen Gesamtumsatz von rund 150 Millionen Euro. Über die vergangenen drei Jahrzehnte ist CONET stetig bewusst und erfolgreich gewachsen. Diesen Kurs wollen wir fortsetzen, uns dabei aber unseren Charakter als mittelständisch geprägtes Beratungshaus bewahren, denn diesen schätzen unsere Kunden neben unserer Fachkompetenz besonders.

Ulrich Parthier: *Sie bedienen vorrangig den gehobenen Mittelstand und das Behördenumfeld. Wo liegen ihre Themenfelder und Kernkompetenzen?*

Dirk Lieder: CONET ist als gewachsener Berater und Dienstleister im Bereich IT enorm breit aufgestellt. Unser Ziel ist es, bei unseren Kunden möglichst viele Aspekte moderner Arbeit und Technik aus einer Hand zu unterstützen. Insofern reichen unsere Kompetenzen von SAP Consulting, Management Consulting und Cyber Security über Cloud Computing und Managed Services, Data Intelligence, Digital Communications und E-Commerce bis hin zu Critical Communications und agilem Software Engineering. Dabei legen wir sowohl bei unseren Technologiepartnern als auch unseren Kunden Wert auf langfristige Beziehungen. Damit kennen wir in fast allen diesen Bereichen Entwicklungen, Trends, Prozesse und Arbeitsweisen seit Jahrzehnten und unsere Fachleute finden sich auch in komplex gewachsenen Architekturen schnell zurecht.

Ulrich Parthier: *Es gibt derzeit ja eine Reihe von Topthemen, die die Unternehmen bewegen. Auf welche dieser Themen treffen Sie immer wieder bei ihren Kundengesprächen.*

Dirk Lieder: Im Augenblick stehen Cyber Security und Künstliche Intelligenz vielerorts weit oben auf der Agenda. Ohne ersteres geht heute geschäftlich nichts mehr. Und letzteres bietet die vermeintlich größten Chancen für die Zukunft. Und zudem sind beide keine Nischenaspekte moderner IT, sondern betreffen nahezu alle Arbeitsschritte, Abläufe und Strukturen. Oft geht es dann auch gerade um das Zusammenwirken beider.

Ulrich Parthier: *Angesichts stetig wachsender IT-Sicherheitsrisiken, Angriffsvektoren und Angriffsmuster im Zeitalter der Digitalisierung, in Industrie 4.0 und dem Internet der Dinge (IoT) greifen traditionelle Technik und Methoden der IT-Sicherheit oftmals zu kurz. Wie gehen Sie das Thema Cyber Security bei ihren Kunden an?*

Dirk Lieder: In der Vergangenheit waren Sicherungsansätze und -maßnahmen meist vorrangig technisch ausgerichtet. Dies reicht heute aber nicht mehr aus, um angemessen geschützt zu sein, denn Cyber Security durchdringt alle Unternehmensbereiche. Technische Aspekte von Infrastruktur und Netzwerken bis zu Anwendungen und Datenhaltung sind dabei ebenso betroffen wie Geschäftsabläufe, physische Sicherheit von Firmengelände und Gebäuden bis hin zu den Mitarbeitern selbst. Angesichts dieser komplexen Anforderungen gewinnt ein strategischer Ansatz mit passenden Konzepten, Notfall-Strategien und Analysen zur Bestimmung des notwendigen Schutzbedarfs für Informationen, Maschinen und Menschen zunehmend an Bedeutung. Daher steht bei unseren Kundenkontakten zunächst die Bestandsaufnahme mit allen relevanten Bezugsgruppen im Vordergrund, um darauf aufbauend in gemeinsamen Workshops die strategische Marschrichtung festzulegen und besonders kritische Bereiche zu identifizieren, in denen der größte akute Handlungsbedarf besteht. Dabei darf wie schon beschrieben aber der Blick über den Tellerrand einzelner Lösungen nicht verloren gehen.

Ulrich Parthier: *Wie können wirkungsvolle Strategien und Lösungen für Cyber-Sicherheit und sichere Systeme aussehen?*

Dirk Lieder: Damit Cyber Security einen wirkungsvollen Schutz und angemessene Resilienz gegenüber Angriffen gewährleisten kann, muss sie neben der technischen Komponente ein Kernbestandteil aller Geschäftsprozesse und Organisationsstrukturen sein. Security-Überlegungen dürfen nicht erst nachträglich in neue IT-Lösungen einfließen, sondern müssen gemäß einer „Business-driven Security" schon bei der Konzeption neuer Geräte und Anwendungen von Beginn an berücksichtigt werden. Benötigt werden also die schon beschriebene übergreifende Cyber-Sicherheitsstrategie und eine inte-

grierte IT-Sicherheitsarchitektur, die sich im Sinne von „Security by Design" an festgelegten IT-Sicherheitsrichtlinien und Best Practices in Prozessgestaltung, Technologieauswahl und Anwendungsentwicklung orientiert.

Ulrich Parthier: *Welche Methoden und Werkzeuge steigern die Information Security?*

Dirk Lieder: Informationssicherheit umfasst eine Vielzahl von Teilaspekten in der Erfassung, Verarbeitung und Speicherung. Als Orientierung haben sich die Leitlinien der ISO-27000-Reihe und insbesondere in Deutschland der IT-Grundschutz des BSI weitgehend etabliert. Wie genau diese Standards aber für das eigene Geschäft und die eigenen Strukturen umzusetzen sind, ist eine sehr individuelle Fragestellung. Dabei spielen auch weitere Aspekte wie Business Continuity und IT Service Management mit hinein. Daher geht es auch hier nicht ohne eine wiederum langfristig angelegte Gesamtbetrachtung aller relevanten Prozesse und Architekturen, denn Cyber Security ist nie eine Einmalaktion, sondern ein kontinuierlicher Anpassungs- und Verbesserungsprozess.

> UNSER ZIEL IST ES, BEI UNSEREN KUNDEN MÖGLICHST VIELE ASPEKTE MODERNER ARBEIT UND TECHNIK AUS EINER HAND ZU UNTERSTÜTZEN.
>
> Dirk Lieder, Geschäftsführer, CONET Solutions GmbH, www.conet.de

Ulrich Parthier: *Ist Managed IT Security ein sinnvoller Ansatz, wenn das eigene Know-how und die eigenen Ressourcen der Kunden an ihre Grenzen stoßen?*

Dirk Lieder: Auf jeden Fall, denn die Anforderungen werden und sind teilweise bereits viel zu weitrechend und komplex, als dass man sie als einzelnes Unternehmen alleine stemmen könnte. Erst recht, da es angesichts des Fachkräftemangels nahezu unmöglich ist, entsprechend qualifizierte Fachleute zu finden – oder zu bezahlen. Zudem macht das schlichtweg auch keinen Sinn – auf der einen Seite sind die Herausforderungen so groß, dass sie sich nur mit enormem eigenen Aufwand und teurer Technologie bewältigen lassen würden. Auf der anderen Seite gibt es aber genauso viele Standardaufgaben, die unnötig eigene wertvolle Ressourcen binden und einfach auszulagern sind.

Ulrich Parthier: *KI hält ja in vielen IT-Bereichen Einzug. Das gilt auch für die IT-Sicherheit. Wird da nicht zu viel von einer Technologie erwartet und was halten Sie für realistische Einsatzszenarien?*

Dirk Lieder: Der Ruf nach Künstlicher Intelligenz und selbstlernenden Systemen, die IT-Sicherheitsverantwortliche bei der Identifikation von Sicherheitsbedrohungen und entsprechenden Reaktionen unterstützen und fehlende personelle Kapazitäten ergänzen oder sogar ersetzen sollen, liegt auf der Hand. Die Fähigkeiten der Künstlichen Intelligenz seien längst soweit, bei der Reaktion auf diese Herausforderungen weitgehend automatisiert zu helfen. Richtig ist: Ohne den Einsatz Künstlicher Intelligenz bleiben IT-Sicherheitsverantwortliche oftmals zum bloßen und oft verspäteten Reagieren verdammt, da sich gegebenenfalls gefährdende Vorgänge und die schiere Datenmenge im Netz ohne technische Unterstützung nicht sinnvoll beobachten und auswerten lassen. Eine so genannte

OHNE DEN EINSATZ KÜNSTLICHER INTELLIGENZ BLEIBEN IT-SICHERHEITSVERANTWORTLICHE OFTMALS ZUM BLOSSEN UND OFT VERSPÄTETEN REAGIEREN VERDAMMT, DA SICH GEGEBENENFALLS GEFÄHRDENDE VORGÄNGE UND DIE SCHIERE DATENMENGE IM NETZ OHNE TECHNISCHE UNTERSTÜTZUNG NICHT SINNVOLL BEOBACHTEN UND AUSWERTEN LASSEN.

Schwache Künstliche Intelligenz, die sich mit der Bearbeitung konkreter Anwendungsfälle auf Basis festgelegter Entscheidungsalgorithmen und Mustererkennung befasst, wird daher etwa in technischen Lösungen wie einem Security Information and Event Management (SIEM) eine zunehmend zentrale Rolle im Filtern und Aufbereiten von Informationen spielen. Einfache, auf klaren Erfahrungswerten basierende Entscheidungen kann die künstliche Intelligenz dem menschlichen Entscheider abnehmen und damit für schnellere Reaktionen sorgen. Kritische Entscheidungen kann und muss unserer Erfahrung nach aber immer noch ein Mensch als Analyst und Überwachungsinstanz mit Urteilsvermögen und Empathie treffen – insbesondere solange es in KI-gestützten Systemen keine lückenlose Dokumentation und damit Nachvollziehbarkeit dahingehend gibt, an welcher Stelle der Informationsverarbeitung und anhand welcher Kriterien die KI eine bestimmte Entscheidung getroffen hat.

Ulrich Parthier: *CONET hat ja ein eigenes SOC (Security Operations Center) eingerichtet. Was war ihr Ziel?*

Dirk Lieder: SOCs selber aufzubauen und zu unterhalten ist für Unternehmen und Organisationen der öffentlichen Hand extrem teuer und aufwändig. Daher gibt es SOC-Dienstleistungen als Service. Diese sind aber zum überwiegenden Teil auf Großkonzerne und deren Bedarf und Ressourcen ausgerichtet. Unser Ziel war, diese wertvollen Dienstleistungen auch maßgeschneidert für mittelständische Kunden zur Verfügung zu stellen – mit überschaubarem Aufwand, transparenter Abrechnung und genau den Services, die unsere Kunden aufgrund ihrer individuellen Schutzbedarfsanalyse tatsächlich benötigen.

Technisch basierend auf einem SIEM-System, bedient sich unser CONET SOC primär der besonders aussagefähigen Detektion und Bewertung von Events mittels der so genannten Netflow-Analyse, bei der statt der alleinigen Auswertung beispielsweise von Log-Dateien die Netzwerkaktivitäten fortlaufend auf Anomalien geprüft werden. Anhand dieser Überwachung sind unsere Fachleute in der Lage, früh Risiken und Sicherheitsvorfälle zu identifizieren und entsprechende Gegenmaßnahmen zu empfehlen oder selber einzuleiten. Die operativen Analyseprozesse wurden eigens von uns entwickelt und werden ständig den aktuellen Erfordernissen angepasst.

Ulrich Parthier: *Welche Services bieten Sie hier im Detail an?*

Dirk Lieder: Ganz akut identifizieren und klassifizieren wir im Security Incident Monitoring potenzielle Sicherheitsvorfälle und melden diese über individuelle Sofortnachricht in unserem Security Incident Response Service an unsere Klienten. Das schließt auch fortlaufende Statusmeldungen ein und wird im Customer Reporting durch regelmäßige Informationen über die Sicherheitslage und Sicherheitsberichte ergänzt. Zusammen mit unserer Threat & Impact Analysis, die eine detaillierte Bestandsaufnahme der IT-Infrastruktur und Erstellung einer Eskalationsmatrix umfasst, schaffen wir dabei auch die Basis für weitere Optimierungen von Technik und Maßnahmen auf der Kundenseite.

Ulrich Parthier: *In der IT Security ist immer mehr ein ganzheitlicher Ansatz gefragt. Welche Szenarien bilden Sie in ihrem Portfolio ab?*

Dirk Lieder: Neben unserem SOC spielt die Cyber-Security-Beratung wie beschrieben eine wesentliche Rolle. Aus ihr ergeben sich dann konkrete Ansatzpunkte für benötigte Prozessanpassungen oder Tools: Das reicht von Cloud Security und IT Governance bis hin zur Härtung von Infrastrukturen. Einen Schwerpunkt bilden auch weiterhin Lösungen zur Verwaltung von Berechtigungen und Zugängen wie Identity und Access Management oder der bewusste Umgang mit besonders berechtigten Anwendern im Privileged User Management.

Denn im Faktor Mensch schlummert vielfach trotz aller technischer Finessen auch ein wesentliches Risikopotenzial. Cyber-Angreifer erkennen und nutzen verstärkt die ‚Schwachstelle Mensch', indem sie über Social Engineering und Phishing gezielt User-Accounts anstelle von technischen Systemen ins Visier nehmen oder versuchen, über Fake-News-Kampagnen und Reputationsschädigungen die Führungs- und Entscheidungsfähigkeit zu beeinträchtigen. Mehr als 80 Prozent der Sicherheitsbedrohungen kommen so bereits von innen. Dieses Bedrohungspotenzial lässt sich aber mit einer Kombination aus Berechtigungsmanagement mit Identitäten, Zugriffsrechten und Nutzerrollen, mehrstufigen Authentifizierungsmechanismen und der Aufklärung der Anwender Zug um Zug entschärfen.

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

SERVICE-ORGANISATION

WIE SERVICE-AUTOMATISIERUNG IN KRISENZEITEN GELINGT

Beratungshotlines sind überlastet, ganze Unternehmen müssen von heute auf morgen aus dem Homeoffice produktiv arbeiten: Die Entwicklung rund um COVID-19 ist auch eine große Herausforderung für alle Service-Organisationen.

Neben dem klassischen Kundenservice ist vor allem der IT-Service mit mehr Aufgaben und Serviceanfragen konfrontiert. Denn über Nacht sollen alle Mitarbeiter aus dem Homeoffice arbeiten – und dafür gilt es VPN-Zugänge einzurichten, Laptops bereitzustellen und vieles mehr. Damit die Belegschaft rasch produktiv arbeiten kann, benötigt der IT-Service intelligente Tools zur Service-Automatisierung: Die Kombination aus Self-Service-Lösungen, Alerting-Systemen und Self-Healing-Lösungen ermöglicht es Anwendern, selbst nach Lösungen zu suchen und diese direkt vom System beheben zu lassen. Zahlreiche IT-Probleme lassen sich mit nur einem Klick automatisiert lösen, und die IT kann bei Störungen proaktiv die betroffenen Anwender informieren. Das führt zu deutlich weniger Tickets, schnelleren Ticketdurchlaufzeiten und einer höheren Produktivität im IT Service Desk.

Schnellere Problemlösung ist erfolgskritisch

Entscheidend für den Erfolg einer Self-Service Lösung ist die Akzeptanz der Anwender. In der Praxis haben sich neben einer leistungsstarken Suche in FAQs intelligente Chatbots bewährt. Besonders häufig binden Standardanfragen die Service Agenten, zum Beispiel zu den Themen Hardware (Drucker, Maus), Software (E-Mailprogramme, Internetbrowser, Downloads), Passwörtern oder die Abfrage des IT-Ticketstatus. Ein Chatbot spezifiziert durch passende Rückfragen das Problem immer weiter bis er das richtige Lösungsdokument ausgegeben kann. Sollte der Chatbot einmal doch nicht weiterwissen, bietet er die Möglichkeit, mit einem Service Agenten in Kontakt zu treten oder direkt ein Ticket zu eröffnen. In beiden Fällen werden die bereits vom Chatbot gesammelten Informationen übergeben, sodass der Anwender sein Problem nicht neu beschreiben muss.

Chatbots bekommen „Hände“

Bots für den IT Self-Service können aber noch viel mehr: Sie zeigen nicht nur die Lösung für ein IT Problem, sondern beheben es einfach selbst. Das funktioniert mit Hilfe einer Self-Healing Komponente, die direkt auf dem Native Client des Anwenders verschiedene Aktionen ausführt. Lediglich die Symptome des Problems werden dem Chatbot mitgeteilt, und nach der bestätigten Diagnose ist das Problem nach einem Klick Vergangenheit.

Im Standard bereits integrierte IT-Services sind beispielsweise das Wiederherstellen fehlender Netzlaufwerke, das Löschen des Browser Caches oder der Neustart des Computers – generell vieles rund um Konfigurationsprobleme. Aber auch individuelle Anwendungsfälle können im Self-Healing integriert werden. Damit wird der Bot zum hilfreichen und für die Anwender persönlichen Service-Kollegen, der viele der Alltagsprobleme automatisch aus dem Weg schafft.

Wenn jetzt auch noch ein IT Alerting proaktiv Anwender bei Störungen informiert und dadurch keine Tickets im IT Service auslöst, ist die Service-Automatisierung perfekt.

Mit den richtigen Lösungen die Krise bewältigen

Mit einer Kombination aus Self-Service, Ticketing, IT Alerting und Chatbot mit Self-Healing-Komponenten sind IT-Service-Teams auch in der derzeitigen Krisensituation gut gerüstet. Entsprechende Lösungen sind entweder als individuelle Module oder als Gesamtlösung rasch verfüg- und nutzbar. Gerade in der aktuellen Krise bieten sie Anwendern schnelle Selbsthilfe und dem IT-Service eine konkrete und nachhaltige Entlastung.

Sven Kolb

> MIT EINER KOMBINATION AUS SELF-SERVICE, TICKETING, IT ALERTING UND CHATBOT MIT SELF-HEALING-KOMPONENTEN SIND IT-SERVICE-TEAMS AUCH IN DER DERZEITIGEN KRISENSITUATION GUT GERÜSTET.
>
> Sven Kolb, Geschäftsführer USU GmbH, Geschäftsbereich unymira, www.unymira.com

CLOUD FIRST

LEADEC: PHASE 1 DES IT-CARVE-OUTS ERFOLGREICH ABGESCHLOSSEN

Leadec baut seine IT-Infrastruktur derzeit kräftig um und macht sich fit für die Zukunft. Der globale Industrie-Dienstleister steckt mitten im digitalen Wandel. Er modifiziert weltweit Geschäftsprozesse und verlagert Applikationen und Infrastruktur-Systeme konsequent in die Cloud. Mit Unterstützung von SPIRIT/21 wurde die erste Phase des IT-Umbaus Ende 2019 erfolgreich abgeschlossen: Innerhalb von sechs Monaten gelang es, alle zentral verwalteten Server-Systeme transparent und ohne „Impacts" in die AWS Cloud zu migrieren und in die Managed Services-Verantwortung des Böblinger IT-Unternehmens zu übergeben.

LEADEC SETZT AUF "CLOUD FIRST"

„Cloud First" zählt für viele Unternehmen längst nicht mehr zu den großen Unbekannten. Bei IT-Projekten wird oft zunächst die Realisierbarkeit einer Cloud-Lösung geprüft, bevor andere Alternativen in Betracht gezogen werden. Doch nur wenige Mutige setzen die Strategie auch tatsächlich um. Denn mit einer über die Jahre gewachsenen IT vollständig in die Cloud zu gehen, ist nach wie vor ein großer Schritt und stößt bei den beteiligten Funktionen nicht immer nur auf Begeisterung. Leadec hat den Sprung gewagt und setzt beim Umbau seiner IT-Organisation konsequent auf „Cloud First".

„Man muss das gesamte Bild betrachten, um zu verstehen, warum wir dieses Thema bei Leadec so radikal angehen", erklärt Domenico Manzo, Leiter Global IT Operations & Services. Als die Dienstleistungssparte VOITH Industrial Services vor rund vier Jahren aus der VOITH Gruppe

ABSCHIED VON DER ON-PREMISES-WELT

herausgelöst und unter dem Namen Leadec selbständig wurde, stand das neue Unternehmen erstmal ohne zentrale Infrastruktur da. Denn diese lag nach wie vor bei der VOITH Group und wurde dort verwaltet. „Die Applikationen wurden zwar in den lokalen Einheiten gemanaged, aber infrastrukturell gab es bei Leadec nichts. Es gab weder eine Abteilung noch Mitarbeiter. Die Infrastruktur-Organisation war schlichtweg nicht vorhanden", schildert Domenico Manzo die Situation als er im Juni 2017 bei Leadec einstieg.

Schnell war klar, dass der neue Infrastruktur-Chef die Verantwortung für die Trennung der zentralen IT vom ehemaligen Mutterkonzern übernehmen würde und damit auch die Aufgabe, diese neben dem Carve-Out neu aufzubauen. Drei Ziele standen für ihn von Anfang an fest: Der Aufbau musste schnell gehen, kostengünstig sein und der Betrieb für die weltweit 20.000 Mitarbeiterinnen und Mitarbeiter ohne Unterbrechung weiterlaufen. Außerdem sollten innerhalb der neuen Struktur IT-Prozesse hochgradig automatisiert und Skalierungen ebenso wie Modernisierungen einfach und schnell umgesetzt werden können. Und die Systeme, die weltweit an 240 Standorten genutzt werden, sollten sehr flexibel und von einer überschaubaren Anzahl an IT-Experten zentral gesteuert werden können. Deshalb kam für das IT-Management nur der Weg in die Cloud infrage.

Seit zwei Jahren läuft der IT-Umbau auf Hochtouren. An mehreren „Streams" wird parallel gearbeitet. 5.000 Rechner wurden zu Beginn des Projektes auf Windows 10 umgestellt, die Microsoft Office Suite mit Exchange und Teams auf Office 365 „umgeswitched" und alle zentralen Applikationen aus der On-Premises-Welt in die Cloud gebracht. Um möglichst flexibel und unabhängig von den eigenen IT-Ressourcen agieren zu können, arbeitet Leadec bei vielen Projekten mit Partnern zusammen. Ein wichtiger ist die SPIRIT/21 GmbH.

Der IT-Dienstleister ist seit Anfang 2019 mit an Bord. Mit Unterstützung seines Migrations- und Service Delivery-Teams gelang es, alle Windows und Linux Server-Systeme, die bis dato im VOITH-Rechenzentrum beheimatet waren, innerhalb von sechs Monaten in das Cloud Data Center von Leadec umzuziehen. Dabei ging es um zentrale Systeme wie Active Directory, Citrix, Microsoft Office sowie Data Ware House-, Back Office- und HR-Anwendungen, die hauptsächlich im „Lift-and-Shift"-Verfahren und über „Rebuild"-Migration in die Cloud verschoben wurden.

SPIRIT/21 CLOUD LAUNCH PLATTFORM ALS BASIS

Die größte Herausforderung lag für den IT-Dienstleister darin, in der Kürze der Zeit die Cloud Launch Plattform kundenspezifisch aufzubauen, diese zu testen und zu implementieren sowie sämtliche Migrationen während des laufenden Betriebs durchzuführen. „SPIRIT/21 hat uns bei Konzeption und Umsetzung sehr

stark und sehr gut unterstützt", bestätigt Domenico Manzo. „Obwohl die SPIRIT-Kollegen sehr unter Druck standen, haben sie es geschafft, die Migration ohne Ausfälle innerhalb des extrem sportlichen Zeitplans mit uns gemeinsam umzusetzen. Das war eine großartige Teamleistung. Die flexible und kollegiale Zusammenarbeit hat uns sehr dabei geholfen."

Im November und Dezember 2019 wurden jeweils freitags bestimmte Gruppen von Servern umgezogen. Das Migrationsteam bestand in der Regel aus zehn bis zwölf Personen - dem Infrastrukturteam und den jeweiligen Applikationsverantwortlichen von Leadec sowie den Transition- und Service Delivery-Teams von SPIRIT/21. Alle arbeiteten aus dem Homeoffice und hatten Wochenend-Rufbereitschaft.

„Aufgrund der komplexen Umgebungen waren die Wartungsfenster sehr großzügig geplant, so dass wir noch den Samstag und Sonntag für Nacharbeiten zur Verfügung hatten", erzählt Kevin Wildenau, Cloud Consultant Architect, SPIRIT/21 GmbH. „Je nachdem wie kritisch die Applikationen für den Geschäftsablauf waren, gab es das ganze Wochenende über immer wieder Checkpoints, bei denen wir dem Management telefonisch Rückmeldung zum aktuellen Status gegeben haben." Auch wenn nicht immer alles 100%ig nach Plan gelaufen sei, habe es das Team gemeinsam geschafft, alle Systeme innerhalb des Wartungsfensters erfolgreich zu migrieren. „Wir sind sehr stolz, dass wir sämtliche Systeme bei der ersten Migration umziehen konnten, ohne auf ein „Rollback-Szenario" zurückgreifen zu müssen."

MIT AUTOMATISIERUNG SCHNELLER ANS ZIEL

Um einzelne Arbeitsschritte und damit den Migrationsprozess insgesamt zu beschleunigen, nutzte SPIRIT/21 die AWS Standardsoftware CloudEndure und die Automatisierungswerkzeuge RedHat Ansible und CloudForms, die speziell auf den Einsatz bei Leadec zugeschnitten wurden. Dadurch konnten viele Prozesse während der Migration automatisiert werden. Dazu gehörten der Rollout von Servern, die Anpassung von Systemparametern oder die Deinstallation von Altsoftware. Aber auch Themen, die für den Betrieb von Bedeutung sind - Server Monitoring, Patch Management, Backup und

Security – wurden über Automationsroutinen bereits beim Set-Up berücksichtigt.

Für Automatisierungs-Evangelist Domenico Manzo war von Anfang an klar, dass dieses Projekt nur mit einem Partner umgesetzt werden konnte, der mit den Themen Automation und Konfigurationsmanagement bestens vertraut ist. „Dass SPIRIT/21 hier konsequent mit Open-Source Software arbeitet, war einer der Gründe, warum wir uns für diesen Dienstleister entschieden haben." Mit offener Software könne Leadec sehr flexibel agieren. Außerdem sei die Nutzung durch den Wegfall hoher Lizenzgebühren auch aus Kostengründen attraktiv, fasst der Infrastruktur-Chef die Vorteile zusammen.

Diese Punkte hatten nur wenige Dienstleister bei der Ausschreibung adressiert. So kam SPIRIT/21 zum Zug und wurde schließlich aufgrund der besseren Konditionen im Vergleich zu anderen Anbietern Anfang 2019 als Migrations- und Managed Services-Partner an Bord genommen.

AB IN DIE CLOUD – MIT AWS

Zu diesem Zeitpunkt war noch offen, mit wem es in die Public Cloud gehen sollte. „Für uns war es nicht wirklich wichtig, welchen Provider wir nehmen", stellt IT-Leiter Manzo fest. Aus seiner Sicht schenken sich die führenden Cloud-Anbieter nicht viel. „Alle bieten heute solide Cloud-Technologien." Das attraktivere Preis-/Leistungsverhältnis war ausschlaggebend, warum Amazon Web Services (AWS) bei diesem Projekt das Kopf-an-Kopf-Rennen gewann.

Mit dem Abschluss des physischen Carve-Outs hat Leadec eine weitere große Etappe seines IT-Umbaus erreicht. Und plangemäß zeigen sich die ersten positiven Effekte: Die zentrale IT kann mit Hilfe verschiedenster Automationsroutinen erheblich schneller agieren. So können einzelne Systeme heute über einige wenige Klicks und innerhalb von Minuten ausgeliefert werden. Damit hat sich für Leadec der Umstieg in die Cloud schon nach wenigen Wochen gelohnt.

In der zweiten Phase des Carve-Outs, in der weitere Server in die Cloud verschoben werden, liegt der Fokus nicht nur auf den technischen Aspekten. Hier rücken Themen wie „Change-Management" und Veränderungen im „Mindset" in den Vordergrund. Denn in der aktuellen Phase geht es nicht mehr um die zentral verwalteten Systeme, sondern um die Infrastruktur in den Regionen und das bringt neue Herausforderungen mit sich.

MODERNE IT-BASIS FÜR DEN DIGITALEN WANDEL

Die eingeschlagene Richtung ist klar. Leadec ist davon überzeugt, dass der digitale Wandel nur mit Hilfe modernster IT-Lösungen zu schaffen ist, die mittelfristig für alle Stakeholder Vorteile bieten – für den einzelnen Mitarbeiter, für Leadec als Unternehmen und insbesondere für seine Kunden.

„Wir bauen gerade das Fundament für die künftige Struktur unseres Unternehmens. Nur über den Weg in die Cloud können wir uns weiterentwickeln, schneller und besser werden und unseren Kunden die Services bieten, die sie künftig von uns erwarten", davon ist der Leiter der globalen IT überzeugt. „Neue Dienste, die auf der Cloud aufbauen und innovative Services in den Bereichen IoT, künstliche Intelligenz und Big Data ermöglichen, werden uns helfen, als Industrie-Dienstleiter weiterhin die Nummer 1 zu bleiben."

www.leadec-services.com

www.spirit21.com

ÜBER DAS PROJEKT

Migration von Windows und Linux Server-Systemen aus den lokalen Rechenzentren von Leadec Industrial Services in die AWS Cloud; Übergabe der Betriebsverantwortung an die SPIRIT/21 GmbH.

Migrationstrategie und -Technik

- 6 R-Migrationsstrategie mit Fokus auf „Lift and Shift", „Rebuild" und „Retire"
- AWS CloudEndure Standardsoftware Unterstützung
- RedHat Ansible und CloudForms Unterstützung

Betriebsübernahme durch SPIRIT/21

- Server Service: Monitoring, Patch Management, Backup, Security
- Cloud Service: Kosten-, Account-, Authentication-, Console- und Netzwerk-Management
- Application Service: Datenbank-Management, DHCP-Management, VPN Client-to-Site Service, Print Service, Wifi-Management

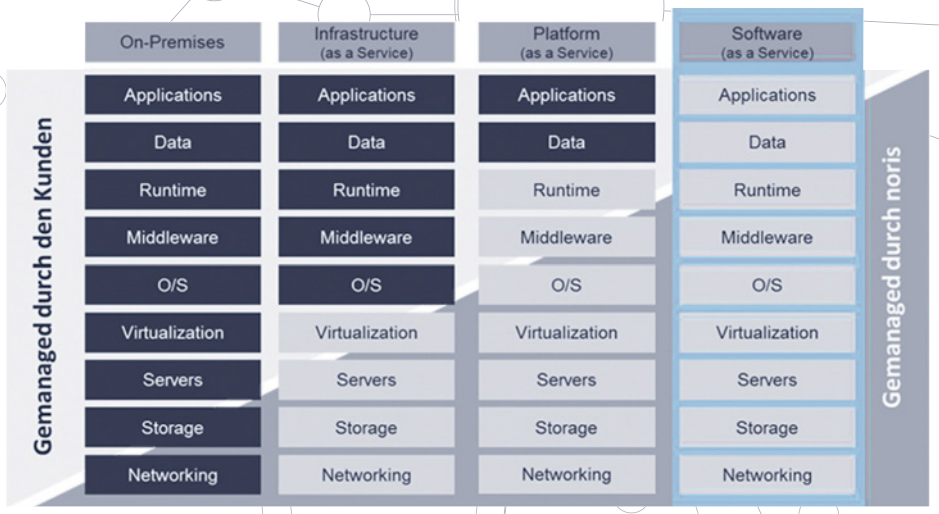
PaaS & DEVOPS

UNTERSTÜTZUNG FÜR AGILE ENTWICKLUNG UND MICROSERVICES

Alles aus einer Hand und maßgeschneiderte Unterstützung mit DevOps-Teams und Platform-as-a-Service-Angeboten „Made in Germany" mit einem Technologie-Stack aus Docker-, Kubernetes- und Continuous-Delivery-Technologien – so punktet Premium-IT-Dienstleister noris network im Wettbewerb mit den Hyperscalern AWS & Co.

„Wir wollen Unternehmen eine Lösung bieten, die sich auf den Migrationspfad Richtung Cloud begeben und eine sichere Umgebung für die agile Entwicklung und die hochskalierbare Bereitstellung von Microservices suchen", erläutert Stefan Keller, CMO bei der Nürnberger noris network AG. „Wir helfen auch dort, wo Cloud-Lösungen die performante Anbindung an Legacy-Lösungen brauchen, wo Entwicklerteams die Hilfe von erfahrenen DevOps bei Aufbau und Betrieb von Continuous Delivery Pipelines wünschen oder spezielle Sicherheitsbedürfnisse oder regulatorische Anforderungen bestehen. Das große Plus: Alles aus einer Hand – bis hin zur Anbindung spezieller Services der großen internationalen Anbieter."

Die Plattform für Cloud-Native-Anwendungen in Private, Hybrid und Public Clouds bietet noris network in seinen Hochsicherheitszentren in Nürnberg, München und Hof. Basierend auf Red Hat OpenShift und einem Managed-Kubernetes-Cluster können Entwicklerteams Microservices in Docker-Containern orchestrieren und skalieren – inklusive Repository-Management, Monitoring und andere für den Betrieb erforderlichen Funktionalitäten. Die gezielte Bereitstellung der unterschiedlichen Microservices auf der Applikationsplattform kann in Zusammenarbeit mit DevOps-Teams von noris network automatisiert werden – beispielsweise auf Basis von Lösungen wie Thoughtworks, Go oder Jenkins.



Verantwortung übernehmen

Anders als bei den großen Anbietern übernimmt noris network Verantwortung für die Gesamtlösung – auch dort, wo Legacy-Systeme Daten für die Cloud-Native-Anwendungen bereitstellen. IT-Verantwortliche und Entwickler finden hier kompetente Ansprechpartner, die bei Bedarf mit maßgeschneiderten Lösungen für Plattform und Betrieb helfen. Wo Unternehmen auf spezielle Microservices von Public-Cloud-Anbietern wie AWS, Microsoft oder Google zugreifen wollen oder müssen, stellt der Anbieter die performante Anbindung über einen leistungsstarken noris network Backbone bereit.

Wichtig für viele Unternehmen: Sämtliche Nodes befinden sich in noris network-eigenen, zertifizierten Hochsicherheitszentren in Deutschland. Das Servicemanagement verfügt über viele Jahre praktischer Audit-Erfahrung mit unterschiedlichen Organisationen und Behörden und unterstützt Unternehmen bei der Auditierung.

„Der Projekterfolg von Cloud-Native-Entwicklungen hängt nicht allein am Code. Unsere Expertenteams ergänzen Erfahrung und Kompetenzen für Plattform, Betrieb und für das komplette Lifecycle-Management und begleiten Unternehmen aktiv sowie beratend im Migrationsprozess. Das minimiert die Risiken und verbessert die Erfolgsquoten bei der Migration", so Stefan Keller.

www.noris.de

noris network

DIGITALE TRANSFORMATION

HIER LIEGEN DIE GRÖSSTEN HINDERNISSE

DA DIE DIGITALISIERUNG SOWOHL DIE INTERNE ALS AUCH DIE EXTERNE UNTERNEHMENSORGANISATION BEEINFLUSST, BILDET SIE EINE STRATEGISCHE AUFGABE FÜR DAS TOP-MANAGEMENT.

Sven Kreimendahl, Director Business Technology Services, Campana & Schott, www.campana-schott.com

Bereits die Hälfte der Unternehmen im deutschsprachigen Raum konnte ihre Marktposition verbessern, indem sie die Digitalisierung in ihre Strategie integriert haben. In Zukunft erwarten sogar knapp zwei Drittel eine Verbesserung ihrer Marktposition durch die digitale Transformation. Die hohe Komplexität der IT-Infrastruktur sowie der Datenschutz und Datensicherheit zählen für die Befragten zu den größten Hürden der digitalen Transformation. Diese Ergebnisse ermittelte der Future IT Report 2020 von Campana & Schott und der Universität Duisburg-Essen.

Da die Digitalisierung sowohl die interne als auch die externe Unternehmensorganisation beeinflusst, bildet sie eine strategische Aufgabe für das Top-Management. So gaben vier von fünf Befragten an, dass der CEO die verantwortliche, treibende Kraft für die digitale Transformation ist. Die Digitalisierung hat allerdings auch großen Einfluss auf Geschäftsmodelle. Wo zwei Drittel der befragten Unternehmen eine Förderung ihres bestehenden Modells sehen, ist jedes fünfte durch sie bedroht.

Die größten Hindernisse

Der Future IT Report zeigt deutlich, dass die digitale Transformation in deutschen Unternehmen schon heute zu grundlegenden Veränderungen in strategischer, organisatorischer, prozessualer und kultureller Hinsicht führt. Herausforderungen bilden dabei die Lücke zwischen gesetzten Zielen und greifbaren Ergebnissen sowie fehlendes Know-how und eine konträre Unternehmenskultur. Dies lässt sich jedoch durch eine strategische Ausrichtung am Markt, Kunden und Nutzen sowie Kooperationen und professionelles Change Management überwinden.

Zu den größten Hürden für die digitale Transformation zählen die Bereiche Datenschutz und IT-Sicherheit, komplexe IT-Infrastruktur, hohe Investitions- und Betriebskosten sowie Vernachlässigung der Digitalisierung im Bildungs- und Ausbildungssystem. Gerade dieser Punkt führt unter anderem dazu, dass entsprechende Fachkräfte fehlen. So ist in knapp der Hälfte der Unternehmen das benötigte Know-how nicht vorhanden. Zur Behebung des Fachkräftemangels setzen sie vorwiegend auf die Weiterbildung ihrer MitarbeiterInnen

KONKRETE HANDLUNGSEMPFEHLUNGEN

- Durch eine Standardisierung und das Outsourcing von Commoditiy Services in der IT-Infrastruktur, lässt sich die Komplexität reduzieren. Gleichzeitig ermöglicht dieser Schritt den Abbau von Altsystemen und steigert die Kosteneffizienz.
- Die Einführung eines Security Operating Centers (SOC) ermöglicht die Sicherstellung der hohen Anforderungen an Datenschutz und IT-Sicherheit bei wachsender Digitalisierung.
- Kooperationen mit Kunden zur Entwicklung von Innovationen und Durchführung von Digitalisierungsvorhaben fördert die bedarfsgerechte Erfüllung von Kundenbedürfnissen und erhöht Marktanteile sowie Umsatz.
- Aufbau intensiver Kooperationen mit Startups sowie Forschungs- und Entwicklungsnetzwerken zur Erhöhung der Innovationsfähigkeit und Entwicklung einer digitalen Unternehmenskultur.
- Erhöhung der Investitionen in die Weiterbildung der eigenen Mitarbeiter, um digitale Skills und Know-how aufzubauen. So wird dem Fachkräftemangel entgegen gewirkt und die Innovationsfähigkeit erhöht.
- Einführung eines flexiblen Innovationsbudgets für die Konzeption und Prüfung von Mitarbeiterideen, um Ideen schnell zu testen und umzusetzen.

Zur vollständigen Studie: www.campana-schott.com/future-it-report

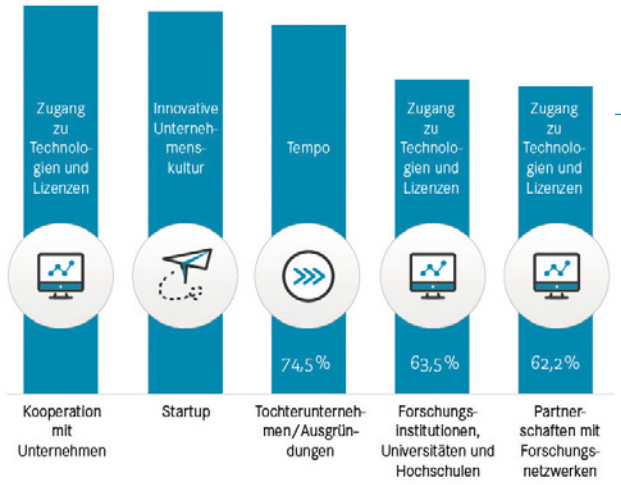


Bild 1: Die wichtigste Motivation zur Zusammenarbeit mit verschiedenen Partner-Typen

vor Neueinstellungen und Dienstleistern. Doch in der Praxis stellt nur die Hälfte der Unternehmen interne Angebote für die Weiterbildung bereit.

Zudem sind die MitarbeiterInnen in mehr als einem Drittel aller Unternehmen Veränderungen gegenüber skeptisch. Eine mögliche Ursache ist eine mangelhafte Fehlerkultur. Nur etwas über die Hälfte der Unternehmen geht mit Fehlern konstruktiv und positiv um. Häufig können MitarbeiterInnen weder eigenverantwortlich und initiativ handeln noch eigene Ideen einbringen. In fast jedem dritten Unternehmen gibt es keine offene, direkte und regelmäßige Kommunikation. Diese lässt sich durch eine Zusammenarbeit mit anderen Organisationen verbessern. So können insbesondere Kooperationen mit Startups eine frische und innovative Unternehmenskultur etablieren.

Der Kunde im Mittelpunkt

Durch die digitale Transformation stellen Kunden immer höhere Erwartungen an Produkte, Dienstleistungen und Prozesse der Unternehmen. Dies gilt vor allem in Bezug auf deren Verfügbarkeit, Geschwindigkeit und Zuverlässigkeit. Doch weniger als die Hälfte der Unternehmen konnte im Zuge der Digitalisierung bereits erfolgreich die Kundenzufriedenheit erhöhen. Dies gelingt zum Beispiel über eine stärkere Einbindung von Kundinnen und Kunden in Prozesse, etwa im Rahmen von Innovationsprojekten.

Entsprechend bildet höhere Kundenzufriedenheit eines der wichtigsten Ziele der Digitalisierung – neben gesteigerter Effizienz durch die Automatisierung von Prozessen und verbesserter Qualität. Darüber hinaus sind auch Zeitersparnis sowie die Entwicklung neuer oder verbesserter digitaler Produkte und Dienstleistungen wichtig. Jedoch wurden bislang die meisten Ziele noch nicht erreicht.

Sven Kreimendahl

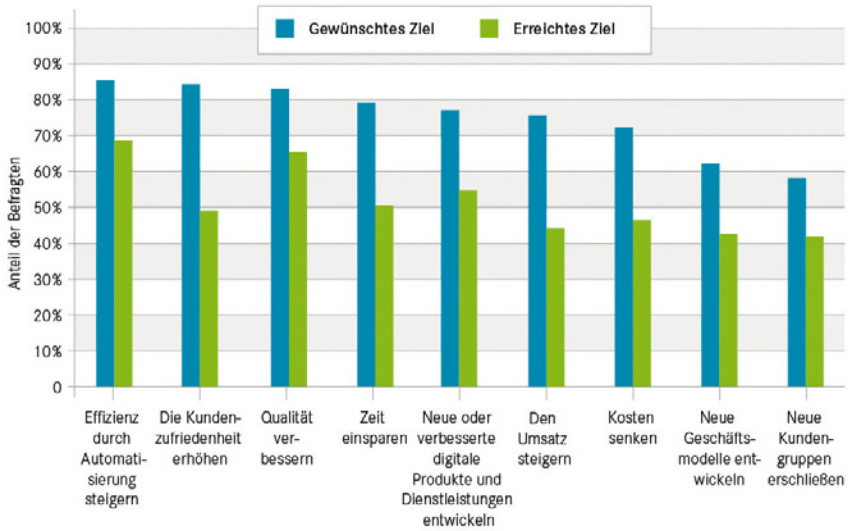


Bild 2: Vergleich der gewünschten und bereits erreichten Ziele der Initiativen zur digitalen Transformation

DATENSCHUTZ IN DER

VERTRAUEN IST GUT, WISSEN IST BESSER

Vertrauen in eine Cloud darf nicht allein auf der Reputation eines Anbieters und seiner Kunden basieren, sondern muss systemisch begründet sein. Nur wenn ein System sowohl technisch wie auch organisatorisch so angelegt ist, dass es die Schutzziele des Datenschutzes erfüllt, kann ihm vertraut werden.

Dazu zählen insbesondere die drei Schutzziele der Vertraulichkeit, der Integrität und Verfügbarkeit. Dies sind drei zentrale IT-Sicherheits-Schutzziele, an denen jeder Cloud-Anbieter im Wettbewerb gemessen wird. Wer diese erste Hürde in der Auswahl genommen hat, muss auch bei den vier datenschutzspezifischen Schutzzielen der Transparenz, Intervenierbarkeit, Nicht-Verkettbarkeit und der Datensparsamkeit zeigen, wie es mit Blick auf Verfahrensabläufe um die Leistungsfähigkeit bestellt ist.

1. Schutzziel Transparenz

Nutzt der Anwender ein Software-as-a-Service-Angebot, muss er sich auf die Infrastruktur, die Plattform und die Anwendungssoftware des Anbieters verlassen. Er muss prüfen können, ob der Anbieter hinreichende Maßnahmen in Bezug auf alle Schutzziele hat. Transparenz ist dann gegeben, wenn die Datenverarbeitung des Anbieters anhand von Systemdokumentation und Protokollen nachvollzogen, geprüft und bewertet werden kann. Dabei geht es etwa um die Frage, wer auf die Daten zugreifen kann und welche technischen und organisatorischen Sicherheitsmechanismen greifen. Bestandteil einer einfachen Prüfbarkeit ist auch der Nachweis der Revisionsfähigkeit.

2. Schutzziel Intervenierbarkeit

Der Anwender muss wissen, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. So kann er festlegen, welche Daten lokal gespeichert und welche in die Cloud übermittelt werden. Er muss außerdem kontrollieren können, wer von wo auf was wie zugreifen darf. Außerdem sollte der Anwender vertraglich regeln, dass der Anbieter ihn über Sicherheitsvorfälle informiert, die seine Anwendung betreffen.

3. Schutzziel Vertraulichkeit

Vertraulichkeit ist gegeben, wenn nur Befugte personenbezogene Daten sehen und nutzen können. Eine Lösung kann bloß dann wirklich „Vertraulichkeit" herstellen, wenn der Anbieter gewährleistet, dass ständig kontrolliert wird, ob nur Befugte personenbezogene Daten verarbeiten können. So sollte etwa ein Administrator des Anbieters nicht befugt sein, auf Inhaltsdaten Zugriff zu nehmen. Ein weiteres Kriterium besteht darin, dass Datenbestände separiert und verschlüsselt gespeichert werden. Außerdem muss die Datenübertragung verschlüsselt erfolgen. Zudem gilt es zu klären, wer auf die Krypto-Schlüssel zugreifen kann.

GRUNDSÄTZLICH SOLLTEN UNTERNEHMEN IMMER WISSEN, WELCHE ANWENDER ODER WELCHE CLOUD-DIENSTE IM UNTERNEHMEN PERSONENBEZOGENE DATEN VERARBEITEN.

Michael Jacob, Senior Pre-Sales Consultant, Brainloop AG, www.brainloop.com/de-de

4. Schutzziel Integrität

Aus Datenschutzperspektive ist ein System dann integer, wenn personenbezogene Daten während der Datenverarbeitung unversehrt, vollständig und aktuell bleiben. Die Authentizität ist ein Aspekt der Integrität, die darauf zielt, dass der Ursprung der Daten festgestellt werden kann. Ein Hilfsmittel bezogen auf Dokumente sind beispielsweise digitale Wasserzeichen oder ein „Information Rights Management". Die „Integrität" eines Systems lässt sich nur dann einschätzen, wenn der Anbieter eine permanente Kontrolle gewährleisten kann, Datenbestände, Schnittstellen und Prozesse zu sichern. Personenbezogene und -beziehbare Daten dürfen nur exakt so verarbeitet werden, wie es der Anbieter gewährleistet. Es kommt also auf die Zweckbindung an.

5. Schutzziel Verfügbarkeit

Die außerordentlich hohe und endgeräteunabhängige Verfügbarkeit von Daten ist eines der Hauptmotive für Anwender, Cloud-Lösungen zu nutzen. Sie müssen deshalb darauf achten, ob der Anbieter in den relevanten vertraglichen Vereinbarungen auch eine zeitgerechte Verfügbarkeit des Dienstes vorhält. Dies kann in Form von Service Level Agreements erfolgen.

6. Schutzziel Nichtverkettbarkeit

Die Nichtverkettbarkeit ist schließlich das klassische Schutzziel des Datenschutzes,

CLOUD

das verhindern soll, dass personenbeziehbare Verkettungen von Dritten vorgenommen werden können. Dabei geht es speziell um die Nutzung von Adress- und Profildaten. So stellen sich folgende Fragen: Ist die Cloud-Lösung etwa mit weiteren Diensten des Anbieters verknüpft, sodass er über die Zusammenführung verschiedener Nutzungsdaten ein Personenprofil erstellen kann? Und wer kontrolliert die Verknüpfbarkeit oder eben die Nichtverkettbarkeit der personenbezogenen Nutzungsdaten? Das Schutzziel der Nichtverkettbarkeit kann sich auch auf das Identitätsmanagement beziehen: Erlaubt der Anbieter anonyme Nutzung oder die Verwendung von Pseudonymen? Reicht es, wenn der Nutzer etwa nur die Attribute angibt, die zur Authentifizierung absolut notwendig sind?

7. Schutzziel Datensparsamkeit

Der Grundsatz der Datensparsamkeit wird verwirklicht, wenn nicht mehr personenbezogene Daten erhoben, verarbeitet und genutzt werden, als unbedingt erforderlich ist. Das gilt für die Daten, die innerhalb der Anwendung verarbeitet wie auch für die Protokolldaten, die erzeugt werden. Deshalb müssen die Anwendungen auch ein Löschprozedere anbieten. Beim Löschen geht es darum, wie schnell und durchgreifend Benutzer ihre Daten auf der Ebene der Plattform löschen können. Zu den einschlägigen Cloud-Risiken gehört es, dass eventuell an unterschiedlichen Verarbeitungsorten Datensicherungen vorgenommen werden.

Fazit

Die 2014 von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder veröffentlichte „Orientierungshilfe Cloud Computing" richtet sich nach diesen sieben Schutzzielen. Grundsätzlich sollten Unternehmen immer wissen, welche Anwender oder welche Cloud-Dienste im Unternehmen personenbezogene Daten verarbeiten. Hierfür sollten sie erfassen, welche Cloud-Dienste unternehmensintern sowie in Beziehung zu Kunden und Lieferanten genutzt werden. In einem nächsten Schritt müssen sie evaluieren, inwieweit die genutzten Cloud-Dienste, mit denen personenbezogene Daten verarbeitet werden, die Datenschutz-Vorgaben erfüllen.

Michael Jacob

KNOWLEDGEMANAGEMENT

WISSEN FÜR EINEN OPTIMALEN SERVICEDESK

Hat Ihr Service Desk mit vielen einfachen, wiederkehrenden Anfragen zu tun? Neigen Ihre Mitarbeiter dazu, zu viele Anfragen an den 2nd-Level-Support weiterzuleiten? Fragen Sie sich, wie Sie diesen Prozess effektiver gestalten könnten? Die Antwort hierfür ist Knowledge Management.

Mithilfe dieses eBooks können Sie lernen, wie Knowledge Management Ihrem Unternehmen helfen kann. Lesen Sie, was Knowledge Management im Zusammenhang mit einem Knowledge Centered Service (KCS) bedeutet und warum Sie in Knowledge Management investieren sollten.

Das eBook enthält zudem eine Musterkalkulation, anhand der Sie berechnen können, wie viel Zeit Ihr Unternehmen durch den Einsatz von Knowledge Management sparen könnte.

WHITEPAPER DOWNLOAD

Das eBook umfasst 32 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/Download

PLANUNGSSICHERHEIT

AUTOMATISIERTE GESCHÄFTSPROZESSE

Der niedersächsische Maschinen- und Anlagenbauer Thiel liefert Fördertechnik für die Futter- und Lebensmittelindustrie. Den Großteil seiner Produkte legt der inhabergeführte Familienbetrieb kundenspezifisch aus. Darüber hinaus fertigt das Unternehmen Lagersilos sowie Komponenten für die Stalleinrichtung in Serie. Insgesamt beläuft sich der Output auf 5.000 bis 6.000 Aufträge pro Jahr. Um ein ausreichendes Maß an Transparenz und Planungssicherheit zu gewinnen, hat Thiel das Auftragsmanagementsystem ams.erp eingeführt. Die integrierte Business-Software führt alle kaufmännischen und technischen Informationen zusammen, die im Rahmen der Kundenprojekte entstehen. Um die Auftragsdaten auch auf Maschinenebene nutzen zu können, hat Thiel die Laserschneiden und Stanzen sowie das automatische Regallagersystem an die Lösung angebunden.

Nach einer sechsmonatigen Einführungsphase ging ams.erp im November 2016 live. Bereits in den Anfangstagen ergaben sich konkrete Mehrwerte. Geschäftsführer Michael Thiel erinnert sich: „Durch die neue Bestandsführung konnten wir unser Einkaufsvolumen in den ersten Monaten um rund fünf Prozent reduzieren. Zudem sorgte die integrierte Auftragsplanung dafür, dass sich die Produktionskapazitäten in kürzester Zeit deutlich erweitert haben."

Der Fördertechnikspezialist nutzte den Schwung des Systemwechsels und begann sofort mit dem Ausbau der neuen Business-Lösung. Dabei konzentrierte sich das Unternehmen zunächst auf das Dokumentenmanagement (DMS) und das Produktdatenmanagement (PDM), für die ams.erp die integrierte Gesamtlösung ams.dms / ams.pdm bietet.

Grundlegend hat sich Thiel Fördertechnik entschlossen, sämtliche Dokumente nur noch elektronisch vorzuhalten. Ganz gleich, ob es sich dabei um die Korrespondenz mit den Kunden und Zulieferern, die technische Auftragsdokumentation oder um Unterlagen handelt, die während der Nutzungsphase der ausgelieferten Produkte entstehen. Lediglich im Einkauf gibt es noch einen Ordner mit den Eingangsrechnungen. Alle übrigen Dokumente werden über die Benutzeroberfläche der Software im integrierten DMS abgelegt.

Zeitgleich mit dem Dokumentenmanagement hat Thiel auch ams.pdm in Betrieb genommen. Das ebenfalls integrierte Produktdatenmanagementsystem automatisiert den Datenaustausch mit der Konstruktion, die in Thiels Fall mit dem CAD-System Inventor arbeitet. Die dort erstellten Zeichnungen werden direkt im System gespeichert und verwaltet. Zudem werden im PDM auch die mit den Zeichnungen korrespondierenden Stücklisten angelegt und automatisch an das Auftragsmanagement übermittelt. Um den Anforderungen der konstruktionsbegleitenden Fertigung gerecht zu werden, unterstützt ams.pdm die versionssichere Verarbeitung von Auftragsstücklisten: Jede Konstruktionsänderung führt automatisch zu einer Aktualisierung der davon betroffenen Auftragsstückliste. Auf diese

Südansicht der Hallen.
Quelle: www.foerdertechnik-thiel.de

Weise erkennen alle Projektbeteiligten, inwiefern der laufende Konstruktionsfortschritt neue Bedarfe in der Disposition, dem Einkauf und der Fertigung auslöst.

Gemeinsame Datenbasis

Somit stellt das Unternehmen sicher, dass Konstruktion und Auftragssteuerung auf einer gemeinsamen Datenbasis arbeiten. „Für uns ist dies ein großer Entwicklungsschritt", hält Michael Thiel fest und erläutert: „Über das Zusammenspiel von ERP und PDM entsteht eine geschlossene Informationskette, so dass alle Verantwortlichen auch nach Jahren noch wissen, was tatsächlich verbaut wurde." Ohne eine solche Integration sei eine solche Transparenz nicht zu haben. Schon allein deshalb nicht, da sich die Kollegen in der Produktion aus pragmatischen Gründen oftmals für ein Vorgehen entschieden, das mit der zugrundeliegenden Zeichnung nur teilweise übereinstimmt. „Erst wenn die entsprechende Änderungen lückenlos zurückgespiegelt werden, können wir jederzeit präzise nachvollziehen, wie wir das Produkt an den Kunden ausgeliefert haben", hebt Michael Thiel hervor.

Zusätzlich zum elektronischen Datenaustausch zwischen Produktion und Konstruktion setzt das Unternehmen auch unmittelbar innerhalb der Fertigungsorganisation auf Prozessautomatisierung. Herzstück ist eine bidirektionale Schnittstelle zwischen dem Auftragsmanagement und der NC-Programmierung der Laserschneide- und Stanzmaschinen. Um den aktuellen Arbeitsvorrat unterbrechungsfrei an die eingesetzten Produktionsanlagen zu senden, übermittelt ams.erp die Baugruppenstruktur an die jeweils zuständigen Schachtelprogramme. Bei der eigentlichen Verschachtelung nutzt Thiel auch weiterhin das Know-how seiner Mitarbeiter. Steht der Schachtelplan, wird die Spezifikation des erforderlichen Materials automatisch hinterlegt und an die Materialwirtschaft übermittelt. Sobald das Programm dann abgearbeitet ist, meldet die Maschine die Zeiten und den Verschnitt an das Auftragsmanagement zurück. „Der Nutzen der NC-Integration ist enorm", erklärt Michael Thiel. „Vor der Automatisierung haben wir die Laser zweischichtig betrieben. Inzwischen konnten wir auf Einschichtbetrieb wechseln und damit eine komplette Schicht einsparen."

Neues Wissen zur Unternehmenssteuerung

Seit der Inbetriebnahme von ams.erp hat Thiel Fördertechnik 12.000 Aufträge über das integrierte Informationssystem abgewickelt. Mit jedem Auftrag wächst das Wissen darüber, wie wirtschaftlich die unterschiedlichen Bereiche im Unternehmen arbeiten. Gleichzeitig erhält das Management belastbare Informationen dazu, wie hoch der Kostendeckungsgrad der unterschiedlichen Produkte ist. „Der Informationsgewinn in der Nachkalkulation hat dazu geführt, dass wir uns von einigen Produkten getrennt haben", sagt Michael Thiel. Darunter waren Komponenten, bei denen niemand daran gezweifelt hätte, dass man gegenüber der internationalen Konkurrenz preislich würde mithalten können. Die Überprüfung in der Controlling-Anwendung der ERP-Software ergab jedoch ein völlig anderes Bild.

„Mit Informationen wie diesen bekommen wir eine tragfähige Planungsgrundlage für die Zukunft unseres Unternehmens", resümiert der Geschäftsführer. Neben analytischen Themen wie der Nachkalkulation interessiert sich das Management auch für prognostische Auswertungen, wie zum Beispiel den Auftrags-Forecast oder die Berichte zur Kapazitätsentwicklung. „Das Anwendungsspektrum des Controllings reicht von kurzfristigen Make-or-Buy-Entscheidungen bis zu langfristigen Investitionsüberlegungen", erläutert Michael Thiel. „Hierdurch erschließen wir uns das Wissen, um die Unternehmensentwicklung vorausschauend zu steuern und unsere bisherige Wachstumsgeschichte erfolgreich fortzuschreiben.

www.ams-erp.com

FLEISSIGES BIENCHEN

VOM AUSSTERBEN BEDROHTE SPEZIES

Die digitale Transformation verändert viel – auch die traditionellen Prozesse im Finanz- und Rechnungswesen. Da, wo der Abgleich von Excel-Listen bisher zum festen Bestandteil der Jobbeschreibung zählte, hat sich viel getan. Moderne, weitestgehend automatisierte Workflows halten Einzug und prägen das neue Bild. Aufgaben, Anforderungsprofile und Verantwortlichkeiten ändern sich und damit nicht zuletzt das Image einer ganzen Finanzbranche.

Basis dieses grundlegenden Wandels ist eine IT, deren Lösungen sich zunehmend smarter in die Prozesse von Unternehmen und Abteilungen integrieren. Innovative Technologien sorgen dafür, dass die Arbeiten, die man landläufig als „Fleißarbeit" bezeichnet, durch automatisierte Workflows ersetzt werden. Das entlastet die Mitarbeiter und schafft Freiraum für andere, anspruchsvollere Tätigkeiten, so auch im Finanzwesen. Hier sorgt die Automatisierung zudem für mehr Transparenz und validere Ergebnisse – Mehrwerte, die gerade im Finanzwesen von großer Bedeutung sind.

Ein Praxisbeispiel, das jedes Unternehmen kennt und an dem sich Automatisierungseffekte eindrucksvoll aufzeigen lassen, ist der Monatsabschluss. Die manuellen Tätigkeiten zum Monatsende sind eine enorme zeitliche Belastung für die Mitarbeiter in der Buchhaltung: Sie sehen sprichwörtlich „den Wald vor lauter Bäumen" nicht mehr, wenn sie Massen von Buchungen manuell durcharbeiten müssen, um die Konten auf Vollständigkeit und Korrektheit zu überprüfen. Nicht nur, dass dieser Prozess mühsam ist, er birgt auch zahlreiche Fehlerrisiken, wie nicht zuletzt eine im Jahr 2018 von Censuswide international durchgeführte Studie zeigt. Demnach gaben etwa zwei Drittel (65 Prozent) der Befragten Finanzverantwortlichen an, dass sie schon einmal in einem Unternehmen gearbeitet haben, das seine Gewinne aufgrund nicht rechtzeitig erkannter Fehler, noch einmal anpassen musste. Umso wichtiger ist es, Fehlerpotenziale zu ermitteln und eliminieren. Immerhin scheinen die Ursachen der Fehler bekannt zu sein. Laut Studie geben 41 Prozent menschliches Versagen, 40 Prozent vielfältige Datenquellen, 28 Prozent einen Mangel an automatisierten Kontrollen sowie schwerfälligen Technologien (28 Prozent) an.

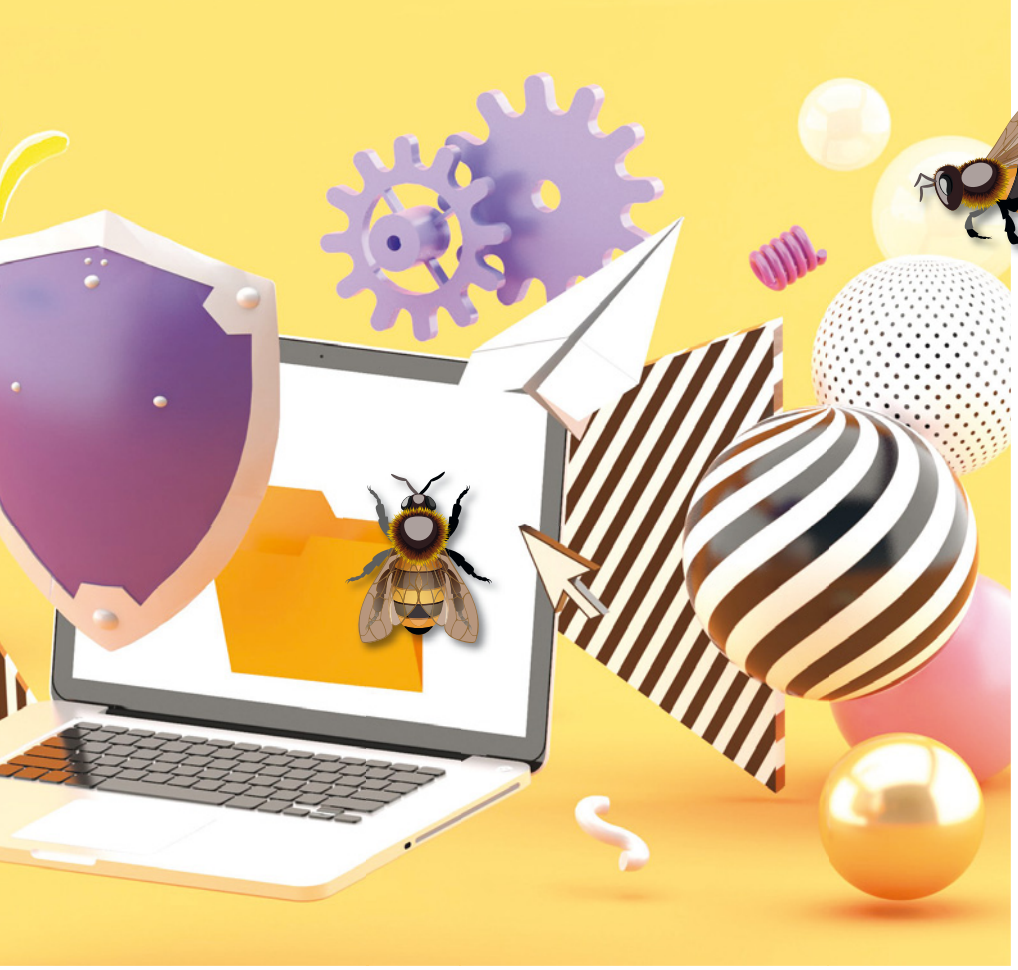
Continuous Accounting

Diesem Problem können moderne Automatisierungslösungen entgegenwirken. Sie sorgen dafür, dass die Daten aus den ERP-Systemen der Unternehmen so aufbereitet werden, dass sie automatisch von den Accounting-Systemen übernommen und weiterverarbeitet werden können - wie ein Katalysator sitzen die Automatisierungslösungen zwischen beiden Systemen. Da wo das fleißige Bienchen früher mühsam Excel-Listen gegenüberstellen musste, wird jetzt die Automatisierungslösung aktiv und macht den zeitaufwendigen manuellen Abstimmungsprozess obsolet. So werden die Daten konsistent und der gesamte Workflow transparent und nachvollziehbar.

Positiver Nebeneffekt derartiger Automatisierungslösungen ist, dass Aufgaben, die sich üblicherweise zum Monatsende kumulieren, auf die gesamte Bilanzierungsperiode verteilt werden. Dieses Prinzip bezeichnet man als Continuous Accounting: Es sorgt dafür, dass sich der Abschlussprozess nicht mehr nur über ein paar Tage am Monats-, Quartals- oder Geschäftsjahresende erstreckt, sondern die einzelnen Aufgaben durch Automatisierung sukzessive erledigt werden. Das Resultat: Weniger Aufwand, weniger Stress, ein deutlich geringeres Fehlerrisiko und damit validere Zahlen.

Machine Learning: Wie die Ausnahme zur Regel wird

Bei der Automatisierung des Monatsabschlusses spielt das „Exception Driven Concept" eine wichtige Rolle. Dieses besagt, dass Standardaufgaben in der Finanzabteilung weitestgehend automatisiert werden und manueller Handlungsbedarf nur dann besteht, wenn es Ausnahmen oder besondere Fälle zu bewältigen gilt. Betrachtet man vor diesem Hintergrund die Kontenabstimmung, werden die Vorteile schnell deutlich: Weil moderne Automatisierungslösungen den Kontenabgleich auf Basis von Algorithmen automatisch durchführen, muss der Buchhalter zum Schluss nur noch die Transaktionen klären, die das System nicht selbstständig bewältigen kann. Die Automatisierungslösung von BlackLine beispielsweise verfügt über ein solches Machine-Learning-Prinzip. Mit jeder Ausnahme, die manuell geklärt und zugeordnet wird, lernt das System dazu – sprich der Algorithmus wird mit jedem manuel-



len Kontenabgleich zunehmend intelligenter, so dass die Anzahl der händischen Zuordnungen schließlich gen Null gehen. So nimmt der Automatisierungsgrad des Monatsabschlusses kontinuierlich zu und das Risiko menschlicher Fehler ab.

Mit derartigen, auf innovativen Technologien basierenden Lösungen lassen sich auch komplexe Bilanzen validieren, denn dem System ist es egal ob es einen oder Millionen Abgleiche vornehmen soll. Der Algorithmus macht es möglich, dass das, was bisher von vielen Mitarbeitern in Fleißarbeit überprüft wurde, jetzt mit Millionen von Transaktionen innerhalb von nur wenigen Sekunden machbar ist.

Ungeahnte Perspektiven durch Echtzeitzahlen

Die neue Technologie löst beim einen oder anderen Mitarbeiter im Finanzwesen durchaus Ängste aus, zukünftig nicht mehr gebraucht zu werden. Aber das Gegenteil ist der Fall. Das Bureau of Labor Statistics prognostiziert beispielsweise, dass die Nachfrage nach Buchhaltern bis 2026 um 10 Prozent steigen wird. Das ist schneller als die durchschnittliche Wachstumsrate in anderen Berufen. Gleichzeitig nimmt das Angebot an qualifizierten Buchhaltern ab. Umso wichtiger ist es, dem bestehenden Expertenstamm in der Buchhaltung neue Perspektiven zu bieten – beispielweise, dass sie zukünftig stärker eine beratende Position einnehmen werden.

Wie muss man sich das vorstellen? Dadurch, dass die Buchhaltung auf Continuous Accounting setzt und jetzt einen bisher nicht dagewesenen Überblick über die Unternehmenssituation hat, kann sie die Geschäftsführung früher, umfassender und zuverlässiger als bisher über Chancen, Risiken oder andere Veränderungen informieren und vor allem auch zu beraten. Dank der Tatsache, dass bei Bedarf ein Monatsabschluss simuliert werden kann, ist die Finanzabteilung zu einem früheren Zeitpunkt im Monat in der Lage, valide Aussagen treffen und belastbare Auswertungen anbieten zu können. Diese Analysen kann sie dem CFO zur Verfügung stellen, so dass auch dieser erstmals in der Lage ist, noch während des Closing-Prozesses seinen Kollegen in der Geschäftsführung Detailfragen zu beantworten. Der zentrale, weitestgehend automatisierte und vor allem durchgängige Prozess bildet die Grundlage für dieses moderne Accounting, in dem jederzeit präzise Zahlen zur Verfügung stehen und im Bedarfsfall das Business nachjustiert werden kann – unabhängig von der Größe und Komplexität des Unternehmens.

Blick in die Zukunft: Predictive Accounting

Von all diesen Vorteilen können Unternehmen heute schon profitieren, wenn sie Prozesse digitalisieren und automatisieren. Experten allerdings sind schon einen Schritt weiter. Sie beschäftigen sich mit Predictive Accounting, also einem Accounting, das bereits im Vorfeld in der Lage ist, den angenommenen Monatsabschluss zu prognostizieren. Was im ersten Moment wie ein Blick in die Glaskugel anmutet, ist durchaus nicht abwegig. Wenn Unternehmen in der Lage sind, den überwiegenden Teil ihres Monatsabschlusses bereits Wochen im Voraus zu erledigen, so dass nur noch ein geringer Prozentsatz der Buchungen vakant ist, rückt die Idee einer zuverlässigen Vorhersage in greifbare Nähe – vorausgesetzt, man räumt der Digitalisierung Priorität ein und vertraut Algorithmen-getriebenen Automatisierungslösungen.

Ralph Weiss

BESONDERS IM FINANZWESEN SORGT DIE AUTOMATISIERUNG FÜR MEHR TRANSPARENZ UND VALIDERE ERGEBNISSE – MEHRWERTE, DIE GERADE HIER VON GROSSER BEDEUTUNG SIND.

Ralph Weiss,
Geo VP DACH, BlackLine,
www.blackline.com/de

BESSERE SERVICEQUALITÄT

IN FÜNF SCHRITTEN ZUR WISSENSDATENBANK

Die Servicequalität zu verbessern, ist ein erstrebenswertes Ziel. Die tägliche Arbeitslast verhindert aber oft dem gerecht werden zu können. Die wenigsten haben Zeit sich Gedanken über eine gut strukturierte Wissensdatenbank zu machen. Oft wird diese sehr stiefmütterlich behandelt. Unsere brasilianische Niederlassung hat mit Erschrecken festgestellt, dass 85 Prozent aller Unternehmen, die ein Servicemanagement-Tool einsetzen, entweder gar keine Wissensdatenbank haben oder diese nicht voll ausreizen.

Wir leben in einer Zeit, in der Suchmaschinen die meisten alltäglichen Fragen beantworten. Demzufolge haben die Konzepte Knowledgemanagement und Shift-Left viel an Dynamik gewonnen. Der Shift-Left-Ansatz bezeichnet die Verlagerung des Wissens „nach links", also näher an den Melder (Mitarbeiter oder Kunde). Das bedeutet, dass Sie Meldern ohne jegliches Vorwissen, Informationen zur selbstständigen Problemlösung zur Verfügung stellen können. Der Servicedesk hat so mehr Zeit komplexere Aufgaben zu erledigen. Um das umzusetzen, sollten Sie sich drei Schritte merken:

- **Veröffentlichen:** Wissen, das nur in Dokumentenform oder im Kopf von Mitarbeitern existiert, wirkt sich negativ auf die Effizienz der Betreuung Ihrer Melder aus.
- **Teilen:** Ihr Serviceteam sollte Informationen, sofern möglich, immer teilen – auch mit den Meldern.
- **Überprüfen:** Es bringt nichts, ein hilfreiches Dokument öffentlich zu teilen, wenn die darin enthaltenen Informationen bereits veraltet sind.

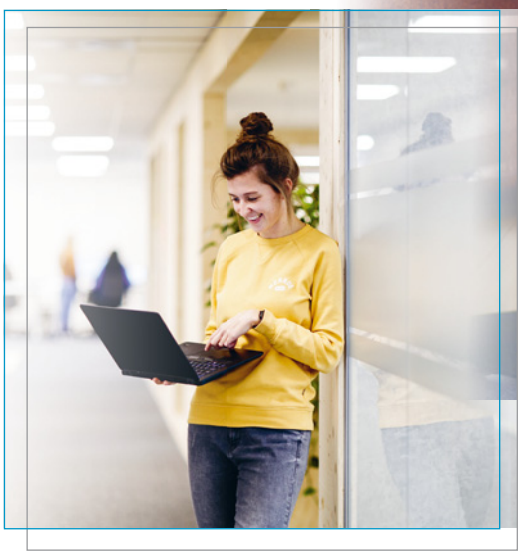
Wie halten Sie Ihre Wissensdatenbank aktuell?

Ihr Knowledgemanagement sollte diesem Prozess folgen und ihn als Mantra verinnerlichen: veröffentlichen, teilen, überprüfen, veröffentlichen, teilen, überprüfen. Das Hauptaugenmerk sollte dabei auf dem Punkt „überprüfen" liegen. Wenn Sie zum Beispiel neue Drucker kaufen, sich die Anleitung zum „Papier wechseln" in Ihrer Wissensdatenbank aber auf Ihre alten Drucker bezieht, ist damit niemandem geholfen.

1. Struktur

Zuerst sollten Sie beachten, dass es keinen Sinn macht, viele Dokumente in kurzer Zeit zu erstellen. Das ist nicht effizient. Viele der Dokumente werden möglicherweise nie benutzt. Stattdessen sollten Sie Ihre Wissensdatenbank kontinuierlich erweitern – lassen Sie sich dabei von einem Spezialisten helfen. Entwickeln Sie einen Prozess, der dem Spezialisten zeigt, ob das Problem vom Melder hätte gelöst werden können oder nur von einem technischen Ansprechpartner.

Hätte das Problem leicht gelöst werden können (wie etwa das Zurücksetzen eines Passwortes), erstellt der Spezialist nach der Anfrage einen Eintrag in der Wissensdatenbank. So können Ihre Melder benötigte Informationen finden, ohne den Servicedesk kontaktieren zu müssen. Falls der Spezialist direkt beim Abschluss der Anfrage keine Zeit hat den Eintrag zu erstellen, kann er vermerken, dass daraus noch ein Wissenseintrag erstellt werden soll. Dabei kann es sich um Inhalte für Melder, aber auch Servicedesk-Mitarbeiter handeln - frei nach dem Motto „Wissen ist Macht".



2. Erstellen Sie Wissenseinträge

Wenn Sie viele Anfragen als „enthält Wissen" markiert haben, können Sie beginnen, die Wissenseinträge zu erstellen. Dabei sollten die Einträge nach Auswirkung und Zeitaufwand für den Spezialisten priorisiert werden. Reservieren Sie Zeit für die Erstellung, fördern Sie Teamwork und versuchen Sie Ihre Mitarbeiter zu dieser Methode zu motivieren, um Ihre Wissensdatenbank wachsen zu lassen.

3. Legen Sie Parameter fest

Nachdem Sie einige Wissenseinträge erstellt haben, können Sie sich ein neues Ziel setzen: Jede abgeschlossene Anfrage muss mit einem Wissenseintrag verlinkt sein. Sie dürfen nicht davon ausgehen, dass das direkt zu 100 Prozent funktioniert. Je mehr Erfahrung Ihr Team mit der Zeit sammelt, umso größer wird dieser Anteil sein. Neue Supportmitarbeiter können sich anhand dieser Methode auch viel schneller einarbeiten, da Ihnen Erfahrungen aus sämtlichen vorherigen Problemlösungen zur Verfügung stehen.

4. Teilen Sie Ihr Wissen

Geht eine Anfrage ein, die ohne die Hilfe eines Spezialisten gelöst werden kann und für die es schon einen Wissenseintrag mit einer Lösung gibt, sollte dieser Eintrag dem Melder direkt angezeigt werden. Um das zu erreichen, sollten Sie Ihr gesamtes Unternehmen an den Komfort eines Self Service Portals gewöhnen! Dort können Ihre Melder Anfragen aufgeben, aber auch selbst über die Google-ähnliche Suche Lösungen in Ihrer Wissensdatenbank finden.

5. Überprüfen Sie Ihre Wissensdatenbank

Prüfen Sie Ihre Einträge so oft wie möglich und nötig. Erstellen Sie Maßnahmen, um die Dokumente hinsichtlich der Effektivität zur Lösung der Probleme Ihrer Melder bewerten zu können.

Wie gehen Sie im Servicedesk am effektivsten mit einer Wissensdatenbank um?

1. Durchsuchen Sie die Wissensdatenbank

Durchsuchen Sie immer zuerst die Wissensdatenbank, selbst wenn Sie die Lösung kennen. Es spart Ihnen Zeit eine Antwort zu formulieren. Vielleicht hatte schon einmal jemand dieses Problem und es ist eine Lösung vorhanden? In diesem Fall können Sie die Lösung bei Bedarf aktualisieren oder einfach kopieren, einfügen und das Ticket schließen. Falls kein Eintrag vorhanden ist, schreiben Sie die Lösung ins Ticket, schließen es und legen danach einen Eintrag an.

2. Korrigieren Sie die Wissensdatenbank

Wenn Sie feststellen, dass in dem Wissenseintrag etwas fehlt, sollten Sie dies umgehend beheben. Nur so wird Ihre Wissensdatenbank zu einer kontinuierlich aktualisierten Anlaufstelle für jegliches Wissen Ihres Servicedesks. Vielleicht setzen Sie eine schnellere Lösung ein als die, die in der Wissensdatenbank vorhanden ist. Warum helfen Sie dann nicht Ihren Teammitgliedern, indem Sie diese Lösung hinzufügen?

DENKEN SIE IMMER DARAN, DASS KNOWLEDGE-MANAGEMENT EIN FORTLAUFENDER PROZESS IST.

Kristin Pitz, Marketing Manager, TOPdesk Deutschland GmbH, www.topdesk.de

3. Die Anfrage bearbeiten

Jetzt sind Sie bereit, die Anfrage zu lösen. Während Sie das tun, sollten Sie aufmerksam sein und schauen, ob irgendetwas im Lösungsprozess von dem abweicht, was im Wissenseintrag angegeben ist.

4. Die Anfrage abschließen

Sie haben die Anfrage gelöst und können nun die Anfrage schließen. Prüfen Sie, ob Sie etwas zur Lösung in der Wissensdatenbank hinzufügen können. Müssen Sie vielleicht einen Tippfehler korrigieren, die Lösung aktualisieren oder könnte der Artikel einen Screenshot für bessere Klarheit vertragen? Selbst kleine Anpassungen können hilfreich sein!

Denken Sie immer daran, dass Knowledgemanagement ein fortlaufender Prozess ist. Wenn Sie gerade erst mit der Implementierung beginnen, müssen Sie zunächst einige Male den langen Weg gehen. Je mehr Lösungen zur Wissensdatenbank hinzugefügt werden, umso häufiger kann das ganze Team Abkürzungen nehmen, um Anfragen schneller zu lösen. Stellen Sie es sich wie eine Physiotherapie vor. Zunächst müssen Sie hart mit einigen schwierigen Übungen trainieren, aber der Langzeitnutzen ist immens!

Kristin Pitz | https://blog.topdesk.de

SIEBEN AUSLÖSER FÜR SOFTWARE-AUDITS

WENN DER SOFTWAREANBIETER KLINGELT

Software-Audits wirken heute fast schon wie ein Relikt aus einer anderen Zeit. Für IT-Verantwortlichen sind sie jedoch eine lästige Realität. Bei 66 Prozent der Unternehmen steht in den nächsten 12 Monaten mindestens ein Audit an. Um vom Auditbrief im Posteingang nicht überrascht zu werden, sollten sich CIOs sieben häufige Auslöser genauer ansehen.

Die Zahl der Microsoft-Audits ist schon seit einigen Jahren rückläufig. Adobe hat sein Audit-Programm in Europa und den USA sogar ganz eingestellt. Andere Tier-1-Anbieter wie IBM jedoch fahren mit der Überprüfung der Software Compliance wie gewohnt fort. Nach einem Bericht von Flexera planen sogar 19 Prozent der befragten Anbieter, die Zahl der Audits anzuheben, um die nichtlizenzierte Nutzung ihrer Softwareprodukte besser in den Griff zu bekommen. Dazu gehören viele Tier-2- und sogar Tier-3-Anbieter, die auf dem SAM-Radar von Unternehmen kaum Beachtung finden. Quest beispielsweise baut sein Audit-Programm weiter aus und ist dabei aggressiver als es Dell je war. Ivanti und Citrix verfügen mittlerweile über strukturierte Audit-Programme. Andere wie Micro-Focus, OpenText, Software AG, Tibco, StoneBranch, JD, BMC und Corel haben die Anzahl ihrer Lizenzprüfungen deutlich angehoben.

Für CIOs und IT-Manager gestalten sich Audits nicht nur langwierig und aufwendig. Sie können auch teuer werden. Dabei gibt es durchaus Gründe, warum gerade das eigene Unternehmen ins Blickfeld der Auditoren gerückt ist. Wer die häufigsten Auslöser für Audits sowie die Motive der Anbieter kennt, gewinnt Zeit und kann sich gemeinsam mit dem Team durch die Festlegung eines standardisierten Auditprozesses optimal vorbereiten.

Auslöser für Software-Vendor-Audits

1. Fusionen und Übernahmen

Übernahmen, Fusionen oder Veräußerung sind wohl das sicherste Zeichen für ein kommendes Audit. Lizenzvereinbarungen beziehen sich immer auf eine klar definierte rechtliche Einheit, sprich einem Unternehmen oder einem Konzern. Ändert sich diese rechtliche Struktur, wie im Falle eines M&A, heißt es die vertraglichen Regelungen zur Softwarelizenzierung zu überprüfen und gegebenenfalls anzupassen. Nicht selten steigen beispielsweise die Zahl der Mitarbeiter und damit die Anzahl von IT-Assets und Cloudumgebungen sprunghaft an. Viele Anbieter warten daher zunächst ab und kündigen erst dann ein Audit an, wenn sie davon ausgehen können, dass die Fusion oder Übernahme aus IT-Sicht abgeschlossen ist. Die Schonfrist kann sechs Monate oder ein Jahr dauern. Wurden jedoch in diesem Zeitraum keine neuen Vereinbarungen hinsichtlich der Softwarelizenzierung getroffen, sind Verstöße zu erwarten.

2. Änderungen der IT-Infrastruktur

Es gibt unterschiedliche Gründe, warum die IT-Infrastruktur sich verändert: von der Einführung von virtuellen Anwendungen, das Einrichten eines Disaster-Recovery-Rechenzentrums oder die Migration in die Cloud. Egal was sich ändert, die Wahrscheinlichkeit ist hoch, dass die IT den Vertrag im Zuge der Anpassungen für bestimmte Softwareprodukte nicht mehr verlängert (Phase-Out). Bevor es jedoch soweit ist, schlagen die Anbieter dieser Produkte noch einmal zu und kündigen ein Audit an.

3. Abnehmende Geschäftsbeziehung mit einem Hersteller

Gehen die Einnahmen bei einem Kunden deutlich zurück, gehen beim Softwareanbieter verständlicherweise die Alarmglocken an. Das Microsoft Enterprise Agreement beispielsweise verpflichtet Unternehmen in der Regel dazu, jedes Jahr eine True-Up-Meldung zu verfassen, wobei exakte und verlässlich erhobene Angaben zu den genutzten Lizenzen im Rahmen des Lizenzvertrages abgefragt werden. So soll das Unternehmenswachstum des Kunden in den letzten 12 Monaten in Erfahrung gebracht werden. Gibt es keine Änderungen zum Vorjahr, können IT-Führungskräfte ein Formular namens „Zero Sum True-Up" einreichen, nach dem keine zusätzlichen Lizenzkäufe erforderlich sind. Hier ist jedoch Vorsicht geboten, denn das Einreichen eines solchen Formulars kann Fragen zum IT-Inventar und der Mitarbeiteranzahl (gemäß Geschäftsbericht) aufwerfen und zu einer genauen Prüfung (Audit) führen.

4. Auslaufen von Wartungs- und Supportvereinbarung

Die Kündigung oder das Nicht-Verlängern von Support- und Wartungsverträgen, kann Softwareanbieter ins Grübeln bringen. Die Frage ist hier häufig, ob der Kunde die Software weiter einsetzt und wenn ja, warum ohne Wartung? Da Anbieter einen Großteil ihrer Einnahmen mittlerweile über den Kundenservice generieren (Versionsupgrades, technischer Support), wird hier lieber doppelt und dreifach überprüft. Das ist auch deshalb der Fall, da Anbieter selbst nach Beendigung von Supportverträgen in den meisten Fällen ihr Anrecht auf Audits behalten.

WER DIE HÄUFIGSTEN AUSLÖSER FÜR AUDITS SOWIE DIE MOTIVE DER ANBIETER KENNT, GEWINNT ZEIT UND KANN SICH GEMEINSAM MIT DEM TEAM DURCH DIE FESTLEGUNG EINES STANDARDISIERTEN AUDITPROZESSES OPTIMAL VORBEREITEN.

Marius Dunker,
Vice President DACH Sales, Flexera,
www.flexera.de

5. Support-Tickets für nicht lizenzierte Anwendungen

Support-Tickets bei technischen Problemen sind mittlerweile selbst in kleinen Unternehmen Standard. Dabei wird oft vergessen, dass die im Ticket enthaltenen Informationen vom Softwareanbieter intern genutzt und mit bestehenden Verträgen abgeglichen werden können. Immer wieder wenden sich Mitarbeiter, Partner und Dritte hilfesuchend an Softwareanbieter, um ein Problem mit einer Anwendung zu lösen, die nicht oder ungenügend lizenziert ist. Abweichungen und Ungereimtheiten zu bestehenden Lizenzvereinbarungen fallen hier schnell auf und können zu unangenehmen Fragen für den verantwortlichen IT-Manager führen.

6. Statistischer Ausreißer

Die meisten Anbieter verfügen über riesige Mengen an statistischen Daten und nutzen diese, um Auffälligkeiten, Muster und Ausreißer auszumachen. Dazu zählt beispielsweise die Anzahl der Mitarbeiter/Unternehmensgröße in Relation zu den durchschnittlich lizenzierten Applikationen. Fällt ein Unternehmen bei der Nutzung seiner Software aus der Norm, macht es sich automatisch verdächtig und die Chancen eines Auditbriefs steigen.

7. Fehlende Kommunikationsrichtlinien

Eine gute Beziehung zum Softwareanbieter ist wichtig. Geht die Auskunftswilligkeit jedoch zu weit, laufen Unternehmen Gefahr in der Kommunikation zum Key Account-Manager zu viele Informationen preiszugeben. Das kann ein Mitarbeiter sein, der stolz von einem Trick berichtet, mit dem sich besondere Features einer Anwendung nutzen lassen. Oder ein Chart in einer Präsentation, aus dem sich der detaillierte IT-Footprint eines Unternehmens ablesen lässt. Klare Richtlinien, Vorgaben und Templates, die festlegen, wer mit wem in Kontakt tritt, und welche Informationen in welchem Umfang geteilt werden dürfen, sind daher wesentlich, um solche Schnitzer zu vermeiden. Diese klaren Kommunikationsrichtlinien sind dann natürlich auch im akuten Auditfall zwingend notwendig.

An Gründen für Audits mangelt es demnach nicht. In einer sich ständig ändernden IT-Umgebung nehmen automatisierte SAM- und Audit-Prozesse damit eine zentrale Rolle ein. Mit ihnen gewinnen CIOs und IT-Verantwortliche die Informationshoheit über die IT-Assets im Unternehmen zurück, können Fragen von Auditoren gezielt beantworten und den langwierigen Audit-Besuch, wenn auch nicht verhindern, so doch wenigstens verkürzen.

Marius Dunker

THE NEXT STEP

DIGITAL PROCESS AUTOMATION

Die digitale Transformation benötigt eine starke Basis für zukunftssichere Anwendungen. Ein Fall für AgilePoint NX.

Die digitale Transformation bedeutet für die meisten Unternehmen radikal mehr Softwareentwicklung:

- Back-Office-Anwendungen, die funktionsübergreifende Zusammenarbeit zwischen Abteilungen ermöglichen
- Apps, die jeden Berührungspunkt mit internen/externen Kunden in jedem Prozess unterstützen und die nahtlos mit Back-Office-Prozessen interagieren
- (Teil-)Automatisierte Prozesse, die den Betrieb rationalisieren, die schnelle Änderbarkeit ermöglichen und somit die Kundenbindung verfestigen

> DIE DIGITALE TRANSFORMATION BEDEUTET FÜR DIE MEISTEN UNTERNEHMEN RADIKAL MEHR SOFTWAREENTWICKLUNG.
>
> Marcus Armbruster, Regional Manager DACH, AgilePoint, www.agilepoint.com

Die Herausforderung besteht darin, all diese Anwendungen so zu entwickeln, dass sie nicht zu einer Belastung werden und bei jeder Innovation oder Änderung aufwendig neu gestaltet oder angepasst und ausgerollt werden müssen. Kurz gesagt, damit die digitale Transformation erfolgreich ist, müssen Sie all diese Anwendungen auf wechselnde, neue Anforderungen schnell adaptieren können.

Die zukunftssichere Plattform

Die Tiefe und Breite der Anforderungen an die digitale Transformation erfordern sowohl die Leistung von BPMs der „Enterprise-Klasse“ (für eine kleine Anzahl von „tiefen“, hochkomplexen Prozessen, deren Erstellung Monate dauern kann) als auch die Geschwindigkeit und Flexibilität einer Low-Code-Plattform (für eine große Anzahl leichter, kleiner Apps, die unzählige Anforderungen innerhalb eines Unternehmens erfüllen). Plattformen, die sowohl BPM- als auch Low Code-Funktionen enthalten, können das, was Forrester Research als „Digital Process Automation“ (DPA) bezeichnet: die Ausweitung/Er-

weiterung Ihrer automatisierten Prozesse auf Kunden, Lieferanten und Partner. Mit DPA handeln Sie idealerweise proaktiv, reagieren schnell auf unvorhergesehenes und erreichen ein verbessertes Kundenerlebnis. AgilePoint NX ist eine leistungsstarke DPA Plattform, die alle oben beschriebenen zukunftssicheren Eigenschaften umsetzt (Bild 1).

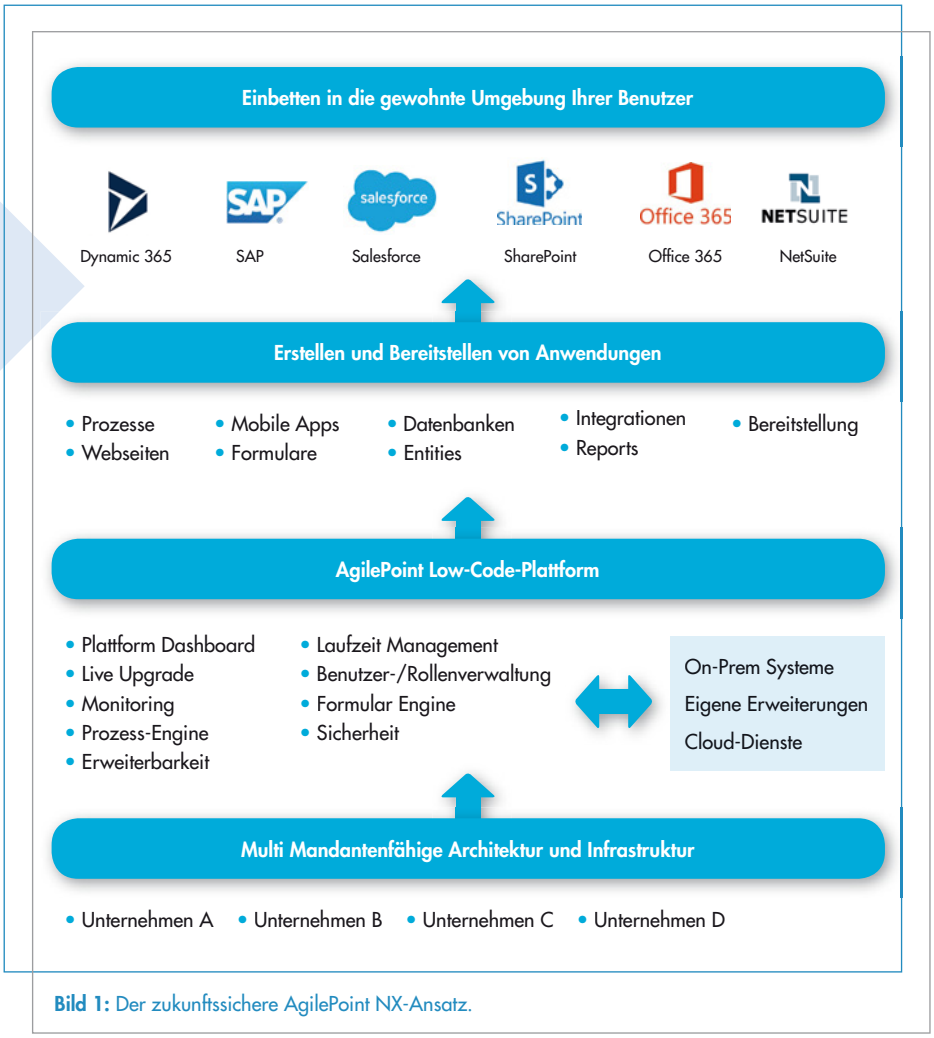


Bild 1: Der zukunftssichere AgilePoint NX-Ansatz.

Der Ansatz

Der Ansatz definiert die Grenzen dessen, was für prozessorientiere Unternehmensanwendungen möglich ist, neu. Die Kunden sind global agierende Unternehmen, aber auch kleine und mittlere. AgilePoint wird in verschiedensten Branchen bereits erfolgreich eingesetzt (etwa Gesundheitswesen, Banken, Engineering, Energie, Automotive). Die Plattform ist erschwinglich und ermöglicht Kunden schnell, kontinuierlich verbesserte Abläufe mit messbaren ROI. Die initialen und laufenden Betriebskosten unserer Produkte sind am Markt für Low-Code und BPMS beispiellos.

AgilePoint NX ist eine prozessorientierte „Low-Code Anwendungs-Plattform As-a-Service" (aPaaS), mit der Nicht- Programmierer schnell anspruchsvolle Formulare, Workflows und unternehmensfähige Geschäftsanwendungen erstellen, bereitstellen, nutzen und verwalten können. AgilePoint NX wurde speziell entwickelt, um die digitale Transformation heutiger Organisationen zu katalysieren und zu erleichtern, sodass jeder in einer Organisation die Rolle des Innovators übernehmen kann. AgilePoint NX verwendet eine deklarative „Point-and-Click" Entwicklungsumgebung, verfügt über einen leistungsstarken Formular Designer und ermöglicht die einfache Darstellung von Daten in Diagrammen und Grafiken. Die entwickelten Anwendungen reagieren „Responsive" auf verschiedenen Endgeräte, Ausrichtungen, Browser und sich ändernde geschäftliche und technische Anforderungen.

Eigenschaften von zukunftssicheren Apps

Die Notwendigkeit, neue Anwendungen schnell zu erstellen, hat die Entstehung von Low-Code Development Plattformen (LCDPs) katalysiert, die eine Anwendungsentwicklung um das Zehnfache beschleunigen können. Ebenso verwenden LCDPs durchgängig einen „Drag-Drop-and-Configure-Ansatz" für die Anwendungsentwicklung, was die Entwicklung erheblich vereinfacht, da Nicht-Programmierer funktionale Anwendungen erstellen können. Aber im Kontext der digitalen Transformation ist schnell und einfach nicht gut genug. Anwendungen benötigen eine Reihe von Merkmalen, die es ihnen ermöglichen, weiter zu arbeiten, auch wenn unvermeidliche Änderungen auftreten.

Die Prozess Engine

Die wesentliche Kernkomponente einer BPM-Suite und einer Low-Code-Prozessplattform ist die Prozess-Engine (Bild 2). Die Prozess-Engine von AgilePoint NX ist ein Schlüsselaspekt der zukunftssicheren Architektur und weist mehrere definierende Alleinstellungsmerkmale auf:

A. Skalierbarkeit

AgilePoint NX verwendet eine zustandslose Prozess-Engine. Das bedeutet, nicht der ganze Prozess wird während der Ausführung geladen, sondern nur die aktiven Prozessaufgaben/-aktivitäten. Dieses Design gewährleistet eine optimale Performance. Darüber hinaus unterstützt die AgilePoint NX-Engine automatisierte Prozesse nahezu jeder erdenklichen Größe und Last. Ebenso beschränkt die AgilePoint- Engine weder die Anzahl der automatisierten Prozesse, die Organisationen erstellen können, noch die Anzahl der Versionen einer bestimmten App. Dieser Aspekt der Skalierbarkeit ist für eine

zukunftssichere Plattform von entscheidender Bedeutung, da für die Transformation leicht Tausende von Prozess-Apps erforderlich sein können, von denen viele mehrere Versionen haben werden. Schließlich hängt die Anzahl der gleichzeitigen Prozessinstanzen, die in NX-Infrastrukturen ausgeführt werden, von der zugrunde liegenden Hardware- beziehungsweise Cloud-Infrastruktur ab. Diese Funktion ist besonders wichtig für große Unternehmen.

B. Zuverlässigkeit

Die Tatsache, dass die zustandslose Engine von AgilePoint während der Ausführung nicht ganze Prozesse im Speicher hält, verringert die Möglichkeit eines Datenverlusts im Falle eines Systemausfalls erheblich. Stellen Sie sich zum Beispiel einen Prozess mit fünfzig Schritten vor. Angenommen, während der Ausführung von Schritt 23 ist ein Stromausfall aufgetreten. Keine der Daten aus den ersten 22 Schritten würde verloren gehen - sie wurden bereits persistiert. Wenn das System zurückkommt, lädt die Engine die aktuell anstehenden Aufgaben/Aktivitäten (etwa der abgebrochene Vorgang wird in Schritt 23 fortgesetzt).

C. Hyperagilität

IDC prognostiziert, dass Unternehmen immer anspruchsvollere Anwendungen gerecht werden müssen – getrieben durch steigende Kundenanforderungen. AgilePoint NX wird dem gerecht durch eine hochgradig anpassbaren Prozess-Engine. Die Vision eines „AI-Driven-Task-Routing“ führte zu einer Engine, die sowohl manuelle Zuordnung, AI-Zuordnung, als auch vordefinierte Zuordnung von Aufgaben unterstützt. Mit der AgilePoint- Engine können Live-Prozesse während der Ausführung aktualisiert oder sogar heruntergestuft werden, ohne dass die Plattform neu gestartet werden muss. Auch die AgilePoint NX- Plattform selbst kann ohne Ausfallzeiten aktualisiert werden. Anwender betreiben verschiedene Versionen derselben Anwendung ohne Seiteneffekte parallel.

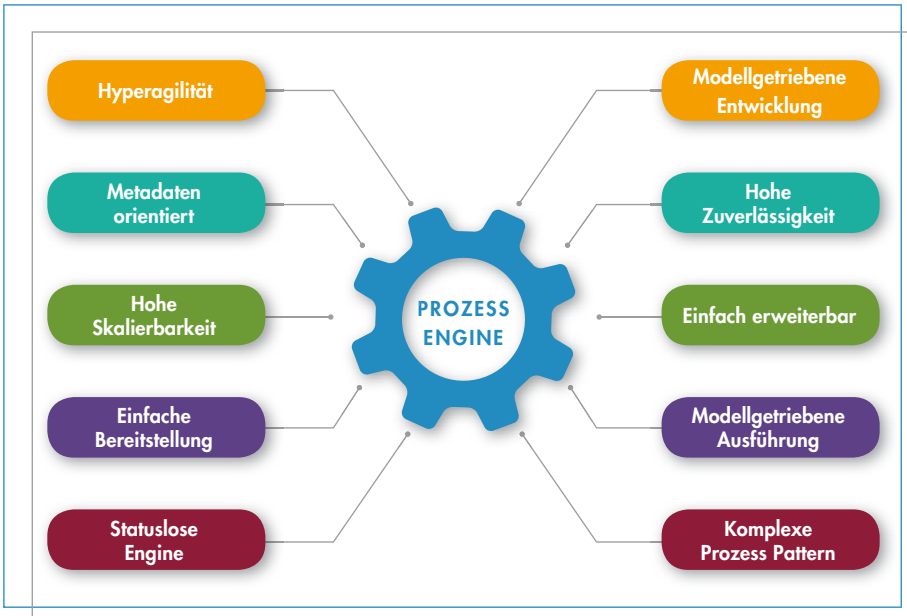


Bild 2: Hauptmerkmale der AgilePoint NX Prozess-Engine.

AKTUELLE SITUATION

Der Druck und Umfang der anstehenden Digitalisierung wächst stetig. Tatsächlich prognostizieren viele Marktanalysten einen exponentiellen Anstieg der Änderungsrate in Anwendungen für die kommenden Jahre. Unternehmen, die mit dieser Realität konfrontiert sind, müssen sich gegen potenziell katastrophale Marktereignisse absichern. Dazu übernehmen sie das Paradigma der schnell anpassbaren, kundenspezifischen Softwareentwicklung zur initialen Transformation. Genauso wichtig ist die Aufrechthaltung der kontinuierlichen Transformation mit minimalem Aufwand. AgilePoint NX ist die einzige vorhandene Plattform am Markt, die diese Strategien umfassend unterstützt.

Die Engine ermöglicht das Erstellen von „Verbundanwendungen“. Eine zusammengesetzte Anwendung bezieht Funktionen aus anderen/mehreren Quellen. Dieser zusammengesetzte Ansatz ermöglicht die einfache Integration neuer Technologien. Darüber hinaus erfordert die Integration neuer Technologien in eine zusammengesetzte App nicht, dass die App neu aufgebaut oder überarbeitet wird. Kernpunkte sind Wiederverwertbarkeit und ein schnelles „Time-to-Market“.

D. Erweiterbar

Die Prozess- Engine verfügt über eine ereignisgesteuerte Architektur, die erweitert werden kann. Jede Aktivität löst Ereignisse aus, die abonniert werden können, um das Verhalten des Systems zu ändern. Beispielsweise wird die Standardausnahmehandlung gemäß den Organisationsrichtlinien festgelegt und erzwungen. Ebenso kann eine Organisation ihre eigenen Prozessaktivitäten erstellen.

Marcus Armbruster

In der nächsten Ausgabe lesen Sie was „echte“ Low-Code-Entwicklungsplattformen ausmacht.

KOSTENGÜNSTIGER EINSTIEG IN IOT-ANALYTICS

LIVE WEBINAR AM 28.05.2020, 10-11 UHR

Wie wäre es, sich den Themen IoT und Maschinendatenanalyse endlich über einen praktikablen Ansatz zu nähern? Der ERP-Spezialist ams.Solution zeigt in diesem Live Webinar, wie Unternehmen Maschinendaten erfassen, analysieren und verarbeiten können, um automatisierte Workflows auszulösen, zielgerichtete Wartungs- oder ganz neue Service-Modelle zu entwickeln.

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

Was Sie im Webinar erfahren

Martin Hinrichs, Produktmanager der ams.Solution, erläutert, wie

- man mit der RNA IoT ConnectBox auch ältere Maschinen im Retrofit-Verfahren schnell und kostengünstig intelligent macht.
- die erfassten Daten in der bimanu-BI-Cloud aggregiert und gewinnbringend aufbereitet werden.
- das Zusammenspiel zwischen der BI-Cloud und dem ERP-System ams.erp funktioniert, um Service-Tasks und/oder andere individuelle Workflows automatisiert auszulösen.

---

eBOOK

IT SERVICE MANAGEMENT – VIELE WEGE, EIN ZIEL

Das eBook „IT Service Management – To be ahead!" stellt aktuelle Entwicklungen aus der Welt des IT Service Management vor. Es geht zum Beispiel um die richtige Auswahl von ITSM-Tools, darüber was Identity & Access Management mit Enterprise Service Management zu tun hat und über die Vorteile der Wertstromanalyse für IT-Services.

Highlights aus dem eBook „IT Service Management"

➤ Prozesse und Wertströme

Wertströme konzentrieren sich auf den Fluss der Aktivität, Informationen und Materialien von der Nachfrage oder Chance bis zum Kundenwert. So sind Prozess-Taxonomie, Managementtools und -techniken auf Wertströme anwendbar, aber nicht alle Prozesse sind per se wertschöpfend: Ein Prozess, der etwa Kennzahlen berichtet, die niemand zum Steuern verwendet, kann vielleicht gefordert sein, erzeugt jedoch als Ganzes keinen Wert.

➤ 5 Wahrheiten über die Auswahl von ITSM-Tools

Die Einführung eines Tools erscheint vielen als Abkürzung auf dem Weg zu echter Serviceorientierung. Ein Fehler! Konzentrieren Sie sich auf einen Kernbereich, der mit dem Tool unterstützt werden soll. Legen Sie Ihre Schwerpunkte fest. Wo soll das Tool seine Stärken haben? Überlegen Sie sich die Punkte, anhand derer Sie sich konkret gegen ein Tool entschieden würden. Und: erstellen Sie ganz konkrete Szenarien, wie sie in diesen Schwerpunkten mit dem Tool arbeiten wollen und können.

➤ IAM auf dem Weg zum ESM

bi-Cube als IAM ist mit seinem Rollenmodell, dem Regelwerk und den generischen Prozessmodellen einfach um die Modellierung allgemeiner Objekte zu erweitern. Da diese Objekte beliebige Ausprägungen haben können sind dazu je nach Typ auch differenzierte Attribute zu definieren. Die Einbindung dieser Objekte in die Verwaltungsprozesse und in das Self-Service-Portal ist die wesentliche Basis für ein Enterprise Service Management (ESM).

Das eBook „IT Service Management" ist 56 Seiten lang und steht kostenlos zum Download bereit.

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
30. JUNI 2020

LOW CODE PLATTFORMEN

Geschwindigkeit & Flexibilität

MACHINE LEARNING

Condition Monitoring reloaded

LIZENZ-MANAGEMENT

Freiraum für die Digitalisierung

DIE AUSGABE 07/08 VON IT MANAGEMENT ERSCHEINT AM 30. JUNI 2020.

INSERENTENVERZEICHNIS

it management	
it Verlag Gmb	U2, U4
ams.Solution AG	3
USU Software AG	9
noris network AG (Advertorial)	17
c.a.p.e. IT GmbH	19
E3 Magazin/B4B Media	U3

it security	
it Verlag GmbH	U2, U4
HiScout GmbH	3
Akamai Technologies (Advertorial)	9
SEPPmail Dtschl. GmbH (Advertorial)	11

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:
Marcus Armbruster, Gerald Beuchelt, Marius Dunker, Günter Esch, Emile Hansmaennel, Alexander Haugk, Michael Jacob, Christian Koch, Sven Kolb, Sven Kreimendahl, Sascha Martens, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Kristin Pitz, Katarina Preikschat, Eberhard Scheuble, Andreas Scheurle, Mike Schuricht, Ralph Weiss

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 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

THOUGHT LEADERSHIP

DIE NEUE DIMENSION DES IT-WISSENS.

Jetzt neu auf www.it-daily.net

it-daily.net

itsecurity
MAI/JUNI 2020

DAS SPEZIAL

CYBERSICHERHEIT VS. CORONA

SICHERE IT-ÖKOSYSTEME

Gerald Beuchelt, LogMeIn

SCHWACHSTELLEN-MANAGEMENT

IT-Sicherheit in der Operational Technology-Welt

SECURE ACCESS SERVICE EDGE

Effektive Sicherheit in der Cloud

KÜNSTLICHE INTELLIGENZEN

Optimales Ergebnis für die IT-Security

www.it-daily.net

Visionen, Träume, Ziele auf den Punkt gebracht!

Expertenwissen für

IT-Strategien & Innovationen

itmanagement

www.it-daily.net

INHALT

COVERSTORY

IT SECURITY

CYBERSICHERHEIT VS.

WIE UNTERNEHMEN GENAU JETZT IHR IT-ÖKOSYSTEM SICHERER MACHEN

Es ist eine Ironie des Schicksals: Ausgerechnet ein realer Virus zwingt Unternehmen im Kontext von Lockdown, Homeoffice und virtueller Zusammenarbeit über virtuelle Viren, Hacker und IT-Sicherheit neu nachzudenken.

Wenn man sich fragt, was Unternehmen in diesen Tagen tun können, um ihre Cybersicherheit zu verbessern, so steht ein Umstand im Vordergrund: Wir sehen uns heute mehr denn je einer dynamischen Workforce gegenüber, die permanent von verschiedenen Orten und mit verschiedenen Devices zusammenarbeitet - logisch, dass die Corona-Krise diese Entwicklung rasant beschleunigt.

Oft gibt es nicht genügend Laptops im Haushalt, Zugänge sind unsicher oder Passwörter werden geteilt. Die „Homeoffice Workforce" arbeitet dann aber auch oft mit „Schatten IT", indem sie eigene Anwendungen oder Apps benutzt - sei es, weil die Leute das gewohnt sind oder weil sie die unternehmenseigenen Angebote zu kompliziert finden. Das schafft aber natürlich auch neue Angriffspunkte.

Gute Tipps zur Verbesserung der Cybersicherheit

Aus den obengenannten Gründen ist es wichtig, dass IT sicherstellt, dass es für Fälle wie jetzt den Corona-Shutdown einen Notfallplan gibt, der die Geschäftsaktivitäten aufrechterhalten kann. Der Betrieb über ein Netzwerk von Homeoffices erfordert vorab Absprachen zwischen IT, HR, IT-Sicherheit und den operativen Einheiten. Es muss bei allen Leuten ein Bewusstsein geschaffen werden, sich auch zu Hause „cybersmart" zu verhalten. Umgekehrt müssen Unternehmen dafür Sorge tragen, dass sie ihre Mitarbeiter mit dieser Botschaft auch erreichen - etwa mit einer Informationsseite oder einem ständigen Kommunikationskanal für solche Belange; am besten beides. Und schließlich, um das Risiko von Phishingangriffen zu reduzieren, bei denen die Nutzerdaten von Mitarbeitern gestohlen werden, sollten Unternehmen die Multifaktor-Authentifizierung (MFA) einführen, um ihre Mitarbeiter auch im Homeoffice vor Cyberangriffen zu schützen.

Historische Chance?

Die Regierungen sagen ihren Bürgern, dass sie daheim bleiben sollen und das heißt, dass eine ganze Menge Menschen von zuhause aus arbeitet. Mehr als je zuvor. Dadurch wächst das Risiko, dass Unternehmen in dieser neuen und unübersichtlichen Situation über verschiedene Kanäle angegriffen werden.

ES MUSS BEI ALLEN LEUTEN EIN BEWUSSTSEIN GESCHAFFEN WERDEN, SICH AUCH ZU HAUSE „CYBERSMART" ZU VERHALTEN. UMGEKEHRT MÜSSEN UNTERNEHMEN DAFÜR SORGE TRAGEN, DASS SIE IHRE MITARBEITER MIT DIESER BOTSCHAFT AUCH ERREICHEN.

Gerald Beuchelt, Chief Information Security Officer, LogMeIn, www.lastpass.com

Cyberkriminelle werden Menschen ins Visier nehmen, die Homeoffice nicht gewohnt sind, oder sie werden nach Unternehmen Ausschau halten, die nur ungenügend für Homeoffice gerüstet sind.

Das ist jetzt tatsächlich eine einmalige Chance für Unternehmen, ihre Verteidigung aus der IT-Implementierungs- und Sicherheitsperspektive zu schärfen: Mit Security-as-a-Service und starken Passwörtern, die Mitarbeiter und Business für längere Zeit gut absichern. Das sind die Basics gegen Viren und andere Malware.

Wahrscheinlich werden wir nach Corona nie wieder so arbeiten wie früher. Deshalb ist es nur schlüssig Sicherheitsmaßnahmen für Homeoffice und die neue Zusammenarbeit zu ergreifen. Langfristig werden Unternehmen mit einer flexiblen, agilen Sicherheitsphilosophie und schneller Adaptionsfähigkeit davon profitieren. Es geht jetzt darum Sicherheit zu „straffen" und ein Modell zu entwickeln, das für Justierung offen bleibt.

Bedrohungen im Kontext der neuen Zusammenarbeit

Oft ist der Mensch selbst das schwächste Glied in der Sicherheits-Kette: Mitarbeiter, die keine Passwörter ändern oder dieselben Passwörter über viele Nutzerkonten hinweg benutzen. Das gilt besonders,

wenn diesbezüglich keine Aufklärung betrieben wurde oder kein Sicherheits-Bewusstsein entwickelt wurde. Eine IT-Sicherheitsbereitschaft und -kultur zu schaffen braucht Zeit und viel Schulung, aber in der derzeitigen Situation müssen wir alle schnell reagieren. Beim Zugangsmanagement sollte jeder begreifen, dass schlechte Passwort-Hygiene (Default-Passwörter nicht ändern, Passwort Wiederbenutzung oder schwache Passwörter) die Chance erhöht, Opfer eines Hackers zu werden.

Hier kann ein Passwort-Manager schnell, nahtlos und einfach in den Workflow integriert werden. Diese verwenden auch oft Multifaktor-Authentifizierung, die zusätzliche Sicherheit bringt gerade wenn Mitarbeiter sich von unterschiedlichen Standorten aus einloggen.

Motivierte Mitspieler und gute Coaches

Wie jeder Teamsport braucht auch Cybersecurity motivierte Mitspieler und gute Coaches. Es war noch nie eine Einbahnstraße, aber mit Homeoffice wird es noch etwas komplexer. Da braucht es gemeinsame Anstrengungen von allen Mitarbeitern, egal mit welchem Senioritätsgrad. Das bedeutet, dass man jede Änderung der Sicherheitsstruktur offen und transparent an die Mitarbeiter kommuniziert, und dass IT, IT-Sicherheit, HR und operative Einheiten sich koordinieren, um sicherzustellen, dass es keine Sicherheitslücken gibt. Natürlich ist auch die Stimme von „oben" ein erfolgskritischer Faktor: Wenn Mitarbeiter sehen, dass der CEO und die Manager die Wichtigkeit solcher Sicherheits-Programme betonen, werden sie selbst auch ihren Teil dazu beitragen. Dazu müssen Mitarbeiter die Sicherheitsziele und Maßnahmen ihrer Firma verstehen. Sie brauchen Training und bewusstseinsbildende Maßnahmen, um cybersmartes Verhalten im Homeoffice zu fördern. Das wird dann wirklich helfen, die Organisation sicher zu halten und Viren und andere Malware abzuwehren.

Also: Unternehmen und Mitarbeiter müssen ihre Identität managen und sichern, und zwar möglichst unaufdringlich. Eine gute User Experience aufrechtzuerhalten ist deshalb wichtiger Bestandteil der Sicherheitskultur, denn andernfalls werden die Heimarbeiter sie wieder umgehen. Wirklich gute Sicherheit ist deshalb beinahe unsichtbar für die, die sie schützt.

Heimarbeit bedeutet für die meisten Menschen, dass Dokumente und Gespräche offener für andere zugänglich sind, sei es auch nur für die Familie. Deshalb ist es noch wichtiger als zuvor, dass alle Programme lange, zufallsgenerierte Passwörter besitzen. Mit einem Passwort Manager schlägt man hier zwei Fliegen mit einer Klappe, indem man einzigartige Passwörter für jeden Login generiert und speichert. Der Username und die Passwörter werden dann in einem „Safe" gespeichert, wo sie verschlüsselt und organisiert werden. Die Produkte sind höchst kosteneffektiv.

Sicherere Arbeit

Einen Passwort-Manager mit Multifaktor-Authentifizierung zu nutzen, wird Usern helfen, ihre Passwort-Hygiene zu verbessern und das Risiko zu senken, Opfer eines Hackers zu werden - und übrigens auch das unbeabsichtigte Teilen von Inhalten. Alles in allem ein Schritt zu sicherer Arbeit.

Kein Zweifel: Es ist eine herausfordernde Zeit, die hoffentlich auch für mehr Aufmerksamkeit für die Planung von Notfallszenarien in Zusammenarbeit mit IT-Sicherheitsteams führt.

Gerald Beuchelt

HOMEOFFICE – WAS NUN?

WARUM REMOTE ARBEITEN FÜR DIE DEUTSCHE WIRTSCHAFT LANGFRISTIG ZUM PROBLEM WERDEN KÖNNTE

Der erste Schock über das neuartige Virus ist überwunden, der erste Staub nach der Umsattlung auf Homeoffice hat sich gelegt. Nachdem sämtliche Tools kurzfristig zum Laufen gebracht wurden, drängt sich nach und nach die Frage auf: „Sind wir richtig aufgestellt?" Denn Angreifer nutzen neue Sicherheitslücken und die Unwissenheit von Unternehmen sofort aus.

Zuhause arbeiten? „Nein, danke!"

Laut einer Statista Umfrage waren sich Arbeitnehmer schon vor Corona uneins, ob sie gerne von zuhause arbeiten würden. Fast jeder 5. Mitarbeiter in Deutschland stand der Heimarbeit unentschlossen gegenüber. Nun hat aber im Zuge der Corona-Krise eine hohe Anzahl von Unternehmen ihre Mitarbeiter gezwungenermaßen auf unbestimmte Zeit ins Homeoffice versetzen müssen.

Trotz massiver Anschaffung von Hardware und Ausstattung von Mitarbeitern mit Lösungen wie virtuellen Desktops in Azure und AWS konnten dabei nicht alle Unternehmen richtig aufrüsten. Laut TeleTrust wurden sogar bei 12 Prozent der Befragten keine IT-Sicherheitsvorkehrungen vorgenommen. Verbesserungen und das Nachholen dieser Maßnahmen stehen für viele Administratoren deshalb nun im Fokus.

Denn auch nach Corona wird Remote Working in einem ganzheitlichen Konzept für besseres Arbeiten unverzichtbar sein. So können die Erfahrungen mit dem anderen Extrem für einen zukünftigen Mix aus Remote und Office Arbeit auch ein wertvoller Vorteil sein.

Homeoffice über Nacht

Die digitale Verwaltung und Kommunikation mit dem Transfer ins Homeoffice hat sich mit einem Schlag um ein Vielfaches erhöht. Ein deutlicher Anstieg von E-Mails und Webinaren sowie über 50 Prozent mehr Video-Konferenzen sind die Folge. Laut DE-CIX zeigen die Server in Deutschland bereits jetzt einen weltweiten Rekord in der Datenauslastung mit 9,1 Terabit pro Sekunde.

Wie immer ist das Wettrennen zwischen Hackern und InfoSec Lösungen dabei in vollem Gange – die Verlegung des Spielfeldes hat für beide Seiten große Chancen geschaffen. Administratoren versuchen konsequent, ungeliebte Systeme und Sicherheitslücken im Zuge der Umstellung zu eliminieren. Für Hacker werden Ziele wie Collaboration-Lösungen, die den Kaffeeklatsch und Flurgespräche bis zum Meeting ablösen sollen, durch steigende Nutzerzahlen immer attraktiver.

Waren Sie vorbereitet?

In der Hektik, schnellstmöglich digital autark arbeiten zu können, wurden IT-Sicherheitsmaßnahmen leider notgedrungen nur lückenhaft umgesetzt. Wer dabei auf einen Notfallplan zurückgreifen konnte, steht möglicherweise besser da – ist aber leider in der Unterzahl. Das Ergebnis sind ein Mangel an VPN-Lizenzen oder Mitarbeiter, die sich bestenfalls mit kostenlosen, aber dafür unsicheren Password Managern selbst zu helfen wissen sowie der Einsatz privater Endgeräte à la BYOD, die eine Software-Nachrüstung dringend nötig hätten.

Auch Angestellte fühlen sich allein gelassen: „Wie erhalte ich Zugang zur Video-Konferenz? Darf ich diese Software überhaupt selbst installieren und ist diese E-Mail vielleicht gefährlich?" Um der Erwartungshaltung gerecht zu werden, zuhause genauso produktiv wie vorher zu sein, wird auf eigene Faust herumprobiert und die Überforderung steigt auf Kosten der Sicherheit. Darunter fällt auch das Risiko, E-Mails zu öffnen, die nur auf den ersten Blick vertraulich wirken und Schadsoftware enthalten könnten.

WELCHE IT-SICHERHEITSMASSNAHMEN HABEN SIE IM HOME OFFICE GETROFFEN?

> NUR, WENN JETZT AUF LANGE SICHT IN DIE ZUKUNFT INVESTIERT WIRD, KANN DER DIGITALISIERUNGSSCHUB IN DEUTSCHLAND FRÜCHTE TRAGEN, DAMIT WIR IM NACHHINEIN BESSER AUFGESTELLT SIND ALS ZUVOR.
>
> Sascha Martens, CTO & Cybersecurity Evangelist, MATESO, www.passwordsafe.de

Die Branche der Cyberkriminellen hat längst die aktuelle Situation ausgenutzt, um sich neu zu justieren, wie das BSI warnt. Dabei könnte die derzeit eher improvisierte IT-Sicherheit vieler Unternehmen für diese daher nur die Ruhe vor dem nächsten Sturm bedeuten.

Notlösungen statt Notfallmanagement

Denn digitale Viren sind auf dem Vormarsch und Hacker machen selbst vor Corona und Solidarität gewiss nicht halt. Erst kürzlich bekam der deutsche Impfstoffhersteller CureVac das Resultat mangelnder IT-Sicherheit zu spüren, als durch Data Leaks über 60 seiner Passwörter im Internet auftauchten.

Bei der weltweiten Dringlichkeit und Wichtigkeit ihrer Arbeit eine Gefahr, die klar macht: Wenn Unternehmen bei der aktuellen Transformation ins Digitale die Cybersicherheit nicht gebührend beachten, sind sie auf lange Sicht doppelt in Gefahr. Denn wer jetzt durch Remote Work noch mehr auf seine IT-Infrastruktur angewiesen ist, diese aber eher notdürftig umgesetzt hat, ist ein noch attraktiveres Angriffsziel für Hacker und hat noch mehr zu verlieren als vor der Krise.

Beim Nachrüsten auf langfristige, ganzheitliche Lösungen setzen

Vom Kleinbetrieb bis zu den großen Firmen mussten alle Branchen schnellstmöglich umsetzen, was normalerweise monatelange Vorbereitung bedeutet hätte. Nicht nur Organisation und Technik stehen dabei im Vordergrund. Nachdem sich der erste Sturm gelegt hat, ist jetzt ein kritisches Nachrüsten mit Software-Updates und Co. unabdingbar.

Deshalb ist es dringend ratsam, die Rechner und auch das WLAN im Homeoffice mit einem starken Passwort auszurüsten, E-Mail-Verschlüsselung und eine sichere VPN-Verbindung zu bieten, den Virenschutz up to date zu halten und die Daten mit 2-Faktor-Authentifizierung doppelt zu schützen.

Für die Einhaltung des Qualitätsversprechens sollte der Dienst aus Deutschland betrieben werden. Vollumfänglichen Schutz bietet dabei nur eine Lösung, die auf allen Endgeräten funktioniert und online sowie offline betrieben werden kann sowie die notwendigen Schnittstellen zur Integration bietet wie AD Import.

Dabei gilt es, das angestrebte Sicherheitsniveau durch Schulungen und Sensibilisierung zum Thema Cybersicherheit wiederherzustellen. Angestellte mit Bedenken müssen spätestens jetzt abgeholt und Unsicherheiten in Bezug auf Remote Working beseitigt werden. Parallel sollten trotz allem Administratoren vom Worst Case ausgehen und überprüfen, ob sich Hacker vielleicht schon längst Zutritt verschafft haben, um dementsprechend agieren zu können.

Krisenzeiten als Chance für Wachstum

Investitionen fallen Unternehmen in Krisenzeiten besonders schwer. Anspruchsvolle Lösungen können vor allem KMUs aktuell aufgrund der erforderlichen Systeme, Einarbeitungsdauer und des Budgets überfordern. Dabei ist es gerade jetzt essentiell, die beschleunigte digitale Transformation auch als Chance wahrzunehmen und sich im Homeoffice über die Krise hinweg richtig aufzustellen.

Denn was vor Corona bei vielen Berufen noch undenkbar schien, hat schon zu einer unwiderruflichen Veränderung von Arbeitsprozessen im Sinne von New Work geführt. Nach den bisherigen Anstrengungen und Herausforderungen können Unternehmen jetzt neue Potentiale durch Automatisierungen, Ortsflexibilität und Vernetzung für mehr Produktivität und Zeitersparnis nutzen. Denn nur, wenn jetzt auf lange Sicht in die Zukunft investiert wird, kann der Digitalisierungsschub in Deutschland Früchte tragen, damit wir im Nachhinein besser aufgestellt sind als zuvor.

Sascha Martens

49% Privater Rechner und Dienstrechner getrennt

41% E-Mail-Verschlüsselung

37% VPN-Verschlüsselung

27% Mehr-Faktor-Authentifizierung

(Quelle: 2020 Bundesverband IT-Sicherheit e.V.)

HOMEOFFICE

IST DIE ARBEIT VON ZU HAUSE AUS EINE BEDROHUNG FÜR DAS UNTERNEHMEN?

In Anbetracht der aktuellen Situation sind alle Unternehmen in Deutschland dazu angehalten, wenn möglich ihre Mitarbeiter von zu Hause aus arbeiten zu lassen. Dieses Modell der Arbeit wirft jedoch Fragen nach der Sicherheit des Unternehmens auf. Insbesondere die begrenzten Möglichkeiten zur Kontrolle der IT-Ressourcen stellen hier ein Problem dar. Die Verwendung nicht ordnungsgemäß gesicherter, privater Geräte für berufliche Zwecke oder die Verbindung von firmeneigenen Mobilgeräten in ungesicherten WLAN-Netzwerken setzt das Unternehmen einem erhöhten Risiko von Cyberattacken aus. Wie kann man sich während der Arbeit im Home-Office wirksam vor diesen schützen?

Angriffe auf Smartphones

Die Arbeit von zu Hause aus war in vielen Unternehmen bisher ein Privileg. Jetzt ist sie oft die einzige Möglichkeit, den Betrieb am Laufen zu halten. Deshalb ist es wichtig, Sicherheitsprozeduren zu etablieren, die den Einsatz von mobilen Geräten für Geschäftszwecke regeln. Angriffe richten sich häufig gegen Smartphones, auf denen Mitarbeiter private Anwendungen installieren. Diese verschaffen sich Zugriff auf sensible Systemressourcen und Daten, einschließlich Firmenkontakten und GPS-Informationen. Laut des jüngsten Cisco „2020 CISO Benchmark Report" gaben mehr als die Hälfte (52%) der Cyber-Security-Spezialisten an, dass mobile Geräte derzeit für sie nur sehr schwer zu schützen sind. Um das Risiko eines illegalen Zugriffs auf sensible Informationen zu minimieren, lohnt es sich, eine Geschäftsdaten von privaten Daten trennende Lösung zu implementieren. Hier hilft ein Enterprise Mobility Management, mit der IT-Administratoren auf Unternehmens-Smartphones zwei, voneinander getrennte Profile für geschäftliche und private Nutzung erstellen können. Selbst wenn ein Mitarbeiter dann eine infizierte Anwendung in sein privates Profil herunterlädt, erhalten Cyberkriminelle keinen Zugang zu vertraulichen Unternehmensdaten.

IT-Sicherheit in Zeiten des Heimarbeitsplatzes

Wenn die Büros leer sind und die Arbeit nach Hause verlegt wird, müssen IT-Teams besonders vorsichtig sein. Aufgrund des fehlenden physischen Zugangs zu den Geräten des Unternehmens müssen die Administratoren ihre IT-Umgebung per Fernzugriff verwalten. Dies gelingt am besten mit Hilfe einer Unified Endpoint Management (UEM) Lösung, die es ermöglicht, die Software auf allen Unternehmens-Laptops aus der Ferne zu aktualisieren. Um effektiv für die Sicherheit aller Endgeräte zu sorgen, muss die IT-Infrastruktur zunächst grundlegend überprüft und erfasst werden: Hardware, Betriebssysteme, Anwendungen und Lizenzen. Erst mit diesen Informationen können die Administratoren die Geräte sicher verwalten und zum Beispiel notwendige Patches installieren beziehungsweise eine automatisierte Installation veranlassen.

Fazit

Unternehmen, die ihre Mitarbeiter ins Home-Office schicken, verlieren zwangsläufig ein Stück Kontrolle über die eigene IT-Infrastruktur. Umso wichtiger ist es daher, dass die IT-Abteilungen über wirksame Werkzeuge zur Fernwartung und -verwaltung der Home-Office-Geräte verfügen. Die Investition in eine UEM-Lösung verringert hier deutlich das Risiko Opfer von Cyberattacken zu werden. Insbesondere ein automatisiertes Patch Management hilft dabei, die Geräte vor Angriffen über bekannte Schwachstellen zu schützen.

Alexander Haugk

DIE INVESTITION IN EINE UEM-LÖSUNG VERRINGERT DEUTLICH DAS RISIKO VON LAPTOPS UND SMARTPHONES, OPFER VON CYBERATTACKEN ZU WERDEN.

Alexander Haugk,
Product Manager, baramundi software AG,
www.baramundi.com

SCHNELL UND SICHER

OVER-THE-AIR-UPDATES FÜR VERNETZTE FAHRZEUGE

Über Funkverbindungen spielen Automobilhersteller aus der Ferne wichtige Software-Updates auf Fahrzeuge auf – eine Herkulesaufgabe mit Tücken. Mit dem Content Delivery Network von Akamai gelingt das schnell und sicher.

In heutigen vernetzten Fahrzeugen sind bis zu 100 Steuergeräte verbaut, die mit ihrer Software nahezu alle Funktionen kontrollieren. Die Software mit Updates auf dem neuesten Stand zu halten, ist damit wichtiger denn je. Software-Aktualisierungen fügen Fahrzeugen neue Funktionen hinzu, beheben Fehler, lösen technische Probleme und sorgen für Sicherheit. Je schneller und sicherer ein Update bereitgestellt wird, umso besser.

Sicher und effizient werden die Aktualisierungen Over-the-Air über eine Funkschnittstelle wie WLAN oder das Mobilfunknetz an Millionen Fahrzeuge verteilt. Über eine einheitliche Schnittstelle verwalten Automobilhersteller die Software-Aktualisierungen nahtlos. So senken sie die Kosten über den gesamten Lebenszyklus eines Autos erheblich, denn Werkstattbesuche werden größtenteils überflüssig.

Content Delivery Network

Große Aktualisierungskampagnen sind für die Automobilhersteller allerdings eine Herkulesaufgabe, weil die Updates zuverlässig und in sehr kurzer Zeit erfolgen müssen. So lassen Fahrzeuge Funkverbindungen meist nur dann zu, wenn der Motor läuft. Durch Schwankungen in den Verbindungsgeschwindigkeiten und der Netzabdeckung reduziert sich die Übertragungsrate. Dadurch lässt sich das Update nicht rechtzeitig zustellen. Darüber hinaus öffnen sich über das Gateway des Mobilfunkproviders und das Rechenzentrum des Automobilherstellers Angriffsmöglichkeiten für Cyberkriminelle.

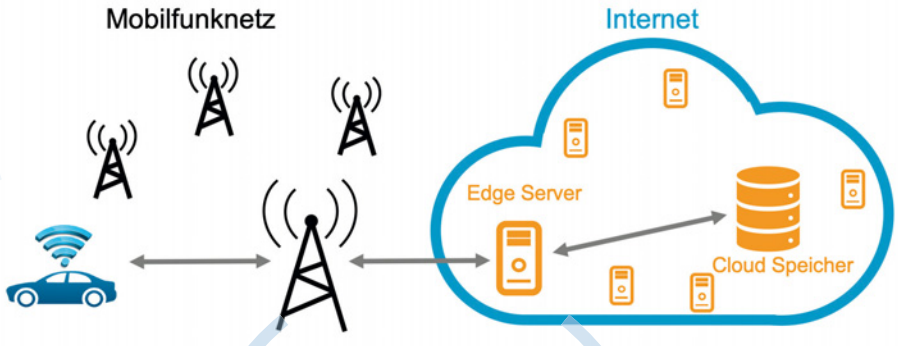
All diese Probleme löst ein Content Delivery Network (CDN) mit integrierten Sicherheitslösungen. Ein solches global verteiltes Netzwerk gewährleistet mithilfe von Optimierungstechnologien wie TCP-Beschleunigung und Edge Caching eine zuverlässige und sichere Datenübermittlung. Beim Edge Caching werden die Dateien auf Servern gespeichert. Fragt ein Endnutzer, also das Auto, die Software-Updates an, beantwortet ein nahegelegener Edge-Server anstelle des weit entfernten Ursprungsservers die Anfrage. Die Edge-Server stehen teilweise direkt bei den Gateways der Mobilfunkprovider. Somit ist gewährleistet, dass die Updates immer von dem Edge-Server ausgeliefert werden, der dem Fahrzeug am nächsten ist.

Vorteile ausschöpfen

Sicherheit hat bei den Edge-Servern oberste Priorität: Im Fahrzeug oder beim Händler sind nur Datenpakete von definierten IP-Adressen erlaubt, wodurch sich der Zugang zum Fahrzeug besser kontrollieren lässt. Für die Authentifizierung der Fahrzeuge werden zudem Client-Zertifikate oder Token-basierte Methoden unterstützt. Auch hier erfolgt die Authentifizierung so früh wie möglich direkt auf dem Edge-Server.

In Zukunft verspricht die nächste Mobilfunkgeneration mit 5G-Technik höhere Übertragungsraten und geringere Latenzen. Dadurch rückt das Internet noch näher an die Mobilfunkmasten heran. Eine hochverteilte und -skalierbare Plattform wie die Akamai Intelligent Edge Platform hilft auch hier, die Vorteile von 5G besser auszuschöpfen.

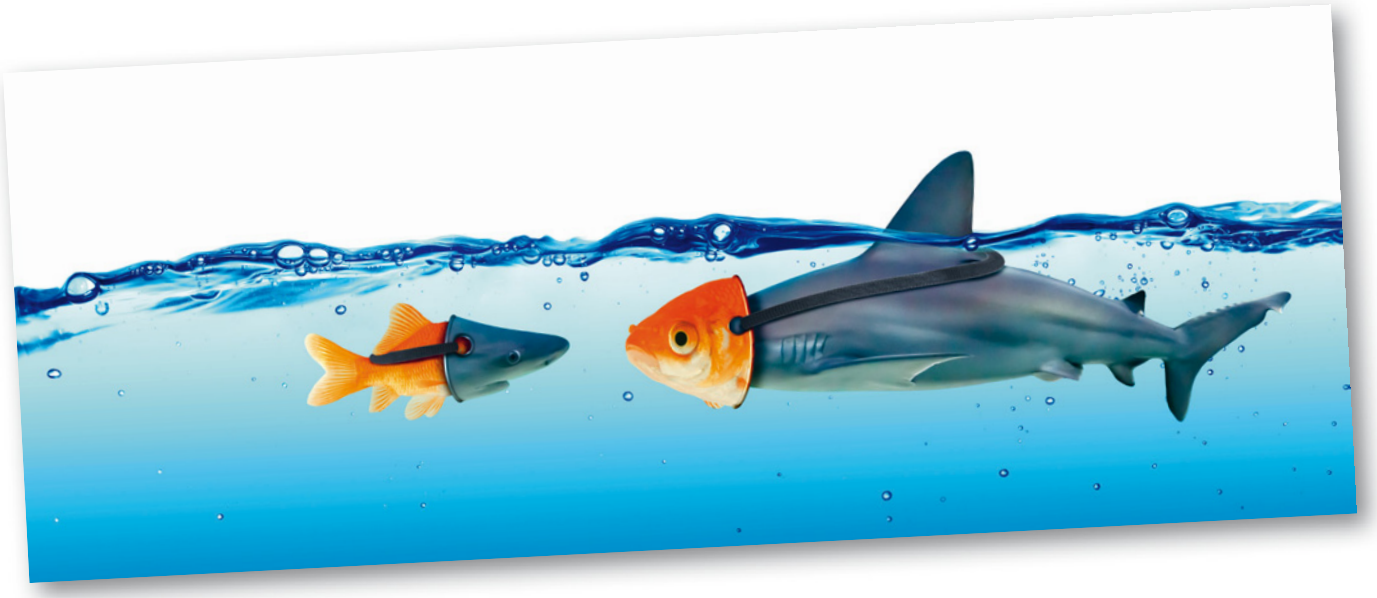
Eberhard Scheuble | www.akamai.com



Edge-Server versorgen die Fahrzeuge mit Daten über das Mobilfunknetz.

DIE EDGE PLATTFORM VON AKAMAI (Content Delivery Network)

Akamai liefert täglich 130 Terabyte Daten aus. Die Akamai Plattform interagiert mit 1,3 Milliarden Devices und erfasst über 100 Millionen IP-Adressen pro Tag. Der große Vorteil der Akamai Edge liegt in der direkten Integration von Sicherheitslösungen in die Plattform. Damit werden Cyber-Angriffe bereits an der Peripherie abgewehrt.



PRIVILEGIERTE ACCOUNTS

DECEPTION ALS LÖSUNG

Mit einer neuen Deception-Funktion, also einer Sicherheitstechnologie, die Täuschungsmanöver nutzt, unterbindet CyberArk den Diebstahl von privilegierten Zugangsdaten auf PCs, Workstations oder Servern. Sie hindert Cyber-Angreifer an einer längeren unerkannten Verweildauer oder der Seitwärtsbewegung im Unternehmensnetz.

Lokale Administratorrechte werden oft auf Endgeräten belassen, sodass sie zu attraktiven Zielen für Angreifer werden, da sie über diese Berechtigungen in das Unternehmensnetz eindringen können. CyberArk hat nun seinen Endpoint Privilege Manager um eine neue Deception-Funktion erweitert, um einen Angriff bereits im Anfangsstadium zu erkennen und proaktiv zu unterbinden. Bei Deception-Lösungen handelt es sich um Täuschungstools, die reale Systeme und Applikationen nachbilden und als Köder dienen. Die Lösung führt potenzielle Angreifer durch die Nutzung solcher Deception-Komponenten in die Irre und verhindert damit eine missbräuchliche Nutzung privilegierter Zugangsdaten.

Privilegierte Zugangsdaten auf Endgeräten sind nach wie vor eine Goldgrube für Angreifer. Malware für den Diebstahl von Credentials ist bereits verfügbar und leicht zu nutzen. Und was noch schlimmer ist: Sie ist sehr erfolgreich. Deception-Techniken werden deshalb zunehmend populär, da sie helfen, zum einen die Vorgehensweise eine Hackers zu verstehen und zum anderen Angriffe ins Leere laufen zu lassen."

Endpoint Privilege Manager

Der Endpoint Privilege Manager ist eine SaaS-basierte Lösung und Teil der Privileged Access Security Suite von CyberArk. Er ermöglicht Unternehmen, das Risiko eines nicht verwalteten administrativen Zugriffs auf Windows- und Mac-Endgeräte zu reduzieren. Zu den Funktionen gehören unter anderem:

- Just-in-Time-Bereitstellung und -Zugriff: Just-in-Time-Funktionen ermöglichen es Unternehmen, Risiken zu minimieren, indem sie Administrationszugriffe nur bei Bedarf und für eine bestimmte Zeitspanne bei vollständigem Audit-Protokoll gewähren – verbunden mit der Möglichkeit, die Zugriffsrechte jederzeit zu entziehen.

- Beschränkung der Zugriffsrechte: Durch die Umsetzung von Least-Privilege-Strategien können Unternehmen die Angriffsfläche reduzieren, da nicht benötigte lokale Administrator-Privilegien eliminiert werden; User erhalten nur diejenigen Rechte, die sie für ihre Tätigkeit benötigen.

- Credential-Schutz: Mit einem erweiterten Schutz können Unternehmen den versuchten Diebstahl von Zugangsdaten aufspüren und blockieren, sei es auf Endgeräten oder in Betriebssystemen, IT-Applikationen, Remote-Access-Anwendungen oder gängigen Webbrowsern.

Die Deception-Funktion, die auf den Diebstahl von IT-Admin-Zugangsdaten fokussiert, soll ab sofort im CyberArk Endpoint Privilege Manager verfügbar sein. Weitere Köder (Lures) etwa für Browser-Credentials sollen bald folgen.

www.cyberark.com/epm

E-MAILS IN DER CLOUD

SEPPMAIL SECURE E-MAIL-GATEWAY FÜR OFFICE 365

In vielen Unternehmen ist Office 365, die cloud-basierte Version des Office-Anwendungspaketes von Microsoft, nicht mehr wegzudenken. Ein Großteil der Nutzer macht sich jedoch keine Gedanken darüber, ob die offerierten Sicherheitsvorkehrungen ausreichen. So bietet Office 365 selbst beispielsweise keine umfangreiche DSGVO-konforme Verschlüsselung nach internationalen Standards für den E-Mail-Versand an. Mit dem Secure E-Mail-Gateway von SEPPmail hingegen erhalten Betriebe eine ergänzende Lösung für die zertifikatsbasierte Signatur und Verschlüsselung in der Office 365-Cloud.

Microsoft zählt mit seinen Anwendungen zu einem beliebten Ziel von Cyberkriminellen. Daher ist es für Firmen, die ihre E-Mail-Server als Online-Exchange in der Cloud betreiben, wichtig, geeignete Schutzmaßnahmen zu treffen. Denn bei dem Einsatz von E-Mail-Verschlüsselungslösungen sollten Hacker zu keinem Zeitpunkt in der Lage sein, entsprechende Schlüssel abzugreifen. Auch eine Spontanverschlüsselung ist nur bedingt sicher, wenn es lediglich einen einzigen Unternehmensschlüssel gibt. Entwendet ein Angreifer diesen, ist sogleich die gesamte Unternehmenskommunikation gefährdet. Hinzu kommt, dass eine E-Mail-Signatur über Zertifikate möglich sein sollte. SEPPmail hat sich auf diese Anforderungen spezialisiert und bietet seine Lösungen auch für Kunden an, die ihre E-Mail-Infrastruktur in Office 365 nutzen.

Datenschutzkonforme E-Mail-Kommunikation

Das Secure E-Mail-Gateway von SEPPmail lässt sich problemlos in den Office 365-Mailstrom integrieren. Dabei bleibt Exchange Online unverändert die zentrale Stelle für den E-Mail-Verkehr, und Sicherheitsfeatures wie Anti-Virus oder Anti-Spam kommen weiterhin zum Einsatz.

SEPPmail unterstützt alle gängigen Standards wie S/MIME, OpenPGP, Domainverschlüsselung und TLS. Verfügt der Empfänger über eigenes Schlüsselmaterial, kommt beim E-Mail-Versand die jeweils beste Methode automatisch zum Einsatz. Der private Schlüssel liegt hierbei ununterbrochen in der Infrastruktur des Kunden. Die patentierte GINA-Technologie erlaubt zudem die verschlüsselte Spontankommunikation mit Adressaten, die selbst keine Verschlüsselungslösung verwenden. Das Verfahren benötigt weder beim Absender noch beim Empfänger eine zusätzliche Softwareinstallation. Alle E-Mails lassen sich wie gewohnt empfangen und werden nach einer kurzen Passworteingabe entschlüsselt. Hier gibt es allerdings nicht nur einen übergreifenden Unternehmensschlüssel, sondern jeder Empfänger besitzt einen eigenen Schlüssel. So wird auch bei Office 365 ein sicherer, vertraulicher und unkomplizierter Informationsaustausch gewährleistet.

Zertifikatsbasierte E-Mail-Signatur

Um die Identität des Unterzeichners nachzuweisen, beherrscht die SEPPmail-Appliance außerdem die RFC-konforme Signatur über Zertifikate. Dadurch lässt sich belegen, dass E-Mails vom entsprechenden Absender stammen und auf dem Versandweg nicht verändert wurden. Bei Erstversand beantragt die SEPPmail-Appliance vollautomatisiert ein Zertifikat bei einer der akkreditierten Zertifizierungsstellen, den sogenannten Certificate Authorithies. Im Anschluss wird die E-Mail im Namen des Benutzers signiert und derart dessen Herkunft und Integrität bekräftigt.

Large File Transfer (LFT)

Zu guter Letzt erweitert SEPPmail Office 365 um die Funktion des vollintegrierten LFT, dank dem sich auch übergroße Dateien verschlüsselt versenden lassen. Hierfür gibt es ein Extra-Add-In für den Outlook-Client.

Günter Esch | www.seppmail.de

SEPPMAIL

BLOCKCHAIN

IDENTITÄTSMANAGEMENT IN DER DIGITALEN WELT

DIGITALE IDENTITÄTEN, DIE AUF DER BLOCKCHAIN BASIEREN, SORGEN FÜR VERTRAUEN UND ADRESSIERBARKEIT IN DIGITALEN PROZESSEN. DAS POTENZIAL DER DISTRIBUTED-LEDGER-TECHNOLOGIE GEHT ABER WEIT DARÜBER HINAUS: DIE BLOCKCHAIN ERÖFFNET UNS NEUE MÖGLICHKEITEN IN VIELEN BEREICHEN UND INDUSTRIEN.

Katarina Preikschat,
Blockchain Portfolio Developer,
MHP Management- und IT-Beratung GmbH,
www.mhp.com

In der analogen Welt ist die Feststellung der Identität einer Entität vergleichsweise simpel. In der Regel genügt es, bestimmt Attribute in Augenschein zu nehmen und eventuell mit einer Urkunde abzugleichen. Ein Mensch zeigt dann sein Gesicht und bei Bedarf seinen Ausweis, um nachzuweisen, dass er wirklich er selbst ist. Bei einem Fahrzeug beispielsweise dienen dazu die Vehicle Identification Number (VIN) und der Fahrzeugschein, bei einer Maschine sind es die Seriennummer und das Typenschild. Wichtig dabei: Die Verknüpfung von Entität und Urkunde muss von einer vertrauensvollen Instanz vorgenommen werden.

In der digitalen Welt ist das alles deutlich schwieriger, weil der Augenschein hier nur bedingt funktioniert. Das ist problematisch, weil in vielen digitalen Prozesse irgendwann eine Identitätsfeststellung erforderlich ist. Kann diese nicht auch digital erfolgen, kommt der Prozess zum Erliegen oder wird erheblich verlangsamt. Digitale Identitäten können für Abhilfe sorgen: Entitäten werden dann statt durch analoge Attribute durch digitale Attribute repräsentiert. Das sind in Bezug auf Menschen typischerweise Benutzernamen und Passwörter. In einigen Fällen kommen auch digitalisierte biometrische Daten zum Einsatz. Bei Fahrzeugen, Maschine und anderen Devices werden in der Regel Nummern bzw. Codes genutzt. Elaborierter sind digitale Signaturen und digitale Zertifikate, weil diese mit Bezug auf bestimmte Instanzen auch die Überprüfung von bislang unbekannten digitalen Identitäten zulassen.

Aus unserer Sicht nimmt vor allem die Bedeutung von digitalen Identitäten für Hardware zu, weil immer mehr Devices im Internet of Things miteinander interagieren. Vor diesem Hintergrund sind drei Aspekte erfolgskritisch.

1. Verlässliche Verknüpfung von Entität und digitaler Identität

Es muss sichergestellt werden, dass Entität und digitale Identität unzweifelhaft miteinander verknüpft sind. Das kann durch eine vertrauensvolle Instanz geschehen. Die Schwierigkeit dabei: Bei der absehbaren Zunahme von vernetzbarer Hardware und der damit steigenden Nachfrage nach digitalen Identitäten kann eine solche Instanz rasch zum Bottleneck werden.

2. Schutz vor Missbrauch durch Dritte

Bei digitalen Identitäten besteht grundsätzlich die Gefahr, dass Dritte sich diese missbräuchlich aneignen und nutzen. Insofern gilt es, den Schutz digitaler Identitäten kontinuierlich auszubauen. Das bezieht sich zum einem auf die Speicherorte, die gegen Angriffe geschützt werden müssen. Das betrifft aber auch die Authentisierungs- bzw. Authentifizierungsverfahren.

3. Nachvollziehbarkeit der Daten

Digitale Identitäten können auch dafür genutzt werden, Daten über den Lebenszyklus eines Devices hinweg zu sammeln. Wichtig ist dabei, dass die Interaktionspartner die Herkunft und Echtheit der außerhalb des Devices abgelegten Daten nachvollziehen können. Dazu sind Signaturen geeignet.

Um diese drei Aspekte möglichst optimal zu handhaben, hat sich das Identitätsmanagement (IdM) bzw. das Identity and Access Management (IAM) herausgebildet und konkretisiert. So definiert beispielsweise die Norm ISO/IEC JTC 1/SC 27/WG 5 A framework for IdM drei Aufgaben eines Identitätsmanagements: den Identifikationsprozess einer Entität (samt optionaler Authentisierung), die Information, die mit der Identifikation einer Entität innerhalb eines bestimmten Kontexts verbunden ist, und die sichere Verwaltung von Identitäten.

Blockchain als Enabler

Um es klar zu sagen: Beim Management von digitalen Identitäten stehen wir noch vergleichsweise weit am Anfang. Für einen Teil der bestehenden Herausforderungen eignet sich aus unserer Sicht sehr gut die Distributed-Ledger-Technologie Blockchain. Denn aufgrund ihrer spezifischen Architektur lassen sich in einer Blockchain digitale Identitäten von Hardware-Entitäten sicher, unveränderbar und nachvollziehbar kreieren und speichern.

So zum Beispiel bei Automobilen. Hier steht aktuell nicht nur der Wechsel vom Verbrennungs- zum Elektromotor an. Es findet auch mit hoher Dynamik die digitale Transformation statt. Auf den Punkt bringt diese Entwicklung das Akronym CASE: Fahrzeuge werden connected, autonomous, shared, und electrified. Und damit interagieren sie als Entitäten auf vielfache Weise mit ihrer Umwelt – durch die zunehmende Vernetzung der Mobilitätswelt mit anderen Bereichen wie dem Energiesektor oder dem Finanzwesen steigt die Menge an Interaktionspunkten drastisch. Eine verlässliche digitale Identität wird unbedingt erforderlich.

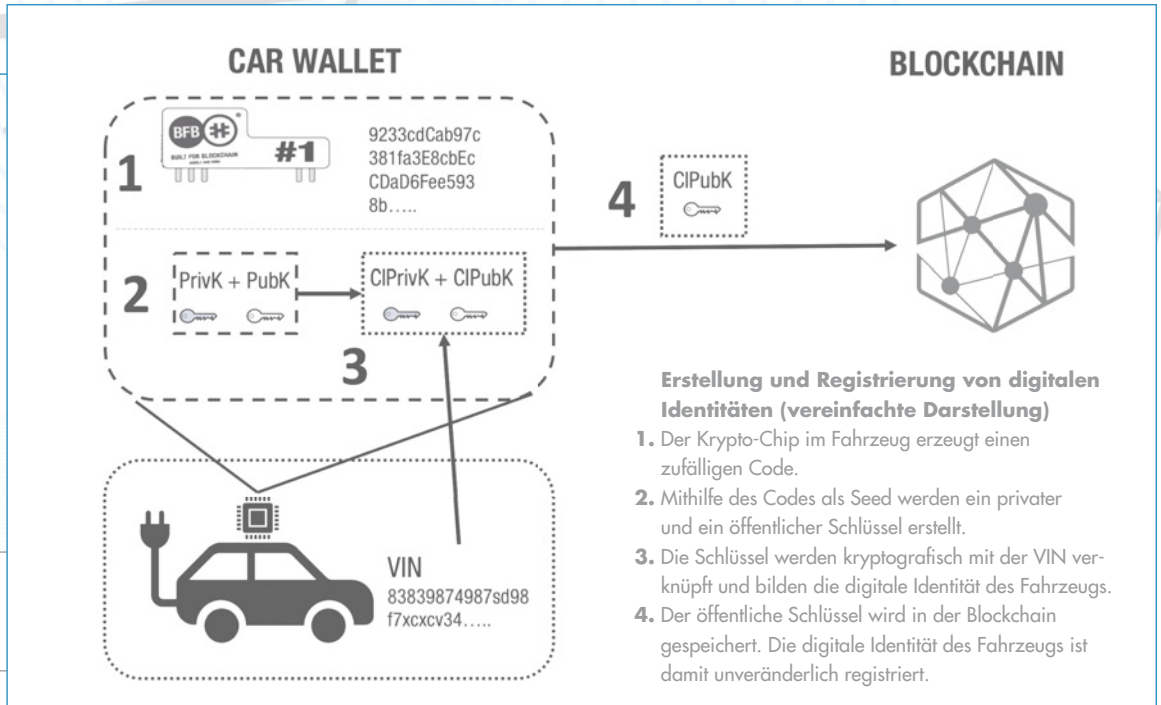
So lassen sich etliche Anwendungen finden, bei denen es auf eine eindeutige Identifikation eines Fahrzeugs ankommt: etwa bei der Einfahrt in einen beschrankten Bereich, beim automatisierten Laden eines Elektrofahrzeugs samt Payment oder dessen Teilnahme im Balancing eines Stromnetzes. Der eindeutige Identitätsnachweis kann auch andersherum notwendig sein: wenn zum Beispiel eine Kamera für die Verkehrsüberwachung dem Connected Car mitteilt, dass sich ein Fußgänger nicht sichtbar in der Kurve befindet und deshalb gebremst werden sollte. Das Fahrzeug muss sich bei solchen Informationen unbedingt auf den Sender verlassen können. Und: Eine verlässliche digitale Identität ist auch mit Blick auf die zu einem Fahrzeug gespeicherten Daten wichtig.

Die Vehicle Identification Number genügt nicht

Die VIN ist zwar eine eindeutige Identität. Als digitale Identität eignet sich diese aber nur bedingt. Denn sie ist offen angebracht und für jeden erkennbar. Das ist natürlich beabsichtigt, damit eine Identitätsfeststellung in der analogen Welt durch Augenschein erfolgen kann. Gleichzeitig ermöglicht das allerdings auch Dritten, eine fremde VIN in digitalen Prozessen zu missbrauchen.

Benötigt wird also eine weitere Nummer, die mit der VIN verknüpft, aber nicht offen zugänglich ist. Theoretisch könnte diese von einer vertrauensvollen Instanz vergeben und gespeichert werden – naheliegend ist in Deutschland das Kraftfahrt-Bundesamt. Damit ergeben sich allerdings drei Schwierigkeiten: Erstens kann sich die Instanz als Engstelle erweisen. Zweitens ist die zentrale Speicherung anfällig für Angriffe und Missbrauch. Und drittens lässt sich so kaum die von einem Fahrzeug erzeugten und übermittelten Daten sicher signieren und verlässlich überprüfen.

Durch den Einsatz einer Blockchain kann all dem wirkungsvoll begegnet werden. Das Unternehmen Riddle&Code aus Wien hat dafür ein Hard- und Software-basiertes Verfahren entwickelt, das wir auch in unserem gemeinsamen Whitepaper „The Automotive Sector and Blockchain" beschreiben. Startpunkt ist die sichere Verknüpfung der Fahrzeug-Entität mit einer digitalen Identität. Dafür wird möglichst schon bei der Herstellung ein Krypto-Chip embedded im Fahrzeug verbaut. Dieser erzeugt initial einen oder mehrere zahlenbasierte öffentliche und private Schlüssel, die logisch mit der VIN verbunden werden. Der öffentliche Schlüssel wird in einer Blockchain gespei-



Future Mobility
(Quelle: Riddle&Code)

Erstellung und Registrierung von digitalen Identitäten (vereinfachte Darstellung)

1. Der Krypto-Chip im Fahrzeug erzeugt einen zufälligen Code.
2. Mithilfe des Codes als Seed werden ein privater und ein öffentlicher Schlüssel erstellt.
3. Die Schlüssel werden kryptografisch mit der VIN verknüpft und bilden die digitale Identität des Fahrzeugs.
4. Der öffentliche Schlüssel wird in der Blockchain gespeichert. Die digitale Identität des Fahrzeugs ist damit unveränderlich registriert.

chert, der private Schlüssel verbleibt ausschließlich auf dem Krypto-Chip. Während des gesamten Lebenszyklus des Fahrzeugs werden beide Schlüssel verwendet, um bei sämtlichen Transaktionen bzw. Interaktionen die Identität und Herkunft von Daten zu überprüfen. Das Fahrzeug übermittelt Daten wie beispielsweise den Kilometerstand, die mit dem Fahrzeug-spezifischen privatem Schlüssel signiert wurden. Den öffentlichen Schlüssel nutzen die Interaktionspartner, um zu validieren, ob die Daten tatsächlich von der Entität stammen. Dadurch entsteht eine systematisch sichere Verbindung zwischen der digitalen Identität und den verknüpften Daten (gesamt: Digital Twin) des Fahrzeugs in der Blockchain.

In sechs Schritten zum Blockchain-basierten Identitätsmanagement

Was für Fahrzeuge gilt, lässt sich grundsätzlich auch auf viele andere Devices übertragen. Allerdings: Auch wenn sich die Blockchain als Technologie hervorragend eignet, reicht das allein nicht aus! Vor allem werden verbindliche Konventionen benötigt, auf die sich alle Partner aus Gesellschaft, Politik und Wirtschaft verständigen. Und mehr noch: Die einzelnen Partner müssen bereit sein, Kooperationen einzugehen, um Standards zu entwickeln und eine der Grundlagen der Blockchain-Technologie – das verteilte Netzwerk – mitbetreiben zu können. Das ist vor allem für Unternehmen ein gewaltiger Schritt, die in der Regel nicht Cooperation, sondern Competition gewohnt sind. Für sie sollte Coopetition das neue Credo sein. Die Mobility Open Blockchain Initiative (MOBI) macht in diesem Zusammenhang Hoffnung. Weltweit arbeiten mehr als 30 OEM, Zulieferer und IT-Unternehmen in dem Konsortium zusammen, um genau solche Standards zu entwickeln. Ein wichtiger Aspekt sind dabei die unterschiedlichen rechtlichen Vorgaben zum Umgang mit Daten, vor allem mit personenbezogenen Daten. In Europa ist hier die DSGVO maßgeblich. Explizite Aussagen fehlen dazu bislang aber noch.

Unternehmen müssen aber nicht abwarten, um selbst aktiv zu werden: Wollen sie die vielen Potenziale der Blockchain für sich nutzen, sollten sie sich schon heute mit der Technologie befassen. Die digitale Identität ist dabei ein sehr zentraler Anwendungsfall. Aber sie ist auch nur ein Use Case. Kreieren lassen sich viele mehr.

Erfolgsversprechend ist nach unserer Erfahrung in einer ganzen Reihe von Projekten in der Praxis ein schrittweises Vorgehen:

Schritt 1: Education

Wichtig ist zunächst, dass Unternehmen Wissen zu der vergleichsweise neuen Technologie aufbauen. Dazu gehört auch, eine realistische und kritische Haltung zu entwickeln. In der Blockchain steckt ohne Zweifel enormes Potenzial – und sie ist weit mehr als ein Hype. Allerdings ist die Blockchain auch nicht die Antwort auf alle Fragen.

Schritt 2: Ideation

Insofern sollten Unternehmen konkrete Szenarien identifizieren, bei denen sich der Einsatz der Blockchain anbieten könnte. Hilfreich sind dabei Design-Thinking-Workshops mit interdisziplinär besetzten Teams. Wichtig: Zunächst muss ein tatsächliches Problem identifiziert werden, bevor die Blockchain als mögliche Lösung in Betracht gezogen wird.

Schritt 3: Evaluation

Die skizzierten Ideen sollten daraufhin – zum Beispiel mit dem Blockchain Canvas von MHP – evaluiert werden, ob die Blockchain bzw. welche Art von Blockchain tatsächlich passt und ob sie die beste Technologie ist, um die formulierten Anforderungen zu erfüllen. Möglicherweise stellt sich dabei heraus, dass sich eine andere Distributed-Ledger-Technologie viel besser eignet. Oder dass ein ganz anderer Ansatz verfolgt werden muss.

Schritt 4: Conception

Matchen Use Case und Blockchain sollte die spezifische Blockchain-Architektur konzipiert werden. Dazu gehört auch, die relevanten Partner im jeweiligen Ökosystems zu identifizieren und die richtigen Partner zu finden.

Schritt 5: Prototyping

In Rahmen eines Proof of Concept sollte ein Prototyp realisiert und getestet werden. So ist schnell erkennbar, ob der Use Case machbar ist und an welchen Stellen noch nachjustiert werden muss.

Schritt 6: Integration

Funktioniert der Prototyp wie er soll, sollte er zum Produkt weiterentwickelt und bei Bedarf in bestehende Systeme integriert werden – um auf diese Weise zum Beispiel das ERP-System sinnvoll zu ergänzen.

Katarina Preikschat

WHITEPAPER

Die Management- und IT-Beratung MHP und der Blockchain-Spezialist Riddle&Code haben gemeinsam das Potenzial der Blockchain-Technologie für die Mobilitätsbranche untersucht. Die Erkenntnisse sind im kostenlosen Whitepaper „The Automotive Sector and Blockchain" zusammengestellt.

Das Papier kann auf der Seite von MHP heruntergeladen werden: https://www.mhp.com/de/services/focus-topics/blockchain

KÜNSTLICHE INTELLIGENZEN

OPTIMALES ERGEBNIS FÜR DIE IT-SECURITY

In der IT-Welt wird noch ein Großteil der Tätigkeiten vom Menschen vollzogen. Computer werden meist nur als unterstützende Komponenten oder als Hilfsmittel eingesetzt, beispielsweise Taschenrechner, doch dies liegt deutlich unter dem Potenzial moderner Computer.

Als konkretes Beispiel im Bereich des Penetrationstests, kurz Pentest, ist der Computer zwar das Hauptarbeitsmittel, jedoch werden diese von Menschen bisher ausschließlich orchestriert, um aktiv nach Sicherheitslücken zu suchen.

Künstliche Intelligenzen (KIs) sollten menschliches Handeln und die dazugehörige Wahrnehmung automatisieren. Dies funktioniert – wie beim Menschen – anhand von Erfahrungen, durch die sich Menschen und Computer grundlegend unterscheiden. Menschen können vergleichsweise schnell lernen, Computer dagegen brauchen dafür Unmengen an Daten.

DIE ZUSAMMENARBEIT ZWISCHEN MENSCH UND MASCHINE WIRD IN DER ZUKUNFT ENTSCHEIDENDER ALS JE ZUVOR SEIN, UM OPTIMALE ERGEBNISSE LIEFERN ZU KÖNNEN.

Emile Hansmaennel, Cybersecurity, Sogeti Deutschland GmbH, www.sogeti.de

Bereits existierende Anwendungsbereiche

Einige Wirtschaftszweige haben die KI für sich entdeckt und in ihren alltäglichen Ablauf eingepflegt, um Aufgaben zu optimieren. Amazon setzt KIs zur Prognose der Nachfrage ein, in der Landwirtschaft werden KIs zur Schädlingserkennung genutzt und der Bereich des Autonomen Fahrens wird fast ausschließlich von KIs bestimmt.

Herausforderungen: Lernen ohne Wissen

Um zu verstehen, warum die Verwendung von KIs in der IT-Security noch nicht weit fortgeschritten ist, muss verstanden werden, wie diese Mechanismen lernen. Dies geschieht anhand von riesigen, bereits existierenden Datenmengen, die am Ende des Pentests aus Datenschutzgründen vernichtet werden und somit nicht als Trainingsdaten verwendet werden können. Es ist somit mithilfe der im Pentest generierten Daten nicht möglich, KIs zu trainieren, da das Wissen welches benötigt wird, nicht mitgeteilt werden darf.

Um KIs verwenden zu können, müssten alle in einem Pentest gesammelten Daten anonymisiert werden, um keine Rückschlüsse auf einen Kunden zu hinterlassen. Dies ist quasi unmöglich, da in einem Web-Pentest, bei dem unter anderem Anfragen an den Server untersucht werden, die meisten Anfragen an einen Webserver den Namen des Kunden beinhalten. Würde man diese rausfiltern, würden grundlegende Funktionalitäten kaputt gehen.

Um trotzdem eine KI zu trainieren, müssen Daten aus einer anderen Quelle bezogen werden. Dies kann jedoch erst mal nur sehr allgemein passieren, da die Daten, wie bereits beschrieben, datenschutzkonform behandelt werden müssen. Eine weitere Möglichkeit wäre es, frei verfügbare Daten aus dem Internet zu nutzen. Das Problem hierbei ist, das kein Standard für Sicherheitslücken existiert, da diese zu unterschiedlich sein können. Dadurch ist es nicht ohne weiteres möglich, einer KI allgemein alle Arten von bekannten Sicherheitslücken beizubringen.

Fazit

KIs werden nicht die Lösung für alles sein, denn eines fehlt ihnen: Intuition. Tipps aus internen Quellen sowie sehr neue Fehler, zu denen noch nicht viele Daten existieren, können der KI nicht einfach mitgeteilt werden. Das Zusammenspiel wird wichtiger denn je, denn so können die Schwachstellen des jeweils anderen ausgeglichen und ein optimales Ergebnis geliefert werden.

Emile Hansmaennel

SECURE ACCESS SERVICE EDGE (SASE)

KONVERGENTE TECHNOLOGIEN FÜR SICHERHEIT IN DER CLOUD

Mit wachsenden digitalen Geschäftsanforderungen investieren Unternehmen massiv in die Erweiterung ihrer Netzwerkverbindungsfähigkeiten, um sicherzustellen, dass ihre Daten den richtigen Personen zur richtigen Zeit zur Verfügung stehen. Insbesondere für Cloud-basierte, hochgradig vernetzte und agile Geschäftsmodelle ist die Gewährleistung eines ordnungsgemäßen Zugriffs auf Daten und Systeme unerlässlich. Zusammen mit der Konnektivität in immer komplexeren Infrastrukturen wachsen auch die Anforderungen an Netzwerk- und Datensicherheit. Wenn nicht die richtigen Schutzvorkehrungen getroffen werden, können Bedrohungen, die von Datenlecks und Fehlkonfigurationen bis hin zu Risiken durch Insider reichen, in jedem komplexen Cloud- und Netzwerkökosystem ihr Schadenspotenzial entfalten

An dieser Stelle kommt das Secure Access Service Edge (SASE) Konzept ins Spiel, ein Akronym, das vom Analystenhaus Gartner geprägt wurde. Der Netzwerkperimeter wird dabei nicht als Standort, sondern als ein Satz dynamischer Edgefunktionen, die bei Bedarf als Service aus der Cloud bereitgestellt werden, verstanden. SASE bezeichnet also eine Architektur, die Lösungen bereitstellt, die aus der Konsolidierung von Netzwerk- und Sicherheitswerkzeugen entstehen. Dieses Zusammenspiel gewährleistet sowohl einen effektiven als auch sicheren Zugang zu den IT-Ressourcen von Unternehmen.

Verschiedene Möglichkeiten

Die Kombination von Sicherheitstechnologien mit WAN-Technologien kann sich aus verschiedenen konvergierenden Technologien zusammensetzen, wie beispielsweise den folgenden:

➤ **CASB** – Ein Cloud Access Security Broker (CASB) ermöglicht die Durchsetzung von Richtlinien, um Daten vor Bedrohungen in der Cloud und auf jedem Gerät an jedem beliebigen Ort zu schützen. Anforderungen an einen CASB sind unter anderem Sichtbarkeit von und Bereinigung nach risikoreichen Ereignissen, proaktive Sicherheitsfunktionen, sowie Schutz sowohl vor bekannten wie auch unbekannten Datenverlust-Risiken und Malware-Bedrohungen.

CASBs werden in verschiedenen Varianten angeboten. API-CASBs nutzen den API-Zugriff auf SaaS-Anwendungen, um auftretende Datenlecks zu schließen. Mit ihnen lässt sich also ausschließlich reaktiv operieren. Die erste Generation der Multi-Mode-CASBs hingegen nutzt eine API-Integrationen sowie Forward Proxies und bietet damit die Sichtbarkeit aller Cloud-Daten sowie proaktive Sicherheitsfunktionen. Jedoch verfügen sie lediglich über signaturbasierten Schutz für bekannte Malware und Datenverlustwege und dies nur bei bestimmten Anwendungen. Der Zugriff von nicht-verwalteten Geräten auf Cloud-Anwendungen beispielsweise kann damit nicht geschützt werden.

Eine Lücke, die durch Multi-Mode-CASBs der neuesten Generation geschlossen wird: Sie passen sich dynamisch an, um

jegliche Anwendungen vor bekannten und unbekannten Datenverlust-Risiken und Malware-Bedrohungen zu schützen. Sie nutzen zusätzlich Reverse Proxys, womit Cloud-Daten auch beim Zugriff über nicht-verwaltete Endgeräte geschützt sind.

➤ **Secure Web Gateway (SWG)** – SWGs bieten URL-Kategorisierung und -Reputation sowie Schutz vor Bedrohungen. Sie stellen sicher, dass Personen nur eine angemessene Internetnutzung aufweisen, und schützen gleichzeitig vor Bedrohungen wie Phishing-Websites und Malware. Diese Technologien können auch Intrusion Prevention-Systeme (IPS), Intrusion Detection-Systeme (IDS) und Firewall-Funktionen umfassen.

➤ **Zero Trust Network Access (ZTNA)** – ZTNA sorgt für den sicheren Zugriff auf Unternehmensanwendungen, die entweder in der öffentlichen Cloud oder in firmeneigenen Netzwerken gehostet werden. Wenn Remote-Mitarbeiter auf bestimmte IT-Ressourcen zugreifen, erhalten sie oft vollen Zugriff auf alles im Netzwerk. Das Risiko für Datenverluste ist dabei allerdings überaus hoch. ZTNA erlaubt Nutzern lediglich den Zugriff auf bestimmte Anwendungen. Eine VPN-Verbindung ist dafür nicht erforderlich.

➤ **DNS-Schutz** – Domain Name System (DNS)-Technologien suchen in den Domains nach Risiken und Bedrohungen, wie zum Beispiel bekannten Malware-Hosts. Werden Bedrohungen entdeckt, kann der entsprechende DNS-Server mit einem Sinkhole-Zugriff antworten, um die Malware-Infektion zu verhindern.

➤ **Firewall-as-a-Service (FWaaS)** – FWaaS-Tools bieten Port-, Protokoll- und applikationsbasierte Richtlinien für den Netzwerkzugriff und die Segmentierung. Sie können auch Module für Dienstgüte (QoS), IPS, IDS und VPNs bereitstellen.

➤ **SD-WAN** – Dabei handelt es sich um eine MPLS-Alternative (Multi-Protocol Label Switching) für die Site-to-Site-Verbindung um einen sicheren Netzwerkzugang bereitzustellen. Darüber hinaus gibt es auch WAN-Beschleunigung oder -Optimierung zwischen getrennten Standorten, wie zum Beispiel Büros und Rechenzentren.

SASE: Verschiedene Wege in der Umsetzung

Die Einführung von Secure Access Service Edge-Architekturen wird weiter vorangetrieben durch zunehmend heterogene Geräteumgebungen und die voranschreitenden mobilen Nutzergewohnheiten in Unternehmen. Mitarbeiter greifen unterwegs auf Unternehmensanwendungen und -daten von Unternehmensgeräten aus zu oder nutzen ihre eigenen Laptops in der Erwartung, ohne Einschränkungen auch am Flughafen oder im Coffeeshop arbeiten zu können. Einige Mitarbeiter, zum Beispiel im Außendienst tätige, gehen womöglich überhaupt nicht in die Unternehmensumgebung. Unabhängig davon gibt es inzwischen eine große Anzahl verschiedener Zugangspunkte, die die Herausforderungen bei der Sicherung von Daten in der Cloud und im Netzwerk darstellen.

DIE KOMBINATION VON SICHERHEITSTECHNOLOGIEN MIT WAN-TECHNOLOGIEN KANN SICH AUS VERSCHIEDENEN KONVERGIERENDEN TECHNOLOGIEN ZUSAMMENSETZEN.

Mike Schuricht, VP Product Management, Bitglass, www.bitglass.com

So bilden sich bei der Umsetzung des Secure Access Service Edge-Konzepts gegenwärtig zwei verschiedene Ansätze heraus:

➤ **1. Appliance und einfache Endpoint-Agenten:** Dabei werden physische Appliances im Rechenzentrum des Unternehmens platziert, um die von den Organisationen angestrebte Sicherheit und Kontrolle zu gewährleisten. Sämtlicher Datenverkehr wird dabei von den Endpoint-Agenten auf den Geräten der Mitarbeiter an die Appliance weitergeleitet. Durch diesen Hop im Netzwerk entsteht eine Latenzzeit, die besonders bei großen Organisationen mit tausenden von Benutzern problematisch ist. Da die Kosten für Verwaltung und Aufrüstung verhältnismäßig hoch sind, ist dieser Ansatz vor allem für die Verarbeitung von massenhaftem Datenverkehr zu unflexibel.

➤ **2. Intelligente Endpoint-Agenten und Cloud-Proxy-Technologien:** Dieser über einen Cloud-Service bereitgestellte Ansatz bietet eine Möglichkeit, die Aktivitäten auf jedem Gerät zu kontrollieren, indem die Netzwerkkontrolle und die Cloud-Sicherheit vom Perimeter bis hinunter zu den Endpoints selbst verlagert werden. Dies beseitigt die Abhängigkeit von physischen Appliances sowie die Nachteile der durch Backhauling-Verkehr verursachten Latenzzeiten und ist insgesamt flexibler.

Derzeit ist noch kein Anbieter in der Lage, das gesamte Portfolio an SASE-Funktionen bereitzustellen, jedoch gibt es einige, die jeweils über den Großteil der erforderlichen Funktionen verfügen. Der Ausbau der Netzwerkinfrastruktur treibt bei Organisationen weltweit jedoch den Bedarf an umfassenderen Lösungen, die ihren wachsenden Anforderungen gerecht werden können, weiter voran. Mit der fortschreitenden Cloud-Nutzung wird sich dieser Markt im Jahr 2020 voraussichtlich rasant entwickeln.

Mike Schuricht

BIOS

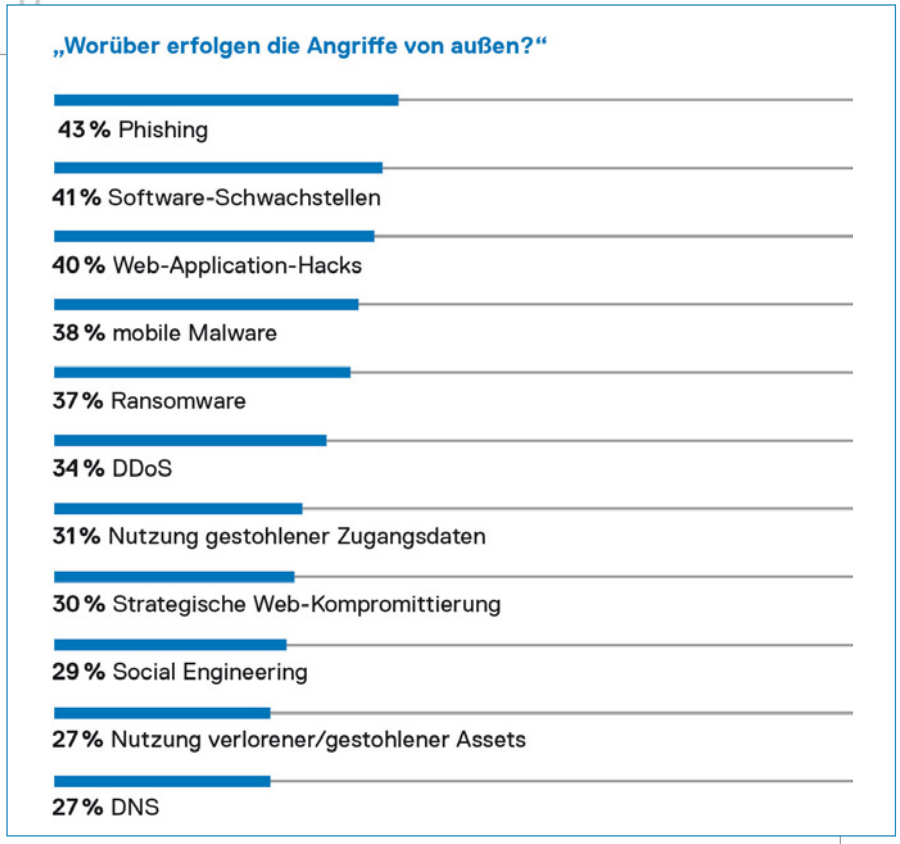
ANGRIFFE AUF DAS HERZSTÜCK DES RECHNERS

Das BIOS ist ein stark unterschätzter Angriffspunkt für Cyber-Kriminelle. Wird das Herzstück eines Rechners gehackt oder mit Viren infiziert, können sich die Angreifer unerkannt in der Firmware des Computers einnisten und Daten auslesen. Die meisten Unternehmen sichern ihre IT gegen Zugriffe von außen ab, vergessen dabei aber oftmals den Schutz des BIOS selbst.

Ein Bewusstsein für die Gefahren, die aus dem Cyber-Raum drohen, ist inzwischen bei den meisten Unternehmen vorhanden: Sie schützen ihre IT-Infrastruktur mit leistungsstarker Sicherheitssoftware vor Angriffen von außen. In der Regel setzt dieser Schutz allerdings erst auf der Ebene des Betriebssystems an – das darunterliegende BIOS ist oftmals nicht oder nur unzureichend abgesichert. Mit BIOS, Firmware und UEFI (Unified Extensible Firmware Interface) ist die Software gemeint, mit der ein Rechner, genauer gesagt dessen Hauptplatine, beim Einschalten in Gang kommt. Schutzmechanismen wie Virenscanner greifen an dieser Stelle nicht, da sie zu diesem Zeitpunkt noch nicht aktiv geladen sind. Das bedeutet, wer die Firmware kontrolliert, kontrolliert auch das Betriebssystem. Deshalb sind Angriffe auf das BIOS für Hacker so interessant, und gerade die Endpunkte sind lohnende Ziele. Insbesondere Notebooks können oftmals nicht von der IT-Administration überwacht werden und sind damit besonders gefährdet.

DA CYBER-KRIMINELLE SEHR KREATIV SIND, MUSS IT-SICHERHEIT IN UNTERNEHMEN AUF ALLEN EBENEN GESCHEHEN.

Andreas Scheurle,
OSS Product Specialist Endpoint Security,
Dell Technologies Deutschland,
www.delltechnologies.com

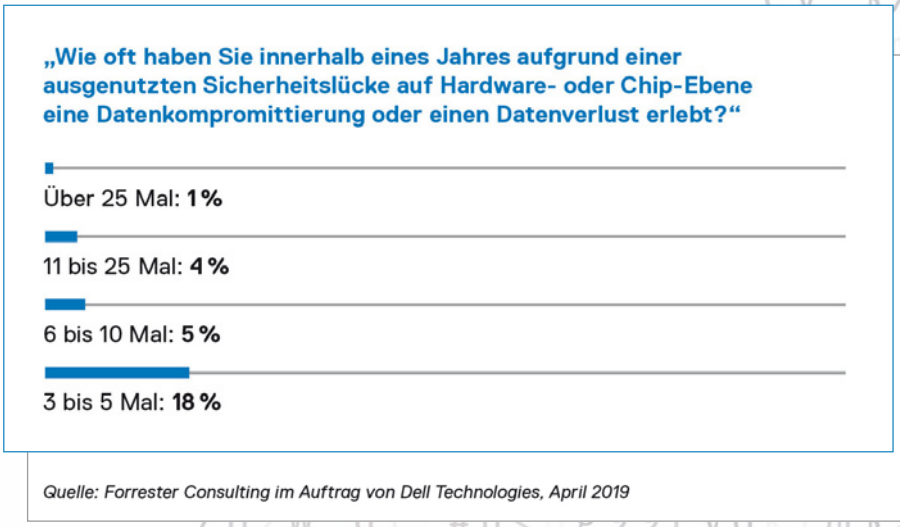


Quelle: Forrester Consulting im Auftrag von Dell Technologies, April 2019

Zahl der Angriffe auf BIOS-Ebene nimmt rasant zu

Laut der Forrester-Studie BIOS Security – The Next Frontier for Endpoint Protection haben fast zwei Drittel (63%) aller befragten Unternehmen innerhalb eines Jahres aufgrund einer ausgenutzten Sicherheitslücke auf Hardware- oder Chip-Ebene eine Datenkompromittierung beziehungsweise einen Datenverlust erlebt. Verantwortlich dafür waren an erster Stelle Angriffe von außen (29,4%), die wiederum hauptsächlich über Pishing-Attacken (43%), Software-Schwachstellen (41%), Web-Application-Hacks (40%), mobile Malware (38%) oder Ransomware (37%) erfolgten. Für die von Dell Technologies in Auftrag gegebene Studie wurden 307 Entscheidungsträger in den USA, Kanada, Großbritannien, Frankreich und Deutschland aus den Bereichen IT, Sicherheit, Risiko und Compliance in Unternehmen mit mehr als 500 Mitarbeitern befragt.

Die Studie zeigt auch, dass die Mehrheit der Unternehmen in puncto Abwehrmaßnahmen auf Hardware-Ebene auf den „Worst-Case" nicht beziehungsweise nur schlecht vorbereitet ist. So wird klassischen Sicherheitsmaßnahmen rund um Infrastruktur und Endgeräte für dieses Jahr eine sehr hohe Priorität eingeräumt. Geht es um den BIOS-Schutz, sind Unternehmen deutlich nachlässiger und setzen sich damit einem großen Risiko aus. Lösungen, die die Erkennung von BIOS- und Boot-Level-Anomalien ermöglichen, lassen sich aber nicht so einfach installieren. Umso wichtiger ist es, dass Unternehmen Hard- wie auch Software nur von vertrauenswürdigen, validierten Lieferanten beziehen.



Quelle: Forrester Consulting im Auftrag von Dell Technologies, April 2019

Anbieter von Hardware-Sicherheit sind der Schlüssel

Was Notebooks & Co. betrifft, bietet eine Endpoint Protection, die bereits vom Hersteller in der Hardware verankert wird, eine hohe Sicherheit. Solche Lösungen agieren unterhalb der Betriebssystem-Ebene. Mit SafeBIOS bietet Dell Technologies beispielsweise eine Off-Host-BIOS-Verifizierungsfunktion, die in VMware Workspace ONE und den Sicherheitslösungen von Secureworks und CrowdStrike integriert ist. Durch diese vom Host unabhängigen BIOS-Kontrollen minimieren Unternehmen das Risiko von Manipulationen und werden auf solche hingewiesen, sodass alle infizierten PCs rasch lokalisiert und unter Quarantäne gestellt werden können.

Da Cyber-Kriminelle sehr kreativ sind, muss IT-Sicherheit in Unternehmen auf allen Ebenen geschehen. Herkömmliche Security-Lösungen, die auf Betriebssystem-Level angesiedelt sind, helfen bei einem Angriff auf das BIOS nicht weiter. Um Unbefugten den Zugang zu erschweren und eine zusätzliche Sicherheitsbarriere einzurichten, sollten Unternehmen auf jeden Fall das BIOS-Setup mit einem sogenannten Admin- oder Supervisor-Passwort schützen. Darüber hinaus sollten regelmäßig BIOS-Updates aus verlässlicher Quelle eingespielt werden, um potenzielle Sicherheitslücken so schnell wie möglich zu schließen. Neben diesen zwei grundlegenden Maßnahmen ist die Wahl eines vertrauenswürdigen IT-Anbieters der beste Weg, um Angriffe auf das Herzstück des Rechners zu verhindern.

Andreas Scheurle

DER DIGITALE WELTKRIEG …,

… DEN KEINER BEMERKT

Der niederländische Investigativjournalist Huib Modderkolk gibt einen erschreckenden Einblick in der Verletzlichkeit unserer Systeme aufgrund von Cyberkriminalität. Dafür hat er zahlreiche Interviews mit (ehemaligen) Geheimdienstmitarbeitern, Sicherheitsexperten und Hackern geführt.

Er beschreibt in seinem Buch, wie durch Hackerangriffe ganze Staaten lahmgelegt werden können und wie Terroristen anhand von Simkarten-Standorten mit Drohnen ausgeschaltet werden. Er schreibt, wie spielend leicht sich in das Datensystem von Telekommunikationsanbietern eingehackt werden konnte, wie ganze Rechenzentren ausgespäht werden und warum es Regierungen nicht gelingt, ihre Bevölkerung vor Cyber-Angriffen zu schützen.

Der digitale Weltkrieg; Huib Modderkolk;

Ecowin Verlag, 2020

SCHWACHSTELLENMA

IT-SICHERHEIT IN OT-NETZEN

In der Welt der Office-IT haben sich Vulnerability- und Patch-Management weitgehend etabliert. Nicht so in den Fertigungsumgebungen. Prozesse zur Ermittlung und Überwachung der Schwachstellen sind mindestens ebenso so selten wie das Patch-Management. Wer diese Herausforderungen nicht angeht, riskiert Opfer von gravierenden Cyber-Attacken zu werden.

Change-, Configuration- und Patch-Management sowie der Betrieb eines Information Security Management Systems (ISMS) bilden in der Office-IT-Welt die Grundpfeiler für einen zuverlässigen Betrieb von IT-Infrastrukturen. Die für die Sicherheit in der Operational Technology (OT)-Welt der Industrie- und Produktionsanlagen Verantwortlichen befassen sich nur selten mit Configuration- und Patch-Management; sie aktualisieren bestenfalls in unregelmäßigen Zeitabständen die Software der eingesetzten OT-Komponenten.

Dies hat nicht zuletzt historische Gründe. Bei der Entwicklung und dem Aufbau einer Maschine stehen die funktionalen Anforderungen im Vordergrund. Ist die Fertigung der Maschine abgeschlossen, installiert der Hersteller die Software, konfiguriert das System, testet die Lösung funktional und liefert sie aus. Anforderungen an das Sicherheitsmanagement und Incident Handling kommen nur am Rande vor. Standardmäßig sind keine Prozesse vorgesehen, um Schwachstellen und die damit verbundenen Risiken und Änderungen der Sicherheitsanforderung im Alltagsbetrieb über den gesamten Verlauf des Lebenszyklus zu überwachen und zu bewerten.

Fakt ist: PLCs, RTUs, Sensoren, Aktoren, Server-basierte SCADA-Systeme und andere Komponenten von OT-Netzwerken sind verwundbar. Das liegt auch an den heterogenen Kommunikationsnetzen, denn zusätzlich zu neueren IT-Protokollen kommen auch weiterhin Legacy-Protokolle zum Einsatz, möglicherweise „encapsulated" in Ethernet Frames. Authentifizierung und Verschlüsselung fehlen weitgehend und es existieren unbekannte Hintertüren, die geradezu eine Einladung für maßgeschneiderte Angriffe auf OT-Komponenten bilden.

Mehr Sicherheit durch Transparenz

Als eine der ersten Maßnahmen für mehr Sicherheit sollten Unternehmen Transparenz über die vorhandene Produktionsanlage herstellen. Ziel dabei ist es, Anomalien und kritische Zustände in den Prozessen sowie Bedrohungen einzelner OT-Komponenten oder gar der gesamten OT-Infrastruktur schnellstmöglich zu erkennen und Abwehrmaßnah-

NAGEMENT

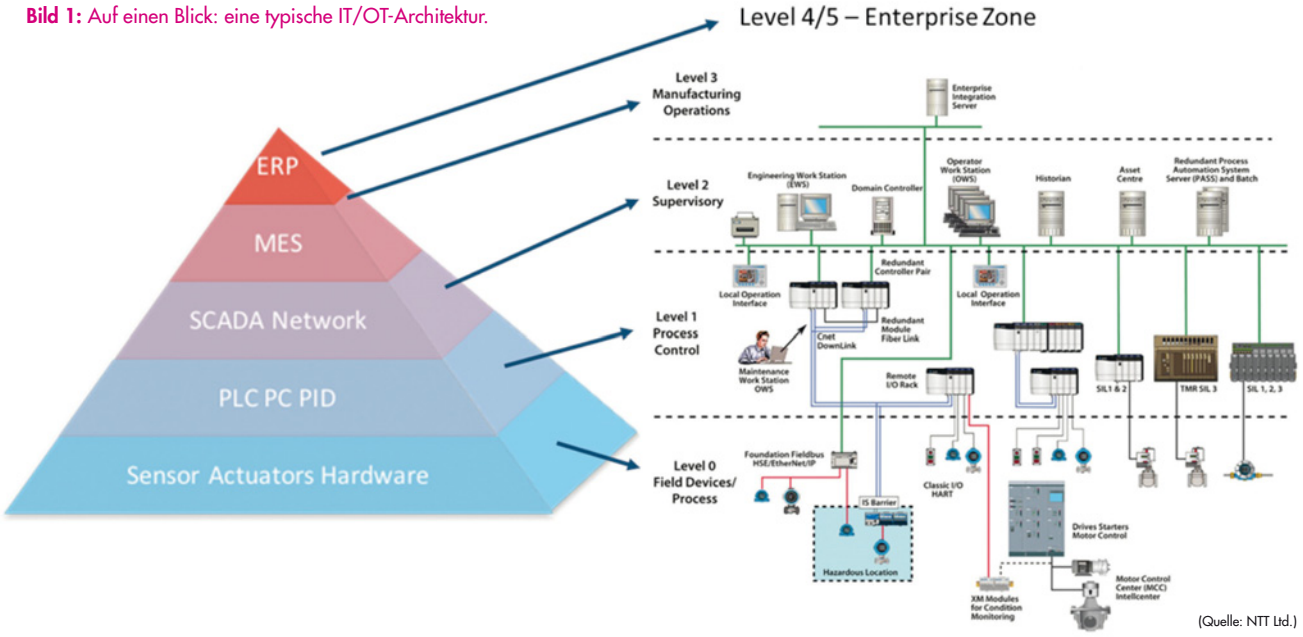
IN DER IT-WELT DER OFFICE-UMGEBUNGEN HAT SICH EIN INTELLIGENTES SCHWACHSTELLENMANAGEMENT SEIT VIELEN JAHREN BEWÄHRT UND DESSEN METHODEN UND PRINZIPIEN LASSEN SICH AUCH IN OT-NETZEN NUTZBRINGEND EINSETZEN.

Christian Koch, Director GRC & IoT/OT Security Division, NTT Ltd., https://hello.global.ntt/

men, heutzutage meist manuell aufgrund der Verfügbarkeitsanforderungen und des geringen Sicherheitsreifegrades von OT-Systemen, einleiten zu können. Um die vorhandenen Schwachstellen ausfindig zu machen, sollten Unternehmen eine genaue Bestandsaufnahme in ihren OT-Netzen vornehmen und eine kontinuierliche Überwachung implementieren. Geeignet für diese Aufgabe sind beispielsweise Tools wie Continuous Threat Detection von Claroty oder SCADAguardian von Nozomi Networks. Unterstützt durch einen externen IT-Security-Spezialisten können Unternehmen mit diesen „passiven Tools" die eingesetzten Komponenten inklusive Softwareversionen, Kommunikationsprotokollen und Kommunikationspartnern ermitteln. Beide Tools beeinflussen nicht die regulären Abläufe und die Kommunikation im OT-Netz. Zusätzlich zur Bestandsaufnahme der Vulnerabilities und resultierenden Risiken empfiehlt es sich, Schwachstellendatenbanken hinzuzuziehen. Diese sind für viele PLCs verfügbar und Unternehmen können sich damit einen sehr guten Überblick über die Gefährdungslage der von ihnen eingesetzten Produkte verschaffen.

Die Tools von Nozomi Networks ermöglichen eine Echtzeitüberwachung von Prozessen und kompletten ICS-Netzwerken und liefern Unternehmen einen genauen Einblick in das operative Geschehen. Netzwerk-Visualisierung und -überwachung zeigen Details von Nodes und Variablen, den Kommunikationsbeziehungen und Inhalte von Datenpaketen. Mit Threat- und Anomaly-Detection lassen sich Verhaltensauffälligkeiten erkennen. Darüber hinaus können Unternehmen auch eigene Regeln erstellen, beispielsweise zur Festlegung, welche Verbindungen nach außen beziehungsweise welche Zugriffe von außen als legitim angesehen werden. Sinnvoll sind eigene Regeln auch für die individuelle Risikobewertung und die Gefahrenerkennung. In sehr umfangreichen Umgebungen kann die verhaltensbasierte Anomalie-Erkennung darüber hinaus auch die Ergebnisse einer KI- und Analytics Engine mit einbeziehen.

Bild 1: Auf einen Blick: eine typische IT/OT-Architektur.



(Quelle: NTT Ltd.)

Um anomales Verhalten, nicht autorisierte Zugriffe und andere Risiken zu erkennen, definieren die Tools Baselines als „Normalzustand". Bei jeder Abweichung davon erfolgt automatisch ein Alarm, etwa dann, wenn ein neues Endgerät mit unbekannter MAC-Adresse oder zum Beispiel eine neue Modbus-Verbindung diagnostiziert wird. Die Aufgabe regelbasierter Analysen ist es, Cyber-Attacken, aber auch Angriffe von innen, sowie Malware jeder Art in Echtzeit zu erkennen.

Integration in die vorhandene IT-Welt eines Unternehmens

Um die sicherheitstechnische Kluft zwischen der Produktions- und der klassischen IT-Welt zu überwinden, sollten sich die in den OT-Netzen eingesetzten Tools in das Security Operation Center (SOC) des Unternehmens beziehungsweise von spezialisierten Dienstleistern für IT- und OT-SOC Services einbinden lassen. Damit stellen Unternehmen sicher, dass in der OT-Welt keine neuen Silos entstehen.

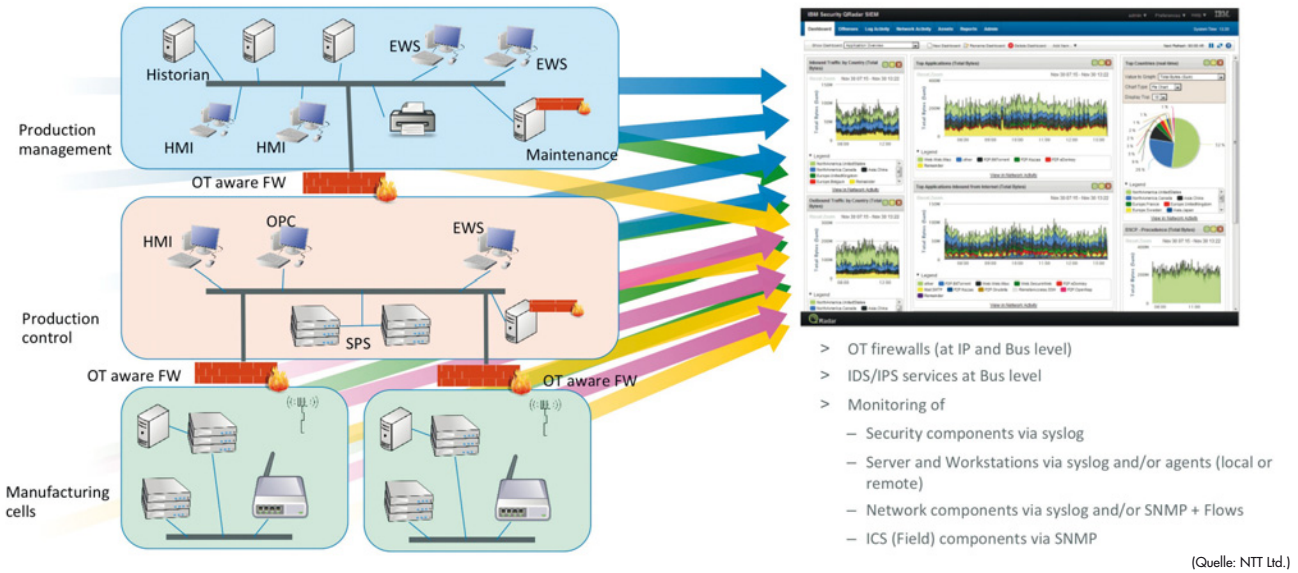
Letztlich geht es dabei um die Implementierung und Einhaltung einer ganzheitlichen Security-Strategie, die die herkömmliche IT- und die OT-Welt umfasst. Nur damit können die bestehenden Risiken strukturiert erfasst und mitigiert werden. Die Basis bildet ein zentrales Asset Inventory sowie koordinierte reaktive und proaktive Abwehrmaßnahmen bei Incidents und Angriffen.

Intelligentes Schwachstellenmanagement

In der IT-Welt der Office-Umgebungen hat sich ein intelligentes Schwachstellenmanagement seit vielen Jahren bewährt und dessen Methoden und Prinzipien lassen sich auch in OT-Netzen nutzbringend einsetzen. Dieses Smart Vulnerability Management beginnt bei der Bestandsaufnahme der vorhandenen PLCs, RTUs, Sensoren, Aktoren, Server-basierten SCADA-Systeme und anderen Komponenten von OT-Netzwerken. Vorbilder eines OT Asset Inventory sind unter anderem die Konfigurationsdatenbanken (Configuration Management Database, CMDB) der IT-Systeme in der Office-Welt. Das Schwachstellenmanagement bewertet, filtert und priorisiert die mit den einzelnen OT-Komponenten verbundenen Risiken. Diese Risikoabschätzung ist ein zentraler Baustein des Smart Vulnerability Managements, da jede Fertigungsumgebung und jedes OT-Netz ein individuelles Risikoprofil aufweist, das durch eine Klassifizierung und Bewertung der schützenswerten Daten und Prozesse ermittelt werden muss. Darauf bauen alle weiteren Maßnahmen im Rahmen einer umfassenden Vulnerability-Management-Strategie auf, beispielsweise eine strukturierte Planung der weiteren Schritte zur Steigerung der OT-Sicherheit.

Das Schwachstellenmanagement nutzt auch systemübergreifende Informationen, die eine Priorisierung ermöglichen. Tritt etwa eine Schwachstelle bei einer bestimmten OT-Komponente auf, muss nicht zwangsläufig ein Patchen mit hoher Priorität erforderlich sein. So liegen möglicherweise durch Echtzeit-Informationen der OT-Threat-Detection-Sensoren Erkenntnisse darüber vor, welche Systeme überhaupt betroffen und welche regulär erreichbar sind. Möglicherweise sind auch über die bereits im Einsatz befindlichen Intrusion-Prevention- und Intrusion-Detection-Systeme Pattern-Updates für diese Verwundbarkeit vorhanden. Setzt ein Unternehmen zudem eine CMDB ein, kennt es auch diejenigen Systeme, die überhaupt kritische Daten beinhalten.

Bild 2: Eine mögliche Architektur sicherer OT-Umgebungen.



(Quelle: NTT Ltd.)

Auch durch die damit mögliche Priorisierung können Patch-Prozesse entscheidend optimiert werden.

Ein umfassendes intelligentes Smart-Vulnerability-Managementsystem beinhaltet:

- **Visibility:** Erfassung aller Komponenten des OT-Netzwerkes inklusive detaillierter Informationen über Aufbau, eingesetzte Softwareversionen, Module, genutzte Protokolle
- **Identifizierung:** Echtzeit-Vulnerability-Informationen in einer zentralen Datenbank
- **Priorisierung:** eine anforderungsspezifische Schwachstellen-Klassifizierung
- **Management:** Maßnahmen-Tracking, Echtzeitreports, Dash-boards und Charts
- **Audit:** Auditierbare Prozesse von der Schwachstellen-Identifizierung bis zur -Beseitigung
- **Vulnerability-Threat-Korrelation**

In der Office-IT-Welt gilt als Gebot, Schwachstellen mit Patches zeitnah zu schließen. In den OT-Netzen ist die pauschale Empfehlung, alle Komponenten immer zu aktualisieren praktisch nicht umsetzbar. Die Transparenz und die Kenntnis der bestehenden Risiken und Vulnerabilities ist hier der ausschlaggebende Faktor, um mittels risikobasierter Netzwerksegmentierung, OT-Angriffserkennung, der Erkennung von Veränderungen in der Infrastruktur und kontrolliertem Zugriff auf das Netzwerk auch von extern Maßnahmen umzusetzen, die den Betrieb der Anlage nicht stören, aber das Sicherheitsniveau verbessern. Hier sind nicht nur Fertigungsunternehmen gefordert, sondern auch die Hersteller von PLCs, RTUs, Sensoren und Aktoren. Sie müssen bei der Produktentwicklung von Anfang an nach dem Security-by-Design vorgehen: Bereits die fachliche Anforderungsanalyse sollte die aktuell mit Geräten verbundenen Sicherheitsrisiken berücksichtigen, aber auch solche, die im weiteren Lebenszyklus auftreten könnten. Die IEC 62443, eine internationale Normenreihe zu industriellen Kommunikationsnetzen, bietet hier eine gute Basis. Eine Zertifizierung der Produkte nach diesem Standard ist möglich und ein Wettbewerbsvorteil für jeden Hersteller.

Christian Koch

PHISHING

SCHULUNGEN UND TRAINING FÜR MEHR AWARENESS

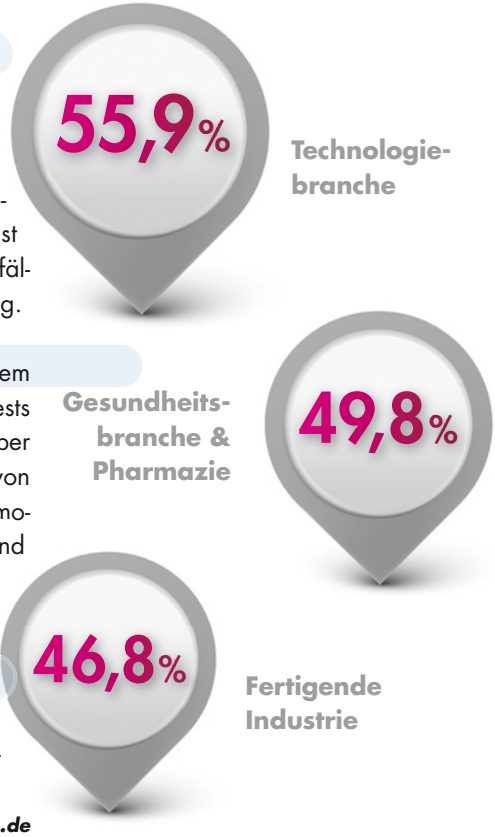
KnowBe4 veröffentlicht die Ergebnisse seines Benchmarking Reports 2020 zum Thema „Phishing by Industry". Gemessen wird der sogenannte Phish-Prone-Percentage (PPP), der angibt, wie viele Mitarbeiter eines Unternehmens wahrscheinlich auf einen Phishing- oder Social-Engineering-Betrug hereinfallen würden.

Der anfängliche Basis-Phishing-Test wurde in Unternehmen durchgeführt, die bisher kein Security Awareness Training absolviert hatten. Die Ergebnisse zeigten ein hohes Risiko, mit einem durchschnittlichen anfänglichen Basis-PPP-Wert von 38 Prozent, was einem Anstieg von 8 Prozent gegenüber 2019 entspricht – und zwar über alle Branchen und Unternehmensgrößen hinweg. Jedes Unternehmen, unabhängig von seiner Größe und seiner Hierarchieebenen, ist ohne computergestütztes Training anfällig für Phishing und Social Engineering.

Nach 90 Tagen computergestütztem Training und simulierten Phishing-Tests konnte der durchschnittliche PPP um über 60 Prozent reduziert werden und fiel von 38 auf 14 Prozent. Nach einem Jahr monatlicher simulierter Phishing-Tests und regelmäßiger Schulungen sank der PPP sogar auf nur 5 Prozent. Über alle Branchen hinweg konnte eine durchschnittliche Verbesserungsrate von 87 Prozent vom ersten Test bis zum Ende eines 12-monatigen Trainings erzielt werden.

www.knowbe4.de

WER IST DEM GRÖSSTEN RISIKO AUSGESETZT?



Immer gut informiert!

Tägliche News für die Enterprise IT

finden Sie auf **www.it-daily.net**

it-daily.net
Das Online-Portal von
itmanagement & itsecurity