itmanagement

MAI 2021

INKLUSIVE 24 SEITEN
IT SECURITY

noris network

Colocation im TSI-Level-4-Rechenzentrum **ab Seite 16**

BLACK HAT & SEO

Manipulative Methoden

AGILE PROJEKTE

Hybrides Requirements Engineering

IT-SICHERHEIT IM HOMEOFFICE

REMOTE WORK UND HOCHSENSIBLE DATEN

Ralf Lautenbacher, Brainloop

www.it-daily.net

Das E-3 Magazin

itmanagement

SAP: Innovation & Digitale Transformation

15. Juni 2021 | Digitalevent

#SAPdigital21

Jetzt anmelden

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

SECURITY, SECURITY, SECURITY

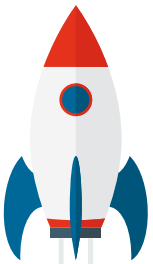
Homeoffice und IT-Sicherheit – mit diesem Thema könnte man dieses Jahr wahrscheinlich alle Ausgaben des it management und der it security füllen. Homeoffice bleibt im Trend, wenn auch nicht immer freiwillig. Viele Firmen haben sich bereits umgestellt, ihre IT-Umgebungen und Netzwerke gesichert und an die veränderte Situation angepasst – angefangen bei sicheren Zugängen und erweiterten Sicherheitsmaßnahmen, bis hin zu Mitarbeiterschulungen in Bezug auf Security-Awareness.

Doch viele Unternehmen halten an der Vorstellung fest, dass die Zeit des Homeoffice vorübergehen wird und die Mitarbeiter früher oder später wieder ganz normal im Büro sitzen werden. Bis zu einem gewissen Grad wird das wahrscheinlich tatsächlich wieder so werden – einfach, weil sich viele Dinge in einem persönlichen oder direkten Gespräch leichter klären lassen, weil Brainstorming einfach besser funktioniert, wenn man sich gegenübersitzt und weil man manche Aufgaben einfach nicht allein im Homeoffice erledigen kann. Doch der jetzt erreichte Grad an Flexibilität und Eigenständigkeit ist etwas, der längerfristig in den Geschäftsstrukturen verankert werden sollte, denn das werden viele Mitarbeiter nicht so leicht wieder aufgeben wollen.

Wie man dies am besten bewerkstelligt, auf was man achten muss und welche Vor- und Nachteile Remote Work noch hat, lesen Sie in dieser Ausgabe des it management und des Supplements it security.

Viele Spaß beim Lesen

Carina Mitzschke | Redakteurin it management



22

44

14

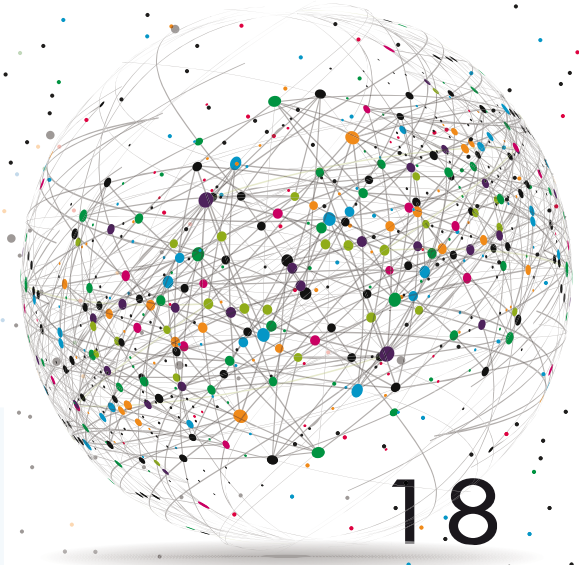
INHALT

30

COVERSTORY

IT MANAGEMENT

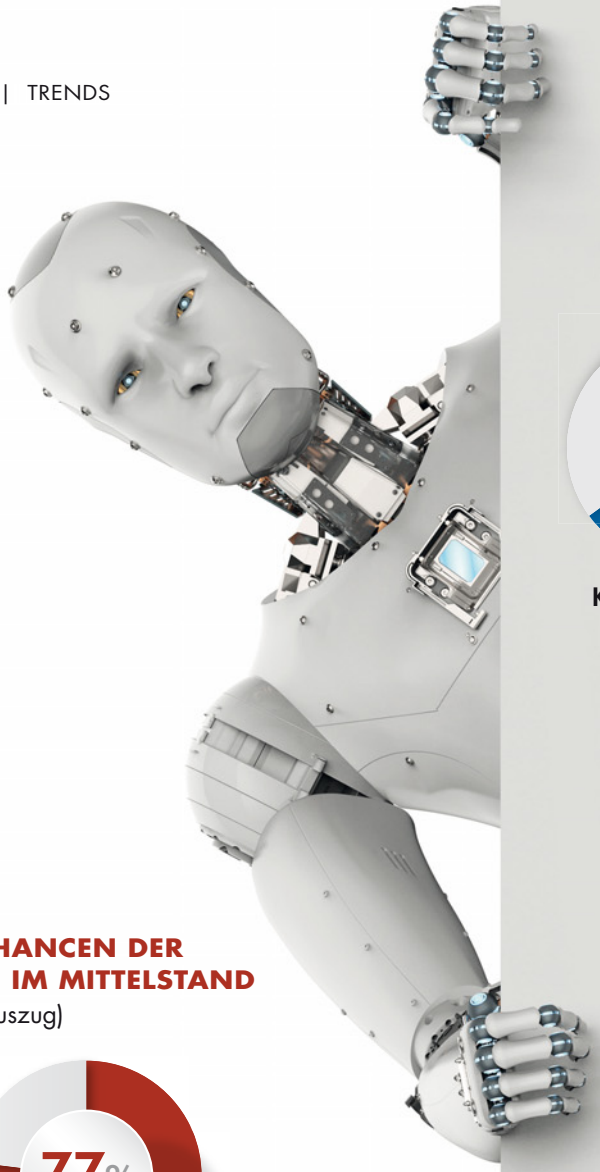
IT INFRASTRUKTUR



eBUSINESS

Inklusive 24 Seiten

IT SECURITY SPEZIAL



KÜNSTLICHE INTELLIGENZ

ZIEHT DER DEUTSCHE MITTELSTAND MIT?

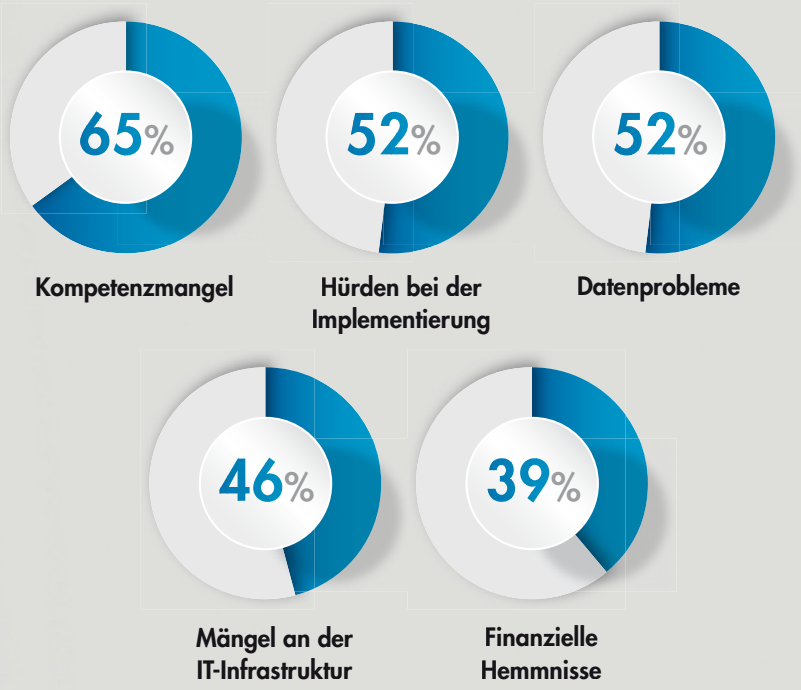
So präsent die Begriffe „Deep Learning", „Process Mining" oder „Natural Language Processing" in der Arbeitswelt mittlerweile sind, so häufig kommt künstliche Intelligenz (KI) schon in den unterschiedlichsten Bereichen zum Einsatz. Der deutsche Mittelstand scheint KI-Technologien hingegen noch verhalten gegenüberzustehen – das zeigt eine aktuelle Deloitte-Studie.

64 Prozent der Befragten messen KI eine lediglich mittlere bis niedrige Relevanz für den Mittelstand als Ganzes bei. Auch in Bezug auf das eigene Geschäftsmodell sprechen ihr 58 Prozent eine niedrige Bedeutung zu. Werfen die Befragten einen Blick in die Zukunft, ändert sich das Meinungsbild: 59 Prozent sind davon überzeugt, dass die Bedeutung von KI zunehmen wird.

www.deloitte.de

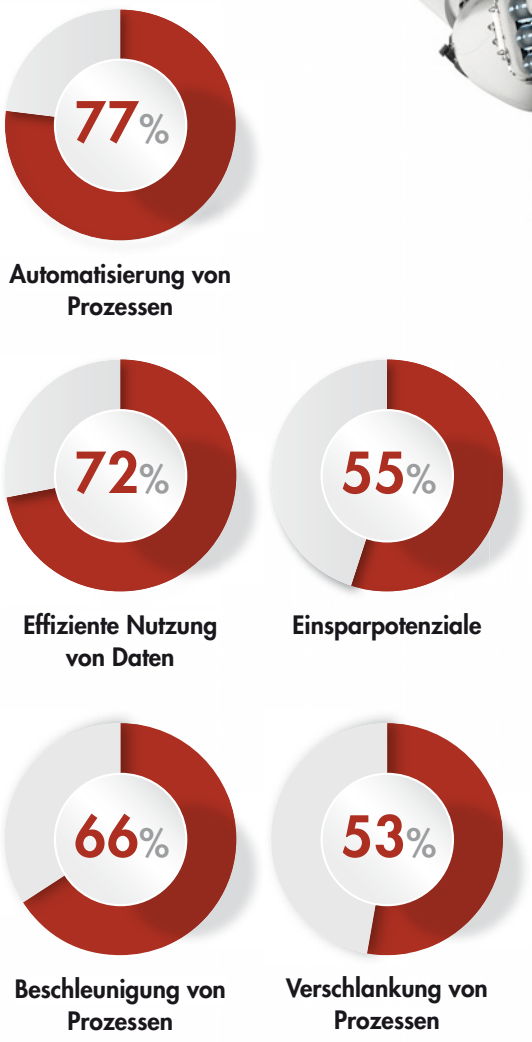
HEMMNISSE DER KI IM MITTELSTAND

(Auszug)



CHANCEN DER KI IM MITTELSTAND

(Auszug)

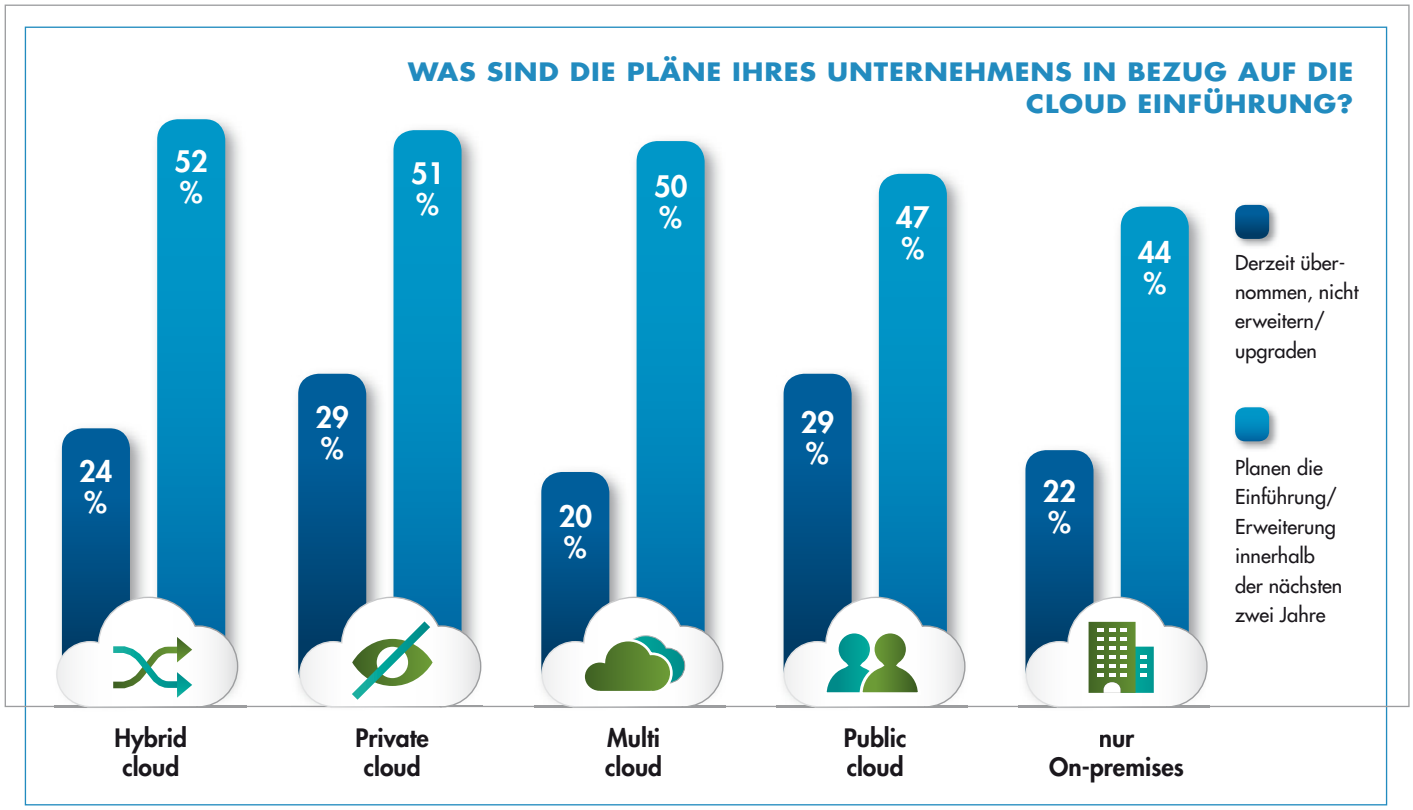


HYBRID-CLOUD

IAM ZUR LÖSUNG VON SICHERHEITSPROBLEMEN

ForgeRock gibt die Ergebnisse der allerersten Studie zur Akzeptanz von Hybrid-Cloud in Unternehmen bekannt. Aus der Studie geht hervor, dass mehr als 80 Prozent der globalen IT-Entscheidungsträger planen, in den nächsten zwei Jahren cloudbasierte Identity und Access-Management-Initiativen (IAM) einzuführen oder bestehende Projekte zu erweitern.

www.forgerock.com



der deutschen Unternehmen nutzen Cloud-native Technologien

der deutschen CIOs sagen, dass die Komplexität ihrer Cloud-Umgebung die menschlichen Möglichkeiten übersteigt

SKALIERBARE OBSERVABILITY

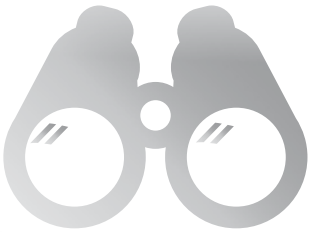
ihrer Zeit verbringen IT- und Cloud-Teams mit manuellen Routineaufgaben, die lediglich „die Systeme am Laufen halten"

FÜNF HERAUSFORDERUNGEN

Um effektiv mit der ständig wachsenden Nachfrage nach digitalen Services Schritt zu halten, benötigen IT-Teams umfassende Einblicke in ihre IT-Umgebungen. Herkömmliche Monitoring-Lösungen und manuelle Ansätze scheitern jedoch daran, die dynamische Natur heutiger Multi-Cloud- und Cloud-nativer Umgebungen zu überwachen. Dynatrace hat fünf wesentliche Herausforderungen identifiziert, die Unternehmen im Blick behalten sollten, wenn sie schnell und effizient eine skalierbare Observability erreichen möchten:

1 Container, Microservices und Kubernetes

Der Einsatz Cloud-nativer Architekturen mit Microservices, Containern und Kubernetes bietet Unternehmen höhere Agilität, Effizienz und Skalierbarkeit und ermöglicht somit schnellere Innovationen. Allerdings führen diese Architekturen auch zu extrem dynamischen Umgebungen, die sich im Minutentakt oder noch schneller verändern. Mit manuellen Ansätzen zur Konfiguration und Instrumentierung von Apps oder zum Erstellen von Skripten und Quellen für die Daten ist es nahezu unmöglich, mit diesem Veränderungstempo Schritt zu halten.



2 Tatsächliche User Experience

Exzellente Benutzererfahrungen sind geschäftsentscheidend. Dazu werden digitale Angebote kontinuierlich überprüft und verbessert. Wenn Unternehmen jedoch nicht sehen, wie reale User ihre Anwendungen und Software erleben, reduziert dies den konkreten Wert, den Unternehmen durch ihre Observability-Aktivitäten erzielen können. Ohne die Messung des Nutzererlebnisses aus der Perspektive des Anwenders ist es unmöglich zu wissen, ob die Anwendungen so funktionieren, wie sie sollten.

3 IT-Silos

Die IT wird immer mehr zu einer geschäftlichen Notwendigkeit. Trotzdem betrachten die meisten Unternehmen ihre Observability-Daten isoliert von wesentlichen Geschäftskennzahlen wie Umsatz und Konversionsraten. Dadurch werden die Zusammenhänge zwischen wichtigen Kennzahlen aus IT und Business leicht übersehen und somit der Kontext nicht beachtet.

4 Viel zu viele Überwachungstools

Unternehmen nutzen durchschnittlich zehn verschiedene Monitoring-Tools, um ihre Multi-Cloud-Umgebungen zu überwachen. Daraus resultieren enorme Datenmengen und widersprüchliche Alarmmeldungen in sehr kurzer Zeit, die IT-Teams nicht mehr manuell zusammenfassen oder auswerten können. Sie verlieren trotz vieler Tools den Überblick.

5 Manuelle DIY-Lösungen

Viele Unternehmen verfolgen einen Do-it-yourself-Ansatz bei der Observability, indem sie die Instrumentierung manuell in den Anwendungscode einbauen, während sie entwickeln. Dies ist nicht nur ein zeitaufwändiger Prozess, der Team-Ressourcen beansprucht, er schafft auch blinde Flecken. Während neuere Systeme oft eine eingebaute Observability-Funktion besitzen, ist dies bei vielen älteren Systemen nicht der Fall. KI und Automatisierung sind der Schlüssel, um Herausforderungen im Bereich der Observability zu meistern und IT-Teams in die Lage zu versetzen, Risiken zu erkennen und bessere Geschäftsergebnisse zu erzielen.

www.dynatrace.de

PRÄSENZ AUF MESSEN

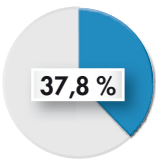
AKTUELLE STUDIENERGEBNISSE

Rund 70 Prozent aller Messen mussten im vergangenen Jahr aufgrund der Corona-Pandemie bundesweit abgesagt werden. Ein schwerer Schlag, schließlich gelten Messen gemeinhin besonders für KMU als wichtiges Instrument für die Geschäftsanbahnung und die Vorstellung neuer Innovationen. Aber ist dem wirklich so?

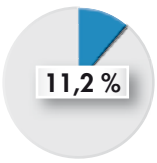
www.visable.com

WAS FEHLT AN DEN KLASSISCHEN PRÄSENZMESSEN?

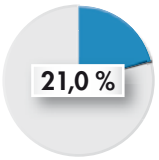
ZURÜCK ZU PRÄSENZMESSEN?



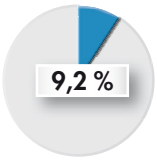
waren sowieso noch nie auf Messen unterwegs



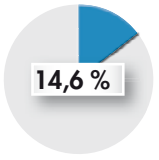
werden weiterhin nur als Gäste hingehen



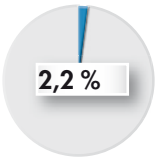
werden auch weiterhin aktiv auf Messen ausstellen



werden gar nicht mehr hingehen



werden weniger ausstellen



werden neuerdings auch ausstellen

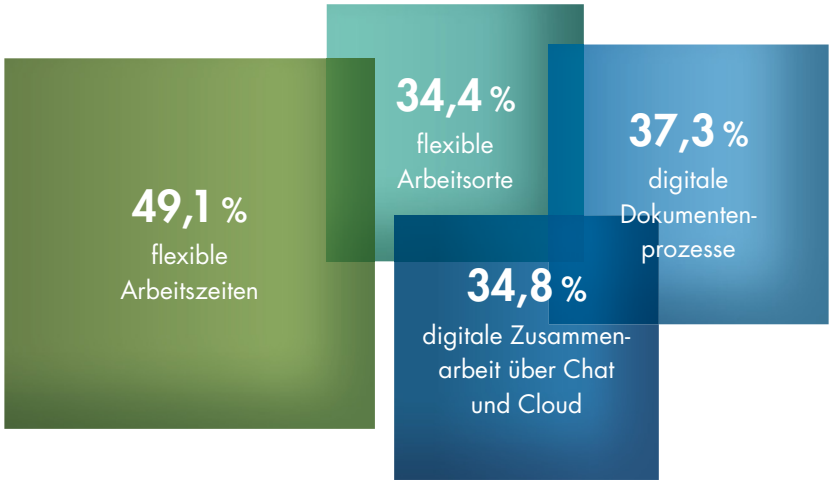
NEW WORK

NEULAND ODER GELEBTE REALITÄT?

Alle sprechen vom neuen Arbeiten, doch haben digitale Tools und agile Strukturen tatsächlich ihren Weg aus den Ideenschmieden in den Arbeitsalltag gefunden? Eine aktuelle Adobe Studie ermittelt den Status Quo in deutschen KMUs. Das Ergebnis: Das Potenzial moderner Arbeitsweisen wird in der Realität zwar noch nicht vollends ausgeschöpft, doch die Vorteile werden erkannt.

blog.adobe.com

DIESE ASPEKTE DES MODERNEN ARBEITENS WERDEN IN KMUS REGELMÄSSIG GENUTZT.



IT-SICHERHEIT

WIE HOCHSENSIBLE INFORMATIONEN GESCHÜTZT WERDEN KÖNNEN

Die Digitalisierung ist nicht erst seit Corona Teil der Unternehmensagenda – die Pandemie hat das Bewusstsein dafür aber noch einmal drastisch geschärft. Dies schuf eine solide Grundlage für den Wandel hin zu flexibleren Arbeitsmodellen. In diesem Kontext nimmt IT-Sicherheit einen immer wichtigeren Stellenwert ein. Doch wie lässt sie sich effektiv umsetzen in einer Zeit, in der Cyberkriminelle verstärkt nach Schwachstellen suchen? Ulrich Parthier, Herausgeber it management, sprach mit Ralf Lautenbacher, CISO von Brainloop.

Ulrich Parthier: *Was sind aktuell die größten Herausforderungen in Sachen Remote Work und Remote-IT-Sicherheit?*

Ralf Lautenbacher: Viele Unternehmen schafften den spontanen Übergang zu Remote Work in der akuten Krisensituation. Die nächste große Herausforderung besteht nun darin, die neuen Arbeitsmodelle, die neu gewonnene Flexibilität und Eigenständigkeit sowie die (Cyber-) Sicherheit aller Mitarbeiter auf lange Sicht in Geschäftsstrukturen zu verankern. Besonders der IT-Sicherheit muss höchste Priorität zukommen, denn es besteht das Risiko, dass Cyberkriminelle Unsicherheit und unerkannte Schwachstellen ausnutzen, um in Unternehmensnetzwerke einzudringen und kritische Informationen abzugreifen. Die Angriffsfläche vergrößert sich, je mehr Mitarbeiter sich unterwegs oder von ihren Heimbüros aus über ihre Endgeräte mit dem Unternehmensnetzwerk verbinden.

Ulrich Parthier: *Mit welchen technischen Hilfsmitteln lässt sich verhindern, dass sich Endgeräte zur Sicherheitsfalle im Homeoffice entwickeln?*

Ralf Lautenbacher: IT-Teams müssen sich im Klaren sein, welche Kanäle, die zum Austausch von sensiblen Daten dienen, besonders gefährdet sind – vor allem dann, wenn diese Daten Unternehmensgrenzen verlassen. Damit die Arbeit zwischen verteilten Teams funktioniert, migrieren Unternehmen in die Cloud und greifen auf Cloud-basierte Kollaborationslösungen zurück. Doch die Sicherheitsfunktionen der Cloud Service Provider reichen häufig nicht aus, um die Daten in der Cloud umfassend zu schützen. Daher sollten Unternehmen parallel zentrale digitale Datenraum-Plattformen implementieren, auf denen sie sensible Informationen ablegen können. Die Einrichtung von Virtual Private Networks (VPNs) und Multifaktor-Authentifizierung (MFA) sollte ebenfalls zur Standardausstattung eines sicheren Heimarbeitsplatzes gehören.

> DIE NÄCHSTE GROSSE HERAUSFORDERUNG BESTEHT DARIN, DIE NEUEN ARBEITSMODELLE, DIE NEU GEWONNENE FLEXIBILITÄT UND EIGENSTÄNDIGKEIT SOWIE DIE (CYBER-) SICHERHEIT ALLER MITARBEITER IN GESCHÄFTSSTRUKTUREN ZU VERANKERN.
>
> Ralf Lautenbacher, CISO, Brainloop, www.brainloop.com

Ulrich Parthier: *Und wie gestaltet sich IT-Sicherheit zum Beispiel auf privaten oder mobilen Geräten wie Smartphones, die sich mittlerweile als „Arbeitstool für unterwegs" durchsetzen konnten?*

Ralf Lautenbacher: Grundsätzlich sollten Mitarbeiter nur Geräte nutzen, die das Unternehmen bereitstellt, da so das Kontrollniveau von Seiten der IT-Abteilung am höchsten ist. Sollte es erforderlich sein mit einem Privatgerät auf Geschäftsdaten zugreifen zu müssen, so können digitale Lösungen dabei helfen, das Arbeiten vom eigenen Gerät aus sicherer und „compliant" zu gestalten. Ein Bring-Your-Own-Device-Konzept (BYOD) mit klar definierten Richtlinien – wie beispielsweise die Trennung von privaten und geschäftlichen Daten – sollte dem vorangehen. Privat- und Geschäftsgeräte sollten mit einer Mobile-Device-Management-Lösung (MDM) ausgestattet werden, damit das IT-Team diese Systeme identifizieren, in ihre Sicherheitsstruktur einbinden und verwalten kann. Bei Smartphones ist die Gefährdungslage besonders hoch, da sie leichter verloren gehen oder gestohlen werden. Auch hier können sichere Datenraum- und MDM-Lösungen genutzt werden.

Ulrich Parthier: *Was können die Mitarbeiter selbst tun, um IT-Risiken im Homeoffice Einhalt zu gebieten beziehungsweise sie so gering wie möglich zu halten?*

Ralf Lautenbacher: Besonnen handeln ist für alle Mitarbeiter ein Must-do. Dies umfasst Maßnahmen, die im ersten Moment selbstverständlich erscheinen: Geräte durch ein Passwort sichern, Bildschirmsperre aktivieren, komplexere Passwörter verwenden, Arbeitsergebnisse regelmäßig ins Unternehmensnetzwerk übertragen oder verdächtige E-Mails ignorieren und auch melden. Mitarbeiter mit Zugang zu besonders sensiblen Informationen wie Finanzdaten oder Privatadressen sollten den Informationsaustausch über

verschlüsselte Verbindungen regeln. Jeder Mitarbeiter kann zur Datensicherheit beitragen, jedoch müssen Führungskräfte die Verantwortung tragen, dass Sicherheitsrichtlinien in ihren Teams etabliert und regelmäßig überprüft werden.

Ulrich Parthier: *Das heißt, IT-Sicherheit ist für Sie also Chefsache?*

Ralf Lautenbacher: Der Arbeitgeber muss mithilfe von technischen und organisatorischen Maßnahmen die Einhaltung von DSGVO-Richtlinien gewährleisten können. Führungskräften obliegt es, diese Richtlinien an ihre Teams zu kommunizieren und durchzusetzen. Außerdem müssen sie der IT-Sicherheit in ihren Strategien eine hohe Priorität schenken. Denn viele Geschäftsbereiche bringen den Einsatz verschiedener Plattformen, Anwendungen und Anforderung mit sich, die die IT überblicken und absichern muss. Da für diese Ansammlung in vielen Fällen keine „One-size-fits-all"-Lösung zum Tragen kommt, müssen Führungskräfte ihrem IT-Team einen ausreichenden Handlungsspielraum verschaffen, wenn es um die Wahl der passenden Lösungen geht.

Führungskräfte stoßen zudem den notwendigen Kulturwandel an. Zum einen, indem sie sich selbst Wissen über IT-Sicherheit aneignen und bei der Entwicklung einer Sicherheitsstrategie die richtigen Fragen stellen. Zum anderen, indem sie mit gutem Beispiel vorangehen und jene Handlungsweisen vorleben, die sie von ihren Teams erwarten.

Ulrich Parthier: *Welche Besonderheiten ergeben sich daraus für die Kommunikation und Arbeit von Führungsgremien?*

Ralf Lautenbacher: Vorstände, Aufsichtsräte und Gremien tauschen in der Regel sensible und höchst vertrauliche Informationen aus, die es entsprechend vor Cyberkriminalität und Spionage zu schützen gilt. Spezielle Datenraum-Lösungen können bei dieser Herausforderung für eine sichere und effiziente Kommunikation sorgen. Diese Lösungen sollten über eine durchgängige Verschlüsselung der Daten – sowohl im gespeicherten Zustand als auch während des Versandes – verfügen, um Vertraulichkeit und Integrität zu wahren.

Ulrich Parthier: *In der Big-Data-Ära kann Data Management auch unabhängig von Corona zur Herausforderung werden. Haben Sie zum Schluss Tipps, wie sich Data Management effizient und sicher umsetzen lässt?*

Ralf Lautenbacher: Es gibt zwei Bereiche des Data Managements, auf die ich an dieser Stelle eingehen möchte: die Datenverwaltung sowie das Gewinnen von handlungsorientierten Erkenntnissen aus diesen Daten. Effizienz und Sicherheit bei der Verwaltung von Daten aus verschiedenen Quellen lassen sich unter anderem erreichen, wenn diese zentral erfolgen. Um aus Daten wichtige Insights über wichtige Markttrends oder Kundenbedürfnisse zu generieren, auf deren Grundlage sich schnell Entscheidungen treffen lassen, empfiehlt sich der Einsatz einer Business-Intelligence-Lösung, die alle relevanten Informationen aus dem Datenfluss zieht. In jedem Fall braucht es ein solides Sicherheitskonzept, das die Daten über ihren gesamten Lebenszyklus hinweg vor unautorisierten Zugriffen durch Cyberkriminelle schützt.

Ulrich Parthier: *Herr Lautenbacher, vielen Dank für dieses Gespräch.*

ENVIRONMENTAL SOCIAL

SOFTWARE-UNTERSTÜTZUNG ZUR EINHALTUNG VON ESG-RICHTLINIEN

Unternehmen sind heute vielfach gefordert, nicht nur Gewinn zu erwirtschaften, sondern auch Verantwortung zu übernehmen, die über gesetzliche Anforderungen hinausgeht. Dieses Feld wird mit dem Begriff Environmental Social Governance – ESG (Umwelt, Soziales und Unternehmensführung) – umschrieben. Da es sich nicht um verbindliche Vorgaben handelt, können Unternehmen diese Richtlinien für sich selbst festlegen, müssen dann aber auch selbst auf die Einhaltung und Umsetzung achten. Das ist eine Herausforderung, jedoch keine unlösbare, bei der Sie das Produktportfolio von Diligent unterstützen kann.

Die Zeiten, in denen allein harte betriebswirtschaftliche Kennzahlen den Erfolg und Wert von Unternehmen bestimmten, sind lange vorbei. Die Erwartungen, die die Gesellschaft an verantwortungsvolle Unternehmen stellt, finden sich auch immer häufiger bei Investoren wieder. ESG-Portfolios, wie sie beispielsweise von Blackrock aufgelegt wurden, sind im Trend. Unternehmenswerte, die in den sozialen und Umweltbereich einzahlen, sind also nicht nur ein Nice-to-Have, sondern können große Auswirkungen auf die finanzielle Situation haben.

Hintergrund zu ESG

Zum ersten Mal tauchte der Begriff 2006 im Rahmen der Initiative Principles for Responsible Investment der Vereinten Nationen auf. Seitdem verzeichnen nachhaltige Investments ein stetiges Wachstum. 2020 befassten sich auch das Weltwirtschaftsforum in Davos und der International Business Council (IBC) mit den ESG-Prinzipien. Dort wurden 22 Metriken definiert, deren Messung für die ESG-Beurteilung ausschlagegebend sein soll. Ziel des Ganzen soll ein neuartiger „Stakeholder-Kapitalismus" sein. Die 120 großen multinationalen Unternehmen im IBC wollen hier mit gutem Beispiel vorangehen. Das Davos Manifest 2020 als zentrales Dokument des Weltwirtschaftsforums zeigt, welchen Stellenwert die ESG-Prinzipien mittlerweile haben.

Vorbehalte ausräumen

An vielen Stellen im Unternehmen mag es noch Vorbehalte oder sogar Widerstände gegenüber ESG-Initiativen geben. Das könnte aber auch tatsächlich mit einem Mangel an Wissen zu erklären sein. Viele Vorstände sehen bisher hinter ESG-Initiativen eher eine Sammlung von wohlklingenden Buzzwords. Der Umstand, dass es verschiedene Rahmenwerke und Rating-Agenturen für ESG gibt, verstärkt die Verwirrung noch. Das sollte aber Unternehmen nicht von diesen wichtigen Projekten abhalten. Stattdessen benötigen sie ein Framework sinnvoller Kennzahlen, um messbare Ergebnisse vorweisen zu können. Studien zufolge können Unternehmen, die nach ESG-Prinzipien handeln, ihr Risiko signifikant verbessern, während es für nachlässige Firmen steigt. Außerdem legen heute immer mehr Arbeitnehmer Wert darauf, für ein nachhaltiges Unternehmen mit starken Werten zu arbeiten.

Kunden wollen auch immer genauer wissen, wo Produkte herkommen, die sie kaufen und wie diese produziert werden. Um derartige Fragen ihrer Kunden zufriedenstellend zu beantworten, brauchen Unternehmen einen kompletten Überblick entlang ihrer gesamten Lieferkette. Antworten auf derartige Fragen von Konsumenten zu haben, kann sich wiederum auch finanziell auszahlen. Verbraucher sind durchaus bereit, für nachhaltige und sozial verträgliche Produkte einen höheren Preis zu bezahlen. Insgesamt können ESG-Initiativen also ein lohnendes Investment darstellen.

Doch zunächst müssen sich Unternehmen die Frage stellen, nach welchen Standards sie sich richten wollen. Neben des Sustainable Development Goals der Vereinten Nation existieren noch weitere Frameworks, eines der bekanntesten dürfte die Global Reporting Initiative (GRI) darstellen. Von Morgan Stanley Capital International wurde ein Framework veröffentlicht, das sich besonders auf Investments fokussiert. Daneben existieren noch etliche weitere Modelle, die alle eine unterschiedliche Methodik nutzen und andere Kennzahlen liefern. Daher ist es von größter Wichtigkeit, dass sich Unternehmen im Vorfeld klar werden, was sie messen wollen und wel-

GOVERNANCE

MODERNE ESG-LÖSUNGEN ERLAUBEN NICHT NUR INTERNES MEASUREMENT, SONDERN AUCH BENCHMARKING MIT DIREKTEN KONKURRENTEN ODER EINEM BRANCHENINDEX. SO SEHEN UNTERNEHMEN DIREKT, WO SIE GEGENÜBER DER KONKURRENZ NOCH NACHHOLBEDARF HABEN UND WAS DIESE BESSER MACHT.

Peter Herr, Regional Sales Director Germany, Diligent, www.diligent.com

ches Framework für diesen Zweck am besten passt.

Mit einer All-in-One-Plattform zum Ziel

Wenn die Relevanz von ESG erkannt wurde und Unternehmen sich für ein bestimmtes Framework entschieden haben, nach dem sie ihren Erfolg messen und beurteilen wollen, stehen sie vor der Frage, wie sich das alles im Geschäftsalltag umsetzen lässt. Mit der richtigen Software können Verantwortliche das aber auch vergleichsweise einfach bewerkstelligen. Eine Plattformlösung vereint idealerweise die Komponenten internes Audit, Risikomanagement und Verbesserungsplanung. Dort können Unternehmen auch Zugang zu ganzen Bibliotheken mit verschiedenen Measurement-Standards erhalten, sodass für ihre Branche der richtige enthalten sein sollte.

Gegenüber dem gewählten Standard kann dann der Fortschritt des eigenen Unternehmens gemessen und dargestellt werden. Dashboards und automatisierte Berichte sparen darüber hinaus Zeit, indem sie die Abhängigkeit von manuellen Methoden zum Abrufen geschäftskritischer Informationen über Compliance und Richtlinien verringern. Die so erzielten Erfolge können außerdem direkt in der Software visualisiert werden. Um stets auf dem neuesten Stand zu bleiben, erlaubt die Software Unternehmen auch, Trends und Nachrichten zu überwachen, sodass sie schnell auf neue Entwicklungen im Bereich ESG-reagieren können.

Moderne ESG-Lösungen erlauben aber nicht nur internes Measurement, sondern auch Benchmarking mit direkten Konkurrenten oder einem Branchenindex. So sehen Unternehmen direkt, wo sie gegenüber der Konkurrenz noch Nachholbedarf haben und was diese besser macht.

ESG als strategisches Asset

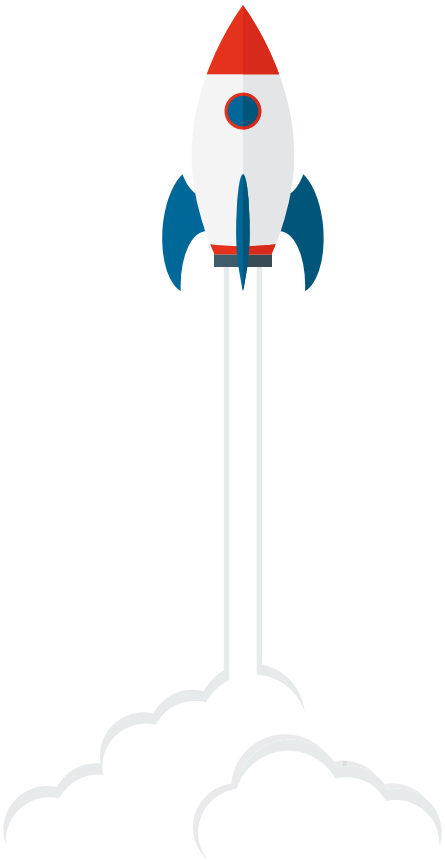
Unternehmen, denen es gelingt, konkrete ESG-Ziele zu definieren und ihre Fortschritte auf diesem Weg mittels geeigneter Software-Lösungen darzustellen, haben schon viel geleistet. Da diese Maßnahme aber kein Selbstzweck bleiben sollen, müssen die ESG-Initiativen auch in der Außendarstellung des Unternehmens klar erkennbar sein – nur so können sich beispielsweise potentielle Investoren ein Bild machen. Unternehmen, die ihre ESG-Anstrengungen als Vorteil für ihre langfristige Geschäftsentwicklung nutzen möchten, sollten die folgenden Fragen beantworten können:

- Sind ESG-Risiken in das ERM-Programm des Unternehmens einbezogen? Wenn ja, was sind die wichtigsten ESG-Risiken und wie gehen wir mit ihnen um? Wie ist ESG in unsere langfristige Strategie eingebettet?
- Verfügen wir über ein Nachhaltigkeits- oder Corporate-Responsibility-Team, das als Bindeglied zwischen dem Unternehmen und den Investoren agieren kann?
- Sind wir darauf vorbereitet, unsere ESG-Strategien und -Risiken zu überwachen? Bekommt der Vorstand die richtigen Kennzahlen, um eine angemessene Überwachung zu gewährleisten?
- Haben wir die Verwendung eines Rahmenwerks zur Bewertung und Berichterstattung von ESG-Kennzahlen auf Unternehmensebene in Betracht gezogen?
- Können wir die Transparenz in unseren ESG-Offenlegungsprozessen verbessern, um die Erwartungen der Investoren zu erfüllen?
- Erzählen wir unsere ESG-Geschichte effektiv? Ist es für Investoren klar, wie ESG mit der übergeordneten Strategie unseres Unternehmens zusammenhängt? Sind die Führungskräfte, die sich mit den Aktionären treffen, in der Lage, diese Fragen zu beantworten?
- Wenn es gelingt, eindeutige ESG-Ziele zu definieren, den Fortschritt dorthin zu messen und das konsistent nach außen zu kommunizieren, sind Unternehmen auf einem guten Weg, um den gesellschaftlichen Anforderungen von heute gerecht zu werden.

Peter Herr

GUTE DATEN, SCHLECHTE DATEN

DAS ASSET FÜR DEN UNTERNEHMENSERFOLG



Daten gelten als das neue Öl. Doch um ihr Potenzial ausschöpfen zu können, müssen sie qualitativ hochwertig sein und korrekt genutzt werden. Das betrifft auch die Stammdaten. Denn sie enthalten Grundinformationen über betrieblich relevante Objekte wie Produkte, Dienstleistungen, Lieferanten, Kunden sowie Personal und werden zur laufenden Verarbeitung in Geschäftsprozessen benötigt. Stammdaten im Rahmen eines Master Data Managements (MDM) entsprechend zu organisieren, ist daher für jedes Unternehmen essenziell.

Häufig aber wird das MDM unprofessionell betrieben. Unternehmen halten Stammdaten in verschiedenen Quellen redundant vor, zum Beispiel im ERP- und im CRM-System sowie zusätzlich bei einigen Mitarbeitern lokal. Zudem werden die Daten oft manuell mit Programmen wie Microsoft Excel gepflegt. Das kann schnell zu Inkonsistenzen führen, wenn Änderungen an nur einer Stelle vorgenommen werden – erfolgen sie indes systemübergreifend, ist damit ein erheblicher Aufwand verbunden. Zudem verlieren Unternehmen den Überblick, welche Daten aktuell sind und ob beziehungsweise wo Änderungen, etwa bei Familienstand, Adresse oder Rechtsform, bereits erfasst wurden. Nicht zuletzt gelangen Daten durch Tippfehler oder Betrugsversuch fehlerhaft ins System. Die Folgen: Die Kosten für Datenhaltung und Datenpflege explodieren. Gleichzeitig führen fehlerhafte Prozesse zu Beschwerden und Korrekturen, zu Retouren, einer sinkenden Conversion Rate und so weiter. Allein die Vernachlässigung der Adressqualität kostet nach einer Faustregel 100 Euro pro Datensatz.

MIT DEN KORREKTEN DATEN UND DEM PASSENDEN KONZEPT IST EINE OPTIMALE ZIELGRUPPENANSPRACHE MÖGLICH UND MARKETING-AKTIONEN FÜHREN ZU BESSEREN ERGEBNISSEN.

Bud Walker, Vice President of Enterprise Sales & Strategy, Melissa, www.melissa.de

Konzept und Software – ein unschlagbares Team

Professionelles MDM wirkt dem entgegen. Wichtig ist eine Vorgehensweise, die strategische Planungen, die Organisation sowie die Wahl einer geeigneten Methodologie und Technologie einschließt. Grundsätzlich sollten Stammdaten immer nur in einem System hinterlegt werden – Stichwort Golden Record. In Bezug auf bereits vorhandene Daten ist zunächst eine Überprüfung und Bereinigung zu empfehlen. Anschließend gilt es sicherzustellen, dass nur korrekte Daten ins System gelangen. Zeitgemäße Cloud-Services wie von Melissa leisten hierbei gute Dienste. So lässt sich Datenvalidierungssoftware in Shopsysteme einbinden. Dort prüft die Lösung in Echtzeit eingegebene Adressdaten rund um den Globus und kontrolliert auch weitere Daten auf Plausibilität. Ob Titel, Name, Straße, Postleitzahl, E-Mail-Adresse, Telefonnummer oder IP-Lokalisierung – sämtliche Bestandteile eines Kontaktes können verifiziert, ihre Schreibweise geprüft und Alternativen zur Vervollständigung angeboten werden. Eine Autovervollständigung sorgt darüber hinaus für Benutzerfreundlichkeit, denn nach Eingabe einiger Buchstaben durch den User werden ihm passende Vorschläge angezeigt, unter denen er lediglich noch auszuwählen braucht. Dadurch halbieren sich die Tastenanschläge und das Risiko einer fehlerhaften Eingabe.

So wird es für Unternehmen ein Leichtes, die Qualität ihrer Stammdaten zu sichern, Kosten für fehlerhafte Daten zu vermeiden und eine zuverlässige Basis für Prozesseffizienz zu schaffen. Denn mit den korrekten Daten und dem passenden Konzept ist eine optimale Zielgruppenansprache möglich und Marketingaktionen führen zu besseren Ergebnissen. Etwaige Sendungen erreichen die Kunden innerhalb kürzester Zeit. Dies wirkt sich positiv auf die Kundenzufriedenheit aus. Kurz: Stammdaten werden so zu einem Asset für den Unternehmenserfolg.

Bud Walker

OPERATIONAL SERVICES
YOUR ICT PARTNER

DATA CENTER KONSOLIDIEREN CLOUD SERVICES INTEGRIEREN

ICT Transformation sicher, verlässlich und stabil umsetzen

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

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

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

operational-services.de/transition-transformation

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

SO ETWAS KANN MAN MIETEN?

COLOCATION IM TSI-LEVEL-4-RECHENZENTRUM

Ulrich Parthier, Herausgeber IT Management, spricht mit Florian Sippel, COO und Rechenzentrumsplaner bei noris network AG, über neue Hochsicherheitsrechenzentrumsflächen des Nürnberger IT-Dienstleisters.

Ulrich Parthier: *noris network wirbt seit Langem mit den hohen Sicherheitsstandards ihrer Rechenzentren. Inwiefern ist Ihr jüngster Neubau etwas Besonderes?*

Florian Sippel: Unser neues Colocation-Rechenzentrum in Nürnberg wird derzeit nach Trusted Site Infrastructure Level 4 und DIN EN 50600 zertifiziert und gehört damit nach diesen Kriterien zum sichersten Colocation-Rechenzentrum in Deutschland. Weltweit gibt es erst 12 Rechenzentren, die dieses Niveau erreicht haben. Bisher gibt es keine Einrichtungen auf diesem Niveau, in denen Unternehmen Flächen und Cages für die eigenen Server mieten könnten und gleichzeitig IT- und Cloud-Services aus einer Hand beziehen.

Ulrich Parthier: *Wenn man bedenkt, dass viele Bankenrechenzentren nicht mehr als TSI Level 3 haben, erscheint ein Colocation-Rechenzentrum mit TSI Level 4, mit Verlaub, ein wenig extrem. Wie kommt man darauf, so etwas anzustreben?*

Florian Sippel: Im Gegensatz zur Klassifikation nach dem Standard des Uptime Institute endet die Auditierung nach dem Trusted-Site-Infrastructure-Standard nicht mit der Inbetriebnahme, sondern umfasst auch den Betrieb. Das ist extrem sinnvoll und kommt unserem Anspruch gelebter Sicherheit entgegen. Wir hatten am Standort Nürnberg Süd, direkt neben unserer Unternehmenszentrale, noch freie Fläche und haben dort nebeneinander zwei weitere Rechenzentren mit zusammen 4.000m Quadratmetern IT-Fläche errichtet. Das eine haben wir für FI-TS gebaut, die Finanz Informatik Technologie Service GmbH & Co. KG, ein IT-Partner von Landesbanken und Finanzwirtschaft. Der Kunde hatte hohe Anforderungen und strebte dafür auch TSI Level 4 an. Wir haben uns entschlossen, in dem zweiten Rechenzentrumsabschnitt mit 2.000 Quadratmetern IT-Fläche das identische Sicherheitsniveau zu verwirklichen, wie wir es für den ersten Kunden erarbeitet haben und wie es jetzt dem TÜV zur Prüfung vorliegt. Mit beiden Rechenzentren gemeinsam in die Auditierung zu gehen, hat Vorteile. So ist bei TSI Level 4 schon die Standortwahl bezüglich möglicher Elementarrisiken und Umgebungsgefahren entscheidend. Hier sind wir in der glücklichen Lage, einen geologisch, städtebaulich und verkehrstechnisch unbedenklichen Standort zu haben – also

beispielsweise außerhalb von Einflugschneisen oder fernab von großen Industriebetrieben. Und es gibt natürlich Synergieeffekte: Der Perimeterschutz umfasst beide Rechenzentren. Zu diesem gehören Fahrzeugschleusen und Roadblocker, die auch schwere Lkws stoppen können. Das Gelände ist extrem gut gesichert, die Maßnahmen sind aber dezent gestaltet.

Ulrich Parthier: *Wie spiegelt sich der Sicherheitsanspruch in der Architektur des Rechenzentrums selbst wider?*

Florian Sippel: Wie schon bei unserem Rechenzentrum in Aschheim bei München folgt der Bau dem Schalenprinzip aus der EN 50600. Jeweils ein Sicherheitsbereich umschließt den nächsthöheren, es gibt keine direkten Zugänge zur IT-Fläche. Die Zonen sind durch Vereinzelung und biometrische Zutrittskontrolle von jeder anderen Zone getrennt. Diese Prinzipien haben wir in den beiden neuen Rechenzentren perfektioniert. Auch Fahrzeuge, mit denen beispielsweise IT-Equipment angeliefert wird, werden konsequent vereinzelt und an jeder Personenschleuse ist eine Zwei-Faktor-Authentisierung nötig. Die technischen Bereiche mit den modularen Energie- und Klimatisierungszellen, für die wir wieder das energieeffiziente KyotoCooling verwenden, sind baulich getrennt von den IT-Flächen. Es gibt nach Rollen getrennte Flure und Zugangskontrollen für IT-Personal und Techniker. Wer die Notstromaggregate wartet, hat keine Möglichkeit, auch nur in die Nähe von Servern zu kommen.

Ulrich Parthier: *Sie sagten, ein Vorteil von TSI gegenüber anderen Normen im Bereich der Rechenzentrumsinfrastruktur sei der Fokus auf den Betrieb? Wie gehen Sie da vor?*

Florian Sippel: Man braucht starke Prozesse, deren Einhaltung man lückenlos überwachen muss. Das betrifft zum einen die physischen Betriebsbedingungen für die IT-Systeme. Hier haben wir ein einzigartig hohes Maß an Granularität im Monitoring realisiert, beispielsweise beim Sensorennetz für Luftfeuchtigkeit und Temperatur. Das betrifft aber auch die Überwachung jeglicher Aktivitäten. Die Videoüberwachung der Anlage ist lückenlos und zusammen mit der Identifikation jeder Person an jeder vereinzelnden Schleuse ist sichergestellt: In diesen Rechenzentren bewegt sich niemand, dessen genauer Standort nicht in jeder Sekunde dokumentiert wäre. Als zusätzliche Sicherheitsmaßnahme gilt ein Vier-Augen-Prinzip für den Zugang zu IT-Hardware: Cages können nur zu zweit betreten werden, niemals könnte sich eine einzelne Person an den Systemen zu schaffen machen. Das Überwachungssystem lässt keine Ausnahmen zu. Auch nicht für Topmanager. Potenzielle Kunden, die die Anlage besichtigen wollen, müssen Zeit mitbringen. Wer das Rechenzentrum betreten will, muss sich den Prozeduren der Zwei-Faktor-Authentisierung und Vereinzelung unterwerfen.

VIELLEICHT SIND WIR IN PUNCTO ZERTIFIZIERUNG UND SICHERHEIT EXTREM, ABER ES GIBT EBEN UNTERNEHMEN, DIE SICH GENAU DIES VON EINEM IT-PARTNER WÜNSCHEN.

Florian Sippel, COO und Rechenzentrumsplaner noris network AG, www.noris.de

Ulrich Parthier: *Wer wären potenzielle Kunden für TSI Level 4 Colocation?*

Florian Sippel: Lassen Sie mich ein plakatives, aber durchaus realistisches Szenario nennen: Eine Rechtsanwaltskanzlei, die im Auftrag eines großen internationalen Unternehmens ein Verfahren gegen einen US-Konzern führt. Weder Unternehmen noch Kanzlei werden wollen, dass die Daten auf Servern eines US-Cloud-Anbieters liegen oder dass die Einhaltung wichtiger Eingabefristen an Gerichten durch mangelnde Verfügbarkeit von Systemen gefährdet wird. Es geht um Datenschutz und Datensicherheit. Wer hochverfügbare Systeme betreibt, braucht auch eine extrem zuverlässige Rechenzentrumsinfrastruktur. Und ein TSI-Level-4-Rechenzentrum selbst zu bauen, ist für ein einzelnes Unternehmen nur in Ausnahmefällen wirtschaftlich. Wer durch branchenspezifische Normen oder Auflagen von Aufsichtsbehörden einen sicheren IT-Betrieb nachweisen muss, hat in einem zertifizierten Hochsicherheitsrechenzentrum die besten Voraussetzungen. Wir erwarten Nachfrage besonders aus dem Finanz- und Versicherungsbereich, der Rechtspflege und von KRITIS-Institutionen. Aber auch für industrielle Anwendungen wie Produktionssteuerungssysteme könnte unser neues Rechenzentrum ein sicherer Hort sein. Prinzipiell gibt es zwei Gründe, gerade in diesem Rechenzentrum Flächen zu mieten: ein reales, sehr hohes Schutzbedürfnis oder die Notwendigkeit, höchste Sicherheitsmaßnahmen nachweisen zu können. Gerade Kunden, die hier Verpflichtungen haben, können wir sehr gut unterstützen. Um Ihre Frage zu Anfang nochmals aufzunehmen: Ja, vielleicht sind wir in puncto Zertifizierung und Sicherheit extrem, aber es gibt eben Unternehmen, die sich genau dies von einem IT-Partner wünschen.

Ulrich Parthier: *Herr Sippel, vielen Dank für dieses informative Gespräch.*

TPM-ANBIETER ALS GLOBALER PARTNER

GEGEN HARDWARE-AUSFÄLLE UND KOSTENDRUCK

Seit Jahren richten sich Wachstumsbestrebungen deutscher Unternehmen verstärkt ins Ausland. Nicht nur Konzerne denken und handeln global, auch der Mittelstand unterstützt seine Marktposition durch Niederlassungen in Europa, Asien oder Amerika. Für IT-Abteilungen ist der Aufbau oder gar der Kauf von Standorten im Ausland oft eine große Herausforderung. Gewachsene, heterogene IT-Landschaften erworbener Niederlassungen in die eigenen Systeme zu integrieren ist kompliziert. Ebenso den reibungslosen Betrieb der Systeme und Rechenzentren über die Distanz hinweg zu gewährleisten. Nun tritt noch ein neuer Herausforderer auf das Spielfeld: der gestiegene Kostendruck aufgrund der weltweiten Wirtschaftskrise, ausgelöst durch die Covid-19-Pandemie. Drittwartung durch einen globalen Dienstleister kann eine Möglichkeit sein, die Wartung der Systeme und Rechenzentren im In- und Ausland zu stemmen, die Ausfallsicherheit zu erhöhen und gleichzeitig die Betriebskosten zu senken.

IT-Abteilungen international agierender Mittelständler stehen vor einer schwierigen Aufgabe. Sie haben auf globaler Ebene die gleichen Anforderungen an ihre IT-Landschaft wie große Unternehmen, sie müssen diese Aufgabe aber mit wesentlich weniger Personal bewältigen. Je nach Größe des Standorts im Ausland verfügt dieser nicht über eigene Verantwortliche für die IT-Infrastruktur oder eben nicht mit den nötigen Kapazitäten. Daher sind viele Unternehmen entweder auf die Wartung ihrer IT-Systeme durch die Hersteller oder durch Dienstleister vor Ort angewiesen. Doch die Herstellerwartung ist ein hoher Kostenfaktor. Zudem hat eine Umfrage der Technogroup IT-Service GmbH aus dem Jahr 2019 ergeben, dass nur 17 Prozent der Befragten mit dem Wartungsangeboten der Hersteller zufrieden sind, kein Teilnehmer war sehr zufrieden, 62 Prozent waren weniger oder gar unzufrieden.

Auch einzelne Wartungsdienstleister vor Ort können Nachteile mit sich bringen. Es ist für die IT-Abteilungen aufwendig mit den jeweiligen Dienstleistern vor Ort Verträge zu schließen und diese zu erweitern, wenn neue Hardware in die Infrastruktur Einzug hält. Gegebenenfalls unterscheiden sich die Service Level Agreements (SLAs) in den einzelnen Ländern. Zudem sind sie oft anders als es die Unternehmen von Dienstleistern und Herstellern in Deutschland gewohnt sind. Die Kontrolle der Qualität der Dienstleister ist zudem über die räumliche Distanz hinweg schwierig. Noch schwieriger ist es, ein Vertrauensverhältnis über die Entfernung hinweg aufzubauen. Kommt es zu einer Störung oder gar einem Ausfall der Hardware in einer Niederlassung im Ausland sind schnelles Handeln und Vertrauen in den Dienstleister aber maßgeblich.

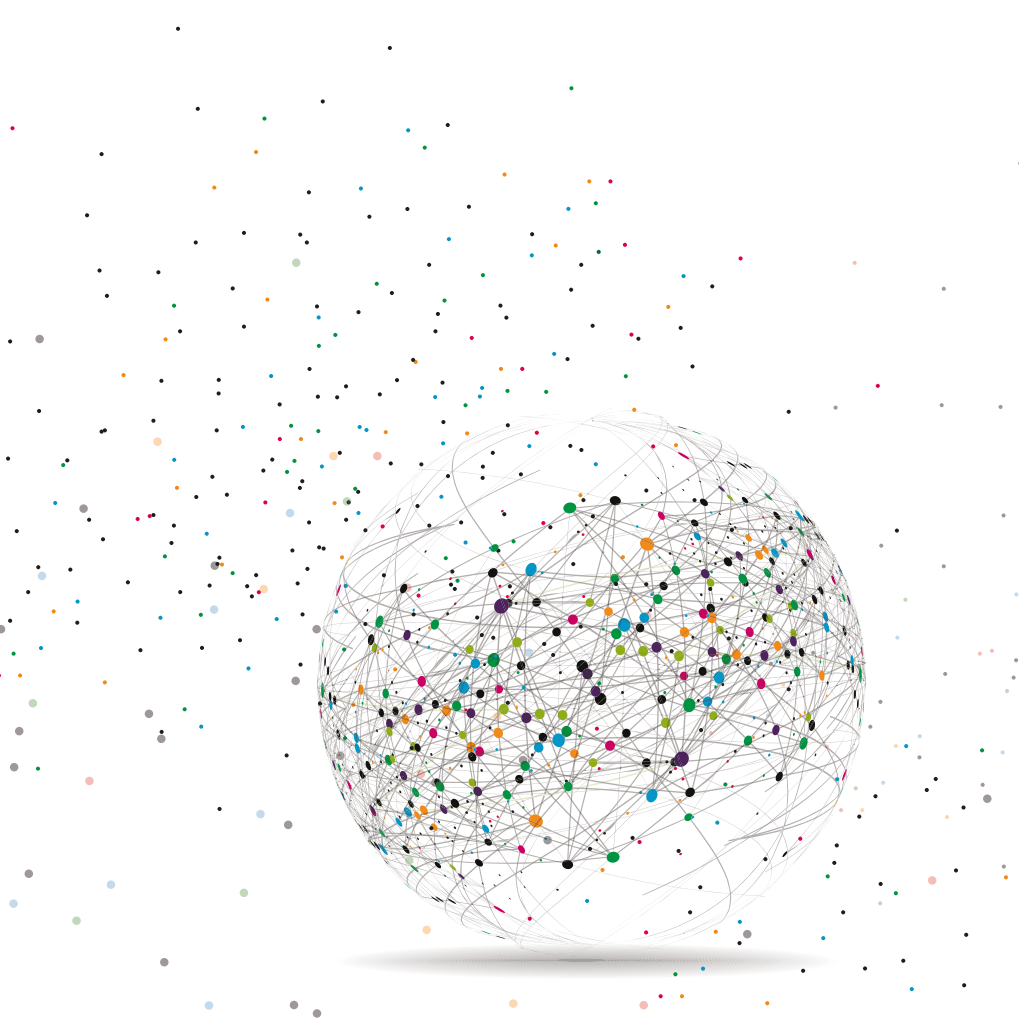
EIN TPM-ANBIETER KANN HARDWARE AUCH NACH DEM ENDE DES SUPPORTS DURCH DEN HERSTELLER WARTEN. SO KANN SIE LÄNGER SICHER IN BETRIEB SEIN UND TEURE NEUINVESTITIONEN EINGESPART ODER VERSCHOBEN WERDEN.

Klaus Stöckert,
CEO, Technogroup IT-Service GmbH,
www.technogroup.com

Globale Abdeckung mit einem zentralen Partner

International ausgerichtete Drittwartungs-Dienstleister können eine sinnvolle Alternative zur Wartung durch den Hersteller oder durch einzelne Dienstleister vor Ort sein. Sie sind in vielen Ländern mit eigenem Personal vertreten und bieten dort direkt ihre Dienstleistung sowie Kundenbetreuung an. Zudem verfügen sie über ein qualitätsgesichertes weltweites Partner-Netzwerk. Damit können große Anbieter von Third-Party Maintenance (TPM) einen qualitätsgesicherten Service rund um den Globus anbieten.

Wenn notwendig, schließt der Drittwartungsanbieter dabei Partnerverträge mit Dienstleistern in anderen Ländern ab. Dadurch erweitert er seine geografische Präsenz und seine Kapazitäten für den Kunden. Die Partner übernehmen gegenseitig qualitätsgarantiert die Dienstleistung in ihrer jeweiligen Region. So schließt ein TPM-Anbieter in Deutschland zum Beispiel einen Vertrag mit einem indischen Partner, der die Betreuung des



Kunden vor Ort in der Niederlassung in Mumbai übernimmt. Die Vorteile dieses internationalen Netzwerks für den Kunden sind vielfältig:

➤ Er hat einen festen Ansprechpartner für Hardware-Probleme weltweit. Das minimiert nicht nur die Reaktionszeit bei einer Störung, sondern ist auch die Grundvoraussetzung dafür, eine Vertrauensbasis aufzubauen.

➤ Er hat festgelegte Service Level Agreements, die eine schnelle Reaktionszeit überall auf dem Globus gewährleisten

➤ Er hat eine hohe Service-Qualität, die sein TPM-Anbieter in Deutschland sicherstellt

➤ Er kann auch refurbished Hardware in seine Systeme integrieren. Der Dienstleister kann die gebrauchten, aber sorgfältig getesteten und qualitätsgarantierten Komponenten im Rechenzentrum ergänzen, warten und ersetzen. Der Einsatz von refurbished Hardware schafft ein Einsparpotenzial von bis zu 50 Prozent gegenüber Neuware. So können hochqualitative Hardware-Komponenten auch in finanziell schwächer aufgestellten Niederlassungen genutzt werden, da die Investitionssumme geringer ausfällt.

Mit Drittwartung Betriebskosten senken

Womit wir bei dem zweiten Thema wären: dem gestiegenen Kostendruck der Unternehmen, der auch in den IT-Abteilungen spürbar ist. Die Covid-19-Pandemie hat viele Branchen in aller Welt wirtschaftlich geschwächt. In einer aktuellen Umfrage der Technogroup IT-Service GmbH, gaben fast drei Viertel der Befragten an, negative Auswirkungen durch die Coronakrise und die damit einhergehende Wirtschaftskrise zu verspüren. Die Firmen reagieren auf diese Herausforderung, indem sie Prozesse optimieren, Investitionen verschieben oder Budgets kürzen. Das Bestreben der Geschäftsleitung, die Kosten für die Hardware und IT zu senken, wird von 62 Prozent der Umfrage-Teilnehmer als hoch oder sehr hoch angesehen.

Da lohnt sich ein Kostenvergleich der unterschiedlichen Möglichkeiten der Hardware-Wartung. Bereits 2019 errechneten die Analysten von Gartner ein Einsparpotenzial von bis zu 70 Prozent, wenn Unternehmen von der Herstellerwartung auf Third-Party Maintenance umsteigen. Diese Zahl beruht zum einen auf der Tatsache, dass herstellerunabhängige Drittwartungs-Dienstleister oft deutlich flexiblere und wirtschaftlichere Konditionen bieten als die OEMs. Zudem entfällt ein Großteil des Administrationsaufwands, da es nur einen Ansprechpartner gibt.

Ein weiterer, sehr wichtiger Punkt ist die Zeitspanne, in der die Hardware im Rechenzentrum im Einsatz ist. Hersteller rufen im Schnitt nach drei bis fünf Jahren das End of Service Life (EOSL) für Geräte aus. Dennoch können Server und andere Hardware deutlich darüber hinaus genutzt werden – ohne Kompromisse bei der Verfügbarkeit oder Performance-Verluste. Viele Unternehmen haben ihre Hardware im Rechenzentrum bis zu zehn Jahre oder sogar darüber hinaus im Einsatz. Ein TPM-Anbieter kann die Hardware auch nach dem Ende des Supports durch den Hersteller warten. Er hält die entsprechenden Ersatzteile vor und verfügt über qualifiziertes Fachpersonal. So kann Hardware länger sicher in Betrieb sein und teure Neuinvestitionen eingespart oder verschoben werden. Das schafft IT-Abteilungen gerade in der jetzigen Zeit wertvollen Spielraum in ihren Budgets und schont die Umwelt.

Nachhaltigkeit erhält im Bereich der Rechenzentrums-Hardware gerade einen Schub durch die Ökodesign-Verordnung 2019/424. Diese hat zum Ziel, dass Geräte künftig länger genutzt werden können. Kurz gesagt: Um die sichere Nutzungsdauer zu erhöhen, sind Hersteller verpflichtet, für bestimmte Server, die ab dem 01. März 2021 auf dem Markt kommen, die sicherheitsrelevante Firmware kostenlos zur Verfügung zu stellen und Firmware zur Funktionserweiterung zwei Jahre nach dem Inverkehrbringen für mindestens acht Jahre kostenlos oder zu fairen Preisen zur Verfügung zu stellen. Das macht Unternehmen unabhängiger von der Wartung durch die Hersteller und gibt ihnen mehr Handlungsfreiraum.

Klaus Stöckert

INTEGRIERTE SMART FACTORY

INTERNET OF THINGS AUF DEM WEG IN DIE INDUSTRIE

Der Begriff Internet of Things (IoT) beziehungsweise „Internet der Dinge" ist in unserem Alltag bereits fester Bestandteil. Und auch im industriellen Umfeld findet gerade ein großer Wandel hin zur Smart Factory statt. Technologien des sogenannten Industrial Internet of Things (IIoT) sind inzwischen so gut weiterentwickelt, dass sie wichtiger Bestandteil von Unternehmen werden und den entsprechenden Mehrwert bieten. Grundsätzlich wird unter IoT die Vernetzung von Gegenständen untereinander beziehungsweise auch nach außen zum Beispiel via Internet verstanden, mit dem Ziel eines Effizienzgewinns. Eines der wichtigsten Schlagwörter in diesem Zusammenhang ist die Vernetzung. Die Gegenstände, die miteinander verbunden werden sollen, werden dazu zu intelligenten Geräten – sogenannten Smart Devices – etwa durch deren Ausstattung mit Mikroprozessoren. So können möglichst viele Informationen erfasst und anschließend miteinander verknüpft werden. Die Geräte können dann sowohl untereinander kommunizieren, bieten darüber hinaus aber auch eine Schnittstelle mit einem Netzwerk, wodurch sie sich vom Anwender von überall aus steuern und bedienen lassen.

> EIN ERP-SYSTEM STEUERT DIE GESCHÄFTSPROZESSE DER VERSCHIEDENEN GESCHÄFTSBEREICHE, ZUDEM LIEFERT ES RELEVANTE BUSINESSDATEN, DIE OFT ALS ENTSCHEIDUNGSGRUNDLAGE FÜR STRATEGISCHE ENTSCHEIDUNGEN DIENEN.
>
> Christian Geißler, Sales Represntative,
> Industrial Application Software GmbH (IAS), www.canias40.de

Anwendungsbereiche

Im privaten Umfeld sind Smart Homes bereits etabliert: Begonnen bei der zentralen Steuerung der Beleuchtung via App lassen sich damit inzwischen ganze Gebäudesysteme steuern. Smart Speaker, wie Amazon Echo oder Google Home integrieren via Sprachsteuerung intelligente Assistenten, um bestimmte Dienste im Internet auszuführen. Daneben nutzen wir Paketverfolgung, Wearables und Ähnliches.

Ebenso vielfältig sind die Anwendungsmöglichkeiten im industriellen Umfeld. Durch die Ausstattung der Geräte mit intelligenten Sensoren sind sie untereinander vernetzt und ständig im Intranet oder Internet präsent, das führt zu einer höheren Flexibilität und Anpassbarkeit auf veränderte Anforderungen. Ein Beispiel ist hier die Variantenfertigung, die für Unternehmen keine Herausforderung mehr darstellt. So kann auf Veränderungen des Marktes durch individuelle konfigurierbare Produkte besser reagiert werden.

Ziel soll eine Fertigung sein, die sich komplett ohne menschliche Eingriffe optimiert. Dies wird auch unter dem Begriff Industrie 4.0 geführt. Es lassen sich nicht mehr nur einzelne Produktionsschritte, sondern ganze Wertschöpfungsketten automatisieren und wesentlich effizienter gestalten. Produktionsabläufe werden so robuster und gestalten sich kosten- und zeiteffizienter, sodass insgesamt ein nachhaltigeres Qualitätsmanagement gewährleistet werden kann.

Die Kommunikation zwischen Produkt und der Fertigungsanlage, beispielsweise über RFID-Chips, ermöglicht so etwa eine autonome Steuerung und Optimierung des Produktionsweges und der Fertigungsschritte. Ein weiterer wichtiger Faktor ist der Wartungsbereich: Durch den Informationsaustausch können Belastungs- und Verschleißdaten, sowie Umgebungseinflüsse von einer Fertigungsmaschine berücksichtigt und genauer eingeplant werden, wann ein Gerät ausgetauscht werden muss.

Informationen sammeln

Durch leistungsfähige Mikroprozessoren lassen sich Geräte mit relativ geringem Aufwand mit elektronischer Intelligenz ausstatten. Ein weiterer Vorteil der Mikroprozessoren ist eine kabelgebundene oder drahtlose Schnittstelle (WLAN, Bluetooth oder Mobilfunk), die zur Anbindung an das Internet und für eine eindeutige Internetadresse genutzt wird. Hierüber können Daten gesendet oder empfangen werden.

Die Daten sind ein wichtiger Bestandteil im Bereich IIoT. Dazu gehören beispielsweise die Zustandsinformationen. Diese können etwa Informationen über die Nut-

Quelle: istock.com/Machine Headz

zung oder Umweltbedingungen liefern und sich daran anpassen. Auch digitale Services sind eine wichtige Datenquelle, die die Parametrisierung von Geräten erleichtern und verbessern. Diese konnten in der Vergangenheit aus Kostengründen oft nicht realisiert werden.

Um die notwendigen Informationen zu erhalten, müssen verschiedene Voraussetzungen geschaffen werden: Dazu zählt die Standardisierung aller IIoT-Gegenstände und Dienste die Einführung einer Netzwerkanbindung für alle IoT-Devices, die einfach zugänglich und sicher ist, die Herabsetzung der Gerätekosten, Inbetriebnahmekosten oder Anschlusskosten für integrierte Teilnehmer sowie die Entwicklung von kostengünstigen, automatisierten (bis hin zu autonomen) digitalen Services im Netzwerk, die den zusätzlichen Nutzen der Vernetzung realisieren.

Sicherheitsaspekte

Durch die Vernetzung der Geräte via Internet besteht grundsätzlich auch immer ein Sicherheitsrisiko. Um diese zu minimieren, ist die Kommunikation zwischen den Geräten so abzusichern, dass sich Abläufe und Prozesse nicht stören oder manipulieren lassen und die erfassten Daten geschützt sind. Dabei werden keine exklusiven Sicherungsmechanismen eingesetzt, vielmehr handelt es sich um die Anwendung verschiedener Maßnahmen auf Software- und Netzwerkebene, um Informationssicherheit zu gewährleiten.

Die Architektur von IoT und deren Komponenten sollte deshalb verschiedene Sicherheitsaspekte berücksichtigen: Dazu zählt etwa ein effizientes und zuverlässiges Identitäts- und Zugriffsmanagement. Außerdem sollten sämtliche über das öffentliche Internet übertragene Daten codiert und die einzelnen Systeme durch Firewalls geschützt werden. Auch die sogenannte Systemhärtung minimiert Angriffsmöglichkeiten. Dazu werden bestimmte Funktionen mit Zugriff auf sensible Daten abgeschaltet. Zuletzt verhilft ein Software- und Patchmanagement über den kompletten Betriebszeitraum bei der Behebung von erkannten Fehlern und Sicherheitsmängeln.

Zusammenspiel von ERP und IIoT

Da ERP-Systeme ein wichtiger Bestandteil von Unternehmen sind, stellt sich natürlich die Frage, wie das Unternehmemssystem sinnvoll mit IIoT-Lösungen zusammenarbeiten kann. Ein ERP-System steuert die Geschäftsprozesse der verschiedenen Geschäftsbereiche, zudem liefert es relevante Businessdaten, die oft als Entscheidungsgrundlage für strategische Entscheidungen dienen. Daten sollen hier also gebündelt werden, während IoT erst einmal eher dezentral und autonom arbeitet und die Komplexität des Gesamtsystems auf eine Vielzahl von Einzelkomponenten verteilt.

IIoT ist jedoch für die Entscheidungsfindung ein wichtiger Lieferant von differenzierten Daten. Die Kommunikation aller Maschinen und Produkte miteinander bietet hier hohes Potenzial und führt zu einer sehr hohen Datenmenge, was als Big Data definiert wird. Diese Datenmenge kann für Unternehmen zu völlig neuen Geschäftsmodellen führen und damit große Chancen bieten. Damit Unternehmensprozesse von diesen Daten profitierten und neue Geschäftsmodelle etabliert werden können, muss die ERP-Software von jedem Ort, zu jeder Zeit und von jedem Endgerät aus erreichbar sein.

Ein anderer Punkt ist die IT-Infrastruktur, die in Echtzeit die dezentralen Daten in Form von Business-Prozessen leistungsstark verarbeiten kann. Dabei müssen diese IT-Infrastrukturen je nach Bedarf skalierbar sein, um auf Leistungsspitzen oder Wachstum flexibel reagieren zu können.

Christian Geißler

S/4HANA-MIGRATION: LEARNING BY DOING?

BESSER VOM EARLY ADOPTER LERNEN UND DIE TRANSFORMATION GANZHEITLICH ANGEHEN

Wer sich jetzt an die S/4HANA-Einführung wagt, kann vom Erkenntnisgewinn der „Early Adopter" profitieren. Thomas Frey, Senior SAP Authorizations Consultant SAST SOLUTIONS, erklärt, was man beim Wechsel unbedingt vermeiden sollte, wo Projekte häufig straucheln und was intelligentes Projektmanagement ausmacht. Dabei verrät er auch die Vorteile einer Tool-Unterstützung.

In einer Kurzumfrage während der IT-Onlinekonferenz „SAP S/4HANA und Digitale Transformation 2021" nach dem Stand ihrer S/4HANA-Migration, antworten im Januar lediglich sieben Prozent der Teilnehmer, sie seien bereits S/4HANA-ready. Während 20 Prozent der Befragten mit der Umstellung immerhin begonnen haben, befinden sich ganze 64 Prozent noch in oder vor der Planungsphase. Gerade für diese gibt es sowohl schlechte als auch gute Nachrichten.

Höchste Zeit für den Wechsel

Zunächst die schlechten Nachrichten: Für den Großteil der Anwenderunternehmen wird die Zeit knapp. Laut Investitionsreport 2021 der DSAG (Deutschsprachige SAP-Anwendergruppe e.V.) dauert der S/4HANA-Umstieg, besonders ohne zusätzliche Expertise, deutlich länger als viele annehmen. 2018 planten 38 Prozent der Unternehmen den Umstieg innerhalb der nächsten drei Jahre, diesen haben heute aber erst 14 Prozent erfolgreich vollzogen. Die absehbare Folge dieser Stagnation: Der Bedarf an professioneller externer Unterstützung wird sich exponentiell steigern und wer weiterhin zögert, unweigerlich auf einen Beratungsstau zusteuern. Wie rasant die Relevanz von S/4HANA zunimmt, wird laut DSAG daran erkennbar, dass Anwenderunternehmen im deutschsprachigen Raum 2021 doppelt so viel in S/4HANA-Vorhaben wie in die SAP Business Suite investieren, während bei 75 Prozent die IT- und SAP-Investitionsbudgets gleichbleiben oder sogar steigen.

Die Herausforderung als Chance begreifen

Nun die gute Nachricht: Wer jetzt den Umstieg ebenso entschlossen wie überlegt angeht und sich kompetente Unter-

stützung an die Seite holt, kann von Beginn an eine ganzheitliche S/4HANA-Migration realisieren, die nicht nur die erhofften Verbesserungen erzielt, sondern auch folgenschwere Fehler vermeidet. „Wir erleben oft, dass Verantwortlichen zu Projektbeginn nicht wirklich bewusst ist, welche Herausforderungen insgesamt vor ihnen liegen, und dass besonders Sicherheit und Berechtigungen gerne erst einmal auf die lange Bank geschoben werden", sagt Thomas Frey, „und das kostet später nicht nur Zeit, sondern verursacht häufig auch erhebliche Extrakosten." Daher seine klare Empfehlung: „Denken Sie Ihre S/4HANA-Migration ganzheitlich: Coding, Prozesse, Berechtigungen."

Ob Green-, Brown- oder Bluefield – es gilt, eine Reihe grundlegender Entscheidungen bereits vor der Einführung von S/4HANA zu treffen, mahnt der Experte. Denn ein Migrationsprojekt biete etwa die ideale Gelegenheit, die IT-Sicherheit mit einer sauber aufgesetzten und ganzheitlich geplanten SAP Security & Compliance-Strategie auf ein neues Level zu heben: „Damit ist diese Herausforderung auch eine Chance, die IT-Sicherheit in SAP-Systemen grundlegend zu verbessern, Rollenkonzepte effizienter zu gestalten und so das neue System mit all seinen Vorteilen zu nutzen."

Aus Anfängerfehlern lernen

Nach seinen Erfahrungen, so Frey, vernachlässigen heute noch zu viele Unternehmen, die eine Migration auf S/4HANA planen, so wie manche Early Adopter zuvor die Absicherung der neuen Systeme. Bei einer Konvertierung sei es jedoch entscheidend, von vornherein eine belastbare und konsistente Grundsicherheit in die Strategie miteinzubeziehen. Das koste zwar zu Beginn mehr Zeit, so vermieden Unternehmen aber nicht nur typische Stolperfallen beim Plattformwechsel wie das Außerachtlassen von Schnittstellen und Altsystemen, sondern auch eine zu späte Überführung der SAP-Berechtigungen. Er empfiehlt: „Planen Sie mehr Zeit ein. Den Fachbereichen fehlt häufig das erforderliche Prozess-Know-how und das Wissen, wie sie künftig in S/4HANA arbeiten wollen. Geschäftsprozesse bereichsübergreifend sinnvoll zu optimieren geht nicht mal eben neben dem Tagesgeschäft."

Eine grobe und noch häufig zu beobachtender Fehleinschätzung seien zudem Altlasten, die ins neue System übernommen werden. „Ich denke hier ganz konkret an Coding. Anstatt zunächst zu analysieren, was wirklich noch gebraucht wird, wird alles 1:1 kopiert. Doch dadurch werden auch alle Sicherheitsmängel mit übernommen und bieten dann beliebte Hintertüren, um Schäden im System anzurichten." Ein hartnäckiger Irrglaube sei zudem, dass die SAP FIORI Apps eine Lösung für nahezu alles sind: „Doch noch sind gar nicht alle Prozesse durch FIORI abgedeckt. Daher ist unsere Empfehlung, FIORI nur da einzusetzen, wo sich ein echter Mehrwert bietet."

S/4HANA ganzheitlich angehen

All diese Stolperfallen sind mit einer guten und von Beginn an ganzheitlichen S/4HANA-Migrationsstrategie vermeidbar, wenn man auf Partner wie SAST SOLUTIONS und ihre Tools setzt. „Aufgrund der vielen grundlegenden Entscheidungen direkt zu Projektbeginn unterstützen wir unsere Kunden von Anfang an, die grundlegenden Fragen individuell für ihr Unternehmen zu beantworten", sagt Thomas Frey. „Welche Transaktionen müssen ausgetauscht werden oder sind obsolet? Wie erkennt man passende FIORI-Apps zu den Rollen? Wie hält man sein Berechtigungskonzept ein?"

Mit dem richtigen Tool sparen Verantwortliche zudem durch die signifikante Reduzierung manueller Arbeiten sowohl Zeit als auch Geld, betont der Experte. „Unsere Software verbessert Analyseergebnisse, gibt eine Empfehlung, ob eine Migration oder eine Neukonzeption der Berechtigungsrollen sinnvoller ist, und liefert direkt Vorschlagswerte. Zudem werden obsolete oder getauschte Transaktionen erkannt beziehungsweise passende FIORI-Apps identifiziert. Also idealerweise ein perfektes Zusammenspiel aus SAP Security & Compliance-Know-how und Tool-Unterstützung, durch das gewährleistet wird, dass im neuen S/4HANA-System unserer Kunden vermeidbare Risiken gar nicht erst auftauchen."

Dominierendes Thema 2021

Gefragt nach seiner Einschätzung, welche Themen in diesem Jahr von Bedeutung für SAP-Anwender sein werden, antwortet Thomas Frey zusammenfassend, dies werde nach wie vor die S/4HANA-Migration sein „und sicherlich, ob mehr Unternehmen von den Early Adopters lernen und beginnen, die S/4HANA-Transformation wirklich ganzheitlich zu betrachten." Und natürlich bleibe es spannend, „wie Unternehmen, die das Thema Migration noch hinauszögern – auch bedingt durch die Pandemie –, mit der zu erwartenden weiteren Verknappung an Berater-Expertise umgehen werden."

DENKEN SIE IHRE S/4HANA-MIGRATION GANZHEITLICH: CODING, PROZESSE, BERECHTIGUNGEN.

Thomas Frey,
Senior SAP Authorizations Consultant SAST SOLUTIONS,
https://sast-solutions.de

PUNKTGENAUER PERSONALEINSATZ

MITARBEITER LOGISTISCH EFFIZIENT PLANEN

Moderne ERP-Systeme für die Losgröße 1+ müssen die Projektabwicklung in allen Phasen durchgängig und effizient unterstützen. Dazu bedarf es variabler Steuerungsinstrumente, die dem Umsetzungsfortschritt entsprechend eine immer feinere Granulierung der Planung zulassen. Das Projektmanagement-ERP-System ams.erp erfüllt diese zentrale Anforderung, indem es beginnend mit seiner inhärenten Ressourcen-Grobplanung bis hin zur detaillierten Personaldisposition alle Projektabschnitte übergreifend steuert.

Viele Einzel-, Auftrags- und Variantenfertiger sehen vor dem Hintergrund wachsender Kundenanforderungen und härterer Vertragsbedingungen die Notwendigkeit, mehr Transparenz in ihre Multiprojektplanungsaktivitäten zu bringen. Das Ziel ist es, die anberaumten Außendienst-, Service- und Montageeinsätze effizienter zu takten und bestmöglich aufeinander abzustimmen. Dazu müssen die Planer (Dispatcher) zunächst wissen, welche Mitarbeiter verfügbar sind, welche Stundenkapazitäten dadurch verplanbar sind und wer aufgrund von Urlaub, Krankheit oder sonstigen Fehlzeiten nicht anwesend ist.

Diese Informationen bilden die Grundlage für die Personaleinsatzplanung. Gerade in dem technisch geprägten Umfeld der Losgröße 1+ spielt jedoch vermehrt der Faktor hinein, dass für eine zunehmende Zahl an Tätigkeiten spezielle Qualifikationen, Fähigkeiten oder Nachweise erforderlich sind. Um die Fachkräfte mit entsprechenden Befähigungen und Berechtigungen optimal in den Planungsvorgang zu integrieren, sind grafische Plantafeln unabdingbar. Mit ihnen lassen sich die verfügbaren Fachkräfte den anstehenden Projektaufträgen punktgenau zuordnen.

MIT DER LÖSUNG ENTSTEHT EINE UMFASSENDE KOMBINATION DER DISPOSITIVEN PLANUNG DER MITARBEITER UND DES MATERIALS.

Jens Schulte,
Product Owner für Workforce Planning,
ams.Solution AG, www.ams-erp.com

Tiefe Integration für eine detaillierte Planung

Um diese detaillierte Personalsteuerung zu ermöglichen, kooperiert ams.Solution eng mit dem Field-Service-Management-Spezialisten Innosoft, zu dessen Software der ERP-Anbieter eine tiefe, bidirektionale Integration geschaffen hat. Die Integration beinhaltet, dass die notwendigen Stammdaten wie Kundenadressen, Personaldaten, Artikelnummern und – wenn vorhanden – der Anlagenstamm ebenso wie die gekennzeichneten Arbeitsgänge aus dem ERP-System an Innosoft übergeben werden. Über das in ams.erp integrierte Modul zur Personalzeiterfassung werden zudem die bekannten Fehlzeiten der Mitarbeiter für die Planung bereitgestellt. In Innosoft werden die Informationen dann um die entsprechenden Skills der Mitarbeiter ergänzt. Gepaart werden die Daten daraufhin in der Plantafel, die aufzeigt, welche Aufträge anstehen und welche freien Kapazitäten noch verplant werden können.

Unter Berücksichtigung der Plantafel sorgt das ERP-System in der Folge dafür, dass die für den jeweiligen Einsatz benötigten Materialien basierend auf der Terminierung der dahinterliegenden Auftragsstückliste an den korrekten Bestimmungsort gelangen.

Nach erfolgter Planung werden die Mitarbeiter über ihre Outlook-Kalender respektive über ihre mobilen Endgeräte informiert. Im Falle von Änderungen der Auftragsreihenfolge erfolgt eine Ad-hoc-Korrektur. Ihre Reise-, Anwesenheits- sowie die Auftragszeiten werden ebenso wie das Material über die mobilen Devices erfasst und gebucht und als Berichte ins Field Service Management übergeben. Die Ist-Zeiten werden sodann in die Plantafel übernommen und die Berichte nach ihrer Freigabe als Tätigkeitsberichte an ams.erp übergeben, wo eine automatisierte Abrechnung gegenüber dem Endkunden erfolgen kann.

Ein weiterer Vorteil der Field-Service-Management-Software ist deren Einbindung von Geodaten zur Optimierung der Tourenplanung. Das System hilft also entscheidend dabei, die Mitarbeiter logistisch effizient zu planen und damit die An- und Abreisezeiten so kurz wie möglich zu halten.

Jens Schulte

LOW-CODE PLATTFORMEN

NICHTS GEHT MEHR OHNE SIE

Low-Code – das wird in der Softwareentwicklung eine der Prämissen für 2021 sein. Was aber ist das Besondere an Low-Code? Alles was Sie über diese Plattformen wissen sollten und wie sie erfolgreich ausgerollt werden, erfahren Sie in diesem eBook.

Highlights aus dem eBook

Low-Code erfolgreich im Unternehmen ausrollen

Auf einer Low-Code Plattform fügen sich einzelne Applikationen wie Bausteine in ein stimmiges Ganzes ein. So können unterschiedliche Use Cases auf einer einzigen Plattform abgebildet werden. Den Rollout eines Low-Code-Projektes gehen Sie am Besten in drei Phasen an.

Konkurrenz für Low-Code: Funktionale Programmierung

Low-Code-Programmierung kommt mit weniger Code aus, was aber mit Kompromissen verbunden ist. Der Beitrag beschreibt, warum die ebenfalls auf Effizienz getrimmte funktionale Programmierung hier punkten kann.

Hyperautomatisierung: ein Begriff, unterschiedliche Interpretationen

IDC beschreibt ihn als den orchestrierten Einsatz von RPA, iBPMS und KI als „intelligente Prozessautomatisierung". Forrester bezeichnet dieses Zusammenspiel von Tools als „digitale Prozessautomatisierung" und bei Gartner ist die automatisierte Orchestrierung mit dem einprägsamen Begriff der „Hyperautomatisierung" verknüpft.

Das eBook umfasst 39 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download

LIVE WEBINAR AM 19.05.2021 11 UHR

PASSWORT LOS, KOPF FREI!

WIE SIE IHR UNTERNEHMEN EFFIZIENTER UND SICHERER MACHEN

Sascha Martens, CTO und Spezialist für Cybersecurity bei der MATESO GmbH

Herrscht bei Ihnen auch das Passwort-Chaos? Durchschnittlich hat jeder Mitarbeiter 15 Login-Daten, die er sich merken muss, und verbringt mehr als 10 Stunden pro Jahr mit der Eingabe von Passwörtern. Das raubt Zeit und Nerven. Deswegen nutzen viele das gleiche, leicht zu merkende Passwort für alle Anwendungen. Das ist einfach für den Mitarbeiter. Und den Hacker. Der Leidtragende ist Ihr Unternehmen. Die Lösung lautet „passwortlos"! Ob Anmeldung per Smartcard, Single Sign-on oder Identity Provider – es gibt unzählige Möglichkeiten, Ihren Alltag passwortlos zu gestalten und gleichzeitig die Sicherheit Ihres Unternehmens zu erhöhen. Damit Sie den Kopf frei haben für die wirklich wichtigen Dinge.

Erfahren Sie in diesem Webinar:

- Wie Sie Ihre Mitarbeiter von der Passwortlast befreien und Ihre IT entlasten
- Wie Sie Ihr Unternehmen effizienter und sicherer machen
- Wieso die Zukunft passwortlos ist – aber nur mit einem Password-Manager

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

DIGITALE TOOLS IN DER VORSTANDSETAGE

ALLES, WAS SIE WISSEN MÜSSEN

Digitale Kommunikation besteht aus dem Senden und Empfangen von Daten. Dabei besteht das Risiko, dass die gesendeten Daten in falsche Hände geraten. Aus diesem Grund führen Mitarbeiter in Vorstandsetagen ihre Besprechungen auf dem Papier aus. Das ist zwar viel Arbeit, bei Vorstandssitzungen sind dann aber immer alle Unterlagen griffbereit. Auf diese Weise entfällt das Risiko auf digitale Datenlecks.

Dieses Whitepaper beschreibt die Trends im Markt der Board Portale. Was sind die Gründe für die Popularität dieser Tools, wie entwickelt sich der Markt und was müssen Führungs- und Verwaltungsmitglieder über diese Innovationen wissen.

WHITEPAPER DOWNLOAD

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

VERNETZTE PRODUKTION

WIE DIE DIGITALISIERUNG FÜR INTEROPERABILITÄT SORGT

WHITEPAPER DOWNLOAD

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

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

KI IM IT-SERVICEMANAGEMENT

WIE KI DIE KAPAZITÄTEN IM IT-SERVICE STEIGERT UND DABEI KOSTEN SENKT

Wie sieht die Zukunft des IT-Servicemanagement (ITSM) aus? Welche Herausforderungen gilt es zu meistern? Und welche IT-Service-Leistungen lassen sich konkret durch die „Königsdisziplin" der Digitalisierung – Künstliche Intelligenz (KI) – verbessern? Der folgende Beitrag zeigt anhand von 6 Impulsen, welches Potenzial KI besitzt.

1. First Level Support entlasten

Virtuelle Agenten, die mit KI-basierten Algorithmen arbeiten, unterstützen überlastete Service-Desks. Denn sie verstehen zum Beispiel, dass „Outlook funktioniert nicht" beziehungsweise „Ich kann keine Mails empfangen" dasselbe bedeuten. Sie sind die Problemlöser für Routineaufgaben. Automatisch werden Tickets erfasst und versendet, deren Status abgefragt, Passwörter zurückgesetzt, Konten gesperrt, Berechtigungen vergeben.

2. Wissen filtern

Gezielt finden – ist eine Schlüssel-Herausforderung für Mitarbeiter im Service Desk, um auch bei komplexen Themen und vielfältigen Quellen ihre Tickets effizient bearbeiten zu können. KI-basierte Assistenten helfen, indem sie Ähnlichkeiten zwischen Vorschlägen erkennen, bewerten und relevante Ressourcen vorschlagen, zum Beispiel passende Broschüren, „How to-Videos", Anleitungen.

3. Zum richtigen Experten leiten

Predictive Routing erkennt Routine- oder spezifische Anfragen und die Priorität von Tickets: Je nach identifiziertem Thema lassen sich dadurch Tickets automatisch an den richtigen Service-Agenten weiterleiten. NLP-basierte KI kann die Dringlichkeit einer Anfrage bewertet und Prio1-Tickets bevorzugt weiterleiten.

KÜNSTLICHE INTELLIGENZ WIRD DIE IT-SERVICE-WELT IN DEN NÄCHSTEN JAHREN GRUNDLEGEND VERÄNDERN. CIOS HABEN MIT EINER PROFESSIONELLEN ITSM-LÖSUNG EINE GUTE GRUNDLAGE, UM IHRE IT-SERVICES MIT KI SUKZESSIVE ZU VEREDELN.

Dr. Benjamin Strehl, CIOs, USU Software AG, www.usu.com

4. Fehler und Störungen rechtzeitig erkennen

Moderne, KI-basierte Systeme erlauben inzwischen eine vorausschauende Wartung von IT-Komponenten und optimieren so Wartungskosten und -zyklen. Dazu lesen sie zahlreiche Zustands- und Funktionsdaten wie beispielsweise die Temperatur der Devices, Latenzzeiten, die Anzahl der Schreib- und Lesezugriffe, Logfiles und ähnliches aus und melden ggf. Anomalien.

5. Optimierungspotenziale identifizieren

Durch kontinuierliche Analysen und Mustererkennung lassen sich Schwachstellen bei Anwendungen und im Service erkennen und verbessern. Als virtueller Trainer eingesetzt, kann KI außerdem die User Experience der Service-Mitarbeiter verbessern, indem sie zum Beispiel Redundanzen in Abläufen erkennt oder die ideale Kategorisierung und Priorisierung von Aufgaben übernimmt.

6. Vor Betrug und Identitätsdiebstahl schützen

Durch KI bleiben auffallende Verhaltensänderungen oder Aktivitäten in standardisierten Nutzerprofilen nicht unbemerkt. Bei verdächtigen Aktionen dem Herunterladen großer Datenmengen greifen automatisch Schutzmechanismen wie Kontosperrung oder das Anfordern einer Zwei-Faktor-Identifizierung. Das Risiko von Schäden wird so minimiert, ohne dabei die Persönlichkeitsrechte der Betroffenen einzuschränken.

KI & ITSM – es rechnet sich

Künstliche Intelligenz wird die IT-Service-Welt in den nächsten Jahren grundlegend verändern. CIOs haben mit einer professionellen ITSM-Lösung eine gute Grundlage, um ihre IT-Services mit KI sukzessive zu veredeln. Das ist auch nötig, um die großen Herausforderungen vor allem im Bereich der Automatisierung zu meistern. Nicht nur der Maschinenbau, auch die IT kann durch KI-gestützte datengetriebene Services neue Servicemodelle anbieten und außerdem ein begeisterndes persönliches Service-Erlebnis schaffen. Denn das Erlernen von Vorlieben und Verhaltensweisen von Kunden ist die Voraussetzung für höchste Kundenzufriedenheit – und rechnet sich.

Dr. Benjamin Strehl

WHITEPAPER DOWNLOAD

Dieser Artikel ist ein Auszug aus einem Whitepaper, das hier heruntergeladen werden kann:
https://bit.ly/39MnMuj

TIPPS FÜR EINE SICHERE RÜCKKEHR INS BÜRO

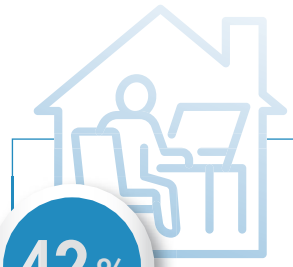
DIGITALES UMDENKEN FÜR EINE INTELLIGENTE UND INNOVATIVE ARBEITSUMGEBUNG

Seit Ausbruch der Pandemie arbeiten Millionen Berufstätige aus dem Homeoffice. Viele Arbeitnehmerinnen und Arbeitnehmer wissen das ortsunabhängige und flexiblere Arbeiten zu schätzen. Sobald die Entwicklungen es zulassen, wünschen sich zahlreiche Arbeitskräfte jedoch eine – zumindest teilweise – Rückkehr ins Büro. Digitale Lösungen können dazu beitragen, die Gesundheit der Menschen zu schützen und Unternehmen zugleich dabei helfen, sich auf die Herausforderungen des New Normal vorzubereiten.

„In der neuen hybriden Normalität ist das Arbeiten von zu Hause ebenso selbstverständlich wie die Präsenz im Büro. Doch bevor diese neuen Arbeitsweisen wirklich normal werden, müssen Unternehmen signalisieren, dass das Wohlergehen ihrer Beschäftigten oberste Priorität hat und sich so ihr Vertrauen sichern. Arbeitnehmerinnen und Arbeiternehmer wünschen sich zwar die Rückkehr ins Büro, haben aber zugleich Sorgen wegen Corona – ob beispielsweise vor Ort noch ein Arbeitsplatz frei ist, bei dem die Abstandsregeln eingehalten werden können oder ob die Auslastungsgrenze schon erreicht ist und welche Maßnahmen noch ergriffen werden, um mich als Person zu schützen.“, erklärt Ingo Wittrock, Director Marketing & New Work Experte bei Ricoh Deutschland.

Die Nutzung optimieren

Eine Eine Desk-Management-App wie Ricoh Spaces kann helfen, diese elementaren Fragen zu beantworten. So zeigt sie unter anderem an, welche Räumlichkeiten im Büro bereits besetzt, reserviert oder noch verfügbar sind. Von Zuhause aus können die Arbeitnehmerinnen und Arbeiternehmer jederzeit den Status prüfen und sich auf Wunsch einen Arbeitsplatz buchen. Zudem erhalten sie eine Benachrichtigung, wenn die maximale Auslastung erreicht ist. So wird von Anfang an verhindert, dass sich zu viele Personen in einem Raum oder im Gebäude aufhalten. Zusätzlich ist es für den Admin möglich, einzelne Arbeitsplätze online zu stellen und auch wieder offline zu nehmen. Besprechungsräume können zudem ganz einfach zugewiesen werden, sodass fest geplante Meetings ohne Raumchaos stattfinden können.



HERAUSFORDERUNGEN BEI DER TELEARBEIT

Studie „Mitarbeiterorientierte Digitalisierung", Ricoh, 2021

42 % der Befragten berichten, dass ihre Unternehmenskultur unter den Coronavirus-Einschränkungen gelitten hat

65 % vermissen bei der Arbeit den persönlichen Kontakt zu Kolleginnen und Kollegen

31 % finden es aufgrund von schlechter Kommunikation und technischen Problemen schwierig, motiviert und engagiert zu arbeiten

„Mit Ricoh Spaces bieten wir eine Desk-Management-App, die auch Auslastungs-Trends abbilden und somit dabei helfen kann, die Nutzung der Büroräumlichkeiten zu optimieren. Weitere digitale Lösungen wie das kontaktfreie IT-Asset-Management über unser Smart-Locker-System sowie unsere Thermalkameras helfen zusätzlich, eine intelligente und sichere Arbeitsumgebung zu schaffen. Sie ist für heutige Unternehmen essentiell und zeichnet sich primär durch flexibel einsetzbare Büroräume und Infrastrukturen aus. Nur so können Arbeitgeber heutzutage schnell genug auf neue behördliche Vorgaben und hybride Arbeitsweisen reagieren, ohne den Geschäftsbetrieb zu stören. Zugleich sorgt sie dafür, dass Mitarbeiterinnen und Mitarbeiter ohne Bedenken an ihren Arbeitsplatz zurückkehren können", sagt Ingo Wittrock.

Die Messung der Körpertemperatur beim Betreten von Gebäuden mit Hilfe von Thermalkamers hat sich im letzten Jahr in vielen Ländern zunehmend durchgesetzt und ist ein wichtiger Baustein für den „Safe Return to Work". Die Thermalkameras ermöglichen die kontaktlose Kontrolle der Körpertemperatur von allen Personen, die das (Büro)Gebäude betreten wollen und reduzieren so die Risiken für Mitarbeiter und Mitarbeiterinnen und externe Besucher und Besucherinnen. Falls eine eintretende Person keine Maske trägt, kann das System auf Wunsch den zuständigen Admin informieren, sodass weitere Maßnahmen zur Wahrung der Sicherheit eingeleitet werden können. Neben der kontaktlosen Temperaturkontrolle sollten Unternehmen berührungsarme oder berührungslose Abläufe fördern. Smart-Locker-Systeme ermöglichen beispielsweise ein kontaktfreies IT-Asset-Management. Die intelligenten Schließfächer können unter anderem genutzt werden, um technisches Equipment, das vorher per App angefordert wurde, abzuholen. Auch Briefe und Pakete können über diese moderne Infrastruktur sicher zugestellt werden.

Das Büro der Zukunft

Innovative Technologien waren die Retter in der Not und haben die schnelle Umstellung auf das Homeoffice für Unternehmen möglich gemacht. Auch bei einer teilweisen Rückkehr ins Büro werden die neu eingeführten Systeme und Lösungen keinesfalls obsolet – sie sorgen weiterhin dafür, dass Kolleginnen und Kollegen in Kontakt bleiben und über räumliche Distanzen hinweg zusammenarbeiten. Dennoch ist die Rückkehr ins Büro für viele essentiell um soziale Kontakte und die Unternehmenskultur lebendig zu halten. Durch die digitale Transformation hat das Homeoffice einen neue Akzeptanz erfahren, doch Teams und Abteilungen in Unternehmen leben vom persönlichen Austausch, spontanen Begegnungen, gemeinsamen Veranstaltungen und dem firmeninternen Netzwerk. Die Geschäftsführung sowie die Personal- und IT-Abteilung haben die große Aufgabe vor sich, unter Zuhilfenahme der digitalen Möglichkeiten eine sichere Rückkehr ins Büro zu gewährleisten. Innovative Technologien können eine sichere Nutzung von Unternehmensräumen für eine kollegiale Zusammenarbeit wieder möglich machen. Im Zusammenspiel mit den im Homeoffice eingeführten Tools und Systemen hat der veränderte Arbeitsalltag großes Potential eine neue Arbeitskultur zu etablieren, das Büro als Inspirationsquelle neu aufleben zu lassen und die Zukunftsfähigkeit der Unternehmen zu sichern.

> MIT RICOH SPACES BIETEN WIR EINE DESK-MANAGEMENT-APP, DIE AUCH AUSLASTUNGSTRENDS ABBILDEN UND SOMIT DABEI HELFEN KANN, DIE NUTZUNG DER BÜRORÄUMLICHKEITEN ZU OPTIMIEREN.
>
> Ingo Wittrock, Director Marketing & New Work Experte, Ricoh Deutschland GmbH, www.ricoh.de

MICROSOFT SCHAFFT OPEN LICENSE AB

DIE ALTERNATIVEN FÜR UNTERNEHMEN IM ÜBERBLICK

Zum 31. Dezember 2021 beendet Microsoft die Vertragsform „Open License". Damit stellt der Software-Hersteller seine Kunden einmal mehr vor Herausforderungen. Eine offizielle Information darüber, was mit bereits eingesetzten Programmen geschieht, und welche Alternativen es für Unternehmen gibt, blieb der Konzern bisher schuldig.

Dieser Beitrag zeigt die Alternativen auf und liefert IT-Managern eine übersichtliche Entscheidungshilfe für das richtige Lizenzmodell nach Open License.

Akuter Handlungsbedarf: Open License mit SA

Ab 1. Januar 2022 sind Buchungen im Open-License-Modell von Microsoft nicht mehr möglich. Wer vor diesem Termin Lizenzen mit Software Assurance (SA) ersteht, kann diese ab dem Buchungstag genau zwei Jahre nutzen. Eine Verlängerung wird nicht möglich sein. Damit werden Funktionen der Software Assurance – beispielsweise die Hochverfügbarkeit von Servern – nach Ablauf der zwei Jahre wertlos.

„Wer bisher auf Open License mit SA gesetzt hat, sollte sich jetzt umorientieren!" Auf diesen Umstand weist das Team vom Microsoft Gold Partner Vendosoft aktuell Kunden und Interessenten hin. Zur Wahl stehen in Zukunft die Lizenzierung über einen Cloud Solution Provider oder die Open-Value-Pakete von Microsoft.

Cloud Solution Provider: Keine SA-Verpflichtung

Manches Unternehmen hat sich in der Vergangenheit für Open License entschieden, weil es so die Software ohne SA nutzen konnte. Wem das weiterhin wichtig ist, der kann seine Programme in Zukunft via CSP erwerben. Beim Cloud Solution Provider sind diese in allen von Microsoft bereitgestellten Modellen verfügbar: gekauft als sogenanntes CSP Perpetual, oder gemietet in Form von CSP Subscription. Letzteres wahlweise für ein Jahr oder drei Jahre.

ANGESICHTS DER ABSCHAFFUNG VON MICROSOFT OPEN LICENSE ZUM JAHRESENDE BLEIBT UNTERNEHMEN KEINE WAHL: SIE MÜSSEN SICH NEU ORIENTIEREN.

Björn Orth, Geschäftsführer beim Microsoft Gold Partner VENDOSOFT, www.vendosoft.de

„Nach dem Wegfall von Open License stellt CSP die einzige Möglichkeit dar, Microsoft-Lizenzen ohne Support zu beziehen", erläutert VENDOSOFT-Geschäftsführer Björn Orth. Mit CSP Perpetual kaufen Firmen ihre Software ohne weitere Verpflichtungen. Wer Support wünscht, dem bietet die Subscription-Lösung ähnliche Leistungen, wie sie aus der Software Assurance bekannt sind.

Open Value: Software Assurance inklusive

Die zweite Alternative zu Open License heißt Open Value. Dieses Modell sieht eine dreijährige Lizenzierung vor, die immer auch Software Assurance enthält. Support und Software-Updates sind somit inkludiert. Open Value bedingt eine Abnahme von mindestens fünf Lizenzen. Während der gesamten Laufzeit können flexibel neue Programme hinzugebucht werden.

Ein Name drei Optionen

Open Value gliedert sich in drei Lizenzmodelle.

Mit Open Value Subscription bietet Microsoft eine Miet-Variante an, bei der Unternehmen ihre Lizenzen jederzeit aufstocken oder reduzieren können. Nach Ablauf der Vertragsdauer geht hier allerdings keinerlei Eigentum auf den Kunden über. Das wäre über einen Buyout möglich, davon jedoch rät VENDOSOFT-Geschäftsführer Orth ab. „Wirtschaftlich unrentabel", kommentiert er.

Mit der Open Value Non-Company-Wide können unterschiedliche Geräte im Unternehmen mit verschiedenen Business-Suites ausgestattet werden. Dieses Lizenzmodell ist eine Kauf-Lizenz.

Die dritte Alternative, Open Value Company-Wide, ist ebenfalls eine Kauf-Lizenz. Ihr Nachteil: Kunden müssen sämtliche Geräte unternehmensweit auf einen Standard für Core Client Access Licenses, Office und/oder Windows lizenzieren. Da fehlt es schnell an Flexibilität und ei-

ner individuellen Gestaltung der Systemlandschaft.

Die beiden zuletzt genannten Open-Value-Szenarien bieten denselben Vorteil wie auch CSP Perpetual: Gekaufte Programme bleiben als Wirtschaftsgut im Unternehmen und können jederzeit an Reseller wie VENDOSOFT verkauft und somit in bares Geld umgewandelt werden. Orth verweist an dieser Stelle auf einen Umstand, den IT-Verantwortliche oft übersehen: Mietangebote erscheinen aufgrund ihrer geringen monatlichen Gebühr finanziell attraktiv. Im Mehr-Jahresvergleich schneidet gekaufte Software jedoch deutlich günstiger ab. Umso mehr, wenn sie gebraucht gekauft wird.

„Kunden, die gebrauchte Lizenzen bei uns erwerben, sparen 80 Prozent gegenüber der entsprechenden Cloud-Lösung!" Diesen Kostenvergleich zieht VENDOSOFT am Beispiel eines Microsoft Exchange Servers 2019 Standard versus Exchange Online Plan 1 über einen Zeitraum von sechs Jahren. Für andere Microsoft-Produkte sieht es ähnlich aus.

Fazit

Angesichts der Abschaffung von Microsoft Open License zum Jahresende bleibt Unternehmen keine Wahl: Sie müssen sich neu orientieren. Schon heute macht der Kauf neuer Open-License-Programme mit Software Assurance keinen Sinn mehr. Mit den aufgezeigten Optionen bietet der Microsoft Gold Partner VENDOSOFT für jede Herangehensweise – kaufen oder mieten, mit oder ohne Software Assurance – eine Lösung. Besonders günstig kommen hier gebraucht gekaufte Lizenzen.

Angelika Mühleck

WERTVOLLE ENTSCHEIDUNGSHILFE

Eine transparente Gegenüberstellung mit allen Vor- und Nachteilen der Open-License-Alternativen steht unter **www.vendosoft.de/microsoft-open-license** zur Verfügung.
Bei Fragen helfen die Microsoft-Experten von VENDOSOFT unverbindlich weiter. Der Reseller führt neben neuen Microsoft-Lizenzen und Mietmodellen auch gebrauchte Software. Damit sind Unternehmen hier objektiv beraten, was bekanntlich zu den besten Ergebnissen führt.

speicherguide.de
Das Storage-Magazin

itmanagement

Storage: Im Zeichen der Digitalen Transformation

Digitalevent

11. Mai 2021

Storage-Experten haben viele Themen auf ihrem Radar. Ob Virtualisierung, software-defined Storage, Hyperkonvergenz, Hyperscaler, Objektspeicher. Es gibt viele Themen zu beackern. Innovation und Digitale Transformation tun ihr übriges.

Behalten Sie den Überblick und besuchen Sie unseren Storage-Event.

Das Event findet live am Dienstag, 11. Mai 2021 statt. Die Teilnahme ist kostenlos.

#storage2021

Highlights aus der Agenda

Objektspeicher & S3

Sicherheit von Cloud/Objektspeicher unter der Lupe
Manfred Rosendahl, Pre-Sales, PoINT Software & Systems GmbH

Object Storage: das neue Schweizer-Messer unter den Storage-Lösungen Praxisberichte und Erfahrungsaustausch
Michael Jordan, Director Channel & Inside Sales Central Europe, Quantum

Backup & Recovery

Datensicherung für die Cloud-Ära
Dietmar Simon, Senior Presales System Engineer, Druva

Silent Bricks - die flexible Antwort auf die stetig wachsenden Anforderungen an ein sicheres Backup
René Weber, Field Application Engineer, FAST LTA GmbH

Software Defined Storage

Die richtigen Daten zur richtigen Zeit am richtigen Ort
Alexander Best, Regional Technologist Central Europe & EMEA Alliances, DataCore Software GmbH

Storage & IT-Sicherheit

5 Gründe für weiter steigende Kosten durch Ransomware-Angriffe
Reiner Bielmeier, Geschäftsführer, FAST LTA GmbH

Jetzt anmelden

SCAN ME

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

HYBRIDES REQUIREMENTS ENGINEERING

Herausforderungen agiler Projekte in klassischen Organisationsstrukturen

Hybride Prozessmodelle bieten Unternehmen eine Möglichkeit, agile Projektmanagement-Ansätze in sonst eher klassischen Kontexten zu pilotieren. Oft entscheiden organisatorische Prozesse über den Erfolg oder Misserfolg eines solchen Projekts. Dieser Artikel gibt praktische Tipps für den Umgang mit den Herausforderungen der veränderten Arbeitsumgebung eines Requirements Engineers in einem hybriden Projektmodell.

Konsistenz über Tool-Brüche hinweg

Die Spezifikation eines agilen Projekts in einer klassischen Organisationsstruktur wird an zwei Stellen benötigt: Während der Projektlaufzeit arbeiten das Entwicklungsteam und weitere Projektbeteiligte mit einem sogenannten User Story Mapping Tool. Nach Projektabschluss nutzt

TIPPS ZUM HANDLING DES USER STORY MAPPING TOOLS.

Oft dauert es seine Zeit, um mit einer neuen Software warm zu werden. Die nachfolgenden Tipps können die Arbeit mit einem User Story Mapping Tool erleichtern.

1. **Epics aus Benutzersicht schreiben:** Eine einfache, nicht technische Sprache sorgt dafür, dass selbst an den Sprint Review-Meetings teilnehmende Kunden die Aufgabe verstehen.

2. **Epics clever strukturieren:** Um die Übersicht zu wahren, sollte ein Projekt nicht mehr als 7-10 Epics umfassen. Eines dieser Epics sollte dabei für Analyseaufgaben genutzt werden, um bspw. während des Sprints Workshops durchzuführen, sich mit anderen Abteilungen abzustimmen oder generell Lösungen zu besprechen. Diese Tätigkeiten kosten Zeit, die wie jeder andere Aufwand eingeplant werden muss. Darüber hinaus lohnt es sich, Muster-Stories und -Aufgaben anzulegen und diese immer wieder zu verwenden: Ein einheitlicher Aufbau der Stories und Aufgaben kann das Lesen erleichtern.

3. **Im letzten Sprint keine Kernfunktionalitäten mehr umsetzen:** Der letzte Sprint sollte dazu dienen, das Projekt sauber abzuschließen. Die Zeit kann z. B. dafür genutzt werden, noch offene Punkte aus dem vorangegangenen Sprint zu erledigen, den Code und die Spezifikation „aufzuräumen", oder auch, um kleinere aber prestigeträchtige Anforderungen mit sogenannten „Begeisterungsfaktoren" umzusetzen.

die zugehörige Linieneinheit das im Unternehmen standardmäßig eingesetzte Spezifikationstool. In solchen Fällen ist es besonders wichtig, beide Spezifikationen zueinander konsistent zu halten. Nur auf diese Weise lässt sich sicherstellen, dass das restliche nicht agil arbeitende Personal keine zusätzliche Einarbeitung braucht, um an alle für seine Arbeit erforderlichen Informationen zu gelangen.

Bei Medien- und/oder Tool-Brüchen, die bei derartigen Konstellationen nahezu immer auftreten, sollten die Artefakte untereinander durchgängig referenziert werden. Dadurch werden eine konsistente Zuordnung und Auffindbarkeit sichergestellt. Zum Beispiel kann im User Story Mapping Tool ein Link zum betreffenden Dokument oder auch Modell der Standard-Spezifikation ergänzt und im Gegenzug auch im betreffenden Dokument oder Modell die Nummer der zugehörigen User Story angegeben werden. So ist die Zuordnung zwischen den beiden Spezifikationen immer eindeutig.

UM ZUM ERFOLG EINES HYBRIDEN PROJEKTMODELLS BEIZUTRAGEN, SOLLTE DER REQUIREMENTS ENGINEER ÜBER EIN TIEFERGREIFENDES TECHNISCHES VERSTÄNDNIS VERFÜGEN UND AUCH DIE ZUVOR BESCHRIEBENEN REGELN FÜR DIE AGILE SPEZIFIKATION BEFOLGEN.

Alexa Ziesch, Senior Consultant, DYNACON GmbH, www.dynacon.de

Kommt für das agile Projekt ein User Story Mapping Tool zum Einsatz, empfiehlt sich außerdem das Benutzen von Tags zur Organisation der Stories. So können Tags der Status-Indizierung der User Stories dienen, zum Beispiel „Sprint OK" wenn die User Story für einen Sprint ausreichend definiert ist und eingeplant werden kann, oder „Spec OK" wenn die Spezifikation aus dem agilen Projekt im Standard-Spezifikationstool des Unternehmens nachgezogen wurde. Zur qualitativen und quantitativen Übersicht kann in den meisten Tools ein Report zu allen

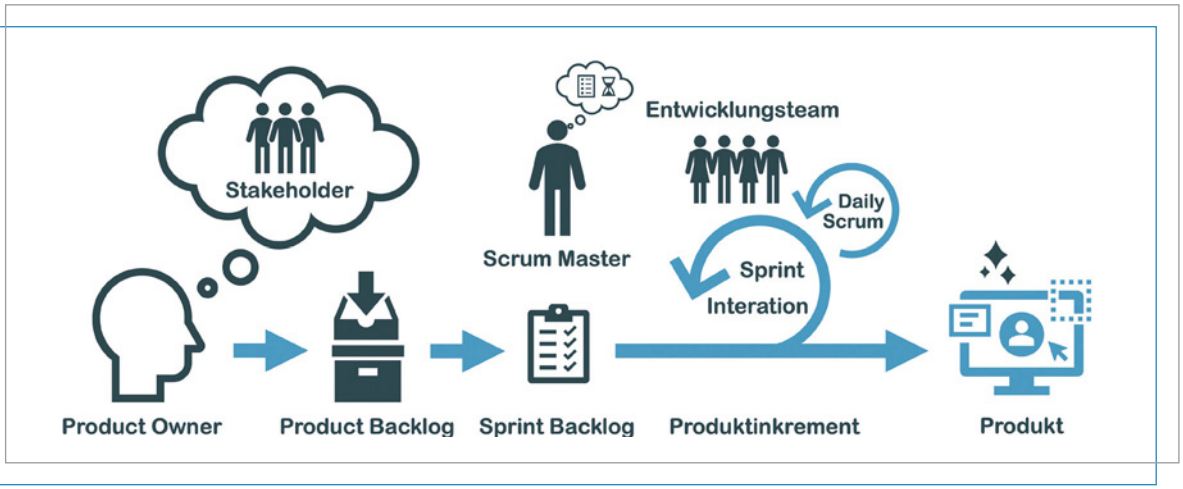


Bild 1: Vereinfachte Darstellung des Scrum-Flows

User Stories inklusive der beschriebenen Tags erzeugt werden.

User Stories vorbereiten

Um Sprints planen zu können, müssen die User Stories im Product Backlog vorbereitet werden (siehe auch Bild 1). Diese Tätigkeit übernehmen Requirements Engineers entweder in der Rolle des Product Owners (PO) oder bei größeren Projekten direkt als Teil des Scrum Teams. Das bedeutet nicht nur, dass die Anforderungen in Form von User Stories zu formulieren sind (Sprachmustervorlagen vereinfachen diese Aufgabe), sondern diese müssen auch priorisiert werden. Mit der Priorisierung wird auch die Reihenfolge für die nachher anstehende Entwicklung festgelegt. Aus diesem Grund ist es sinnvoll, Abhängigkeiten der Anforderungen untereinander, die Einfluss auf die Reihenfolge der Umsetzung der Anforderungen haben, direkt mit dem Scrum Team zu besprechen. So profitiert der Requirements Engineer von den Skills und Erfahrungen des Scrum Teams, das durch die Team-weite Einigung auf eine bestimmte Reihenfolge dem Product Owner einen Teil seiner Verantwortung abnimmt.

Doch mit welchen User Stories sollte begonnen werden? Priorisiert werden sollten vor allem diejenigen Anforderungen, die gleich zu Beginn den größten Wert für den späteren Benutzer schaffen, aber auch solche, die die Basis für Folgeaktivitäten oder auch Aktivitäten außerhalb des agilen Projekts darstellen. Sobald eine Abteilung außerhalb des agilen Teams betroffen ist, empfiehlt es sich, zuerst die entsprechenden User Stories der übergreifenden Schnittstellen zu beschreiben. Durch die priorisierte Formulierung dieser Funktionen wissen die Betroffenen, welche Anforderungen sie in ihrer Domäne umsetzen müssen und können rechtzeitig einschätzen, welche Aufwände auf sie zukommen und wann diese einzuplanen sind.

In der agilen Welt gibt es einfache Schätzmethoden, die den Product Owner bei seinen Planungsaufgaben unterstützen. Beispielsweise kann einer Anforderung ein bestimmter Wert zugeordnet werden (zum Beispiel in Form von Story Points). Alle anderen Funktionen, die danach entwickelt werden, werden dann an dieser Beispiel-Zuordnung gemessen. Je wertvoller eine Funktion für den Auftraggeber ist, desto mehr Story Points bekommt die zugehörige Anforderung. Nutzen kann der PO diese Zuordnung, indem er eben jene User Stories priorisiert, die durch verhältnismäßig wenig Aufwand einen hohen Nutzen (= viele Story Points) bringen. User Stories mit einem geringeren Wert und dafür erhöhtem Aufwand können zu einem späteren Zeitpunkt umgesetzt werden.

Klare Vorgaben für Spezifikation und Nachdokumentation

Die Unternehmensleitung sollte daher noch vor dem Start von agilen Projekten hinsichtlich des Spezifikationswerkzeugs eine klare Linie verfolgen. Die Empfehlung: Die Erhaltung des Standard-Tools bis eine anderweitige Entscheidung getroffen wird (etwa die komplette Ablösung durch ein User Story Mapping Tool, wenn zukünftig ausschließlich agil entwickelt werden soll).

Pilotprojekte auch nachträglich im Standard-Tool zu dokumentieren, sollte nicht als doppelte Arbeit, sondern eher als eine vorausschauende Investition betrachtet werden. Hierdurch muss nicht das gesamte Personal des Unternehmens Schulungen durchlaufen, um auch noch im Nachhinein die Spezifikation lesen zu können. Außerdem sollte es unbedingt vermieden werden, nach Projektende zwei verschiedene Spezifikationsquellen zu haben. Sonst steht zu befürchten, dass die ehemaligen Projektbeteiligten immer wieder erklären müssen, wo welche Spezifikation anfängt und aufhört bzw. wie die Spezifikationen miteinander in Verbindung stehen. Oder es besteht das Risiko, Widersprüche zwischen den Spezifikationen festzustellen, weil die Spezifikation über Tool- und Medienbrüche hinweg nur schwer konsistent gehalten werden kann.

Übrigens: Erfolgt die Nachdokumentation im Standardtool erst nach Ende des agilen Projekts, hat das mehrere Vorteile. Durch die priorisierte Spezifikation im User Story Mapping Tool kann sichergestellt werden, dass das Scrum Team jederzeit arbeiten kann und nicht stillsteht (was zusätzliche Kosten verursachen würde).

Außerdem können alle Änderungen, die sich noch während des Projekts ergeben haben, direkt in die Spezifikation im Standardtool einfließen. Dadurch werden nachfolgende Korrekturläufe überflüssig. Es kann jedoch auch sein, dass dem Requirements Engineer nach dem Projekt keine Zeit mehr für diese Tätigkeit eingeräumt wird. In solchen Fällen empfiehlt es sich, die Spezifikationen im User Story Mapping Tool und im Standard-Spezifikationstool direkt parallel zu erstellen.

Wie sich die Arbeit eines Requirements Engineers in agilen Projekten ändert

Wird ein Produkt nach einem klassischen Vorgehensmodell entwickelt, ist es für den Requirements Engineer, der die zugehörige Spezifikation erstellt, in der Regel irrelevant, welcher Teil des Produkts zuerst entwickelt wird. Hierin unterscheidet sich die agile Vorgehensweise deutlich. Anstatt umfangreiche Konzepte, Lasten- oder Pflichtenhefte in großen Textdokumenten festzuhalten, muss ein agiles Projekt in viele kleine Häppchen aufgeteilt und mit einer User Story Mapping-Software verwaltet werden. Die Anforderungen werden vom Requirements Engineer (oftmals in der Rolle des Product Owners) in Form von User Stories im Product Backlog hinterlegt und priorisiert. Eine solche Priorisierung setzt voraus, dass sich der PO mit der späteren technischen Umsetzung seiner Anforderungen auseinandersetzt. Anderenfalls könnte er die Spezifikation nicht in sinnvolle Blöcke aufteilen und auch nicht beurteilen, welcher dieser Blöcke zuerst umgesetzt werden muss. Eine tiefere technische Einarbeitung als bei klassischen Entwicklungsprojekten ist sowohl bei einer hybriden als auch einer agilen Vorgehensweise für den Requirements Engineer unumgänglich.

Agile Vorgehensweisen sind vor allem bekannt durch ihre zahlreichen Review-Meetings und Retrospektiven

Aber auch in der Kommunikation mit den Projektbeteiligten gibt es wesentliche Änderungen. Agile Vorgehensweisen sind vor allem bekannt durch ihre zahlreichen Review-Meetings und Retrospektiven (siehe Bild 2) – diese gibt es in klassischen Projekten meist nicht. Diese Meetings machen die Scrum-Methode besonders effektiv und helfen dabei, dass sich das Team schnell weiterentwickelt und in zukünftigen Sprints zügiger vorankommt. Indem die eigenen Prozesse reflektiert und kontinuierlich verbessert werden, können genauere Schätzungen abgegeben werden und das Team spielt sich besser aufeinander ein. Das agile Entwicklungsteam sorgt in den Sprint Reviews dafür, den Kunden von Anfang an in die Entwicklung einzubinden und ihm die Gelegenheit zu geben, Feedback zu (Zwischen-) Ergebnissen zurückzumelden noch bevor das nächste Feature gebaut wird. Die typische Aufgabe eines Requirements Engineers, unter den Stakeholdern einen Konsens zu schaffen, wird an dieser Stelle auf alle Schultern, die an den Sprint Reviews teilnehmen, verteilt. Außerdem ermöglichen die Reviews dem Projektteam die unmittelbare Reaktion auf sich ändernde Anforderungen des Kunden. Dessen Rückmeldungen können durch den PO nach den Meetings einfach in Form von User Stories erfasst und in einen der nächsten Sprints eingeplant werden, sobald das nötige Refinement durchlaufen wurde.

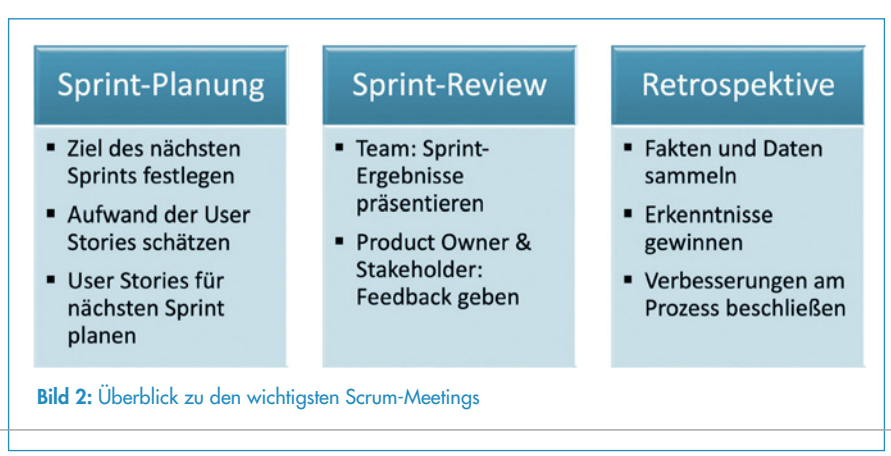


Bild 2: Überblick zu den wichtigsten Scrum-Meetings

Der Aufwand lohnt sich

Es lässt sich schlussfolgern, dass agile Projekte in klassischen Organisationsstrukturen mit Hilfe einer gut durchdachten Strategie erfolgreich durchgeführt werden können.

In Pilotprojekten mag dies zunächst einen erhöhten Zeitaufwand nach sich ziehen. Dieser erhöhte Aufwand ist jedoch nicht der agilen Vorgehensweise an sich, sondern vielmehr dem für diese Vorgehensweise notwendigen Change Management (also der Einführung der neuen Arbeitsweise) zuzuschreiben.

Hybrides Requirements Engineering kombiniert klassisches Anforderungsmanagement (dazu gehören die Erhebung, Analyse und die Priorisierung von Anforderungen) mit den Tätigkeiten eines Product Owners in iterativen Verfahren wie der Scrum-Methode. Um zum Erfolg eines solchen hybriden Projektmodells beizutragen, sollte der Requirements Engineer über ein tiefergreifendes technisches Verständnis verfügen und auch die zuvor beschriebenen Regeln für die agile Spezifikation befolgen. So wird am Ende eines Projekts ein Produkt entwickelt, das für Nutzer und/oder Kunden einen relevanten Mehrwert schafft und gleichzeitig durch konsistente Spezifikation eine lückenlose Dokumentation des Produkts sicherstellt.

Alexa Ziesch

INTELLIGENTE AUTOMATISIERUNG

MIT INTEGRIERTEN PLATTFORMEN DIE DIGITALISIERUNG VORANTREIBEN

Der RPA Markt wächst stetig und das Potenzial ist noch nicht ausgeschöpft. Wie sieht die Zukunft der Technologien aus? Der neueste Gartner Report für Robotic Process Automation (RPA) beziehungsweise Intelligent Automation trifft die folgende Aussage über einen der Schlüsseltrends im RPA Markt: Fast kein RPA-Anbieter verkauft nur RPA. Die meisten RPA-Softwareunternehmen haben Capabilities in verwandten Softwaretools erworben oder aufgebaut, insbesondere Process Mining und Discovery, OCR mit maschinellem Lernen und BPMS Rule Engines. Gartner erwartet, dass sich diese Investitionen in verwandte Software-Tools fortsetzen werden.

Setzt man dies in Beziehung mit einer weiteren Aussage des Artikels „Neben RPA gibt es intelligente Geschäftsprozessmanagement-Suiten, Integrationsplattformen-as-a-Service (iPaaS) und Entscheidungsmanagement-Systeme." wird klar, dass Robotic Process Automation sich auf lange Sicht nicht weiter nur im Umfeld der GUI-Automatisierung bewegen wird, sondern der Trend klar hin zu integrierten Plattformen geht, welche die Capabilities bereitstellen müssen, um eine End-to-End Automatisierung von Prozessen zu ermöglichen, ohne eine Vielzahl von verschiedenen Tools in einem Unternehmen einzusetzen.

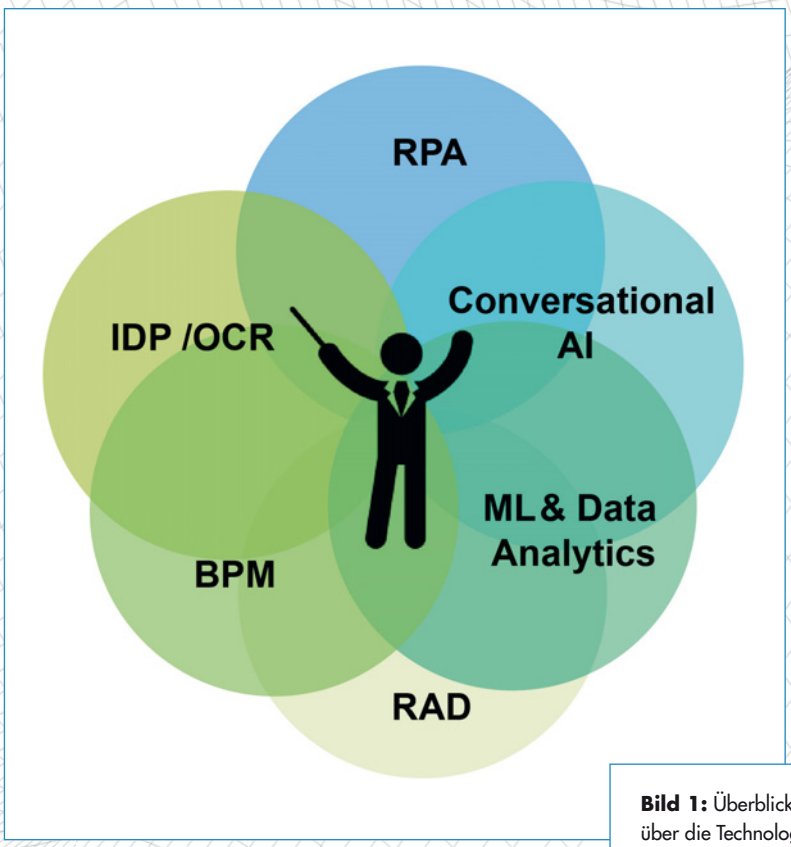


Bild 1: Überblick über die Technologien

Um einen Eindruck zu gewinnen, wie weit diese Integration bereits fortgeschritten ist, werden kurz die einzelnen Komponenten, die der Marktführer UiPath in seiner Plattform neben RPA bereitstellt, vorgestellt.

Process Mining

Ermöglicht das Suchen von für die Automatisierung geeigneten Prozessen durch eine KI-gestützte ETL-Engine, welche aus unterschiedlichen Datenquellen befüllt werden kann.

Task Mining

Wird auf dem Client eines Mitarbeiters ausgeführt und zeichnet die Tätigkeiten des Benutzers auf. Mit Hilfe eine Machine Learning (ML) Algorithmus wird versucht aus den Aufzeichnungen repetitive Abläufe zu extrahieren welche sich für die Automatisierung eignen.

Document Understanding

Intelligentes Optical Character Recognition (OCR) Tool, welches durch ML-gestützte Erweiterungen das Auslesen von zum Beispiel Rechnungen ermöglicht.

AI Center

Bietet die Möglichkeit ML-Algorithmen direkt in der Entwicklungsumgebung bereitzustellen und so auch von Citizen Developern einen einfachen Zugang zu dieser Technologie zu geben.

Apps

Low-Code Plattform für die Erstellung von Formularen oder kompletten, webbasierten Applikationen für die Interaktion des Mitarbeiters mit RPA – Rapid App Development (RAD).

Action Center

Business Process Management (BPM) Komponente, welche eine Schnittstelle zwischen Mitarbeiter und Robot während des Ablaufs eines Prozesses bildet.

Chatbots

Direkt in die Plattform integrierte Möglichkeit zur Verbindung von Google Dialogflow und RPA – Conversational AI.

Der Trend zu integrierten Plattformen bietet enorme Chancen, stellt Unternehmen allerdings auch vor die Herausforderung der Bewertung der optimalen Verknüpfung der verschiedenen Technologien (Integriert vs. Best of Breed) sowie die Notwendigkeit einer ganzheitlichen Betrachtung, um den optimalen Mix aus Integration und Capabilities zu finden, welcher zu dem Unternehmen und dessen Digitalisierungsstrategie passt.

Beispielprozess für End-to-End Digitalisierung

Im Folgenden soll anhand eines konkreten Beispiels des Einsatzes von verschiedenen Technologien für die Automatisierung eines Geschäftsprozesses beispielhaft die Möglichkeiten der Verknüpfung, sowie die Vor- und Nachteile der integrierten Plattformen diskutiert werden. Hierfür wird ein End-to-End Prozess betrachtet, welcher verschiedene Inputkanäle verwendet, um den Rechnungseingang ganzheitlich abzubilden.

INTEGRIERTE PLATTFORMEN ERMÖGLICHEN ES UNTERNEHMEN, DAS GESAMTE SPEKTRUM DER AUTOMATISIERUNGSTECHNOLOGIEN NAHTLOS ZU NUTZEN.

Nicolas Hess,
Co-Founder und CEO Europa, Roboyo,
www.roboyo.de

Mit funktionsübergreifenden Lösungen wie Chatbots können sowohl einzelne Geschäftsprozesse als auch eine Klassifizierung dieser Prozesse durchgeführt werden. Ein Chatbot interagiert mit einem Benutzer und identifiziert so den zu erstellenden Geschäftsprozess. Als Beispiel erkennt der Chatbot den Bedarf, eine „Rechnungsbearbeitung" durchzuführen und nimmt die notwendigen Unterlagen entgegen. Hierdurch ergeben sich zwei Konstellationen: Der Chatbot initiiert den Geschäftsprozess in einem dedizierten Intelligent Business Process Management System (iBPMS), das die End-to-End-Kontrolle über den Prozess hat und mehrere Technologien und Anbieter bündelt (Bild 2), oder die Aufga-

ben werden in einer integrierten Plattform abgebildet und mithilfe der eingebauten Capabilities des Anbieters automatisiert (Bild 3).

Sobald der Auftrag gestartet wird, wird für den Geschäftsvorfall jede maschinelle und menschliche Arbeitszeit protokolliert und somit für fachlichen Auswertungen bereitgestellt. Innerhalb des Prozesses werden Informationen aus Dateien (Rechnungen) extrahiert. Nachfolgend wird einen ML-Klassifizierungsservice verwendet, um Auffälligkeiten in den ausgelesenen Informationen zu erkennen und somit zusätzliche Prüfungen durch Mitarbeiter zu ermöglichen. Weiterhin kann eine fachliche Abnahme durch einen Mitarbeiter, bei der auch evtl. Kommunikationen mit dem Kunden oder Vorgesetzten stattfinden können, erfolgen.

Sind alle Freigaben korrekt erfolgt, werden alle Informationen an einen RPA-Prozess weitergegeben und von diesem in externen oder internen Systemen aktualisiert und Ergebnisse über die korrekte Ausführung zurückgeliefert. Prozessinformationen werden zu Auswertungszwecken in den Datenbanken des iBPMS beziehungsweise der IAP nativ bereitgestellt.

Integrierter Plattformen oder Best of Breed?

Die Digitalisierung des vorgestellten Prozesses kann über beide Varianten erreicht werden. Es bestehen jedoch Unterschiede bei dem Implementierungsaufwand, der langfristigen Ausrichtung der Software und Eintrittshürden der vorgestellten Technologien.

MIT DER SINNVOLLEN VERBINDUNG AUTOMATISIERTER TECHNOLOGIEN IST ES UNTERNEHMEN MÖGLICH, PROZESSE END-TO-END AUTOMATISIERT ABZUBILDEN.

Frank Schikora,
Global Head of Delivery, Roboyo,
www.roboyo.de

Verfügt ein Unternehmen bereits über intelligente Automatisierungssysteme von unterschiedlichen spezialisierten Anbietern, sollte genau geprüft werden, ob es möglich ist diese flexibel zum Beispiel über ein iBPMS zu verbinden und somit keine weiteren Investitionen in Richtung einer integrierten Automatisierungsplattform tätigen zu müssen. Sollte dies nicht möglich sein, etwa durch einen nicht ausreichenden Funktionsumfang oder zu hohe Lizenzkosten, können die integrierten Plattformen eine echte Alternative bereitstellen, da diese einen ähnlichen Funktionsumfang bei teils geringeren Kosten abdecken können. Zudem ist die Komplexität der Einführung eines Service-Layers auf Grundlage eines iBPMs Systems im Vergleich zu einer integrierten Plattform wesentlich höher anzusehen.

Aufgrund des breiten Spektrums an Technologien, die innerhalb einer IAP-Lösung angeboten werden, ist eine schnellere Automatisierung des Prozesses möglich, da die gewährleistete Interoperabilität und das zentralisierte Wissen über die Plattformarchitektur einen geringeren Implementierungsaufwand und somit einen schnelleren Time-To-Market ermöglichen. Der Bedarf nach spezialisiertem Wissen in den integrierten Technologien abseits von RPA ist jedoch nicht zu unterschätzen.

Insgesamt muss genau betrachtet werden, welche Capabilities eine integrierte Plattform bereitstellen kann und ob diese ausreichend für die Digitalisierungsstrategie sind. Ist dies nicht der Fall sollte ein „Best of Breed" Ansatz in Betracht gezogen werden.

Fazit

Aus dem vorgestellten Beispiel geht hervor, dass integrierte Plattformen für Unternehmen eine fast nie dagewesen Möglichkeit darstellen, vorhandene Ressourcen zu nutzen, um neue Technologien und Capa-

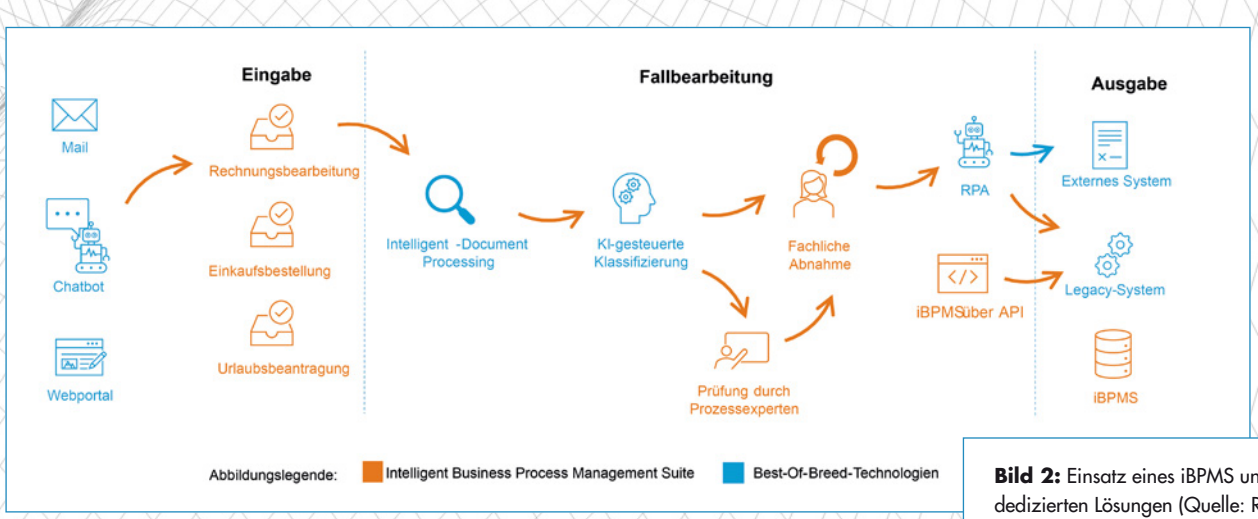


Bild 2: Einsatz eines iBPMS und dedizierten Lösungen (Quelle: Roboyo)

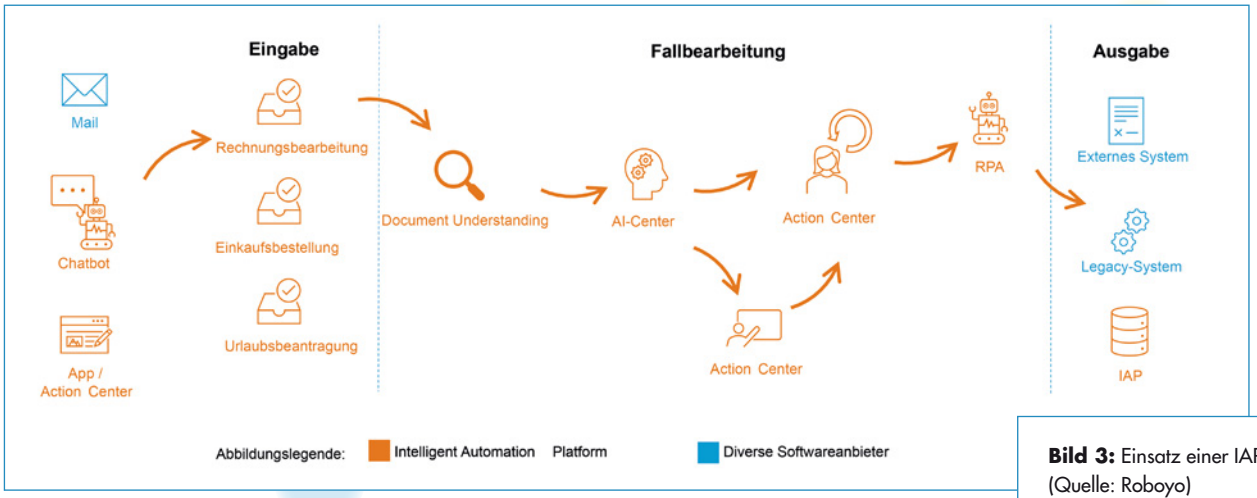


Bild 3: Einsatz einer IAP (Quelle: Roboyo)

bilities zu erschließen und zu integrieren, ohne die bereits erstellte Systemlandschaft komplett verändern zu müssen.

Es wird klar, dass Technologien wie RPA, BPM, IDP und AI nicht ohne Grund von den Herstellern in die Plattformen integriert werden. Mit der sinnvollen Verbindung dieser Technologien wird es Unternehmen ermöglicht, immer mehr in die Richtung einer komplette End-to-End Automatisierung von Prozessen vorzudringen. Kombiniert man dies mit dem Ansatz des Process Mining, welches darauf abzielt, möglichst übergreifende Prozesse zu identifizieren, bietet sich Unternehmen in den nächsten Jahren eine große Chance, mit der Digitalisierung zu wachsen und nicht von dieser überrollt zu werden.

Gerade was die intelligente Automatisierung angeht, wird es immer einfacher ML- und/oder AI-Komponenten in bestehende Workflows zu integrieren oder neue Prozesse durch die Integration zu erschließen. Es ist jedoch unbedingt erforderlich im Unternehmen Ressourcen zu haben, welche die Algorithmen und Modelle verstehen und steuern können – ansonsten kann es sehr einfach dazu kommen, dass Entscheidungen durch eine Blackbox Implementierung der Algorithmen nicht mehr nachvollzogen werden können. Hier ist es aus unserer Sicht nicht möglich, ohne speziell ausgebildetes Personal erfolgreich zu sein.

Die Prominenz von Low-Code und No-Code Bestandteilen in den Plattformen hilft Unternehmen in der Digitalisierung Erfolg nicht nur über Kostenreduzierungen abzubilden, sondern die Belegschaft im Sinne eines zukunftsorientierten Ansatzes mit in die Digitalisierungsstrategie zu integrieren und so auch die Agilität des Unternehmens zu steigern. Das Training beziehungsweise die Fortbildungen, vor allem im Bereich RPA, richten sich verstärkt auf Mitarbeiter aus Fachabteilungen, die nur wenige oder keine Vorkenntnisse in der Programmierung haben. Diese neue Art von Entwicklern wird Citizen Developer genannt. Ziel ist es, dass einzelne ausgebildete Mitarbeiter aus Fachabteilungen kleine Automatisierungen selbst erstellen können, welche dann gegebenenfalls als kleiner Bestandteil in einen übergreifenden End-to-End Prozess integriert werden.

Ein Nachteil der integrierten Plattformen ist aus unserer Sicht, dass die bereitgestellten Capabilities, durch die breite Fächerung nicht an den Funktionsumfang und die Robustheit von dedizierten Lösungen in einem Best-Of-Breed Ansatz heranreichen. Die Abwägung, welche hier getroffen werden muss, ist, ob der Funktionsumfang (auf der Roadmap der Plattform) ausreichend ist um die Digitalisierungsstrategie und die zu automatisierenden Prozesse ausreichend zu unterstützen. Ist dies nicht der Fall, muss gegebenenfalls ein dedizierter Hersteller in das Konzept integriert werden und zum Beispiel durch eine iBPMS Plattform die Vermittlungsschicht erstellt werden.

Zusammenfassend bieten die integrierten Plattformen zur intelligenten Automatisierung Unternehmen die Chance, die Digitalisierung voranzutreiben, ohne eine Vielzahl von verschiedenen eventuell neuen Systemen einführen zu müssen und ermöglichen es die eigene Belegschaft direkt in die Digitalisierungsstrategie einzubetten, um das gesamte Unternehmen besser auf die bevorstehende Digitalisierung vorzubereiten.

Nicolas Hess, Frank Schikora, Ligia Pastrán
www.roboyo.de

DIE PROMINENZ VON LOW-CODE UND NO-CODE BESTANDTEILEN IN DEN PLATTFORMEN HILFT UNTERNEHMEN DIE AGILITÄT ZU STEIGERN.

Ligia Pastrán, Automation Lead, Roboyo, www.roboyo.de

SCHWARMINTELLIGENZ FÜR IOT-TESTING

WEITER, IMMER WEITER, ...

Die Evolution macht keinen Halt, auch nicht in der IT-Welt. Eines der Phänomene, das zunehmend in den Fokus rückt, ist das der Schwarmintelligenz. Ob Gesetze und Umsetzungen der Physik, der Aerodynamik oder der Arzneimittelkunde. Überall wird verstärkt die Natur observiert und wo möglich deren Millionen Jahre alten Erfahrung adaptiert.

Nichts anderes ist die Schwarmintelligenz, auch unter dem Begriff Kollektive Intelligenz oder Gruppenintelligenz bekannt. Sie ist das Phänomen, bei dem Gruppen von Individuen durch Zusammenarbeit intelligente Entscheidungen treffen können. Eine Variante ist durch die Crowd-Bewegung entstanden. Ob Crowdtesting oder Crowdfunding. Immer geht es darum, durch Lastverteilung, die Dynamik, sprich time-to market, zu beschleunigen und/oder Risiken zu minimieren.

Eine weitere Ausprägung findet sich nun in einer IoT-Testplattform für Unternehmen. Der Name könnte kaum passender gewählt sein: Swarm. Das Besondere daran: Manpower wird durch Simulationen ersetzt, also quasi der Sprung von der physikalischen in die virtuelle Welt.

Aufbau der Plattform

Basis des Ganzen ist HiveMQ, eine MQTT-Plattform für die Vernetzung von Maschinen, Geräten und Applikationen im IoT-Bereich. Auf Basis des IoT-Standard-Kommunikationsprotokolls MQTT, ermöglicht der HiveMQ Broker eine absolut sichere und jederzeit hochverfügbare Datenübertragung zwischen vernetzten Geräten und der Cloud. Einzigartig sind dabei sowohl die Hochverfügbarkeitsgarantie, als auch die hohe Skalierbarkeit in Millionenhöhe.

Das Swarm-Modul ist nun eine Lösung mit der Unternehmen aller Größenordnungen umfangreiche IoT-Netzwerke zuverlässig simulieren und testen können. HiveMQ Swarm ermöglicht es so, nicht nur die Skalierbarkeit und Performance von IoT-Implementierungen ganz einfach zu testen, sondern zudem die Qualität und Zuverlässigkeit ihrer Systeme deutlich erhöhen. Damit können Großkonzerne und Unternehmen zudem erstmals Prognosen zu Kapazitäten, Infrastruktur und Finanzkosten erstellen, bevor sie ihr IoT-System in Betrieb nehmen.

Warum ist das wichtig? Weil sowohl die Größe als auch die Anwendungsbereiche von IoT-Lösungen rasant wachsen. Anwender wollen die Validierung ihrer Systeme prüfen, bevor sie live beziehungsweise in Produktion gehen. Swarm erfüllt diese Anforderungen perfekt.

IoT-Lösungen werden von immer mehr Unternehmen verschiedener Branchen wie der Fertigung, der Logistik, dem Gesundheitswesen oder der Automobilbranche eingesetzt. Laut einer aktuellen Studie von Business Insider führt dies dazu, dass der IoT-Markt bis 2027 jährlich um über 2,4 Milliarden US-Dollar wachsen wird. IoT-Systeme zu testen, bevor sie produktiv gehen, ist jedoch extrem schwierig. Das Verhalten und Zusammenspiel der verschiedenen IoT-Geräte in einer Produktionsumgebung nachzubilden, funktioniert oft nur unzuverlässig, insbesondere da einzelne IoT-Geräte mitunter verschiedene komplexe Verhaltensmuster aufweisen können.

Last- und Stresstests unvermeidbar

Zum Beispiel verhalten sich autonome Fahrzeuge im Ruhezustand ganz anders, als wenn sie auf einer Autobahn oder auch nur in der Fabrikhalle auf ein unerwartetes Ereignis treffen. Trotz dieser Herausforderungen sind Last- und Stresstests unvermeidbar, da die Behebung von IoT-Produktionsfehlern im laufenden Betrieb extrem kostspielig ist. Ganz zu schweigen davon, dass solche Fehler

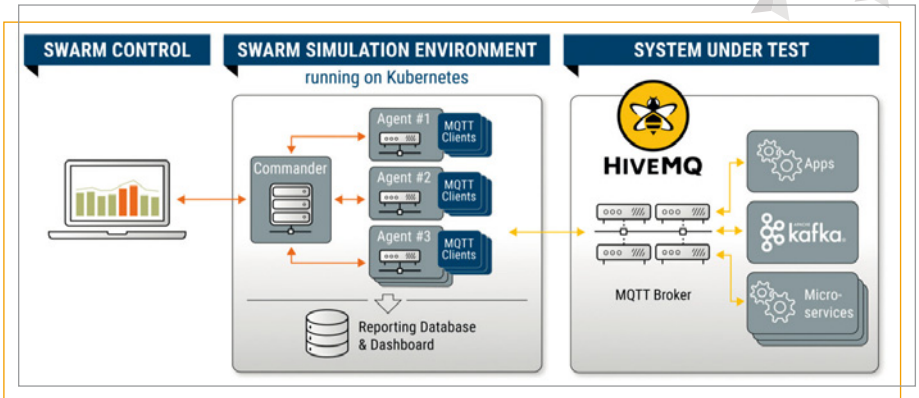


Bild 1: Architektur der IoT-Testplattform.

> MIT HIVEMQ SWARM LASSEN SICH DIE FÜR GROSSE IOT-UMGEBUNGEN UNVERMEIDLICHEN LAST- UND STRESSTESTS NUN IN EINER PLATTFORM SIMULIEREN."
>
> Dominik Obermaier, CTO und Gründer, HiveMQ, https://www.hivemq.com/hivemq-swarm

potenziell katastrophale Folgen für das System selbst haben können. Sprich, die Bestimmung der Belastbarkeit eines Systems ist eine unternehmenskritische Aufgabe.

System-Resilienz wird oft auf Grund von Hochrechnungen und Schätzungen errechnet, basierend auf veralteten Tools und Protokollen, die nicht zweckdienlich sind", so James Governor, Analyst und Mitbegründer von RedMonk, einem führenden US-amerikanischen Analystenhaus mit Schwerpunkt auf Softwareentwicklung. HiveMQ Swarm hingegen ist speziell auf umfangreiche moderne IoT-Anwendungsfälle und Protokolle ausgelegt.

Neue Testszenarien

Swarm wurde entwickelt, um die Herausforderungen beim Testen heutiger groß angelegter IoT-Implementierungen zu meistern. Als verteilte Plattform ist sie in der Lage, Hunderte von Millionen einzelner Netzwerkverbindungen zu erstellen. Diese simulieren Geräte, Nachrichten und MQTT-Topics (eine Form der Adressierung, mit der MQTT-Clients Informationen austauschen) und entwickeln wiederverwendbare Szenarien, die das Verhalten von Geräten nachbilden.

Die Software bietet einen benutzerdefinierten Datengenerator, mit dem sich komplexe Anwendungsfälle für Tests erstellen lassen. Darüber hinaus ist die Software so konzipiert, dass sie sich nahtlos in die Cloud-Infrastruktur von Unternehmen integrieren lässt, einschließlich öffentlicher Clouds (etwa AWS, Azure, GCP) und Kubernetes-basierter Systeme.

Das Swarm-Modul ist infrastrukturmäßig betrachtet eine ergänzende Erweiterung für HiveMQ MQTT – eine MQTT-Broker-Messaging-Plattform für schnelle, effiziente und zuverlässige Daten-Übertragung zwischen miteinander verbundenen IoT-Geräten. Sie nutzt das MQTT-Protokoll für eine sofortige, bidirektionale Datenübertragung (per Push) zwischen Geräten und Unternehmenssystemen.

Dominik Obermaier

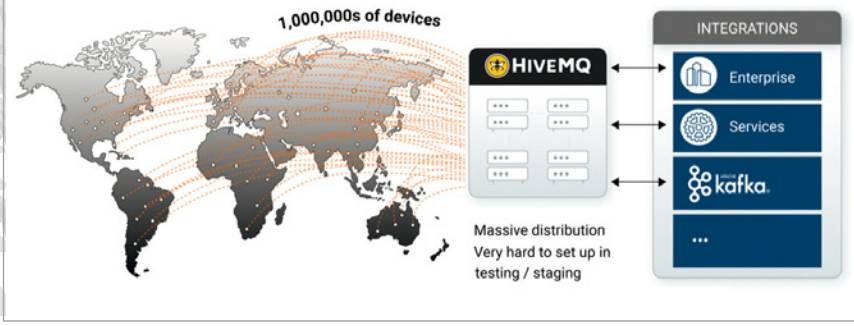


Bild 2: Weltweit können Millionen unterschiedlicher Devices einem Last- und Stresstest unterzogen werden.

BLACK HAT SEO EINFACH ERKLÄRT

MANIPULATIVE METHODEN DER SUCHMASCHINENOPTIMIERUNG

Die Bezeichnung Suchmaschinenoptimierung (SEO oder search engine optimization) beschreibt Marketing-Maßnahmen, mit deren Hilfe die Sichtbarkeit einer ganzen Internet-Domäne oder einzelner Webseiten in den Suchmaschinen nachhaltig gesteigert werden kann. Das langfristige Ziel von SEO: eine höhere Platzierung im organischen Ranking von Suchmaschinen wie Google, Bing oder Yahoo. Dieses Ziel ist aus unternehmerischer Sicht derart erstrebenswert, dass manche Webseitenbetreiber oder deren SEOs (Suchmaschinenoptimierer) auf sogenannte Black-Hat-SEO-Praktiken zurückgreifen, um dasselbe zu erreichen.

In diesem Artikel werden die Definition Black Hat SEO, die Richtlinien der Suchmaschinen, die Vor- und Nachteile von Black Hat SEO, 7 Black-Hat-SEO-Methoden sowie 4 relevante SEO-Tipps zur Vermeidung dieser Praktiken beleuchtet.

Was ist Black Hat SEO?

Der Begriff Black Hat SEO (Blackhat-SEO, Schwarzer-Hut-SEO) umfasst SEO-Methoden, die gegen die Richtlinien von Suchmaschinen verstoßen. Grundsätzlich lassen sich die sogenannten „Schwarzer-Hut-Methoden" in zwei Kategorien einordnen:

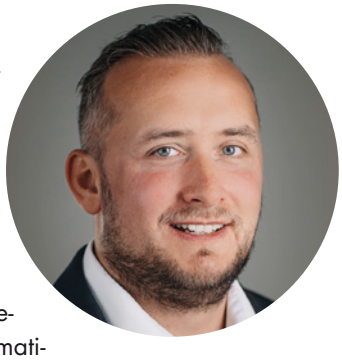
- **Kategorie 1:** Durch die Maßnahmen stärkt ein Unternehmen oder eine Person die eigene Domain oder Website.
- **Kategorie 2:** Durch Black Hat SEO wird eine fremde Website oder Domain mutwillig geschädigt – Thema unlauterer Wettbewerb.

Somit handelt es sich bei einigen Black-Hat-SEO-Maßnahmen nicht nur um einen Verstoß von bestehenden Suchmaschinen-Richtlinien, sondern auch um eine Straftat, die ein juristisches Nachspiel zur Folge haben kann.

Ursprung der Bezeichnung Black Hat

Der Begriff Black Hat wird der Hacker-Szene zugeordnet, da er dort sehr häufig verwendet wird. Ursprünglich stammt er allerdings aus dem Bereich der Cowboy- und Westernfilme: Die Bösewichte in alten amerikanischen Westernfilmen tragen einen schwarzen Hut, während der Gute, der Held der Geschichte, mit einem weißen Hut ausgestattet ist.

Demzufolge sind SEOs und Webseitenbetreiber, die mit diesen fragwürdigen Taktiken arbeiten, die Bösewichte, die nicht mit dem Gesetz konform gehen.



WHITE HAT SEO ZAHLT SICH AUS. FLANKIERT VON WEITEREN ONLINEMARKETING-STRATEGIEN BRINGT ES DAUERHAFT BESUCHER AUF DIE WEBSEITE, AUCH WENN ES ETWAS LÄNGER DAUERT.

Sebastian Prohaska, Gründer und Inhaber, ithelps, ithelps-digital.com

Suchmaschinen-Richtlinien

Internet-User suchen mithilfe ihrer bevorzugten Suchmaschine nach Informationen und Antworten zu den unterschiedlichsten Themen und Fragestellungen. Die Suchmaschinen sorgen ihrerseits dafür, dass ihre Nutzer relevante und korrekte Suchergebnisse zu ihren Suchanfragen finden und angezeigt bekommen.

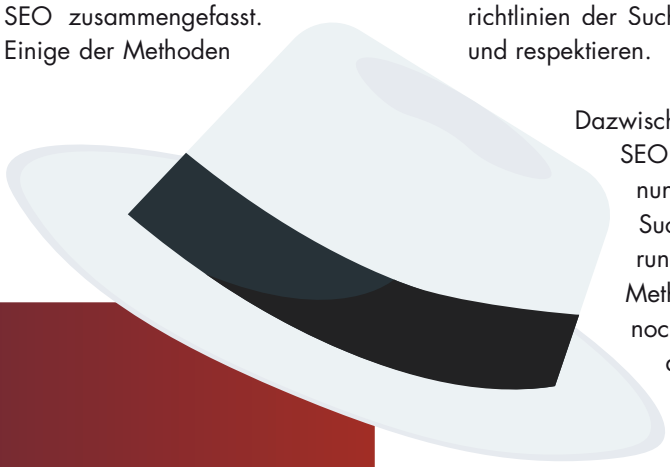
Zu diesem Zweck – und um marginale oder illegale Anzeigen in ihren Ergebnisseiten (SERPs) zu verhindern – haben Suchmaschinen wie Google, Bing oder Yahoo Richtlinien erstellt.

Google beispielsweise hält in seinen Qualitätsrichtlinien für Webmaster die gewünschten Handlungs- und Verhaltensweisen fest, an welche sich Webseitenbetreiber und SEO-Verantwortlichen zu halten haben.

SEO-Definitionen

Optimierungsmethoden, die gegen die Richtlinien von Suchmaschinen verstoßen, werden unter dem Begriff Black Hat SEO zusammengefasst.
Einige der Methoden täuschen die Domain-Besucher, andere widersprechen dem Bundesgesetz gegen den unlauteren Wettbewerb (UWG).

White Hat SEO ist das Gegenstück zu Black Hat SEO. Die Bezeichnung steht für alle legitimen Praktiken der Suchmaschinenoptimierung, welche die Qualitätsrichtlinien der Suchmaschinen einhalten und respektieren.



Dazwischen hat sich Grey Hat SEO oder die Bezeichnung „grenzwertige Suchmaschinenoptimierung“ positioniert, deren Methoden zum gerade noch legitim, aber hart an der Grenze zum Regel- oder Gesetzesverstoß angesiedelt sind.

Vorteile von Black Hat SEO

Um mit einer neuen Unternehmenswebseite Spitzen-Positionen in den gängigen Suchmaschinen zu erreichen, benötigt es einige Zeit, da neben der Reputation auch das Vertrauen der Nutzer/Besucher gewonnen werden muss. Diese beiden Faktoren einer Webseite werden neben zahlreichen anderen von Google bewertet. Durch die Nutzung von Black-Hat-SEO-Methoden können neue Webseiten in vergleichsweise kurzer Zeit Top-Platzierungen in den Google-Rankings oder eine hohe Linkpopularität erreichen, indem Reputation du Domain Trust (beispielsweise durch den Kauf fragwürdiger Backlinks) vorgetäuscht werden. Dadurch locken die Betreiber der Websites kurzfristig mehr Besucher auf ihre Seiten, wo-

durch sie einen Gewinn erwirtschaften können.

Black Hat SEO wird also eingesetzt, um wissentlich oder unwissentlich die Ranking-Ergebnisse einer Webseite im Suchindex durch unlautere Vorgehensweise und Manipulation zu verbessern.

Nachteile von Black Hat SEO

Während einige Webseitenbetreiber aus fehlendem Wissen die offiziellen Qualitätsrichtlinien der Suchmaschinen nicht einhalten, ignorieren andere die Regeln bewusst: Sie nehmen die möglichen Abstrafungen vonseiten der Suchmaschinen oder die Streichung aus dem Suchmaschinen-Index in Kauf. Denn sie wissen, dass ihre angewandten Methoden mitunter nicht sofort erkannt werden.

Mittlerweile erkennen und reagieren die verschiedenen Suchmaschinen jedoch immer schneller auf betrügerisches und manipulatives Black Hat SEO. Infolgedessen kann eine Seite oder Domain mit einem Rankingverlust oder einer kompletten Verbannung aus dem Suchmaschinen-Index abgestraft werden.

Eine Marke (Brand) oder eine Webseite, welche einmal aus der Indexierung ausgeschlossen oder im Suchmaschinen-Ranking herabgestuft wurde, hat es später sehr schwer, ihr Ranking und Image wieder herzustellen. Der finanzielle Schaden und der Imageverlust sind bei einer Abstrafung oder Verbannung häufig größer als der anfängliche Nutzen.

Sieben Black-Hat-SEO-Methoden

Einige der im Folgenden aufgelisteten Techniken sind schon sehr alt und daher auch den Suchmaschinen bekannt. Das bedeutet, sie funktionieren mittlerweile nicht mehr. Wiederum andere funktionieren noch teilweise oder zur Gänze. Man muss sich jedoch bewusst sein, dass jedes neue Google-Update die Gefahr mit sich bringt, dass manipulative Maßnahmen besser und schneller erkannt und abgemahnt werden.

VIER RELEVANTE SEO-TIPPS

Um die bereits erwähnten Probleme – De-Indexierung oder Positionsverlust – zu vermeiden, gibt Google Webseitenbetreibern folgende vier Tipps. Für Unternehmen oder Webseitenbetreiber lohnt sich die Einhaltung dieser Tipps – denn dadurch werden De-Indexierung und Positionsverluste bereits im Vorfeld vermieden.

1. Erstellen Sie den Inhalt vorrangig für Ihre User – nicht für Google oder eine andere Suchmaschine.
2. Täuschen und betrügen Sie die Besucher Ihrer Website nicht.
3. Verzichten Sie auf manipulative Methoden, um Ihr Ranking in den Suchmaschinen zu beeinflussen. Fragen Sie sich stattdessen, ob Ihre potenziellen Kunden von Ihrem Handeln einen Vorteil haben.
4. Gestalten Sie Ihre Website attraktiv und einzigartig.

Diese kontroversen Maßnahmen zählen zu Black Hat SEO:

– **Cloaking:** Website-Besucher sehen einen anderen Inhalt als Suchmaschinen.

– **Keyword-Stuffing:** Eine der ältesten Black-Hat-Maßnahmen ist die Überoptimierung mit Keywords. Websites, die auf diese Weise ihre Keyword-Dichte manipulieren, werden von Google abgemahnt.

– **Hidden Content:** Dabei handelt es sich um für die Leser unsichtbare Textpassagen, die jedoch von den Suchmaschinen ausgelesen werden können. In Verbindung mit dem zuvor erwähnten Keyword-Stuffing wird den Suchmaschinen eine tatsächlich nicht vorhandene Relevanz vorgetäuscht.

– **Doorway Pages:** Brückenseiten fungieren als Zwischenseiten, welche der Seitenbesucher gar nicht zu Gesicht bekommt, da er zu einer anderen Seite weitergeleitet wird. Diese Seiten beinhalten wichtige Keywords und stärken die eigene Linkpopularität.

– **Text-Spinning:** Bestehende Artikel werden mithilfe von Softwareanwendungen in neue und einzigartige Texte von minderer Qualität umgewandelt. Das geschieht durch die häufige Verwendung von Synonymen, die verschiedene Wörter, Phrasen und Abschnitte eines Textes ersetzen.

– **Kauf von Links/Teilnahme an Linktauschprogrammen:** Linkbuildung (Links von Dritten) ist eine wichtige Maßnahme der OffPage-Optimierung. Legitim erworbene beziehungswise erhaltene Backlinks sind ein legitimer Teil des organischen Linkbuildings und stärken die Seitenautorität (Domain Authority). SEO-Verantwortliche, die die Linkpopularität durch ihre Teilnahme an einem Linktausch-Programm stärken oder Links bei fragwürdigen und unseriösen Webseiten kaufen, handeln den Google-Richtlinien zuwider.

– **Duplicate Content:** Inhalte werden von fremden Webseiten 1 zu 1 oder nur unwesentlich verändert übernommen. Dies ist aufgrund des Copyrights und Urheberrechts untersagt und widerspricht den Richtlinien der Suchmaschinen.

Während einige Tricks lediglich eine Verletzung der Suchmaschinen-Richtlinie anvisieren, handelt es sich in anderen Fällen um eine Straftat.

Sebastian Prohaska

CORE WEB VITALS

GOOGLES PAGE EXPERIENCE UPDATE

Googles Page Experience-Update rückt immer näher. War bisher immer die Rede von Mai, gab Google vor Kurzem bekannt, dass das Roll-out der Algorithmus-Änderung nicht vor Mitte Juni beginnen wird und sich bis August hinzieht. Höchste Zeit also, sich mit dem Thema näher zu beschäftigen und zu überprüfen, ob bei der eigenen Website Handlungsbedarf besteht.

Was steckt hinter dem Page Experience-Update?

Das kommende Update ordnet die Zusammensetzung der Rankingfaktoren neu. Google verfolgt damit mehrere Ziele:

- Verbesserung der Nutzerfreundlichkeit
- Vereinfachung der Bedienbarkeit
- Erhöhung der Sicherheit

WER SICH VON SEINEN WETTBEWERBERN ABHEBEN MÖCHTE, SOLLTE SICH ZUSÄTZLICH ZU INFORMATIVEN UND QUALITATIV HOCHWERTIGEN INHALTEN MIT DEN TECHNISCHEN ASPEKTEN SEINER WEBSITE AUSEINANDERSETZEN.

Ann-Kathrin Grottke, Marketing, eology GmbH, www.eology. de

Ein Begriff fällt am häufigsten im Zusammenhang mit der Algorithmus-Änderung: Performance. Dieser Faktor einer Website ist bisher nur schwer zu messen. Das Update und vor allem die enthaltenen Core Web Vitals schaffen hierfür Abhilfe. Eine Folge kann die komplette Neuordnung der Suchergebnisse sein, dies wird sich nach und nach zeigen.

Was beinhaltet der Rankingfaktor Page Experience?

Nach aktuellem Stand ist die Performance einer Website mit den vorhandenen Metriken nicht eindeutig messbar. Google ändert dies mit dem Page Experience-Update.

Diese vier bereits vorhandenen Rankingsignale sind Teil dieses Faktors:

- Mobile Friendly: Website ist für Mobilgeräte optimiert

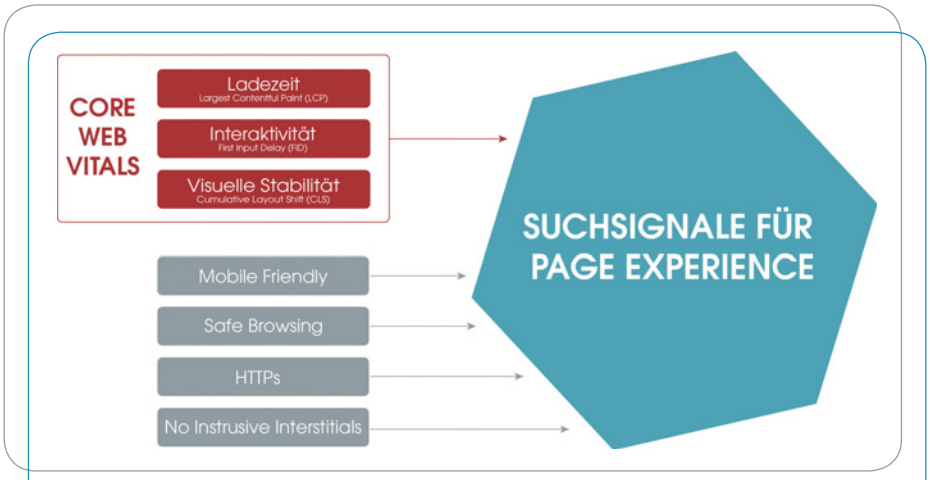


Bild 1: Zusammensetzung des Rankingfaktors Page Experience

- HTTPs: Daten werden verschlüsselt über HTTPs übermittelt
- Safe Browsing: Google stuft die Website als sicher ein
- No Intrusive Interstitials: Auf der Website gibt es keine unterbrechenden oder aufdringlichen Werbebanner, Pop-ups, oder ähnliches.

Diese Messwerte wurden ursprünglich noch um den PageSpeed ergänzt. Um diesen greifbar zu machen, kommen mit dem Update an dieser Stelle die Core Web Vitals in Spiel. Diese sind einfacher nachzuvollziehen und die Bestandteile sind besser zu dokumentieren. Somit ist die Leistung einer Website mit den festgelegten Zahlen quantifizierbar.

Die Gewichtung der einzelnen Bestandteile ist noch nicht klar. Als sicher gilt allerdings, dass die Kombination aus den „alten" Metriken und den Core Web Vitals einen neuen Rankingfaktor ergeben wird: die Page Experience.

Was sind die Core Web Vitals?

Sinn und Zweck der Core Web Vitals ist es, die Erfahrung von Nutzern mit einer Website zu bestimmen. Folglich lassen sich Seiten besser vergleichen und Optimierungspotenziale einfacher identifizieren. Klar im Fokus steht hier die Verbesserung der Usability von Websites. Da die Core Web Vitals Bestandteil des Rankingfaktors Page Experience sind, ergeben sich bei entsprechender Optimierung bessere Chancen auf organische Rankings in den Suchergebnissen.

Die Core Web Vitals bestehen aus drei Teilen:

1. Largest Contentful Paint (LCP)
2. First Input Delay (FID)
3. Cumulative Layout Shift (CLS)

Für die Dreiteilung gibt es zwei Gründe. Zum einen erkennen Webmaster durch die Trennung der Werte einfacher, welcher Teil einer Website Aufmerksamkeit benötigt und optimiert werden sollte. Zum anderen ermöglicht sie ein schrittweises Vorgehen, so dass es sich leichter bestimmen lässt, wann und wie schnell eine Seite vollständig geladen ist beziehungsweise wie diese performt.

CORE WEB VITALS

Wie findet man heraus, ob für die eigene Seite Handlungsbedarf besteht? Welche Optimierungsansätze gibt es, um die Werte in den grünen Bereich zu bekommen? Und wie behält man die Metriken langfristig im Blick? Mehr dazu im 5-teiligen Core Web Vitals Crashkurs der Online Marketing Agentur eology. Kostenlose Anmeldung unter: ***eology.de/anmeldung***

Largest Contentful Paint – Ladezeit

Diese Metrik beschäftigt sich mit der Frage: Wann ist der Hauptinhalt der Website geladen? Der Wert spiegelt wider, wie hoch die Renderzeit des größten Bild- oder Textblocks der Website ist. Für die beste User Experience ist ein LCP-Score unter 2,5 Sekunden perfekt. Innerhalb dieser Zeit können Nutzer den Hauptinhalt der Seite sehen. Googles Empfehlung lautet: mindestens 75 Prozent der LCP-Werte sollen im grünen Bereich sein, damit die Website insgesamt einen guten LCP-Wert erreicht.

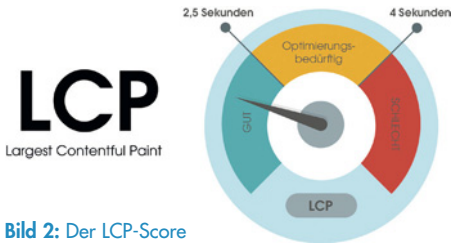


Bild 2: Der LCP-Score

First Input Delay – Interaktivität

FID bedeutet übersetzt „erste Eingangsverzögerung". Es misst die Zeit, die es braucht, bis ein Nutzer mit der Website interagieren kann beziehungsweise bis die Seite auf eine Nutzereingabe reagiert. Die Metrik vermittelt einen Eindruck über die Reaktionsfähigkeit und Interaktivität einer Seite. Ein FID-Score unter 100 Millisekunden fällt dabei in den erstrebenswerten Bereich. Übersetzt heißt das: Sowohl mobil als auch am Desktop benötigt die Website nicht mehr als 0,1 Sekunden, um bereit für die Ein-

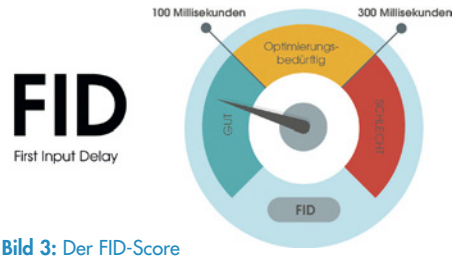


Bild 3: Der FID-Score

gabe eines Users zu sein und darauf zu reagieren. Alles, was über diesem Wert liegt, sollte optimiert werden.

Cumulative Layout Shift – Stabilität

Mit der Metrik CLS lässt sich feststellen, ob eine Seite von unerwarteten Verschiebungen betroffen ist. Sie misst die visuelle Stabilität einer Seite. Dazu zählen Verschiebungen von:

- Buttons
- Bildern
- Videos
- Textblöcken, und so weiter.

Nichts ärgert einen User mehr, als wenn beim Laden beispielsweise ein Button auf der Seite um ein paar Zentimeter nach unten rutscht. Im schlimmsten Fall klickt er stattdessen etwas Anderes an, was sich negativ auf die Usability und das Nutzererlebnis auswirkt. Der CLS-Score wird in Prozent angegeben und berechnet sich folgendermaßen: Der betroffene Anteil der Website (affected area) wird multipliziert mit der prozentualen Verschiebung (percentage of shift). Eine prozentuale Verschiebung unter 10 Prozent gilt als gut. Dringender Optimierungsbedarf besteht bei Werten über 25 Prozent.

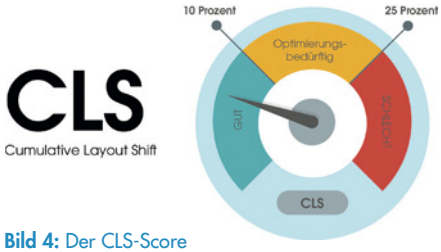


Bild 4: Der CLS-Score

Welche Tools eignen sich zur Analyse?

Um die Core Web Vitals zu messen, benutzt Google Feld-Daten, also Daten von reellen Usern, sowie Labor-Daten, die unter perfekten und gleichbleibenden Umständen erhoben wurden. Beide zeigen, wie User die eine Website wahrnehmen und erleben könnten. Obwohl das Update noch nicht ausgerollt ist, sind die meisten Google-Tools schon auf die neuen Metriken vorbereitet. Auch in den Tools erfolgt eine Unterteilung in Labor- und Feld-Daten. Die Grafik in Bild 5 zeigt, welche Zahlen in welchem Tool einsehbar sind.

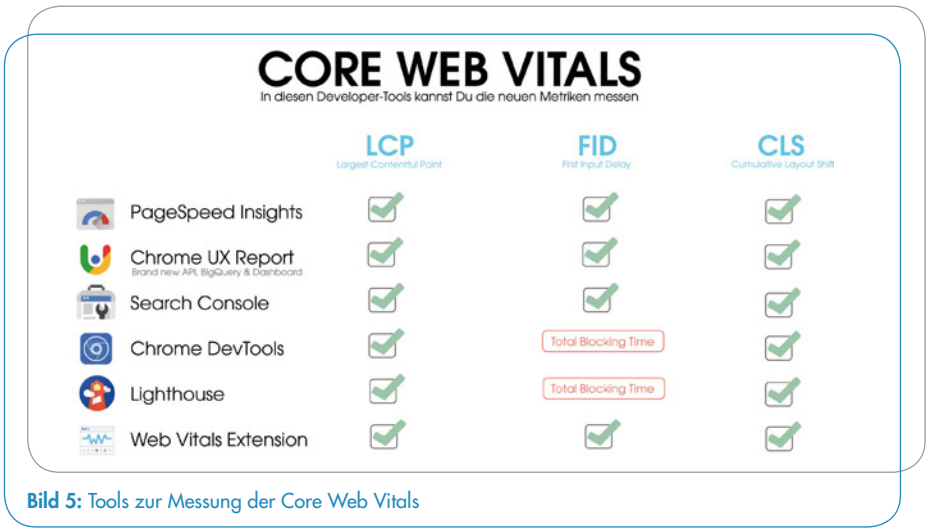


Bild 5: Tools zur Messung der Core Web Vitals

Warum ist eine SEO-Optimierung für das Update wichtig?

Die mobilen Zugriffe auf Websites steigen seit Jahren immer weiter an. Vor allem auf mobilen Endgeräten sind langsame Seiten sowie Inhalte, die sich verschieben oder nicht reagieren, ein No-Go. Es ist also nicht verwunderlich, dass Google die bereits vorhandenen Werte wie mobile Nutzerfreundlichkeit, sicheres Surfen, HTTPs und Regularien zur Vermeidung von „nervigen" Interstitials jetzt noch um die Core Web Vitals erweitert. Wer sich also von seinen Wettbewerbern abheben möchte, sollte sich zusätzlich zu informativen und qualitativ hochwertigen Inhalten mit den technischen Aspekten seiner Website auseinandersetzen. Außerdem ist eine Optimierung für die Page Experience in erster Linie vor allem eines: eine Optimierung für mehr Nutzerfreundlichkeit!

Ann-Kathrin Grottke

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
30. JUNI 2021

SAP PARTNER-LÖSUNGEN

Der Weg zur Digitalisierung

NEW WORK

Chancen und Herausforderungen

CONTROLLING & FINANCE

Auf der sicheren Seite

DIE AUSGABE 6/2021 VON IT MANAGEMENT ERSCHEINT AM 31. MAI 2021.

INSERENTENVERZEICHNIS

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Carina Mitzschke, Silvia Parthier (-26)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Christian Geißler, Ann-Kathrin Grottke, Peter Herr, Nicolas Hess, Ralf Lautenbacher, Carina Mitzschke, Angelika Mühleck, Dominik Obermaier, Silvia Parthier, Ulrich Parthier, Ligia Pasträn, Sebastian Prohaska, Frank Schikora, Jens Schulte, Florian Sippel, Klaus Stöckert, Dr. Benjamin Strehl, Bud Walker, Ingo Wittrock, Alexa Ziesch

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

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

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

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

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

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

Erscheinungsweise:
10x pro Jahr

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

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

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

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

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

Wir machen es Ihnen leicht, es Hackern schwer zu machen.

pwc

Trust in Transformation: Vertrauen Sie auf einen Partner, der mit Ihnen flexible Strategien für sich schnell wandelnde Bedrohungen entwickelt, und Abwehrmechanismen implementiert, mit denen Sie Angreifer in die Verzweiflung treiben: www.pwc.de/cybersecurity

itsecurity
MAI 2021

DAS SPEZIAL

Informations-Sicherheitsmanagement
ab Seite 14

ivanti
Datensicherheit in der Post-Corona-Welt
ab Seite 10

CYBER SECURITY

IT-SICHERHEIT IST EIN GESCHÄFTSPROZESS

Timo Schlüter, Arvato Systems

AUTOMATION CORE FRAMEWORK
THOUGHT LEADERSHIP

GUTES BCM

Vom Säbelzahntiger zum Hackerangriff

CYBERSICHERHEIT

Hybride Systemumgebung als Unternehmensrisiko

DDoS-ANGRIFFE

Präventive Maßnahmen und konsequentes Handeln

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

16

20

INHALT

4 COVERSTORY

CYBER SECURITY ALS BUSINESS PROCESS

IT SICHERHEIT IST KEINE SOFTWARE, SONDERN EIN GESCHÄFTSPROZESS

Das Risiko, einem Cyber-Angriff zum Opfer zu fallen, nimmt kontinuierlich zu. Welche Gefahren hier lauern und wie Unternehmen damit umgehen sollten, hat Timo Schlüter, Business Consultant Cyber Security bei Arvato Systems, im Gespräch mit it security-Herausgeber Ulrich Parthier erläutert.

Ulrich Parthier: *Wenn wir über die IT und deren Weiterentwicklung sprechen, geht es immer um den Dreiklang von Menschen, Prozessen und Tools. Gilt das auch für unternehmenskritische Bereiche wie IT-Security?*

CYBER SECURITY IST NICHTS, DAS UNTERNEHMEN OUT-OF-THE-BOX BEZIEHEN KÖNNEN UND AUCH KEINE STANDARD-LÖSUNG. IN UNSERER DEFINITION IST CYBER SECURITY EIN BUSINESS-PROZESS, DER IN DER GESAMTEN ORGANISATION VERANKERT SEIN MUSS. DENN DIE BEDROHUNGSLAGE VERÄNDERT SICH PERMANENT.

Timo Schlüter, Business Consultant Cyber Security, Arvato Systems, www.arvato-systems.de

Timo Schlüter: Auf jeden Fall. Tools sind wichtig, keine Frage. Dennoch ist es keine Lösung, Software um ihrer selbst willen anzuschaffen. Es braucht Tools, die zum individuellen Bedarf von Unternehmen passen. Darum sollten Firmen zunächst analysieren, welche Security-Lösungen und Sensoren bereits vorhanden sind. Und was zusätzlich erforderlich ist, um Schwachstellen zu erkennen und zu beheben. So ist der Mensch selbst ein großes Einfallstor für Hacker, man denke nur an Social Engineering. Aber auch bei der Abwehr von Angriffen kommt es auf den Menschen an. Natürlich ließen sich Detection und Response vollautomatisieren. Doch: Sobald Hacker erkennen, dass eine Handlung X automatisch eine Reaktion Y auslöst, können sie das ganz gezielt ausnutzen. Darum sollte der Mensch entscheiden, was in Sachen Remediation zu tun ist, wenn ein Tool einen drohenden oder tatsächlichen Angriff erkennt. Womit wir bei den Prozessen wären. Viele Unternehmen verstehen Cyber Security nach wie vor als Software, die man einmalig anschafft. Doch damit ist es bei weitem nicht getan. IT-Sicherheit ist vielmehr Ergebnis eines fortlaufenden Prozesses. Diese Erkenntnis und die damit einhergehende Awareness für das Thema Cyber Security kommen nun auch im Management an.

Ulrich Parthier: *Welchen Stellenwert hat IT-Sicherheit in Unternehmen? Welche Erfahrungen haben Sie diesbezüglich in Projekten gemacht?*

Timo Schlüter: Die Gespräche, die wir mit Unternehmen führen, ähneln sich meistens sehr. Der Tenor lautet: Wir sind unzufrieden mit unserer IT Security. Das Problem dabei ist, dass viele keine greifbare Vorstellung davon haben, was Cyber Security überhaupt ist und welchen Mehrwert sie stiftet. Auf den ersten Blick scheint IT-Sicherheit viel Geld zu kosten, ohne messbare Resultate zu liefern. Das ist jedoch zu kurz gedacht. Erst wenn Unternehmen IT-Sicherheit als Geschäftsprozess wie jeden anderen verstehen, der mit Bedacht modelliert, mit Metriken gesteuert, mit Tools überwacht und kontinuierlich optimiert sein will, erlangen sie eine Ahnung vom Wert der Cyber Security – und in welchem Maß sie zur Sicherheit des gesamten Unternehmens beiträgt.

Ulrich Parthier: *Wie sollte Ihrer Meinung nach die Frage lauten, die sich Unternehmen im Kontext von Cyber Security stellen sollten?*

Timo Schlüter: Die entscheidende Frage ist: Wie organisiere ich meine Security-Prozesse, damit meine Mitarbeiter genau jene Probleme angehen, die aktuell wichtig sind? Die Betonung liegt dabei auf „Prozesse". Was in anderen Bereichen selbstverständlich ist, muss auch bei der IT-Sicherheit gelten. Abläufe müssen nicht nur strategisch definiert sein. Es braucht ebenso messbare KPIs, anhand derer sich der Prozess im Hinblick auf das angestrebte Ziel bewerten lässt. Ohne Kennzahlen kann es natürlich keine validen Ergebnisse geben. Für viele Unternehmen ist der Weg hin zu dieser Erkenntnis sehr steinig und mitunter auch schmerzhaft. Denn sie müssen einsehen, dass sie das Thema bis dato falsch angegangen sind – und so letztlich Geld verschwendet haben. Ein Beispiel aus der Praxis: Es kommt immer wieder vor,

dass Unternehmen ihre eigene IT-Systemlandschaft überhaupt nicht kennen. Sie wissen nicht, welche Lösungen und Systeme in welchen Abteilungen zum Einsatz kommen – Stichwort: Schatten-IT. Diese Unternehmen müssen zunächst ihre Hausaufgaben machen, also sich einen Überblick über ihre IT-Landschaft verschaffen, bevor wir dann gemeinsam Prozesse modellieren, damit sie zukünftig Schwachstellen und etwaige Angriffe erkennen können.

Ulrich Parthier: *Sie sprechen von der Messung des Security Levels?*

Timo Schlüter: Jein. Hierbei geht es nicht um Risk Reports, sondern darum, Prozesse operativ zu steuern. Ein Beispiel aus dem Schwachstellenmanagement: Der Security Scan einer Umgebung liefert detaillierte Ergebnisse über die zum Vermessungszeitpunkt existierenden Risiken, etwa als Risk Score Metrik. Der gemessene Wert könnte bei 20.000 liegen, zwei Wochen später dann bei 25.000. Was sagen diese Zahlen aus? Dass sich das Gesamtrisiko erhöht hat. Doch hat die zuständige IT-Abteilung in der Zwischenzeit an der Problembehebung gearbeitet? Und wie gut funktioniert das Schwachstellenmanagement? Beide Fragen lassen sich mit Einzelbetrachtungen dieser Art nicht beantworten, weil IT-Sicherheit kein statisches Thema ist. Ein Security Score ist also keine Lösung, sondern lediglich Ausgangspunkt für weitere Maßnahmen. Der Score zeigt nur die Qualität der Prevention an, nicht aber von Maßnahmen in den Bereichen Detection und Response. Daher ist es so wichtig, Cyber Security als Geschäftsprozess zu betrachten. Wenn Unternehmen alle Schwachstellen in einem Einmalprojekt schließen, kann die Bedrohungslage einige Wochen später eine ganz andere sein. Eben weil sie sich permanent ändert. Darum ist ein kontinuierliches Security Monitoring unverzichtbar.

Ulrich Parthier: *Wie gelingt es, diese Prozesse zu definieren?*

Timo Schlüter: Unternehmen müssen zuallererst herausfinden, wo sie am verwundbarsten sind. Dabei sind das MITRE ATT&CK Framework und eine Heatmap, welche die Bedrohungslage in der eigenen Branche darstellt und die permanent aktualisiert wird, wirkungsvolle Hilfsmittel. Das individuelle Risiko zu evaluieren – und zwar kontinuierlich –, ist ein sinnvoller Startpunkt für die Prozessdefinition.

Ulrich Parthier: *Wie geht es dann weiter?*

Timo Schlüter: Dann geht es ans Eingemachte. Dann kommt der Faktor Mensch ins Spiel. Um es mit gewieften Hackern aufnehmen zu können, braucht es hochqualifizierte Experten, idealerweise mit einem Abschluss als Cyber Security Master. Es ist doch so: Die Mehrzahl der Hacker ist auf eine Technik spezialisiert, wohingegen die Mitarbeiter nicht nur alle Techniken kennen und beherrschen, sondern auch ausgeprägte analytische Fähigkeiten haben müssen. Solch ein Team zusammenzustellen und zu unterhalten, können sich nur die ganz großen Konzerne leisten. Mittelständische Unternehmen sind gut beraten, auf die Unterstützung eines externen SOC zurückzugreifen. Die Mitarbeiter in einem SOC überwachen alle eingehenden Notables – wahlweise auch 24/7 – und bewerten, ob es sich tatsächlich um einen kritischen Incident handelt. Sollte das der Fall sein, leiten sie die nötigen Response-Maßnahmen ein. Dabei ist Vertrauen sehr wichtig. Denn im Zweifel greift der Managed Security Services Provider auf hochsensible Daten zu. Übrigens geht der Trend eindeutig in diese Richtung. Moderne Security-Lösungen sind derart komplex, dass Anwender deren Voraussetzungen, Funktionsweisen und Auswirkungen nicht mehr verstehen. Darum kommen immer mehr Hersteller von Security-Lösungen auf Arvato Systems als Security-Experten zu. Im Rahmen solcher Partnerschaften monitoren unsere Mitarbeiter im SOC die Gefahrenlage und leiten im Fall der Fälle die erforderlichen Response- und Remediation-Maßnahmen ein. So wird Cyber Security zu einem erfolgskritischen Business-Prozess.

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

Jeder führende IT-Security Hersteller hat heute sein „Lab“, in dem Innovationen heranreifen und getestet werden. Basis für alles ist jedoch die Vision einer Sicherheitsarchitektur, die über das Merkmal von reiner Abwehr und Prevention hinausgeht.

Watchguard hat mit der Übernahme von Panda Security nicht nur die Brücke vom Perimeter bis zum Endpunkt geschlagen. Aktuell arbeitet das Unternehmen daran, alle Bereiche seines Vier-Säulen-Portfolios über eine Oberfläche mit nahtlosem Zusammenspiel im Hintergrund abzubilden. Es geht also grundsätzlich um die nahtlose Verbindung unterschiedlicher Security-Bausteine.

Das bedeutet, das wir jetzt also nicht mehr nur vom potenziellen Erkenntnis- und Effizienzgewinn reden, der sich durch die Integration der einzelnen Lösungen ergibt, sondern über die konkrete Umsetzung. In der Architektur, siehe Bild Seite 7, spielt das Automation Core Framework eine zentrale Rolle als Enabler.

Es verzahnt spezifische Sicherheitsfunktionalität vom Perimeter bis zum Endpunkt und setzt dabei auf cloudbasiertes Management und Automatisierungstechnologie. Natürlich ist es skalierbar, potenziell erweiterbar und steuerbar und kann als Managed Service betrieben werden.

SECURITY-KONSOLIDIERUNG

DAS ZÜNGLEIN AN DER WAAGE

Immer weniger Fachpersonal für IT-Security trifft auf eine zunehmend komplexere Gefahrenlandschaft. Michael Haas, Vice President Central Europe bei WatchGuard Technologies, spricht mit Ulrich Parthier, Publisher it security, über allgegenwärtige Herausforderungen und zukunftsfähige Lösungsszenarien bei der Absicherung von Unternehmensressourcen.

Ulrich Parthier: *Der Fachkräftemangel im IT-Bereich bewegt nicht erst seit gestern die Gemüter. Durch die Pandemie wurde dieses Problem nochmals befeuert. Wie schätzen Sie die aktuelle Lage ein?*

Michael Haas: Es klafft eine große Lücke. Durch die Dezentralisierung der Arbeitsstrukturen, die von COVID-19 ausgelöst wurde, ist der Aufwand innerhalb der IT-Abteilungen im Frühjahr 2020 quasi von heute auf morgen in die Höhe geschnellt. Insbesondere im Hinblick auf IT-Security sind ganz neue Aufgaben hinzugekommen. Die Absicherung von Homeoffice-Szenarien geht mit vielfältigen Herausforderungen einher, die so und in diesem Umfang vor zwei Jahren noch kein Unternehmen auf dem Schirm hatte. Natürlich kam es im Zuge des Lockdowns zunächst vor allem darauf an, die Produktivität im Tagesgeschäft zu gewährleisten. Die mit dezentralen Arbeitsmodellen einhergehenden, sicherheitsrelevanten Implikationen dürfen aber auf gar keinen Fall vergessen werden. Denn entsprechende Security-Lücken sind ein gefundenes Fressen für Cyberkriminelle. Endpoint Protection ist das Gebot der Stunde – wobei auch die Absicherung des klassischen Perimeters nicht in den Hintergrund rücken sollte. Die Analysen des WatchGuard Threat Labs, das kontinuierlich aktuelle Angriffsszenarien auswertet, belegen ganz eindeutig, dass Angreifer alle Fronten nutzen und dabei immer perfider und vielschichtiger vorgehen. Und je mehr Angriffsvektoren es gibt, desto mehr Arbeit haben die IT-Sicherheitsverantwortlichen auf Unternehmensseite. Dies unterstreichen nicht zuletzt einschlägige Studien.

WatchGuard Technologies verzahnt spezifische Sicherheitsfunktionalität vom Perimeter bis zum Endpunkt und setzt dabei auf cloudbasiertes Management und Automatisierungstechnologie.

Ulrich Parthier: *Können Sie dies weiter präzisieren?*

Michael Haas: In einer 2020 von LogMeIn durchgeführten Umfrage geben 54 Prozent der teilnehmenden IT-Administratoren an, dass sie heute mehr Zeit für die Abwehr von Bedrohungen aufwenden müssen als je zuvor. Darüber hinaus verbringen 47 Prozent von ihnen mittlerweile fünf bis acht Stunden pro Tag nur mit dem Thema IT-Sicherheit. Die dafür aufgewendete Zeit fehlt an anderer Stelle. Zum Vergleich: 2019 betrug dieser Wert noch 35 Prozent. Diese Entwicklung deckt sich absolut mit unseren Einblicken in die weltweite Gefahrenlandschaft. Denn Angriffe nehmen nicht nur quantitativ zu, sondern sind darüber hinaus von ganz anderer Qualität als noch vor wenigen Jahren. Wer hier nicht am Ball bleibt, kann schnell zum Opfer

werden. Doch dieses „am Ball bleiben" ist eben auch aufwendig. Und obwohl die gerade erwähnte Umfrage unter IT-Verantwortlichen in Nordamerika stattfand, sieht die Lage in den hiesigen IT-Abteilungen kaum anders aus. Viele stehen an der Grenze der Belastbarkeit, eine Trendwende ist nicht in Sicht. Das Aufstocken der Kapazitäten gestaltet sich jedoch gerade für kleine und mittelständische Unternehmen immer schwieriger. Im Kampf um qualifiziertes Personal haben sie häufig das Nachsehen. Angreifer nehmen darauf leider keine Rücksicht – ganz im Gegenteil. Umso mehr gilt es, nach alternativen Lösungswegen zu suchen, wenn die internen Möglichkeiten limitiert sind.

Ulrich Parthier: *Welche Alternativen sehen Sie in dem Fall?*

Michael Haas: Hier gibt es in meinen Augen über kurz oder lang eigentlich nur zwei Optionen: Outsourcing oder konsequente Konsolidierung.

Ulrich Parthier: *Dann fangen wir mal bei der Konsolidierung an: Was genau verstehen Sie darunter?*

> IM ZWEIFELSFALL IST GUT OUTGESOURCT BESSER ALS SCHLECHT SELBST GEMACHT.
>
> Michael Haas,
> Regional Vice President Central Europe,
> WatchGuard Technologies GmbH,
> www.watchguard.de

Michael Haas: Klassischerweise ist es ja so, dass die IT-Security-Konzepte auf Unternehmensseite über die Jahre gewachsen sind. Sicherheitsmaßnahmen wurden nicht in einem Guss, sondern Schritt für Schritt aufgebaut und an neue Anforderungen angepasst. In Folge kommen heute meist unterschiedlichste Lösungen und Prozesse zum Tragen, die alle einen ganz spezifischen Zweck verfolgen – sei es die Absicherung des Perimeters oder auch der Schutz von Endpunkten. Ein solches Stückwerk im Werkzeugkasten der IT-Sicherheit ist jedoch in gleich zweifacher Hinsicht kontraproduktiv. Zum einen erhöht sich mit jeder „Einzellösung" der Aufwand, da jede für sich im Auge behalten und gepflegt werden muss. Der andere Punkt ist die Sicherheitseffizienz. Denn selbst wenn über Schnittstellen und (meist) komplexe Prozesse ein Austausch zwischen den verschiedenen Sicherheitssilos unterstützt wird, ist der kumulative Erkenntnis- und Effizienzgewinn bei weitem nicht so groß wie bei einem nativen Zusammenspiel der einzelnen Security-Funktionalitäten. Hier haben wir mittlerweile eindeutige Erfahrungswerte.

Ulrich Parthier: *Bezieht sich diese Aussage auf die im vergangenen Jahr erfolgte Übernahme von Panda Security als Spezialisten für Endpoint Security?*

Michael Haas: Auch, aber nicht nur. Mit der Erweiterung unseres Produktspektrums um die hochentwickelten Technologien von Panda Security ist es uns gelungen, die Brücke vom Perimeter bis zum Endpunkt zu schlagen. WatchGuard bietet heute ein breites Portfolio, das neben der klassischen Netzwerksicherheit,

Multifaktor-Authentifizierung und sicherem cloudbasiertem WLAN eben auch Endpoint Protection umfasst. Gerade dieser Bereich hat im Zuge der Pandemie massiv an Fahrt aufgenommen. Themen wie Endpoint Detection and Response, Threat Hunting, Endpoint AV, E-Mail-Sicherheit, Patching, Daten-Compliance und Verschlüsselung sind auf der Agenda vieler IT-Verantwortlicher schlicht und ergreifend aufgrund der Umstände in den letzten Monaten an oberste Stelle gerückt. Den entsprechenden Bedarf mit einer spezifischen Lösung bedienen zu können, ist vor diesem Hintergrund natürlich per se schon von Vorteil. Mit der Konsolidierung unserer umfangreichen Security-Funktionalitäten auf einer einzigen Plattform nehmen wir jedoch eine weitere wichtige Stufe. Einzelne Produktsegmente wie Netzwerksicherheit und Multifaktor-Authentifizierung hatten wir ja bereits vorher in der Cloud zusammengeführt und damit sowohl den Nerv unserer Kunden als auch Partner getroffen. Aktuell arbeiten wir daran, wirklich alle Bereiche über eine Oberfläche abzubilden, mit nahtlosem Zusammenspiel im Hintergrund. Wir reden jetzt also nicht mehr nur vom potenziellen Erkenntnis- und Effizienzgewinn, der sich durch die Integration der einzelnen Lösungen ergibt, sondern schaffen Tatsachen.

? **Ulrich Parthier:** *Können Sie hier weiter ins Detail gehen?*

Michael Haas: Gerne. Grundsätzlich geht es um die nahtlose Verbindung der unterschiedlichen Security-Bausteine. Für uns konkret besteht die erste Schicht aus den jeweiligen Einzellösungen im Produktportfolio, die über die WatchGuard Cloud eng miteinander verzahnt werden und sich dadurch einheitlich und zentral verwalten lassen. Anpassungen hinsichtlich des Leistungsumfangs sind darüber im Handumdrehen möglich. Dadurch ergibt sich größtmögliche Flexibilität, um auch auf neue Anforderungen jederzeit schnell reagieren zu können. Last but not least steht hinter allem das WatchGuard Automation Core Framework, wodurch wir viele Prozesse zusätzlich automatisieren können – sowohl im Hinblick auf operative Aufgaben wie etwa Updates als auch bei der Bedrohungsabwehr selbst. So werden nicht nur Auffälligkeiten über alle Funktionsbereiche hinweg korreliert und bewertet, sondern bei Bedarf und entsprechender Einstellung auch automatisch die erforderlichen Gegenmaßnahmen ergriffen. Durch diese Automatismen auf Basis integrierter Funktionalitäten lässt sich der Aufwand, den IT-Verantwortliche bisher betreiben, um bis zu 80 Prozent reduzieren. Es ergeben sich also vielfältige Vorteile: Zeiteinsparung dank Automatisierung, Kostenvorteile durch Cloud-Einsatz sowie Reduktion von Einzellösungen und sicher nicht zuletzt auch ein besserer Schutz, da durch den integrativen Ansatz tote Winkel bei der Gefahrenabwehr weiter minimiert werden. Gerade vielschichtigen Angriffsmustern lässt sich auf diese Weise deutlich besser auf die Spur kommen, da Vorfälle aus unterschiedlicher Richtung unter Zuhilfenahme von künstlicher Intelligenz und maschinellem Lernen zu einem aussagekräftigen Gesamtbild zusammengefügt werden können.

? **Ulrich Parthier:** *Mit einer Konsolidierung erhöht sich aber gleichzeitig die Herstellerabhängigkeit auf Anwenderseite. Wie bewerten Sie dies?*

Michael Haas: Ich glaube, dass dieser Punkt eigentlich kaum eine Rolle spielt. Laut Gartner befassen sich bereits 80 Prozent der Unternehmen mit dem Thema IT-Security-Konsolidierung oder sind bereits dabei, in den eigenen Reihen aufzuräumen, um der Komplexität Einhalt zu gebieten und für Entlastung zu sorgen. Wichtig ist eigentlich nur, dass das Gesamtkonzept stimmt. Eine Lösung, die unterschiedlichste Anforderungen vom Netzwerk bis zum Endpunkt abbildet, weniger Aufwand verursacht und darüber hinaus bei der Leistungsfähigkeit der Gefahrenabwehr durch ganzheitliche Betrachtung sogar noch eine Schippe drauflegt, ist dann eher ein Türöffner. Es ist bereits angeklungen, dass die Absicherung von Unternehmensressourcen immer mehr einer Sisyphos-Aufgabe gleicht. Fertig wird man damit eigentlich nie und ohne ausreichende Personalkapazitäten schon gar nicht. Es verwundert daher kaum, dass sich auch das Outsourcing zunehmender Beliebtheit erfreut. Im Zweifelsfall ist gut outgesourct immer noch besser als schlecht selbst gemacht. Hier tut sich gerade einiges im Markt.

? **Ulrich Parthier:** *Gutes Stichwort für eine abschließende Frage: Gehört Managed Security Services die Zukunft?*

Michael Haas: Ich bin der festen Überzeugung, dass sich solche Angebote gerade im KMU-Umfeld mittel- bis langfristig durchsetzen werden. Schließlich bieten die neuen Möglichkeiten auch IT-Partnern – die beim Aufbau unserer Unified Security Plattform im Fokus standen – ein optimales Fundament, um attraktive Angebote zu schnüren, mit denen sich der aktuelle Schmerz auf Unternehmensseite effektiv heilen lässt. Firmen sind nur zu gerne bereit, die aufwendigen Aufgaben im IT-Security-Bereich komplett in professionelle externe Hände zu geben – vorausgesetzt, das Preis-Leistungs-Verhältnis stimmt. Und Systemhäuser greifen die zusätzlichen Umsatzmöglichkeiten natürlich mit Eifer auf, wenn Einsatz und Gewinn in einem lohnenswerten Verhältnis stehen. Und genau darauf zielt Konsolidierung ab.

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

DATENSICHERHEIT

FÜNF TIPPS FÜR DIE POST-CORONA-WELT

Der rasche und flächendeckende Umzug ganzer Belegschaften ins Homeoffice schuf Cyberkriminellen ungeahnte Optionen, um Remote-Mitarbeiter ins Visier zu nehmen – mit immensen Kosten. Nach vorsichtigen Schätzungen waren 80 Prozent der Organisationen weltweit im Jahr 2020 von Phishing-Angriffen betroffen, und allein im dritten Quartal stiegen die durchschnittlichen Lösegeldzahlungen im Vergleich zum Vorquartal um mehr als 31 Prozent.

Die IT hat sich der neuen Bedrohungsrealität angepasst. So sind automatisierte IT-Security-Lösungen verfügbar, um mit einer verteilten Belegschaft sicher zu arbeiten. Aber um diese auch sicher umzusetzen, ist ein strategischer Unterbau nötig. Dabei hat sich ein Zero Trust Framework in den letzten Monaten als gangbarer Weg herauskristallisiert. Bis 2025, so aktuelle Schätzungen, werden Zero-Trust-Zugang und -Architektur die Norm sein. Der Grundgedanke hinter Zero Trust: Firmen müssen davon ausgehen, dass sich Angreifer bereits im Netzwerk befinden – unabhängig davon, welche Sicherheitskontrollen oder -technologien eingesetzt werden. Sicherheit lässt sich nur dann gewährleisten, wenn ein „never trust, always verify"-Ansatz konsequent umgesetzt wird. 5 Tipps von Ivanti helfen, um diesen Zero-Trust-Pfad einzuschlagen:

1. Geräte verstehen und validieren

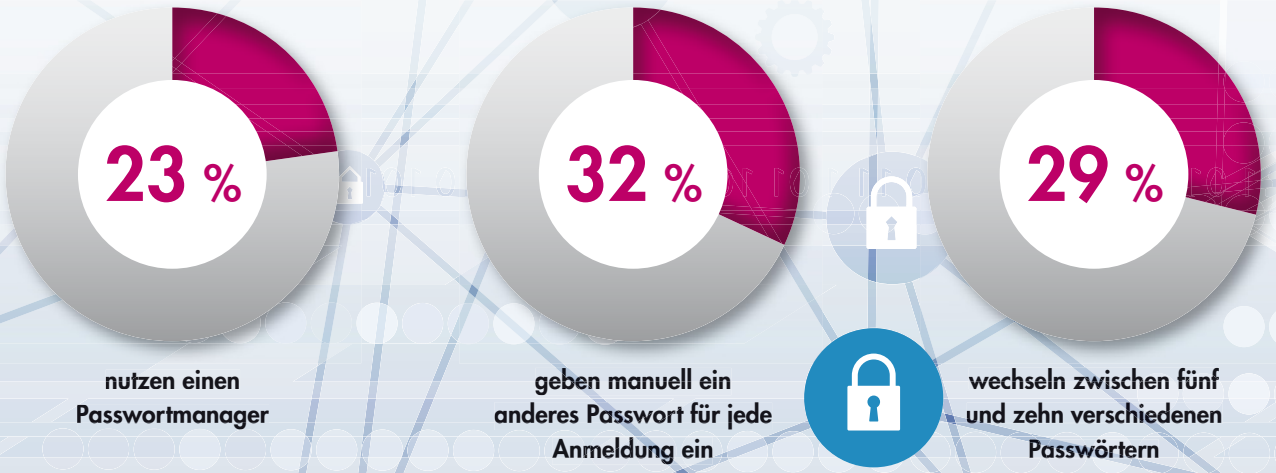
In remoten Arbeitsumgebungen existiert ein zunehmend wachsender Gerätezoo: Assets, die alle in irgendeiner Form Zugriff auf Geschäftsdaten benötigen, um produktiv zu sein. Wie hoch die Bedrohungsexposition für ein einzelnes Gerät ist, muss individuell abgewogen werden, bevor ihm der Zugriff auf eine Unternehmensressourcen erlaubt wird. Eine Plattform, die die Bereitstellung beliebiger Geräte ermöglicht, ist dazu unerlässlich. Darin eingeschlossen sind unternehmenseigene wie auch mitarbeitereigene Devices. Dies gibt IT-Teams einen bestmöglichen Überblick über alle Endgeräte, die für den Zugriff auf Geschäftsdaten verwendet werden.

2. Verschärfte Sicherheit ohne Passwörter

Die Kombination aus Passwort und Benutzername ist mit Remote Work schlicht nicht mehr vereinbar. Eine aktuelle Studie von Ivanti sagt aus, dass 78 Prozent der deutschen CISOs der Ansicht sind, dass Passwörter kein wirksames Mittel zum Schutz von Unternehmensdaten mehr sind. An ihre Stelle sollten Technologien wie digitale Zertifikate zum Einsatz kommen, die mit biometrischen Funktionen kombiniert werden.

Damit müssen IT-Mitarbeiter allerdings auch besser in der Lage sein, kontextbezogene Attribute zu berücksichtigen: „Von wo aus verbindet sich der Mitarbeiter?" oder „Welcher Gerätetyp wird kompromittiert?". Nur durch die konsequente Prüfung der wichtigsten Sicherheitsattribute, gesammelt vom Benutzer und Ge-

PASSWORT MANAGEMENT



FIRMEN MÜSSEN DAVON AUSGEHEN, DASS SICH ANGREIFER BEREITS IM NETZWERK BEFINDEN – UNABHÄNGIG DAVON, WELCHE SICHERHEITSKONTROLLEN ODER -TECHNOLOGIEN EINGESETZT WERDEN.

Andreas Schmid, Sales Engineering Manager, EMEA Central, Ivanti, www.ivanti.de

rät, lässt sich eine Zero-Trust-Beziehung herstellen.

3. Richtlinien für Apps...

Unternehmen sollten den Datenzugriff nur solchen Apps erlauben, denen sie vertrauen und die sie verwalten können. Doch selbst für vertrauenswürdige Apps müssen DLP-Richtlinien (Data Loss Prevention) implementiert werden. Sie legen fest, wie und mit wem Daten geteilt werden können. Wenn eine App, der Benutzer oder das Gerät nicht mehr vertrauenswürdig sind, sollten Möglichkeiten existieren, den Zugriff auf einen Cloud-Dienst zu sperren, eine nicht vertrauenswürdige App zu entfernen oder sensible Daten vom Gerät zu löschen.

4. ... und den Netzwerkzugriff

Ebenfalls empfehlenswert sind Richtlinien, die vorschreiben, wie Nutzer auf Daten über unsichere Netzwerke zugreifen können. An VPN-Verbindungen führt dabei kein Weg vorbei. Die bei weitem sicherste Lösung für Remote-Mitarbeiter bietet der Einsatz eines Per-App-VPNs. Es handelt sich um einen verschlüsselten Split-Tunnel, bei dem sich mobile Nutzer über eine sichere SSL-Verbindung mit Unternehmensressourcen verbinden und über das Internet auf persönliche Apps und Webseiten zugreifen. Nur zugelassene Apps greifen dann auf den sicheren Tunnel und letztlich auf die geschützte Unternehmensressource zu.

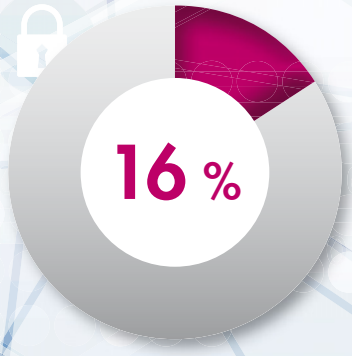
5. Automatisierter Schutz

Automatisierte Tools und maschinelles Lernen (ML) zeigen ihre Stärke, wenn es darum geht, die Angriffsvektoren remoter Mitarbeiter zu verringern. Denn Zeit spielt eine wichtige Rolle. Bedrohungen müssen frühzeitig erkannt werden und proaktive Maßnahmen zur Eindämmung anlaufen. Eine gute Lösung sollte hier eine Verteidigungslinie aufbauen, wenn verdächtige Aktivitäten erkannt werden. Das kann eine Warnung an den Benutzer oder die Sperrung einer Cloud-Ressource sein.

Selbstheilung implementieren

Unternehmen stellen ihren Mitarbeitern Arbeitsmittel zur Verfügung, die sie produktiv und gerne nutzen. Mitarbeiter, die in der Warteschleife des Helpdesks hängen sind nicht zielführend. Deshalb gilt es, neben allen Zero-Trust-Sicherheitsmaßnahmen, Möglichkeiten zu bieten Dienste wieder bereitzustellen, sobald eine Bedrohung vorüber ist. Ein Bedrohungs-Dashboard reicht letztlich nicht aus. Essenziell ist es, rasch auf einen Angriff zu reagieren und den Betrieb unmittelbar wieder aufnehmen zu können, sobald die Bedrohung gebannt ist.

Andreas Schmid



nutzen für alle Accounts ein bis zwei Passwörter

Quelle: www.proofpoint.com; 2020 State of the Phish)

QUANTENCOMPUTING & IT SICHERHEIT

EINE NEUE ÄRA BEGINNT

Das eBook umfasst 69 Seiten und steht kostenlos zum Download bereit. www.it-daily.net/download

Quantencomputer – Noch sind sie nicht da, aber es gibt jede Menge Ankündigungen. Ganz so trivial ist die Entwicklung also doch nicht. Schon jetzt stellen sich die gleichen Fragen wie bei anderen IT-Themen auch: Wie sieht es mit der IT-Sicherheit aus? Wer betreibt meine Rechner und wo bekomme ich entsprechendes Fachpersonal her?

Highlights aus dem eBook

Daten von heute sind morgen unsicher

Viele Daten, die Unternehmen heute speichern, werden noch dann schützenswert sein, wenn Quantencomputer schon längst verbreitet sind. Ihre Verschlüsselung ist dann aber obsolet.

Quantencomputer und die IT-Sicherheit

Kryptographie hat die Aufgabe, Informationen verschlüsselt zu übertragen und nach Empfang wieder zu entschlüsseln. Die Kryptoanalyse ist gegenteilig ausgelegt. Ihr geht es um das Brechen von Verschlüsselungen, ohne das dies von Sender und Empfänger bemerkt wird.

Was bringt die Post-Quantum-Kryptographie?

Bereits heute wird an Quantenschlüsselaustausch geforscht. Das Ziel lautet, sensible Informationen so zu übertragen, dass deren Vertraulichkeit gewahrt bleibt. Diese kryptographischen Schlüssel können weder unbemerkt kopiert noch mitgelesen werden.

EDR ON PREMISES?

WARUM EDR IM EIGENEN RZ GENAUSO GUT FUNKTIONIERT WIE IN DER CLOUD

Endpoint Detection and Response (EDR) war bis vor wenigen Jahren großen Unternehmen mit vielen Mitarbeitern oder besonders hohen Sicherheitsansprüchen vorbehalten. Angesichts der heutigen Bedrohungslage und neuer Regulierungen, ist EDR heute auch für die meisten Mittelständler unverzichtbar.

Neue Lösungen setzen auf Automatisierung, geringen Personalaufwand und die Reduktion von Fehlalarmen. Doch ein Problem bleibt: Fast alle EDR-Angebote laufen in der Cloud. Bestimmte Branchen setzen dagegen oft auf eine lokale IT-Infrastruktur, um Datenschutzbestimmungen Rechnung zu tragen. Technisch ist es möglich, EDR im eigenen Rechenzentrum zu betreiben.

Dieses Whitepaper beschreibt Lösungen zur Erkennung und Abwehr von Bedrohungen am Endpunkt.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 11 Seiten und steht kostenlos zum Download bereit. ***www.it-daily.net/download***

Multifaktor-Authentifizierung und sicherem cloudbasiertem WLAN eben auch Endpoint Protection umfasst. Gerade dieser Bereich hat im Zuge der Pandemie massiv an Fahrt aufgenommen. Themen wie Endpoint Detection and Response, Threat Hunting, Endpoint AV, E-Mail-Sicherheit, Patching, Daten-Compliance und Verschlüsselung sind auf der Agenda vieler IT-Verantwortlicher schlicht und ergreifend aufgrund der Umstände in den letzten Monaten an oberste Stelle gerückt. Den entsprechenden Bedarf mit einer spezifischen Lösung bedienen zu können, ist vor diesem Hintergrund natürlich per se schon von Vorteil. Mit der Konsolidierung unserer umfangreichen Security-Funktionalitäten auf einer einzigen Plattform nehmen wir jedoch eine weitere wichtige Stufe. Einzelne Produktsegmente wie Netzwerksicherheit und Multifaktor-Authentifizierung hatten wir ja bereits vorher in der Cloud zusammengeführt und damit sowohl den Nerv unserer Kunden als auch Partner getroffen. Aktuell arbeiten wir daran, wirklich alle Bereiche über eine Oberfläche abzubilden, mit nahtlosem Zusammenspiel im Hintergrund. Wir reden jetzt also nicht mehr nur vom potenziellen Erkenntnis- und Effizienzgewinn, der sich durch die Integration der einzelnen Lösungen ergibt, sondern schaffen Tatsachen.

? **Ulrich Parthier:** *Können Sie hier weiter ins Detail gehen?*

Michael Haas: Gerne. Grundsätzlich geht es um die nahtlose Verbindung der unterschiedlichen Security-Bausteine. Für uns konkret besteht die erste Schicht aus den jeweiligen Einzellösungen im Produktportfolio, die über die WatchGuard Cloud eng miteinander verzahnt werden und sich dadurch einheitlich und zentral verwalten lassen. Anpassungen hinsichtlich des Leistungsumfangs sind darüber im Handumdrehen möglich. Dadurch ergibt sich größtmögliche Flexibilität, um auch auf neue Anforderungen jederzeit schnell reagieren zu können. Last but not least steht hinter allem das WatchGuard Automation Core Framework, wodurch wir viele Prozesse zusätzlich automatisieren können – sowohl im Hinblick auf operative Aufgaben wie etwa Updates als auch bei der Bedrohungsabwehr selbst. So werden nicht nur Auffälligkeiten über alle Funktionsbereiche hinweg korreliert und bewertet, sondern bei Bedarf und entsprechender Einstellung auch automatisch die erforderlichen Gegenmaßnahmen ergriffen. Durch diese Automatismen auf Basis integrierter Funktionalitäten lässt sich der Aufwand, den IT-Verantwortliche bisher betreiben, um bis zu 80 Prozent reduzieren. Es ergeben sich also vielfältige Vorteile: Zeiteinsparung dank Automatisierung, Kostenvorteile durch Cloud-Einsatz sowie Reduktion von Einzellösungen und sicher nicht zuletzt auch ein besserer Schutz, da durch den integrativen Ansatz tote Winkel bei der Gefahrenabwehr weiter minimiert werden. Gerade vielschichtigen Angriffsmustern lässt sich auf diese Weise deutlich besser auf die Spur kommen, da Vorfälle aus unterschiedlicher Richtung unter Zuhilfenahme von künstlicher Intelligenz und maschinellem Lernen zu einem aussagekräftigen Gesamtbild zusammengefügt werden können.

? **Ulrich Parthier:** *Mit einer Konsolidierung erhöht sich aber gleichzeitig die Herstellerabhängigkeit auf Anwenderseite. Wie bewerten Sie dies?*

Michael Haas: Ich glaube, dass dieser Punkt eigentlich kaum eine Rolle spielt. Laut Gartner befassen sich bereits 80 Prozent der Unternehmen mit dem Thema IT-Security-Konsolidierung oder sind bereits dabei, in den eigenen Reihen aufzuräumen, um der Komplexität Einhalt zu gebieten und für Entlastung zu sorgen. Wichtig ist eigentlich nur, dass das Gesamtkonzept stimmt. Eine Lösung, die unterschiedlichste Anforderungen vom Netzwerk bis zum Endpunkt abbildet, weniger Aufwand verursacht und darüber hinaus bei der Leistungsfähigkeit der Gefahrenabwehr durch ganzheitliche Betrachtung sogar noch eine Schippe drauflegt, ist dann eher ein Türöffner. Es ist bereits angeklungen, dass die Absicherung von Unternehmensressourcen immer mehr einer Sisyphos-Aufgabe gleicht. Fertig wird man damit eigentlich nie und ohne ausreichende Personalkapazitäten schon gar nicht. Es verwundert daher kaum, dass sich auch das Outsourcing zunehmender Beliebtheit erfreut. Im Zweifelsfall ist gut outgesourct immer noch besser als schlecht selbst gemacht. Hier tut sich gerade einiges im Markt.

? **Ulrich Parthier:** *Gutes Stichwort für eine abschließende Frage: Gehört Managed Security Services die Zukunft?*

Michael Haas: Ich bin der festen Überzeugung, dass sich solche Angebote gerade im KMU-Umfeld mittel- bis langfristig durchsetzen werden. Schließlich bieten die neuen Möglichkeiten auch IT-Partnern – die beim Aufbau unserer Unified Security Plattform im Fokus standen – ein optimales Fundament, um attraktive Angebote zu schnüren, mit denen sich der aktuelle Schmerz auf Unternehmensseite effektiv heilen lässt. Firmen sind nur zu gerne bereit, die aufwendigen Aufgaben im IT-Security-Bereich komplett in professionelle externe Hände zu geben – vorausgesetzt, das Preis-Leistungs-Verhältnis stimmt. Und Systemhäuser greifen die zusätzlichen Umsatzmöglichkeiten natürlich mit Eifer auf, wenn Einsatz und Gewinn in einem lohnenswerten Verhältnis stehen. Und genau darauf zielt Konsolidierung ab.

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

DATENSICHERHEIT

FÜNF TIPPS FÜR DIE POST-CORONA-WELT

Der rasche und flächendeckende Umzug ganzer Belegschaften ins Homeoffice schuf Cyberkriminellen ungeahnte Optionen, um Remote-Mitarbeiter ins Visier zu nehmen – mit immensen Kosten. Nach vorsichtigen Schätzungen waren 80 Prozent der Organisationen weltweit im Jahr 2020 von Phishing-Angriffen betroffen, und allein im dritten Quartal stiegen die durchschnittlichen Lösegeldzahlungen im Vergleich zum Vorquartal um mehr als 31 Prozent.

Die IT hat sich der neuen Bedrohungsrealität angepasst. So sind automatisierte IT-Security-Lösungen verfügbar, um mit einer verteilten Belegschaft sicher zu arbeiten. Aber um diese auch sicher umzusetzen, ist ein strategischer Unterbau nötig. Dabei hat sich ein Zero Trust Framework in den letzten Monaten als gangbarer Weg herauskristallisiert. Bis 2025, so aktuelle Schätzungen, werden Zero-Trust-Zugang und -Architektur die Norm sein. Der Grundgedanke hinter Zero Trust: Firmen müssen davon ausgehen, dass sich Angreifer bereits im Netzwerk befinden – unabhängig davon, welche Sicherheitskontrollen oder -technologien eingesetzt werden. Sicherheit lässt sich nur dann gewährleisten, wenn ein „never trust, always verify"-Ansatz konsequent umgesetzt wird. 5 Tipps von Ivanti helfen, um diesen Zero-Trust-Pfad einzuschlagen:

1. Geräte verstehen und validieren

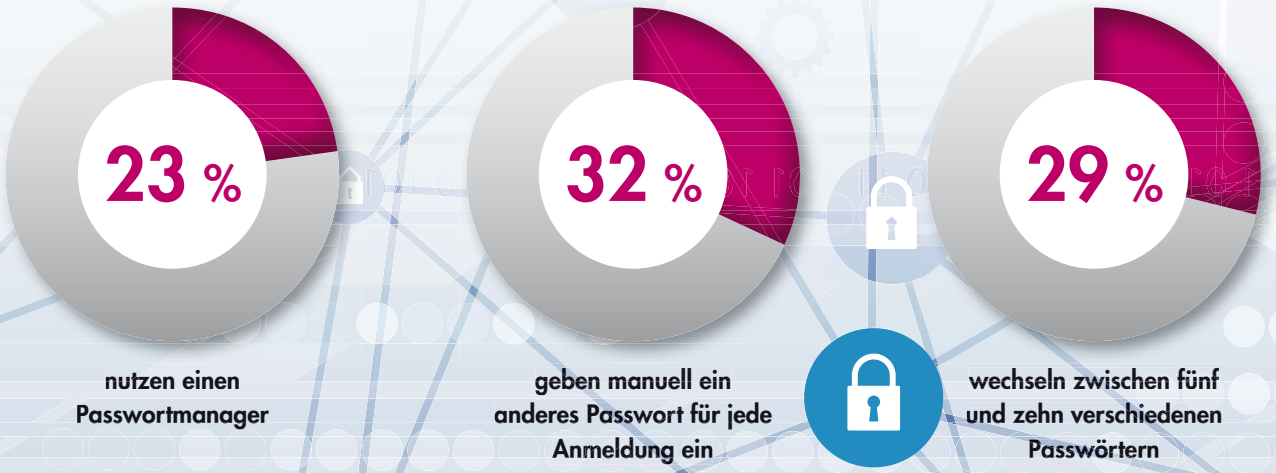
In remoten Arbeitsumgebungen existiert ein zunehmend wachsender Gerätezoo: Assets, die alle in irgendeiner Form Zugriff auf Geschäftsdaten benötigen, um produktiv zu sein. Wie hoch die Bedrohungsexposition für ein einzelnes Gerät ist, muss individuell abgewogen werden, bevor ihm der Zugriff auf eine Unternehmensressourcen erlaubt wird. Eine Plattform, die die Bereitstellung beliebiger Geräte ermöglicht, ist dazu unerlässlich. Darin eingeschlossen sind unternehmenseigene wie auch mitarbeitereigene Devices. Dies gibt IT-Teams einen bestmöglichen Überblick über alle Endgeräte, die für den Zugriff auf Geschäftsdaten verwendet werden.

2. Verschärfte Sicherheit ohne Passwörter

Die Kombination aus Passwort und Benutzername ist mit Remote Work schlicht nicht mehr vereinbar. Eine aktuelle Studie von Ivanti sagt aus, dass 78 Prozent der deutschen CISOs der Ansicht sind, dass Passwörter kein wirksames Mittel zum Schutz von Unternehmensdaten mehr sind. An ihre Stelle sollten Technologien wie digitale Zertifikate zum Einsatz kommen, die mit biometrischen Funktionen kombiniert werden.

Damit müssen IT-Mitarbeiter allerdings auch besser in der Lage sein, kontextbezogene Attribute zu berücksichtigen: „Von wo aus verbindet sich der Mitarbeiter?" oder „Welcher Gerätetyp wird kompromittiert?". Nur durch die konsequente Prüfung der wichtigsten Sicherheitsattribute, gesammelt vom Benutzer und Ge-

PASSWORT MANAGEMENT



FIRMEN MÜSSEN DAVON AUSGEHEN, DASS SICH ANGREIFER BEREITS IM NETZWERK BEFINDEN – UNABHÄNGIG DAVON, WELCHE SICHERHEITSKONTROLLEN ODER -TECHNOLOGIEN EINGESETZT WERDEN.

Andreas Schmid, Sales Engineering Manager, EMEA Central, Ivanti, www.ivanti.de

rät, lässt sich eine Zero-Trust-Beziehung herstellen.

3. Richtlinien für Apps...

Unternehmen sollten den Datenzugriff nur solchen Apps erlauben, denen sie vertrauen und die sie verwalten können. Doch selbst für vertrauenswürdige Apps müssen DLP-Richtlinien (Data Loss Prevention) implementiert werden. Sie legen fest, wie und mit wem Daten geteilt werden können. Wenn eine App, der Benutzer oder das Gerät nicht mehr vertrauenswürdig sind, sollten Möglichkeiten existieren, den Zugriff auf einen Cloud-Dienst zu sperren, eine nicht vertrauenswürdige App zu entfernen oder sensible Daten vom Gerät zu löschen.

4. ... und den Netzwerkzugriff

Ebenfalls empfehlenswert sind Richtlinien, die vorschreiben, wie Nutzer auf Daten über unsichere Netzwerke zugreifen können. An VPN-Verbindungen führt dabei kein Weg vorbei. Die bei weitem sicherste Lösung für Remote-Mitarbeiter bietet der Einsatz eines Per-App-VPNs. Es handelt sich um einen verschlüsselten Split-Tunnel, bei dem sich mobile Nutzer über eine sichere SSL-Verbindung mit Unternehmensressourcen verbinden und über das Internet auf persönliche Apps und Webseiten zugreifen. Nur zugelassene Apps greifen dann auf den sicheren Tunnel und letztlich auf die geschützte Unternehmensressource zu.

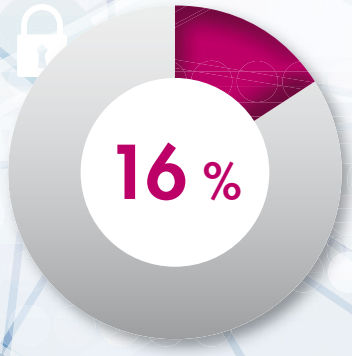
5. Automatisierter Schutz

Automatisierte Tools und maschinelles Lernen (ML) zeigen ihre Stärke, wenn es darum geht, die Angriffsvektoren remoter Mitarbeiter zu verringern. Denn Zeit spielt eine wichtige Rolle. Bedrohungen müssen frühzeitig erkannt werden und proaktive Maßnahmen zur Eindämmung anlaufen. Eine gute Lösung sollte hier eine Verteidigungslinie aufbauen, wenn verdächtige Aktivitäten erkannt werden. Das kann eine Warnung an den Benutzer oder die Sperrung einer Cloud-Ressource sein.

Selbstheilung implementieren

Unternehmen stellen ihren Mitarbeitern Arbeitsmittel zur Verfügung, die sie produktiv und gerne nutzen. Mitarbeiter, die in der Warteschleife des Helpdesks hängen sind nicht zielführend. Deshalb gilt es, neben allen Zero-Trust-Sicherheitsmaßnahmen, Möglichkeiten zu bieten Dienste wieder bereitzustellen, sobald eine Bedrohung vorüber ist. Ein Bedrohungs-Dashboard reicht letztlich nicht aus. Essenziell ist es, rasch auf einen Angriff zu reagieren und den Betrieb unmittelbar wieder aufnehmen zu können, sobald die Bedrohung gebannt ist.

Andreas Schmid



nutzen für alle Accounts ein bis zwei Passwörter

Quelle: www.proofpoint.com; 2020 State of the Phish)

QUANTENCOMPUTING & IT SICHERHEIT

EINE NEUE ÄRA BEGINNT

Das eBook umfasst 69 Seiten und steht kostenlos zum Download bereit. www.it-daily.net/download

Quantencomputer – Noch sind sie nicht da, aber es gibt jede Menge Ankündigungen. Ganz so trivial ist die Entwicklung also doch nicht. Schon jetzt stellen sich die gleichen Fragen wie bei anderen IT-Themen auch: Wie sieht es mit der IT-Sicherheit aus? Wer betreibt meine Rechner und wo bekomme ich entsprechendes Fachpersonal her?

Highlights aus dem eBook

Daten von heute sind morgen unsicher

Viele Daten, die Unternehmen heute speichern, werden noch dann schützenswert sein, wenn Quantencomputer schon längst verbreitet sind. Ihre Verschlüsselung ist dann aber obsolet.

Quantencomputer und die IT-Sicherheit

Kryptographie hat die Aufgabe, Informationen verschlüsselt zu übertragen und nach Empfang wieder zu entschlüsseln. Die Kryptoanalyse ist gegenteilig ausgelegt. Ihr geht es um das Brechen von Verschlüsselungen, ohne das dies von Sender und Empfänger bemerkt wird.

Was bringt die Post-Quantum-Kryptographie?

Bereits heute wird an Quantenschlüsselaustausch geforscht. Das Ziel lautet, sensible Informationen so zu übertragen, dass deren Vertraulichkeit gewahrt bleibt. Diese kryptographischen Schlüssel können weder unbemerkt kopiert noch mitgelesen werden.

EDR ON PREMISES?

WARUM EDR IM EIGENEN RZ GENAUSO GUT FUNKTIONIERT WIE IN DER CLOUD

Endpoint Detection and Response (EDR) war bis vor wenigen Jahren großen Unternehmen mit vielen Mitarbeitern oder besonders hohen Sicherheitsansprüchen vorbehalten. Angesichts der heutigen Bedrohungslage und neuer Regulierungen, ist EDR heute auch für die meisten Mittelständler unverzichtbar.

Neue Lösungen setzen auf Automatisierung, geringen Personalaufwand und die Reduktion von Fehlalarmen. Doch ein Problem bleibt: Fast alle EDR-Angebote laufen in der Cloud. Bestimmte Branchen setzen dagegen oft auf eine lokale IT-Infrastruktur, um Datenschutzbestimmungen Rechnung zu tragen. Technisch ist es möglich, EDR im eigenen Rechenzentrum zu betreiben.

Dieses Whitepaper beschreibt Lösungen zur Erkennung und Abwehr von Bedrohungen am Endpunkt.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 11 Seiten und steht kostenlos zum Download bereit. ***www.it-daily.net/download***

PASSWORD SAFE

AUF IN DIE PASSWORTLOSE ZUKUNFT

Mitarbeiter haben heutzutage unzählige geschäftliche Accounts, idealerweise mit komplexen, individuellen und regelmäßig wechselnden Login-Daten. Doch die Realität sieht anders aus: ein und dasselbe Passwort, immer wieder recycelt und mit Zahlen oder Sonderzeichen versehen. Sicher ist das nicht. Und so gehen noch immer 81 Prozent aller Datenschutzverletzungen auf angreifbare Credentials zurück.

IT- und Security-Verantwortliche suchen daher nach neuen Lösungen. Viele setzen ihre Hoffnungen in die aufkommenden biometrischen Angebote. Finger auflegen und los geht's – das klingt verlockend einfach. Was viele vergessen: Auch biometrische Daten sind fehleranfällig und können gehackt werden. Die Kosten der daraus folgenden Imageschäden sind in solchen Fällen kaum zu bemessen.

Deswegen kommen Unternehmen heute nicht mehr an einem Password Manager vorbei. Mit Password Safe von MATESO können Sie Ihre Passwörter sicher generieren, verwalten, teilen und archivieren – dank modernster Verschlüsselungstechnologie und innovativen Features. Das heißt: Passwortsicherheit für Ihre betrieblichen Geheimnisse, Passwortfreiheit für Ihre Mitarbeiter.

Passwortlose Anmeldung: ein passwortfreies Heute

Die passwortlose Anmeldung ist mit Password Safe längst Wirklichkeit. Sie können sich mithilfe von Smartcards oder FIDO-konformen Token einloggen und sicher auf all Ihre Anmeldedaten zugreifen – ohne sich ein einziges Passwort merken zu müssen. Natürlich bietet Password Safe auch die Möglichkeit, sich mit biometrischen Faktoren anzumelden, beispielsweise Touch ID für Mac oder Windows Hello für Windows.

Das ist nicht nur einfacher, sondern schließt auch eventuelle Sicherheitslücken auf Seiten der Endanwender, denn die Gefahr von Social Engineering Hacks wird auf diesem Weg reduziert. Admins und IT-Mitarbeiter können sich weiterhin besonders sicher mittels Master-Passwort einloggen – am besten im Rahmen einer Zwei-Faktor-Authentifizierung in Kombination mit einem Token oder einem biometrischen Faktor.

Single Sign-on: praktische Einmal-Anmeldung

Einmal angemeldet, öffnen sich die Türen zu den gespeicherten Anwendungen, die der User auch direkt aus Password Safe starten kann. Und dank der Browser-Erweiterung werden Passwörter für den Nutzer quasi unsichtbar: Das Programm erkennt automatisch, ob für eine Webseite Anmeldedaten hinterlegt sind, und weist den Nutzer darauf hin.

Password Safe agiert darüber hinaus als Identity Provider und kann mit jedem SAML-Service verknüpft werden. Das heißt, der Nutzer kann sich einfach über Password Safe identifizieren und erhält Zugriff auf Applikationen, ohne dass er seine Credentials speichern oder eintragen muss.

Password Sharing: geteiltes Passwort, doppelte Sicherheit

Es gibt auch immer wieder Situationen, in denen Mitarbeiter zwar Zugriff auf Anwendungen benötigen, aber die dazugehörigen Passwörter nicht einsehen sollen. Dafür bietet Password Safe ein rollenbasiertes Rechtesystem, in dem genau definiert ist, welcher User welches Passwort wie nutzen kann. Darüber hinaus können mittels Password Masking geteilte Passwörter mit einem Sichtschutz angelegt werden, sodass User sie zwar anwenden, aber nicht einsehen können.

Password Safe: für ein sicheres Morgen

Starten Sie mit Password Safe schon heute in die passwortlose Zukunft – zur Entlastung Ihrer Mitarbeiter und Ihrer IT. Denn gut gemanagte Passwörter sind der sicherste Weg, um Ihre Geheimnisse heute und auch morgen zu schützen.

www.passwordsafe.de

MATESO
PASSWORD SAFE

INFORMATIONS-SICHERHEITSMANAGEMENT

DAS HEUTIGE QUALITÄTSMANAGEMENT EINES UNTERNEHMENS

Daten sind das Gold des 21. Jahrhunderts. Umso wichtiger ist es, dass Unternehmen ihre sensiblen Informationen schützen, um finanzielle Schäden zu vermeiden und Firmengeheimnisse zu wahren. Hierbei spielt die Normen-Reihe ISO/IEC 2700x oder deren deutsche Entsprechung DIN EN ISO/IEC 2700x eine zunehmend wichtige Rolle. Darüber sprach Ulrich Parthier, Herausgeber it security, mit Alexander Häußler, Product Compliance Manager ISO/IEC 27001, TÜV SÜD Management Service.

? **Ulrich Parthier:** *Inwieweit entscheidet das Prozess- und Informationssicherheitsmanagement heute über den Erfolg von Unternehmen?*

Alexander Häußler: Ob von der Idee zum fertigen Produkt oder vom Quellcode zur finalen Anwendung – Unternehmen definieren sich über Prozesse. Diese Prozesse bilden die Nervenbahnen der Organisation und bestimmen, wann und wie Arbeitsschritte auszuführen sind. Entsprechend wichtig ist es, diese Prozesse soweit wie möglich zu optimieren. Früher fiel das in den Aufgabenbereich des Qualitätsmanagements, welches durch verschiedene Ansätze versuchte, die eigenen Prozesse dahingehend zu verbessern, dass mit möglichst wenig Aufwand eine möglichst große Wertschöpfung betrieben werden konnte. Zudem war diese Qualitätssicherung dafür verantwortlich, die Prozesse hinsichtlich der gängigen Normen und Standards auszurichten, da diese sowohl für die Qualität des Produktes bürgen, als auch die rechtliche Absicherung bei Haftungsfragen sind.

? **Ulrich Parthier:** *Wie wirkt sich die Digitalisierung darauf aus?*

Alexander Häußler: Wegen des zunehmenden Grades der Digitalisierung von Unternehmen hat sich nun ein Großteil aller Prozesse verändert. Viele sind nur noch digital verfügbar – fast alle greifen an irgendeinem Punkt auf digitale Infrastruktur zurück. Angetrieben werden diese neuen Prozesse besonders von einer Sache: Daten und Informationen auswerten. Informationen sind mittlerweile das höchste Gut innerhalb von Unternehmen geworden, wobei der Inhalt derselbigen von Kundendaten hin zu Produktinformationen reichen kann. Entsprechend wichtig ist es geworden, diese empfindlichen Informationen eines Unternehmens zu schützen, um finanzielle Schäden zu vermeiden und Firmengeheimnisse unter Verschluss zu halten. Die Qualität dieses Schutzes ist dabei nicht nur messbar, sondern kann sogar objektiv überprüft und zertifiziert werden – nach der Norm-Reihe ISO/IEC 2700x.

? **Ulrich Parthier:** *Ist Informationssicherheit auch Datenschutz?*

Alexander Häußler: Informationssicherheit ist nicht gleichbedeutend mit Datenschutz. Die Normenreihe ISO/IEC 2700x zu Informationssicherheit behandelt Daten aller Art gleich – ob personenbezogen oder nicht. Sie fordert beispielsweise in der ISO/IEC 27001 für den Schutz der Informationen die Implementierung eines Informationssicherheits-Managementsystems (Information Security Management System, ISMS) zur Sicherung der unternehmenseigenen IT-Struktur. Dabei handelt es sich um eine Aufstellung von Regelungen, Maßnahmen und Programmen, die innerhalb eines Unternehmens angewendet werden sollen.

? **Ulrich Parthier:** *Worauf kommt es bei Informationssicherheitsmanagement wirklich an?*

Alexander Häußler: Wichtig ist, dass dabei mehr als nur die verwendete Technologie und die digitale Infrastruktur eines Unternehmens betrachtet wird. Wie beim Qualitätsmanagement setzt auch ein

ISMS auf der Prozessebene an, um sein Ziel der Informationssicherheit im gesamten Unternehmen zu erreichen. Natürlich werden eingesetzte Technologien, Zugriffsrechte und Datenströme betrachtet – allerdings sind nicht alle schützenswerten IT-Informationen eines Unternehmens digitalisiert worden. Dennoch: Zugangsdaten von Mitarbeitern, Zahlen aus Unternehmensvorgängen oder schlicht die technische Dokumentation eines Unternehmens enthalten allesamt Informationen, die es im Rahmen der Planung und Einführung eines ISMS zu berücksichtigen gilt. Entsprechend mahnt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI), wie wichtig Informationssicherheit ist und aktualisiert regelmäßig die eigenen Empfehlungen und Richtlinien, wie die Maßnahmen für den IT-Grundschutz nach der BSI-Standard-Reihe 200x.

Ulrich Parthier: *Welche Risiken können abgesichert werden?*

Alexander Häußler: Welche Informationen wie geschützt werden müssen, bedarf einer Einschätzung vor der Einführung eines ISMS. Diese Einschätzung wiederum basiert auf der Art der Information und dem möglichen Schaden, sollte sie abhandenkommen – auch gängige Compliance-Regelungen spielen bei der Bewertung eine Rolle. Gleichzeitig gilt es, neben dem Schutz auch die Verfügbarkeit und Integrität der jeweiligen Informationen zu gewährleisten. Die Ergebnisse und die resultierenden Maßnahmen gilt es wiederum zu prüfen – schließlich müssen diese Maßnahmen den gewünschten Schutz garantieren. Dieser Vorgang wird wiederholt, bis der Prozess optimiert ist – wie früher im Rahmen einer Qualitätssicherung.

DIE WICHTIGSTE BINDUNG, DIE EIN UNTERNEHMEN ODER EINE MARKE ZUR KUNDSCHAFT UND DEN PARTNERN AUFBAUEN KANN, IST VERTRAUEN.

Alexander Häußler, Product Compliance Manager ISO/IEC 27001, TÜV SÜD Management Service, www.tuvsud.com

Ulrich Parthier: *Wie kann das im Unternehmen konkret umgesetzt werden?*

Alexander Häußler: Verantwortet wird das ISMS im Betrieb in der Regel von einem dedizierten Informationssicherheitsbeauftragten. Dieser muss fortan in die strategischen Entscheidungen der (IT-) Abteilungen eingebunden werden und dient als Ansprechpartner in Sachen der Datensicherheit, sowohl intern als auch für extern, etwa für Kunden oder Prüfer. Ihm obliegt es nicht nur, darauf zu achten, dass die Prozesse und Maßnahmen gemäß den Regelungen und Policies des ISMS eingehalten werden, sondern er ist darüber hinaus verantwortlich, das ISMS selbst im Auge zu behalten. Schließlich verändern sich die Anforderungen nicht nur im Zuge einer Integration neuer Systeme oder zusätzlicher technologischer Lösungen durch das Unternehmen, wie die erhöhte Einbindung von Cloud-Lösungen und -Strategien, sondern zusätzlich durch äußerliche Umstände, wie gesetzliche Rahmenbedingungen.

Ulrich Parthier: *Welche Vorteile bietet eine Zertifizierung?*

Alexander Häußler: Die wichtigste Bindung, die ein Unternehmen oder eine Marke zur Kundschaft und den Partnern aufbauen kann, ist Vertrauen. Ein Weg, der zu gesteigertem Vertrauen der Kunden in die Produkte oder Dienstleistungen führt, ist die Zertifizierung der Sicherheit dieser Produkte ab Werk. Sie belegt auch die Gewissenhaftigkeit, mit der ein Unternehmen arbeitet.

Ebenso verhält es sich bezüglich der Sicherheit und Absicherung von Informationen. Besonders Zulieferer werden von Konzernen oftmals aufgefordert, die eigenen Prozesse von unabhängigen Experten prüfen, gegebenenfalls verbessern und anschließend zertifizieren zu lassen. Die Zertifikate dienen hier als Versprechen, das ein bestimmter Standard oder eine bestimmte Normierung gewährleistet wird. Diese unterstreichen die Qualität der eigenen Arbeit, auf welche sich Kunden und Partner verlassen möchten. Es hat sich im Grunde nichts verändert: Früher gab ein Unternehmen das Qualitätsversprechen, dass seine Produkte nach anerkannten Normen produziert werden und nun ist es zusätzlich essenziell geworden, in digitaler Form die Sicherheit von Informationen zu versprechen, die im eigenen Unternehmen gespeichert und ausgewertet werden.

Außerdem mindert eine Zertifizierung durch unabhängige Prüfstellen das Risiko einer Schadenshaftung, denn wer nachweisen kann, sich an gängige Normen gehalten zu haben, hat ein solides Fundament in einem Rechtsstreit. Auf solch einem Fundament aufgebaut gerät zugleich das Vertrauen von Kunden und Partnern in ein Unternehmen nicht ins Wanken – was zu den wertvollsten Vermögenswerten jeder Firma gehört.

Ulrich Parthier: *Herr Häußler, wir danken für das Gespräch.*

VOM SÄBELZAHNTIGER ZUM HACKERANGRIFF

SCHON UNSERE VORFAHREN WUSSTEN: GUTES BCM IST KEIN ZUFALL!

Die Frage nach einem ordentlichen Business Continuity Management oder kurz „BCM" ist so alt wie die Menschheit selbst: „Was tun, wenn der Winter vor der Tür steht und ein hungriger Säbelzahntiger auf der Lauer liegt?" Man suche sich eine bequeme Höhle, lege rechtzeitig Vorräte an und rolle einen großen Stein in den Eingang – BCM at its best.

In der heutigen Zeit werden die Bedrohungen und notwendigen Maßnahmen der Notfallvorsorge zunehmend komplexer. Bei steigender Abhängigkeit von heterogenen technischen Systemen in einer hoch arbeitsteiligen Welt fällt es schwer, den Überblick zu behalten. Unvorhersehbare Entwicklungen wie die Ausweitung der Homeoffice-Nutzung in der Coronakrise schaffen neue Risiken. Organisationen, die sich mit dem Aufbau eines BCM auf den Ernstfall vorbereiten wollen, sollten mindestens diese Anforderungen stellen:

➤ Komplexe Sachverhalte auf ein handhabbares Maß reduzieren

➤ Vollzähligkeit und Vollumfänglichkeit der beschriebenen Maßnahmen gewährleisten

➤ Verfügbarkeit und Durchführbarkeit der Maßnahmen im Ernstfall sicherstellen und genaue Anweisungen für den Notfall bereithalten

➤ Kontinuierliche Verbesserung durch Tests, Übungen und Schulungen im PDCA-Zyklus

Komplexe Situationen lassen sich vereinfachen, indem der zu betrachtende Bereich so gewählt wird, dass er für das menschliche Beurteilungsvermögen überschaubar ist. Ist dies geschehen, werden alle unkritischen Prozesse aussortiert.

Schritt für Schritt zu mehr Sicherheit

Im nächsten Schritt müssen den komplexen Bedrohungen strukturierte Lösungen entgegengesetzt werden. Ob es dabei um eine kleine Gruppe Steinzeitmenschen oder einen multinationalen Konzern geht, spielt keine Rolle: Es darf kein kritischer Prozess übersehen werden und mit Risiken behaftet bleiben. Alle relevanten Prozesse müssen erfasst und entsprechend ihrer Risikoanfälligkeit mit Maßnahmen zur Minderung der Risiken bedacht werden. Der ordentlich versperrte Höhleneingang nutzte dem Steinzeitmenschen nichts, wenn ein zweiter Eingang ungesichert blieb.

In der Umsetzungsphase muss sichergestellt werden, dass alle vorgesehenen risikomindernden Maßnahmen auch real existieren, einsatzbereit sind und nicht an Unvorhergesehenem scheitern. Alle geplanten Maßnahmen müssen im Falle eines Vorfalls nachvollziehbar und verfügbar dokumentiert sein.

Im letzten Schritt der BCM-Einführung werden die Notfallmaßnahmen eingeübt und optimiert. Regelmäßige Tests, Übungen und Schulungen versetzen die betroffenen Mitarbeiter in die Lage, Lücken der vorherigen Planung zu erkennen und entsprechende Verbesserungen vorzunehmen, damit ihr BCM kontinuierlich an Reife gewinnt.

Fazit

In der heutigen Zeit helfen Rahmenwerke wie die ISO 22301:2019, der BSI-Standard 200-4 und die Good Practice Guidelines (GPG), die Anforderungen an ein BCM zu definieren und konkrete Umsetzungshilfen zu geben. Die derzeit am Markt verfügbaren Softwaretools sind noch sehr heterogen, die Integration in standardisierte Managementsysteme steht noch am Anfang. Nach Veröffentlichung des Community Drafts des BSI Standard 200-4 hat HiScout es sich zur Aufgabe gemacht, diese in der Software abzubilden und Synergie-Effekte zu anderen Managementsystemen zu schaffen.

Daniel Linder | www.hiscout.com

PASSWORD SAFE

AUF IN DIE PASSWORTLOSE ZUKUNFT

Mitarbeiter haben heutzutage unzählige geschäftliche Accounts, idealerweise mit komplexen, individuellen und regelmäßig wechselnden Login-Daten. Doch die Realität sieht anders aus: ein und dasselbe Passwort, immer wieder recycelt und mit Zahlen oder Sonderzeichen versehen. Sicher ist das nicht. Und so gehen noch immer 81 Prozent aller Datenschutzverletzungen auf angreifbare Credentials zurück.

IT- und Security-Verantwortliche suchen daher nach neuen Lösungen. Viele setzen ihre Hoffnungen in die aufkommenden biometrischen Angebote. Finger auflegen und los geht's – das klingt verlockend einfach. Was viele vergessen: Auch biometrische Daten sind fehleranfällig und können gehackt werden. Die Kosten der daraus folgenden Imageschäden sind in solchen Fällen kaum zu bemessen.

Deswegen kommen Unternehmen heute nicht mehr an einem Password Manager vorbei. Mit Password Safe von MATESO können Sie Ihre Passwörter sicher generieren, verwalten, teilen und archivieren – dank modernster Verschlüsselungstechnologie und innovativen Features. Das heißt: Passwortsicherheit für Ihre betrieblichen Geheimnisse, Passwortfreiheit für Ihre Mitarbeiter.

Passwortlose Anmeldung: ein passwortfreies Heute

Die passwortlose Anmeldung ist mit Password Safe längst Wirklichkeit. Sie können sich mithilfe von Smartcards oder FIDO-konformen Token einloggen und sicher auf all Ihre Anmeldedaten zugreifen – ohne sich ein einziges Passwort merken zu müssen. Natürlich bietet Password Safe auch die Möglichkeit, sich mit biometrischen Faktoren anzumelden, beispielsweise Touch ID für Mac oder Windows Hello für Windows.

Das ist nicht nur einfacher, sondern schließt auch eventuelle Sicherheitslücken auf Seiten der Endanwender, denn die Gefahr von Social Engineering Hacks wird auf diesem Weg reduziert. Admins und IT-Mitarbeiter können sich weiterhin besonders sicher mittels Master-Passwort einloggen – am besten im Rahmen einer Zwei-Faktor-Authentifizierung in Kombination mit einem Token oder einem biometrischen Faktor.

Single Sign-on: praktische Einmal-Anmeldung

Einmal angemeldet, öffnen sich die Türen zu den gespeicherten Anwendungen, die der User auch direkt aus Password Safe starten kann. Und dank der Browser-Erweiterung werden Passwörter für den Nutzer quasi unsichtbar: Das Programm erkennt automatisch, ob für eine Webseite Anmeldedaten hinterlegt sind, und weist den Nutzer darauf hin.

Password Safe agiert darüber hinaus als Identity Provider und kann mit jedem SAML-Service verknüpft werden. Das heißt, der Nutzer kann sich einfach über Password Safe identifizieren und erhält Zugriff auf Applikationen, ohne dass er seine Credentials speichern oder eintragen muss.

Password Sharing: geteiltes Passwort, doppelte Sicherheit

Es gibt auch immer wieder Situationen, in denen Mitarbeiter zwar Zugriff auf Anwendungen benötigen, aber die dazugehörigen Passwörter nicht einsehen sollen. Dafür bietet Password Safe ein rollenbasiertes Rechtesystem, in dem genau definiert ist, welcher User welches Passwort wie nutzen kann. Darüber hinaus können mittels Password Masking geteilte Passwörter mit einem Sichtschutz angelegt werden, sodass User sie zwar anwenden, aber nicht einsehen können.

Password Safe: für ein sicheres Morgen

Starten Sie mit Password Safe schon heute in die passwortlose Zukunft – zur Entlastung Ihrer Mitarbeiter und Ihrer IT. Denn gut gemanagte Passwörter sind der sicherste Weg, um Ihre Geheimnisse heute und auch morgen zu schützen.

www.passwordsafe.de

MATESO
PASSWORD SAFE

INFORMATIONS-SICHERHEITSMANAGEMENT

DAS HEUTIGE QUALITÄTSMANAGEMENT EINES UNTERNEHMENS

Daten sind das Gold des 21. Jahrhunderts. Umso wichtiger ist es, dass Unternehmen ihre sensiblen Informationen schützen, um finanzielle Schäden zu vermeiden und Firmengeheimnisse zu wahren. Hierbei spielt die Normen-Reihe ISO/IEC 2700x oder deren deutsche Entsprechung DIN EN ISO/IEC 2700x eine zunehmend wichtige Rolle. Darüber sprach Ulrich Parthier, Herausgeber it security, mit Alexander Häußler, Product Compliance Manager ISO/IEC 27001, TÜV SÜD Management Service.

? **Ulrich Parthier:** *Inwieweit entscheidet das Prozess- und Informationssicherheitsmanagement heute über den Erfolg von Unternehmen?*

Alexander Häußler: Ob von der Idee zum fertigen Produkt oder vom Quellcode zur finalen Anwendung – Unternehmen definieren sich über Prozesse. Diese Prozesse bilden die Nervenbahnen der Organisation und bestimmen, wann und wie Arbeitsschritte auszuführen sind. Entsprechend wichtig ist es, diese Prozesse soweit wie möglich zu optimieren. Früher fiel das in den Aufgabenbereich des Qualitätsmanagements, welches durch verschiedene Ansätze versuchte, die eigenen Prozesse dahingehend zu verbessern, dass mit möglichst wenig Aufwand eine möglichst große Wertschöpfung betrieben werden konnte. Zudem war diese Qualitätssicherung dafür verantwortlich, die Prozesse hinsichtlich der gängigen Normen und Standards auszurichten, da diese sowohl für die Qualität des Produktes bürgen, als auch die rechtliche Absicherung bei Haftungsfragen sind.

? **Ulrich Parthier:** *Wie wirkt sich die Digitalisierung darauf aus?*

Alexander Häußler: Wegen des zunehmenden Grades der Digitalisierung von Unternehmen hat sich nun ein Großteil aller Prozesse verändert. Viele sind nur noch digital verfügbar – fast alle greifen an irgendeinem Punkt auf digitale Infrastruktur zurück. Angetrieben werden diese neuen Prozesse besonders von einer Sache: Daten und Informationen auswerten. Informationen sind mittlerweile das höchste Gut innerhalb von Unternehmen geworden, wobei der Inhalt derselbigen von Kundendaten hin zu Produktinformationen reichen kann. Entsprechend wichtig ist es geworden, diese empfindlichen Informationen eines Unternehmens zu schützen, um finanzielle Schäden zu vermeiden und Firmengeheimnisse unter Verschluss zu halten. Die Qualität dieses Schutzes ist dabei nicht nur messbar, sondern kann sogar objektiv überprüft und zertifiziert werden – nach der Norm-Reihe ISO/IEC 2700x.

? **Ulrich Parthier:** *Ist Informationssicherheit auch Datenschutz?*

Alexander Häußler: Informationssicherheit ist nicht gleichbedeutend mit Datenschutz. Die Normenreihe ISO/IEC 2700x zu Informationssicherheit behandelt Daten aller Art gleich – ob personenbezogen oder nicht. Sie fordert beispielsweise in der ISO/IEC 27001 für den Schutz der Informationen die Implementierung eines Informationssicherheits-Managementsystems (Information Security Management System, ISMS) zur Sicherung der unternehmenseigenen IT-Struktur. Dabei handelt es sich um eine Aufstellung von Regelungen, Maßnahmen und Programmen, die innerhalb eines Unternehmens angewendet werden sollen.

? **Ulrich Parthier:** *Worauf kommt es bei Informationssicherheitsmanagement wirklich an?*

Alexander Häußler: Wichtig ist, dass dabei mehr als nur die verwendete Technologie und die digitale Infrastruktur eines Unternehmens betrachtet wird. Wie beim Qualitätsmanagement setzt auch ein

ISMS auf der Prozessebene an, um sein Ziel der Informationssicherheit im gesamten Unternehmen zu erreichen. Natürlich werden eingesetzte Technologien, Zugriffsrechte und Datenströme betrachtet – allerdings sind nicht alle schützenswerten IT-Informationen eines Unternehmens digitalisiert worden. Dennoch: Zugangsdaten von Mitarbeitern, Zahlen aus Unternehmensvorgängen oder schlicht die technische Dokumentation eines Unternehmens enthalten allesamt Informationen, die es im Rahmen der Planung und Einführung eines ISMS zu berücksichtigen gilt. Entsprechend mahnt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI), wie wichtig Informationssicherheit ist und aktualisiert regelmäßig die eigenen Empfehlungen und Richtlinien, wie die Maßnahmen für den IT-Grundschutz nach der BSI-Standard-Reihe 200x.

Ulrich Parthier: *Welche Risiken können abgesichert werden?*

Alexander Häußler: Welche Informationen wie geschützt werden müssen, bedarf einer Einschätzung vor der Einführung eines ISMS. Diese Einschätzung wiederum basiert auf der Art der Information und dem möglichen Schaden, sollte sie abhandenkommen – auch gängige Compliance-Regelungen spielen bei der Bewertung eine Rolle. Gleichzeitig gilt es, neben dem Schutz auch die Verfügbarkeit und Integrität der jeweiligen Informationen zu gewährleisten. Die Ergebnisse und die resultierenden Maßnahmen gilt es wiederum zu prüfen – schließlich müssen diese Maßnahmen den gewünschten Schutz garantieren. Dieser Vorgang wird wiederholt, bis der Prozess optimiert ist – wie früher im Rahmen einer Qualitätssicherung.

DIE WICHTIGSTE BINDUNG, DIE EIN UNTERNEHMEN ODER EINE MARKE ZUR KUNDSCHAFT UND DEN PARTNERN AUFBAUEN KANN, IST VERTRAUEN.

Alexander Häußler, Product Compliance Manager ISO/IEC 27001, TÜV SÜD Management Service, www.tuvsud.com

Ulrich Parthier: *Wie kann das im Unternehmen konkret umgesetzt werden?*

Alexander Häußler: Verantwortet wird das ISMS im Betrieb in der Regel von einem dedizierten Informationssicherheitsbeauftragten. Dieser muss fortan in die strategischen Entscheidungen der (IT-) Abteilungen eingebunden werden und dient als Ansprechpartner in Sachen der Datensicherheit, sowohl intern als auch für extern, etwa für Kunden oder Prüfer. Ihm obliegt es nicht nur, darauf zu achten, dass die Prozesse und Maßnahmen gemäß den Regelungen und Policies des ISMS eingehalten werden, sondern er ist darüber hinaus verantwortlich, das ISMS selbst im Auge zu behalten. Schließlich verändern sich die Anforderungen nicht nur im Zuge einer Integration neuer Systeme oder zusätzlicher technologischer Lösungen durch das Unternehmen, wie die erhöhte Einbindung von Cloud-Lösungen und -Strategien, sondern zusätzlich durch äußerliche Umstände, wie gesetzliche Rahmenbedingungen.

Ulrich Parthier: *Welche Vorteile bietet eine Zertifizierung?*

Alexander Häußler: Die wichtigste Bindung, die ein Unternehmen oder eine Marke zur Kundschaft und den Partnern aufbauen kann, ist Vertrauen. Ein Weg, der zu gesteigertem Vertrauen der Kunden in die Produkte oder Dienstleistungen führt, ist die Zertifizierung der Sicherheit dieser Produkte ab Werk. Sie belegt auch die Gewissenhaftigkeit, mit der ein Unternehmen arbeitet.

Ebenso verhält es sich bezüglich der Sicherheit und Absicherung von Informationen. Besonders Zulieferer werden von Konzernen oftmals aufgefordert, die eigenen Prozesse von unabhängigen Experten prüfen, gegebenenfalls verbessern und anschließend zertifizieren zu lassen. Die Zertifikate dienen hier als Versprechen, das ein bestimmter Standard oder eine bestimmte Normierung gewährleistet wird. Diese unterstreichen die Qualität der eigenen Arbeit, auf welche sich Kunden und Partner verlassen möchten. Es hat sich im Grunde nichts verändert: Früher gab ein Unternehmen das Qualitätsversprechen, dass seine Produkte nach anerkannten Normen produziert werden und nun ist es zusätzlich essenziell geworden, in digitaler Form die Sicherheit von Informationen zu versprechen, die im eigenen Unternehmen gespeichert und ausgewertet werden.

Außerdem mindert eine Zertifizierung durch unabhängige Prüfstellen das Risiko einer Schadenshaftung, denn wer nachweisen kann, sich an gängige Normen gehalten zu haben, hat ein solides Fundament in einem Rechtsstreit. Auf solch einem Fundament aufgebaut gerät zugleich das Vertrauen von Kunden und Partnern in ein Unternehmen nicht ins Wanken – was zu den wertvollsten Vermögenswerten jeder Firma gehört.

Ulrich Parthier: *Herr Häußler, wir danken für das Gespräch.*

VOM SÄBELZAHNTIGER ZUM HACKERANGRIFF

SCHON UNSERE VORFAHREN WUSSTEN: GUTES BCM IST KEIN ZUFALL!

Die Frage nach einem ordentlichen Business Continuity Management oder kurz „BCM" ist so alt wie die Menschheit selbst: „Was tun, wenn der Winter vor der Tür steht und ein hungriger Säbelzahntiger auf der Lauer liegt?" Man suche sich eine bequeme Höhle, lege rechtzeitig Vorräte an und rolle einen großen Stein in den Eingang – BCM at its best.

In der heutigen Zeit werden die Bedrohungen und notwendigen Maßnahmen der Notfallvorsorge zunehmend komplexer. Bei steigender Abhängigkeit von heterogenen technischen Systemen in einer hoch arbeitsteiligen Welt fällt es schwer, den Überblick zu behalten. Unvorhersehbare Entwicklungen wie die Ausweitung der Homeoffice-Nutzung in der Coronakrise schaffen neue Risiken. Organisationen, die sich mit dem Aufbau eines BCM auf den Ernstfall vorbereiten wollen, sollten mindestens diese Anforderungen stellen:

➤ Komplexe Sachverhalte auf ein handhabbares Maß reduzieren

➤ Vollzähligkeit und Vollumfänglichkeit der beschriebenen Maßnahmen gewährleisten

➤ Verfügbarkeit und Durchführbarkeit der Maßnahmen im Ernstfall sicherstellen und genaue Anweisungen für den Notfall bereithalten

➤ Kontinuierliche Verbesserung durch Tests, Übungen und Schulungen im PDCA-Zyklus

Komplexe Situationen lassen sich vereinfachen, indem der zu betrachtende Bereich so gewählt wird, dass er für das menschliche Beurteilungsvermögen überschaubar ist. Ist dies geschehen, werden alle unkritischen Prozesse aussortiert.

Schritt für Schritt zu mehr Sicherheit

Im nächsten Schritt müssen den komplexen Bedrohungen strukturierte Lösungen entgegengesetzt werden. Ob es dabei um eine kleine Gruppe Steinzeitmenschen oder einen multinationalen Konzern geht, spielt keine Rolle: Es darf kein kritischer Prozess übersehen werden und mit Risiken behaftet bleiben. Alle relevanten Prozesse müssen erfasst und entsprechend ihrer Risikoanfälligkeit mit Maßnahmen zur Minderung der Risiken bedacht werden. Der ordentlich versperrte Höhleneingang nutzte dem Steinzeitmenschen nichts, wenn ein zweiter Eingang ungesichert blieb.

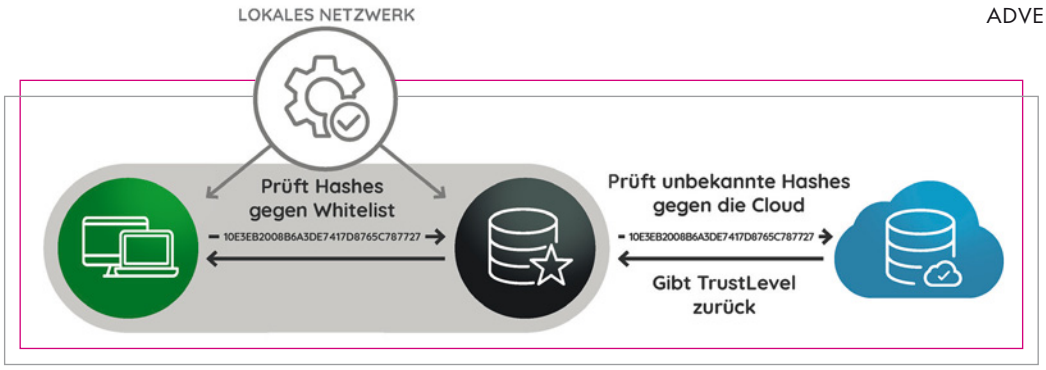
In der Umsetzungsphase muss sichergestellt werden, dass alle vorgesehenen risikomindernden Maßnahmen auch real existieren, einsatzbereit sind und nicht an Unvorhergesehenem scheitern. Alle geplanten Maßnahmen müssen im Falle eines Vorfalls nachvollziehbar und verfügbar dokumentiert sein.

Im letzten Schritt der BCM-Einführung werden die Notfallmaßnahmen eingeübt und optimiert. Regelmäßige Tests, Übungen und Schulungen versetzen die betroffenen Mitarbeiter in die Lage, Lücken der vorherigen Planung zu erkennen und entsprechende Verbesserungen vorzunehmen, damit ihr BCM kontinuierlich an Reife gewinnt.

Fazit

In der heutigen Zeit helfen Rahmenwerke wie die ISO 22301:2019, der BSI-Standard 200-4 und die Good Practice Guidelines (GPG), die Anforderungen an ein BCM zu definieren und konkrete Umsetzungshilfen zu geben. Die derzeit am Markt verfügbaren Softwaretools sind noch sehr heterogen, die Integration in standardisierte Managementsysteme steht noch am Anfang. Nach Veröffentlichung des Community Drafts des BSI Standard 200-4 hat HiScout es sich zur Aufgabe gemacht, diese in der Software abzubilden und Synergie-Effekte zu anderen Managementsystemen zu schaffen.

Daniel Linder | www.hiscout.com



Dank automatisierter Prüfung der Hashes gegen die von der SecuLution GmbH zentral gepflegte TrustLevel-Datenbank mit über 10 Millionen vertrauenswürdigen Hashes ersparen sich Admins den bei Whitelists sonst üblichen Aufwand.

PATENTIERTE ANTIVIRENLÖSUNG

IT-SECURITY MADE IN GERMANY MIT SCHRIFTLICHER GARANTIE

Whitelisting: Sobald IT-Experten diesen Begriff nur lesen, beginnt schon das Augenrollen. Wer will schon ständig eine Liste aller erlaubten Programme pflegen, und das womöglich in einem großen Unternehmen, in dem quasi täglich neue Probleme auf IT-Verantwortliche einprasseln?

Dabei ist, wie nationale Sicherheitsbehörden – darunter das BSI – seit Jahren betonen, Whitelisting dem Konkurrenzprinzip Blacklisting in puncto Sicherheit eindeutig vorzuziehen. Es müsste also eine Lösung her, die Whitelisting für Unternehmen nutzbar macht, indem der Aufwand auf ein absolutes Minimum reduziert wird.

Genau dieser Gedanke bewegte Torsten Valentin, Gründer und Geschäftsführer der SecuLution GmbH, als er vor über 20 Jahren SecuLution Application Whitelisting entwickelte. Das patentierte Automatisierungsverfahren (siehe Bild) sorgt für maximale Sicherheit. Das kontinuierlich weiterentwickelte System ist inzwischen so kugelsicher, dass SecuLution als einziger Antivirus-Anbieter den Schutz vor sämtlicher Schadsoftware schriftlich garantiert. Sogar vor den Folgen der verheerenden MS Exchange Server Hacks blieben SecuLution-Kunden verschont, ohne dafür irgendetwas tun zu müssen. SecuLution Application Whitelisting hat per Default Schutz geboten.

99 Prozent des Aufwands ausgelagert

Immer mehr Unternehmen vertrauen auf SecuLution und genießen den bestmöglichen Schutz vor Schadsoftware bei einem Aufwand, der mit klassischen Antivirusprodukten vergleichbar ist: Denn 99 Prozent des Aufwandes werden durch die Prüfung der Hashes in der TrustLevel-Datenbank ausgelagert!

Diesen Vorteil bestätigt etwa Bernhard Wiedemann, IT-Leiter des Landkreises Landshut. Seit 2016 nutzt die Kreisverwaltung SecuLution zur Absicherung von rund 700 Clients. „Die Appliance läuft praktisch von selbst", außerdem habe die Version 2.0 den administrativen Aufwand nochmals gesenkt. „Ich bin davon überzeugt, dass Application Whitelisting durch den Ansatz ‚Ich erlaube nur das, was ich kenne' einen deutlichen Sicherheitsvorteil bringt!"

Ralf Plomann, IT-Leiter des Krankenhausverbundes St. Rochus, setzt SecuLution bereits seit mehr als 15 Jahren bei vielen Hundert Clients ein. Er schätzt die Systemstabilität sowie die Option, die TrustLevel-Datenbank im Bedarfsfall mit vordefinierten Werten laden zu können: „Dies verschafft uns bei Personalengpässen eine größere Flexibilität. Der Betrieb einer komplexen IT-Infrastruktur ohne SecuLution ist für mich nur noch schwer vorstellbar."

Treue Kunden sprechen für den Erfolg

Auch in Industrieunternehmen findet SecuLution immer größere Verbreitung. Erleichtert zeigt sich etwa Jochen Pflesser, Fachleiter ITK-Infrastruktur/-Sicherheit bei BOGE Kompressoren: „Stellen Sie sich vor, dass Sie über Jahre hinweg Schmerzen haben, die täglich schlimmer werden. Eines Tages gibt Ihnen jemand eine Pille, die Sie einwerfen, und schon nach kurzer Zeit sind Sie dauerhaft von der Qual erlöst."

Übrigens: Als IT-Sicherheitsmaßnahme ist der Einsatz von SecuLution Application Whitelisting beispielsweise im Rahmen des Krankenhauszukunftsgesetzes oder des KMU-Programms „Digital Jetzt" förderfähig. Somit ist maximale Sicherheit mit minimalen Kosten erreichbar.

Kein Outsourcing

Viele IT-Fachkräfte schätzen auch, dass SecuLution Qualität Made in Germany bietet. Vom Firmensitz in Werl über den deutschsprachigen Support bis hin zum Frankfurter Rechenzentrum und den heimischen Softwarekomponenten – mit SecuLution erhalten Unternehmen und Verwaltungen zuverlässige Wertarbeit statt Outsourcing.

Mehr über seculution erfahren Sie hier: via Shortlink: 4ss.de/it-sec

seculution
application whitelisting
www.seculution.de, info@seculution.com,
Tel.: 0 29 22/95 89-2 10

CYBERSICHERHEIT 2021

HOMEOFFICE BLEIBT GEFÄHRDET

Durch die Corona-Pandemie haben sich neben Einkaufs- und Freizeitgewohnheiten die Arbeitsbedingungen stark verändert. Unternehmen, die es konnten, schickten ihre Mitarbeiter ins Homeoffice. Für ein Durchschnittsunternehmen bedeutete dies, dass es sein bestehendes Netzwerk und die Endpunktsicherheit für eine von 30 Prozent auf etwa 90 Prozent angewachsene Remote-Belegschaft aufstocken musste. Leider wurde bei der schnellen Einführung von Fernarbeitskapazitäten der Cybersicherheit nicht immer die höchste Priorität eingeräumt. Da auch zukünftig nicht alle Mitarbeiter wieder ins Büro zurückkehren werden, ist die hybride Systemumgebung ein bleibendes Faktum.

Daraus ergeben sich Gefahren, mit denen wir 2021 zu kämpfen haben. Mit dem Homeoffice-Boom haben sich nicht nur die Zahl der Angriffe, die sich das Thema Corona in Form von SPAM und Phishing als Aufmacher zu Nutze machten, erhöht, sondern sich neue Angriffsvarianten ausbreitet. War vor der Krise das Verhältnis von bekannten zu neuen Angriffen noch bei 80 Prozent zu 20 Prozent, so eroberten neue Angriffsvarianten (neues Phishing, Malware und -varianten) nun einen Anteil von 35 Prozent. Wir müssen auch davon ausgehen, dass Mitarbeiter zuhause unter weniger Aufsicht eher geneigt sind, Datendiebstahl oder Betrug zu begehen.

Neue Angriffsvarianten und Insider-Attacken lassen sich oft erst an ihrem Verhalten erkennen. Typische neue Angriffe, sogenannte dateilose Schadsoftware, zweckentfremden systemeigene, legitime Tools. Von Antivirenscannern werden diese Angriffe nicht erkannt. Dagegen hilft nur Applikationskontrolle und Beschränkung der Berechtigungen. Ein schadenfreies 2021 wird also nicht nur davon abhängen, ob sondern wie granular Cybermaßnahmen nachgezogen werden.

Anton Kreuzer | www.DriveLock.de

IT-Sicherheitsmanagement: Das umfassende Praxis-Handbuch; Thomas W. Harich, mitp-Verlag, 03-2021

IT-SICHERHEITS-MANAGEMENT

DAS UMFASSENDE PRAXIS-HANDBUCH

Daten werden in Public Clouds verlagert und dort verarbeitet, auf Mobiltelefonen gespeichert, über Chat-Apps geteilt oder im Rahmen von Industrie 4.0 in einer Größenordnung erfasst, die bislang kaum denkbar war. IT-Security-Manager müssen die entsprechenden Maßnahmen nicht nur an diese Veränderungen anpassen, sondern auch an die EU-Datenschutz-Grundverordnung, das IT-Sicherheitsgesetz, die Anforderungen von Kunden oder das China Cybersecurity Law. Alle diese Regelungen haben immense Auswirkungen darauf, wie Unternehmen Daten erfassen, verarbeiten, speichern oder austauschen dürfen.

Dieser Praxisleitfaden wird Ihnen anhand vieler konkreter Beispiele und Checklisten dabei helfen, sich in der riesigen Menge an Einzelthemen und Aufgaben zurechtzufinden. Das Buch eignet sich sowohl für den Berufseinstieg als auch als umfassendes Nachschlagewerk für IT-Profis bei der täglichen Arbeit.

MANAGED DETECTION AND RESPONSE

DER FAKTOR MENSCH IN DER PRÄVENTION UND ABWEHR VON CYBER-ATTACKEN

Solange menschliche Hacker ständig neue Angriffe kreieren, braucht es auch menschliche Verteidiger. Welche Rolle spielt der Faktor Mensch für eine intelligente Abwehr? Und was bietet Managed Detection and Response (MDR) als ausgelagerte zusätzliche Sicherheitskompetenz?

Vor dem Einkauf die Analyse

Viele Unternehmen suchen nach Abwehrlösungen, ohne zu wissen, was diese leisten sollen. Diese Reihenfolge ist falsch, denn hundertprozentigen Schutz bietet keine Software. Jedes Unternehmen hat eigenen Risiken und Lücken – je nach Branche, Geschäftsprozessen, eingesetzten Technologien und zu schützenden Daten. Wer nicht weiß, was er braucht, muss später in der Regel Software dazukaufen. Die Abwehr wird dadurch immer komplexer. Zunächst gilt es daher, den Ist-Status in Sachen Sicherheit intelligent zu analysieren und ein individuelles Risikoprofil zu erstellen. Schon hier spielt der Expertenrat eine wichtige Rolle.

Vorbeugende und anwendbare Intelligenz

Angesichts ständig sich ändernder neuer Gefahren muss die IT-Sicherheit zudem proaktiv und kontinuierlich nach Hinweisen auf stattfindende oder bevorstehende Angriffe suchen. Daten zu Unternehmensendpunkten und aus der Telemetrie liefern dem geschulten und erfahren Auge der Experten dafür umsetzbare Erkenntnisse. Unternehmen erhalten dadurch rechtzeitige Informationen. So bleibt Zeit zur Abwehr, bevor eine Attacke die Unternehmensprozesse behindert oder Daten gestohlen beziehungsweise verschlüsselt werden. Zum anderen erhalten die Verantwortlichen relevante branchenspezifische Daten zu Angriffen - etwa auf Wettbewerber. Diese Informationen unterstützen die Cyber-Abwehr taktisch und operativ: Indexwerte zeigen, wie stark Systeme kompromittiert sind und wo Angriffe unmittelbar bevorstehen.

Eine gute Defensive wächst zudem kontinuierlich und agiert langfristig. Sie kann abschätzen, wie sich die Gefahrenlage weiterentwickelt und baut die notwendigen Fähigkeiten auf, um Effekte zu minimieren. Geschulte und erfahrene Experten, die diese Daten interpretieren und ihren Rat geben, spielen eine unverzichtbare Rolle.

Denken wie ein Angreifer – Threat Hunting

Die externen Experten der MDR-Dienstleister sind zudem für die Abwehr komplexer Angriffe (Threat Hunting) unersetzlich. Die Analysten wissen unterstützt durch modernste EDR-Tools und dank ihrer Expertise sowie Intuition, wonach sie Ausschau halten müssen. Sie können in Echtzeit durchspielen, was der Angreifer als nächstes tun wird und wie man das verhindern kann.

Die meisten mittelständischen, aber auch viele große Organisationen verfügen weder über die Technologie noch über die Fachkräfte für das Threat Hunting. Erfahrene MDR-Teams in einem Security Operations Center wie von Bitdefender bieten jedoch für wenige Euro pro Monat und Endpunkt genau diesen menschlichen Faktor für die Abwehr aktueller und zukünftiger Gefahren.

Das Bitdefender MDR-Portfolio kombiniert führende Sicherheitstechnologien für Endpunkt-Detection, Sicherheits- und Netzwerkverkehranalyse mit der Kompetenz und Erfahrung hochqualifizierter Experten. Der Dienst bietet fortschrittliche Erkennung von Sicherheitsvorfällen mit einer schnellen Reaktion dank automatisierter, zuvor genehmigter Abwehrprozesse. So können die Experten zügig reagieren, den Effekt von erfolgten Angriffen abschwächen und diese abwehren. Die Analyse wird durch die Bitdefender-Telemetrie von 500 Millionen Endpunkten und proprietäre Techniken zur Erkennung von Bedrohungen unterstützt und mit kuratierten Informationen kombiniert.

www.bitdefender.de

Bitdefender

Weitere Informationen unter:
https://bit.ly/3wQdseo

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Michael Haas, Alexander Häußler, Anton Kreuzer, Daniel Linder, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Timo Schlüter, Andreas Schmid, Alexander Zachow

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

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

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

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

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

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

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

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

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

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

Erscheinungsweise:
10x pro Jahr

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

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

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

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

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

DREI JAHRE DSGVO

DIE FÜNF GRÖSSTEN FALLSTRICKE

Am 25. Mai 2018 trat die EU-Datenschutzgrundverordnung in Kraft. Viele Unternehmen haben auch nach knapp drei Jahren noch nicht ausreichend adäquate Maßnahmen getroffen, um Daten entsprechend der Vorgaben zu verarbeiten, zu speichern und zu löschen.

Bei der Umsetzung der DSGVO lauern fünf große Fallstricke:

➤ Interne Interessenskonflikte und mangelndes Verständnis. Die zentrale Aufgabe des Datenschutzbeauftragten ist es, die Einhaltung der DSGVO-Bestimmungen zu überwachen. In der Konsequenz müsste er sich also selber überwachen. Ein anderer Stolperstein sind fehlende Kenntnisse in puncto Daten-Compliance.

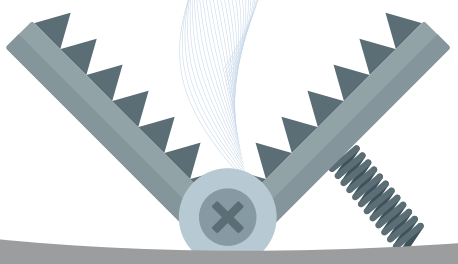
➤ Probleme bei der technischen und organisatorischen Umsetzung. Zu den zentralen Elementen der DSGVO gehören die Betroffenenrechte, darunter das Auskunftsrecht. Die Auskunft muss in verständlicher Form, präzise und transparent erfolgen sowie ein gängiges Datenformat haben.

➤ Korrekte Erstellung und Abnahme von Verträgen. Für die Verarbeitung von Daten liegt in der Regel eine sogenannte Auftragsverarbeitung (AV) vor, für die Unternehmen im Rahmen der DSGVO besondere Maßnahmen treffen müssen. Pflicht ist ein entsprechender AV-Vertrag, dessen Inhalt überwiegend vorgegeben ist.

➤ Design und Implementierung von TOMs. Technische und organisatorische Maßnahmen (TOM) umfassen alle in der Praxis getroffenen Vorkehrungen zur Gewährleistung der Sicherheit personenbezogener Daten. Die Implementierung angemessener TOMs stellt eine gesetzliche Anforderung dar und ist dokumentationspflichtig.

➤ Rechtliche Unklarheiten und fehlende Unterstützung. Erschwerend kommen für Unternehmen rechtliche Unklarheiten durch Änderungen seitens der Gesetzgebung und eine mangelnde Umsetzungshilfe durch die Aufsichtsbehörden hinzu.

https://de.nttdata.com



MULTI-CLOUD? ABER SICHER!

AUF MULTI-CLOUD-UMGEBUNGEN MIGRIEREN

Multi-Cloud-Strategien erfreuen sich nicht umsonst steigender Beliebtheit. Sie ermöglichen es Unternehmen, von den Funktionen und Innovationen unterschiedlicher Service-Provider zu profitieren und zugleich eine höhere Ausfallsicherheit zu gewährleisten. Aber wie sieht es mit der Datensicherheit aus? Welche Aspekte verlangen bei einer Multi-Cloud-Infrastruktur besondere Beachtung?

Geteilte Verantwortung

Im wachsenden Markt für Cloud Services ist Sicherheit ein zentrales Kriterium. Die größten Cloud Service Provider (CSPs) setzen Verschlüsselungstechnologien ein, welche die Daten in Cloud-Workloads und -Speichern schützen und sie für Angreifer wertlos machen. Vorausgesetzt natürlich, die Angreifer haben keinen Zugriff auf die kryptografischen Schlüssel. Zu beachten ist jedoch, dass die CSPs den für die Verschlüsselung verwendeten Schlüssel zumeist behalten. So könnten Dateien jederzeit entschlüsselt werden, wenn zum Beispiel berechtigtes Interesse bei Behörden besteht.

Es ist außerdem wichtig zu wissen, dass CSPs im Rahmen des branchenweit üblichen Modells der geteilten Verantwortung nur für die von ihnen angebotene Infrastruktur und den Servicevertrag verantwortlich sind. Den Vertragspartnern auf Unternehmensseite wiederum fällt die Verantwortung für die Sicherheit ihrer Daten und die Privatsphäre ihrer Kunden zu.

Da jeder CSP eigene Tools zur Verschlüsselung und Schlüsselverwaltung einsetzt, sehen sich Unternehmen mit Multi-Cloud-Implementierungen mit einer Vielzahl verschiedener Verschlüsselungs- und Schlüsselverwaltungsfunktionen konfrontiert.

Mehr Kontrolle

Um Unternehmen mit Multi-Cloud-Infrastrukturen mehr Kontrolle über ihre Schlüssel und Daten zu ermöglichen, sollten geschäftskritische Daten bereits vor dem Upload in die Cloud verschlüsselt werden. So sind sie während des Transfers und in der Cloud vor unbefugten Zugriffen geschützt. Eine weitere Möglichkeit ist die Verschlüsselung von Datensicherungs-Workloads innerhalb von Cloud-native-Applikationen. Mit formaterhaltender Verschlüsselung, formaterhaltendem Hashing sowie zustandsloser Tokenisierung kann sichergestellt werden, dass chiffrierte Daten ihr Format beibehalten und für ihre Nutzung keine Änderungen erforderlich sind.

Sichere Schlüsselverwaltung

Da die Sicherheit von Daten in der Cloud auf kryptografischen Schlüsseln basiert, ist deren Verwaltung über den gesamten Lebenszyklus hinweg von entscheidender Bedeutung. Hier kommen Hardware-Sicherheitsmodule (HSMs) ins Spiel: Zertifiziert nach FIPS 140-2 Level 3 und Common Criteria EAL4+, garantieren HSMs die sichere Generierung und Codeausführung, den Schutz und die Zugriffskontrolle für kryptografische Schlüssel in einer gehärteten, hardwarebasierten Appliance – und schaffen so eine starke Vertrauensbasis für die Sicherheit geschäftskritischer Anwendungen und Daten in der Cloud. Entrust bietet HSMs auch als einfach skalierbares und flexibles Service-Modell an: nShield as a Service ermöglicht es Unternehmen, Kryptografie und Schlüsselverwaltung über mehrere Clouds hinweg auszudehnen. Die HSMs können jederzeit ergänzt oder ersetzt werden, was die Budgetierung geschäftskritischer Sicherheit vereinfacht, während der Zeitaufwand für Wartung und Kontrolle sinkt. So lassen sich Anforderungen an die Sicherheit und die Einhaltung gesetzlicher Vorschriften mit hoher Wirtschaftlichkeit in Einklang bringen.

Sicherheitsbewusst migrieren

Die Migration in eine Multi-Cloud-Umgebung bringt spezielle Anforderungen in punkto Datensicherheit, Verschlüsselung und Schlüsselverwaltung mit sich. Mit der richtigen Security-Strategie und fortschrittlichen Tools können Organisationen vollumfänglich von der Flexibilität und den finanziellen Vorteilen verschiedener Cloud-Dienste profitieren und so das Beste aus ihrer Cloud-Umgebung herausholen.

www.entrust.com

PRÄVENTIVE MASSNAHMEN

DDOS-ANGRIFFE NEHMEN SEIT BEGINN DER CORONA-PANDEMIE ZU

Nie zuvor war das Risiko eines Distributed-Denial-of-Service-Angriffs (DDoS) höher. Bei DDoS-Angriffen überhäufen Hacker Webserver mit Anfragen aus dem Internet, damit diese unter der Vielzahl der Aufrufe zusammenbrechen. Doch es gibt geeignete Gegenmaßnahmen.

Das Jahr 2020 verzeichnete einige rekordverdächtige DDoS-Angriffe, die teils tausende von Unternehmen betrafen. Dazu gehörten Angriffe wie die des „Fancy Bear" genannten Kollektivs, das DDoS-Attacken nutzte, um Unternehmen zu erpressen und hohe Bitcoin-Forderungen zu stellen. Außerdem verzeichnete Akamai seit Beginn des vorigen Jahres deutlich mehr Angriffe und Notabschaltungen von Kundensystemen als je zuvor. Dabei waren auch viele Branchen stark betroffen, die zuletzt weniger unter Cyberkriminellen zu leiden hatten.

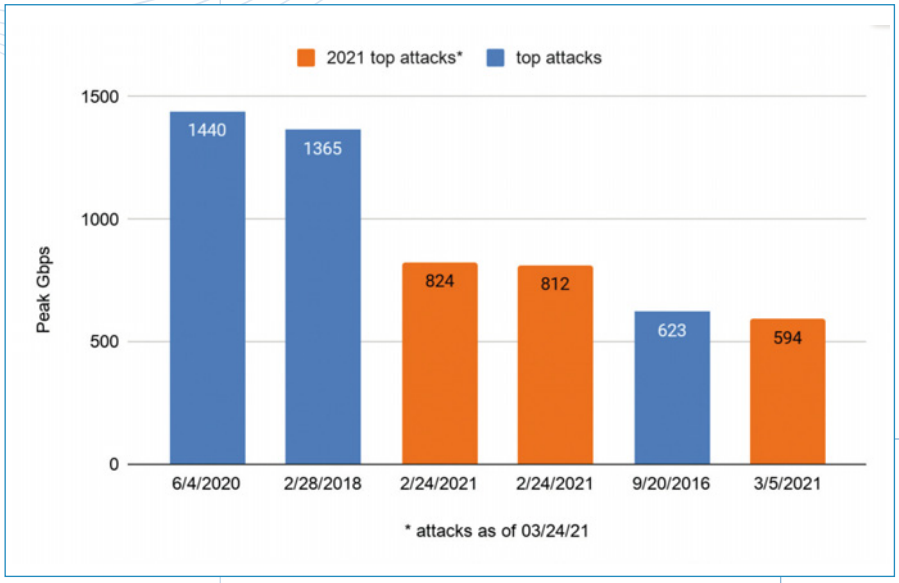
Viele Experten sprachen dabei von einer Renaissance der DDoS-Angriffe und suchten nach den Hintergründen der neuen Angriffswelle. Ein Teil der Antwort ist die Verbesserung der Tools, die Angreifern zur Verfügung stehen und die die Einstiegshürde für hochvolumige und komplexe DDoS-Angriffe gesenkt haben – perfekte Voraussetzungen für die größte Angriffswelle seit 2016. Politisch motivierte DDoS-Angriffe sind dabei zuletzt zwar nicht verschwunden, spielen aktuell aber eine eher untergeordnete Rolle.

DDoS-Angriffe werden immer größer

Mit dem Beginn der COVID-19-Pandemie stiegen sehr große Angriffe (über 100 Gbit/s) dramatisch an. Alternativ (oder in Kombination) überlasten Kriminelle mit einer hohen Anzahl von Datenpaketen Netzwerkgeräte wie Router und Load-Balancer sowie Anwendungen in Rechenzentren. Da sich Unternehmen aller Branchen an Remote-Arbeit und die zunehmende Abhängigkeit von Internetkonnektivität anpassen mussten und sich mehr auf den Schutz von VPNs und Kommunikationsendpunkten als auf „allgemeine" Rechenzentren konzentrierten, wurden sie immer mehr zu einem attraktiven und lukrativen Ziel für DDoS-Aktivitäten.

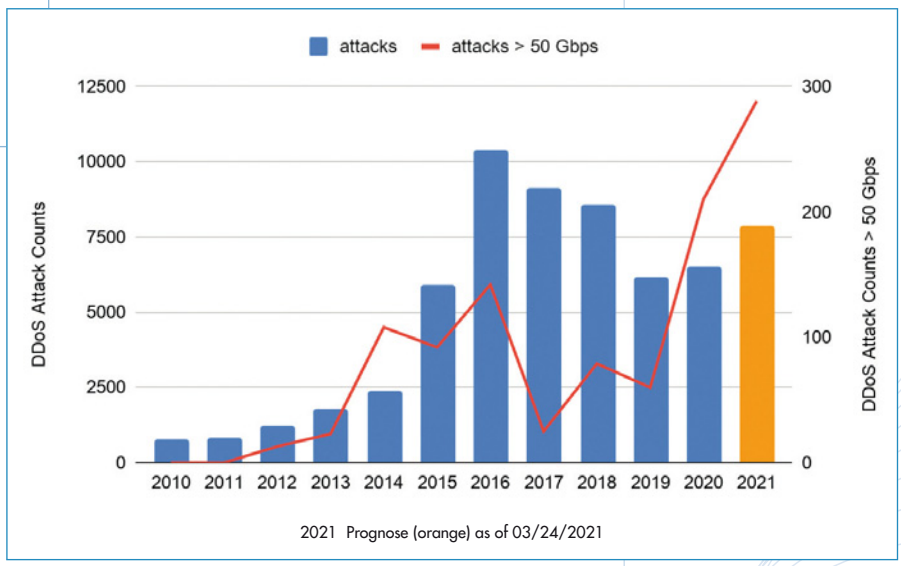
Im Juni 2020 erfolgten sogar rekordverdächtige 1,44 Tbps- und 809 Mpps-Angriffe (DDoS-Attacken in Millionen Paketen pro Sekunde (Mpps)) gegen eine große europäische Bank und ein Internet-Hosting-Unternehmen. Der massive Tbps-Angriff war zudem hoch komplex und umfasste neun verschiedene Angriffsvektoren und mehrere Botnet-Angriffstools. 65 Prozent der DDoS-Angriffe waren Multi-Vektor-Attacken; bei einem Angriff kamen 14 verschiedene DDoS-Vektoren zum Einsatz.

Die Angreifer bedrohten die betroffenen Unternehmen zielgerichtet und betonten, dass sie Schwachstellen in der dem Internet zugewandten Infrastruktur aufgedeckt und Hostnamen und IPs von geschäftskritischen beziehungsweise umsatzrelevanten Anwendungen identifiziert hatten. Diese würden sie offline nehmen, sollten ihre Bitcoin-Erpressungsforderungen nicht erfüllt werden. Mehrfach wurden dabei Unternehmen wiederholt Opfer von Attacken und Erpressungsversuchen, denn bezahlte Forderungen verursachen häufig erneute Forderungen. Die Zahl der Angriffe größer als 50 Gbps stiegen vor allem in folgenden Branchen sprunghaft an: Business Services (960 %), Bildung (180 %), Finanzdienstleistungen (190 %), Einzelhandel & Konsumgüter (445 %) und Software &



Top DDoS Gbps aufgezeichnete/mitigierte Angriffe.

DDoS-Angriffe und Prognosen nach Jahren.
Balken = DDoS-Angriffe,
rote Linie = Angriffe über 50 Gbps.



Technologie (196 %). Es ist davon auszugehen, dass auch im Jahr 2021 die Menge und Größe der DDoS-Attacken weiter zunehmen werden.

Effektiver Schutz gegen DDoS-Angriffe

Ein DDoS-Angriff ist keine Naturgewalt, dem ein Unternehmen machtlos ausgesetzt ist. Aber er erfordert konsequentes Handeln – vor allem vor dem Angriff. Die folgenden Empfehlungen helfen, einen wirksamen Schutz gegen DDoS-Angriffe aufzubauen.

1. Wer den „normalen" Datenverkehr im Unternehmen kennt und Tools zur Netzwerk- und Anwendungsüberwachung nutzt, der entdeckt leichter ungewöhnliche Aktivitäten, die möglicherweise auf einen DDoS-Angriff hindeuten.

2. Unternehmen sollten sicherstellen, dass das Risiko in Übereinstimmung mit den strategischen Modellen zum Management von Informationsrisiken analysiert wird. Außerdem sollten die Prioritäten für die DDoS-Abwehr und die Wiederherstellung von Diensten in aussagekräftigen Kennzahlen wie „entgangenem Umsatz" des Unternehmens festgelegt werden.

3. DDoS-Angriffe können für das Unternehmen genauso verheerend sein wie eine Naturkatastrophe und sollten ein integraler Bestandteil der ausgearbeiteten Notfallpläne des Unternehmens werden.

4. Eine starke DDoS-Abwehrstrategie beginnt mit einer soliden Online-Hygiene. Die Unternehmenskultur sollte sicherheitsorientiert sein. Zudem sollten Entwickler und Systemadministratoren die Best Practices der Branche für Cybersicherheit befolgen.

5. Unternehmen benötigen die richtige Kombination aus Experten-Engagement, Automatisierung und definierten Prozessen, um Angreifern immer einen Schritt voraus zu sein und sich gegen immer raffiniertere, sich ständig weiterentwickelnde Angriffe zu verteidigen.

6. Die Implementierung eines Zero-Trust-Sicherheitsmodells ist ratsam. Das Modell trägt zum Schutz vor DDoS-Angriffen bei, indem es den Zugriff mit den wenigsten Privilegierten erzwingt und sicherstellt, dass nur autorisierte Benutzer Zugriff auf kritische Anwendungen und Dienste erhalten.

7. Auch die Upstream-Provider sind ein wichtiger Faktor, um sich auf Risiken vorzubereiten und diese zu adressieren – gemeinsam mit ihnen sollten DDoS-Risiken bewertet und Bereitschafts- und Wiederherstellungspläne entwickelt werden. Mit dem richtigen Mitigation-Partner und den passenden Sicherheitskontrollen haben Angreifer in der Regel keine Chance. So werden fast alle DDoS-Angriffe entschärft, nur ein kleiner Prozentsatz erforderte eine aktive Mitigation.

8. Testen, erneut testen, dokumentieren und messen. Penetrationstests sollten DDoS-Angriffe integrieren. Denn die Simulation komplexer Angriffe ermöglichen Unternehmen, Schwachstellen zu identifizieren und die Abwehrkräfte zu stärken.

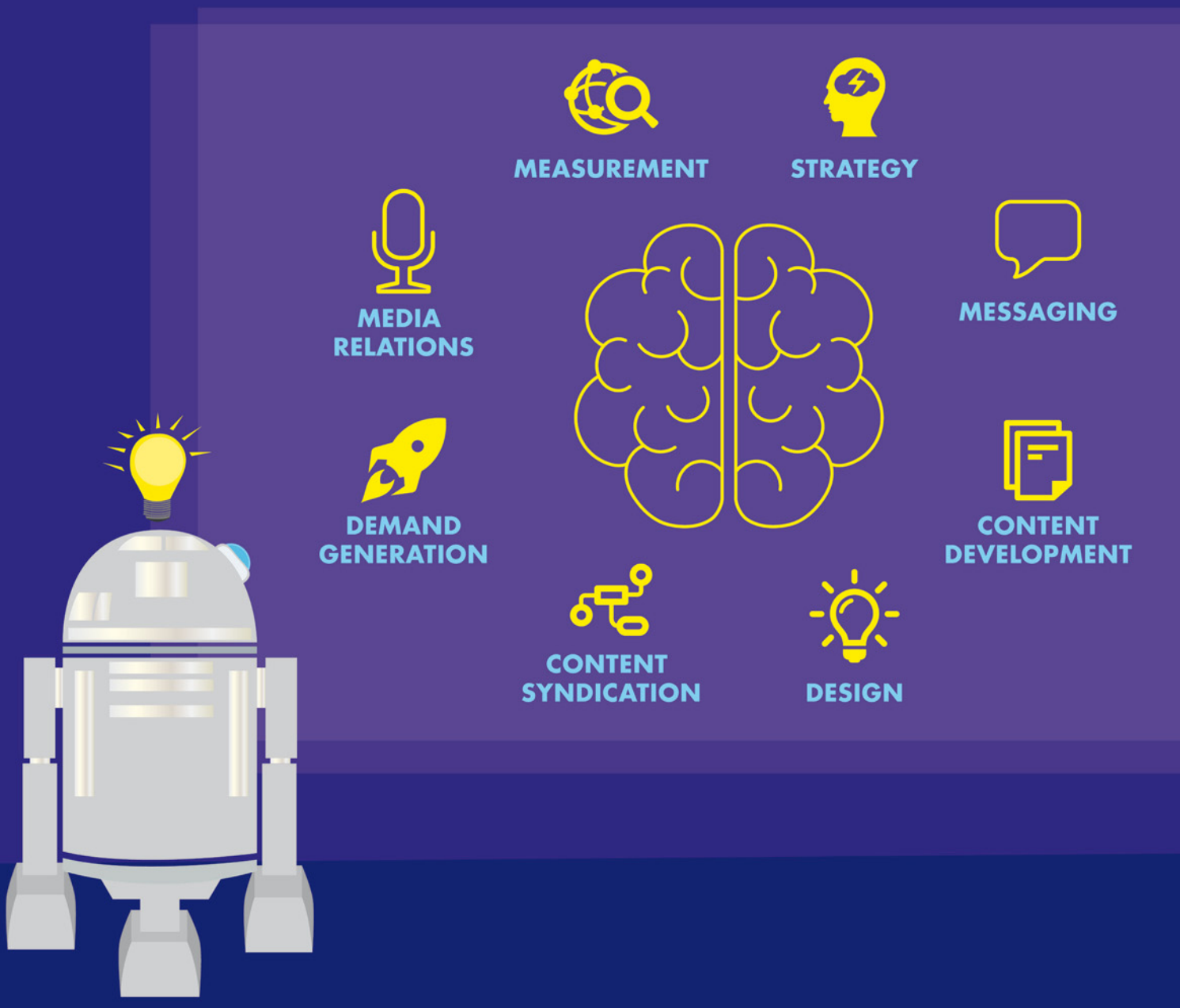
9. Im Falle eines DDoS-Angriffs sollten Unternehmen Kernbereiche und geschäftskritische Dienste schnell wiederherstellen können.

10. Bei der Reaktion auf einen DDoS-Angriff ist Zeit das A und O. Das Sicherheitsteam sollte die Möglichkeit bekommen, schnell Abwehrmaßnahmen zu ergreifen, ohne dass eine Kette von Kontrollinstanzen und Genehmigungen notwendig ist.

11. Und zu guter Letzt: Lösegeld- oder Erpressungszahlungen sollten niemals geleistet werden. Denn es gibt keine Garantie, dass der Angreifer seine Drohungen wahr macht oder dass die Zahlung einen DDoS-Angriff verhindern würde. Bedrohungsakteure versuchen oft, aus der „Angst vor dem Unbekannten" Kapital zu schlagen, um schnell Geld zu verdienen, bevor sie zum nächsten Ziel weiterziehen.

Alexander Zachow | www.akamai.com

Thought Leadership



KÜNSTLICHE INTELLIGENZ
THOUGHT LEADERSHIP

Die neue Dimension des IT-Wissens.

Jetzt neu **www.it-daily.net**

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