itmanagement

MÄRZ 2021

INKLUSIVE 24 SEITEN
IT SECURITY

PROJEKT-MANAGEMENT

Hybride Methoden

NEW WORK

Was muss die IT leisten?

IT-SERVICE-MANAGEMENT

KI-BASIERTE AUTOMATISIERUNG

Peter Machat, Ivanti

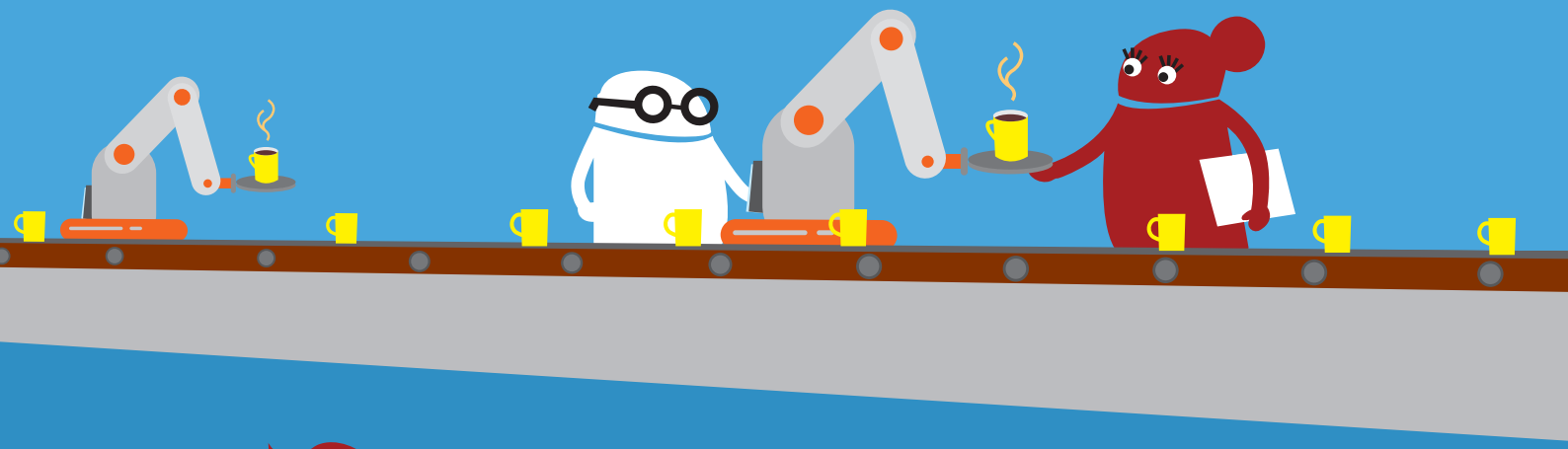
www.it-daily.net

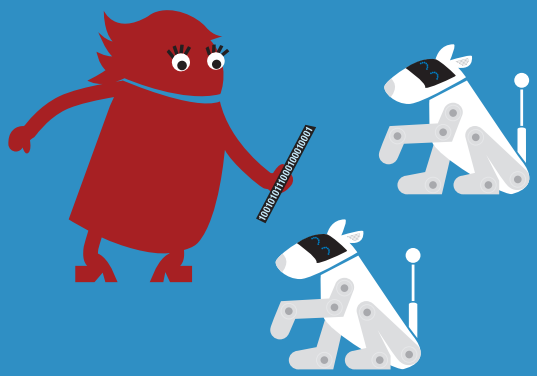
itmanagement

Roadmap für die IT-Zukunft

IT Management Digitalevent

28.04.2021





#itmanagementroad21

Jetzt anmelden

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

VERTRAUEN IST GUT, DIE RICHTIGE SOFTWARE IST BESSER

Einer aktuellen Studie des Bitkom zufolge, erhöht sich das Vertrauen in die Internetsicherheit jedes Jahr mehr!! Ich dachte, ich les nicht richtig!

Wieso erhöht sich das Vertrauen? Gehöre ich einfach zu einer Generation, die der Datensicherheit im Internet schon immer kritisch gegenübergestanden hat? Vielleicht ist es auch einfach berufsbedingt, aber diese Aussage/dieses Ergebnis irritiert mich sehr.

Laut der Studie finden drei von zehn Internetnutzern, dass ihre persönlichen Daten im Internet sicher sind – gut, drei von zehn klingt erst mal nicht viel, aber das macht immerhin 30 Prozent aus. Dass Unternehmen ihre Daten im Internet als sicher erachten, ist die eine Sache - sie nutzen, sollten sie jedenfalls, weitaus innovativere Sicherheitsmaßnahmen, die regelmäßig geupdatet, gepatcht und an die jeweiligen Gegebenheiten angepasst werden. Und selbst dann, erachten sie ihre Daten wahrscheinlich nicht als zu 100 Prozent sicher.

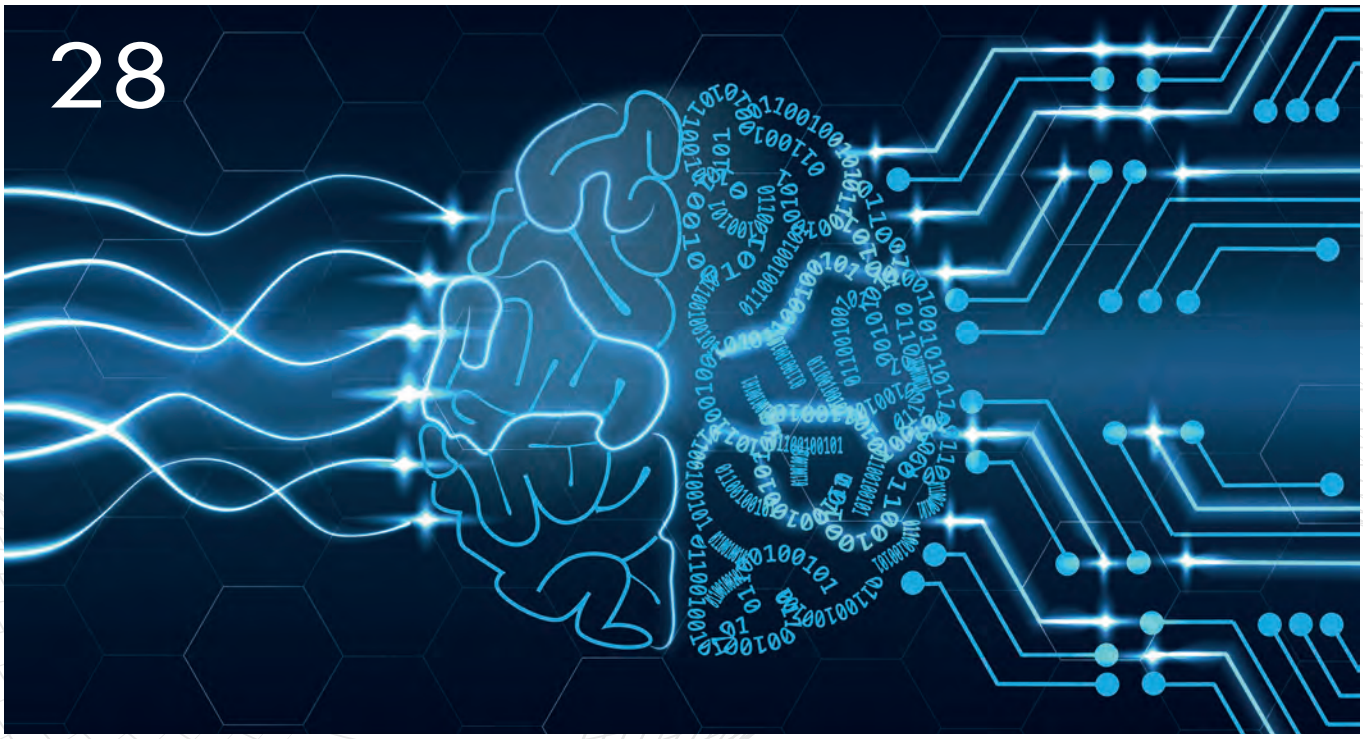
Aber der normal sterbliche Internetuser, der berufsbedingt nichts mit IT zu tun hat? Der hat im Regelfall eine Firewall und einen Antivirenscanner auf seinem internetfähigen Gerät. That's it! DDos-Angriffe, Phishing, Ransomware-Attacken betreffen nur Regierungen und große Unternehmen, mich nicht?

Ohne ein bisschen Vertrauen in mittlerweile alltägliche Dinge, wie eben das Internet, macht man sich das Leben schwer, aber dass ich mir sicher bin, dass meine privaten Daten im www sicher sind, davon bin ich noch weit entfernt. (An dieser Stelle einen schönen Gruß an meine Kollegin, die sich schlapp gelacht hat, weil ich nun doch WhatsApp-Nutzer geworden bin!)

Nicht ohne Grund erreichen uns in der Redaktion jeden Tag Securityfachbeiträge und werden neue, innovativere Lösungen gegen Cybercrime vorgestellt, die wir gern an Sie weiterreichen.

Entscheiden Sie. Vertrauen Sie?

Carina Mitzschke | Redakteurin it management



INHALT

Inklusive 24 Seiten

IT SECURITY SPEZIAL

IT INFRASTRUKTUR

DIGITALISIERUNG

COVID 19: BESCHLEUNIGER ODER AUSBREMSER?

Zu Beginn der Pandemie waren sich Experten schnell einig, dass die Maßnahmen zur Bekämpfung der Coronavirus-Pandemie einen offensichtlichen Nebeneffekt haben würden: die Beschleunigung der Digitalisierung. Neun Monate später zeigt eine aktuelle Umfrage ein differenzierteres Bild, denn die Mehrheit der KMU-Inhaber und -Geschäftsführer sagt, dass Covid-19 die Digitalisierung ihres Unternehmens nicht beschleunigt hat.

Fehlendes Budget oder ein ausreichender Digitalisierungsgrad vor dem Ausbruch der Krise sind die beiden Hauptgründe, warum etliche KMUs keine Beschleunigung der Integration digitaler Technologien in ihre Geschäftprozesse gesehen haben.

Die Umfrage zeigt eine klare Korrelation zwischen der Zufriedenheit von KMU-Inhabern mit öffentlichen Hilfen für digitale Innovationen und ihrer allgemeinen Digitalisierung. Dies bestätigt den wichtigen Einfluss von Regierungen darauf, dass europäische KMUs mit den Anforderungen des Marktes Schritt halten können.

ERGEBNISSE FÜR DEUTSCHLAND

47 %
Pandemie hat die Digitalisierung beschleunigt

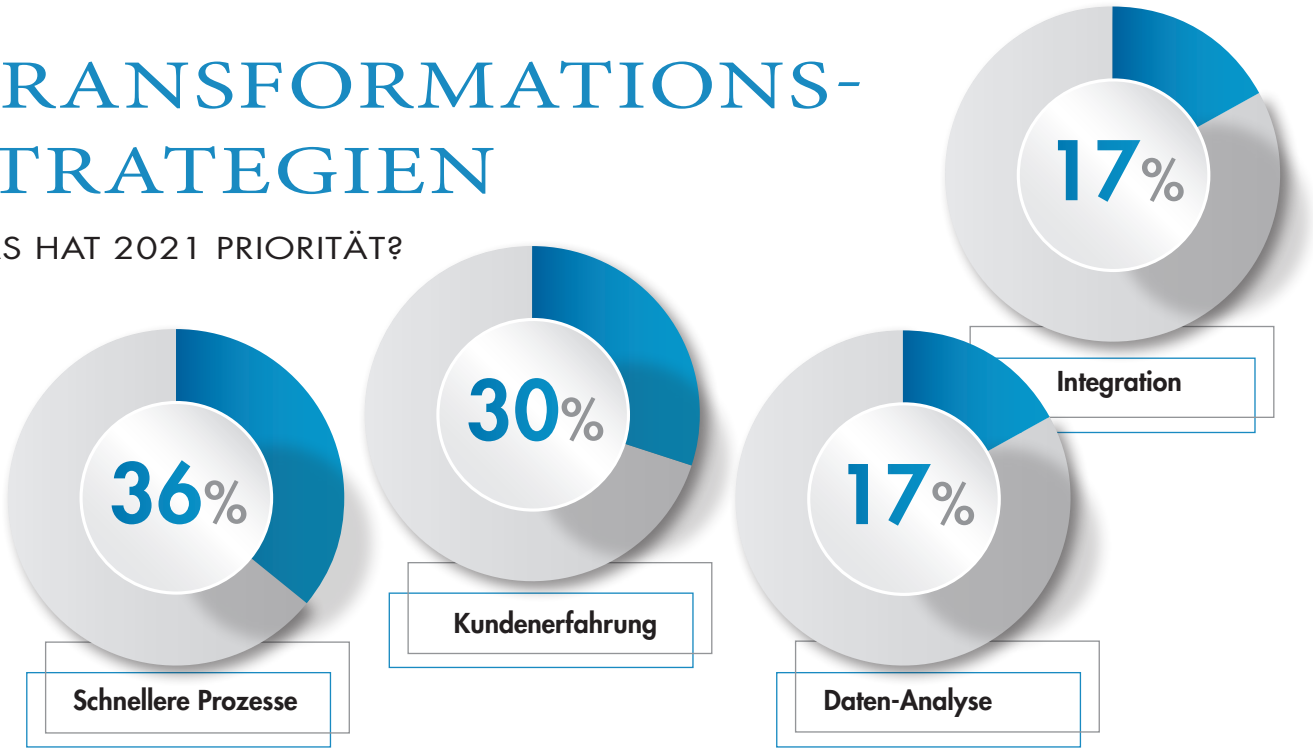
28 %
Pandemie hat Digitalisierung verlangsamt

23 %
es gab keinerlei Veränderungen

www.sortlist.com

TRANSFORMATIONS-STRATEGIEN

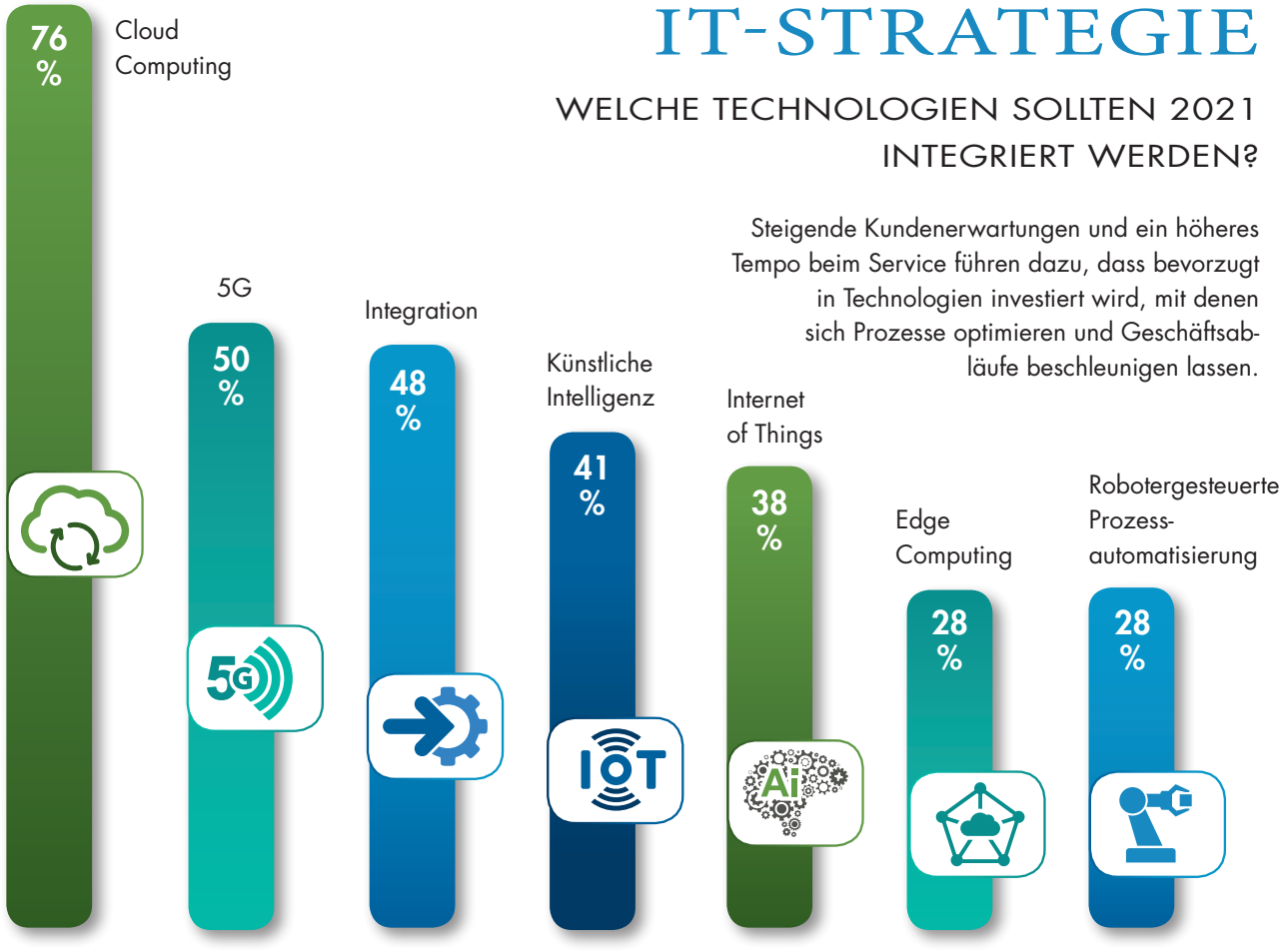
WAS HAT 2021 PRIORITÄT?



IT-STRATEGIE

WELCHE TECHNOLOGIEN SOLLTEN 2021 INTEGRIERT WERDEN?

Steigende Kundenerwartungen und ein höheres Tempo beim Service führen dazu, dass bevorzugt in Technologien investiert wird, mit denen sich Prozesse optimieren und Geschäftsabläufe beschleunigen lassen.



(Quelle: Software AG, 2021 Situation Report)

IT-TRENDS

WOHIN GEHT DIE REISE?

Das Analystenhaus PAC und die teknowlogy Group erwarten für 2021 eine deutliche Erholung der Gesamtsituation, ausgehend von einem niedrigen Vergleichsniveau. Wobei die Wachstumsthemen mehr oder weniger die Gleichen geblieben sind. Die folgenden IT-Trends werden voraussichtlich den stärksten Einfluss auf den IT-Markt haben:

1. **Automatisierte SOCs**
2. **Automatisierung in der Smart Factory**
3. **KI-getriebene Customer Experience**
4. **Massenmigration in die Public Cloud**
5. **Mitarbeiterorientierter neuer Arbeitsstil und digitaler Arbeitsplatz**
6. **Nachhaltigkeit und Dekarbonisierung**
7. **Neuausrichtung der Lieferketten**
8. **Secure Access Service Edge (SASE)**
9. **Transformational Outsourcing der nächsten Generation**
10. **Unternehmensanwendungen in der Public Cloud**

www.teknowlogy.com

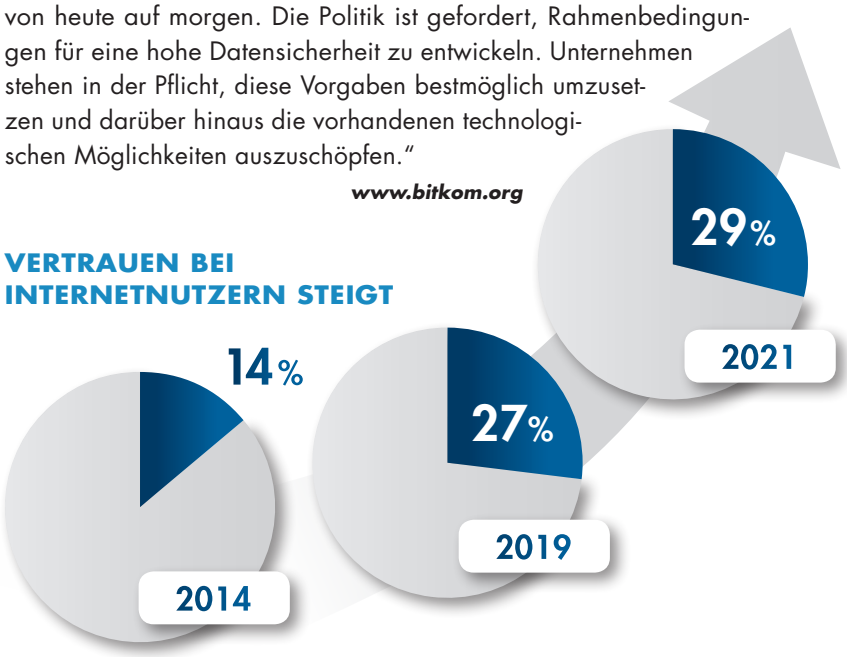
DATEN-SICHERHEIT IM INTERNET

ALLMÄHLICH STEIGT DAS VERTRAUEN

Das Vertrauen in die Datensicherheit im Internet erholt sich mit jedem Jahr mehr. Drei von zehn Internetnutzern finden, dass ihre persönlichen Daten im Internet sicher sind. Im Jahr 2019 gaben dies 27 Prozent an, 2014 lag der Wert bei gerade einmal 14 Prozent. Zwei Drittel der Onliner finden aber weiterhin, dass ihre persönlichen Daten im Internet nicht sicher sind. Das ist das Ergebnis einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitkom in Deutschland. „Nach dem Bekanntwerden der NSA-Affäre im Jahr 2013 war das Nutzervertrauen in Datensicherheit erschüttert", sagt Bitkom-Präsident Achim Berg. „Verlorenes Vertrauen zurückzugewinnen gelingt nicht von heute auf morgen. Die Politik ist gefordert, Rahmenbedingungen für eine hohe Datensicherheit zu entwickeln. Unternehmen stehen in der Pflicht, diese Vorgaben bestmöglich umzusetzen und darüber hinaus die vorhandenen technologischen Möglichkeiten auszuschöpfen."

www.bitkom.org

VERTRAUEN BEI INTERNETNUTZERN STEIGT



BLACKBOX REMOTE WORKING

DIGITAL EMPLOYEE EXPERIENCE

Was in vielen Unternehmen als ein eher zukunftsorientierter Prozess schwelte, wurde zu einer akuten Anforderung katapultiert: Auf breiter Basis eine funktionierende „Work-from-Anywhere" Arbeitsumgebung zu schaffen und zu betreiben.

So ist die Qualität örtlich flexibler, digitaler Arbeitsplätze zur Top-Priorität in Unternehmen geworden. Noch im Mai 2019 wurde das Thema „Digital Employee Experience" (DEX) von immerhin 49 Prozent international befragter Unternehmen als essenziell betrachtet. Ein Jahr später rückte es schon mit 78 Prozent auf der Prioritätenliste nach oben, im Oktober 2020 gaben bereits 96 Prozent dem Thema höchste Bedeutung für ihr Unternehmen.

Trotz aller Brisanz können die meisten Unternehmen aber nur vage einschätzen, wie es ihren Mitarbeitern mit dem digitalen Arbeitsplatz ergeht. Denn 46 Prozent messen dies gar nicht, 34 Prozent versuchen mit manuellen Methoden eine Einschätzung der digitalen Arbeitsplatzqualität zu erlangen, lediglich 19 Prozent haben dafür ausgewiesene, automatisierte Verfahren.

www.nexthink.com

DIES WIRKT SICH NEGATIV AUF DIE MITARBEITER AUS

45%
der IT-Probleme werden von den Mitarbeitern nie gemeldet

Mitarbeiter verlieren durchschnittlich
28 Minuten,
wenn sie ein IT-bezogenes Problem haben

Das sind **100 Stunden**
(mehr als zwei Wochen),
die jedes Jahr pro Mitarbeiter verschwendet werden

IT-SERVICE-MANAGEMENT

KI UND AUTOMATISIERUNG WERDEN VERÄNDERUNGEN BRINGEN

Die „Everywhere Company", in der Mitarbeiter remote oder on-site auf Unternehmensressourcen zugreifen, ist spätestens mit der Pandemie zum neuen Normal geworden. it management-Herausgeber Ulrich Parthier sprach mit Peter Machat, Vice President EMEA Central von Ivanti, zu den Herausforderungen die sich daraus für den IT-Service stellen.

Ulrich Parthier: *Der Name Ivanti ist vielleicht nicht jedem geläufig. In welchem Marktsegment bewegen Sie sich?*

Peter Machat: Unter dem Namen „Ivanti" firmieren wir seit dem Jahr 2017 als Zusammenschluss von LANDesk und Heat Software. Im vergangenen Jahr sind dann die Mobile- und Security-Spezialisten MobileIron und PulseSecure zu uns gestoßen, sodass wir unsere Kunden heute mit einem umfassenden Portfolio an UEM-, ITSM-, ESM- sowie Security-Lösungen unterstützen. Sie automatisieren alle IT- und Sicherheitsprozesse im Unternehmen, angefangen mit der Inventarisierung und Verwaltung von Endpunkten, bis hin zur Absicherung und Wartung aller Geräte – egal, ob dies über die Cloud geschieht oder ob es sich um ein IoT Edge Device handelt.

Ulrich Parthier: *Ivanti hat jüngst mit der Übernahme von MobileIron, PulseSecure und Cherwell auf sich aufmerksam gemacht. Welchen Hintergrund haben diese Zukäufe?*

KI-GESTÜTZTE TECHNOLOGIEN UND TOOLS WERDEN ÜBER KURZ ODER LANG DIE ABLÄUFE UND SCHWERPUNKTE IM ITSM VERÄNDERN. DABEI IST ES WICHTIG ZU VERSTEHEN, DASS SIE DARAUF ABZIELEN, MITARBEITER VON REDUNDANTEN UND AUTOMATISIERBAREN AUFGABEN ZU ENTLASTEN – NICHT ABER, SIE ZU ERSETZEN.

Peter Machat,
Vice President EMEA Central, Ivanti,
www.ivanti.de

Peter Machat: Im Everywhere Enterprise mit hybriden Arbeitsplatzmodellen ist die klassische Silostruktur aus IT, Service Management und IT-Sicherheit schlicht nicht mehr praktikabel. Dezentrale, mobile Arbeitsumgebungen erfordern einen neuen Ansatz im Service Management und im Bereich der Sicherheitsarchitekturen.

Mit den Übernahmen haben wir die Grundlage geschaffen, Unternehmen in dieser Transformation zu unterstützen. Unser Ziel ist es, die drei Bereiche Unified Endpoint Management, Zero Trust Security sowie Enterprise Service Management zusammenzuführen. Wir integrieren dazu die Zero-Trust-Funktionen von Pulse Secure und MobileIron in die KI-gestützte, kontextbezogene Neurons-Plattform von Ivanti. Ziel ist es, die IT-Verwaltung intelligenter und sicherer zu machen. Gemeinsam mit Cherwell werden wir zudem eine tiefergehende und vertikal ausgerichtete ESM-Lösung entwickeln, die ein durchgängiges Service- und Asset Management von der IT bis in die Fachabteilungen ermöglicht.

Ulrich Parthier: *Sie erwähnen das „Everywhere Enterprise". Was meinen Sie damit?*

Peter Machat: Im Everywhere Enterprise laufen Unternehmensdaten frei über Geräte und Server und ermöglichen es den Mitarbeitern, standortunabhängig und produktiv zu arbeiten. Solche Ansätze gab es auch schon früher. Verändert hat sich die Geschwindigkeit und der Umfang in dem sich remotes Arbeiten durchgesetzt hat. Die Erfahrungen, die IT-Teams in den letzten Monaten dabei sammeln konnten, sind wertvolle Assets für die Umsetzung künftiger dezentraler Arbeitsplatzmodelle.

Ulrich Parthier: *Wie verändern sich die Aufgaben der IT-Teams im Service Management in einem solchen hybriden Arbeitsmodell?*

Peter Machat: Die größte Herausforderung im Service Management ist die Lösung von IT-Problemen auf Endgeräten, die sich längerfristig außerhalb des Unternehmensnetzwerkes befinden. Das ist meiner Ansicht nach nur durch Automatisierungstechnologien beherrschbar. Unternehmen benötigen hierzu intelligente Lösungen für den IT-Support, um Risiken zu priorisieren, also Routine-Tickets effektiv von echten Problemfällen zu unterscheiden.

Ein weiterer Aspekt ist die Zusammenarbeit mit anderen Fachabteilungen. Eine moderne Servicebereitstellung beschränkt sich nicht auf die IT. Insbesondere für dezentral arbeitende Unternehmen ist es elementar, die Produktivität ihrer Belegschaft kontinuierlich zu unterstützen. Das heißt für das Service Management, Geschäftsabteilungen proaktiv zu beraten und manuelle Prozesse zu digitalisieren.

Ulrich Parthier: *Die Zufriedenheit mit dem Service Management ist weiter gestiegen. Trotzdem gibt es Hürden. Welche Herausforderungen müssen Firmen beim Thema ITSM/ESM künftig lösen?*

Peter Machat: Das Ansehen der IT in der Belegschaft ist in den letzten Monaten tatsächlich immens gewachsen. Allerdings werden die Herausforderungen bei der Integration von Service Management und geschäftskritischen Prozessen perspektivisch noch steigen. Wir sehen das an der zögerlichen Akzeptanz von ESM-Tools in den Unternehmen. Firmen fällt es immer noch schwer, eine ganzheitliche Sicht auf ihre Geschäftsprozesse zu werfen. Sie denken zu eng, in Silos und agieren in ihren einzelnen Geschäftsbereichen zu autark.

Ulrich Parthier: *Welche Rolle spielen die Themen Automatisierung und KI in dieser Transformation der IT-Service-Teams?*

Peter Machat: KI-gestützte Technologien und Tools werden über kurz oder lang die Abläufe und Schwerpunkte im ITSM verändern. Dabei ist es wichtig zu verstehen, dass sie darauf abzielen, Mitarbeiter von redundanten und automatisierbaren Aufgaben zu entlasten – nicht aber, sie zu ersetzen. KI-basierte Bots ermöglichen die Automatisierung von Service-Management-Prozessen, um Vorfälle und Anfragen genauer zu interpretieren, bevor sie in die ITSM-Lösung eingehen. Hier wird der Übergang von einfacher Automatisierung, also der automatischen Abarbeitung von Routine-Tasks, zur Hyper-Automatisierung deutlich, in der sich Geräte komplett selbst verwalten und absichern.

Ulrich Parthier: *Sie sprechen von einem Wandel hin zu Hyper-Automatisierung. Was genau verstehen Sie darunter?*

Peter Machat: Die klassische Automatisierung ist heute schon in der Lage die IT-Teams substanziell zu entlasten. Hy-

per-Automatisierung geht einen Schritt weiter. Hier geht es um ein proaktives, vorhersagbares und kontinuierliches Self-Healing und Self-Securing von Geräten sowie Self-Service für Endbenutzer.

Beispiel Self-Healing: Automatisierte ITAM-Tools verschaffen sich dabei einen genauen Überblick über die vorhandenen IT-Assets. Danach wird die optimalen Konfigurations- und Performance-Einstellungen für eine gute und sichere Nutzung ermittelt. Automatisiert wird dann geprüft, ob ein Gerät von diesem Zustand abweicht – und gegebenenfalls wieder auf diesen Idealzustand zurückversetzt.

Ulrich Parthier: *Sowohl Ivanti als auch Cherwell sind sehr gut in Gartners Magic Quadrant positioniert. Werden die Produktlinien separat weitergeführt? Und: wann können die Anwender mit einer Roadmap rechnen?*

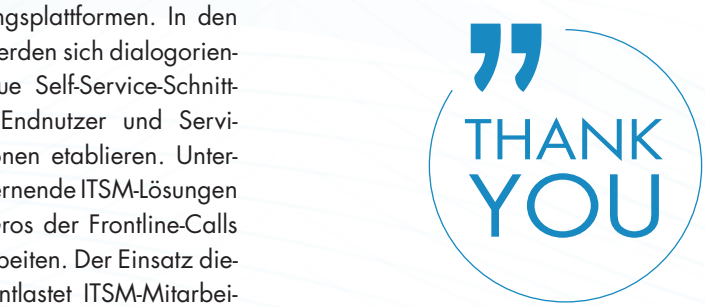
Peter Machat: Wir werden weiterhin sowohl die Cherwell- als auch die Ivanti-Service-Management-Plattformen pflegen und in sie investieren. Über eine gemeinsame Roadmap kann ich vor dem rechtlichen Abschluss der Übernahme allerdings noch nicht sprechen.

Ulrich Parthier: *Zum Schluss noch ein Blick in die Zukunft: Wie wird sich das IT-Service-Management weiterhin entwickeln?*

Peter Machat: Die Zukunft im Service Management gehört ganz klar den KI-basierten Automatisierungsplattformen. In den nächsten Jahren werden sich dialogorientierte Bots als neue Self-Service-Schnittstellen zwischen Endnutzer und Service-Delivery-Funktionen etablieren. Unterstützt durch selbstlernende ITSM-Lösungen werden sie das Gros der Frontline-Calls automatisiert bearbeiten. Der Einsatz dieser Technologie entlastet ITSM-Mitarbeiter, die sich mehr auf größere Incidents sowie das Problem- und Change-Management fokussieren.

Auch im Bereich Zugriffsmanagement wird sich das ITSM in Zukunft neu ausrichten müssen. Neue Sicherheitskonzepte sind dringend gefragt. Eine Zero-Trust-Strategie in Verbindung mit Self-Securing-Lösungen und biometrischen Erkennungsverfahren sehe ich hier als gangbaren Weg.

Ulrich Parthier: *Herr Machat, wir danken für dieses Gespräch*



IM EVERYWHERE ENTERPRISE LAUFEN UNTERNEHMENSDATEN FREI ÜBER GERÄTE UND SERVER UND ERMÖGLICHEN ES DEN MITARBEITERN, STANDORTUNABHÄNGIG UND PRODUKTIV ZU ARBEITEN.

OPERATIONAL SERVICES
YOUR ICT PARTNER

Microsoft Partner

Microsoft

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

MICROSOFT 365 & AZURE GERÄUSCHLOS AUSROLLEN UND SICHER BETREIBEN

Zusammenarbeit gelingt ohne Widerspruch zum deutschen Datenschutz

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

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

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

operational-services.de/microsoft-365

Starten Sie mit uns sichere, cloudbasierte Collaboration

AGILE METHODEN ERLEBEN DURCHBRUCH

BEDEUTUNG VON CHANGEMANAGEMENT STEIGT

Mehr als die Hälfte der Unternehmen in Deutschland nutzt regelmäßig agile Methoden, um neue Produkte oder Dienstleistungen schnell und bedarfsgerecht zu entwickeln. Das zeigt eine repräsentative Umfrage von Bitkom Research im Auftrag des IT-Dienstleisters Tata Consultancy Services (TCS).

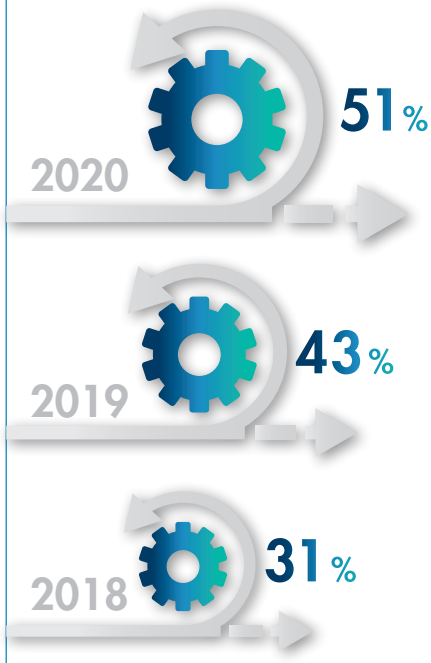
Agile Methoden ermöglichen eine transparente Sicht auf den Entwicklungsstand. Damit kann gezielt und bedarfsgerecht entwickelt werden und Unternehmen sparen so Zeit und Ressourcen. Allerdings ist dafür ein Umdenken erforderlich: „Nur wenn Business und IT eng zusammenarbeiten, zeigen agile Methoden die erwünschten Ergebnisse“, so Dr. Kay Müller-Jones, Leiter Consulting und Services Integration bei TCS.

Veränderungen benötigen Changemanagement

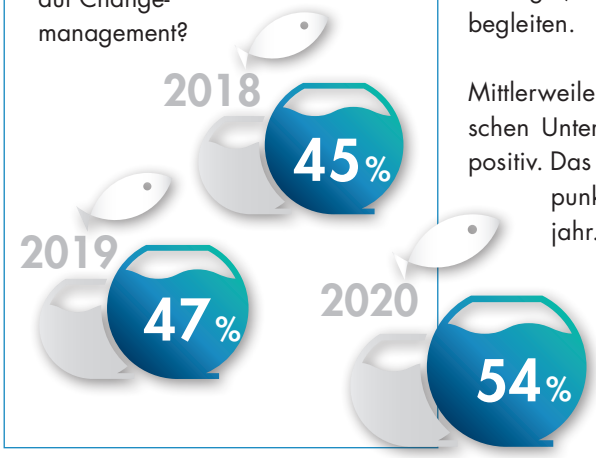
Gleich ob bei digitaler Transformation eines Unternehmens, neuen Lösungen mit Künstlicher Intelligenz oder innovativen Methoden wie Agile, hilft Changemanagment, den Wandel zu begleiten und zu gestalten. Die Mehrheit der Unternehmen hat diesen Bedarf mittlerweile erkannt: Erstmals nutzt mehr als jedes Zweite (54 Prozent) entsprechende Methoden – ein Zuwachs von 18 Prozentpunkten im Vergleich zu 2017, als die Frage erstmals in der Studie enthalten war. Vor allem Großunternehmen haben die Bedeutung des Changemanagements erkannt: Bereits zwei Drittel (69 Prozent) wenden diese Methoden an.

AGILE METHODEN ERLEBEN IHREN DURCHBRUCH

Wie viele Unternehmen setzen manchmal, größtenteils oder immer agile Methoden ein?



Wie viele Unternehmen setzen in puncto Digitalisierung auf Changemanagement?



„Immer mehr Unternehmen erkennen die Bedeutung von Changemanagement“, sagt Müller-Jones. „Das stimmt optimistisch, denn nur gemeinsam mit den Mitarbeitern lässt sich der Wandel erfolgreich gestalten. Es geht darum, Aufklärungsarbeit zu leisten und die eigenen Mitarbeiter für die digitale Transformation zu befähigen. Denn diese gelingt nur dann, wenn sie von den eigenen Mitarbeiterinnen und Mitarbeitern mitgetragen wird.“

Changemanagement wird unterschiedlich verankert

Welcher Unternehmensbereich koordiniert aber das Thema Changemanagement? Am häufigsten sind es die IT-Abteilung (40 Prozent), die eigene Digitalisierungseinheit (38 Prozent), die Unternehmensführung (27 Prozent) und die Unternehmenskommunikation (25 Prozent, Mehrfachnennungen möglich). Die Verantwortlichkeiten variieren je nach Unternehmensgröße jedoch stark. Vorreiter sind auch hier Unternehmen mit mehr als 500 Mitarbeitern: jedes zweite Großunternehmen (53 Prozent) verfügt über eine eigene Digitalisierungseinheit oder einen eigens eingestellten Changemanager, um den digitalen Wandel zu begleiten.

Mittlerweile sehen 85 Prozent der deutschen Unternehmen die Digitalisierung positiv. Das ist ein Anstieg um 7 Prozentpunkte im Vergleich zum Vorjahr. Ebenfalls erfreulich: Zum ersten Mal überhaupt lehnt kein einziges Unternehmen die Digitalisierung pauschal ab.

www.bitkom-research.de

HOMEOFFICE OHNE EINSCHRÄNKUNGEN

SO GELINGT DER EINFACHE UND SICHERE ONLINE-ZUGRIFF AUF DOKUMENTE

Auch nach einem Jahr Corona befinden sich viele Unternehmen im Hinblick auf Remote Work immer noch im Survival Modus. Häufig mangelt es an den benötigten Technologien, wie eine aktuelle Ricoh-Studie zeigt. Demnach stehen knapp einem Viertel der befragten Arbeitskräfte im Homeoffice nicht die nötigen Tools zur Verfügung, um angemessen mit ihren Kollegen zusammenzuarbeiten und ihre Aufgaben zu erfüllen. Das sorgt nicht nur für Frustration bei den Beschäftigten, sondern gefährdet auch den langfristigen Unternehmenserfolg. Über ein Viertel der befragten Büroangestellten gaben weiterhin an, aufgrund der IT-Defizite im Homeoffice Schwierigkeiten bei der Einhaltung von Compliance- und Datenschutzvorgaben zu haben.

Unternehmen müssen daher dringend die Technikprobleme im Zusammenhang mit Remote Working beheben. Damit die Mitarbeiterinnen und Mitarbeiter auch im Homeoffice produktiv arbeiten können, sind flexible und sichere Lösungen für die digitale Organisation der Geschäftsprozesse gefragt. Mit einem Cloud-basierten Dokumentenmanagementsystem haben nicht nur alle Mitarbeiter jederzeit und überall den Zugriff auf die benötigten Informationen und Dokumente. Automatisierte Workflows entlasten sie außerdem bei Routineaufgaben und ermöglichen die rechts- und revisionssichere Archivierung der Dokumente. Die passende Softwarelösung sollte dabei einige grundlegende Anforderungen erfüllen. Die folgenden sechs Funktionen erleichtern die Workflow-Optimierung – und das nicht nur im Homeoffice, sondern auch im Büro:

Reibungslose Kommunikation ermöglichen

1. Dateien lassen sich schnell und unkompliziert per Drag & Drop oder Mail-Upload in das Dokumentenmanagementsystem einpflegen, damit die Mitarbeiter sowohl im Büro als auch im Homeoffice auf alle Dokumente zugreifen können. Verträge, Rechnungen oder Personalakten, die noch in Papierform vorliegen, können mit den Scan-Lösungen moderner Multifunktionsgeräte digitalisiert und dem entsprechenden Dokumenten-Workflow automatisch hinzugefügt werden.

2. Individuell anpassbare Freigabeprozesse und eine automatische Synchronisationsfunktion ermöglichen es, genau den Mitarbeitern die Dokumente zur Verfügung zu stellen, die sie brauchen – ohne dass diese jedes Mal angefragt werden müssen.

3. Mithilfe einer Kommentarfunktion lassen sich Notizen direkt im Dokument vermerken. Das sorgt dafür, dass deutlich weniger Mails geschrieben werden müssen, wodurch die Mitarbeiter merklich entlastet werden.

Sicheres Dateimanagement auch im Homeoffice

1. Die Dokumentenmanagement-Lösung ermöglicht es, ohne manuellen Aufwand gesetzliche Anforderungen wie die DSGVO, firmeninterne Sicherheitsvorgaben oder Branchenregeln einzuhalten.

2. Bei sensiblen Informationen ist es von zentraler Bedeutung, dass nur die Personen darauf zugreifen können, für die sie bestimmt sind. Mit Zugriffsberechtigungen kann gesteuert werden, welche Mitarbeiter nur Lesezugriff haben oder Kommentare hinzufügen können und wer die Dokumente tatsächlich bearbeiten darf. Für besonders vertrauliche Dokumente können außerdem geschützte Links und Gastzugriffe eingerichtet werden. Mithilfe von auditierten Sammlungen lässt sich dann genau nachverfolgen, wer wann auf die Dateien zugegriffen und diese bearbeitet hat.

3. Noch mehr Sicherheit ermöglicht die Datenübertragung mit einer Ende-zu-Ende-Verschlüsselung und eine zusätzlich verschlüsselte Ablage. So sind die digitalen Unterlagen auch im Homeoffice bestens geschützt. Für den mobilen Zugriff über Web-Browser kann darüber hinaus eine 2-Faktor-Authentifizierung einrichtet werden.

NEW WORK

WELCHEN BEITRAG KANN UND MUSS DIE IT LEISTEN?

Der Begriff New Work ist schon seit einiger Zeit ein feststehender Begriff und wird in unterschiedlichen Kontexten verwendet. Im Kern bezeichnet New Work die Arbeitswelt von morgen – und steht somit auch für einen Wandel. Denn bestehende Gewohnheiten und Strukturen in der Art, wie wir leben und arbeiten verändern sich: Arbeiten wird unabhängiger von Zeit, Ort, Netzwerk und Gerät. So sollen Mitarbeiter flexibler entlang ihrer eigenen Bedürfnisse entscheiden können, wann, wo und wie sie arbeiten. Das kann viele Vorteile für Unternehmen und Mitarbeiter mit sich bringen, aber auch Herausforderungen.

Durch Corona sammeln aktuell bereits viele Mitarbeiter Erfahrungen mit der Arbeit im Homeoffice als einem Teilbereich von New Work. Dabei erleben sie auch, dass sich Berufs- und Privatleben immer stärker miteinander vermischen. Doch New Work findet nicht nur in den eigenen vier Wänden statt: Jede Umgebung – sei es das Zugabteil, der Coworking Space (auch innerhalb der eigenen Firma) oder der Konferenzraum eines Kunden – kann hierbei zur idealen Arbeitsumgebung werden.

Die IT als Dreh- und Angelpunkt

Damit die Umsetzung von New Work gelingen kann, muss sich die Arbeitskultur und -organisation verändern. Auch die technischen Gegebenheiten entscheiden über Erfolg oder Misserfolg. Denn die Basis von New Work sind digitale, mobile Arbeitsmöglichkeiten. Dabei stehen IT-Teams vor der Herausforderung, verschiedenen Ansprüchen gerecht zu werden: Der mobile Arbeitsplatz soll die Effektivität und Produktivität von Mitarbeitern fördern, gleichzeitig aber auch umfassend gegen Angriffe sowie Datenspionage abgesichert sein und Compliance-Richtlinien erfüllen. Und das alles mit überschaubarem Aufwand. Es braucht also intelligente Technologien, die diese drei Spannungsfelder vereinen.

New Work technisch umsetzen: Die Basics

Die Umsetzung des mobilen Arbeitens bedarf eigentlich einiger Planung. Wichtige Grundvoraussetzungen sind dabei unter anderem:

➤ Es muss definiert werden, welche Tätigkeiten Mitarbeiter außerhalb des Büros -ausführen sollen und auf welche Dienste und Systeme sie dafür Zugriff benötigen

➤ Mitarbeiter sind mit firmeneigenen mobilen Endgeräten wie Laptops, Smartphones oder Tablets ausgestattet und/ oder dürfen private Geräte nutzen (BYOD)

➤ Private und berufliche Daten werden getrennt voneinander gespeichert und verarbeitet, um sowohl die Privatsphäre der Nutzer als auch die Sicherheit der Geschäftsdaten zu gewährleisten

➤ Die mobilen Endgeräte können von der IT über eine zentrale Plattform verwaltet und abgesichert werden (etwa per Unified Endpoint Management-System oder Container-Lösung, ggf. mit ergänzenden Mobile Threat Defense- und Security-Lösungen, um Angriffen vorzubeugen)

➤ Serverkapazitäten von internen und externen Systemen können eine veränderte Auslastung auffangen

➤ Mitarbeiter können in Echtzeit datenschutzkonform miteinander kommunizieren und Meetings virtuell abhalten

New Work – aber sicher

Beim ortsunabhängigen Arbeiten sind Zugriffe auf Unternehmenslaufwerke und -dienste notwendig. Hierbei geht es teils um sehr sensible Daten. Diese sollten bei der mobilen Arbeit genauso abgesichert sein, wie sie es auch im Unternehmensnetzwerk sind. Denn Cyberkriminelle entwickeln laufend neue Methoden und nehmen mobile Endgeräte immer stärker ins Visier. Um Unternehmensdaten zu schützen ist – neben dem Einsatz von Mobile Threat Defense-Lösungen – die Sensibilisierung von Mitarbeitern fundamental. Mitarbeiter müssen regelmäßig darin geschult werden, wie Gefahren beim mobilen Arbeiten aussehen und welchen Einfluss ihr eigenes Verhalten haben kann.

Zudem ist der Einsatz einer VPN-Lösung zur Absicherung der Kommunikation mit den Unternehmensnetzwerken wichtig. Ein VPN verschlüsselt den Datenverkehr zwischen Mitarbeitergerät und sensiblen Quellen und sorgt so für mehr Sicherheit. In Abhängigkeit der Betriebssysteme der Geräte kann ein VPN auf verschiedene Weisen zum Einsatz kommen: Während ein Per-Device-VPN sämtliche Verbindungen eines Gerätes verschlüsselt, werden bei einem Per-App-VPN nur bestimmte Anwendungen und bei einem Per-Account-VPN nur Zugriffe von bestimmten Konten verschlüsselt.

Der Nutzer im Fokus

Neben der Sicherheit ist auch die Nutzerfreundlichkeit ein wichtiger Erfolgsfaktor beim mobilen Arbeiten. Nutzer sollten von überall aus produktiv und sicher arbeiten können – darauf kommt es bei der Umsetzung des New Work Ansatzes an.

Ein gutes Beispiel dafür ist das Thema Authentifizierung. Mitarbeiter arbeiten täglich mit vielen Anwendungen und müssen auf unterschiedliche Server und Laufwerke zugreifen. Der Zugriff hierauf ist häufig mittels Benutzername und Passwort oder Zwei-Faktor-Authentifizierung abgesichert. Gerade letzteres erhöht zwar die Sicherheit deutlich, ist aber für den Nutzer zeitaufwändig und insbesondere beim mobilen Arbeiten – beispielsweise im Zug – unpraktisch und mindert die Akzeptanz und Zufriedenheit.

Zielführender ist an dieser Stelle der Einsatz von sogenannten Single-Sign-On und Conditional Access-Verfahren. Dabei kann durch die Definition von Richtlinien erreicht werden, dass sich die Authentifizierungsmethode automatisiert jeweils an den Kontext der Zugriffssituation anpasst.

Heißt: Möchte ein im Active Directory hinterlegter Nutzer von seinem gemanagten Firmengerät auf eine Unternehmens-App zugreifen, kann eine passwortlose Authentifizierung ermöglicht werden. Wird die Situation als unsicher eingeschätzt (etwa der Ort und ein anderes Gerät), werden zusätzliche Autorisierungsschritte, wie beispielsweise die Eingabe eines Passworts oder zweiten PINs, notwendig.

Die technische Umsetzung von nutzerfreundlichen Authentifizierungsverfahren funktioniert bei iOS, Android, Windows oder MacOS teils auf unterschiedlichen Wegen. Dennoch sollten Unternehmen auf eine ganzheitliche Gerätestrategie setzen und allen Nutzern komfortable Zugriffe auf Daten ermöglichen.

NEW WORK SPIELT IN DER ZUKUNFT EINE WICHTIGE ROLLE. DER EINSATZ DER RICHTIGEN TECHNOLOGIEN IST BEI DER UMSETZUNG EINE GUTE BASIS UND KANN ARBEITEN AUSSERHALB DER GEWOHNTEN MUSTER ERMÖGLICHEN.

Markus Adolph, Mitbegründer und geschäftsführender Gesellschafter, EBF GmbH, www.ebf.com

Unternehmen sollten das Thema Nutzerfreundlichkeit aber auch auf andere Situationen im Arbeitsalltag übertragen. Beim orts- und zeitunabhängigen Arbeiten ist es besonders wichtig, den persönlichen Austausch mit Kollegen, Geschäftspartnern und Kunden nicht zu verlieren. Videokonferenzen überbrücken die Distanz und kommen daher im New Work Alltag vermehrt zum Einsatz. Einige VPNs können dabei helfen, den Nutzerkomfort hierbei zu erhöhen. Sie können die Verbindung in virtuellen Meetings stabilisieren und so lästige Unterbrechungen, den Verlust der Ton- und Bildqualität oder Mehrfach Log-Ins in Folge von Verbindungsabbrüchen verhindern – ein enormer Mehrwert für mobile Nutzer.

Klappt beim mobilen Arbeiten einmal etwas nicht reibungslos, ist ein schneller Support der Mitarbeiter wichtig. Das ist nicht einfach, da New Work auch bedeutet, dass Nutzer außerhalb der klassischen Arbeitszeiten der IT arbeiten und dabei trotzdem einen zügigen Usersupport benötigen. Mitarbeiter, die abends oder in einer anderen Zeitzone arbeiten, sollten ihr Passwort daher beispielsweise eigenständig zurücksetzen können.

New Work spielt in der Zukunft eine wichtige Rolle. Der Einsatz der richtigen Technologien ist bei der Umsetzung eine gute Basis und kann Arbeiten außerhalb der gewohnten Muster ermöglichen. Technologien müssen die Sicherheit der Daten gewährleisten und dabei genauso die Bedürfnisse von Nutzern adressieren. Denn eines ist klar: Eingesetzte Technologien müssen für Mitarbeiter in ihrem Arbeitsalltag einen Nutzen haben. Ist das nicht der Fall, sinkt deren Akzeptanz – und die Umsetzung von New Work wird enorm erschwert.

Markus Adolph

REMOTE-ONBOARDING

WORÜBER KAUM JEMAND SPRICHT

In letzter Zeit ist ein Thema immer wieder prominent diskutiert worden: Onboarding in Zeiten von Home Office und Remote Work. Viele Stimmen konzentrieren sich dabei nur auf eine Seite der Medaille. Man hört und liest viel über die Herausforderungen für die Unternehmenskultur und Teamstruktur. Diese Facetten sind durchaus wichtig und dürfen nicht vernachlässigt werden, Onboarding umfasst jedoch mehr.

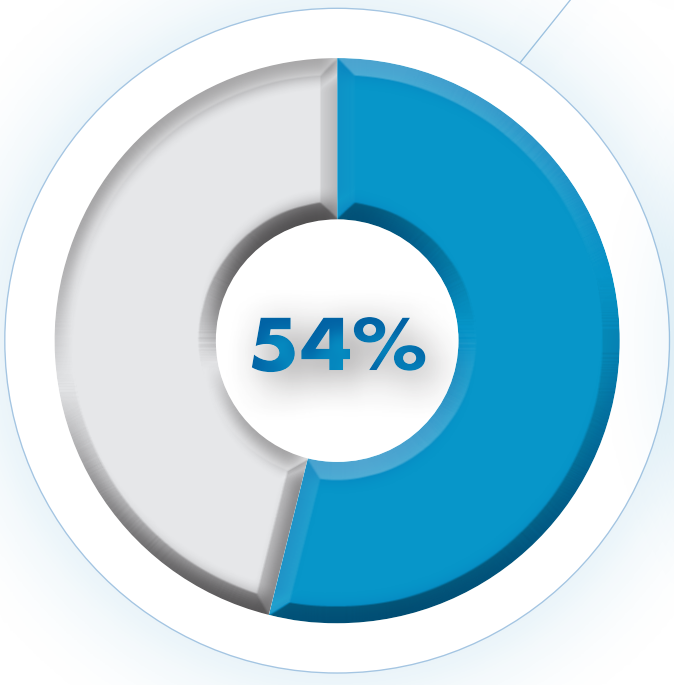
Durch das Wegfallen räumlicher Nähe werden bestimmte Elemente eines erfolgreichen Onboardings eindeutig schwieriger. Gespräche auf dem Büroflur finden nicht statt, Mitarbeiter lernen sich gegenseitig langsamer und in virtuellen Bubbles kennen. Das erschwert natürlich das Entdecken und Adaptieren gelebter Unternehmenskultur. Das Motto, um diesen Wandel zu optimieren: Virtual Coffee statt Watercooler Moments. Die empfohlene Lösung ist also ein „Ersatz": Das Erschaffen einer neuen, digitalen sozialen Struktur. Durch regelmäßige virtuelle Events, Mentoring und ein starkes Employer Branding werden Mitarbeiter an die Hand genommen und sollen so das Miteinander erleben, dass vielen im Home-Office sonst fehlt.

Purpose, Unternehmenskultur und Teamgefühl sind durchaus wichtige Pfeiler der Employee Experience. Ein weiteres Element wird bei der aktuellen Diskussion jedoch oft außen vor gelassen: das Arbeiten an sich.

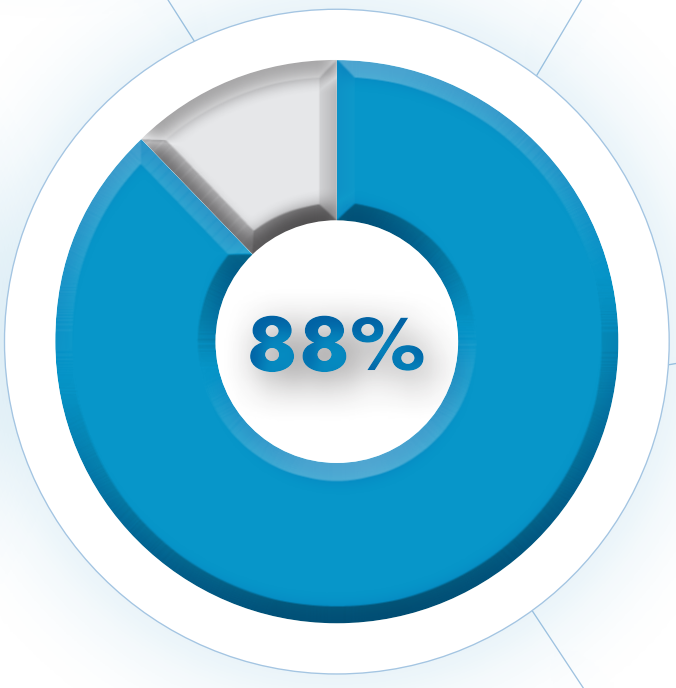
Ob es um das Onboarden neuer Mitarbeiter ins Unternehmen geht oder darum, bestehenden Mitarbeitern neue Remote-Tools näherzubringen – tägliche Arbeitsprozesse und Supportstrukturen müssen im Onboarding ebenfalls eine zentrale Rolle spielen. Auch hier entstehen durch Remote Work neue Herausforde-

1.100 X WECHSELN MITARBEITER TÄGLICH ZWISCHEN ANWENDUNGEN

35 JOB-KRITISCHE APPLIKATIONEN PRO MITARBEITER



DER UNTERNEHMEN MIT ONBOARDING-PROGRAMMEN BERICHTEN ÜBER HÖHERES MITARBEITERENGAGEMENT



ALLER UNTERNEHMEN HABEN PROBLEME BEIM ONBOARDING

EINE DIGITAL ADOPTION PLATTFORM FÜHRT NUTZER SCHRITT FÜR SCHRITT DURCH EIN PROGRAMM UND BIETET SUPPORT WANN UND WO ER AM MEISTEN BENÖTIGT WIRD.

Roland Völkel,
Content Expert, Userlane,
www.userlane.de

rungen. Man kann nicht mal eben seinen Sitznachbarn fragen, wie man eine Rechnung einreicht oder den Urlaubsantrag ändert. Software-Schulungen werden auch durch Videokonferenzen nicht nachhaltiger oder erfolgreicher. Was bleibt also? Natürlich kann man weiterhin Tickets an den IT Support schreiben, aber das führt zum einen zu Wartezeiten, bis man eine Antwort erhält und erhöht zum anderen das Arbeitspensum der Support-Mitarbeiter erheblich.

„Im Durchschnitt arbeiten Angestellte täglich mit 35 Applikationen und müssen teilweise sehr komplexe Prozesse in diesen beherrschen. Prozesslandschaften dominieren dann den Arbeitstag und wichtige Aufgaben bleiben liegen – obwohl die Programme eigentlich die Arbeit erleichtern sollten." sagt Hartmut Hahn, CEO von Userlane. Es muss also umgedacht werden. Die Lösung ist auch hier das Einführen einer digitalen Struktur, die den Mitarbeiter abholt und auf seine Bedürfnisse zugeschnitten mitnimmt. Egal, ob er Remote arbeitet oder nicht.

Fokus auf digitale Adoption

Das Zauberwort heißt: Digital Adoption, also das Lernen, Verstehen und Adaptieren digitaler Prozesse. Eine Digital Adoption Plattform, wie zum Beispiel Userlane, führt Nutzer Schritt für Schritt durch ein Programm und bietet Support wann und wo er am meisten benötigt wird. Der interaktive Guide zeigt ihm dann, welche Pfade er gehen, welche Buttons er klicken (alle anderen sind deaktiviert, er kann also gar nichts falsch machen) oder wo er etwas eintragen muss. So lernt der Mitarbeiter die Software kennen, während er sie nutzt. Die Guides lassen sich jederzeit ein- oder ausschalten, je nachdem wie sicher man sich in der Anwendung der Software fühlt.

Dies hat viele Vorteile für den Mitarbeiter. Zum einen ist Hilfe immer nur einen Klick entfernt, also Just-in-Time verfügbar. Zudem muss man die Anwendung nicht verlassen, sondern kann sich direkt in der Software durch die jeweiligen Prozesse führen lassen. Supportmitarbeiter können darüber hinaus noch stärker entlastet werden, indem man die Guides mit hilfreichen Informationen und weiterführenden Links, zum Beispiel zur eigenen Knowledge Base anreichert.

Unternehmen auf der anderen Seite sparen Kosten für Trainings und Support ein und profitieren von der unkomplizierten, schnellen Einführung einer Digital Adoption Plattform. Zudem erreichen Mitarbeiter schneller höhere Effizienz und das Potenzial der Software wird stärker ausgeschöpft. Das steigert den Return of Investment der eingesetzten Anwendungen.

„Durch die Vielzahl an neuen Programmen und deren stete und schnelle Veränderung wird es immer wichtiger, die Anwender abzuholen und in deren Tempo auf die digitale Reise mitzunehmen. Leider wird das noch immer oft vernachlässigt. Hinzu kommt, dass wir uns gerade in Zeiten von Home Office mit immer mehr Software herumschlagen, die wir effizient anwenden müssen und nicht einfach die Möglichkeit haben, unsere Kollegen um Hilfe zu bitten. Unternehmen müssen ihren Mitarbeitern beim digitalen Wandel helfen und sie dafür begeistern. Es genügt also nicht, neue Technologien anzuschaffen: Der Mensch muss ins Zentrum der digitalen Adaption gerückt werden", so Hartmut Hahn.

Onboarding allumfassend betrachten

Onboarding nimmt einen wichtigen Platz in der Employee Experience ein. Es ist Teil des ersten Eindrucks und kann die Einstellung neuer und alter Talente langfristig beeinflussen. Die Herangehensweise an traditionelle Onboarding-Prozesse muss sich jedoch an wandelnde gesellschaftliche und soziopolitische Gegebenheiten wie Remote Work anpassen. Dafür muss eine offene Einstellung gegenüber Innovationen im Unternehmen vorherrschen. Man darf sich daher auch nicht nur auf einen Bereich konzentrieren, sondern sollte Onboarding allumfassend betrachten. Das beinhaltet Prozesse, Software-Lösungen und Strukturen für die tägliche Arbeit. Nur dann kann man Onboarding erfolgreich neu denken und im Unternehmen verankern.

Roland Völkel

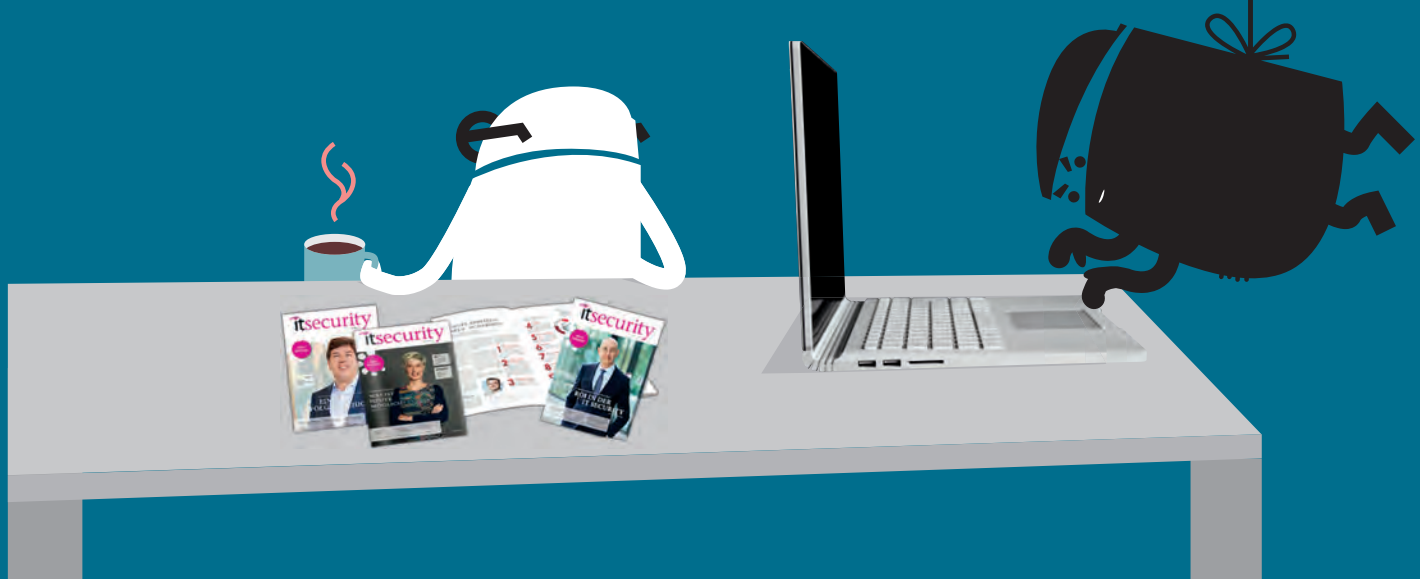
We secure IT

Spring 2021

25.03.2021

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

Die Konferenz findet live am Donnerstag, 25. März 2021, von 10:00 bis 16:30 Uhr statt. Die Teilnahme ist kostenlos.



Highlights aus der Agenda

Threat Protection

Increase the cyber-resilience – Die Widerstandsfähigkeit gegen Cyberattacken stärken
Michael Gisevius, Manager Territory Sales DACH, Bitdefender

Danke für dein Passwort: Reputationsverlust und finanzielle Schäden durch Credential Stuffing wirkungsvoll abwehren
Stefan Schweizer, Geschäftsführer, Nevis Security GmbH

Security Awareness

Live-Demo: Security Awareness - wer klickt, verliert
Felix Betzin, Regional Account Manager, KnowBe4

Human Risk Review 2021 - Sicherheitslücke Remote Work?
Dr. Niklas Hellemann, Geschäftsführer, SoSafe Cyber Security Awareness

Cloud Security

Cloud Apps sicher und effizient nutzen. Geht das überhaupt?
Darko Simic, Solution Engineer, Netskope

Best Practices aus Deutschland: Wie sich Firmen gegen Gefahren aus dem Internet schützen
Elmar Witte, Security Specialist, Akamai Technologies

The New Normal: Die Folgen der Pandemie für die IT-Sicherheit
Andreas Fuchs, Director Product Management, DriveLock SE

Jetzt anmelden

www.it-daily.net/wesecureit/

2021

ALS JAHR DER ERHOLUNG UND DES AUFSCHWUNGS

- Deutsche Unternehmen sind weiterhin optimistisch in Bezug auf die wirtschaftlichen Aussichten für 2021
- Die größten Einflussfaktoren auf das Wachstum sind erweiterte Geschäftsmöglichkeiten und die Digitalisierung
- 75 Prozent der deutschen Unternehmen möchten ihre Mitarbeiterzahl konstant halten; 17 Prozent wollen zusätzliche Stellen schaffen

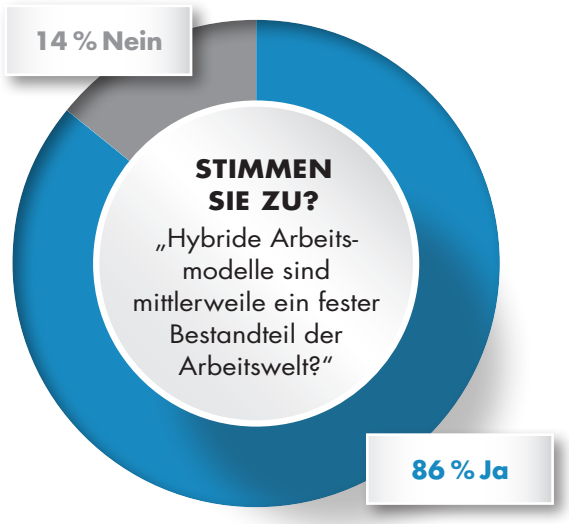
HYBRIDES ARBEITEN

FESTER BESTANDTEIL DER NEUEN ARBEITSWELT?

Der erstmalig von Robert Half veröffentlichte Arbeitsmarkt-Report 2021 gibt einen Überblick über aktuelle Arbeitsmarkttrends und gesuchte Positionen. Dabei wird deutlich: Seit Beginn der Pandemie sind qualifizierte Fachkräfte besonders gefragt und auch die Beliebtheit von hybriden Arbeitsformen ist stark gestiegen.

Die Mehrheit der Arbeitgeber (86 %) sieht hybrides Arbeiten bereits als permanente Arbeitsform der Zukunft an. Dieses Modell hilft Unternehmen dabei, während der dynamischen Situation der Pandemie agil zu bleiben. Außerdem zwingt sie Firmen zu digitalen Arbeitsweisen und beschleunigt dadurch die digitale Transformation. Damit geht auch die Verbesserung technischer Fähigkeiten der Mitarbeiter einher. Ein weiterer Vorteil: Hybrides Arbeiten stellt in Krisenzeiten die Geschäftskontinuität und Produktivität der Firmen sicher. Auch Mitarbeiter schätzen die Möglichkeit, flexibel von zu Hause aus oder nach Möglichkeit im Büro zu arbeiten. Das fördert die Bindung wichtiger Mitarbeiter an das Unternehmen.

www.roberthalf.de



ARBEITEN VON ÜBERALL AUF DEM VORMARSCH

- Die größten Vorteile von hybriden Arbeitsmodellen bestehen in der zunehmenden Agilität der Unternehmen und der Beschleunigung der digitalen Transformation
- Zu den Herausforderungen zählen, das Engagement der Mitarbeiter hochzuhalten und ihr Wohlbefinden gut einzuschätzen

ESG-RICHTLINIEN

WIE DIE RICHTIGE SOFTWARE DIE EINHALTUNG FÖRDERT

ESG steht für Environmental, Social und Governance und bezeichnet eine Art der Unternehmensführung, die sich nicht nur an Profiten orientiert, sondern sich auch nach ethischen und nachhaltigen Maßstäben richtet.

Die treibenden Kräfte von ESG-Initiativen, ganz gleich, ob es sich um Vorstandsmitglieder, Führungskräfte, Governance- oder Compliance-Experten handelt, werden bei deren Implementierung wahrscheinlich auf verschiedenen Ebenen des Unternehmens auf Widerstand stoßen. Ablehnungen von ESG-Richtlinien sind in Wirklichkeit oft nur ein Mangel an Klarheit über den Begriff selbst. Denn für viele Vorstände waren die bisherigen Diskussionen über ESG eher eine Ansammlung von Buzzwords. Doch davon dürfen sich Unternehmen nicht abschrecken lassen, eine tiefergehende Auseinandersetzung mit dem Thema ist heute unumgänglich.

ESG kann geschäftskritisch sein

Aktuell versuchen viele Vorstände besser zu verstehen, wie ESG-Initiativen den langfristigen Wert eines Unternehmens und dessen Erfolg fördern.

Nachhaltiges Investment ist ein großer Trend und entsprechende Fonds verzeichnen ungeahnte Wachstumsraten. Auch große institutionelle Investoren haben inzwischen entsprechende Produkte aufgelegt, die sich bei Anlegern weltweit einer hohen Nachfrage erfreuen. Die Zustimmung der Vermögensverwaltung zum Management von Konzernen hängt mittlerweile sogar von den Fortschritten bei Themen wie Diversity und Klimaschutz ab.

Kunden interessieren sich in zunehmendem Maße dafür, wie Produkte hergestellt und transportiert werden, wo Rohstoffe herkommen und wie die Arbeitsbedingungen entlang der Lieferkette aussehen. Auf derartige Fragen müssen Unternehmen Antworten haben. Fallen diese im Sinne der Verbraucher aus, sind sie auch bereit, einen höheren Preis für Produkte zu bezahlen.

Den Zusammenhang zwischen ESG und Risiken für Unternehmen stellt eine Studie der NASDAQ fest. Für nachhaltig agierende Unternehmen sinkt demnach das Risiko um 6,4 Prozent gegenüber dem Marktdurchschnitt, während es sich für nachlässige Firmen um 10,2 Prozent erhöht.

Software hilft bei der Umsetzung

Es ist eine Sache, die Relevanz von ESG zu verstehen und sich dafür einzusetzen. Aber dieses Engagement in konkrete Ergebnisse umzuwandeln, die auch messbar sind, kann zur Herausforderung werden. Zunächst stellt sich die Frage, an welchen Rahmenwerken man sich überhaupt orientieren möchte. Dafür bieten sich beispielsweise die Standards an, die der International Business Council (IBC) des Weltwirtschaftsforums im September 2020 veröffentlichte. Mit Lösungen wie Diligent Compliance haben Unternehmen außerdem Zugang zu einer Bibliothek von etlichen weiteren Standards (regional oder branchenspezifisch) und regulatorischen Verpflichtungen. Die All-in-One-Plattform verfügt über integrierte Lösungen für interne Audits, Risikomanagement und Verbesserungsplanung.

Regelmäßige, umfassende interne Audits, Risikobewertungen und die Einhaltung von Vorschriften sind entscheidend für eine ethische und nachhaltige Unternehmensführung. Mit Diligent Compliance lassen sich Lücken leicht identifizieren und durch die Erstellung von Verbesserungsplänen beheben. Dashboards und Berichte sparen Zeit, indem sie die Abhängigkeit von manuellen Methoden zum Abrufen geschäftskritischer Informationen über Compliance und Richtlinien verringern. Die erzielten Erfolge können außerdem in der Software visualisiert werden. Um stets auf dem neuesten Stand zu bleiben, erlaubt die Software Unternehmen auch, Trends und Nachrichten zu überwachen, so dass sie schnell auf neue Entwicklungen im Bereich ESG-reagieren können.

Diligent

http://bit.ly/39NY4pE

LÄUFT BEI DIR?

EINFACHES INFORMATIONSMANAGEMENT IN SCHWIERIGEN ZEITEN

Wohl noch nie war die Einfachheit von Software-Anwendung so wichtig wie heute. Nachdem die Komplexität der IT-Umgebung bei vielen Berufstätigen im zurückliegenden Pandemiejahr sprunghaft angewachsen ist, punkten digitale Lösungen mehr denn je durch Merkmale wie Flexibilität, Skalierbarkeit und eine einfache Handhabung. Insbesondere Systeme für das Enterprise Informationen Management (EIM) können hier einen spürbaren Unterschied machen.

Auch wenn das Arbeiten von Zuhause inzwischen kaum noch wegzudenken ist: Home-Office war zum Zeitpunkt des ersten Lockdowns kaum erprobt. Einer Umfrage des Bitkom zufolge wechselten im Laufe des Jahres fast 50 Prozent der Berufstätigen hierzulande zumindest für ein paar Tage pro Woche ins Home-Office. Jeder Vierte arbeitete sogar vollständig von daheim. Vor Ausbruch der Corona-Krise waren es jedoch nur drei Prozent der Arbeitnehmer, die ausschließlich aus dem Heimbüro aktiv waren.

Neue Technologien

Ein rasanter Zuwachs in wenigen Tagen, den die Unternehmen organisieren mussten. Um weiterhin eine effektive Zusammenarbeit zu gewährleisten, wurden diverse neue Technologien freigeschaltet, die vor der Krise nur in bestimmten Situationen oder eher experimentell eingesetzt wurden. So kamen plötzlich weitere Kanäle zu bereits bestehenden Anwendungen für das Informationsmanagement hinzu, ohne dass diese in die Digitalisierungsstrategie integriert werden konnten.

Dabei ist nicht zuletzt das Dokumentenmanagement in den Fokus geraten. Durch das Remote-Arbeiten traten immense Reibungsverluste bei zentralen Unternehmensprozessen zutage, wenn diese nicht digitalisiert abliefen, sondern an papierbasierte Dokumente geknüpft waren. Ein Kernproblem: Bei mobiler Arbeit aus dem Home-Office heraus ist es nicht möglich, schnell zur Bürotür nebenan zu gehen, um einen Kollegen nach einer lokal abgelegten oder gar ausgedruckten Akte zu fragen.

Warum kompliziert, wenn es auch einfach geht?

Die Frage, die jetzt beantwortet werden muss, lautet: Wie wird mit all den Dateien und Chatnachrichten, also Informationen, die in den neuen Werkzeugen liegen, nach Corona umgegangen? Wie werden diese Werkzeuge in die Gesamt-IT-Landschaft eines Unternehmens integriert? Die Zusammenführung von strukturierten Daten, unstrukturierten Dokumenten und den dazugehörigen betriebswirtschaftlichen Anwendungen ist Aufgabe für ein Enterprise Information Management System (EIM).

Ein solches System dient nicht nur als zentrale Plattform für den zeit- und standortunabhängigen Zugriff auf alle notwendigen Informationen, sondern bietet auch optimierte Workflows, welche die digitale Zusammenarbeit verbessern. Bei der Auswahl des richtigen EIM-Systems ist der Faktor Einfachheit indes höher denn je einzustufen. Ein System, das aufwendig zu administrieren und für den Anwender kompliziert zu nutzen ist, ist heute schlichtweg unbrauchbar. Zu hoch wäre der Abstimmungs-, Schulungs- und Anpassungsaufwand in Zeiten des dezentralen Arbeitens. Doch welche Faktoren machen ein EIM eigentlich einfach? Die Aspekte Bedienung, Flexibilität, Berechtigungen, Integration und Skalierbarkeit sollten hierbei besonders berücksichtigt werden.

ÜBER EIN STRUKTURIERTES UND ZENTRALES INFORMATIONSMANAGEMENT ZU VERFÜGEN, SOLLTE DAS ZIEL EINES JEDEN UNTERNEHMENS SEIN.

Michele Barbato, Abteilungsleiter Produktmanagement, Ceyoniq Technology GmbH, www.arbeitneuentdecken.com

Bedienung: Intuitiv und übersichtlich

Moderne EIM-Systeme müssen selbsterklärend und intuitiv bedienbar sein. Übersichtliche Anwenderoberflächen sind ein Muss, egal in welcher Arbeitsumgebung eine Software genutzt wird. Dies sollte auch für Nutzer mit Handicap gelten, was durch die Umsetzung der Normen der Barrierefreiheit wie DIN EN ISO 9241- 171 und BITV 2.0 innerhalb des EIM gewährleistet wird.

Ein entscheidender Aspekt in Sachen Einfachheit ist die Geräteunabhängigkeit. Nutzer müssen über verschiedene Clients auf das System zugreifen können, sei es über einen Desktop-Client, eine Explorer-Integration, eine Office-Integration oder einen Web-Client. Erst diese Flexibilität macht effektives mobiles Arbeiten möglich.

Enterprise-Berechtigungen

Ein leistungsfähiges System für das Informationsmanagement muss zudem mandantenfähig sein. Das beinhaltet die Vergabe verschiedener Benutzerrollen, durch

die ein mitarbeiterspezifischer Zugriff auf Inhalte ermöglicht wird, gepaart mit individuellen Bearbeitungsrechten. Welche Daten dürfen von allen Nutzern eingesehen werden, welche sind nur für bestimmte Anwendergruppen vorgesehen?

Vielschichtige Berechtigungskonzepte schaffen die Voraussetzungen, um auch bei digitalen Informationsmanagementprozessen Konformität zu Compliance-Regeln wie Datenschutz und Informationssicherheit zu gewährleisten – unabhängig vom Arbeitsort und Endgerät der beteiligten Mitarbeiter.

Integration

Bei der Verzahnung mit anderen Anwendungen zeigt sich: EIM-Systeme sind für reibungsloses Arbeiten wie Wasser für den menschlichen Körper – unsichtbar, aber auch unverzichtbar. Denn bei der Arbeit mit verschiedenen Programmen, wie etwa SAP, braucht man schnell einen Zugriff auf eine digitale Akte mit allen E-Mails, Eingangs- und Ausgangsschreiben. Daher müssen EIM-Systeme viele verschiedene und verlässliche Schnittstellen und Industrie-Standards unterstützen. Damit kann jedem Anwender die Information, die er für seine Arbeit oder Entscheidungen braucht, vollständig, verifiziert und auf den Punkt gegeben werden.

Sind die genannten Voraussetzungen geschaffen, wird die Optimierung und Automatisierung wichtiger Geschäftsprozesse durch das EIM-System möglich. Und gerade die Unterstützung zentraler Workflows bietet eine massive Vereinfachung und eine hohe Automatisierung, die Unternehmen durch den Einsatz der richtigen Software-Lösung realisieren können.

Automatisierung

Gemeint sind alltägliche Geschäftsprozesse, beispielsweise in den Bereichen Vorgangsbearbeitung, Personalmanagement, Rechnungswesen oder Vertragsmanagement, bei denen Mitarbeiter oft abteilungs- und standortunabhängig auf sensible Informationen, Dokumente und Akten zugreifen müssen. Hier unterstützt das System die effiziente Abfolge einzelner Prozessschritte und stellt den berechtigten Mitarbeitern durchgängig alle benötigten Informationen digital an einem zentralen Ort bereit. Der Einsatz von Software-Robotern ist dann nicht mehr notwendig, um einen hohen Automatisierungsgrad zu erreichen.

Skalierbarkeit

Um den vielseitigen Anforderungen in volatilen Zeiten gerecht zu werden, müssen moderne Informationsplattformen zudem ein Höchstmaß an Stabilität bieten. Klar: Das Kriterium der einfachen und reibungslosen Anwendung ist mit einem Systemausfall schwer in Einklang zu bringen. Das heißt, dass auch ansteigende Datenvolumina oder Benutzerzahlen einer performanten und stabilen Datenverarbeitung nicht im Wege stehen dürfen.

Server-Komponenten führender EIM-Systeme können deshalb beliebig skaliert und ausfallsicher ausgelegt werden. Der Einsatz von Containertechnologie unterstützt dabei nicht nur die Resilienz des Systems, sondern erhöht zusätzlich die Skalierbarkeit von EIM-Diensten.

Fazit

Über ein strukturiertes und zentrales Informationsmanagement zu verfügen, sollte das Ziel eines jeden Unternehmens sein. Denn nur so kann jeder Anwender zu jeder Zeit von jedem Ort und mit jedem Endgerät auf alle wichtigen Informationen für seinen Arbeitsprozess zugreifen. Wie wichtig dies ist, hat die Corona-Krise deutlich gezeigt. Ein zentrales Informationsmanagement ist nachhaltig und gibt jedem Unternehmen die Flexibilität, die Mitarbeiter zielgerichtet zu unterstützen und ohne Informationslecks arbeiten zu lassen. So entsteht Einfachheit – gerade in schwierigen Zeiten ein echter Erfolgsfaktor.

Michele Barbato

EINKAUF UND BUCHHALTUNG

DIE RICHTIGEN STELLSCHRAUBEN ZUR ENTLASTUNG DREHEN

Angesichts großflächiger Home-Office-Arbeit treiben Unternehmen derzeit im Eiltempo die Digitalisierung und Automatisierung dokumentenbasierter Geschäftsprozesse voran. Damit die Beschäftigten von ihren Arbeitsplätzen zuhause aus unterbrechungsfrei und abteilungsübergreifend zusammenarbeiten können, überprüfen viele Bereiche bereits intensiv, inwieweit Prozesse digitalisiert und automatisiert werden können. Dies betrifft den Einkauf ebenso wie Rechnungsprüfungs- und Zahlungsprozesse. Zusammen spricht man von Procure-to-Pay oder kurz P2P, das heißt von durchgängigen Prozessen, die von der Erstellung einer Bedarfsmeldung bis zur revisionssicheren Rechnungsablage reichen.

P2P heißt nicht automatisch papierlos

Setzen Unternehmen zum Beispiel auf ein ERP-System wie SAP, sollten sich solche ganzheitlichen P2P-Arbeitsabläufe möglichst direkt innerhalb des Systems durchführen lassen – was aber nicht heißt, dass sie damit automatisch schon gänzlich papierlos stattfinden. Workflow- und Prozesslösungen wie die der xSuite Group übernehmen daher die Digitalisierung und sorgen außerdem dafür, dass dokumentenbasierte Prozesse durchgängig automatisiert in SAP abgebildet werden.

Denn sieht man einmal genauer hin, sind die klassischen P2P-Abläufe heute auch noch oft viel weniger digital oder automatisiert, als man zunächst annehmen könnte. Einkaufs- und Buchhaltungsabteilungen sind in der Regel sehr gut organisiert und haben ihre Papierprozesse bereits bis zum Äußersten optimiert. Hohe Compliance-Anforderungen, eine stetig steigende Anzahl zu bearbeitender Vorgänge und schwer nachzubesetzende offene Stellen, dazu noch die steigende Tendenz zum Home-Office – all dies lässt die Arbeitsbelastung in den betroffenen Abteilungen stetig ansteigen.

Digitalisierung startet bei der Bedarfserfassung

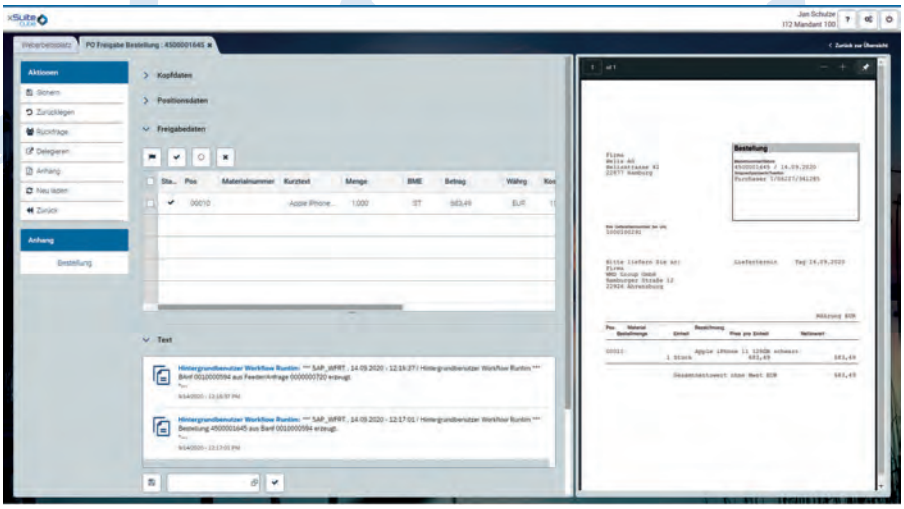
Ein effizientes Arbeiten auch auf Dauer sicherzustellen, bedeutet, die operativen Geschäftsprozesse so weit wie möglich zu digitalisieren und damit Einkauf und Buchhaltung zu verbinden. Arbeitsergebnisse lassen sich auf diese Weise verbessern und gesteckte Zielvorgaben leichter erreichen.

Potenziale für eine Digitalisierung und Automatisierung verbergen sich in vielen einzelnen Arbeitsschritten über den gesamten P2P-Prozess hinweg. Bei der Bedarfserfassung mit SAP können Anfragen mit Hilfe eines Workflows digital erstellt werden. Indem die Bedarfsmeldung bereits digital eingeht, liegen dem Einkauf alle Informationen standardisiert und zentral vor. Auch die nächsten Schritte – Wer soll die Anfrage zur Prüfung und Freigabe vorgelegt bekommen? – können mittels Workflow automatisiert werden. Auftragsbestätigungen durch den Lieferanten, Rechnungseingang, -prüfung und -freigabe bergen zusätzliches Potenzial, wenn dort Daten aus eingehenden Bestätigungen oder Rechnungen automatisiert nach SAP übernommen werden.

Schneller verarbeiten, eher bezahlen

Es zeigt sich: Viele Arbeitsschritte in operativen P2P-Prozessen sind Kandidaten für eine Automatisierung. Voraussetzungen dafür sind stets eine Digitalisierung eingehender Dokumente, die Extraktion der Daten aus ihnen und deren automatische Übertragung ins ERP-System. Workflowgestützte Automatisierung der P2P-Prozesse spart zunächst einmal Zeit und Aufwand. Unternehmen profitieren jedoch von weiteren Vorteilen: höhere Transparenz, besserer Auswertbarkeit und mehr Sicherheit. Und weil Automatisierung zu schnellerer Verarbeitung, das heißt Bezahlung führt, spart man durch Skontogewinne auch noch bares Geld.

Dina Haack | www.xsuite.com



Freigabe einer Bestellung in SAP

Bildquelle: xSuite Group

READY FOR THE FUTURE

FLEXIBEL, ZUKUNFTSSICHER UND BEREIT FÜR INDUSTRIE 4.0

Die Promet AG mit Hauptsitz in Kirchberg (Schweiz) und einem Produktionsstandort in Deutschland fertigt von kleinen flexiblen Kupferverbindungen für Batterien der E-Mobility bis zu 2 Tonnen schweren Baugruppen sämtliche Teile mit höchstmöglicher Automatisierung. „Als wettbewerbsfähiges Unternehmen muss man sich heute immer schneller neuen Marktbedürfnissen anpassen. Das ERP- System ist eines der wichtigsten Instrumente, um diese Bedürfnisse abzubilden. Blindleistung im Innendienst können wir uns nicht erlauben, deshalb sind wir stetig darauf bedacht Optimierungen durchzuführen, insbesondere innerhalb unserer Software-Prozesse." findet Roger Graf, CEO der Promet AG.

shutterstock.com/rawpixel.com

Übersichtlich und transparent

Seit 2011 hat der Spezialist von Energietechnik-Lösungen deshalb das modulare und flexible caniasERP im Einsatz. Als produzierender Betrieb liegt der Fokus der Systemnutzung vor allem in der Produktionsplanung, das konnte das System der Industrial Appliction Software (IAS) GmbH perfekt abdecken. „IAS unterstützt uns in diesem Bereich vorbildlich, kann sich gut in praktische Abläufe hineinversetzen und diese entsprechend umsetzen", lautet das Urteil von Roger Graf.

Der große Nutzen liegt für das Unternehmen in der Übersichtlichkeit und Transparenz der Fertigungsaufträge: „Heute gehen bei Promet im Durchschnitt pro Tag circa 300 unterschiedliche Fertigungsaufträge in Produktion. Sämtliche Arbeitsschritte werden in Echtzeit zurückgemeldet", erläutert Roger Graf. Dabei ist vor allem Industrie 4.0 ein prioritäres Thema: „Wir leben Industrie 4.0. Unsere Roboter und vollautomatischen Fertigungszellen produzieren im 24h Betrieb Busbars aus Kupfer und Aluminium, ohne dass auch nur ein Mitarbeiter anwesend sein muss. Die Aufträge und Artikel werden einmal erfasst und anschließend mannlos hergestellt. Und auch die Rückverfolgung kann so zu 100 Prozent sichergestellt werden."

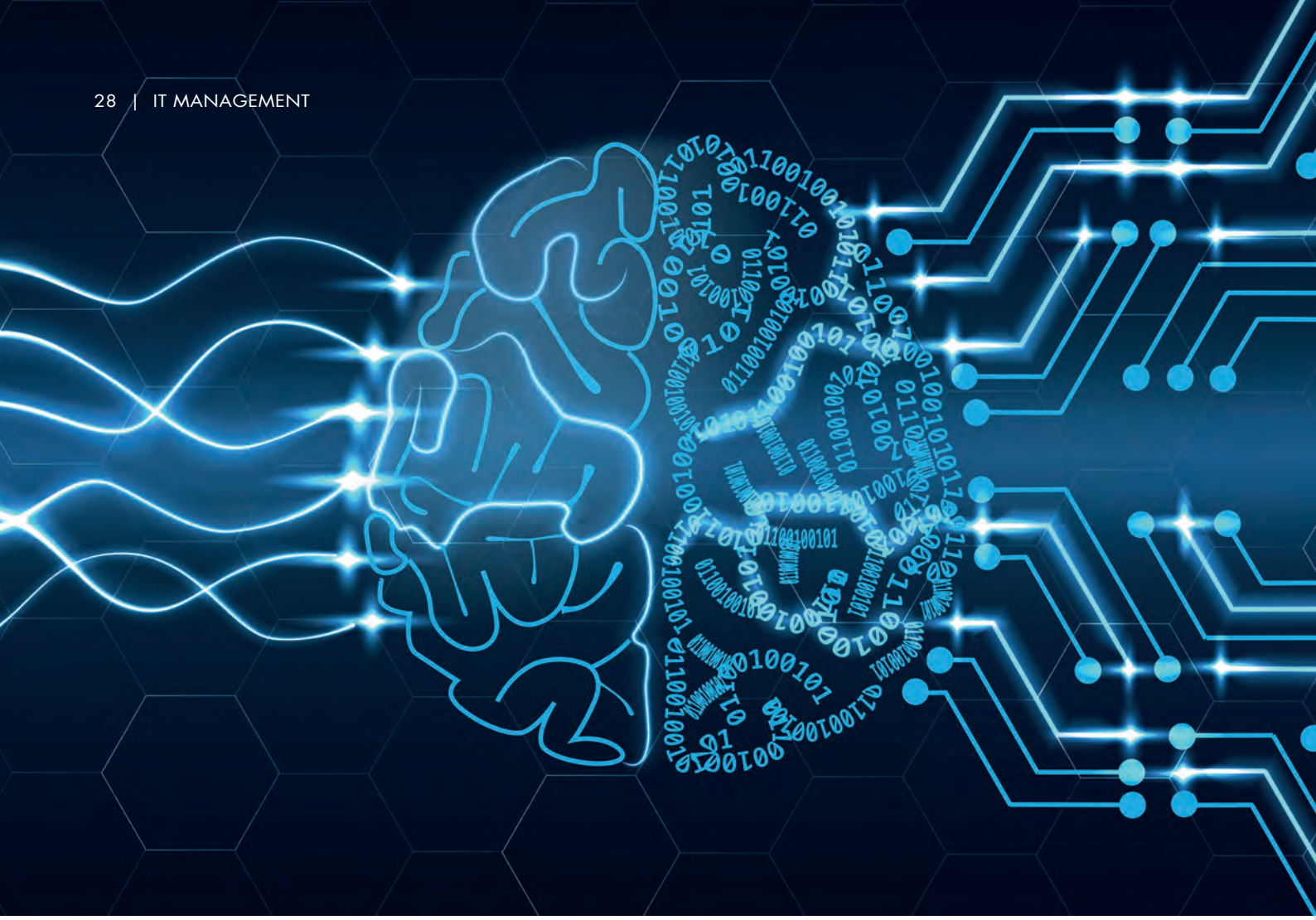
Smart Factory mit canias4.0

Industrie 4.0 und damit verbundene technologische Entwicklungen bergen in Zeiten von Schnelllebigkeit, hohem Wettbewerbs- und Kostendruck hohe Potenziale, um Unternehmen zukunftssicher und leistungsstark zu machen. IAS hat sich deshalb mit daraus entstehenden Fragen auseinandergesetzt und sukzessive eigene Lösungen entwickelt: Wie können große Datenmengen gesammelt und strukturierbar gemacht werden? Wo können Daten gespeichert werden, um sie effizient zu nutzen? Wie können Daten bestmöglich für Analysezwecke eingesetzt werden? Und: wie kann mit gesammelten Daten das System gesteuert werden? Die Antwort auf diese Fragen vereint die IAS nun in einer Industry4.0 Lösung, die das ERP-System mit IoT und Big Data vereint: canias4.0.

Zur Sammlung und Strukturierung großer Datenmengen wurde eine eigene IoT-Technologie entwickelt, die in die ERP-Module integriert ist. Das Datenbankverwaltungssystem iasDB macht die Datenbankseite noch konformer und leistungsfähiger, beseitigt Beschränkungen und schafft so eine flexible und erweiterte Struktur auf der Anwendungsplattform. Mit dem caniasIQ-Modul können die erforderlichen Daten etwa für strategische Entscheidungen multidimensional ausgewertet und visuell aufarbeitet werden. Somit können die Daten zentral analysiert und unabhängig von den Ressourcen gesammelt werden. Und über das Modul Business Process Management, das den Anwender bei der Modellierung, der automatischen Initiierung und anschließenden Auditierung der Prozesse im Unternehmen unterstützt, lässt sich das System steuern. Diese Lösung vereint hohe Flexibilität und Anpassungsfähigkeit mit modernsten Technologien.

www.canias40.de

canias4.0



INTELLIGENT AUTOMATION

WIE AUTOMATISIERUNGSLÖSUNGEN DIE MITARBEITERZUFRIEDENHEIT STEIGERN

Die Digitalisierung – obwohl inzwischen fast Alltag – bringt einen Wandel mit sich, der bei vielen Mitarbeitern Ängste auslöst. Dazu gehören auch neue Technologien, die Aufgaben und Prozesse automatisieren. Die Arbeit vieler Mitarbeiter, so scheint es, könnte damit überflüssig werden. Aber stimmt das? Sehr viel wahrscheinlicher ist es, dass sich Jobs zwar verändern, Unternehmen ihre Mitarbeiter deswegen aber nicht entlassen. Denn Automatisierungstools sorgen dafür, dass Angestellte mehr Zeit für deutlich wertvollere Tätigkeiten haben als bisher. Intelligent Automation steigert sogar die Zufriedenheit der Mitarbeiter, weil sie sie von ungeliebten Aufgaben entlastet. Auch wenn Automatisierungstechnologien im ersten Moment oft Angst vor Jobverlust auslösen – tatsächlich eröffnen sie große Chancen. Für Unternehmen und ihre Mitarbeiter.

Wenn immer mehr Unternehmen sogenannte „Industrie 4.0-Lösungen" einführen, wirkt sich dies definitiv auf Jobs aus. Denn diese Tools werden immer intelligenter. Stand-Alone Robotic Process Automation-Lösungen, wie sie bereits bei vielen Unternehmen im Einsatz sind, genügen den Ansprüchen oft nicht mehr, da sie lediglich sehr einfache Tätigkeiten automatisieren können, wie etwa das Kopieren von Daten aus einem System in ein anderes. Solche RPA-Tools konnten die Arbeit vieler Mitarbeiter schon deutlich erleichtern, aber an vielen Stellen im Prozess musste der Mensch weiterhin aktiv eingreifen. Die neuen Intelligent Automation-Plattformen sind dagegen in der Lage, Prozesse vollständig zu automatisieren.

Angst vor KI

Zu diesen Plattformen gehören in der Regel RPA-Lösungen der nächsten Generation, die um Künstliche Intelligenz und Machine Learning-Funktionalitäten erweitert sind. Eine Intelligent Automation-Plattform ist einem einfachen RPA-System deutlich überlegen. Entsprechend wächst die Sorge der Mitarbeiter, ihr Arbeitgeber könne sie bald vollständig durch KI-Lösungen ersetzen. Auch dies hält manche Unternehmen davon ab, Automatisierungslösungen in ihre IT zu integrieren. Sie möchten wertvolle Mitarbeiter – zumal angesichts des wachsenden

Fachkräftemangels – nicht verunsichern und verlieren. Doch Untersuchungen wie die Dell & Intel Future Workforce Study belegen, dass in Unternehmen, die nicht in neue Technologien investieren, genau das Gegenteil eintritt: 42 Prozent der Millennials sind eher bereit, ein Unternehmen zu verlassen, wenn es veraltete Technologien einsetzt. Gleichzeitig fallen solche Unternehmen natürlich gegenüber ihren Wettbewerbern deutlich zurück.

Die Ansprüche der Arbeitnehmer wachsen

Die Studie unterstreicht zudem den Wandel im Personal-Bereich – Stichwort Fachkräftemangel. Immer häufiger können sich Arbeitnehmer ihre Jobs aussuchen. Wer als Unternehmen nicht aktiv auf potenzielle Mitarbeiter zugeht, hat das Nachsehen. Für die HR-Abteilung ist es eine große Herausforderung, das Unternehmen als attraktive Arbeitgebermarke zu positionieren. Auch darum wird es für Unternehmen entscheidend, neuen Technologien gegenüber offen zu sein und sich den veränderten Möglichkeiten agil anzupassen – gerade wenn die neuen Tools oder Geräte die Mitarbeiter bei ihrer täglichen Arbeit unterstützen können. Durch solche Systeme verschaffen Unternehmen ihren Mitarbeitern nicht nur mehr Zeit für wertschöpfendere Arbeiten, sondern auch für ihre Weiterentwicklung. Während die virtuellen Kollegen – etwa die Software-Roboter von RPA – lästige, repetitive Aufgaben übernehmen, können sich Angestellte darauf konzentrieren, ihr Wissen zu erweitern, Kunden besser und intensiver zu betreuen und die Kundenzufriedenheit zu steigern.

Mitarbeiter mitnehmen

Unternehmen müssen aber nicht nur neue Mitarbeiter und Millenials für sich gewinnen, es gilt genauso, die älteren Mitarbeiter mit an Bord zu holen. Einfach neue Tools einzuführen und die Mitarbeiter dabei vor vollendete Tatsachen zu stellen, kann sogar eine Art Rebellion hervorrufen. Nur ein konsequentes Change Management führt den Prozess des technologischen Wandels zum Erfolg. Denn gerade langjährige Mitarbeiter sind von neuen Prozessen, Tools oder Strukturen nicht leicht zu überzeugen. Sie schätzen Altbewährtes und tun sich schwer, sich auf Neues einzulassen. Deshalb ist es unerlässlich, Angestellte von Beginn an in Digitalisierungsprozesse einzubeziehen und für ihre Partizipation an den Veränderungsprozessen zu sorgen. Im Sinne eines umfassenden Change Managements müssen Unternehmen neue Strukturen, Prozesse oder Systeme mit ihren Mitarbeitern abstimmen. Neben dem Hinweis, was diese Tools alles leisten, ist es wichtig, die allgemeine Veränderung im Wettbewerbsumfeld zu vermitteln: Sich der Digitalisierung und Automatisierung zu verschließen, kann für Unternehmen existenzbedrohend sein. Fest steht: Ängste kann man nur beseitigen, indem man offen darüber kommuniziert und ein klares „Wir"-Gefühl etabliert. Auch darf keine Kluft zwischen jüngeren und älteren Kollegen entstehen – oder zwischen den alten, etablierten Prozessen und den völlig neuen. Darum hilft es, nicht revolutionär, sondern evolutionär zu agieren und Systeme und Prozesse schrittweise und möglichst für alle Mitarbeiter zu migrieren.

NUR EIN KONSEQUENTES CHANGE MANAGEMENT FÜHRT DEN PROZESS DES TECHNOLOGISCHEN WANDELS ZUM ERFOLG.

Chris Huff,
Chief Strategy Officer, Kofax,
www.kofax.de

Vorteile der Automatisierung aufzeigen

Durch Automatisierungsplattformen wandeln sich die Aufgaben der Mitarbeiter. Fürchten müssen sich sie vor ihren virtuellen Roboter-Kollegen aber nicht. Der Großteil der Aufgaben, den die Software-Roboter von ihren echten Kollegen übernehmen können, sind Tätigkeiten, die kaum ein Mensch gern erledigt. Etwa das Abrufen von Daten aus Hunderten von Portalen, um Preisvergleiche durchführen zu können, oder die Recherche nach der Liquidität eines Kunden, bei der Dutzende weitere Portale abzusuchen sind. Ähnliches gilt für das Kopieren von Daten von einem System in das andere. Wenn RPA und Intelligent Automation solche Sisyphos-Aufgaben übernehmen, sorgen sie für eine deutliche Arbeitserleichterung und reduzieren die unangenehmen Fehleingaben, die passieren können. Mit der Integration einer entsprechenden Software gehört das mühselige Kopieren der Vergangenheit an, und Mitarbeiter können sich auf deutlich wertvollere Aufgaben konzentrieren – wie etwa die Kundenberatung. Dadurch steigt nicht nur die Zufriedenheit der Kunden, sondern auch die der Mitarbeiter: Sie sehen mehr Sinn in ihrer Tätigkeit. Die Zeit, in Intelligent Automation zu investieren, ist definitiv gekommen. Nur Unternehmen, die sich dem digitalen Wandel stellen, werden sich am Markt behaupten. Dieser Wandel betrifft nicht nur die Technologie, sondern auch die Mitarbeiter. Es ist entscheidend, sie frühzeitig in Change-Prozesse einzubeziehen, um ihnen die Angst vor neuen Prozessen, Strukturen und Tools zu nehmen. Zudem können Unternehmen somit den Widerstand und dadurch resultierende Leistungsverluste kompensieren. Intelligent Automation schafft schließlich beides: ein wettbewerbsfähigeres Unternehmen und zufriedenere Mitarbeiter.

Chris Huff

Zusätzliche Informationen unter

HYBRIDES PROJEKTMANAGEMENT

Herausforderungen agiler Projekte in klassischen Organisationsstrukturen

Auf Captain Kirk kann man sich verlassen: auch in heiklen Situationen trifft er richtige Entscheidungen. An seiner Seite hat er Commander Spock – den strengen Logiker – und Dr. Leonard McCoy – den Arzt, der sich lieber auf sein Gefühl verlässt und eher aus dem Bauch heraus urteilt. Was lehrt uns Raumschiff Enterprise über hybride Projektmethoden? Ganz einfach: Ein gutes Team besteht aus Mitgliedern, die sich nicht unbedingt gleichen aber sehr wohl einander ergänzen. Je breiter das Spektrum des Teams, desto mehr Perspektiven und Lösungsmöglichkeiten gibt es.

Die positiven Synergieeffekte, die durch die Vielfalt von Captain Kirks Team offensichtlich werden, lassen sich auch auf den Einsatz und die Kombination verschiedener Projektmethoden anwenden, mithilfe derer Unternehmen inzwischen versuchen, der Geschwindigkeit des Wandels der Märkte und Technologien Herr zu werden.

Einerseits erhoffen sich Unternehmen durch die Einführung agiler Methoden eine stärkere Ausrichtung auf Kundenwünsche, andererseits dürfen sie ihre Stabilität als Organisation hinsichtlich der eigenen Firmenkultur, Veränderungsbereitschaft des Personals aber auch in Bezug auf Compliance-Vorgaben nicht verlieren. Wenig verwunderlich, dass aus diesen Gründen nur wenige EntscheidungsträgerInnen dazu tendieren, sofort ins kalte Wasser zu springen. Zu groß ist das Risiko, dass nicht jeder Bereich des Unternehmens agile Methoden unterstützen kann oder nicht jedes Projekt für eine solche Methode geeignet ist. Hybride Prozessmodelle bieten somit für Unternehmen eine Möglichkeit, agile Projektmanagement-Ansätze in sonst eher klassischen Kontexten zu pilotieren. Doch welche Hindernisse sind in solchen Projekten zu erwarten und wie können diese am besten überwunden werden?

Synergien nutzen

Hybride Projektmethoden bieten die Chance, von den Vorteilen beider Komponenten zu profitieren. Klassische Ent-

wicklungsmethoden wie das V- oder auch Wasserfallmodell lassen sich verhältnismäßig verbindlich planen und steuern. Die Vorzüge agiler Entwicklungsmethoden wie der Scrum liegen eher darin, dass man sich durch die stetige Regelmäßigkeit immer wiederkehrender Zeremonien innerhalb kurzer Intervalle proaktiv austauschen und auf bestimmte Themenschwerpunkte konzentrieren kann. Dadurch können Kundenwünsche noch während der Umsetzung einfacher eingebunden werden. Beides lässt sich kombinieren: Feste Projektvorgaben wie zum Beispiel Projektstart- und -endetermin sorgen für ausreichend Planungssicherheit und das agile Vorgehensmodell sorgt für die notwendige Flexibilität hinsichtlich der Anforderungen, die dann tatsächlich umgesetzt werden.

Sorgfältige Vorbereitung

Wird in einem Unternehmen mit klassischen Softwareentwicklungsmethoden ein agiles Pilotprojekt geplant, ist die Schulung des Personals oft die naheliegende Vorbereitungsmaßnahme, da es den zukünftigen Teammitgliedern an Erfahrung mit der neuen Projektmethode fehlt. Um den Projektstart optimal vorzubereiten, sollten darüber hinaus weitere Herausforderungen bedacht und geklärt werden:

- Wie wird damit umgegangen, wenn ein Teil der Anforderungen durch andere (nicht agil arbeitende) Abteilungen umgesetzt werden muss? Wenn die Zeitpunkte der Entwicklungs- und Testphasen voneinander abweichen, sollten diese gleich zu Projektbeginn miteinander abgestimmt werden, um einen möglichst reibungslosen Ablauf zu gewährleisten.

- Welche Möglichkeiten gibt es, die Arbeit des wahrscheinlich noch unerfahrenen Projektteams zu unterstützen? Es gibt einige einfache Tricks mithilfe derer dem Team der Spagat zwischen agilen und klassischen Entwicklungsmethoden einfacher gelingen wird, zum Beispiel:

- Dem Team bei Bedarf einen agilen Coach zur Verfügung stellen. Dieser hilft nicht nur als methodischer Ansprechpartner bei Unsicherheiten zur Vorgehensweise, sondern kann bei notwendigen Entscheidungen auch als Schnittstelle zwischen Projektteam und Geschäftsführung fungieren.

- Bei Pilotprojekten: Kostenlose Online-Tools zur Projektorganisation nutzen, etwa Freemind zur Strukturierung aller offenen Projektfragen; miro (Collaboration Tool), um Whiteboards im gemeinsamen Projektraum zu ersetzen, oder auch Mentimeter, das bei der Retrospektive unterstützen kann.

- In agilen Projekten wird die Rolle des Product Owners (PO) oft mit einem Requirements Engineer besetzt. Mit dem Rollenwechsel ändern sich auch die Tätigkeitsfelder. Product Owner erhalten beispielsweise zusätzlich die Aufgaben eines Project Controllers und arbeiten nicht mehr nur rein auf die Umsetzung von Anforderungen hin, sondern stellen aufgrund der neuen Aufgaben auch sicher, dass das Projektbudget eingehalten wird. Gerade in hybriden Projektmanagement-Ansätzen kann es dadurch zu Rollenkonflikten kommen.

UNTERNEHMEN, DIE AGILE PROJEKTMANAGEMENT-METHODEN IN EINEM KLASSISCHEN ENTWICKLUNGS-RAHMEN AUSPROBIEREN WOLLEN, KÖNNEN VON DEN ERFAHRUNGEN ANDERER FACHLEUTE PROFITIEREN – UND DAS NICHT IRGENDWANN IN EINER FERNEN ZUKUNFT, SONDERN GENAU JETZT.

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

Wie können derlei Konflikte vermieden werden? Sowohl bei Auftraggebern als auch allen Projektbeteiligten sollte das gleiche Rollenverständnis vorhanden sein, um die Erwartungshaltung beiderseitig erfüllen zu können. Dieses sollte noch vor Projektstart offen – vielleicht in einem Workshop – diskutiert, ein gemeinsames Verständnis gefunden und dieses dann auch verbindlich festgehalten werden.

- In klassischen Entwicklungsprojekten sind Auftraggeber häufig Fixpreis-Angebote gewohnt. Befindet sich ein Unternehmen noch in der Aufwärmphase mit agilen Projekten, fällt es Auftraggebern meist schwer, von ihrer Verhaltensweise abzuweichen und ergebnisoffen an ein Pilotprojekt heranzugehen. Die gängigste Erwartung ist daher, dass das gesetzte Budget für eine bestimmte Zielvorgabe ausreicht. Welche Praktiken können Product Ownern dabei helfen, das Projektbudget einzuhalten?

- Die Aufwandsschätzung für das agile Entwicklungsprojekt sollte großzügiger als nach klassischen Entwicklungsmethoden angesetzt werden. Es gibt hier verschiedene Einflussfaktoren, etwa der Erfahrungsgrad des Projektteams mit der neuen agilen Entwicklungsmethode, die Anzahl der Team-Mitglieder, ihre Verfügbarkeit während des Projektverlaufs oder auch die Komplexität der Anforderungsblöcke. Zur reinen geschätzten Entwicklungszeit empfiehlt sich ein Puffer von 15-20 Prozent. In dieser Zeit können Team-interne Meetings, das Kennenlernen der Vorgehensweise, aber auch die zahlreichen Abstimmungen mit dem Kunden stattfinden.

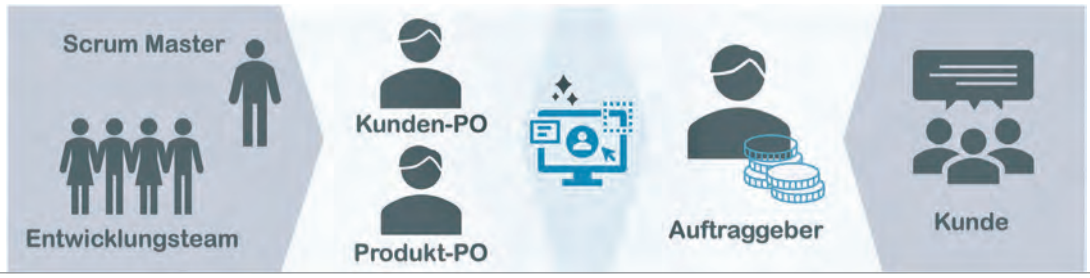


Bild 1: Rollen in einem agilen Projekt.

- Bei Sprint-Reviews sollte der Auftraggeber immer mit dabei sein, damit er
  - den Entwicklungsstand besser versteht und erkennt, warum das Umsetzen ausstehender Anforderungen valide ist,
  - die Ursache eventueller Budget-Nachforderungen besser nachvollziehen kann und
  - Probleme frühzeitig identifizieren und mit dem Team besprechen kann.
- Regelmäßige Status-Meetings wie beim klassischen Projektmanagement einplanen, um über Budget und Zeit (Ist und Soll) zu berichten. Wenn nötig, sollten optionale Produktanforderungen aus dem Projekt Scope entfernt werden.

Auch das regelmäßige Refinement des Projekt Scopes über die Priorisierung des Product Backlogs sorgt für die erforderliche Flexibilität im Falle von Engpässen. Es zielt darauf ab, sich auf die wichtigsten Features des Produkts zu konzentrieren und gegebenenfalls Kann-Anforderungen außen vor zu lassen.

Rahmenbedingungen festlegen

Es ist nicht einfach, die Vorzüge beider Ansätze geschickt miteinander zu kombinieren. Eine der wesentlichsten Herausforderungen stellt die firmeninterne Kommunikation dar. Ungenaue Vorgaben oder gar Missverständnisse können schnell dazu führen, dass das Projekt in Schieflage gerät. Um dem vorzubeugen, ist es wichtig, bereits vor Projektbeginn einen festgelegten Rahmen für das Projekt zu schaffen, der im gesamten Projektverlauf als Orientierungshilfe dient. So ist es vor allem wichtig:

- den Budget- und Zeitrahmen vorzugeben,
- eine von allen Beteiligten getragene Zielvision festzulegen,
- zu bestimmen, welche gesetzlichen oder anderweitig nominalen Vorgaben eingehalten werden müssen und

zu bestimmen, welche Technologien genutzt werden können oder sollen.

Bei der Festlegung der Zielvision sollte vor allem klar sein, welche Benutzerprobleme durch das zu entwickelnde Produkt gelöst werden sollen. Hierbei sollte nicht nur definiert werden, was im Projekt Scope enthalten ist, sondern auch, was außerhalb des Scopes liegt (also welche Anforderungen explizit nicht umgesetzt werden müssen oder sollen).

Bei agilen Projekten erfolgt die Kommunikation in einem iterativen Prozess.

Auftraggeber einbinden

Bei klassischen Entwicklungsmethoden wie dem Wasserfallmodell gibt es genau eine Phase, um Kundenfeedback einzuholen: die Überprüfungsphase. Hierbei gibt die verantwortliche Person auf Kundenseite Feedback zum Produkt und geht anschließend wieder ihren täglichen Aufgaben nach. Dies ist einer der größten Nachteile der klassischen Vorgehensmodelle. Oftmals glauben Auftraggeber, etwas Bestimmtes haben zu wollen, beauftragen es dann und stellen erst am Ende (nach der Entwicklung) fest, dass es gar nicht das war, was sie eigentlich brauchten. Und dann erfordert es weitere Aufwände, um diesen Fehler zu beheben.

Bei agilen Projekten erfolgen die Kommunikation und somit auch die Berücksichtigung der Kundenwünsche in einem iterativen Prozess. Deshalb ist es sowohl für hybride als auch für agile Projekte notwendig, von Kundenseite eine verantwortliche Person („Kunden-Product Owner") zu bestimmen, die regelmäßig durch den Product Owner auf Herstellerseite in den Entwicklungsprozess eingebunden wird. Auftraggeber an die veränderten Prozesse zu gewöhnen, kann dabei eine weitere Herausforderung darstellen, da die Zusammenarbeit viel enger abläuft als in einem reinen Freigabeprozess wie er bei klassischen Methoden durchgeführt wird. Doch die Umstellung lohnt sich.

Nimmt der Kunden-PO während des Projekts an den Daily Scrums teil, kann er von den Vorteilen der agilen Projektführung am meisten profitieren. Er erhält einen besseren Einblick ins Entwicklungsgeschehen und kann jederzeit auf die Priorisierung

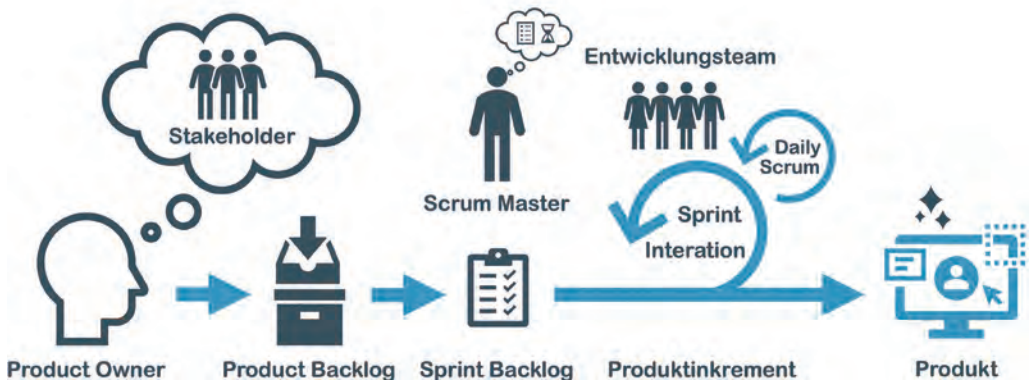


Bild 2: Scrum-Methode grafisch zusammengefasst.

von Anforderungen sowie zentrale Entscheidungen (z. B. zur Definition des Minimal Shippable Product) Einfluss nehmen. Idealerweise ist der Kunden-PO über den Rollout des Produkts hinaus für das Produkt verantwortlich und in alle nachgelagerten Prozesse involviert. So kann er auch bei Aktivitäten wie Schulungen, der Einführungsplanung und ähnlichen Aktivitäten unterstützend tätig sein.

Empfehlung für den Projektstart: Vorbereitungsphase einplanen

Nach dem Festlegen der Rahmenbedingungen sind Unternehmen oft versucht, sofort den Projekt-Kick-Off mit dem gesamten Team zu organisieren und die Entwicklung zu starten. Doch gerade in dieser Phase ist es wichtig, sich noch etwas in Geduld zu üben und genügend Vorbereitungszeit (noch vor Sprint 0) einzuplanen. Es empfiehlt sich hierfür ein Zeitrahmen von etwa zwei bis vier Wochen je nach Projektumfang. In dieser Zeit kann sich der Product Owner in die Domäne einarbeiten, Fragen zu Anforderungen mit dem Kunden-PO klären, Anforderungen in Epics und User Stories schneiden, das Backlog priorisieren und als Folge den Projekt-Kick-Off mit allem nötigen Hintergrundwissen optimal vorbereiten.

Die Enterprise ist viele Lichtjahre von der Erde entfernt im Weltall unterwegs, um fremde Welten zu entdecken. Doch ein solches Wagnis müssen Unternehmen, die agile Projektmanagementmethoden in einem klassischen Entwicklungsrahmen ausprobieren wollen, gar nicht eingehen. Sie können von den Erfahrungen anderer Fachleute auf diesem Gebiet lernen – und das nicht irgendwann in einer fernen Zukunft, sondern genau jetzt. Unternehmen, die gewillt sind, sich darauf einzulassen, werden besser auf sich schnell wandelnde Märkte eingehen können und je nach Ausrichtung ein Gleichgewicht zwischen festgelegten Zielen oder Meilensteinen und der dynamischen Weiterentwicklung ihrer Produkte erreichen.

Alexa Ziesch

Dieser Artikel betrachtet vor allem die organisatorischen Herausforderungen des hybriden Projektmanagements. In der nächsten Ausgabe folgt die Betrachtung der veränderten Arbeitsumgebung eines Requirements Engineers in einem solchen Projektmodell.

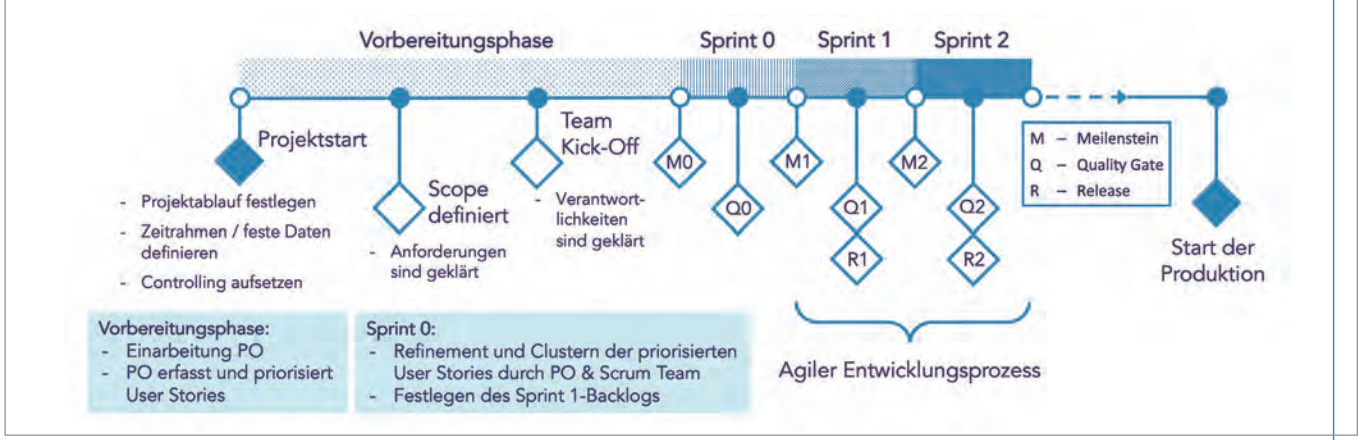


Bild 3: Hybrider Projektmanagement-Ansatz.

EINFÜHRUNG EINER MDM-LÖSUNG

DAS RICHTIGE PROJEKTMANAGEMENT IST GEFRAGT

Unter Mobile Device Management (MDM) versteht man eine IT-basierte, zentrale Verwaltung von mobilen Endgeräten wie Smartphones oder Tablets, die zum einen Transparenz und Sicherheit gewährleistet und zum anderen komfortable Schnittstellen für das Verwalten der Funktionalitäten auf den Geräten liefert.

In dem nachfolgend betrachteten Projekt ist das Ziel der Einführung einer solchen Mobile Device Management-Lösung die Schaffung einer Basis für sichere cloudbasierte, mobile Businessapplikationen durch Erfüllung der ISMS Standards (ISO27001/ISO27002) auf mobilen Endgeräten.

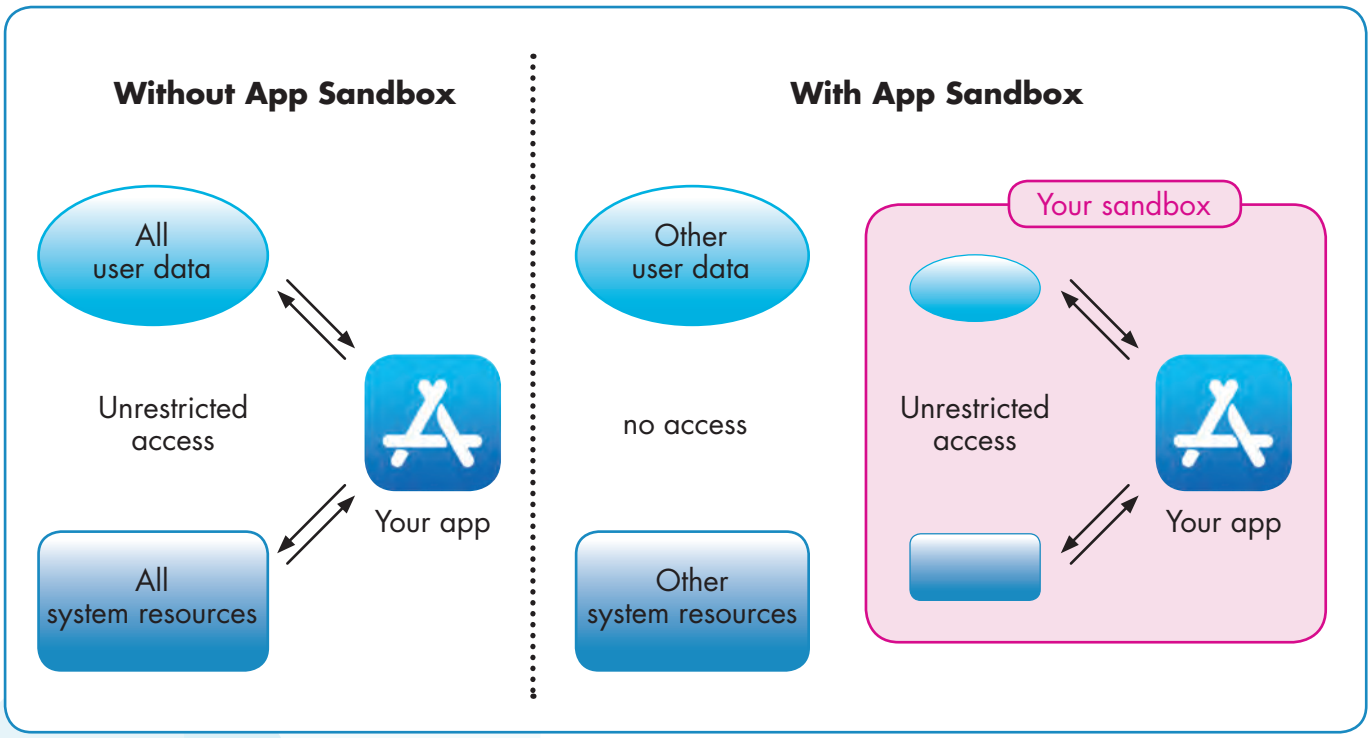
Dem Management ging es vor allem um den Ausbau und die Modernisierung der internen IT-Landschaft, deren Basis eine Cloudinfrastruktur ist, die den organisationsweiten Sicherheitsanforderungen entspricht. Neben den technologischen Fragen ist auch die hybride Organisation des Projekts spannend und zugleich herausfordernd: Während die IT-Abteilung und der beauftrage IT-Dienstleister bereits agil arbeiten, sind andere Geschäftseinheiten und Prozesse hingegen klassisch aufgestellt.

Sechs Punkte gilt es zu beachten:

1. Die Auswahl der Technologie war kniffelig. Warum?

Es gab mehrere Technologien zur Auswahl, die jeweils für unterschiedliche Anwendungsfälle sinnvoll sind. Deshalb war es für das Unternehmen enorm wichtig, vorab zu entscheiden, welchen Rahmen die Technologie abdecken und ob sie eine Gesamtplattform für den Anschluss weiterer Businessapplikationen sein soll. Dafür waren gründliche Überlegungen und ein detaillierter Ausblick in die Zukunft notwendig. Da Office 365 als Projekt bereits in Planung war, stand schnell fest, dass zukünftig eine Nutzung der Mobile Devices für Office 365 relevant sein würde.

Die Schwierigkeit bestand also zunächst darin, heute schon den Scope für morgen festzulegen und die Dringlichkeit der MDM Lösung zu beurteilen. Die Verantwortlichen richteten bei dem Projekt den Fokus auf die nachhaltige Umsetzung und nicht auf die Terminierung, wodurch



Die schematische Darstellung des Wirkungsprinzips einer MDM-Lösung. Quelle: 2016 Apple

die Entscheidung auf eine Anwendungslösung fiel, die im Aufbau zwar aufwändiger war, aber langfristig gesehen den Anforderungen des Unternehmens am besten entsprach.

Man dachte also von Anfang an in größeren Dimensionen und entschied sich dementsprechend für das umfangreichere Management-Tool. Die Auswahl der Microsoft-Technologie wirkte sich allerdings deutlich auf die Laufzeit des Projektes aus: Wir mussten Strukturen neu aufsetzen bzw. bestimmte Bereiche restrukturieren. Auch für den Dienstleister stellte sie ein nicht alltägliches Feld dar, was eine längere Vorbereitungszeit mit sich brachte.

2. Wie wurden die Requirements für das Projekt identifiziert?

Zu Beginn des Projekts wurden Workshops durchgeführt, in denen gemeinsam mit dem unternehmensinternen IT-Experten und dem IT-Dienstleister die Requirements identifiziert wurden. Im Rahmen dieser Workshops wurden die zukünftigen Nutzungsvorgaben für das Mobile Device Management festgelegt – beispielsweise welche Apps heruntergeladen werden dürfen oder wie mit Systemupdates umgegangen werden soll. Die klare Vorgabe des Managements lautete: Company Owned, Business Only – also eine rein geschäftliche Nutzung der Devices.

Besonderes Augenmerk lag auf den Sicherheitsbestimmungen und dem Datenschutz, aber auch auf Gesichtspunkten der Usability. Auf Basis der verschiedenen Perspektiven entstand ein Katalog an Requirements, der wiederum Grundlage für die Roadmap-Planung des Dienstleisters war. Oberste Priorität hatte zunächst einmal der Roll-out-Termin, an dem alle Mobile Devices der Mitarbeiter ausgetauscht werden sollten. Der Zeitplan sah vor, dass bis zu diesem Termin die geplanten Grundfunktionen laufen müssen: Telefonie, E-Mail und die Nutzung spezieller Unternehmens-Apps, beispielsweise individuelle Navigationslösungen des operativen Betriebs.

Darüber hinaus gab es weitere gewünschte Funktionen wie einen VPN-Zugang, deren Umsetzung aber auf einen späteren Zeitpunkt gelegt wurde. Den Fokus legten wir auf den Roll-Out und die Einhaltung dieses Termins. Wir wollten vermeiden, das Timing durch weitere für die Inbetriebnahme nicht zwingend notwendige Funktionen zu gefährden.

In seiner Roadmap-Planung legte der IT-Dienstleister auf Basis der Sprint-Planung fest, welche Funktionen in welchem Sprint realisiert werden sollen. Als Projektleiter habe ich diese Informationen erhalten und konnte genau überprüfen, ob die definierten Requirements umgesetzt wurden. Den aktuellen Projektstand konnte ich dadurch im Reporting auch für die Auftraggeber dokumentieren.

3. Wie lautet das größte Learning aus dem Schnittstellenmanagement zwischen den agilen Teams und dem klassischen Bereich?

Die meisten Bereiche des Unternehmens sind klassisch aufgestellt, die IT hingegen arbeitet überwiegend agil – ebenso der IT-Dienstleister. Als Projektleiter habe ich als Bindeglied zwischen der klassischen

und der agilen Welt fungiert und das Schnittstellenmanagement für diese beiden Bereiche organisiert. Aus der Zusammenarbeit lässt sich resümieren: In der Rolle des Schnittstellenmanagers muss der Projektleiter beide Welten kennen und verstehen.

Das klassische Projektmanagement muss ihm ebenso vertraut sein wie die Prinzipien agiler Projektführung. Entscheidend für einen harmonischen Ablauf ist dann in erster Linie die richtige Kommunikation. Er muss zwischen den Welten vermitteln und erforderliche Maßnahmen definieren. Im besagten Projekt hieß das beispielsweise, dass man verständlich machen musste, warum neu entstandene Anforderungen nicht einfach in einen laufenden Sprint eingefügt werden konnten.

Den klassisch arbeitenden Teams war oft nicht klar, dass wir in unser agiles Vorgehensmodell nicht willkürlich eingreifen und einen laufenden Sprint nicht einfach mit neuen Aufgaben belasten können. Dieses Vorgehen hätte die Zeitplanung ins Wanken gebracht und den Projekterfolg eventuell gefährdet. Sie mussten also erstmal verinnerlichen, dass neue Requirements zunächst bewertet und ins Backlog aufgenommen werden müssen und erst dann können sie – je nach Relevanz und Umfang – zu einem passenden Zeitpunkt umgesetzt werden.

Kommunikation ist der entscheidende Faktor im hybriden PM. Während des Projektverlaufs zeigte sich außerdem ganz deutlich, dass die bestehenden Kenntnisse der Unternehmens-IT in Sachen agilem Projektmanagement von großem Vorteil waren.

4. Welchen Stellenwert hatten die Aspekte Sicherheit und Datenschutz im Projekt?

Fragen wie „Wer bekommt welche Berechtigungen?" und „Welche Punkte müssen hinsichtlich Datenschutz beziehungsweise Datensicherheit berücksichtigt werden?" spielten bei der Umsetzung des Mobile Device Managements eine entscheidende Rolle. Im Falle eines Verlusts sollten die Geräte auf keinen Fall sensible Unternehmensdaten preisgeben. Der Wunsch war, dass die Hoheit über die Daten beim Unternehmen liege, damit sie im Notfall vor dem Zugriff Dritter geschützt sind. Der interne DSGVO-Experte beschäftigte sich intensiv mit Fragen zur Datensicherheit und zur Wahrung der Privatsphäre der Mitarbeiter. Er hat den gesamten Prozess eng begleitet und auch die Empfehlungen des Dienstleisters kritisch geprüft.

5. Welche Rolle hat das Testmanagement gespielt?

Das Testmanagement war ein sehr wichtiges Tool, um die Funktionalität der Devices sicherzustellen. Sobald die mobilen Geräte bereitgestellt wurden, erfolgten die ersten Usability-Tests, die parallel zur Weiterentwicklung durchgängig stattfanden. Die Testgruppe bestand aus einem sehr heterogenen Team an Usern. Durch die unterschiedlichen Tester-Perspektiven wurde sichergestellt, dass eine umfangreiche und individuelle Fallbetrachtung erfolgen konnte, um so möglichst viele Fehlerfälle zu identifizieren.

Die Tests wurden außerdem sorgfältig dokumentiert und die Ergebnisse wöchentlich an den Dienstleister übergeben. Die Umsetzung erfolgte sukzessive, war also nicht an das nächste Release gekoppelt. Auch vom Dienstleister selbst sind Vorab-Tests durchgeführt worden, um in den Releases ein aus IT-Sicht funktionierendes Produkt zur Verfügung zu stellen. Hatte er keine Beanstandungen mehr, wurde die Funktion zum Testen an die User-Gruppe gegeben.

Ziel des ausgefeilten Testings war es, kniffelige Punkte möglichst vorab zu finden, um dann beim Roll-out ein fehlerfreies

Attribut	Active Directory Federation Services	Pass-Through-Authentication	Password-Hash-Synchronization
Availablity	-	O	++
Operational complexity	--	-	+
Complexity of user management	+	+	-
Usability	O	O	O
Operating Costs	-	+	++
...			

Scoringmodell zur Auswahl des eingesetzten Authentisierungsverfahrens (Auszug).

Quelle: House of PM

Produkt an die Mitarbeiter geben zu können. Dadurch sollten aufwändige Hotfix-Aktionen und Optimierungsmaßnahmen nach der Inbetriebnahme des Systems vermieden werden. Die Strategie ging auf: Bis zum Zeitpunkt der Übergabe des Projekts im Juni 2020, gab es keine relevanten Fehlermeldungen oder eingeschränkte Funktionalitäten.

Für Unternehmen, die Mobile Devices in sicherheitskritischen Bereichen oder zur Aufrechterhaltung grundlegender Infrastrukturen einsetzen, ist eine solche Perfektion existenziell. Die Mobile Devices müssen jederzeit einwandfrei funktionieren, damit die Mitarbeiter – beispielsweise im Falle einer Störung von der Endkunden betroffen sind – erreichbar sind und bestmöglich agieren können.

6. Wie wurde die Organisation auf die Einführung des Mobile Device Management vorbereit beziehungsweise im Roll-out abgeholt?

Um alle Mitarbeiter von Anfang an gut zu informieren und abzuholen, existiertes eine klare Kommunikations- und Informationsstrategie. Zu diesem Zweck wurde die interne Kommunikation mit ins Boot geholt, die die Informationen zum Projekt zielgruppengerecht aufbereitet und an die jeweiligen Stellen in die Organisation getragen hat. Es gab verschiedene Kommunikationsmaßnahmen, wie beispielsweise FAQ und Wikis zur Nutzung der Mobile Devices und eine Installationsanweisung.

Zum Zeitpunkt der Inbetriebnahme fanden zusätzlich begleitete Termine statt, an denen immer jeweils vier Mitarbeiter teilnahmen. Dieser für alle verbindliche Termin diente dazu, die alten Mobiltelefone einzusammeln und die neuen Geräte herauszugeben. Alle relevanten Daten mussten übertragen und auf den alten Telefonen gelöscht werden. Danach wurde die neue Management-Lösung auf den ausgegebenen Telefonen installiert, und die Mitarbeiter erhielten eine Einführung in das System.

Dieser Prozess wurde bewusst eng begleitet. Wir wollten sicherstellen, dass die Deinstallation der alten und die Installation der neuen Geräte reibungslos abläuft, alle Daten wirklich gelöscht werden und keine Schwierigkeiten mit der Handhabung auftreten. Vorab wurde für alle Mitarbeiter eine Checkliste ausgegeben, die wir dann im Termin nochmal gemeinsam durchgegangen sind, damit nichts vergessen wird.

Durch diese umfangreichen Maßnahmen wurden alle Beteiligten sehr gut auf die Unternehmung vorbereitet, was eine komplikationsfreie Einführung des neuen Systems ermöglichte.

Fazit

Eine Mobile Device Management-Lösung ist nicht für jedes Unternehmen zwangsläufig sinnvoll. Bei der Auswahl der Technologie gilt es, verschiedene Aspekte in die Entscheidung miteinzubeziehen. Die Entscheider müssen abwägen, welche langfristigen Ziele sie mit der Einführung verfolgen und welche Strukturen dafür aus- oder aufgebaut werden müssen. Das ist notwendig, um eine realistische Zeit- und Projektplanung aufstellen zu können. Auch unterschiedliche Arbeitsweisen der involvierten Teams müssen bei der Planung berücksichtig werden. Arbeiten klassische und agile Teams zusammen, kann es zu Missverständnissen und Spannungen kommen. Kontinuierliche Kommunikation und transparente Projekt Abläufe helfen, um Konflikte zu vermeiden.

Frédéric Woschniak

> ZIEL DES AUSGEFEILTEN TESTINGS WAR ES, KNIFFELIGE PUNKTE MÖGLICHST VORAB ZU FINDEN, UM DANN BEIM ROLL-OUT EIN FEHLERFREIES PRODUKT AN DIE MITARBEITER GEBEN ZU KÖNNEN.
>
> Frédéric Woschniak, Project Manager, House of PM, www.house-of-pm.eu

DEVOPS ASSESSMENT

KICK-OFF FÜR AGILITÄT

Agilität ist zum Zauberwort in der IT geworden – und doch ist es schwer, festzustellen, wie weit ein Unternehmen auf diesem Weg bereits gekommen ist. DevOps gilt derzeit als der Königsweg zur Agilität. Kein Wunder also, dass DevOps Assessments zu einem Türöffner geworden sind. Doch – wie zuverlässig ist so eine Reifegrad-Bewertung, wer sollte sie durchführen und wie geht es danach weiter?

Braucht man wirklich DevOps?

Bevor man sich zu radikalen Umwälzungen im Unternehmen entscheidet, sollte man sich darüber klar werden, was man sich von DevOps erhofft und ob es auch wirklich in allen Bereichen passt. DevOps sorgt dafür, dass Software schneller und in kleineren Schritten aktualisiert und angepasst wird. Das muss aber nicht für jedes Unternehmen notwendig sein. Natürlich ist es von großem Wert, Operations in den Delivery-Zyklus zu integrieren und die Vorteile von Continuous Integration auszuschöpfen. Doch es gibt Fälle, in denen eine vollkommene DevOps Transformation einfach nicht passt. Das heißt nicht, dass die Prinzipien und Prozesse oder auch Tools von DevOps keinen Mehrwert bringen, das heißt nur, dass man auswählen sollte, was man wirklich umsetzen will.

Wenn das Geschäftsmodell nicht wirklich eine kontinuierliche Anpassung der Software erfordert, sondern nur minimale, unregelmäßige Releases, stellt sich die Frage, mit welchem Aufwand diese Änderungen umgesetzt werden. Hier kann ein Ansatzpunkt für Teilbereiche von DevOps sein, etwa für den Einsatz von Tools zur Release Automation. Auch wenn die Software Delivery Methode bereits den Anforderungen genügt, gibt es keinen Anlass, umzusteigen. Kurz, auch der Nicht- oder Teil-Einsatz von DevOps ist eine individuelle Entscheidung, die auch den Aufwand für Tools, Experten und andere operative Kosten in Betracht ziehen sollte. Der durch DevOps bedingte Wandel nimmt viele interne Ressourcen in Anspruch. Ein Unternehmen, das gerade in anderen Veränderungsprozessen steckt – etwa während eines Mergers – sollte sich die zusätzliche Belastung gut überlegen.

Doch wenn die Entscheidung für DevOps gefallen ist, sollte man es auch richtig tun!

Warum ein Outsider besser misst

Um einen Weg zu definieren, muss man wissen, wo man steht. Ein DevOps Assessment steht natürlicherweise am Anfang jeder Veränderung. Es besteht letztlich aus einem Set aus Fragen an verschiedene Unternehmensbereiche, die sich immer um Menschen, Prozesse und Tools drehen. Das Ziel ist klar: die Brüche und Lücke zu identifizieren, die einen sicheren und erstklassigen DevOps Prozess verhindern und eine Roadmap mit KPIs und Milestones zu entwickeln, wie diese behoben werden können. Die nächste Frage ist: Wer macht's?

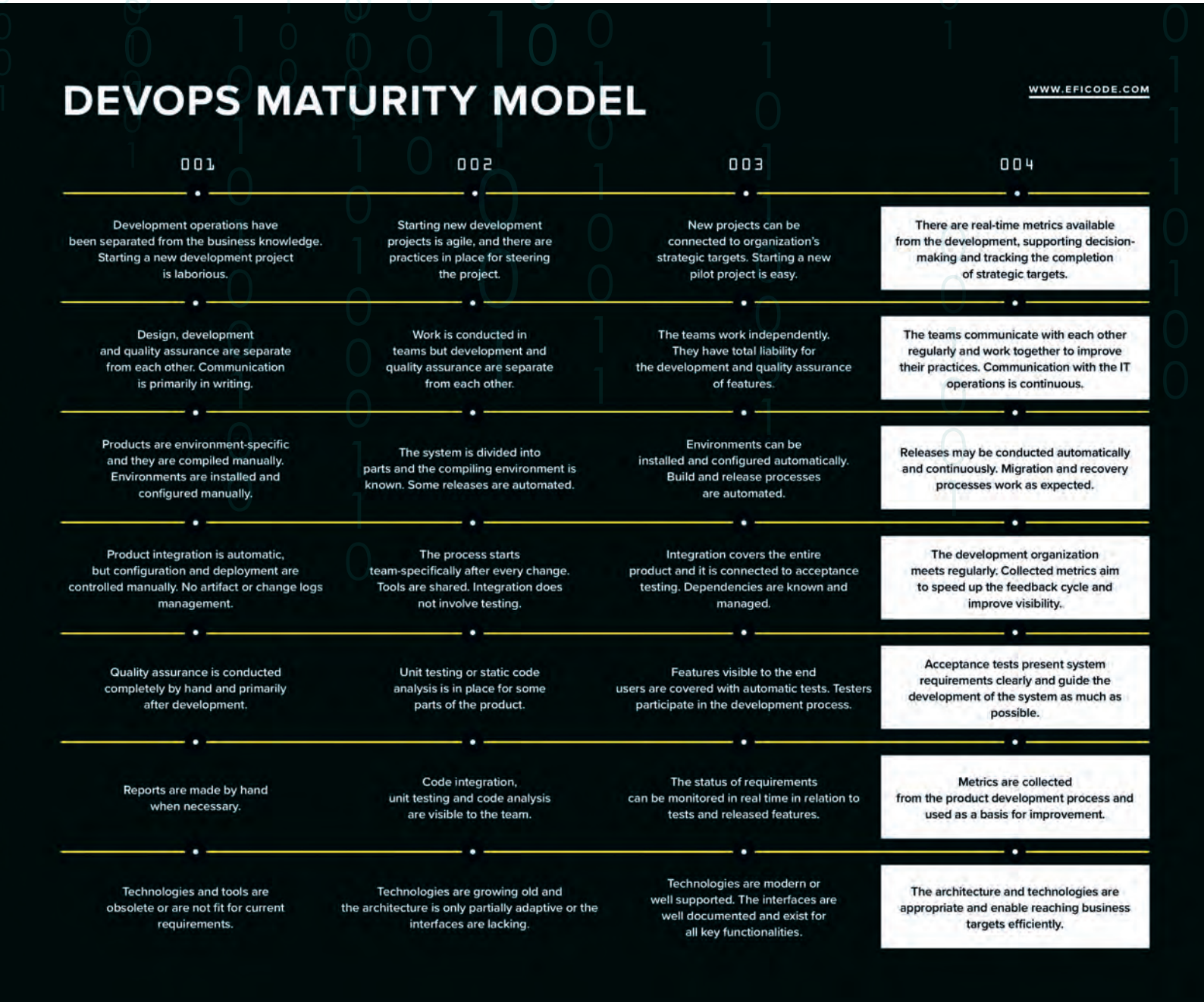
Es gibt unendlich viele Fragebögen und Tools im Internet, die eine DevOps Bewertung versprechen. Dass dies fast nie auf die Individualität eines Unternehmen eingehen kann, versteht sich fast von selbst. Viele dieser Modelle geben nur einen ersten, manchmal verzerrten Einblick und berücksichtigen nicht, dass unterschiedliche Unternehmensbereiche auch einen unterschiedlichen Entwicklungsstand haben können.

Eigene Mitarbeiter kennen das Unternehmen gut und identifizieren Ansatzpunkte schneller zu – vorausgesetzt, sie haben einen relativ neutralen Standpunkt. Wenn ganze Teams sich selbst einschätzen und Verbesserungswege suchen, hat das den

Modell für die Bewertung des DevOps Reifegrads. (Quelle: Eficode)

Vorteil, dass sie von Anfang an am Projekt mitwirken und entsprechend motiviert sind – doch sich selbst einzuschätzen ist keine leichte Aufgabe. Und leider sind gerade die qualifizierten Mitarbeiter, die mit den Stärken und Schwächen vertraut sind und eine fundierte Bewertung abliefern könnten, meist schwer abkömmlich. Einige Untersuchungen zeigen, dass CEOs Optimisten sind, was den Stand der Agilität im Unternehmen angeht. Dass die Wahrnehmung des Führungsteams nicht ganz mit jeder der Mitarbeiter übereinstimmt, könnte Druck aufbauen, wenn nicht ohnehin der Mitarbeiter, der vermutlich aus dem IT-Team kommt, versucht, seine Leistung und die seines Teams positiv darzustellen. Mit „Vanity Metrics" zu messen heißt im schlimmsten Fall, Fehler und Probleme vertuschen.

Ein externer Consultant ist hier neutraler, er verfügt über umfassende Erfahrung und kann auch die in den Interviews gewonnenen Aussagen relativieren. Dennoch kann es notwendig werden, manche Gesprächspartner mehrmals zu befragen, wenn sich im Laufe der späteren Interviews Ungereimtheiten ergeben. Das kostet Zeit, führt aber zu besseren Ergebnissen. Ein weiterer Vorteil externer Spezialisten ist ihr umfassendes und aktuelles Know-how zu Tools und Plattformen – es ist für sie einfacher, direkte, praxisbezogene Empfehlungen mit hohem Detaillevel zu geben. Nützlich ist es auch, sich gegen andere zu messen. Benchmark dabei könnte die eigene Branche sein, oder auch Unternehmen, die dem Ziel schon



sehr nahe gekommen sind. Diesen Vergleich kann nur leisten, wer die Daten und die Erfahrung hat – ein weiteres Argument für einen externen Berater. Wichtig dabei ist aber, dass am Ende nicht eine klare Kaufempfehlung für ein bestimmtes Produkt steht – das würde an der Neutralität des Consultant zweifeln lassen.

Möglichkeiten und Grenzen der Messbarkeit

Eine Reifegradmessung bei DevOps kann für ein ganzes Unternehmen oder nur Teilbereiche durchgeführt werden – abhängig vom Ziel des Unternehmens. So ist es beispielsweise möglich, nur den am weitesten entwickelten Bereich zu untersuchen und zu optimieren, um hier einen internen Benchmark zu schaffen, eine Keimzelle für alle weiteren Bemühungen. Die andere Variante wäre, die ganze Organisation zu untersuchen – in der klassischen Unterteilung nach Kultur, Prozessen und Tools.

In beiden Fällen kostet es sicherlich ein paar Wochen, bis die Datensammlung und die Bewertung abgeschlossen sind. Befragt werden meist Softwareentwickler, Mitarbeiter aus dem Design und aus dem betroffenen Fachbereich, die die Vorgaben für eine Applikation entwerfen oder in ein Lastenheft umwandeln. Wichtig ist es, Entwickler mit verschiedenen Funktionen und auch Mitarbeiter von IT Operations in die oft mehrstündigen Interviews einzubeziehen.

WIR GLAUBEN, DASS DER NEUTRALE BLICK AUF EIN UNTERNEHMEN NUR DANN GEGEBEN IST, WENN MAN GUTEN GEWISSENS NACH DER SCHLUSSPRÄSENTATION UND DER ÜBERGABE DES ASSESSMENT-BERICHTS DEM KUNDEN DIE WEITEREN SCHRITTE ÜBERLASSEN KANN.

Petteri Ahonen,
Managing Director, Eficode GmbH,
www.eficode.com

Welche Unternehmenskultur braucht DevOps, um maximalen Erfolg zu erzielen? Damit Menschen intelligenter und innovativer arbeiten können, brauchen Sie Freiraum innerhalb sinnvoll gesetzter Grenzen. Und Sie brauchen Kommunikation und Transparenz über die bisherigen Silo-Grenzen hinweg. Es gilt, alle mit auf die Reise zu nehmen und den Mehrwert der Änderungen stringent zu vermitteln. Viele Fragen versuchen zu ermitteln, ob ein Unternehmen hier einen guten Job macht – etwa Fragen zu Teamstruktur, Feedbackkultur, Kundenzentriertheit oder zu Werten allgemein. Dennoch ist es re-

lativ schwierig, die Messkriterien dafür richtig aufzusetzen und die Ergebnisse müssen grundsätzlich mit Vorsicht behandelt werden.

Der Schwerpunkt der Interviews liegt meist auf Prozessen und fokussiert auf die Grundfrage nach Produktivität und Arbeitsqualität. Um Softwareentwicklungsprozesse richtig einschätzen zu können, wird sowohl das Coding als auch die Implementierung und das Deployment betrachtet, immer auch in Bezug auf Testing und Security. Es gibt eine Vielzahl an prozessbezogenen KPIs, angefangen von Deployment-Frequenz und -Zeit über Lead Zeiten bis hin zu Change Failure Rates. Doch auch hier lässt sich ein gewisses Maß an Subjektivität nicht vermeiden. Wie misst man beispielsweise Kundenfeedback?

Der am einfachsten zu beantwortende Bereich betrifft Tools beziehungsweise Architekturen. Um den wie den Code einfach von der Entwicklung zur Produktivphase zu bringen, braucht man Builds, Tests, Code Coverage, Security Scans und Monitoring als automatisierte Komponenten der Deployment Pipeline. Das Bestehen, die Funktionalität und die Effizienz dieser modularen, hochintegrierten Tool-Chain sind anhand von Checklisten relativ gut erfassbar. Ebenfalls abgefragt werden können die Infrastruktur, Hardware und Service-Funktionen. Besteht eine Microservice-Architektur? Werden die Tools über eine DevOps Plattform gesteuert? Fragen wie diese erlauben schnelle Rückschlüsse auf die Leistungsfähigkeit der DevOps-Umgebung.

Reifegrad bewertet – und jetzt?

Jedes Assessment endet mit einem Bericht und/oder einer Präsentation. Wie umfassend die Empfehlungen daraus sind, hängt von den Beratern ab, aber auch davon, welcher Reifegrad festgestellt wurde. Wiederum beziehen sich die Handlungsvorschläge auf die drei genannten Kategorien.

Im Normalfall reicht das den Unternehmen aus, um die ersten Schritte zu entscheiden. Wenn nicht, bieten Firmen wie zum Beispiel Eficode auch mehrtägige Workshops an, um die Aufgaben und nächsten Schritte zu vertiefen.

Im besten Falle können die Verantwortlichen im Unternehmen damit direkt weiterarbeiten – sei es in der Überarbeitung der Tool-Chain, sei es in der Veränderung der Infrastruktur oder aber auch mit Kommunikationsmaßnahmen im Unternehmen. Manchen Unternehmen gelingt es alleine, den Paradigmenwechsel in ihrer Infrastruktur durchzuführen und mit allen relevanten Applikationen produktiv zu gehen, andere haben mit dem Abschlussbericht fast schon ein Pflichtenheft für externe Dienstleister.

Auf jeden Fall sollte das Assessment wie ein Kick-off auf dem Weg in eine umfassende DevOps-Kultur wirken – nur dann hat es seinen Sinn erfüllt.

Petteri Ahonen

AGILES PROZESSMANAGEMENT

MIT SCRIBBLE PROZESSE UND ORGANISATIONEN ZUKUNFTSFÄHIG GESTALTEN

Was die VUKA-Welt von modernen Prozessmanagement fordert, kann Scribble leisten: agile Prozessgestaltung, schlanke Dokumentation und rasche Anpassung. Diese Vorgehensweise liefert zu jedem Schritt die zur Umsetzung geeignete Methode und unterstützt nicht nur eine zeitgemäße Ablauforganisation, sondern setzt auch wertvolle Impulse für die Entwicklung zur lernfähigen Organisation. Checklisten, Arbeitshilfen und Praxistipps unterstützen den Praxistransfer.

- Prozesse agiler starten, Kundenzufriedenheit erhöhen, Unternehmenskennzahlen verbessern
- Ablauf- und Aufbauorganisation kundenorientiert ausrichten
- Mitarbeiter begeistern und Ressourcen optimal einsetzen
- Selbstlernen und Weiterentwicklung in Organisationen unterstützen

Das Handbuch für agiles Prozessmanagement: Mit Scribble Prozesse und Organisationen zukunftsfähig gestalten; Manfred Brandstätter, Carl Hanser Verlag GmbH & Co.KG, 04-2021

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
30. APRIL 2021

ROBOTIC PROCESS AUTOMATION

Entwicklung zur intelligenten Automatisierung

MANAGED SERVICES

Maximale Leistungsfähigkeit

INDUSTRIE 4.0

Dynamische Weiterentwicklung

DIE AUSGABE 04/2021 VON IT MANAGEMENT ERSCHEINT AM 31. MÄRZ 2021.

INSERENTENVERZEICHNIS

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Carina Mitzschke, Silvia Parthier (-26)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Markus Adolph, Petteri Ahonen, Markus Grüneberg, Günter Esch, Dina Haack, Chris Huff, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Roland Völkel, Frédéric Woschniak, 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

Das E-3 Magazin

Information und Bildungsarbeit von und für die SAP-Community

Wir leben alle unter dem gleichen Himmel, aber wir haben nicht alle den gleichen Horizont.

Konrad Adenauer

e-3.de | e3zine.com

Wer viel weiß, weiß sich zu wehren.

Der nächste Angriff kommt bestimmt.

Gut vorbereitet mit itsecurity

www.it-daily.net

itsecurity
MÄRZ 2021

DAS SPEZIAL

SICHERHEIT IN DER EDGE

PERFORMANT UND SICHER

Alexander Zachow, Akamai

CYBERANGRIFFE

Schwachstellen erkennen

INDUSTRIE 4.0

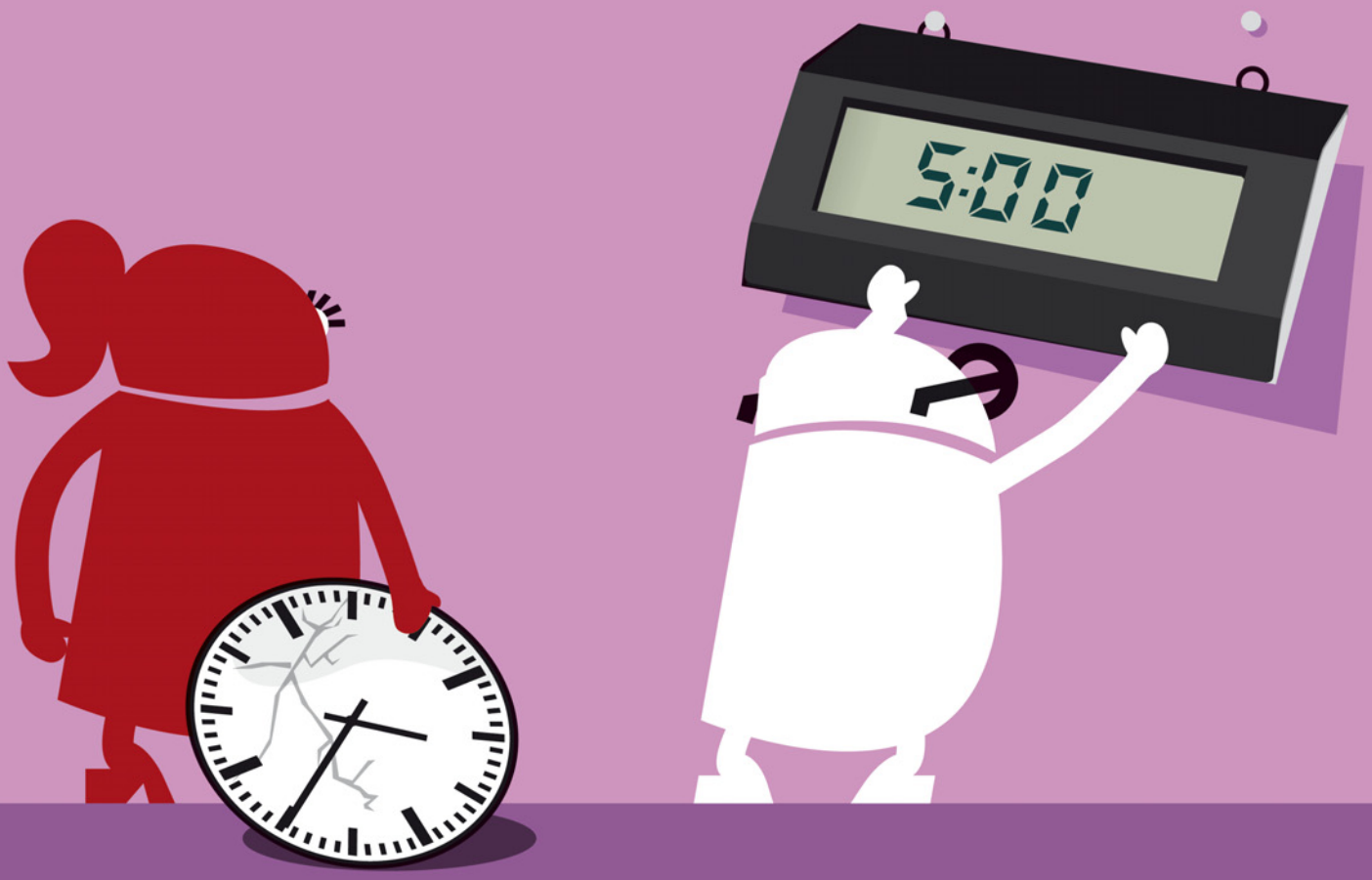
Praxisnahes Lernen

DATENSCHUTZ

Ordnung im Toolchaos schaffen

www.it-daily.net

Digitalisierung leicht gemacht!



Expertenwissen für

IT-Strategien & Innovationen

itmanagement

www.it-daily.net

4 COVERSTORY

INHALT

SICHERHEIT IN DER EDGE

PERFORMANTE UND SICHERE INTERNETKOMMUNIKATION

Edge Computing ist mittlerweile ein gängiger Begriff in der IT-Welt. Doch was bedeutet der Begriff und was genau verbirgt sich dahinter? Alexander Zachow, Regional Director DACH bei Akamai sprach darüber mit Ulrich Parthier, Herausgeber it security.

Ulrich Parthier: *Auf der Akamai-Startseite findet sich die Aussage „Geschwindigkeit, Intelligenz und Sicherheit an der Edge". Ich persönlich kann mit dieser Aussage zunächst einmal wenig anfangen. Was genau verbirgt sich dahinter?*

Alexander Zachow: Hinter dieser Aussage steht der Anspruch unserer Kunden, weltweit personalisierte, performante und sichere Online-Erlebnisse für die jeweils eigenen Kunden zu schaffen. Dabei unterstützen wir unsere Kunden mit der Akamai Intelligent Edge Plattform. Diese ist mit Servern an circa 4200 Standorten in 135 Ländern die größte und am weitesten verteilte Edge-Computing der Welt.

Verteilt ist dabei das entscheidende Stichwort. Durch immer größere Bandbreiten auf der letzten Meile kann es in den zentralen Internetknoten zu Datenstaus kommen. Die performante, sichere und intelligente Internetkommunikation muss somit nahe am Endbenutzer, am sogenannten Edge, gesteuert werden.

Ulrich Parthier: *Wenn ich zurückblicke, verbinde ich mit dem Namen Akamai zuallererst immer das Stichwort WAF (Web Application Firewall). Wie hat sich die Architektur des Produktportfolios verändert und welche Rolle spielen die Themen Performance und Sicherheit?*

Alexander Zachow: Es war nicht immer so, dass Akamai als Security Anbieter wahrgenommen wurde. Unsere Wurzeln liegen im Bereich Content Delivery, also der Auslieferung von Webinhalten an die Endnutzer. In der Edge Technology Group bündeln wir dazu die Produkte, die unsere Kunden befähigen online Business zu betreiben – sei es als Streaming-Dienst, Nachrichtenportal oder Webshop – wir beschleunigen und skalieren die Datenauslieferung zum Endbenutzer.

Mit der zweiten Säule, der Security Technology Group, schützen wir die digitalen Geschäftsaktivitäten gegen Cyberattacken. Das Herzstück dieser Applikationssicherheit ist die zum Beispiel von Gartner als Leader klassifizierte WAF. Mit unseren Botmanagement- und Identity-Lösungen gehen wir konsequent den Weg, Unternehmen vor Online-Betrug zu schützen. Im Bereich der Netzwerksicherheit schützen wir unsere Kunden vor DDoS-Angriffen und bieten Access-Lösungen, die nach dem Zero-Trust-Prinzip einen sicheren Zugang zu Unternehmensapplikationen gewährleisten.

Ulrich Parthier: *Wenn wir einen Blick in die nahe Zukunft werfen: Wie werden sich Internet-Traffic, Geschwindigkeit – Stichwort 5G – und die Security verändern?*

Alexander Zachow: Zuwächse sehen wir kontinuierlich jedes Jahr. Im Dezember verzeichneten wir beispielsweise einen neuen Traffic-Rekord mit 181 Terabit die Sekunde. Dies ist ein Wachstum von gut 50 Prozent im Vergleich zum Vorjahr. Das sind Größenordnungen, die fast nicht mehr vorstellbar sind. Zum Vergleich: die D-CIX in Frankfurt wickelt im Tagesmittel circa 7,5 Terabit die Sekunde ab.

5G wird ein weiterer Treiber dieser Zuwächse sein. Für mich viel spannender ist aber, dass mit 5G nun industrielle Internet-of-Things-Anwendungen in der Breite umgesetzt werden. Das eröffnet komplett neue Märkte, leider aber auch Attack-Vektoren, mit denen wir umgehen müssen.

Ulrich Parthier: *Besonders unangenehm für Unternehmen sind DDoS–Angriffe. Laut Schätzungen von Gartner werden bis 2023 über 30 Prozent der öffentlichen Webanwendungen durch WAAP-Dienste (Web Application and API-Protection) in der Cloud geschützt sein. Welche Lösungsansätze bietet Akamai hier den Anwendern?*

Alexander Zachow: WAAP-Dienste kombinieren DDoS-Schutz, Bot-Abwehr, API-Schutz und Web Application Firewalls. Das sind genau die Lösungen, die in unserer Security Technology Group gebündelt sind. Im Jahr 2020 ist dieser Bereich um 29 Prozent gewachsen. Das zeigt deutlich, dass Anwender ihre digitalen Geschäftsaktivitäten absichern. Dabei ist es für Unternehmen enorm wichtig, einen ganzheitlichen Schutzschirm aufzubauen. Wenn das Rechenzentrum oder die DNS-Infrastruktur mit einer DDoS-Attacke angegriffen wird, ist der singuläre Schutz einer Applikation mit einer WAF nicht effektiv. Das ist vergleichbar mit einem Einbruchsschutz zu Hause: die doppelte oder gar dreifache Sicherung der Eingangstür bringt gar nichts, wenn das Fenster daneben offen steht.

Ulrich Parthier: *Wenn wir über Bedrohungsszenarien sprechen, reden wir meist über Reaktionen auf Sicherheitsvorfälle. Wie sieht es mit der Antizipation von Gefahren, also proaktivem Handeln aus und gibt es so etwas wie Zero-Latenz bei Cyberangriffen?*

Alexander Zachow: Wir liefern circa 25 Prozent des täglichen Internetdatenverkehrs aus. Die Erkenntnisse daraus kommen allen unseren Kunden, etwa in Form von Client-Reputation-Scores, zu Gute. Außerdem erstellen wir Regelwerke, die vorab definieren, welche Anfragen auf welche Ports, Hostnamen und API-Endpoints zulässig sind. Alle anderen werden proaktiv, also mit Zero-Latenz, geblockt. Jeder Kunde hat die Möglichkeit, ein individuelles Regelwerk zu entwickeln. Dabei stehen wir unterstützend zur Seite, denn eine One-Size-Fits-All-Ansatz birgt eine erhöhte Gefahr, legitime Nutzer zu blocken.

Ulrich Parthier: *Forschung spielt ja eine wichtige Rolle bei der Bewältigung künftiger Bedrohungsszenarien. Ein gutes Beispiel ist Mylobot, DGA-basierte unsichtbare Malware, die mittels Deep Learning-Verfahren aufgespürt wurde. Können Sie zu diesem Beispiel exemplarisch etwas sagen?*

Alexander Zachow: Es findet ein „Wettrüsten" statt. IT-Security-Anbieter wie Akamai investieren viel Geld in effektive Lösungen. Auf der Gegenseite stehen die „bad actors". Diese verdienen Geld mit DDos-Angriffen oder Ransomware. Von Regierungen finanzierte Hackergruppen verfolgen andere Motive, sind jedoch finanziell bestens ausgestattet. Der Dritte im Bunde sind die Anwenderunternehmen. Da gibt es ein breites Spektrum an Reifegraden in der IT-Security und in vielen Bereichen einen großen Nachholbedarf.

Ulrich Parthier: *Threat Intelligence, KI, Deep Learning. Wie sollten Anwender mit diesen Schlagwörtern umgehen und wie erkennen sie die Sinnhaftigkeit und Integration in Produkte und Lösungen?*

Alexander Zachow: Im Kontext der Cybersecurity geht es in erster Linie darum, in riesigen Datenmengen Muster zu erkennen, um daraus Strategien für die Gefahrenabwehr zu entwickeln. Das Ganze muss in sehr kurzen Zyklen stattfinden, um wirksam zu sein. Hier nutzen wir KI/ML, aber auch heuristische Verfahren. Ein Beispiel ist der bereits angesprochene Client-Reputation Score oder auch unsere BotManagement-Lösung, die kontinuierlich lernt, durch Menschen verursachte Mausbewegungen oder das Tippen auf dem Smartphone von Signaturen zu unterscheiden, die ein Bot tätigen würde.

Ulrich Parthier: *Bieten Sie ein Assessment oder ein Benchmarking für Interessenten an, damit Sie ihr aktuelles Sicherheitslevel überprüfen und einschätzen können?*

Alexander Zachow: Ich denke, Unternehmen sind gut beraten, wenn sie herstellerunabhängige Assessments durchführen. Alle unsere Lösungen sind von führenden Analystenhäusern bewertet worden. Das BSI führt uns als qualifizierten DDoS-Mitigation Anbieter. Für interessierte Kunden bieten wir Testmöglichkeiten für den Großteil unserer Produkte an. Oft liefern diese Tests dann weitere Erkenntnisse, so dass wir dann recht schnell mit den Kunden über eine gesamtheitliche Security-Strategie sprechen.

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

SICHERHEITSSTRATEGIE

CYBER-VERSICHERER BEOBACHTEN ERHEBLICHE DEFIZITE

2020 war in vielerlei Hinsicht ein besonderes Jahr – auch für die Cyber-Versicherung. Dies hat drei wesentliche Gründe:

1. Die Pandemie war und ist ein Treiber der Digitalisierung. Zum einen wurden Arbeitnehmer in Scharen ins Homeoffice versetzt zum anderen haben zahlreiche Unternehmen schlagartig festgestellt, dass das Internet und digitale Kommunikation die Einschränkungen des Lockdowns zumindest teilweise ausgleichen können. Unternehmen, die bereits stärker digitalisiert waren, hatten Wettbewerbsvorteile. Damit steigt jedoch auch die Abhängigkeit vom Internet, von Daten und EDV-Systemen.

2. Die Verwundbarkeit steigt. Das Ausmaß der Schäden hat insbesondere seit 2019 drastisch zugenommen. Zwar zeigen Statistiken und Studien, dass die Anzahl der Vorfälle sich verringerte, doch sind die Angriffe erfolgreicher geworden. Das heißt, der Schaden, der aus den Angriffen resultiert, hat sich deutlich erhöht. Auch bei mittelständischen Unternehmen sind nicht selten Schäden im Millionen Euro-Bereich zu verzeichnen.

3. Die Cyber-Versicherung hat sich inzwischen auf dem Markt etabliert – damit kommen die oben genannten Schäden aber auch zunehmend bei den Versicherern an. Bei dem noch jungen Portfolio bedeutet das aber auch, dass das Kollektiv in der Cyber-Versicherung noch nicht ausreichend gewachsen ist, um das Schadenaufkommen allein abzupuffern. Die Versicherer reagierten unverzüglich. Sie hinterfragen heute mehr und tiefergehend vorhandene IT-Strukturen ihrer Kunden, investieren deutlich mehr in die Risikoanalyse und suchen gleichermaßen nach Möglichkeiten, die Risikolage bei den Unternehme zu verbessern. Das Ziel dieser Maßnahmen: Die Leistungen für den Versicherungsnehmer hoch und etwaige Beitragsanpassungen moderat halten.

Aufgrund der verbesserten Risikoanalyse sind auch unsere Einblicke in unterschiedliche Unternehmen tiefer und damit auch detaillierter geworden. Wir beobachten in diesem Zuge leider erhebliche Defizite bei deutschen Unternehmen. In Gesprächen mit unseren Kunden wird uns häufig gespiegelt, dass der gesamte Themenkomplex der IT-Sicherheit über Jahre vernachlässigt wurde. Auch hier hat die Corona-Krise einen Teil zu beigetragen. Budgets mussten umgeshiftet werden und das oft nicht zugunsten des IT-Bereichs.

DA JEDES UNTERNEHMEN INDIVIDUELLE PROBLEMSTELLUNGEN IN SACHEN IT-STRUKTUR ZU LÖSEN HAT, HABEN WIR ALS VERSICHERER EIN MEHRSCHICHTIGES VERFAHREN IN DER RISIKOANALYSE ENTWICKELT, UM DIE JEWEILIGEN BEDARFE UND BEDÜRFNISSE DES KUNDEN ZU IDENTIFIZIEREN.

Dirk Kalinowski, Senior Produktmanager IT- und Cyberrisiken, www.axa.de

Schritt für Schritt

Da jedes Unternehmen individuelle Problemstellungen in Sachen IT-Struktur zu lösen hat, haben wir als Versicherer ein mehrschichtiges Verfahren in der Risikoanalyse entwickelt, um die jeweiligen Bedarfe und Bedürfnisse des Kunden zu identifizieren und dann im nächsten Schritt, einen passgenauen Versicherungsschutz zu bieten. Unsere Expertise aus Schadenfällen ermöglicht es uns, die wesentlichen Faktoren der Cyber-Security zu identifizieren. Doch wie gehen wir vor?

Die Ersterfassung des Risikos beginnt mit einer Selbstauskunft. Dafür stellt der Versicherer einen Fragebogen zur Verfügung. Bei komplexen Risiken werden auch Risikogespräche oder -audits durchgeführt. Dabei wird besonders auf die elementaren Sicherheitsmaßnahmen geachtet:

Firewall und Endpoint-Protection setzen wir voraus und sind auch fast überall vorhanden.

Patch-Management: Hier kommt es vor allem darauf an, wie Alt-Systeme isoliert bzw. anderweitig geschützt sind. Solche Systeme gibt es fast noch in jedem Unternehmen.

Backup und Disaster-Recovery: Bei Ransomware-Angriffen ist das die Lebensversicherung von Unternehmen. Dabei glauben viele IT-Verantwortliche noch immer, dass ein echtes Offline-Backup nicht erforderlich ist. Tatsächlich hat aber die Schadenerfahrung gezeigt, dass insbesondere bei Backup-Konzepten die größten Versäumnisse liegen.

Notfallkonzepte: Wie reagiert das Unternehmen im Falle eines Cyber-Angriffs? Sind Maßnahmen dafür definiert? Damit im Ernstfall das Backup auch gesichert ist oder entscheidende Beweise vor einer Löschung geschützt werden, sollte hier regelmäßig geprüft und ggf. nachjustiert werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) setzt allgemeingültige Standards für Notfallkonzepte und passt diese derzeit an den technologischen Fortschritt an.

Mitarbeiter-Awareness: Die Mitarbeitenden sind häufig das Einfallstor für eine Cyberattacke. Bindet man sie aber ein und stattet sie entsprechend aus, können sie auch ein gut funktionierendes Bollwerk gegen Angriffe sein. Daher sollte man die regelmäßige Sensibilisierung z. B. durch web-based Trainings nicht unterschätzen. Wir bei AXA haben dazu mit unserem Partner 8com ein Portal für unsere Kunden eingerichtet, über das sie ihre Belegschaft informieren und schulen können.

Sicherheits-Audits und Pen-Tests: Hilfreich ist, wenn das Unternehmen nachweisen kann, dass Dritte die eigene Sicherheit überprüft haben. Auch wir Versicherer nutzen Möglichkeiten eines Schwachstellen-Scans über das Internet auf die URL bzw. öffentlich verfügbare Informationen. Der Versicherer kann seine Kunden so schon frühzeitig auf konkrete Probleme aufmerksam machen. Ein einmaliger Scan ist allerdings keine ausreichende Prävention vor Cyberangriffen. Er bildet nur eine Momentaufnahme ab.

SIEM und SOC: Daher ist die nächste Stufe der Sicherheit die Installation einer kontinuierlichen Netzwerk- und Schwachstellenüberwachung in den internen Netzen. Diese können entsprechende Dashboards liefern und eine schnelle Reaktion bei Sicherheitsvorfällen ermöglichen. Security Information and Event Management (SIEM) und Security Operations Center (SOC) haben sich dazu am Markt etabliert. So kooperiert AXA mit C-SOC und SOCaaS (Security Operation Center as a Service). Das SOC übernimmt die aktive Überwachung und Analyse aller integrierten Systeme, erkennt IT-Schwachstellen, alarmiert bei Bedrohungen und berichtet unverzüglich an die IT-Verantwortlichen – und das zu einem bezahlbaren Preis, auch für kleinere Unternehmen. Ein auffälliger Zugriff kann so bestenfalls in Echtzeit eliminiert, seine Auswirkungen auf jeden Fall minimiert werden. Auf Wunsch kann das SOC aktiv einschreiten, kritische Systeme aus der Gefahrenzone nehmen und so Sicherheitslücken schließen.

Management: Und schließlich spielen das Management-System und die Grundhaltung des Unternehmens zur Informationssicherheit eine wesentliche Rolle. Sind Richtlinien vorhanden und ist sichergestellt, dass diese umgesetzt werden? Besteht eine Aufbau- und Ablauf-Organisation für Sicherheit? Wird ein Risikomanagement betrieben? Schließlich befinden sich die IT und die Anforderungen daran in einem stetigen Wandel und die Sicherheitsmaßnahmen müssen dementsprechend immer wieder auf neue Situationen angepasst werden.

Fazit

Rein technische Maßnahmen zur Cyber-Security sind eine sinnvolle Ergänzung aber kein vollumfänglicher Schutz. Die Kombination aus geschultem Personal, gezielten Investitionen und technischen Schutzmaßnahmen bilden den Idealzustand. Wir Versicherer sind mit unseren unterschiedlichen präventiven Services ein begleitender Partner in allen Instanzen und forcieren immer den best case. Und sollte es doch einmal zum worst case kommen, sind wir der notwendige Krisenmanager und die finanzielle Absicherung.

Dirk Kalinowski

CYBERKRIMINALITÄT

ZWEI VON DREI UNTERNEHMEN IN DACH BEREITS OPFER

Die Cyber-Bedrohungslandschaft im DACH-Raum entwickelt sich rasant weiter. Dabei versuchen Cyberkriminelle zunehmend menschliche Schwächen statt direkte Schwachstellen in IT-Infrastrukturen auszunutzen. Der mit über 90 Prozent vorherrschende Bedrohungsvektor dabei ist die E-Mail. So sind es auch primär E-Mail-basierte Bedrohungen, wie Business Email Compromise (BEC), aber auch das Phishing von Anmeldeinformationen, kompromittierte Cloud-Konten und Ransomware-Angriffe, mit denen Cyberkriminelle Mitarbeiter zu überlisten versuchen.

Die Anzahl von erfolglosen Angriffsversuchen Cyberkrimineller auf Unternehmen lässt sich seit langem nicht mehr beziffern. Doch trotz aller Vorsichtsmaßnahmen aufseiten der Organisationen sind die Attacken aus Sicht der Kriminellen regelmäßig von Erfolg gekrönt.

Um besser verstehen zu können, wie sich personenbezogene Cyber-Angriffe auf Unternehmen in der Schweiz, in Österreich und Deutschland auswirken, hat Proofpoint eine Umfrage unter CSOs/CISOs in Auftrag gegeben. Im Rahmen der im Sommer 2020 vom Beratungsunternehmen techconsult durchgeführten Studie, wurden 202 Unternehmen mit 250 oder mehr Mitarbeitern aus verschiedenen Branchen befragt.

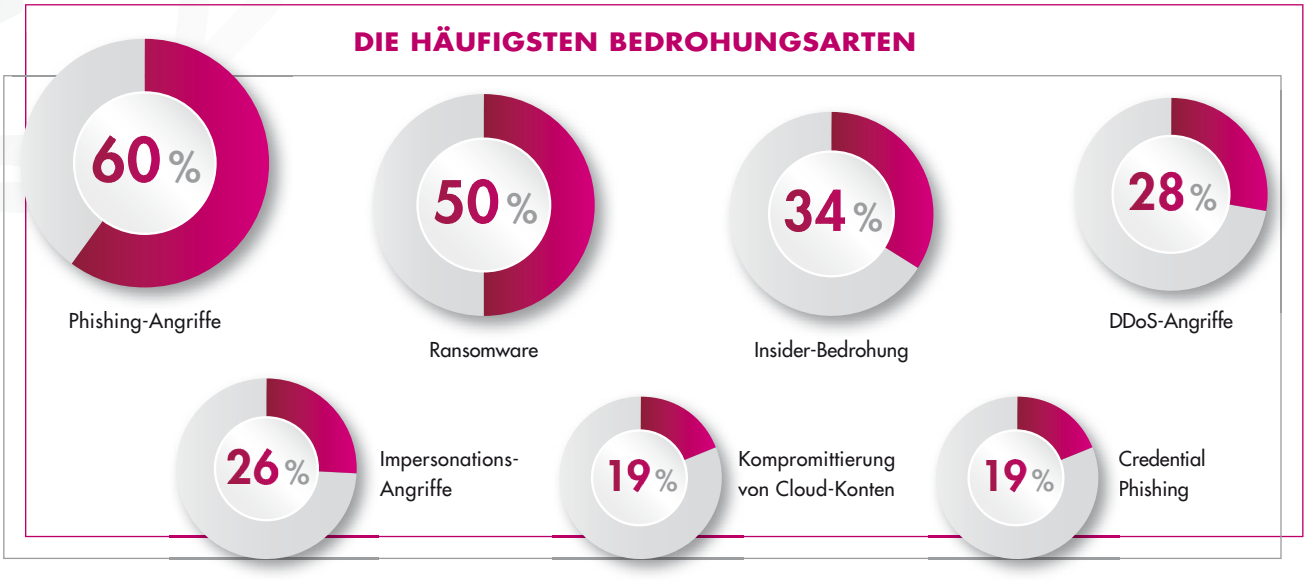
NUR DURCH DEN AUFBAU UND DIE UMSETZUNG EINER ÜBERGREIFENDEN SICHERHEITSSTRATEGIE, WERDEN UNTERNEHMEN EINEN GROSSEN SCHRITT IN RICHTUNG VERBESSERUNG IHRER IT-SICHERHEIT MACHEN KÖNNEN.

Markus Grüneberg, IT Security & Data Privacy Advisor, Proofpoint, www.proofpoint.com

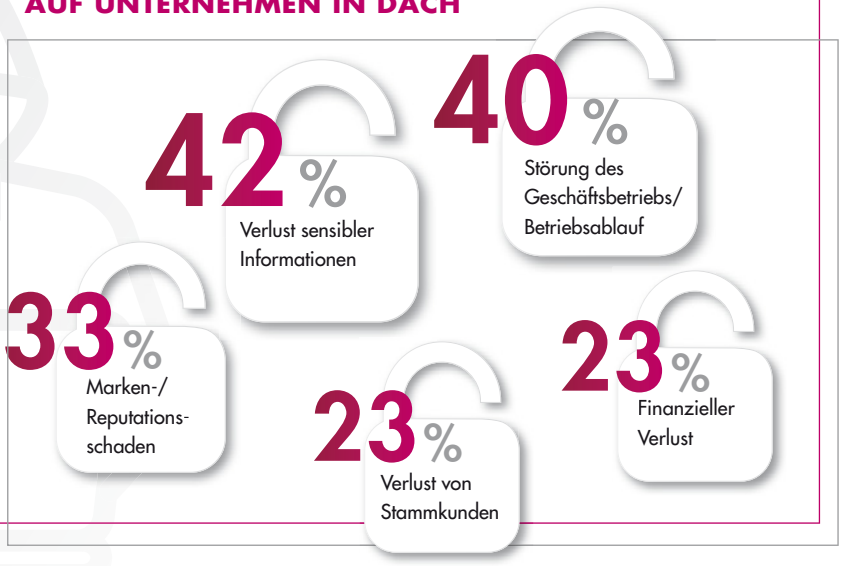
Alarmierende Ergebnisse

Die dabei gewonnenen Erkenntnisse sind alarmierend. Aus der Studie geht unter anderem hervor, dass bereits 66 Prozent der befragten Unternehmen Opfer von Cyberkriminalität waren, jedes zweite davon sogar mehrfach. Oft sind die Schäden, die erfolgreiche Angriffe zur Folge haben, langfristig spürbar. So nannten IT-Security Verantwortliche in 42 Prozent der Unternehmen im DACH-Raum den Verlust sensibler Informationen als häufigste Folge eines Cyberangriffs, gefolgt von Geschäfts- und Betriebsstörungen (40 Prozent). Weitere häufig genannte Folgen waren Marken-/Reputationsschäden (33 Prozent), der Verlust von Stammkunden (23 Prozent) sowie finanzielle Verluste (mit ebenfalls 23 Prozent).

Auch stimmten ganze 70 Prozent der befragten IT-Sicherheitsverantwortlichen aus der Schweiz, Österreich und Deutschland



AUSWIRKUNGEN VON CYBERANGRIFFEN AUF UNTERNEHMEN IN DACH



zu, dass der Faktor Mensch und mangelndes Sicherheitsbewusstsein die größten Risiken für Unternehmen darstellen.

Vorbereitung mangelhaft

Eine weitere Erkenntnis der Studie ist, dass drei von vier Unternehmen nicht optimal auf digitale Angriffe vorbereitet sind. Lediglich 24 Prozent aller Befragten konnten die Frage, ob sie auf eine Cyberattacke vorbereitet seien, vorbehaltlos bejahen. Für die Hacker besonders lohnende Ziele sind dabei große Unternehmen mit mehr als 5.000 Mitarbeitern, denn von ihnen gaben lediglich 12 Prozent an, vorbereitet zu sein. Und auch der öffentliche Sektor gibt eher ein trauriges Bild ab: Während sich immerhin fast drei von vier privatwirtschaftlichen Unternehmen teilweise auf digitale Attacken vorbereitet haben (72 Prozent), konnte dies in der öffentlichen Verwaltung mit 46 Prozent noch nicht einmal jeder Zweite von sich behaupten.

Geringes Vertrauen in eigene Mitarbeiter

Bemerkenswert ist hierbei, dass 53 Prozent der befragten CSOs und CISOs der Meinung sind, dass ihre Mitarbeiter anfällig für Cyberangriffe seien; 77 Prozent jedoch genau hier an Schulungen sparen – in drei von vier Organisationen wird höchstens zwei Mal pro Jahr eine Cybersicherheits-Schulung durchgeführt. Auch hier bildet der öffentliche Sektor das Schlusslicht: ganze fünf von sechs Organisationen führen zu diesem Thema höchstens zwei Mal im Jahr entsprechende Trainings durch.

Der Fokus auf die eigenen Mitarbeiter ist insbesondere anzuraten, bedenkt man folgendes Studienergebnis: Mit Blick auf die nächsten drei Jahre, glauben 54 Prozent der CSOs/CISOs im DACH-Raum, dass Bedrohungen von innen (fahrlässig oder kriminell) zukünftig die größte Cyberbedrohung darstellen und das noch vor Phishing (50 Prozent) und Ransomware mit 32 Prozent.

Unabhängig von den Angriffsmethoden – E-Mail, Cloud-Anwendungen, Web, Social Media – machen sich Angreifer immer stärker den menschlichen Faktor zunutze. Ob es sich um Betrüger handelt, die sich als vertrauenswürdige Kollegen ausgeben, oder um immer überzeugendere Phishing-E-Mails und bösartige Links – es sind die Anwender selbst, die im Kampf gegen Cyberkriminelle an vorderster Front stehen.

Nicht erst seit Beginn der COVID-19-Pandemie verbringen Menschen immer weniger Zeit an ihrem festen Büroarbeitsplatz und mehr Zeit damit, aus der Ferne, sei es im Home Office oder von unterwegs, zu arbeiten. Nach wie vor bleiben sie jedoch das Ziel Nr.1 für Angreifer und noch nie war es so wichtig wie heute, sicher und geschützt von entfernten Standorten aus zu arbeiten.

Cyberbedrohungen durch Remote-Arbeit

Herkömmliche oder veraltete Remote-Zugriffsmethoden lassen sich nur schwer skalieren, sind nicht darauf ausgelegt, moderne cloudbasierte Infrastrukturen zu schützen und führen schnell zu potenziellen Sicherheitsrisiken. Diese erhöhen sich nochmals, wenn Remote-Mitarbeiter nicht den gleichen Sicherheitsstandards unterliegen, wie die Mitarbeiter innerhalb des Unternehmensnetzwerkes. Auf dieser Basis kann nicht sichergestellt werden, dass die gestiegenen Sicherheitsanforderungen und geltenden Vorschriften von den Mitarbeitern auch eingehalten werden.

Nur durch den Aufbau und die Umsetzung einer übergreifenden Sicherheitsstrategie, die den Menschen in den Mittelpunkt stellt, werden Unternehmen einen großen Schritt in Richtung Verbesserung ihrer IT-Sicherheit machen können.

Markus Grüneberg

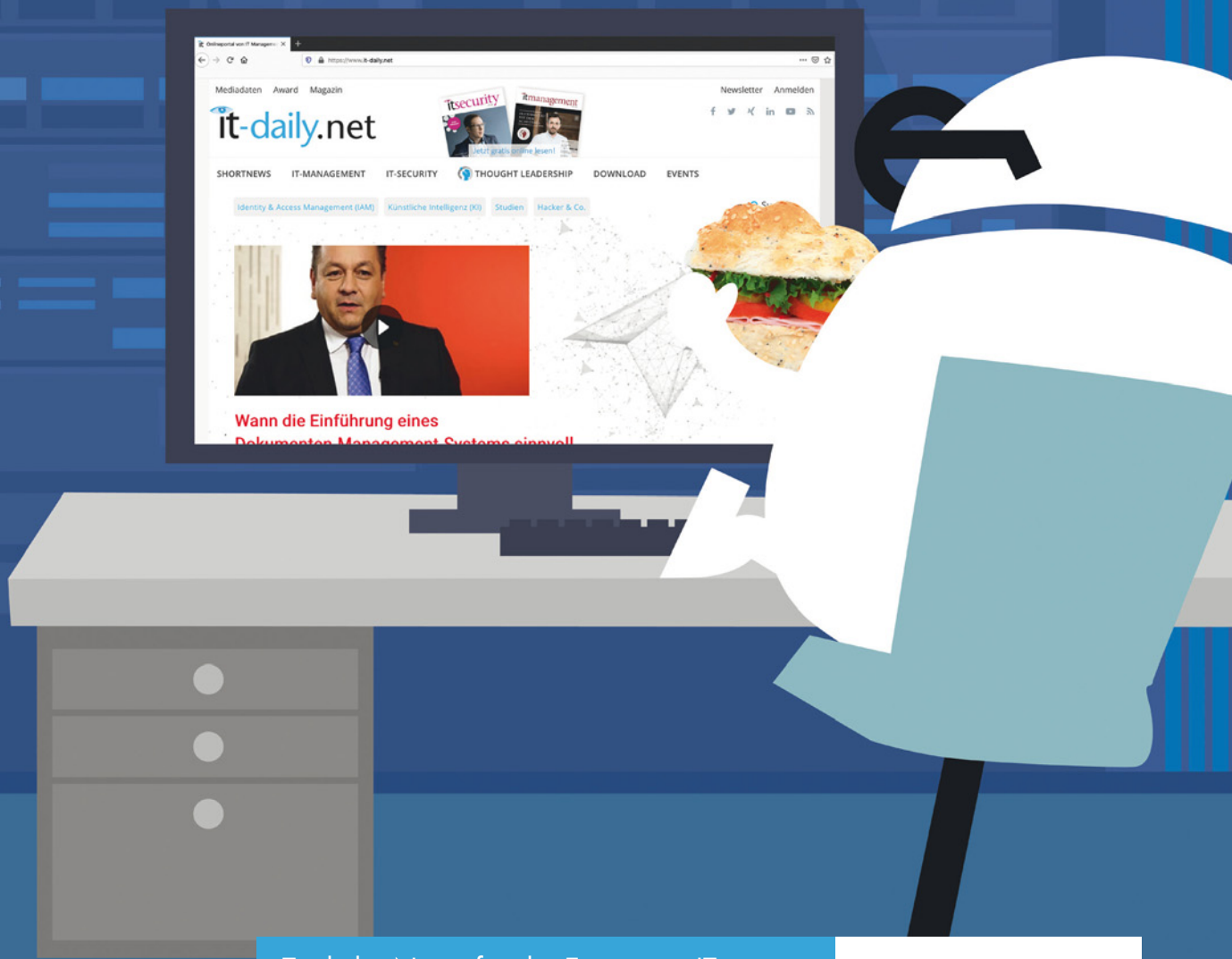
ES HERRSCHT NACHHOLBEDARF

24 %
sehen sich gerüstet für Cyberattacken

31 %
der CSOs/CISOs sehen Cybersecurity nicht als Vorstandsthema verankert

55 %
erwarten, dass ihr Budget für Cybersicherheit um bis zu 20 % in den nächsten zwei Jahren steigen wird

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

SECURE ACCESS SERVICE EDGE

NETZWERK- UND SECURITY-TEAMS (WIEDER) ZUSAMMEN BRINGEN

Vor nicht allzu langer Zeit gab es noch eine klare Grenze zwischen Unternehmensnetzwerken und dem Internet: Netzwerkarchitekten bauten ihre eigenen privaten Netzwerke auf und verbanden diese mit dem Internet an bestimmten, klar definierten Gateways oder Ports. Innerhalb dieses Perimeters sorgten die Security-Teams für Sicherheit und bewachten diese „Tore", damit nichts Unerwünschtes nach außen (wie etwa vertrauliche Daten) oder innen (Malware) gelangte. Mit dem Aufkommen von SaaS, IaaS und der Cloud verschwamm diese klare Linie jedoch immer mehr und der Perimeter löste sich praktisch auf.

Die Aufgaben der Netzwerkarchitekten haben sich in der Folge gewandelt: Jetzt kümmern sie sich in erster Linie um wichtige, in der Cloud gehostete Geschäftsanwendungen mit der zusätzlichen Herausforderung, dass der Zugriff auf Anwendungen über Pfade erfolgt, die meist außerhalb der Grenzen ihres Netzwerks liegen. Die IT-Sicherheit hat sich jedoch nur unzureichend an die neuen Gegebenheiten angepasst. Bei den meisten Unternehmen verlangen die Sicherheitsrichtlinien immer noch, dass der Cloud-Verkehr durch Appliances in den eigenen Rechenzentren geleitet wird. Die Folge diese Routings sind Kompromisse zwischen Sicherheit und Leistung.

Gemeinsamer Nenner

Glücklicherweise findet hier jedoch zunehmend ein Umdenken statt: Der 2019 von Gartner eingeführte Secure Access Service Edge (SASE) erweist sich als wichtiges konzeptionelles Modell, um zu beschreiben, wie Benutzer und Anwendungen geschützt werden können, die jenseits des traditionellen Netzwerkperimeters arbeiten. Dem Ansatz zugrunde liegt die Erkenntnis, dass sowohl Anwender als auch Anwendungen nicht mehr an feste Standorte gebunden sind. SASE bringt damit die Sicherheitsarchitekturen mit der Welt, die Netzwerkteams seit einigen Jahren aufbauen und verwalten, auf einen Nenner und zeichnet sich durch vier Punkte aus:

- **Verteilt:** Die Sicherheit wird über die Grenzen des traditionellen Rechenzentrums hinaus erweitert und ermöglicht es Unternehmen, Sicherheitsfunktionen in die Cloud zu verlagern.
- **Cloud-nativ:** Die Workflows in der Cloud sind anders als beim klassischen Datacenter-zentrierten Ansatz, entsprechend unterscheiden sich auch die Datensicherheit und die Bedrohungen. SASE-Lösungen basieren auf der Konvergenz von Sicherheitsfunktionen und vereinen die Funktionalität etwa von CASB, NG-SWG, SD-WAN und DLP in einer Cloud-nativen Lösung.
- **API-basiert:** APIs ermöglichen es verschiedenen Lösungen und Anwendungen, auf Code-Ebene zu kommunizieren. Dies liefert den für effektive Sicherheitsrichtlinien nötigen Kontext, der nicht durch eine einfache Interpretation von HTTP/S-Protokollen und das Betrachten von URLs generiert werden kann. Ohne diesen Kontext können Unternehmen nur sehen, wer mit wem spricht, aber nicht, worüber sie sprechen oder was sie tun. API-Transparenz ist somit entscheidend für SASE-Lösungen.
- **Offen und verständlich:** In einer offenen und vernetzten Welt sind Interoperabilität, offene Schnittstellen und „Erklärbarkeit" von zentraler Bedeutung. Nur wird sichergestellt, dass die verschiedenen Elemente entsprechend interagieren, und die Sicherheit der Daten und die Einhaltung der Compliance gewährleistet werden.

Es ist an der Zeit, dass Netzwerk- und Sicherheitsteams zusammenarbeiten, um die alten Wege, auf denen sie Unternehmensdaten routen und schützen, zu überdenken. SASE entlastet die Netzwerkperformance und ermöglicht gleichzeitig eine verbesserte Transparenz, Sicherheit und Compliance – ein Gewinn für alle.

PRAXISNAHES LERNEN

IT-SICHERHEIT IN DER INDUSTRIE 4.0

Die digitale Transformation bringt für produzierende Unternehmen eine Vielzahl an Chancen mit sich. Doch mit der Vernetzung steigt auch das Risiko für Cyberangriffe. Ein ganzheitliches Sicherheitskonzept nach IEC 62443 zur Absicherung der Produktion anzuwenden, ist erfolgskritisch – und die gemeinsame Verantwortung von Fach- und Führungskräften. Die Fraunhofer Academy stellt hier in Zusammenarbeit mit dem Fraunhofer IOSB und dem Fraunhofer IOSB-INA das passende Weiterbildungsangebot bereit.

Ganz gleich, ob vernetzte Produktionsanlagen, Fernwartung oder cloudbasierte Planungssysteme – die Digitalisierung eröffnet Unternehmen zahlreiche Ansätze für Innovationen und Effizienz. Mehrwertdienste, wie zum Beispiel Condition Monitoring, überwachen Produktionsanlagen – und Assistenzsysteme ermöglichen mit Hilfe von AR/VR eine neue Art der Fernwartung. Dadurch können Anlagenbetreiber und Servicemitarbeiter aus der Distanz auf Produktionssysteme zugreifen und Fehler beheben. Was sich zunehmend entwickelt, ist nicht nur ein hocheffizientes, sondern gleichzeitig ein immer angreifbareres Produktionssystem – durch die Anzahl der neuen Schnittstellen entstehen zusätzliche Angriffsflächen für Cyberkriminelle.

Über die Netzwerkverbindungen könnten diese auch von außen in die Anlage eindringen, sie manipulieren, mit Schadcode infizieren, Trojaner einschleusen sowie essenzielle Daten verschlüsseln. Die fatale Konsequenz: Wenn Kommunikationssysteme ausfallen, steht in der vernetzten Anlage die Produktion still. Die Folge sind materielle und im Zweifel auch physische Schäden. Industrie 4.0 benötigt deshalb ein ganzheitliches Sicherheitskonzept nach beispielsweise IEC 62443, das gegen diese Art von Angriffen schützt. In der industriellen Produktion gilt es daher, IT-Sicherheit entlang der horizontalen und vertikalen Integration zu realisieren, da sie andere Anforderung als die klassische IT-Sicherheit aufweist.

Aktuelle Situation

Der Status Quo zur Cybersicherheit in der industriellen Produktion weist sehr unterschiedliche Reifegrade auf – von extrem hohen bis hin zu kaum existenten Sicherheitsniveaus. Normreihen und ge-

> IT-SICHERHEIT IST NIE NUR TECHNISCH. SIE IST AUCH ORGANISATORISCH. ZIEL MUSS DESHALB EIN GEMEINSAMES VERSTÄNDNIS ALLER VERANTWORTLICHEN BEZÜGLICH DER CYBERSECURITY-HERAUSFORDERUNG SEIN.
>
> Dr.-Ing. Christian Haas, Gruppenleiter Sichere vernetzte Systeme, Fraunhofer IOSB, www.iosb.fraunhofer.de

> EINMAL IN DIE ROLLE EINES HACKERS SCHLÜPFEN – IN EINEM SICHEREN UMFELD – WÄHREND KOLLEGEN VERSUCHEN DIE IT ZU SCHÜTZEN. SO LERNT MAN PRAXISNAH, WAS IT-SICHERHEIT IN DER INDUSTRIE 4.0 WIRKLICH BEDEUTET.
>
> Jens Otto, Gruppenleiter Cybersicherheit in der Produktion, Fraunhofer IOSB-INA, www.iosb-ina.fraunhofer.de

setzliche Rahmenbedingungen wie die Normreihe IEC 62443, das IT-Sicherheitsgesetzes 2.0 oder die europäische Maschinenrichtlinie treiben die Entwicklung allerdings positiv an. Hinzu kommt die Medienberichterstattung zu erfolgten Cyberangriffen. Auch diese Ereignisse rufen IT-Sicherheit verstärkt auf die Agenda von produzierenden Unternehmen.

Herausforderungen bei IT-Security in der Produktion

Wollen Anlagenbetreiber, Maschinenbauer, Komponentenhersteller und Dienstleister aber ein entsprechendes Schutzniveau erreichen, müssen sie eine Reihe spezifischer Anforderungen betrachten. Beispielsweise beläuft sich die Lebenszeit von Produktionsanlagen oft auf Jahrzehnte – ältere Anlagen können so die bisweilen aktuellen Anforderungen an Cybersicherheit nicht erfüllen. Darüber hinaus ist die Vernetzung der Anlagen oft weitaus umfassender, als den Betreibern bewusst ist. Etwa, dass Maschinenlieferanten für die Fernwartung ebenfalls angebunden sind. Für Produktionsumgebungen gilt es daher, überarbeitete Strategien und Prozesse anzuwenden, damit IT-Sicherheit in der Praxis zum Erfolg wird.

Zusammenspiel der relevanten Akteure

Dazu müssen allerdings alle beteiligten Akteure an einem Strang ziehen. Tatsächlich kristallisiert sich jedoch im Bereich Cybersicherheit oftmals ein Spannungsfeld zwischen den Abteilungen Operational Technology (OT), also den Teams, die für die Technologie und industriellen Systeme für den Herstellungsprozess verantwortlich sind, und der IT heraus. Beide Akteursgruppen haben unterschiedliche Anforderungen an die Produktionsanlagen: Während beispielsweise das Aufspielen von Updates für die IT-Abteilung eine notwendige Maßnahme im Rahmen einer IT-Security-Strategie bedeutet, heißt dies gegebenenfalls für das Team OT, dass die Produktion für eine bestimmte Zeit stillsteht. Diese Interessen müssen zusammengebracht werden. Schulungen bilden hierfür den geeigneten Rahmen. Dort bekommen beide Gruppen die Gelegenheit, sich über die jeweiligen Anforderungen und Bedürfnisse auszutauschen. Beispielsweise erhalten die Akteure bei den Schulungen im Lernlabor Cybersicherheit unter anderem die Aufgabe, in die Rolle des anderen zu schlüpfen. Das stärkt das gegenseitige Verständnis der Verantwortlichen.

Bewusstsein für Wert der IT

Die Schulungen der Fraunhofer Academy vermitteln außerdem ein konkretes Bewusstsein dafür, was die IT für die Produktion bedeutet – und was geschieht, wenn diese ausfällt. Kein mittelständisches Unternehmen und kein Konzern kann es sich heutzutage leisten, dass die Produktion für mehrere Stunden stillsteht. Zudem gilt es, innerhalb der jeweiligen Unternehmen auf verschiedenen Ebenen Verständnis für die Gefahren zu schaffen. Auf Entwicklerebene steht die sichere Softwareentwicklung im Mittelpunkt, während es im Management um Awareness und Verantwortlichkeiten geht.

Praxisnahe Schulungskonzepte

Einen Ansatzpunkt für Führungskräfte bietet beispielsweise die Schulung IT-Sicherheit für Industrie 4.0 – Bedrohungslage und Handlungsbedarf. Das Seminar verschafft einen Überblick zur Bedrohungslage für industrielle Produktionsanlagen. Die Teilnehmenden erhalten neben Informationen zu den Grundbegriffen der IT-Sicherheit viele Praxisbeispiele zu anwendbaren Standards und Richtlinien sowie konkrete Schritte in Richtung eines Cybersecurity Management Systems nach IEC 62443.

Das Seminar IT-Sicherheit in der Automatisierungstechnik bietet Fachkräften eine Vertiefung in die Kommunikations- und Automatisierungstechnik. Bevor der Weg zur Industrie 4.0 beschritten werden kann, muss die Industrie 3.0 zunächst vollständig verstanden sein. Demnach müssen die Werte der kritischen Systeme und Anlagen analysiert werden, um geeignete Schutzmaßnahmen ergreifen zu können. Das Seminar bietet eine praxisnahe Einführung in die Anwendung eines ganzheitlichen Sicherheitskonzeptes nach IEC 62443.

Unternehmen müssen auf dem Weg der digitalen Transformation ihre kritischen Systeme, Anlagen und Werte kennen, um die passenden Schutzmaßnahmen zu treffen. Dazu zählt, Schwachstellen in Design und Risiken der Implementierung in eingebetteten Systemen sowie industriellen Komponenten zu kennen – und zu erkennen. Darüber hinaus gilt es auch, aktuelle Entwicklungen bei Kommunikationsprotokollen und Sicherheitsfunktionen sowie der Entwicklung sicherer Software in den Produktionsanlagen umzusetzen. IT-Sicherheit herzustellen, ist also ein dauerhafter Prozess: Immer neue Taktiken der Angreifer aber auch die technologische Weiterentwicklung erfordern ein kontinuierliches Anpassen der Schutzmaßnahmen, um effektiven Schutz zu gewährleisten.

Dr.-Ing. Christian Haas, Jens Otto
www.cybersicherheit.fraunhofer.de

DevSecOps PRACTICES

Im August 2020 haben das Synopsys Cybersecurity Research Center (CyRC) und Censuswide, eine Umfrage zum Thema DevSecOps durchgeführt. Diese Umfrage berichtet über die Tools, die Unternehmen im Bereich der Softwareerstellung einsetzen, um Open Source Management in ihre DevOps-Praxis zu integrieren. Es werden Strategien untersucht, die verwendet werden, um Open-Source-Lizenzen, das Schwachstellenmanagement und das wachsende Problem von Open-Source-Altlasten in kommerziellen Code in den Griff zu bekommen.

Eines der Interessengebiete von CyRC war, die Verbreitung von DevSecOps – die Praxis der Integration von Sicherheit in jede Phase der DevOps-Pipeline – in verschiedenen Branchen und in Unternehmen auf der ganzen Welt zu untersuchen. Während davon ausgegangen wurde, einen DevSecOps-Trend zu erkennen, deuten die Ergebnisse darauf hin, dass die Akzeptanz bei den Befragten größer ist als erwartet.

WHITEPAPER DOWNLOAD

Das englischsprachige Whitepaper umfasst 24 Seiten und steh kostenlos zum Download bereit. ***www.it-daily.net/download***

FÖRDERUNG FÜR IT-SECURITY

SICHERHEIT VOM STAAT SUBVENTIONIEREN LASSEN

Kleine und mittelständische Unternehmen geraten immer häufiger ins Visier von Cyberkriminellen – mit teilweise verheerenden finanziellen, operativen und rechtlichen Folgen.

Um Gefahren durch Hackerangriffe und Schadprogramme abzuwehren, bedarf es automatisiert arbeitender, spezieller Sicherheitssoftware. Dies hat auch Vater Staat erkannt und fördert Projekte für die digitale Sicherheit mit Zuschüssen von bis zu 550.000 Euro.

Finden Sie in diesem Whitepaper die passende Förderung für die IT-Sicherheit Ihres Unternehmens.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 20 Seiten und steht kostenlos zum Download bereit. ***www.it-daily.net/download***

CYBERSICHERHEIT UND COMPLIANCE

DIE ONAPSIS PLATTFORM IST SAP ENDORSED APP

Mit der Onapsis Plattform können SAP-Anwendungen vor Cyberangriffen, Compliance-Problemen und ungeplanten Ausfallzeiten geschützt werden.

SAP Endorsed Apps sind eine neue Art von Lösungen aus dem SAP-Partnernetzwerk, die Kunden auf dem Weg zum erfolgreichen, intelligenten Unternehmen unterstützen sollen.

„Hunderte der weltweit renommiertesten Unternehmen vertrauen bereits auf Onapsis beim Schutz ihrer geschäftskritischen Anwendungen in ihren SaaS-, PaaS-, IaaS- und On-Premises-Umgebungen", sagt Mariano Nunez, CEO und Mitbegründer von Onapsis. „SAP bietet Kunden erstklassige Lösungen, mit denen sie ihre sensibelsten Geschäftsinformationen und -prozesse schützen können. Jetzt, da die Onapsis Plattform für Cybersicherheit und Compliance den exklusiven Status einer SAP Endorsed App erlangt hat, können wir Kunden im Kampf gegen Cyberangriffe noch besser wappnen und Initiativen zur digitalen Transformation beschleunigen."

Indem Kunden Sicherheit und Compliance in Projekten rund um Cloudlösungen, künstlicher Intelligenz, robotergesteuerter Prozessautomatisierung und DevOps zu einem frühen Zeitpunkt adressieren, können diese besser auf Transformationsprojekte vorbereitet werden und Projekte schneller und sicherer zum Erfolg bringen.

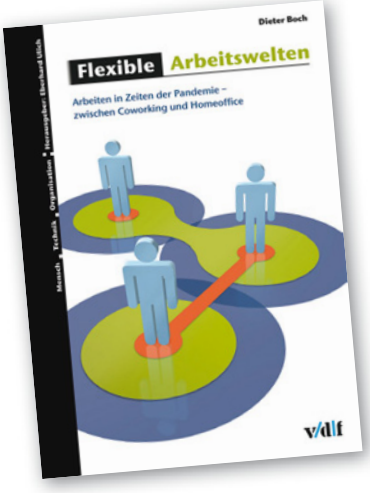
„Wir freuen uns, dass unsere Kunden durch Onapsis nun die Möglichkeit haben, SAP-Anwendungen in ihre Konzepte für Cybersicherheit und Governance, Risk and Compliance (GRC) zu integrieren", sagt Tim McKnight, Chief Security Officer bei SAP.

Die Onapsis Plattform für Cybersicherheit und Compliance ist eine der ersten Lösungen, die den Status einer SAP Endorsed App erreicht haben.

www.onapsis.com

FLEXIBLE ARBEITSWELTEN

ARBEITEN IN ZEITEN DER PANDEMIE



Mit der Corona-Krise sind die Einwände gegenüber neuen Arbeitsmodellen, Führungs- und Kommunikationsformen geringer geworden.

Dieses Buch beschreibt, wie die Arbeit verändert wahrgenommen wurde, wie schnell eine Umstellung auf Homeoffice erfolgte, wie die Menschen mi den Ausgangsbeschränkungen umgingen, wie aber auch erkannt wurde, dass bestimmte Arbeitsanforderungen den direkten Kontakt benötigen. Die gesammelte Erkenntnisse und Maßnahmen aus den befragten Unternehmen des flexible.office.network sind eine hilfreiche Orientierung zum Nachlesen.

Nicht alles, was in den letzten Jahren an Erkenntnissen gewonnen wurde, muss über Bord geworfen und auch die Arbeit nicht neu erfunden werden. Man erkannte sehr schnell, was war – auch aus der veränderten Sichtweise der Krise – bisher richtig, was muss verändert, was muss gecancelt werden. Und was muss neu in unser Bewusstsein aufgenommen werden, um den Weg in eine neue Epoche danach zu beschreiten.

Flexible Arbeitswelten
Arbeiten in Zeiten der Pandemie – zwischen Coworking und Homeoffice
Dieter Boch, vdf Hochschulverlag AG, 2021

Mit HiScout Datenschutz Schritt für Schritt zum rechtssicheren Datenschutzmanagement
(Quelle: ©dragonstock – Fotolia.com)

DATENSCHUTZ VON A BIS Z IN EINER ANWENDUNG

SCHAFFEN SIE ORDNUNG IM TOOLCHAOS

Seit Geltungsbeginn der EU-DSGVO haben viele Organisationen aus Furcht vor Abmahnungen und Geldbußen unter Zeitdruck ein Patchwork aus Teillösungen zum Datenschutz geschaffen. Diese decken zwar die kritischsten Themen ab, sind aber als Gesamtkonzept unvollständig, fehleranfällig und pflegeintensiv.

Der Alltag des Datenschutzbeauftragten besteht üblicherweise aus einer anspruchsvollen Jonglage verschiedenster Anwendungen und Formate. Änderungen müssen dabei zuverlässig und übereinstimmend in allen Dokumenten nachvollzogen werden.

Wie können Unternehmen Ihre Datenschutzprozesse besser organisieren und den Datenschutz effizient in ein Gesamtkonzept der Informationssicherheit einbinden?

Das mit Release 3.1.2. zu voller Reife entwickelte Datenschutzmodul von HiScout führt nicht nur alle Daten und Prozesse in einem System zusammen, sondern bildet auch die zugehörigen Arbeitsabläufe ab. Datenschutzeinsteiger werden Schritt für Schritt von A wie „Verzeichnis der VerArbeitungstätigkeiten" bis Z wie „LöschkonZept" durch die notwendigen Eingabemasken geleitet.

Die Basis für alle weiteren Vorgänge wird im Verarbeitungsverzeichnis gelegt, das alle Fakten der Verarbeitung von personenbezogenen Daten in vier Ebenen steigender Granularität abbildet:

1. Verzeichnis der Verarbeitungstätigkeiten,
2. Verarbeitungstätigkeit,
3. Datenart und
4. Datenobjekt.

Auf diesem Grundgerüst bauen alle weiteren Funktionen auf. Datenschutzfolgenabschätzungen, Löschkonzepte sowie Berichte für Datenschutzvorfälle und Auskunftsanfragen können per Knopfdruck im PDF-Format generiert und an die entsprechenden Behörden oder Prüfstellen weitergeleitet werden. Auftragsverarbeitungsverhältnisse und „Verarbeitungen mit gemeinsamer Verantwortung" lassen sich ebenfalls abbilden und die zugehörigen Dokumente revisionssicher aufbewahren.

Wird die Datenschutzsoftware nicht als Insellösung, sondern als Komponente eines integrierten Managementsystems eingesetzt, sind weitere Synergieeffekte möglich. Die in anderen Modulen der HiScout GRC-Suite eingepflegten Daten, Risiko- und Maßnahmenkataloge stehen bei entsprechender Berechtigung der Anwender sofort zur Verknüpfung und Nutzung im Datenschutz bereit. Ein interessanter Nebeneffekt: Die Daten für Anwendungen und Systeme in IT-Grundschutz, ISO 27001 und Business Continuity Management werden in der Regel durch IT-Spezialisten aufgenommen und zeichnen sich daher durch hohe Qualität und Vollständigkeit aus.

Fazit

Besseres Datenschutzmanagement in zwei Schritten: Die Zusammenführung der Inhalte verschiedener Tools im Modul HiScout Datenschutz entlastet bei allen datenschutzrelevanten Tätigkeiten. Sind bereits andere HiScout Module vorhanden, können die hochwertigen Daten sowie Risiko- und Maßnahmen-Kataloge aus Grundschutz, ISM und Notfallmanagement direkt im Datenschutz verwendet werden.

Daniel Linder | www.hiscout.com

CYBER SECURITY INCIDENT

SO SIND UNTERNEHMEN AUF EINEN SECURITY-VORFALL OPTIMAL VORBEREITET

IT-Security ist ein hohes Gut. Obwohl für viele Unternehmen der Schutz ihrer IT-Infrastruktur, Systeme, Workplaces und Daten oberste Priorität hat, ist die Mehrheit für einen Angriff nicht gewappnet. Wie sich Unternehmen vorbereiten und im Angriffsfall richtig reagieren, zeigen die folgenden sechs Tipps von Arvato Systems.

1. Tipp: Investieren Sie in Cyber Security.

Die meisten Unternehmen haben definierte IT-Krisenprozesse. Häufig eignen sie sich aber nicht, um einen ausgefeilten Angriff abzuwehren. Die Methoden der Hacker werden immer komplexer. Je nach Art des Vorfalls haben Sie binnen kurzer Zeit Maßnahmen einzuleiten, die oft jahrelang niemand angepackt hat. Machen Sie nicht den Fehler, erst dann zu reagieren, wenn Sie durch einen akuten Sicherheitsvorfall dazu gezwungen sind. Investitionen in Cyber Security lohnen sich, weil sie das Risiko eines kritischen Security Incidents nachweislich reduzieren.

2. Tipp: Überprüfen Sie vorhandene Security-Maßnahmen.

Um das Security-Level langfristig hochzuhalten, sollten Sie die präventiven Maßnahmen regelmäßig überprüfen: Sind sie geeignet, um einen Sicherheitsvorfall abzuwehren (Prevention) und einem tatsächlichen Angriff zu begegnen (Detection und Response)? Sie müssen jederzeit gegen hochentwickelte Angriffe gewappnet sein. Angriffsmethoden, die bisher nur von APTs (Advanced Persistent Threats) bekannt waren, sind nun auch bei gewöhnlichen Cyber-Kriminellen zu beobachten.

3. Tipp: Definieren Sie individuelle Maßnahmenpakete.

Cyber Security ist Ergebnis eines fortlaufenden Prozesses und darum höchstindividuell. Für eine erfolgreiche Incident Response (IR) gibt es mehrere Erfolgsfaktoren: Kommunikation, Organisation, Prozesse und Ressourcen. Angelehnt an die jeweiligen Prozesse, sollten Sie einzelne Maßnahmenpakete präventiv ableiten und dokumentieren. Beschreiben Sie das Ziel, die Vorgehensweise sowie die notwendigen Rollen, Unternehmensbereiche und Skills. Auch ein Incident-Response-Kommunikationsplan darf nicht fehlen.

4. Tipp: Gehen Sie strukturiert vor.

Um für den Fall der Fälle bestmöglich aufgestellt zu sein, ist die Incident Response in zwei Handlungsstränge aufzuteilen. Da wäre zunächst die forensische Untersuchung des vermeintlichen Vorfalls. Hier ermitteln Sie, wie und wie tief der Angreifer in Ihre IT-Infrastruktur eingedrungen ist, welche Ziele er verfolgt und welche Technologie er angewendet hat.

Auf dieser Basis können Sie Maßnahmen zur Abwehr des Angriffs und zur Entfernung des Angreifers aus Ihrem Netzwerk planen. Bei laufenden Vorfällen müssen Sie entscheiden, welche Handlungen ad hoc vorzunehmen (Containment) und welche vordefinierten Maßnahmen anzuwenden sind.

5. Tipp: Lernen Sie Ihre eigene Systemkritikalität kennen.

Um schützenswerte Bereiche und neuralgische Punkt zu ermitteln, müssen Sie die Eigenheiten Ihrer Organisation, IT-Infrastruktur und vorhandenen Skills genau kennen. Formen Sie ein Team aus passenden Mitarbeitern und schaffen Sie so einen idealen Mix aus Erfahrung und Skills. Diese Fähigkeiten intern aufzubauen, verursacht großen Aufwand. Regelmäßige Trainings sind unverzichtbar.

1. Tipp: Setzen Sie auf Teamwork.

Bei einem Angriff ist das ganze Security-Team gefragt. Handelt es sich um einen massiven Vorfall, koordiniert das Incident Response Team die Eindämmungs- und Bereinigungsaktivitäten und führt sie durch. Wichtig ist auch die Nachbereitung. Wer aus einem Vorkommnis strategische Maßnahmen ableitet, kann eine bessere Reaktionsfähigkeit und Resilienz entwickeln.

Arne Wöhler

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

Arne Wöhler, Leiter Business Consulting und Development Cyber Security, Arvato Systems, www.arvato-systems.de

TOTGESAGTE LEBEN LÄNGER

DATENSCHUTZBEDENKEN BEI MESSENGER-DIENSTEN

Viele Nutzer des Messenger-Dienstes WhatsApp ließ kürzlich folgende Meldung aufhorchen: „WhatsApp aktualisiert seine Nutzungsbedingungen und Datenschutzrichtlinien." Was das konkret heißt? Sie werden dazu aufgefordert, den neuen Regeln zuzustimmen. In Europa scheint zwar vorerst alles beim Alten zu bleiben, aber außerhalb der EU und Großbritannien fällt zukünftig unter anderem die Opt-Out-Option weg. Damit war es Usern bis dato weltweit möglich zu entscheiden, ob ihre persönlichen Daten an Facebook zu Werbezwecken oder zur Verbesserung von Produkten weitergegeben werden dürfen. Obwohl die Deaktivierung des Opt-Out aufgrund der geltenden Datenschutz-Grundverordnung (DSGVO) in Europa hinfällig ist, befürchten auch hierzulande zahlreiche Nutzer Risiken für den Datenschutz. Während sich also eine Vielzahl an Usern auf die Suche nach alternativen Messenger-Diensten für den privaten Gebrauch begibt, wird im Geschäftsalltag nochmals mehr die E-Mail als zentraler elektronischer Kommunikationskanal genutzt.

Eine Rolle rückwärts

Messenger-Dienste sind aus dem Privatleben vieler Menschen nicht mehr wegzudenken. Laut einer Statista-Umfrage aus dem Jahr 2020 zählt WhatsApp nach wie vor als beliebtester Messenger in Deutschland. Das Chatten über WhatsApp gestaltet sich besonders einfach: Man kann seine Familienmitglieder oder Freunde schnell etwas fragen oder einen Gruppenchat eröffnen, um beispielsweise ein gemeinsames Event zu planen. Bei all den Vorzügen, die der Messenger bietet, werden seit seiner Übernahme durch Facebook aber immer auch Datenschutzbedenken laut. Die erneute Änderung der Nutzungsbedingungen und Datenschutzrichtlinien trägt dabei nicht gerade zur Besserung bei. Im Gegenteil: Es gibt immer mehr Menschen, die sich Gedanken darüber machen, was mit ihren übermittelten Daten passiert. Wenn sich diese Unsicherheiten sogar schon bei Privatnutzern zeigen, sind die Bedenken im Geschäftsumfeld hinsichtlich Messenger-Diensten natürlich umso größer. In puncto elektronischer Kommunikation mit Geschäftspartnern landen Nutzer daher im Endeffekt meistens wieder bei der „guten alten E-Mail", die vor geraumer Zeit bereits totgesagt wurde.

E-Mail als sichere Alternative

Trotz der diversen Messenger-Dienste, die es mittlerweile gibt, sind E-Mails im Unternehmensalltag noch immer das am meisten genutzte Kommunikationsmittel. Denn anders als bei so manchem Messenger kann man sich bei E-Mails sicher sein, dass sie durch den Einsatz professioneller Security-Lösungen jederzeit vor dem Zugriff Dritter geschützt sind. Dies ist für Unternehmen, die tagtäglich sensible Daten an Kollegen, Kunden oder Partner versenden müssen, essenziell. In Anbetracht der steigenden Anzahl an Cyberangriffen reicht es inzwischen nicht mehr aus, den Sicherheitsvorkehrungen von Messenger-Diensten blind zu vertrauen. Stattdessen gilt es, eigene Maßnahmen zu ergreifen, die einen lückenlosen Schutz gewährleisten. Im Gegensatz zu Messengern wie WhatsApp ist dies bei E-Mails problemlos möglich. Durch die Implementierung einer umfassenden europäischen Secure E-Mail-Lösung wird das Mitlesen oder Abgreifen sensibler Informationen zu jedem Zeitpunkt verhindert. Außerdem behält man so stets die Hoheit über die eigenen Daten und geht einen wesentlichen Schritt in Richtung der digitalen Souveränität. Hinzu kommt, dass moderne Lösungen äußerst benutzerfreundlich sind und sich einfach in den Unternehmensalltag integrieren lassen. Auf diese Weise können E-Mails genauso einfach verschickt werden wie per WhatsApp. Dabei sind die Inhalte sicher und die Weitervermarktung der Nutzerdaten wird unterbunden.

Günter Esch

DURCH DIE IMPLEMENTIERUNG EINER UMFASSENDEN EUROPÄISCHEN SECURE E-MAIL-LÖSUNG WIRD DAS MITLESEN ODER ABGREIFEN SENSIBLER INFORMATIONEN ZU JEDEM ZEITPUNKT VERHINDERT.

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

LIVE WEBINAR
AM 17.03.2021
11:00 UHR

SECURITY AWARENESS IN HOLLYWOOD-QUALITÄT

WIE SIE IHRE MITARBEITER MIT TRAININGS BEGEISTERN

IT Security ist nicht nur eine Frage der technischen Maßnahmen, der „Faktor Mensch" spielt eine wesentliche Rolle. Ransomware-Angriffe beispielsweise basieren in neun von zehn Fällen auf Phishing E-Mails und potenziell jeder Mitarbeiter ist gefährdet auf solche Angriffe hereinzufallen.

Um eine eigene „Human Firewall" im Unternehmen zu etablieren, empfiehlt es sich, ein nachhaltig wirkendes Security Awareness Programm aufzulegen – und zwar mit nachhaltigen Verhaltensänderungen statt reiner Wissensvermittlung. Dies gelingt am besten mit Trainingsinhalten, die Nutzer wirklich spannend finden.

Wie Sie Ihre Mitarbeiter wirklich begeistern

- Die Dos & Don`ts wirklich wirksamer Security Awareness Maßnahmen
- Warum reicht „ein bisschen Training" nicht aus?
- Weshalb ist die Qualität der Trainingsinhalte so entscheidend für den Erfolg von Awareness-Kampagnen?

Detlev Weise
ist Security Awareness Advocat für KnowBe4

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

HYPE ASIDE

WIE CYBER SECURITY MIT KI REALISTISCH FUNKTIONIEREN KANN

LIVE WEBINAR
AM 18.03.2021
11:00 UHR

In diesem Webinar skizziert Arnold Krill, genua GmbH, den Einsatz von KI in der Cyber Security. Er schlüpft dazu sowohl in die Rolle des Angreifers als auch des Verteidigers. Abschließend gibt er einen Ausblick, welche KI-Helfer für eine Vertrauensvolle Zusammenarbeit zwischen Maschine, Netzwerkadministrator und Sicherheitsexperte realistisch ist.

Die Möglichkeiten scheinen endlos, der Effizienzgewinn substantiell: Der Einsatz von KI zur Absicherung von Computernetzwerken nimmt laut Technologieanalysten immer mehr Fahrt auf. Doch welche Erwartungen werden heute bereits erfüllt und wo bleibt die Realität bisher hinter den Vorstellungen zurück?

Warum Sie unbedingt teilnehmen sollten:

- Spannende Beispiele für KI in der Cyber Security
- Warum Vertrauen in die Cyber-Security-Kollegen wichtig ist, insbesondere, wenn sie künstlich sind
- Möglichkeiten für den realistischen und effektiven Einsatz von KI in der Cyber Security

Arnold Krille ist
Abteilungsleiter
Productdevelopment
cognitix bei genua

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

WAS MAN NICHT SIEHT, KANN MAN NICHT AUFHALTEN

CYBERANGRIFFEN VORBEUGEN UND SCHWACHSTELLEN ERKENNEN

Viele Unternehmen sind sich der Schwachstellen in ihren IT-Anwendungen nicht bewusst. Wenn es jedoch an kritischer Transparenz an den Endpunkten mangelt, haben Cyberkriminelle leichtes Spiel. Am Ende bleibt häufig nur, Malware-Infektionen zu bereinigen und die Mitarbeiter im Nachhinein über Patches aufzuklären. Was wäre aber, wenn Firmen ihre Mitarbeiter anweisen könnten, die richtigen Anwendungen zu patchen, bevor eine der Schwachstellen einem Angriff zum Opfer fällt?

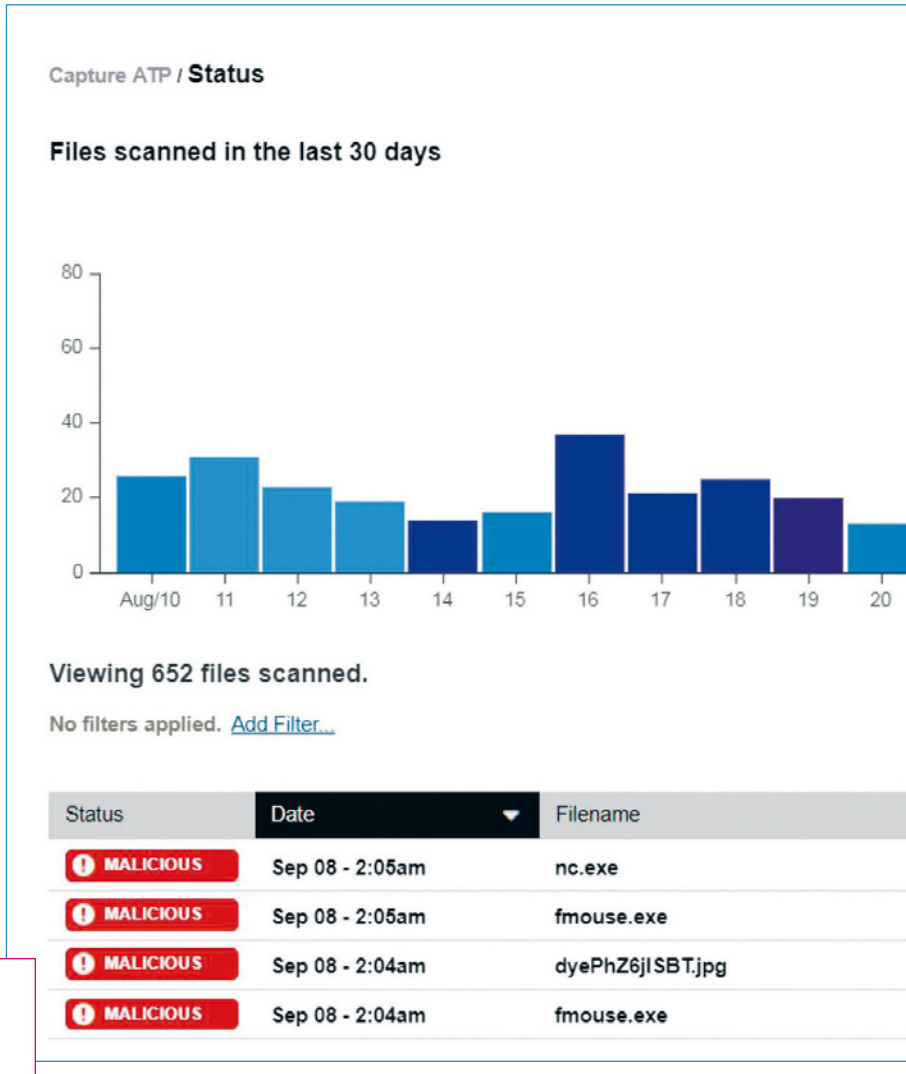
Um das Risiko von Cyberangriffen zu reduzieren und sie im Ernstfall abzuwehren, müssen Unternehmen zuerst kritische Schwachstellen in ihrer IT-Landschaft erkennen. Hierfür eigenen sich Sandbox-Lösungen besonders gut: In isolierten Systemumgebungen können so Anwendungen getestet, auf Schwachstellen untersucht und die Auswirkungen von Malware geprüft werden.

Moderne Plattformen wie SonicWalls Capture Advanced Threat Protection (ATP) nutzen hierbei Virtualisierungstechniken, um verdächtiges Code-Verhalten zu analysieren. Die Lösung scannt den Datenverkehr, extrahiert verdächtigen Code zur Analyse und deckt einen breiten Bereich von Dateigrößen und -typen ab.

Im Speicher versteckte Bedrohungen aufdecken

Netzwerk-Sandbox-Engines führen Dateien aus, protokollieren die resultierende Aktivität und suchen daraufhin nach bösartigem Verhalten. Die Bewertung dieser Aktivitäten und Verhaltensweisen sind in der Praxis anfällig für Fehleinschätzungen. Althergebrachte Sandbox-Systeme zogen häufig Verzögerungen im Arbeitsablauf, eine unbefriedigende Endnutzererfahrung und unzählige IT-Tickets nach sich.

Damit bösartiges Verhalten verborgen bleiben kann, setzen Malware-Autoren



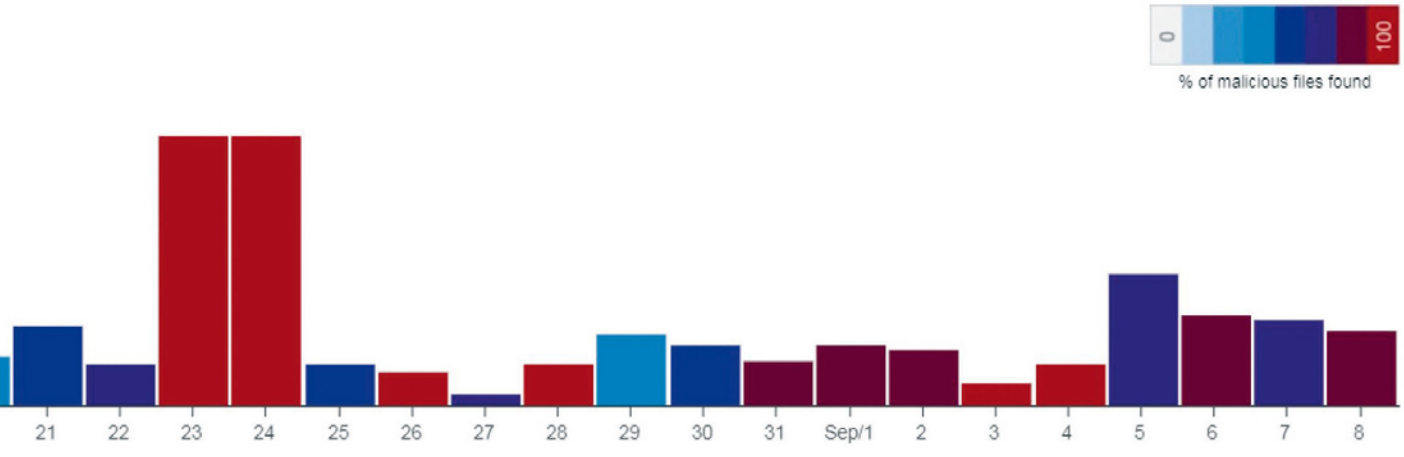
Das SonicWall Capture ATP-Reporting zeigt die täglichen Ergebnisse auf einen Blick.

fortschrittliche Techniken ein, darunter benutzerdefinierte Verschlüsselungen und Verschleierungstaktiken, die gegenüber der Sandbox gutartiges Verhalten vortäuschen. Diese Techniken verbergen oft ausgefeilte Waffen, die nur bei der dynamischen Ausführung der Malware sichtbar werden. In den meisten Fällen ist es unmöglich, diese Vorgänge in Echtzeit mit statischen Erkennungstechniken zu analysieren. Eine aktuelle Multi-Engine-Sandbox verfügt über die Fähigkeit, Dateien am Gateway zu blockieren, bis ein Urteil über sie gefällt wurde. Das Multi-Engine-Design ist darauf ausgelegt, ausweichende Malware zu erkennen und zu stoppen. Unbekannte Dateien können so in isolierten parallelen Umgebungen verarbeitet werden, um zu sehen, was verdächtiger Code zu tun beabsichtigt – von der Anwendung über das Betriebssystem bis hin zur Software, die sich auf der Hardware befindet.

Aktuelle Cybersecurity-Technologie erkennt und blockiert Malware, die kein bösartiges Verhalten zeigt und ihr schadhaftes Potential durch Verschlüsselung versteckt. Um gepackten und komprimierten Malware-Code zu entdecken wird dieser in einer sicheren Sandbox-Umgebung entpackt. Die Sandbox-Engine macht ersichtlich, welche Code-Sequenzen sich in den gepackten Dateien verbergen und vergleicht sie mit vertrauenswürdigen Code-Sequenzen. Die Identifizierung von bösartigem Code im Speicher ist dabei präziser als der gängige Ansatz, das Systemverhalten von Malware dem Verhalten von sauberen Programmen gegenüberzustellen.

Echtzeitanalyse von Malware

Um die eigenen Systeme effektiv abzusichern, muss bösartiger Code im Speicher in Echtzeit während der Ausführung erkannt werden. SonicWalls Capture Advanced Threat Protection bietet hierfür die Technologie Real-Time Deep Memory (RTDMI). RTDMI-Engine erkennt und blockiert proaktiv Zero-Day-Bedrohungen und unbekannte Malware durch Inspektionen direkt im Speicher. Die Echtzeit-Architektur der Technologie macht diese präzise, minimiert Fehlalarme und identifiziert und entschärft anspruchsvolle Angriffe.



	Submitted by	Src	Dest
	C0EAE481E	203.81.81.	192.168.104.
	C0EAE481E	47.89.251.	192.168.104.
	C0EAE481E	185.91.116.	192.168.104.
	C0EAE481E	47.89.251.	192.168.104.

Dabei ist es besonders wichtig, dass die Sicherheitslösung die Analyse eines breiten Spektrums von Dateitypen und -größen unterstützt. Einschließlich ausführbarer Programme, PDFs, MS-Office-Dokumenten, Archiven, JAR- und APK-Dateien. Auch unterschiedliche Betriebssysteme, einschließlich Windows und Android, müssen unterstütz werden. Administratoren müssen die Option haben, den Schutz individuell anzupassen: So sollten sie Dateien auswählen beziehungsweise ausschließen und diese zur Analyse an einen Cloud-Dienst senden können. Um zu verhindern, dass potenziell bösartige Dateien in das Netzwerk gelangen, werden dabei die Dateien, die zur Analyse an den Cloud-Dienst gesendet werden, am Gateway zurückgehalten, bis sie final bewertet werden konnten.

Wenn eine Datei als schädlich identifiziert wird stellen zeitgemäße Cybersecurity-Plattformen eine Signatur für Firewalls zur Verfügung, um Folgeangriffe zu verhindern. Darüber hinaus wird die Malware in der Regel an den Security-Anbieter zur weiteren Analyse und Aufnahme in eine Datenbank weitergeleitet.

Reports und Alerts übersichtlich anzeigen

Eine gute Sicherheitsplattform sollte auch umfassende Übersichtsfunktionen bieten: Zum Beispiel ein Dashboard, das Bedrohungsanalysen und Berichte präsentiert und Analyseergebnisse zusammenfasst – inklusive Quelle, Ziel und weiteren Details zur Malware. Auch Firewall-Protokollwarnungen und Benachrichtigungen über verdächtige Dateien sollten einfach abzurufen sein.

Bei SonicWalls Capture Advanced Threat Protection geben beispielsweise übersichtliche Balkendiagramme Aufschluss darüber, an welchen Tagen Malware entdeckt wurde. Administratoren haben die Möglichkeit, auf einzelne Tagesergebnisse zu klicken und Filter anzuwenden, um schnell bösartige Dateien und relevante Ergebnisse zu sehen.

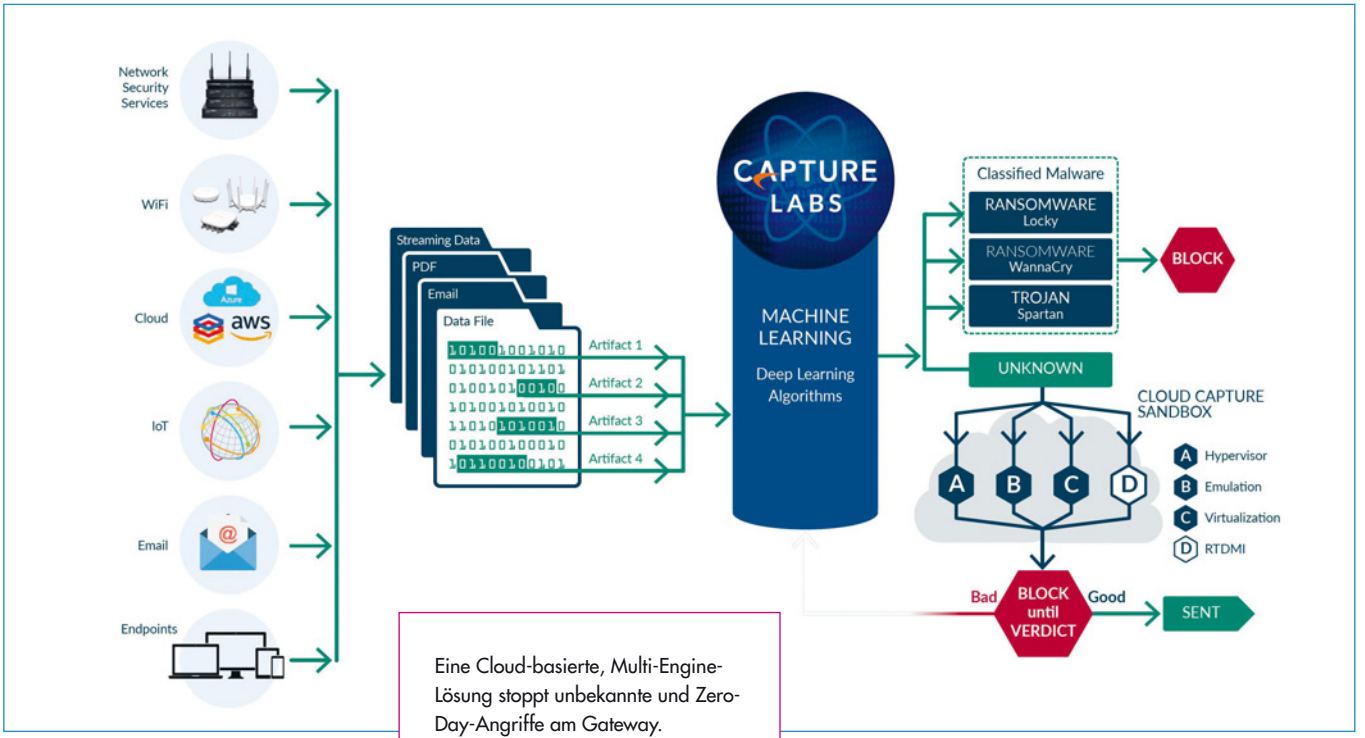
Fazit

Mit einer modernen Cloud-basierten Multi-Engine-Lösung für Cybersecurity stoppen Unternehmen Angriffe auf ihr Netzwerk und verbessern die Erkennungsraten bei der Analyse von Dateien deutlich. Bedrohungen und unbekannte Malware werden proaktiv aufgedeckt, analysiert und beseitigt.

Silvan Noll

EINE GUTE SICHERHEITSPLATTFORM SOLLTE AUCH UMFASSENDE ÜBERSICHTSFUNKTIONEN BIETEN: ZUM BEISPIEL EIN DASHBOARD, DAS BEDROHUNGSANALYSEN UND BERICHTE PRÄSENTIERT UND ANALYSEERGEBNISSE ZUSAMMENFASST.

Silvan Noll, SE Manager Central Europe, SonicWall, www.sonicwall.com



Eine Cloud-basierte, Multi-Engine-Lösung stoppt unbekannte und Zero-Day-Angriffe am Gateway.

EDR ON PREMISES?

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 neuen Regulierung, 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 zu entsprechen. 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 zum kostenlosen Download bereit. ***www.it-daily.net/download***

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Markus Grüneberg, Günter Esch, Dr.-Ing. Christian Haas, Dirk Kalinowski, Carina Mitzschke, Silvan Noll, Jens Otto, Silvia Parthier, Ulrich Parthier, Arne Wöhler

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

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

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

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

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

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

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

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

Erscheinungsweise:
10x pro Jahr

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

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

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

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

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

Thought Leadership