itmanagement

MAI 2019

MAGAZIN FÜR DIE ENTERPRISE IT

INKLUSIVE 32 SEITEN
IT SECURITY SPEZIAL

UX-DESIGN
Schluss mit dem Guesswork

CONTAINER TO GO!
Dank Docker aus der Nische

PROJEKT-MANAGEMENT
Prozesse sinnvoll fit machen

RISK ADAPTIVE PROTECTION
THOUGHT LEADERSHIP

ENTERPRISE-RESOURCE-PLANNING

ARE YOU READY FOR THE FUTURE?

Klaus Bikar, Geschäftsführer, IAS GmbH

www.it-daily.net

STILLSTAND BIRGT GEFAHREN

Analysieren – Informieren – Handeln

www.it-daily.net/leser-service

Jetzt itsecurity lesen!
Den Überblick behalten.

it-daily.net

HP MIT ROLLE RÜCKWÄRTS?

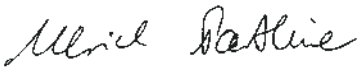
HP galt einst als Technologiekonzern und hatte sich der Innovation verschrieben, ja den Begriff Innovation sogar als Slogan im Logo verankert. Ähnliches konnte man von 3M, IBM und vielen anderen Unternehmen der IT-Branche sagen. Doch diese Zeiten sind passé, seit es nur noch um eins geht: Geld und Märchen für die Börse. Dazu zählen Firmenkäufe, um Wachstum zu suggerieren und im Fall von HP dann halt auch mal Abspaltungen. Beides macht zwar in der Regel keinen Sinn, aber irgendein CEO hat Träume und ist im Märchenerzählen ein Meister. Bei HP waren das mit Cara Carleton „Carly" Fiorina, Léo Apotheker und Margaret „Meg" Cushing Whitman einige zu viel.

Jedenfalls war ich doch ziemlich erstaunt, als ich Mitte April die Meldung bekam, dass auf dem diesjährigen Innovation Summit HP die neue Lösung HP Sure Sense vorstellt. Die auf Künstlicher Intelligenz (KI) basierende Sicherheitslösung soll beim Schutz gegen Angriffe auf Deep Learning setzen.

Unternehmen sehen sich zunehmend mit Bedrohungen durch Malware und Firmware konfrontiert. Damit will laut Pressmitteilung HP seine Position als Anbieter der weltweit sichersten und kontrollierbarsten PCs stärken. HP Sure Sense soll in der neuen HP EliteBook 800 G6-Serie sowie für das HP ZBook 14u und das HP ZBook 15u verfügbar sein.

Aber hatte HP nicht den Softwarebereich in HP Enterprise abgespalten und dann später noch einmal große Teile seiner Enterprise Sparte, einschließlich der Security-Produkte, mit Micro Focus „fusioniert"? Wird es weitere Security-Produkte geben oder ist dies ein singuläres Ereignis, das nur das Ziel hat so etwas wie einen usp für seine Kernprodukte - na sagen wir mal - „zu entwickeln". Obwohl der Ansatz für mehr Schutz sicher richtig ist, sieht Innovation meiner Meinung nach anders aus.

Herzlichst Ihr



Ulrich Parthier | Publisher it management

INHALT

Inklusive
32 Seiten

IT SECURITY SPEZIAL

EFFIZIENZ VOR ECHTEM MEHRWERT

DEUTSCHE UNTERNEHMEN NUTZEN EIGENE INNOVATIONSPOTENZIALE NICHT AUS.

Innovation ist für viele Unternehmen das Mittel der Wahl, um schnelleres Wachstum, höhere Umsätze oder entscheidende Wettbewerbsvorteile zu erzielen. Eine aktuelle Studie des Beratungsunternehmens Accenture zeigt jedoch, dass Unternehmen beim Innovationsmanagement häufig den falschen Schwerpunkt setzen. Demnach konzentrieren sie sich zu sehr darauf, bestehende Produkte und Services effizienter zu gestalten, anstatt neue Geschäftsfelder zu erschließen.

Damit reagieren sie zwar auf kurzfristige Kunden- und Markterwartungen. Um Innovationen in langfristigen Erfolg umzuwandeln, ist jedoch die Etablierung einer echten Innovationskultur entscheidend.

„Deutsche Unternehmen schauen zu sehr darauf, was andere machen", sagt Sigrid Stinnes, Innovation Lead bei Accenture für Deutschland, Schweiz und Österreich. „Ideen zu übernehmen, kann kurzfristig Erfolg bringen. In Zeiten der Digitalisierung sind allerdings die Unternehmen erfolgreicher, die als erste am Markt sind und ihre Innovationen schnell in die Breite bringen – und das weltweit. Allein durch eine Verbesserung der eigenen Wettbewerbsfähigkeit den Status Quo zu wahren, kann nicht unser Anspruch sein."

Die wichtigsten Erkenntnisse

82 %
der Unternehmen wollen mit Innovationen vor allem ihre bestehenden Produkte und Services verbessern. Nur ein Drittel setzt auf Veränderungen in den Management- und Organisationseinheiten.

59 %
der Befragten sieht eine große Herausforderung darin, aus neuen Ideen messbaren Mehrwert für das Unternehmen zu generieren.

87 %
betrachten künstliche Intelligenz als maßgebliche Technologie, um Innovationen voranzutreiben.

Innovation ist Aufgabe für das Top-Management

Als größte Herausforderungen bezeichneten die befragten Manager die Etablierung einer Innovationskultur (61 Prozent), aus Ideen echte Werte zu schaffen (59 Prozent), die Koordination verschiedener Innovationsinitiativen (52 Prozent) sowie die Begeisterung der Belegschaft für Innovation zu wecken (50 Prozent). Nur jedes dritte Unternehmen plant allerdings daraus abgeleitete Veränderungen im Management oder der Organisation. Dies ist jedoch die Voraussetzung, um Innovationen in konkrete neue Produkte, Dienstleistungen oder Geschäftsmodelle zu übersetzen.

Kunde steht bei Innovation im Mittelpunkt

Für die große Mehrheit der befragten Unternehmen sind das Kundenerlebnis und der Kundennutzen Ausgangspunkt für ihre Innovationsbemühungen. So erklärten 87 Prozent der Führungskräfte, dass dies für ihr Unternehmen das Leitmotiv sei. Essenziell ist dafür, die Kundenwünsche genau zu kennen. Immerhin 81 Prozent der Unternehmen nutzen bereits systematische Datenmanagement-Tools für Absatz- und Bedarfsprognosen. Dennoch gelingt es nur etwas mehr als der Hälfte der Unternehmen (56 Prozent), eine umfassende Sicht auf ihre Kunden zu bekommen.

www.accenture.de

Produktfokussierte Innovationen

82 %
nutzen Innovationen, um bestehende Produkte/Services weiterzuentwickeln.

72 %
nennen die Steigerung der eigenen Wettbewerbsfähigkeit als Hauptmotivator für Innovationsarbeit.

55 %
betrachten sich als Innovationsfolger, die Neuheiten zwar schnell übernehmen, selbst aber nicht die Richtung vorgeben.

MENSCH ODER MASCHINE?

WO KÜNSTLICHE INTELLIGENZ DIE FÄHIGKEITEN DES MENSCHEN ÜBERTRIFFT.

Um das Thema KI ranken sich viele Missverständnisse und Mythen. Die AI4U, eine von Deutschlands führenden Konferenzen zum Thema Künstliche Intelligenz (KI), die sich interdisziplinär an alle Stakeholder in diesem Themenumfeld richtet, erklärt in einer vereinfachten Infografik, wo KI die Intelligenzleistung des Menschen heute übertrifft und wo es auch in absehbarer Zukunft nicht ohne den Faktor Mensch gehen wird.

Der Nutzen von künstlich intelligenten Computersystemen für die Menschheit wird in der Öffentlichkeit äußerst kontrovers diskutiert. Bedeutet KI für die einen das Ende stupider Arbeiten und einen Aufbruch in neue Aufgabenfelder, sehen andere vor allem die Bedrohung ganzer Berufsgruppen darin. Tatsache aber ist: KI ist heute noch weit davon entfernt, den Menschen in all seinen Intelligenzleistungen zu ersetzen!

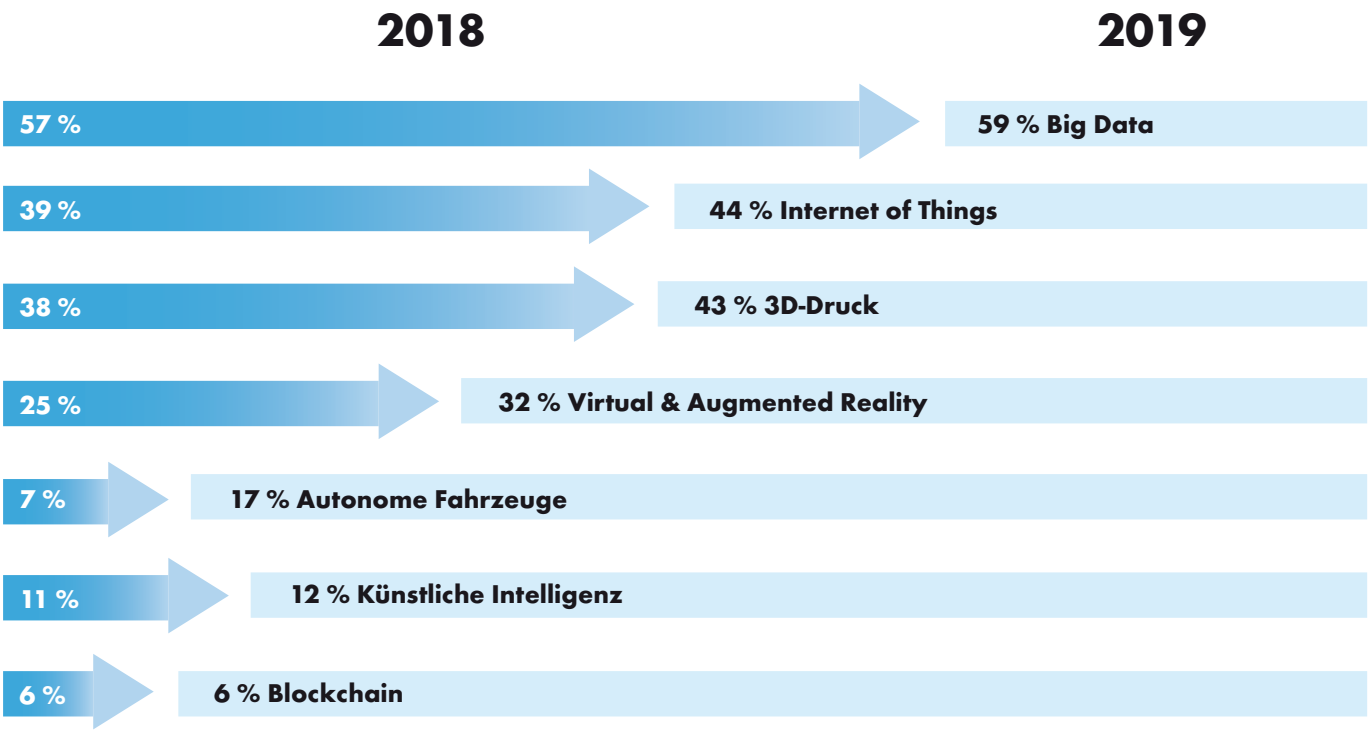
Zwar kann KI in kürzester Zeit gigantische Datenmengen verarbeiten, daraus Muster und Zusammenhänge erkennen, Rückschlüsse ziehen und Vorhersagen treffen. Die Logik hinter den Zusammenhängen aber sieht KI nicht. Denn die menschliche Intelligenz, grob aufgeteilt in die Bereiche Wahrnehmung, Denken, Wissen und Lernen/Trainieren, wird in ihrer Komplexität und Leistungsfähigkeit von KI-Systemen längst nicht erreicht. Prof. Dr. Andreas Dengel, Standortleiter am Deutschen Forschungszentrum für Künstliche Intelligenz in Kaiserslautern und Fachbeirat der AI4U erklärt: „KI-Systemen fehlt ein Bewusstsein. Beispielsweise übersetzen sie heute in Realzeit besser als die allermeisten Simultandolmetscher, haben aber keine Ahnung, welche Sprache sie übersetzen, was der Text bedeutet und welche Wirkung er auf den Leser hat."

www.ai4u-konferenz.de

DIGITALISIERUNG

TOP-TECHNOLOGIEN KOMMEN NUR LANGSAM IN DER PRAXIS AN.

Welche Technologien werden in Ihrem Unternehmen genutzt oder der Einsatz ist geplant/wird diskutiert?

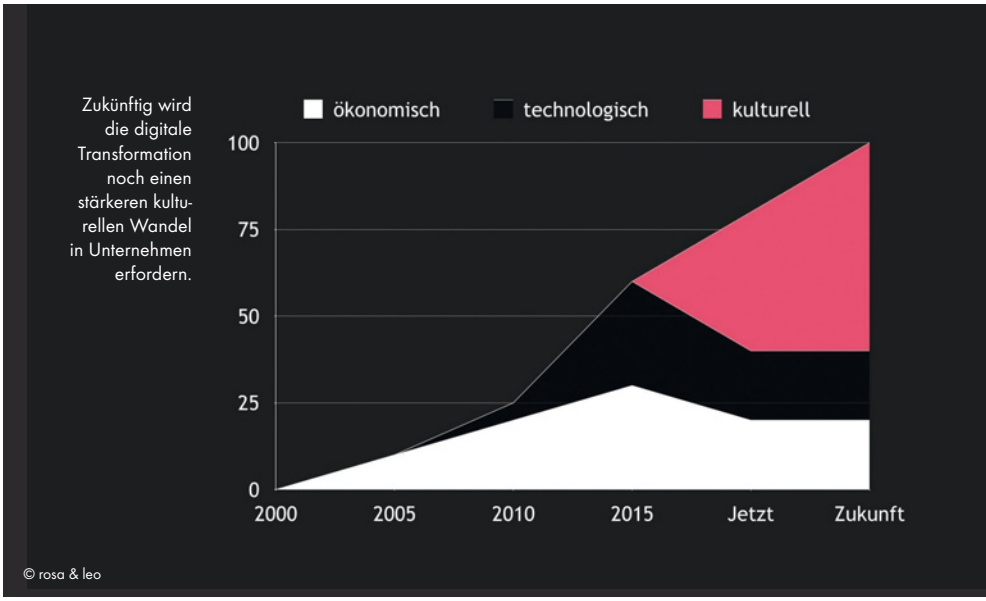


www.bitkom.org

NEW WORK IM ZUGE DER DIGITALISIERUNG

Vielschichtiges Phänomen statt plumper Parole.

Die Digitalisierung hat in der Arbeitswelt zu einem erheblichen Wandel geführt. Während sich einige Unternehmen noch nicht weiter mit dem Thema befasst haben, ist die Digitalisierung für andere schon seit vielen Jahren der Treiber, um sich als Unternehmen neu auszurichten. Dabei beschränkt sie sich nicht auf einzelne Geschäftsbereiche, sondern verursacht einen umfassenden ökonomischen, technologischen und kulturellen Wandel innerhalb von Organisationen. Wenn Unternehmen New Work leben und die digitale Transformation aktiv voranbringen möchten, sollten sie Folgendes beachten:



DREI GUTE GRÜNDE DAFÜR – UND DREI MÖGLICHE FALLSTRICKE.

SICHERHEIT AUS DER CLOUD

Cloud-Lösungen sind auch im IT-Security-Bereich zunehmend verbreitet. Viele Anbieter verlagern Sicherheitsmechanismen und andere Dienste in ihre Rechenzentren, anstatt diese auf klassische Weise bei den Kunden vor Ort (On-Premises) zu betreiben.

Doch ist die Anti-Malware-Lösung aus der Cloud tatsächlich die geeignete Variante für jeden Anwendungsfall? Und wo genau liegen eigentlich die möglichen Vor- und Nachteile des Virenschutzes aus der Wolke?

Pro Cloud:
- Schnellere Reaktion und kleinere Updates
- Erweiterte Untersuchungstechniken
- Schwarm-Intelligenz: Sicherheit durch die Community

Contra Cloud:
- Datenübertragung: Welche Daten fließen ab?
- Echtzeitüberwachung: Geschwindigkeit ist Trumpf
- Die Verbindung zur Cloud ist weg – was nun?

www.tabidus.com

1. Fehlerkultur leben

Galten Fehler bislang als Karrierekiller, sind sie in der Arbeitswelt inzwischen nicht mehr zwingend negativ besetzt. Viel wichtiger ist es allerdings, dass Mitarbeiter ebenso wie die Mitglieder der Führungsebene ihre Schwächen kennen. Denn nur wer sich diese bewusst macht und weiß, wo potenzielle Fehlerquellen lauern, kann aktiv daran arbeiten und sich verbessern. Die wachsende Fehlertoleranz in den Unternehmen zeigt sich auch in der zunehmend agilen Arbeitsweise. Projekte haben sich in den vergangenen Jahren zu Prozessen gewandelt, die Unternehmen heute nur noch sehr selten linear abarbeiten. Üblich ist vielmehr ein iteratives Vorgehen, bei dem das aktuelle Tun permanent hinterfragt wird. In diesem Zusammenhang ist deshalb eine positive Fehlerkultur unerlässlich: Nur ein selbstkritisches Team aus authentischen Menschen wird in der Lage sein, die digitale Transformation erfolgreich zu meistern.

2. Miteinander kommunizieren

In der Realität kommen in vielen Unternehmen Prozesse zum Erliegen, weil es an der Kommunikation untereinander hapert. Ohne gute Kommunikation kann New Work nicht funktionieren. Das Prinzip der „Permanent Communication" ist ein wichtiger Erfolgsfaktor, denn die Kommunikation macht in unserer heutigen Arbeitswelt oftmals mehr als 60 Prozent der Arbeitszeit aus.

Die neue Arbeitswelt dreht sich künftig noch stärker um gelungene Arbeitskultur, zufriedene Mitarbeiter sowie um die räumliche Verschmelzung von beruflichen und privaten Bereichen. Eine solche Kultur erfolgreich im Unternehmen zu etablieren, stellt viele Firmen vor enorme Herausforderungen. New Work ist keine Parole, sondern ein Phänomen eines umfassenden kulturellen Wandels. Im „New Work Trend Report 2019" hat rosa & leo die Top 10 Trends der zukünftigen Arbeitswelt zusammengestellt. Es bietet Unternehmen eine wertvolle Stütze, wenn sie New Work etablieren wollen und steht ab sofort als Download unter folgendem Link zur Verfügung: **https://rosaundleo.agency/new-work-trendreport-2019/.**

ERP: ARE YOU READY

DIE HERAUSFORDERUNGEN FÜR ERP-SYSTEME SIND VIELFÄLTIG.

Wie sieht die Zukunft von ERP-Systemen aus? Hersteller wie Anwender müssen sich aufgrund der Langlebigkeit der Systeme heute mit den Anforderungen von morgen beschäftigen. Klaus Bikar, Geschäftsführer der IAS GmbH, spricht darüber mit Ulrich Parthier, Herausgeber it management.

Ulrich Parthier: *Bei der Vielzahl der ERP-Systeme am Markt fällt Anwendern der Überblick schwer. Welches könnte die passende ERP-Lösung sein? Gibt es aus ihrer Sicht Basisvoraussetzungen?*

Klaus Bikar: Nicht nur die Funktionen, sondern auch die technologische Infrastruktur und Flexibilität sind wichtig. Das ERP-System soll eine Plattform bieten, die neben den aktuellen auch die zukünftigen Anforderungen erfüllen kann. Während die Anzahl der digitalisierten Prozesse steigt, wird die Zeit, in der sich Unternehmen anpassen müssen, kürzer. Deshalb ist es für uns entscheidend ein schnelles und anpassungsfähiges System anzubieten, welches flexibel ist und sich leicht an dynamischen Bedürfnissen heute und in Zukunft anpassen lässt.

Ulrich Parthier: *Bleiben wir bei den Anforderungen auf der Business-Seite. Das Prozessmanagement ist hier ein wichtiges Thema. Die flexible Steuerung und Anpassung von Prozessen ist extrem wichtig und sollte den Anwendern leicht gemacht werden. Wie ist dieses Problem im caniasERP gelöst?*

Klaus Bikar: Leider ist es einem ERP-System nicht möglich, alle Varianten aller Prozesse abzubilden. Wir bieten deshalb flexible Systeme an, die prozessual angepasst werden können. Mit dem Modul Business Process Management, sind unsere Kunden in der Lage, die Geschäftsprozesse innerhalb ihrer ERP-Systeme zu verwalten, zu ändern und neue Prozesse dem System hinzuzufügen. Wenn es um eine drastische Modifikation geht, ist unsere integrierte Entwicklungsplattform TROIA zur Stelle. Zusammen mit unserem Produkt stellen wir auch unsere Quellcodes und Entwicklungsumgebung zur Verfügung. So können unsere Kunden nahezu alle Änderungen in ihren Anwendungen umsetzen oder bei uns anfordern.

Ulrich Parthier: *Das Thema Industrie 4.0 war eines der beherrschenden Themen auf der diesjährigen Hannover Messe Industrie. Wie gehen sie dies Thema für ihre Kunden an?*

Klaus Bikar: Wir betrachten Big Data im Mittelpunkt unseres Konzepts. Wir haben unsere Business Intelligence-Plattform Canias IQ entwickelt, um Analysen zu diesen großen Daten schnell und effektiv zu erstellen. Wir haben unsere Produkte IoT-Gateway und IoT-Connector entwickelt, um Echtzeitdaten aus der Fertigung zu sammeln, zu verwalten und zu überwachen. Wir bieten mit unserem neuen Production Intelligence Modul die Möglichkeit, die Produktion live zu verfolgen. Mit unseren EDI-, XML-, JSON-, HTTP-, TCP- und Webservice-Funktionen können wir ERP-Daten auch mit Daten aus vielen verschiedenen Quellen versorgen. Wir haben an unserer eigenen Datenbankserverlösung IASDB gearbeitet, um Daten in relationaler und objektiver Form effizienter zu verarbeiten und zu speichern. Mit unserem neuen HTML-basierten Client, erweitern wir unsere Mobilitätsmöglichkeiten. Wir haben auch unsere Integrationsfähigkeiten erweitert, um die Kommunikation mit anderen Softwaresystemen zu erleichtern. Alles in allem arbeiten wir kontinuierlich mit großem Einsatz daran, unsere Lösungen zu verbessern, indem wir das Thema Industrie 4.0 aus einer sehr breiten Perspektive betrachten und die Bedürfnisse unserer Kunden in allen Bereichen antizipieren.

Ulrich Parthier: *Industrie 4.0 und die Vernetzung von Mensch und Maschine werden immer mehr nachgefragt. Spielen Sicherheitsaspekte bei Kunden auch eine Rolle und wie können Sie diese Fragen beantworten?*

Klaus Bikar: Mit zunehmender Anzahl der verbundenen Parteien, werden Datenschutz und -sicherheit für alle Systeme zu einem größeren Anliegen. Für unsere Kunden steht dabei insbesondere der Schutz ihrer Unternehmensdaten im Vordergrund. Die Bedeutung des Datenschutzes kommt weltweit auch in neuen Verordnungen zum Ausdruck, wie zum Beispiel in der DSGVO, die seit dem 25. Mai 2018 unmittelbar in allen EU-Ländern gilt. Daher investieren wir in die Verbesserung unserer Sicherheits- und Datenschutzfunktionalitäten.

Ulrich Parthier: *Der dritte Aspekt in der Zukunftsdiskussion von Software ist der der Künstlichen Intelligenz. Die gibt es ja gerade im Bereich der Industrie schon lange, Stichwort: Pattern Recognition. Was erwartet uns hier die nächsten Jahre?*

Klaus Bikar: Intelligenz bedeutet zu verstehen, Maschinen jedoch können in der Tat nicht verstehen; sie speichern nur die Beziehung zwischen Input und Output. Mit neuen Funktionen, wie der Mustererkennung, können wir künstliche Intelligenz in Bereichen, wie der vorausschauenden Wartung, der Bedarfsprognose, der Gruppierung und der Kategorisierung, einsetzen.

Ulrich Parthier: *Eingangs sprachen wir über die Basisvoraussetzungen, die ERP-Software heute erfüllen sollte. Sie nennen 10 Gründe, warum sich ein näherer Blick auf ihre Lösung lohnen soll. Was kann caniasERP on top zu den Basisvoraussetzungen?*

Klaus Bikar:

1. Plattformunabhängig und Multiplattformfähig
2. Breiter Funktionsumfang
3. Zugriff auf Source-Code
4. (Individualisierbares) Standard-ERP
5. Offene Systemarchitektur
6. Software für den Mittelstand
7. Unterstützung von Open-Source Systemsoftware (Linux, Mysql)
8. Vollständige Integration und hohe Transparenz
9. Mehrmandanten-, Mehrsprachen- und Webfähigkeit
10. Integrierte, objektorientierte Entwicklungsumgebung TROIA

FOR THE FUTURE

> DAS ERP-SYSTEM SOLL EINE PLATTFORM BIETEN, DIE NEBEN DEN AKTUELLEN AUCH DIE ZUKÜNFTIGEN ANFORDERUNGEN ERFÜLLEN KANN.
>
> Klaus Bikar, Geschäftsführer, IAS GmbH | www.caniaserp.de

? **Ulrich Parthier:** *In der letzten Trovarit ERP-Studie „ERP in der Praxis" hat ihr System teilgenommen. Wie sah die Bewertung der Jury aus?*

Klaus Bikar: Wir haben hervorragende Noten erreicht und uns damit einen Platz unter den ersten drei geholt. Die Peergroup bewerteten die Aspekte „Gesamtzufriedenheit Anbieter" und „Zufriedenheit mit dem System" jeweils mit der Note 1,7. So konnte sich unser caniasERP im direkten Vergleich mit anderen „Mittleren Installationen (25-99 User)" den zweiten Platz in der Kategorie „Zufriedenheit insgesamt" holen.

? **Ulrich Parthier:** *2018 ist ihr System von der Initiative Mittelstand mit dem Innovationspreis-IT ausgezeichnet worden. Welche Aspekte und Funktionalitäten stehen bei dem nächsten Release auf der Wunschliste der Anwender ganz oben und wann wird es released?*

Klaus Bikar: Wir haben in diesem Jahr die neue Version von caniasERP veröffentlicht. Strategische, aber dynamische Planung und Kontrolle sind wichtiger denn je geworden, deshalb haben wir unser Budgetierungsmodul umstrukturiert. Mit der neuen Version stellen wir einen fortgeschritteneren HTML-Client zur Verfügung. Canias IQ wurde mehr in das System integriert und enthält jetzt mehr Berichte. Canias IoT-Connector und -Gateway Produkte werden in Pilotprojekten eingesetzt. Unser neues Modul, Production Intelligence, wird helfen, die Produktionsdaten zu analysieren. Darüber hinaus ist unser eigener Datenbankserver IASDB einsatzbereit.

! **Ulrich Parthier:** *Herr Bikar, vielen Dank für das Gespräch!*

THANK YOU

DIGITAL FACTORY

EINE NEUE ÄRA FÜR HERSTELLER.

Eine Digital Factory erfordert oft ein ganz neues Regelwerk an Agilität, neuen Technologielösungen und funktionsübergreifenden Teams. Das Umsetzen jener Anforderungen hat bei Unternehmen - die bestrebt sind neue digitale Fähigkeiten schnell zu entwickeln und zu verbreiten - stets zum Erfolg geführt. Heraus kommen permanente Kostensenkung sowie Qualitätssteigerung, die durch das Vernetzen der Funktionsbereiche zustande gekommen sind. Dabei bleibt es jedoch nicht nur bei Verbesserungen der technischen Standards, sondern zusätzlich um methodisches Umdenken: Es werden bereits etablierte Prozesse neu überdacht.

Die industrielle Welt ist schon länger im digitalen Wandel. In erster Line auch durch den Einsatz von ERP-Lösungen (Enterprise Resource Planning), denn hiermit werden unter anderem kritische Planungen, Verwaltung von Lagerbeständen oder auch Logistikprozesse automatisiert beziehungsweise vereinfacht. Des Weiteren wird die Digital Factory mit so wenig Papier wie möglich organisiert. Denn die Daten werden mithilfe des ERPs automatisch zwischen Geräten und Systemen ausgetauscht.

Das Aufkommen komplexer intelligenter Sensoren, künstlicher Intelligenzen, großer Datenpools und Robotik, verbunden mit den gewaltigen Verbindungen der Cloud, läutet eine neue Ära für Hersteller ein, die von vollständig integrierten Fabriken geprägt ist, welche zeitnah Produkte an die individuellen Kundenbedürfnisse anpassen und auf wechselnden Anforderungen und Trends sofort reagieren können. Diese umfassende digitale Fabrik kann eine Beschleunigung für eine starke Wachstumsagenda sein, die Produktivitätssteigerungen, finanzielle und operative Leistung, Produktion und Marktanteil sowie verbesserte Kontrolle und Transparenz in der gesamten Lieferkette ermöglicht. Sie fördert zusätzlich die Reform der Sicherheit, der Umweltverträglichkeit und die Nutzung globaler Werke. Der Fortschritt in der Robotik und Digitalisierung sowie der Ausbau des Internets spielen dabei eine wichtige Rolle. Es ist klar, dass diese Entwicklungen dazu führen, dass etwa die Automatisierung der Fertigung immer kostengünstiger wird und weiter ausgeweitet werden kann.

Durch verschiedene neue Technologien ist eine durchgängige Digitalisierung zunehmend in Reichweite. Die Integration von Systemen (zum Beispiel ERP) sowie der Datenaustausch mit Endgeräten (Integration zwischen ERP und Maschinen) sind nun einfacher als zuvor und werden bereits in großem Umfang angewendet. Hierbei wissen viele noch nicht, welche Möglichkeiten sie durch eine Digital Factory erlangen können. Auch fehlt hierbei die Kenntnis, wie dies in die Tat umgesetzt werden kann. Anhand der Digital Factory finden Unternehmen heraus, welches Potenzial durch die datenbasierte Integration in ihren Wertschöpfungsprozessen entsteht. Es gilt meist auch strategische Ziele, die IT-Infrastruktur, die laufenden operativen Prozesse oder auch den Kenntnisstand der Angestellten in die Überlegungen miteinzubeziehen.

DAS AUFKOMMEN KOMPLEXER INTELLIGENTER SENSOREN, KÜNSTLICHER INTELLIGENZEN, GROSSER DATENPOOLS UND ROBOTIK, VERBUNDEN MIT DEN GEWALTIGEN VERBINDUNGEN DER CLOUD, LÄUTET EINE NEUE ÄRA FÜR HERSTELLER EIN, DIE VON VOLLSTÄNDIG INTEGRIERTEN FABRIKEN GEPRÄGT IST.

Nisanth Thangarajah, Junior Consultant, Industrial Applications Software GmbH | www.caniaserp.de

Welche Vorteile bringt die Digital Factory?

Ohne Zweifel hängt es zum einen stark von der Branche ab, in der ein Unternehmen tätig ist und zum anderen auch an der aktuellen Wettbewerbsposition. Durch verschiedene technologische Entwicklungen weltweit, wird der Wettbewerb immer größer und globaler. Das Unternehmen muss kostengünstig mit Qualität und auch zunehmend mehr nach Kundenspezifikation

beziehungsweise Kundenanforderungen herstellen und arbeiten. Als Unternehmen gilt es schnell zu reagieren, ansonsten kommen einem die Mitbewerber zuvor.

Auch ist es ein entscheidender Schritt neue Technologien anzuwenden, denn man kann den Kunden dadurch viele Vorzüge bieten:

- **Kürzere Lieferzeiten**
  Aufgrund der einfachen Verfügbarkeit von Unternehmensdaten für Mitarbeiter und Maschinen wird weniger Massenproduktion benötigt, denn Aufträge können schneller geplant und terminiert werden. Das Wechseln von Produktionslinien wird immer einfacher und effizienter, sodass die Einzelstückfertigung auch mehr in Reichweite kommt. So kann auf spezifische Kundenanforderungen schneller reagiert werden. Dies hat die Kürzung der Produktionszeiten zur Folge und damit kürzere Lieferzeiten und infolgedessen eine Umsatzsteigerung.

- **Erhöhte Lieferzuverlässigkeit**
  Wenn Bestandsdaten, Anforderungen oder auch Lieferdaten mit Systemen von Kunden und Lieferanten vernetzt sind, gibt es weniger Risiko, dass Produkte unter Lieferschwierigkeiten leiden. Außerdem führen kürzere Durchlaufzeiten für eine erhöhte Liefersicherheit.

- **Erhöhte Effizienz**
  Immer wieder kann es vorkommen, dass Mitarbeiter nach Informationen suchen, die im Büro oder sogar im ganzen Unternehmen verteilt sind. Durch die digitale Vernetzung ist dies innerhalb weniger Klicks im erheblichen Maße weniger zeitintensiv. So können auch viele Prozesse automatisiert werden, denn Daten müssen nur einmalig eingepflegt werden und das Eingeben der Daten in mehrere Systeme bleibt erspart. So kann effektiv Zeit eingespart werden.

- **Erhöhte Qualität**
  Wird die Digitalisierung im Unternehmen intensiver integriert so werden weniger Fehler gemacht. Denn Anleitungen und Anweisungen stehen sofort zur Verfügung, welche von einer zentralen Datenbank oder Server kommen, worauf jeder im Unternehmen bei Bedarf zugreifen kann. Auch ist das Unternehmen dadurch in der Lage die Qualität auf nachhaltige Weise zu verbessern, da die Messung und Prüfung der Standards immer einfacher wird.

- **Höhere Kundenzufriedenheit**
  Anhand der Digital Factory kann zunehmend auf die Wünsche der Kunden eingegangen und gefertigt werden. Zum Beispiel können Lieferzeiten genauer bestimmt werden. Auch könnte man hier den Kunden automatisch über den Liefertermin informieren, indem man das System mit dem des Kunden integriert. So kann er sich die benötigte Zusatzinformation auch selbst abrufen. Damit ist auch ein automatischer Austausch von Serien- oder Chargendaten, Qualitätsdaten und technischer Daten möglich.

- **Höhere Mitarbeiterzufriedenheit**
  Die heranwachsende Generation ist umgeben von den neuesten Technologien, welche in einer noch nie zuvor da gewesenen Geschwindigkeit entwickelt werden. Daher werden diese Technologien auch später für deren zukünftige Arbeit als Voraussetzung betrachtet. Dies bedeutet je älter die Technologie und das digitale Equipment im Unternehmen ist, desto unattraktiver ist das Unternehmen für zukünftige Mitarbeiter. Dabei muss auch beachtet werden, dass gut ausgebildete und auch zufriedene Mitarbeiter im Unternehmen den Unterschied ausmachen und einen beachtlichen Mehrwert darstellen.

» WER DIE HERAUSFORDERUNG ANNIMMT, SEIN/IHR UNTERNEHMEN ZU EINER DIGITAL FACTORY UMZUWANDELN, MUSS ZWANGSLÄUFIG UMDENKEN.

Christine Schuhmacher. www.caniaserp.de

Fazit

Wer die Herausforderung annimmt, sein/ihr Unternehmen zu einer Digital Factory umzuwandeln, muss zwangsläufig umdenken. Grundsätzlich geht es selbstverständlich immer noch um Gewinnmaximierung und Kostensenkung aber eben auch um das Wagnis etwas Neues zu implementieren – zum Beispiel um die Emanzipation von Insellösungen hin zur Etablierung durchgängiger Systeme. Wie eingangs bereits angekündigt, gilt es die bisherigen Regeln und Gewohnheiten zu brechen sowie Veränderungen zuzulassen. Der Grundstein zu einer Digital Factory heißt also mentale Beweglichkeit.

Nisanth Thangarajah, Christine Schuhmacher

WIE TRANSPARENZ ZU MEHR SICHERHEIT FÜHRT

IN MINUTEN REAGIEREN STATT MONATELANGER UNGEWISSHEIT.

Cybersecurity ist ein medial stark strapaziertes, in der täglichen Unternehmenswelt zunehmend kritisches Management-Thema der Digitalisierung. Unternehmen können sich nur dann auf ihr Kerngeschäft konzentrieren und Digitalisierungsprojekte umsetzen, wenn die Systeme stabil und vor allem hochsicher laufen. Mit steigendem Digitalisierungsgrad nimmt die Komplexität der IT zu und stellt die Security-Verantwortlichen vor wachsende Herausforderungen. Wie automatisierte Workflows und eine zentrale Cloud-Plattform für Transparenz sorgen und Schäden vorbeugen, wird im folgenden Beitrag erläutert.

Manuelle oder papierbehaftete Prozesse bergen Gefahren

In vielen Unternehmen verlässt sich das Security-Incident-Response-Team noch immer auf E-Mails und Excel-Tabellen. Jemand meldet eine potenzielle Gefahr beziehungsweise einen Sicherheitsvorfall oder das SIEM-System (Security Incident & Event-Management-System) sendet einen Alarm. Diese Informationen landen mit vielen hundert anderen Meldungen in einer Tabelle, auf deren Basis Security-Verantwortliche die einzelnen Fälle abzuarbeiten versuchen. Statusinformationen werden manuell erfasst und jedes Update birgt ein gewisses Fehlerrisiko. Außerdem können häufig nicht mehrere Mitarbeiter an der gleichen Tabelle arbeiten. Es fehlt an Transparenz, Effizienz und der Möglichkeit zur intelligenten Priorisierung der einzelnen Themen. Wo Sicherheitsexperten mehr damit beschäftigt sind, Listen zu pflegen als Incidents zu beheben, gibt es eindeutig Handlungsbedarf auf Management-Ebene.

Automatisierung schafft Sicherheit

Cloud-Plattformen wie beispielsweise ServiceNow bieten die Möglichkeit, Incidents revisionssicher festzuhalten, nachfolgende Workflow-Prozesse und Entscheidungselemente zu automatisieren und so den Bereich Security Operations (SecOps) ideal zu entlasten. Dabei dient die Lösung einerseits als zentrale Informationsbasis, auf der alle eingehenden und ausgehenden Details zusammenlaufen. Andererseits erzeugt sie jederzeitige Transparenz über den aktuellen Status eines jeden Incidents. Darüber hinaus schaffen automatisierte Prozesse fehlerfreie, schnelle und effiziente Abläufe, die das Eingreifen von Mitarbeitern nur noch in Sonderfällen erfordern. Sie bieten eine vollständige Sicht auf die Incidentbearbeitung. Auf die gängigsten Hinweismeldungen reagiert die Lösung automatisch, stößt entsprechende Workflows an und informiert die First-Line-of-Defense im Notfall sofort. Alarme jeder Art werden so innerhalb von Minuten bearbeitet und das Team kann sich auf die wirklich kritischen Fälle konzentrieren. Neben dieser Ressourcenpriorisierung gewinnt die Behandlung von Security Incidents damit massiv an Geschwindigkeit. So trianguliert ServiceNow einzelne Systemparameter zu Anomalien in der IT-Infrastruktur automatisch. Da potenzielle Angriffe vorklassifiziert werden, können Gegenmaßnahmen unmittelbar eingeleitet und Schäden verhindert werden.

> CLOUD-PLATTFORMEN BIETEN DIE MÖGLICHKEIT, INCIDENTS REVISIONSSICHER FESTZUHALTEN, NACHFOLGENDE WORKFLOW-PROZESSE ZU AUTOMATISIEREN UND SO DEN BEREICH SECURITY OPERATIONS (SECOPS) IDEAL ZU ENTLASTEN.
>
> Dr. Ulrich Müller, Sprecher der Geschäftsführung, operational services GmbH & Co. KG
> www.operational-services.de

Automatisierung ist obligatorisch

Eine Cloud-Plattform wie ServiceNow im Bereich Security Operations bringt vier wesentliche Vorteile mit sich: In erster Linie können die Sicherheitsverantwortlichen effizienter arbeiten, weil das System die Vorfälle nach Kritikalität priorisiert und sie dank automatischer Prozesse weniger manuelle Aufgaben erledigen müssen. Darüber hinaus gelingt eine bessere Vernetzung zwischen Security und IT, weil beide Verantwortungsbereiche mit der gleichen Plattform arbeiten und so effizienter kooperieren können. Unabdingbar sind die revisionssichere Dokumentation und das Nachhalten: „Wer hat was getan?". Zu guter Letzt schafft eine solche Lösung übergreifende Transparenz mittels visueller Dashboards, Trendinformationen und der Analyse von Performance-Daten. Mit dieser technologischen Basis können Unternehmen blitzschnell und wirkungsvoll auf Angriffe und Bedrohungen reagieren.

Darüber hinaus fordert die Meldepflicht des IT-Sicherheitsgesetzes für Unternehmen mit kritischer Infrastruktur (KRITIS) eine unverzügliche Meldung an das BSI bei Feststellung von Major Security Incidents. Das kann effektiv nur dann gelingen, wenn zum einen die gesetzlichen Warn- und Meldevorgaben integrale Bestanteile des operativen IT-Betriebs sind und zum anderen die für das BSI-Meldeformular relevanten Informationen systematisch und automatisiert übermittelt werden könnten. Sie sind Grundvoraussetzungen dafür, dass künftige IT-Störungen organisationsübergreifend verhindert und Auswirkungen von Sicherheitsbedrohungen minimiert werden.

Dr. Ulrich Müller

VORTEILE EINER CLOUD-PLATTFORM:

1. Effizienteres Arbeiten der Mitarbeiter durch Priorisierung der Vorfälle nach Kritikalität
2. Bessere Vernetzung zwischen Security und IT durch Arbeit mit der gleichen Plattform
3. Revisionssichere Dokumentation
4. Übergreifende Transparenz mittels visueller Dashboards

GEBRAUCHTE SOFTWARE FÜR UNTERNEHMEN

WIEVIEL SICHERHEIT BRINGT DIE BLOCKCHAIN?

Die Blockchain ist zurzeit in aller Munde. Insbesondere im Zusammenhang mit dem Kauf gebrauchter Computerprogramme. Doch wieviel Wahrheit steckt tatsächlich hinter der verschlüsselten Dokumentationstechnologie? Software Reseller VENDOSOFT beleuchtet den Hype.

Seit 2012 der Handel mit gebrauchter Software durch Gerichtsurteile europaweit legal wurde, schwelt eine fortwährende Diskussion um mögliche Mehrfachverkäufe ein und derselben Softwarelizenz. Tatsächlich ist es praktisch möglich, dass ein Software-Händler 2.000 gebrauchte Lizenzen einkauft und dokumentiert, jedoch deutlich mehr Nutzungsrechte weiterverkauft. Dies wäre eine Straftat, die für den Endkunden nicht zwangsläufig zu erkennen ist. Im Zeitalter von Bitcoin und Krypto Trading wird deshalb die Forderung laut, die Blockchain auf den Gebrauchtsoftware-Markt zu übertragen. Es geht die These um, sie könne den Handel mit Lizenzen aus zweiter Hand sicherer, transparenter und durchgängig nachvollziehbar machen.

Als Anbieter von gebrauchten Microsoft- und Adobe-Lizenzen hat sich auch die VENDOSOFT GmbH intensiv mit der neuen Technologie auseinandergesetzt.

„Wir haben uns dem Thema Blockchain geöffnet und unsere bisherigen Prozesse auf den Prüfstand gestellt", sagt Geschäftsführer Björn Orth. Schließlich will der Reseller seinen Kunden höchste Sicherheit beim Kauf gebrauchter Lizenzen bieten. Das hat man bisher dadurch erwirkt, dass sämtliche Ankäufe durch einen Wirtschaftsprüfer verifiziert wurden. Dieser bestätigt den Kunden die Rechtmäßigkeit der Lieferkette sowie die vollständige Rechteübertragung.

> WIR HABEN UNS DEM THEMA BLOCKCHAIN GEÖFFNET UND UNSERE BISHERIGEN PROZESSE AUF DEN PRÜFSTAND GESTELLT.
>
> Björn Orth, Geschäftsführer Vendosoft GmbH | www.vendosoft.de

Lässt sich das Blockchain-Verfahren auf gebrauchte Software übertragen?

Ist das noch zeitgemäß oder ist die Blockchain tatsächlich das neue Mittel der Wahl, fragte sich das Management der VENDOSOFT GmbH. Die Erkenntnis fällt anders aus, als es die Berichterstattungen in der aktuellen Medienlandschaft vermuten lassen. Dort scheinen sich vornehmlich Gebrauchtsoftware-Händler zu Wort zu melden, die die Dokumentation via Blockchain als werbewirksame Maßnahme für sich entdeckt haben. Kritische Beiträge finden sich kaum.

So ist zu lesen, dass sich mit Hilfe des Kryptoverfahrens automatisiert und eindeutig nachvollziehen ließe, ob es sich bei Lizenzen aus zweiter Hand um Kauflizenzen handelt und ob diese – wie vorgeschrieben – einmalig oder nicht doch von mehreren Nutzern parallel verwendet würden.

Einige Gebrauchtsoftwarehändler werben damit, ihren Kunden ein auf Blockchain basierendes Online-Portal zur Verfügung zu stellen. Eine unabhängige Zertifizierungsstelle prüft demnach die Konformität der gehandelten Lizenzen und bescheinigt diese dem Kunden innerhalb eines sogenannten Smart Contracts. Die Ausgabe der darin enthaltenen Lizenzen werde mithilfe der Blockchain eindeutig identifiziert.

MEHR ZUM THEMA
BLOCKCHAIN

im Gebrauchtsoftware-Handel unter:
www.vendosoft.de/blockchain

Nonsense in - Nonsense out
So oder ähnlich läuft es bei allen Anbietern, die die neue Technologie eingeführt haben.

Eine unabhängige Zertifizierungsstelle prüft die Konformität der gehandelten Lizenzen und bescheinigt diese dem Kunden?

Spätestens hier muss sich der aufmerksame Leser fragen, wer diese Zertifizierungsstelle denn wohl sei. Die Webseiten der Blockchain-propagierenden Händler geben Aufschluss. Dort bescheinigt zum Beispiel ein von der IHK Köln bestellter und vereidigter Sachverständiger: Ein seriöser Gebrauchtsoftwarehändler kann (...) die Rolle einer LOB-Bescheinigungsstelle ausfüllen.

Für Björn Orth steht damit fest: Jeder Händler definiert selbst, was in die Blockchain seiner gebrauchten Lizenzen geschrieben wird. „Nonsense in – Nonsense out, könnte man es auch nennen", sagt er amüsiert. Keine unabhängige Kontrolle, keine Transparenz, keine zusätzliche Transaktionssicherheit. „Nur schöne Marketingworte, um eine Sicherheit zu suggerieren, die die Blockchain beim Thema Gebrauchtsoftware derzeit so nicht leistet."

Was ist sicher beim Kauf gebrauchter Lizenzen?
Für das Bestehen eines Herstelleraudits – und darum geht es Unternehmen beim Kauf gebrauchter Computerprogramme – ist der Nachweis zu erbringen, dass die Übertragung der Nutzungsrechte rechtskräftig vollzogen wurde und die Software nicht mehrfach im Einsatz ist. Dies zu dokumentieren, ist tatsächlich Aufgabe unabhängiger Zertifizierungsstellen. Für die VENDOSOFT GmbH wird dies weiterhin ein Wirtschaftsprüfer vornehmen. „Damit agieren wir im Sinne von Microsoft", erklärt Björn Orth seine Entscheidung. Denn die Audits des Software-Herstellers werden von eben dieser Instanz durchgeführt: von Wirtschaftsprüfern. Sie bestätigen Microsoft die lückenlose Dokumentation und rechtmäßige Übertragung der Lizenzen vom Vorbesitzer auf den Händler und weiter auf den neuen Lizenzinhaber. Ein Wirtschaftsprüfer prüft also die Angaben eines anderen Wirtschaftsprüfers. Wem wird er mehr glauben? Seiner eigenen Zunft – oder einer Blockchain, deren Input keine lückenlose Historie darstellt, sondern die vom jeweiligen Software-Händler selbst definierten Informationen?

NETOPS MEETS DEVOPS

STAND DER DINGE BEI DER NETZWERKAUTOMATISIERUNG.

400 IT-DevOps- und NetOps-Experten standen für eine Studie von F5 Rede und Antwort auf Fragen nach dem aktuellen Stand der Dinge bei der Netzwerkautomatisierung. Welche Best Practices können NetOps von DevOps adaptieren, um eine agilere, geschäftlich orientierte Wertschöpfung für die Netzwerke von morgen zu erzielen?

Die Ergebnisse der Studie zeigen Möglichkeiten, wie NetOps-Teams von den Best Practices der DevOps-Teams lernen, sich in kontinuierliche Bereitstellungs-Toolchains integrieren und von modernen Open-Source-Automatisierungstechnologien profitieren können. Das Netzwerkteam muss genauso agil und flexibel sein wie das Anwendungsteam und über die nötigen Voraussetzungen verfügen, um die Netzwerkagilität zu fördern. In dem Bericht sind die wertvollen Erkenntnisse aus der Studie zusammengefasst.

Das Whitepaper umfasst 17 Seiten
und steht kostenlos zum Download bereit.
www.it-daily.net/download

KÜNSTLICHE

AUF DEM BODEN DER TATSACHEN DIE SAAT AUSBRINGEN.

Kontrolle, Überwachung, Datensammeln, Neuronale Netze, GPUs, Parallelisierung und Speed, Speed, Speed. Hundertfach werden diese Begriffe in diesen Tagen gelesen und gehört. Der KI-Trend ist allgegenwärtig und wird von Herstellern und Lösungsanbietern marketingseitig positioniert. Das Wachstum ist groß, der Markt noch größer und alles scheint möglich. Doch welchen Nutzen kann man schon jetzt mit angemessenem Aufwand generieren? Mit unseren Kunden haben wir drei Themenbereiche als gute Startpunkte für KI-Initiativen identifiziert, die jeweils gut und schnell einen monetarisierbaren Nutzen stiften.

ChatBots

Wenn man sich die unterschiedlichen Ansätze von ChatBots anschaut, erkennt man schnell, dass diese nicht identisch sind. Es gibt zum einen Lösungen, die regelbasiert den Versuch unternehmen, Menschen zu ersetzen. Doch diese stoßen bei kleinsten Abweichungen vom geplanten Dialogfluss an Grenzen. Zum anderen gibt es kognitive Dialogsysteme, die situativ unter Anwendung von Hintergrundinformationen eine kreative und situative Dialogführung zulassen. Technologisch klassifiziert man regelbasierte Kommunikation im Unterschied zu einem echten KI-basierten Dialogfluss. Ebenso kann die Gruppe von Dienstleistern beziehungsweise Experten unterschieden werden, die für die Einführung von ChatBots benötigt werden. Sind auf der einen Seite klassische IT- und App-Entwickler zu sehen, werden auf der anderen Seite Experten für die Dialogführung (NLP Engineers) und Machine Learning zum Einsatz kommen.

Dass diese Beispiele Auswirkungen auf die Kosten einer Einführung haben, versteht sich von selbst. Damit ergeben sich gleichzeitig weitere Dimensionen der Klassifikation von ChatBot-Lösungen. Alle diese Aspekte zusammen erlauben eine Einordnung in das CENIT-Reifegradmodell, womit die Erwartungshaltung an das Vorhaben klarer wird.

Bewegte Bilder als Schlüssel der Digitalkommunikation

- Personalisiertes, interaktives Video als Vorstufe von KI-basierten Avataren:

Videos, die nur für einen Menschen und nur ein einziges Mal erstellt werden, – und hierbei die Interaktion mit den Anwendern ermöglichen –, sind die innovativste Ansprache im Bereich der Digitalkommunikation. Wenn sie hierbei die Interaktion mit den Anwendern ermöglichen. Bei dieser Art von Videos navigiert jeder Betrachter in seinem eigenen Video. Es findet ein Rollenwechsel statt – man wechselt quasi von einer passiven, konsumierenden Rolle in eine aktive, steuernde Rolle, was zu einer massiven Verlängerung der Beobachtungsdauer führt. Es können verschiedene Informationsobjekte dynamisch personalisiert werden (etwa Bild, Text, Audio, Dokumente, Video-Szenen). Die Personalisierung erfolgt durch die Verwendung von Daten aus internen oder externen Datenquellen in Echtzeit. Erst zum Zeitpunkt des Öffnens des Videos werden diese Daten angezeigt und sind somit immer aktuell – die Datenqualität ist hoch, die Ansprache zielgerichtet.

Dieses Vorgehen erfordert kein separates Rendering, was eine Verwaltung erzeugter statischer Videos überflüssig macht und damit eine kostengünstige Skalierungsmöglichkeit für den Einsatz bei klassischen Marketing- oder Vertriebs-Kampagnen darstellt. In einem persönlichen, interaktiven Video bestimmt der Betrachter seinen eigenen Weg durch das Videoerlebnis und steuert die Informationsdarstellung entsprechend seiner eigenen Präferenzen, indem er oder sie individuelle Auswahlentscheidungen über den Verlauf in Echtzeit trifft. Wenn man diese Technologien weiterdenkt, landet man mittelfristig bei der Einsicht, dass Avatare und VR als zusätzliche Kommunikationskanäle in die 360-Grad-Kundenkommunikation Einzug halten und der KI-Ideen immer mehr Leben einhauchen werden. In einem realen Anwendungsfall wurde bei einem deutschen Versicherer das Herunterladen einer App zur Stärkung der Kundenbezie-

hung genutzt. Dieser Ansatz wurde mit dem Dialog-Award 2018 „Excellence with EIM" (Enterprise-Information-Management) gewürdigt. Der Aufwand und auch der Anteil echter Machine- Learning-Ansätze sind für diesen Anwendungsfall noch überschaubar. Aber vielleicht aus genau diesem Grund so gut zum Einstieg geeignet.

Vorhersagen für den Produktionsprozess

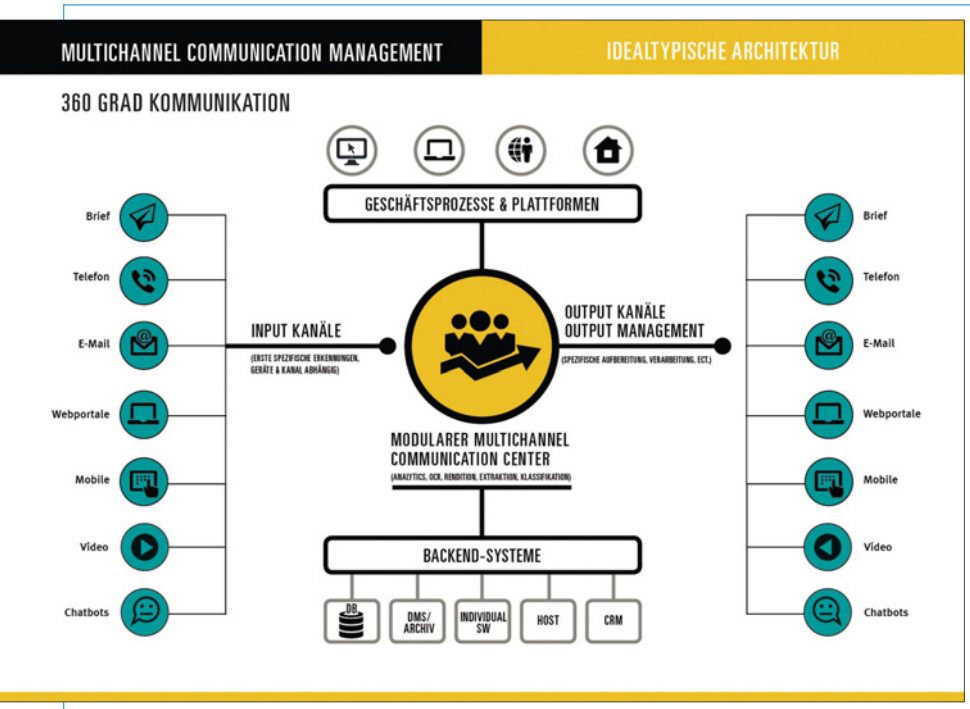
- Predictive Maintenance reduziert Ausfälle in der Produktion und erhöht die Produktqualität – bei gleichzeitiger Kostenoptimierung.

In den bestehenden Produktionsprozessen sind oftmals einzelne Prozessschritte bereits optimiert, mit Sensorik ergänzt, maximal automatisiert und ins Monitoring einbezogen worden. Das ist gut so. Was jedoch oftmals noch nicht vollzogen wurde, ist die Zusammenführung aller Einzelschritte im Prozess um darüber eine vollständige und ganzheitliche Sicht. Denn nur das böte die Chance für Planung und Prognose. Das ist die eigentliche Innovation des Predictive-Maintenance-Ansatzes der CENIT. Gemeinsam mit dem Kunden wird die Strategie zu einer Predictive-Maintenance-Vision definiert und ein Vorgehensmodell einschließlich. Maßnahmenplan und Kostenabschätzung für die Folgeschritte erarbeitet. Dies betrifft jeden Einzelschritt mit einer technischen Komponente, die an die bestehenden Software-Produkte des Unternehmens angepasst werden kann, um zusätzliche Investitionskosten gering zu halten. Für die Bewertung des Nutzens werden die Teilkomponenten in kleine beherrschbare Schritte zerlegt und in einer Art Mini-POC unter Nutzung der Predictive KI-Methoden einer Software analysiert. Hierbei stellt CENIT neben der Statistik- und Analyse-Expertise, die Ingenieur-Erfahrung aus einem ihrer Hauptmärkte bereit und bietet damit Know-how auf Augenhöhe mit den Produktionsexperten des jeweiligen Werks. Gemeinsam werden in diesen Mini-Forschungsprojekten Ansätze zur Optimierung, Korrelationen von Teilschritten und Zusammenhänge zwischen Sensoren identifiziert. Denn diese konnten über die herkömmlichen Leitstände und andere IT-Systeme nicht wahrgenommen werden.

Jede Erkenntnis hat Auswirkungen auf die Priorisierung der Vorgehensweise für den Startpunkt auf dem Weg zur verwirklichten Vision: einer sich selbst steuernden Produktion.

Es stellt sich zurecht die Frage, ob mit diesem explorativen Vorgehen monetärer Nutzen gestiftet werden kann? Ein klares Ja an dieser Stelle. Einer unserer Kunden hat durch Predictive Maintenance nicht nur seine Wartung planbarer gemacht, sondern auch seinen Ausschussanteil im Produktionsprozess deutlich reduzieren können.

INTELLIGENZ



© CENIT AG, Stuttgart

360-Grad-Kundenkommunikation.

> JEDE ERKENNTNIS HAT AUSWIRKUNGEN AUF DIE PRIORISIERUNG DER VORGEHENSWEISE FÜR DEN STARTPUNKT AUF DEM WEG ZUR VERWIRKLICHTEN VISION: EINER SICH SELBST STEUERNDEN PRODUKTION.
>
> André Vogt, Director EIM, CENIT AG
> www.cenit.com

Fazit

Zusammenfassend lässt sich also sagen: Immer, wenn das autonome Fahren noch zu komplex ist, die Mustererkennung in der Diagnostik zu groß und die Sorge vor Überwachungsszenarien einsetzt, sollen diese drei Beispiele daran erinnern, dass kleine, lösbare Ansätze einen wirtschaftlichen Einstieg in KI ebnen. Begriffsklärungen und Reifegradmodelle sorgen zudem für Klarheit und Transparenz – und sichern das Vorhaben ab.

André Vogt

BUSINESS SERVICES ÜBERWACHEN

WARUM IST BUSINESS SERVICE MONITORING GESCHÄFTSKRITISCH?

Der Business-Impact der IT steigt ständig. Digitale Geschäftsmodelle und Unternehmensabläufe erlauben heute keine ungeplanten Downtimes mehr, wie sie jedoch immer wieder passieren. So hielt beispielsweise am 17. Mai 2018 ein landesweiter technischer Totalausfall die Sparda Bank in Atem. Kunden konnten über Stunden kein Geld an Automaten abheben, keine Kontoauszüge drucken und kein Online-Banking nutzen. Das Beispiel zeigt, dass geschäftskritische Services wie das Online-Banking aus einer Fülle zusammenwirkender technischer Komponenten bestehen, deren ebenso filigranes wie komplexes System zusammenbricht, wenn eine relevante Komponente ausfällt.

Dabei muss es nicht immer ein Ausfall sein – auch verzögerte Antwortzeiten würden – beispielsweise bei Amazon – zu signifikanten Umsatzeinbußen führen. Die nachhaltige und umfassende Überwachung von Business Services ist daher geschäftskritisch. Business Service Monitoring ist die hohe Kunst eines geschäftsfokussierten IT-Qualitäts- und -Risikomanagements. Die Realtime-Überwachung von IT-Services setzt einerseits einen hohen Reifegrad der IT-Organisation voraus, andererseits auch die technische 360-Grad-Übersicht, die zudem die Perspektive des End-Users berücksichtigt.

Wichtige Aspekte bei der Umsetzung

Aus der Perspektive der Fachabteilungen wird häufig argumentiert, dass ein übergeordnetes Monitoring nicht nötig sei und individuelle Überwachungssysteme ausreichten. In der Praxis führt die Konstellation parallel laufender Inselsysteme nicht nur zu signifikanten Mehr-Aufwänden für den redundanten Betrieb mehrerer Tools. Der im Ernstfall so wichtige systemübergreifende 360-Grad-Blick ist bei diesem „Silo-basierten" Überwachungsansatz nicht gegeben. Die Folgen können gravierend sein. Denn die Ursachenfindung gestaltet sich in der Regel schwierig und ist sehr zeitraubend. Die Störungsbehebung verzögert sich, da die einzelnen System-Administratoren zunächst ihre eigenen Ansichten überprüfen. Außerdem lässt sich der Schweregrad einer Störung und die Auswirkung auf die Kunden bzw. das Business – isoliert betrachtet – meist nicht richtig einschätzen. Auch mit Blick auf die Schatten-IT durch Cloud-Anwendungen muss die Diskussion zwischen IT und den Fachabteilungen geführt werden, um im positiven Fall zu dokumentierten, transparenten Verantwortlichkeiten und Schnittstellen zu kommen.

> BUSINESS SERVICE MONITORING IST DIE HOHE KUNST EINES GESCHÄFTSFOKUSSIERTEN IT-QUALITÄTS- UND -RISIKOMANAGEMENTS.
>
> Jens Harms, PreSales Consultant, LeuTek GmbH | www.leutek.com

In der Praxis stellt das Modellieren der Business Services anhand der vorhandenen Configuration Items eine große Herausforderung dar, denn das Wissen, wie ein Service im Detail funktioniert (prozessual, technisch, vertraglich) ist häufig auf viele Köpfe verteilt. Ohne CMDB ist Business Service Monitoring möglich, aber schwieriger. Vor allem die Aktualität leidet, da die CMDB über Change Prozesse beispielsweise einen neuen Server sofort und automatisch in die Überwachung integrieren kann.

Was eine ideale Lösung leisten sollte

Eine gute Lösung bietet die nötige 360-Grad-Informationstransparenz und liefert den Systemadministratoren und den

IT-Verantwortlichen in Echtzeit alle Daten, um physikalische und virtuelle Ressourcen sowie die Integration von Cloud-Applikationen und Cloud Services unterschiedlichster Anbieter in die eigene IT-Infrastruktur erfolgreich planen und steuern zu können.

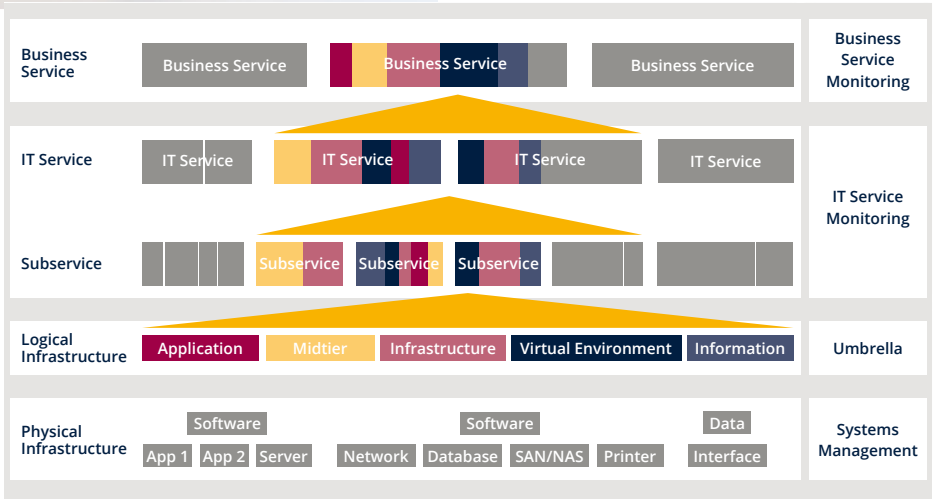
Voraussetzung dafür ist vor allem die Integrationsfähigkeit des Systems. Vielfältige Schnittstellen stellen den Sammelpunkt für unterschiedlichste Daten dar. Beispiele hierbei sind Zustandsinformationen aus der Server-Überwachung und vorgelagerter Management-Tools, die Überwachungsdaten von Großrechnern, Cloud Services, Docker Container oder die Informationen weiterer Fremdsysteme wie beispielsweise Gebäudeleittechnik, USV- und Klimatechnik, Brandmeldezentrale oder Sensoren. Die zu messenden Parameter sind vielfältig, zum Beispiel Temperatur, Lüfterdrehzahl, Speicherbelegung, Speicherverfügbarkeit. Ausgewertet wird das gesamte Spektrum

physikalischer, prozessualer und anwendungsbezogener Daten, die über mandantenfähige Dashboards aggregiert und zentral dargestellt werden können. Gleichzeitig ist es wichtig, bei Problemen über Drill-Down-Funktionalitäten leicht innerhalb der Service-Strukturen bis zu den Detail-Sichten auf Infrastruktur-Ebene zu navigieren.
Entscheidend in der Praxis sind zudem das Thema Automation und die Integration von ITIL-konformen IT Servicemanagement-Modulen. Mit einem zentralen Gesamtsystem ist die Basis dafür geschaffen. Besonders effizient im Sinne einer Automation ist das Zusammenspiel mit einer Configuration Management Database (CMDB), die die vielseitigen Abhängigkeiten zwischen IT-Assets und Services transparent macht. Für den raschen Start sind auch Out-of-the-Box-Best practices für die relevanten Cloud-Anbieter wichtig. Damit legt das System automatisch Objekte an und wählt die spezifischen Überwachungs-Metriken aus. Ein weiterer zentraler Aspekt ist die flexible Skalierbarkeit – gerade angesichts moderner dynamischer IT-Infrastrukturen mittels Cloud Computing. Ein entsprechendes System muss in der Lage sein, kurzfristig und automatisiert zum Beispiel 30 neue Webserver zu überwachen.

Whitepaper:
Dieser Artikel ist ein Auszug aus einem umfangreichen Fach-Whitepaper „Business Service Monitoring im Cloud-Zeitalter", das hier heruntergeladen werden kann:
https://bit.ly/2CGw0Uc

Ein ebenfalls erfolgskritischer Faktor ist ein integriertes, zentrales Alarm-Management, um im Ernstfall eine schnelle und zielgerichtete Problembehebung zu gewährleisten. Eskalationsmechanismen, das Bedienen unterschiedlichster Kommunikationskanäle, das Follow-the-Sun-Prinzip zur Optimierung der weltweiten Bereitschaftskosten oder einheitliche Handlungsanweisungen in einer intelligenten Lösungsdatenbank sind dabei wesentliche Funktionen.

Aufbau eines BusinessService



Die Wirtschaftlichkeit

Die Mehrwerte durch ein zentrales Business Service Monitoring liegen auf der Hand: Neben schwer quantifizierbaren Parametern wie die Zufriedenheit von Endkunden mit der Servicequalität und ein besseres Verständnis, wie das Funktionieren technischer Parameter die Business Prozesse beeinflusst, gibt es konkret messbare Kosteneffekte.
Es entstehen direkt und indirekte Kosten für:

- Personal, das die Informationen zusammenträgt und geeignet aufbereitet (wenn überhaupt möglich),
- System- beziehungsweise Service-Ausfälle (SLA/OLA) wegen fehlendem Überblick an zentraler Stelle,
- Zeitverzug bei der Problemlösung (Dauer des System-Ausfalls),
- den Verlust an Reputation (nicht messbare Kosten),
- Fehlende Transparenz intern und zum Kunden und
- Verzögerung im Time to Market der Services.

Auf den ersten Blick gibt es eine ganze Reihe von Open-Source-Monitoring-Lösungen, die eine Vielzahl von Features haben und unterschiedlichste Bereiche abdecken. Betrachtet man jedoch die Erfahrungen mit dem Handling und den Gesamt- und Folgekosten in komplexeren IT-Umgebungen, schwinden die Vorteile der zunächst vergleichsweise günstig erscheinenden Lösungen. In der Praxis liegt der Aufwand bei der händischen Implementierung und Pflege von Open Source-Lösungen oftmals beim Doppelten bis Dreifachen gegenüber professionellen Standard-Tools, die eine automatisierte Implementierung und einen automatisierten Betrieb erlauben. Integrations- und Mandantenfähigkeit, umfangreiche Eventkorrelation, Benutzer-Rollen-Konzepte und Revisionssicherheit sind weitere Aspekte, bei denen Open-Source-Tools an ihre Grenzen stoßen. Auch der After-Sales-Service ist eine wichtige Komponente – denn nach der Implementierung ist vor der Implementierung.

Jens Harms

PROZESSE SINNVOLL FIT MACHEN

PROJEKT- UND PROZESSMANAGEMENT BEI DER TRANSFORMATION VON PROZESSEN.

Die Gründe für eine Überprüfung, Optimierung oder auch Neugestaltung von Geschäftsprozessen sind vielfältig. Anforderungen und Chancen, die sich aus der Digitalisierung ergeben, kontinuierliche Verbesserungsmaßnahmen oder technische Einflüsse sind nur einige. Welche Bedeutung hat das Projektmanagement und wie kann man sich der Sache annehmen? Sind traditionelle Projektmanagementansätze veraltet? Ist Agilität die Lösung für alle Projekte? Sind alle Unternehmen bereit für ein agiles Vorgehen? Was ist mit den vielen Unternehmen, die nicht bereits über agile Strukturen und Kompetenz verfügen? Welche Methodik passt auf welches Projekt und welche Mitarbeiter? Dies sind Fragen, denen sich Unternehmen und Projektverantwortliche stellen müssen.

Status Quo

Dass Prozesse und deren Tools sich wegen der fortschreitenden Digitalisierung ändern müssen, dürfte außer Frage stehen. Dass sich bei der täglichen Arbeit oder im Regelkreislauf des Prozessmanagements Potenziale zur Verbesserung erkennen lassen ist ebenfalls sehr wahrscheinlich. Wie groß diese Veränderungen sind entscheiden Märkte und Marktteilnehmer individuell.

Die Welt der Prozesse dreht sich schneller. Damit rücken zwei Disziplinen in den Fokus. Zum einen das Prozessmanagement und die stetige Anpassung an neue Anforderungen. Gerade wenn man in diesem Bereich als Unternehmen eine führende Position einnehmen möchte ist erhöhtes Engagement notwendig. Zum anderen erzeugt die Veränderung und Implementierung der Prozesse Kompetenz- und Ressourcenbedarf im Projektmanagement.

In der Praxis erlebt man häufig, dass Personen als Projektmanager eingesetzt werden, die zwar eine Grundlage des Projektes, zum Beispiel ein Softwareprodukt oder ein Fachgebiet besonders gut kennen, nicht aber über eine ausreichend methodische und persönliche Projektmanagementgrundlage verfügen. Das heißt im Ergebnis, dass diese Person Potenzial in einem Gebiet reduziert, in dem eine große Expertise besteht und stattdessen Aufgaben übernimmt, die diese Person vielleicht nicht so gut beherrscht und vielleicht auch gar nicht tun möchte. Eigentlich ein schlechtes Geschäft. Für das jeweilige Fachgebiet der Person und für das Projektmanagement.

> EINE AUSBILDUNG ALS PROJEKTMANAGER, WIE ZUM BEISPIEL DAS PMI (PROJECT MANAGEMENT INSTITUTE) ODER DIE GPM (DEUTSCHE GESELLSCHAFT FÜR PROJEKTMANAGEMENT) SIE ANBIETEN IST NOCH KEINE SELBSTVERSTÄNDLICHKEIT.
>
> Martin Besemann,
> Berater und Projektmanager

Eine Ausbildung als Projektmanager, wie zum Beispiel das PMI (Project Management Institute) oder die GPM (Deutsche Gesellschaft für Projektmanagement) sie anbieten ist noch keine Selbstverständlichkeit. Mit Prince2 wird ein gewachsener Best Practise Ansatz geschult, hier geht es in der Hauptsache eher um den Projektablauf, als die notwendigen persönlichen Kompetenzen, Techniken und Wissensgebiete. Alle drei Varianten verfügen über agile/hybride Elemente und Zusatzausbildungen. Nicht alle Unternehmen und Abteilungen verfügen aber über diese entsprechend ausgebildeten Ressourcen.

Agile Ansätze

Das Thema Agilität im Projektmanagement wird immer präsenter. Scrum, Kanban und einige weitere agile Ansätze sind aus verschiedenen Strömungen in die Unternehmen eingezogen oder tun dies vermehrt. Diese Methoden bergen viel Potenzial. Schnellere Time to Market Zyklen, Reduktion von Risiken und eine hohe Kundenorientierung um nur eine Auswahl zu nennen. Für die erfolgreiche Anwendung reicht aber nicht eine kleine Schulung oder ein Buch. Es sind Veränderungsprozesse notwendig, um das Unternehmen und die Mitarbeiter bereit zu machen, für eine veränderte Denk- und Arbeitsweise. Mitarbeiter und auch Manager, die über viele Jahre anders gearbeitet haben, brauchen Zeit um den Wandel zu vollziehen. Nicht alle Unternehmen, vor allem nicht

alle Bereiche sind heute schon in der Lage erfolgreich agile Methoden zu nutzen. So wird der Begriff Agilität teilweise auch einfach dafür missbraucht, um den vermeintlichen Vorteil einer reduzierten Planung am Anfang zu nutzen. Bei dem Einkauf von Leistungen wird allerdings eher weniger gerne akzeptiert, dass der Festpreis nicht mehr so einfach zu erzielen ist, weil der Aufwand variabel ist oder eine eingeschränkte Möglichkeit zum Lösungsumfang akzeptiert werden muss, weil der akzeptierte Aufwand fixiert ist.

10 EINFACHE FRAGEN FÜR EINE ERSTE PROJEKTBEURTEILUNG:

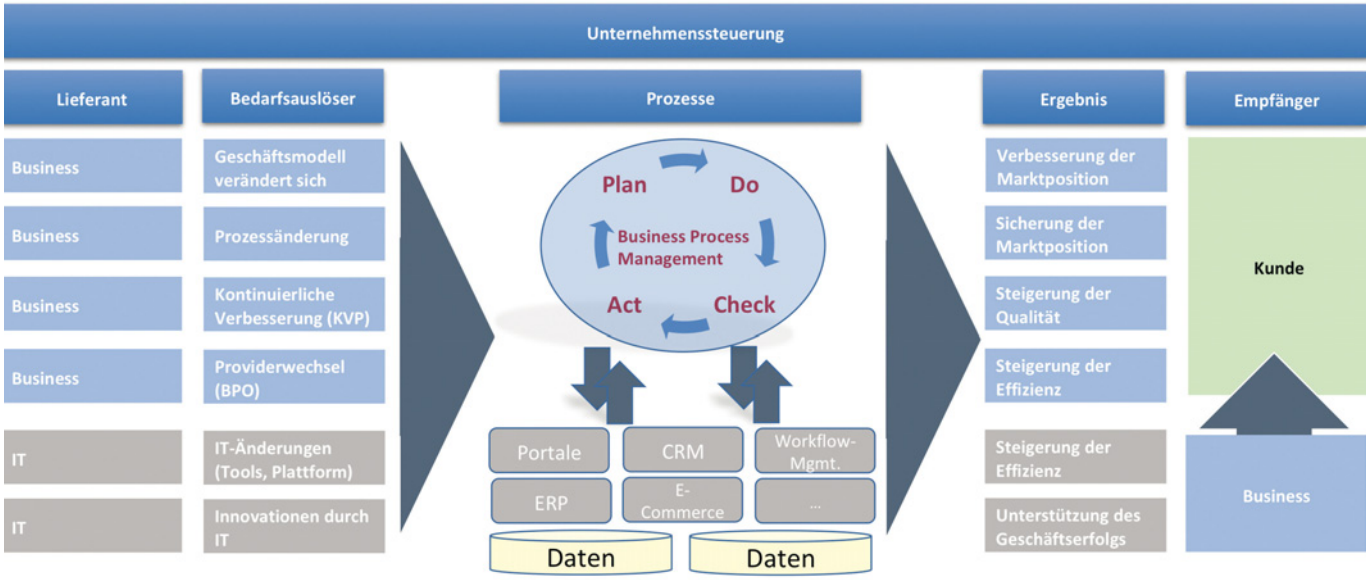
1. Ist ein ausgebildeter Projektmanager eingesetzt worden?
2. Ist der Projektmanager mit der notwendigen Zeit und Kompetenz ausgestattet?
3. Ist ein Lenkungsausschuss dicht genug am Projekt?
4. Verfügt die Projektsicherung real über PM Kompetenz und ist nicht nur wegen ihrer Person/ Position eingesetzt?
5. Gibt es ein ausreichendes Budget auf Basis einer professionellen Aufwandsschätzung?
6. Passt das Unternehmensumfeld zur Projektmethode?
7. Erfolgt die Auswahl der Tools nach dem tatsächlichen Anforderungsprofil?
8. Verfügt das Unternehmen über ein aktives Prozessmanagement?
9. Werden die Geschäftsprozesse bei Transition- und Transformationsprojekten ausreichend beachtet?
10. Gab es bei den letzten Projekten im Bereich Prozesse nachhaltige Erfolge?

Projektvorgehen

Die Frage nach dem besten Vorgehen beantwortet sich individuell nach dem jeweiligen Projektumfeld. Da sind zum Beispiel der Projektgegenstand, die beteiligten Unternehmen und die verfügbaren Ressourcen zu betrachten. Außerdem ist auch das Kostenrisiko zu beachten. Bei dem Einkauf einer Leistung/Lösung möchte der eine nicht zu viel bezahlen und der andere nicht zu viel leisten. Eine oder mehrere Seiten können zum Verlierer werden. Gerade bei großen Projektvorhaben und dem Einkauf von Leistungen und Lösungen kann eine reduzierte Planung am Anfang zu Fehlentscheidungen führen. Zum Beispiel im Outsourcing oder bei der Einführung von IT-Lösungen. Bekannte Projekte, wie die Elbphilharmonie verdeutlichen die Risiken in anschaulicher Form. In Projekten wo tatsächlich ein Gebiet vorliegt, in denen

> „...KLAR IST: WAS WIR BEIM BAU DER ELBPHILHARMONIE ERLEBEN, HÄTTE VERMIEDEN WERDEN KÖNNEN. WENN MAN AM ANFANG DEN MUT UND DIE BEREITSCHAFT GEHABT HÄTTE, DAS GEBÄUDE FERTIG ZU PLANEN UND ERST DANN DIE AUFTRÄGE ZU ERTEILEN, WÄRE MÖGLICHERWEISE VON BEGINN AN KLAR GEWESEN, DASS MAN DIESES ANSPRUCHSVOLLE KONZERTHAUS NICHT FÜR DIE DAMALS VERMITTELTEN SUMMEN ERRICHTEN KANN."
>
> Olaf Scholz

Die Unternehmensgrundlage (Umsatz) wird im Business erzielt.



Ziele sollten mehrdimensional betrachtet werden. Wenn eine Änderung in der IT notwendig ist, darf man auch die Chancen für das Business nicht verstreichen lassen und umgekehrt. Final geht es um kundenorientierte und im Markt erfolgreiche Prozesse und nicht das Werkzeug.

das genaue Ergebnis noch nicht bekannt ist, macht ein agiles Vorgehen Sinn. Man sollte aber beachten, dass das generelle Unternehmensumfeld dies zulassen muss, die Menschen eine besondere Rolle spielen und dieses Vorgehen nicht nur selber wollen, sondern auch über ein agiles Mindset verfügen. Wenn die Grundlagen erfüllt sind, eröffnet Agilität hohe Potenziale. Vielleicht ist die beste Projektvorgehensweise gar nicht schwarz oder weiß, sondern hybrid. Eine entsprechende Mischung, auch innerhalb eines Projektes, kann auch eine rationale und erfolgreiche Grundlage darstellen. Vor allem wenn unterschiedliche persönliche Kompetenzen in einem Gesamtprojekt vereinigt werden. Es besteht in den traditionellen Vorgehensweisen beschriebenen Methoden auch nur eine bedingte Konkurrenz zu agilen Modellen. Der Vergleich ist nicht Agil vs. PMI, IPMA oder Prince2, sondern Agil vs. Wasserfall.

Bedarf

Der Bedarf zu Veränderungen kann sehr unterschiedliche Dimensionen haben. Die Auslösung eines Projektes, in Form der Definition einer Anforderung kann mit klassischen, hybriden und agilen Methoden angereichert werden. Wenn es zu der Auswahl neuer Partner, der Anschaffung von neuen Prozesstools oder auch nur zu einer Prüfung der bestehenden kommt, um eine Entscheidung zu treffen, ob die jeweiligen Werkzeuge geeignet sind, muss der Bedarf genau genug bekannt sein, um eine Fehlinvestition zu vermeiden. Das gilt bei großen Investitionen und zeitlich kritischen Projekten entsprechend mehr. Die Ziele der Veränderung sind wichtig und sollten klar sein, um Prozesse entsprechend auszurichten.

BPM: Status und Vollständigkeit der Prozesse ermitteln

Im professionellen Prozessmanagement gibt es verschiedene Varianten, wie den Deming Cycle um Prozesse stetig zu beobachten und iterativ weiterzuentwickeln. Sollte ein solches Prozessmanagement nicht im Einsatz sein, wird eine Statusaufnahme umso wichtiger. Bevor Prozesse neu implementiert werden, muss klar sein, welche Qualität sie haben. Für die optionale Auswahl von Lösungen und Partnern sind sie eine Grundlage. Eine unbemerkte Implementation von nicht den aktuellen Strategien entsprechenden Prozessen kann zu einem Schildbürgerstreich werden.

BPM: Prozesse optimieren

Die Prozesse bestimmen entscheidend mit bei dem Erfolg von Unternehmen. Effizienz, Kundenorientierung, Prozesskosten und Zufriedenheit der Stakeholder wirken auf den Geschäftserfolg. Wer möchte lange Durchlaufzeiten, veraltete oder ineffiziente Prozesse nutzen? Die Digitalisierung bietet Möglichkeiten, aber sie setzt auch Herausforderungen. Sowohl im Wettbewerb, als auch in den Kosten kann die Prozessqualität einen entscheidenden Einfluss auf den gesamten Unternehmenserfolg nehmen.

Lösung oder Provider bestimmen

Teilweise stehen die Lösungen und Partner mit denen gearbeitet wird im Voraus fest. Teilweise müssen diese noch ergänzend oder komplett gesucht werden und es kann auch bei gesetzten Lösungen Sinn machen, eine Validierung mit den aktuellen Prozessen vorzunehmen. Bei einer vorherigen Prüfung muss etwas zum Prüfen vorhanden sein, denn PoC steht für Proof of Concept und nicht Proof ohne Concept. Die Evaluierung ist eine Entscheidungsgrundlage und kostet je nach Projekt teilweise beachtliche Ressourcen.

Prozesse implementieren

Die Phase der Implementierung kann klassisch, agil und gemischt verlaufen. Das

liegt im Sinne der Projektstrategie. Man kann aber keine Menschen in ein Korsett zwingen was nicht passt. Wenn keine Kollegen mit einem agilen Mindset vorhanden sind gilt das wie umgekehrt.

Projektorganisation

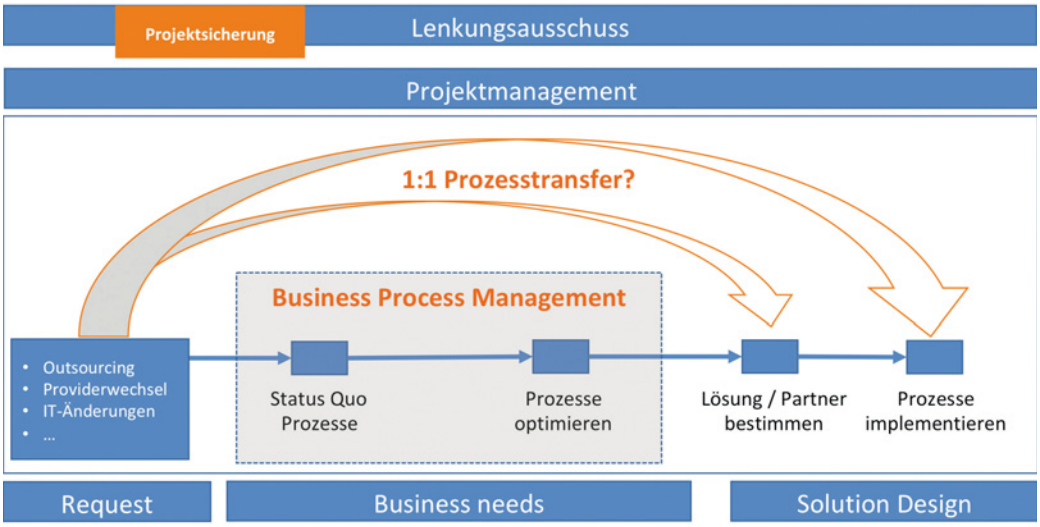
Die Organisation des Projektes kann schon eine richtungsweisende Entscheidung für den Projekterfolg sein. Die führende Position für Prozesstransformationsprojekte wird teilweise vom Business, weil es den Bedarf hat und teilweise von der IT, weil es die Tools hat und stark in die Umsetzung eingebunden ist, eingefordert. Um was geht es bei der Transformation? Doch eigentlich um den geschäftlichen Erfolg des Unternehmens und nicht um eine Fokussierung auf Tools. Damit rückt das Business auch in den Fokus. Die Rolle der IT wird durch sich schnell entwickelnde Trends und Möglichkeiten zu einem wichtigen Berater und Innovationsgeber. Erst Tools auszuwählen und dann zu ergründen welche Prozesse man wie damit abbilden kann, könnte aber der risikoreichere Ansatz sein. Im Ergebnis ist ein Prozessmanagementprojekt mehr ein Organisationsprojekt, als ein IT- Projekt, denn Prozessveränderungen sind weit mehr als die reine IT Umsetzung. In einem Steuerungsgremium, wie dem Lenkungsausschuss, bieten sich beide Seiten, das Business und die Technik, an. Je höher die Managementebene ist, desto weiter wird die Distanz zur operativen Durchführung. Wie beispielsweise in Prince2 beschrieben, kann eine Projektsicherung das Management bei der Qualitätssicherung des Projektes entscheidend unterstützen. Hierfür kann eine interne oder externe Beratungsfunktion eingebunden werden, um das Management zu entlasten und zu beraten. Die Projektberatung des Managements im Steuerungsgremium sollte durch von Stakeholdern und Projektergebnis unabhängigen Experten, die über Fachwissen auch unterhalb der Überschriftenebene verfügen, erfolgen. In der Beurteilung des Projektes ist dies ausgeprägte Praxiserfahrung und Methodenkompetenz statt Buzzword-Bingo. Weiterhin können je nach Projektsituation interne oder externe Kunden als Benutzervertreter und Lieferanten eine Hilfe im Steuerungsgremium darstellen.

Fazit

Es geht nicht um „das schönste Tool, sondern um den geschäftlichen Erfolg", daher sollte dies auch in der Projektvorgehensweise ersichtlich sein. Eine Implementierung von Prozessen ohne Validierung der Qualität kann zu deutlich erhöhten Aufwänden bis zu einer Fehlinvestition führen. Gerade die fortschreitende Digitalisierung verdeutlicht dies. Wenn der Wettbewerb die kundenorientierteren Prozesse hat kann dies zu einem entscheidenden Wettbewerbsnachteil führen. Der Einsatz eines Projektportfoliomanagements hilft die richtigen Prozessprojekte zu erkennen und zu priorisieren. Projektmanagement hilft beim Unternehmenserfolg, daher ist eine Berücksichtigung als Teil der strategischen Unternehmensausrichtung sinnvoll. Projektmanagement ist keine Arbeit für nebenbei. Dazu sind ausreichend und entsprechend qualifizierte Ressourcen notwendig. Professionelles Projektmanagement agil oder klassisch kann einen entscheidenden Mehrwert für ein Projekt darstellen. Auch Mischformen wie hybrides Projektmanagement können Projekte zum Erfolg führen. Man muss mit den Fähigkeiten des Teams arbeiten und nicht das Team in ein System zwängen, wenn es dazu noch nicht oder nicht mehr bereit ist. Die Veränderung ist nicht von heute auf morgen möglich, sondern braucht Zeit, den Willen und das Umfeld dazu. Große und wichtige Projekte sind kein „Jugend forscht" Umfeld. Die Rolle der Projektsicherung kann entscheidend den Projekterfolg beeinflussen. Wenn es zu Defiziten in der Qualität des Projektmanagements, einem falschen Projektvorgehensmodell, einer falschen Projektorganisationsform oder einer Gefährdung der Projektziele kommt muss der Auditor dem Management dies vor der Freigabe einer Projektphase mitteilen.

Martin Besemann

Transition/Transformation von Prozessen in eine andere Umgebung



Bei einer Überführung von Prozessen zu einem anderen Provider oder in eine andere IT Umgebung, kann die vermeintliche Abkürzung und der Verzicht auf die Prozessanalyse- und Optimierungsphase zu einer deutlichen Verlängerung der Gesamtinitiative, unerwarteten Kosten, bis zum Verfehlen der Projektziele führen.

Als Betreiber kritischer Infrastrukturen (Kritis) sind die Berliner Wasserbetriebe gleichzeitig von den Vorgaben des IT-Sicherheitsgesetzes (IT-SiG) betroffen und müssen Informationssicherheitsmanagementsysteme (ISMS) einrichten. Das neue Hochgeschwindigkeitsrechenzentrum musste daher hohen Sicherheitsanforderungen gerecht werden. Weitere klar definierte Ziele waren Umweltfreundlichkeit, Verfügbarkeit und Energieeffizienz, die ebenfalls hohe Priorität haben.

> UNS WAR EIN PARTNER SEHR WICHTIG, DER PLANUNG, BAU UND BETRIEB AUS EINER HAND LIEFERT. WESENTLICHER WEITERER FAKTOR WAR DER KURZE BAUZYKLUS, DER FÜR DIESES PROJEKT AUCH ENTSCHEIDEND WAR.
>
> Gerd Klinke,
> Leiter Informationstechnologie, BWB

Das ehemalige Rechenzentrum der BWB war, bedingt durch die früher voluminöse Technik, ohnehin überdimensioniert und nicht energetisch. Daher entschlossen sich die IT-Verantwortlichen zum Bau eines neuen Hochgeschwindigkeits-RZ auf der „grünen" Wiese. Per Ausschreibung suchte das Unternehmen nach einem Partner mit sowohl zukunftsfähigen als auch gesetzeskonformen Lösungen. Diese konnte die Data Center Group für sich entscheiden. Das Team um Gerd Klinke, IT-Chef der BWB und bereits seit 14 Jahren im Unternehmen tätig, hatte sich im Vorfeld bereits realisierte Projekte des Unternehmens angesehen.

„Wir kannten das Unternehmen auch aus vorheriger Zusammenarbeit. Überzeugt hat allerdings, dass die Lösung Flexibilität, Sicherheit, Energieeffizienz und Nachhaltigkeit vereint. Besonders die Modulbauweise der Sicherheitsprodukte des Tochterunternehmens RZproducts. Schließlich wurden mit den Experten des Generalunternehmers individuelle Optionen besprochen. Uns war ein Partner sehr wichtig, der Planung, Bau und Betrieb aus einer Hand liefert. Wesentlicher weiterer Faktor war der kurze Bauzyklus, der für dieses Projekt auch entscheidend war", sagt Klinke.

DC-ITRoom QuarzITe

Planungsprozess und Projektablauf sind dann zügig verlaufen. Das neue Rechenzentrum besteht aus einer Raum-in-Raum-Lösung, basierend auf dem DC-ITRoom QuarzITe. Sie ist so konzipiert, dass sie in einem bestehenden Gebäude eingepasst und modular zu jeder Größe erweitert werden kann. Die feuer- und temperaturfeste Bauweise aus robusten Materialien, Dichtungen sowie Isolierplatten hält dabei einer intensiven Beflammung stand, ohne technische Schäden am Objekt zu hinterlassen.

Technikräume und eine energieeffiziente Klimalösung sind Teil der Lösung. Im Falle eines Stromnetzausfalls übernimmt die Netzersatzanlage (NEA) die Versorgung von sicherheitsrelevanten Verbrauchern mit elektrischer Energie. Bezüglich des Monitorings sorgt der DCM Agent für Transparenz bei den Kennzahlen der IT-Infrastrukturen, klare Prozesse und definierte Alarmierungsabläufe bei Störungen. Damit ist der geforderten Redundanz und Ausfallsicherheit Sorge getragen.

QuarzITe ist allgemein EI 90 systemgeprüft und zertifiziert nach EN 13501-2 sowie EN 1363-1. Darüber hinaus bietet die Lösung Bauteilprüfungen EI 120 für Wand und Decke gemäß den Normen EN 13501-2 und EN 1636-1, sowohl von innen nach außen wie umgekehrt.

Maßnahmen zum Schutz vor Einbrüchen ergänzen das Leistungsspektrum der Raum-in-Raum-Lösung. Demnach gehören zum allgemeinen QuarzITe Sicherheitspaket auch eine Systemprüfung zur Einbruchhemmung RC2 nach EN 1627/1630. Zusätzlich verfügt der DC-ITRoom über einen EMV-Schirmdämpfung nach EN 50147-1.

GRÜNE IT AUF GRÜNER WIESE

MODULARES RECHENZENTRUM FÜR BERLINER WASSERBETRIEBE.

Dieser kann durch DC-ITShielding erweitert werden. Die Lösung ist eine geprüfte und präzise High-Frequency-Hülle, die IT-Räume und -Equipment vor elektrischen und magnetischen Störungen sowie der Abstrahlung von Informationen schützt.

Baulichen IT-Schutz bietet QuarzITe durch die Systemprüfung hinsichtlich Staub- und Wasserdichtigkeit IP 65 gemäß EN 60529. Das schließt eine 400 mm Wassersäule über 72 Stunden ein. Nicht zuletzt unterliegt die Raum-in-Raum-Lösung dem dreimaligen Kugelstoß nach DIN 4102-2.

Blaue Engel und Grüne IT

Klinke: „Als kritische Infrastruktur nach dem IT-Sicherheitsgesetz richten wir unser Augenmerk speziell auch auf hohe Sicherheit und Verfügbarkeit des gesamten IT-Systems. Bei der Bewertung der Energie- und Ressourceneffizienz in Rechenzentren wurden die Anforderungen des ‚Blauen Engels' für den energiebewussten Rechenzentrumsbetrieb angewendet und erfüllt. Des Weiteren wird das neue RZ den Kriterien einer TÜViT-Level-3-Zertifizierung gerecht."

Mit der integrierten Green-IT-Technik leistet die Informationstechnologie der Berliner Wasserbetriebe ihren Beitrag zur CO2-Reduzierung, um die Klimaziele des Unternehmens zu erreichen. Der Energieverbrauch konnte mittels intelligenter Klimatisierung und Stromkonzepte sowie des Einsatzes energieeinsparender Hard- und Softwarekomponenten nachhaltig gesenkt werden.

Schließlich haben auf der Rechenzentrumsfläche auch zwei weitere Unternehmen ihre Server untergebracht. „Ein zukunftsweisendes Colocation- Modell, das eine Win-win-Situation schafft. Unternehmen können ihre IT sicher unterbringen, ohne eine eigene Infrastruktur dafür schaffen zu müssen", sagt Klinke. „Die DataCenterGroup hat uns im gesamten Projektablauf als kompetenter Ansprechpartner begleitet und stand während des Prozesses jederzeit für uns zur Verfügung.

Die enge Abstimmung und die gute Kommunikation haben uns bereits während der Bauphase darin bestätigt, den richtigen Partner gefunden zu haben. Das erzielte Ergebnis hat dies bestätigt." Sein Resümee: „Es ist ein tolles Konzept, das uns von der Planung über die Realisierung bis zur Fertigstellung überzeugt hat."

Simon Federle
www.datacenter-group.com

UMSETZEN STATT SCHEITERN

8A-Navigation für agiles Führungscoaching

Unternehmen und deren Märkte befinden sich im Wandel. Kontinuierliche Veränderungen verlangen von uns, dass wir nicht in alten Denk- und Verhaltensmustern verharren, sondern schnell neue Entscheidungen treffen, vor allem aber ins Handeln kommen. Ohne Umsetzung kein Erfolg! Wie beides gelingt, beschreiben die beiden Autoren Elmar Lesch und Ralf Koschinski in ihrem neuen Buch „Umsetzen statt Scheitern".

Mit ihrem 8A-Navigator leiten die Autoren die Leser dazu an, von der Ausredenkultur zur Umsetzungskultur zu gelangen. Die innovative 8A-Umsetzungsmethode unterstützt Führungskräfte dabei, Ermöglicher statt Verhinderer zu sein und so zum agilen Führungscoach zu werden, der sein Team flexibel in kleinen Schritten zur Zielerreichung führt. Die dafür notwendigen erweiterten Kompetenzen werden im Buch explizit beschrieben.

Elmar Lesch, Ralf Koschinski , Umsetzen statt Scheitern, 8A-Navigator für agiles Führungscoaching, Haufe Verlag 2019

MANAGED SERVICE PROVIDER

DIE FÜNF MERKMALE ERFOLGREICHER MSP.

Managed Service Provider (MSP) sind genauso unterschiedlich wie die Services, die sie anbieten. Aber wodurch setzen sich die erfolgreichsten vom Rest der Konkurrenz ab? Die Kaseya Benchmark Survey 2019 legt in diesem Jahr ein besonderes Augenmerk auf Service-Provider mit einem jährlichen Umsatzwachstum von über 20 Prozent.

1. **Zentrales Infrastruktur-Management und Monitoring:**
Je mehr Geräte ans Netzwerk angeschlossen sind, desto häufiger treten Performance-Engpässe auf. In Zeiten der Digitalisierung ist das ein No Go, daher gliedern Unternehmen Management und Monitoring der Netzwerkinfrastruktur verstärkt an Dienstleister aus. Erfolgreiche MSP nennen diese Aufgaben auch als den am schnellsten wachsenden Service. Dabei sind präzises Reporting, Echtzeit-Dashboards und kontinuierliches Monitoring der IT-Umgebung über die Cloud allerdings unverzichtbar.

2. **Die Cloud wird immer wichtiger:**
Dies gilt nicht nur für das Management und Monitoring. Immer mehr Unternehmen migrieren ihre IT-Infrastrukturen in die Cloud – starke MSP ziehen hier mit und bieten ihre Dienste auch über die Cloud an. 71 Prozent der Top-MSP hosten zumindest einen Teil ihrer Kundeninfrastruktur in einer privaten Cloudumgebung (gegenüber 59 Prozent aller Befragten) und konnten so ihre Gewinnmargen fast verdoppeln.

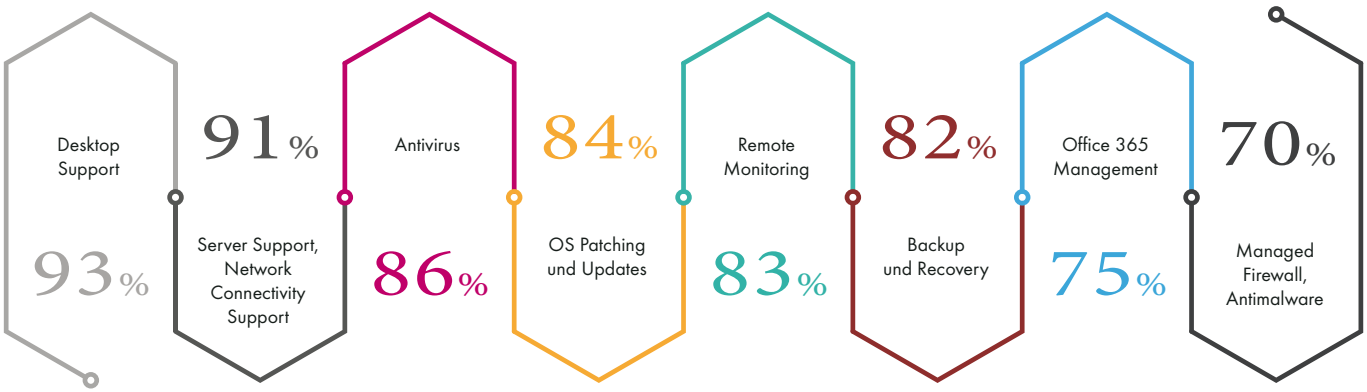
3. **Backup ist unternehmenskritisch:**
Unternehmen sind wegen Technologien wie Big Data, Internet of Things (IoT) und Künstlicher Intelligenz (KI) zunehmend datengetrieben. Damit steigen aber auch die Sicherheitsbedenken wegen Ransomware und Malware-Angriffen. Um dieses Mehr an wertvollen Daten zu schützen und wiederherzustellen, sind leistungsfähige Backup- und Disaster Recovery (BDR)-Funktionalitäten unerlässlich – aus der Hand hochperformanter MSP.

4. **Weniger ist oft mehr:**
Über ein Drittel der besonders starken MSP beschäftigt weniger als zehn Mitarbeiter. Statt einer größeren Belegschaft, setzen sie für zeitintensive Tätigkeiten auf Automatisierung. Die gewonnene Zeit schafft Raum für neue Innovationen, hochwertigere Services und eine effizientere Arbeitsweise. Die Ergebnisse zeigen, dass Umsätze nicht unbedingt proportional zur Mitarbeiterzahl wachsen: Denn auch ein einzelner Techniker kann mit der richtigen Lösung Tausende Endpoints betreuen.

5. **Kostenbasierte Preisgestaltung verschwindet:**
Starke MSP wissen, dass sie nur günstigeren Konkurrenzanbietern in die Karten spielen, wenn sie sich ausschließlich auf die Kosten konzentrieren. Dienstleister müssen stattdessen gezielt auf Kundenbedürfnisse eingehen. Daher sollten sich MSP in erster Linie auf den Mehrwert ihrer Kunden-Services konzentrieren. 22 Prozent der MSP, die dies befolgen, machen mehr als die Hälfte ihres Umsatzes mit einem Mehrwert-basierten Preismodell, verglichen mit MSP (16 Prozent), die auf ein kostenbasiertes Modell setzen.

www.kaseya.com

Die am häufigsten angebotenen Infrastruktur-Management-Dienste, die MSPs anbieten, sind:



© msp-benchmark-survey-report.pdf

USU WORLD 2019

KUNDENSERVICE ZWISCHEN WERTSCHÄTZUNG UND WERTSCHÖPFUNG.

Wie Unternehmen an der Schnittstelle zwischen Mensch & Maschine ihre Services individuell und wirtschaftlich gestalten – das ist eines der zentralen Themen der USU World 2019. Der zehnte Fach- und Anwenderkongress für Kunden, Interessenten und Partner der Aspera GmbH, der LeuTek GmbH und der USU GmbH findet am 14. und 15. Mai 2019 in Berlin statt. Über 500 Fach- und Führungskräfte diskutieren die vielfältigen Aspekte rund um die praxisnahe Digitalisierung von Kundenservices. Wie Serviceorganisationen den digitalen Wandel erfolgreich meistern können, schildern Frank Borchard von der Otto GmbH & Co. KG sowie Oliver Nissen von der Deutschen Telekom Service GmbH in ihren Keynotes.

Trends & Best Practices in sechs parallelen Vortragsreihen

Über 40 Fachreferenten präsentieren praxisnah, wie sich Unternehmen im Wettbewerbsumfeld durch erfolgreiche Service-Konzepte und deren praktische Umsetzung differenzieren. Dabei werden auch neue Trends diskutiert und bewertet, zum Beispiel, ob Service-Organisationen dank KI bereits heute in der Lage sind, Personalisierung mit prädiktiven Fähigkeiten im Service zu kombinieren. Datenbasierte Services sind der Schlüssel für den Erfolg in der vernetzten Wirtschaft von morgen. Es gilt, die damit verbundenen Chancen zu nutzen – für innovative Dienstleistungen, für neue Geschäftsmodelle, für mehr Wertschöpfung – in der IT, im Call Center, beim technischen Kundendienst oder in Vertrieb & Marketing. Themen wie Service-Automatisierung, Self-Service-Strategien, Chatbots, Cloud-Lizensierung und -Monitoring oder Customer Experience Management nehmen ebenso breiten Raum ein wie die Produkt-Neuerungen und -Roadmap für die Anwender. Folgende Schwerpunkte werden in sechs parallel stattfindenden Vortragsreihen behandelt: IT & Enterprise Service Management, Software Asset Management, Business Service & Cloud Monitoring, Knowledge-Lösungen für den digitalen IT- und Kundenservice sowie Portale, Self-Service & UX-Design.

In Vorträgen, Diskussionsrunden, an Demo-Points oder im persönlichen Gespräch liefert die Veranstaltung den Teilnehmern konkrete und kreative Lösungen für ihre individuellen Herausforderungen im Tagesgeschäft und darüber hinaus.

Breites Angebot von USU und Partnern in der Fachausstellung

Gelegenheit zum Networking und Austausch zwischen Kunden und Interessenten besteht auch in der Fachausstellung sowie im Rahmen der kostenlosen Abendveranstaltung. Interessierte können sich vor Ort über das breite Lösungsangebot der USU-Gruppe und ihrer Partner informieren. Folgende Partnerunternehmen beteiligen sich aktiv: endlich GmbH & Co. KG, EWERK, FINANCE ELEMENTS GmbH, FLOWSTER Solutions GmbH, ITSM Group, itSMS GmbH, Liferay GmbH, Pegasystems GmbH, Raynet GmbH, ReLicense AG, scienITec GmbH, Sematell GmbH, SERVIEW GmbH, soffico GmbH und SYSback AG.

Detailinformationen und Anmeldung

Die Konferenz richtet sich an Fach- und Führungskräfte von Service-Organisationen oder -abteilungen und ist branchenunabhängig. Interessierte können sich noch anmelden. Die Teilnahmegebühren belaufen sich auf 600 Euro pro Person für zwei Konferenztage inklusive der Abendveranstaltung mit allen Speisen und Getränken. Rabatte erhalten Gruppen von drei und mehr Personen pro Unternehmen. Detaillierte Informationen und die Möglichkeit zur Online-Anmeldung finden Interessierte auf **https://www.usu.world/de/.**

CONTAINERISIERUNG

WESHALB IT-VERANTWORTLICHE SICH JETZT MIT DIESEM THEMA BESCHÄFTIGEN SOLLTEN.

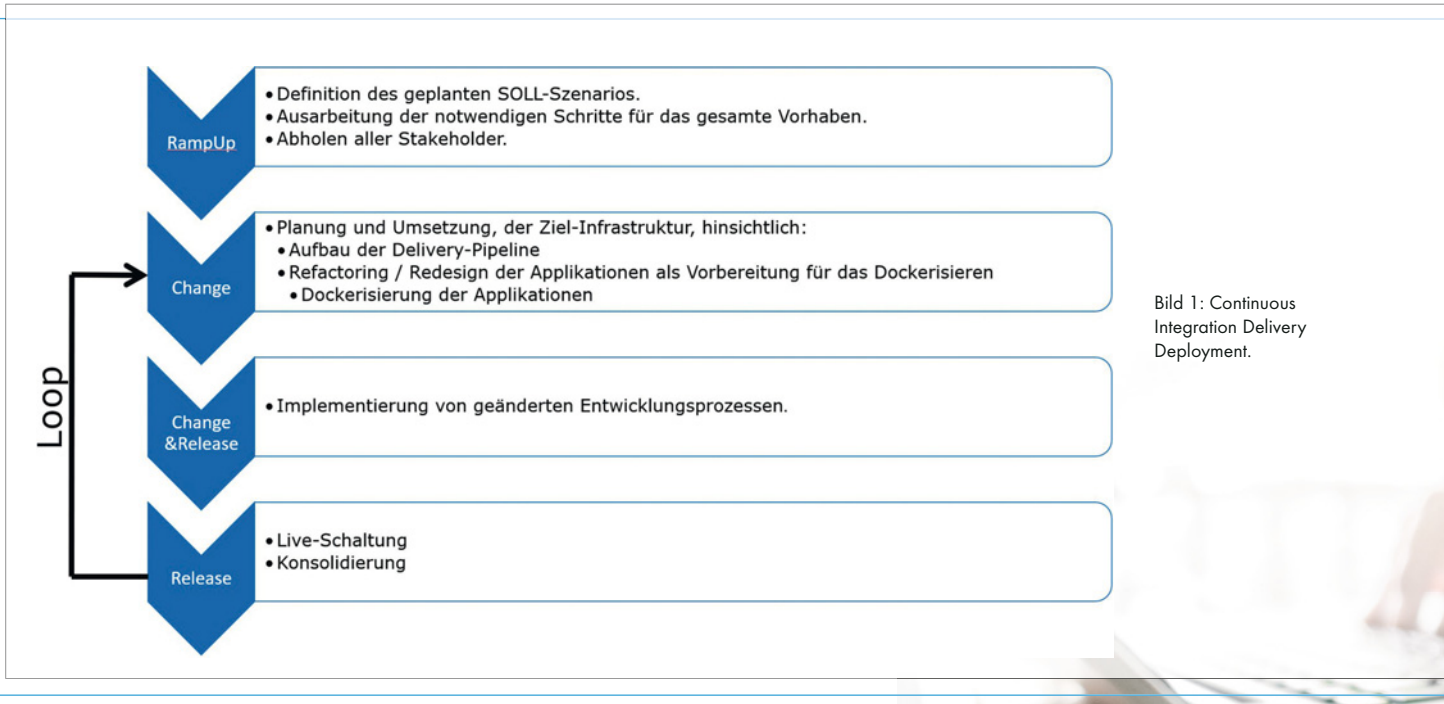


Bild 1: Continuous Integration Delivery Deployment.

Die Digitalisierung stellt IT-Abteilungen auch im Softwarebereich vor neue Herausforderungen. Je mehr Prozesse im Unternehmen digitalisiert werden, desto mehr Anwendungen und IT-Services werden benötigt, um diese digitalisierten Prozesse und die damit verbundenen Produkte und Strukturen abzubilden und zu verwalten. Und je mehr Anwendungen und IT-Services benötigt werden, desto schneller müssen diese entwickelt, ausgerollt und überwacht werden.

Ziel muss es dabei sein, Tempo und Qualität des Software-Lebenszyklus aus Entwicklung, Test, Bereitstellung und Monitoring zu optimieren. Containerisierung stellt einen Ansatz hierfür dar. Laut einer Studie im Auftrag von Microsoft aus dem Jahr 2017 erwarten 90 Prozent der Entscheider in Unternehmen, dass Container-Technologien künftig einen Standard bilden. Dabei sind nur knapp die Hälfte der Unternehmen mit Containern vertraut. Es besteht also deutlicher Nachholbedarf zum Thema Containerisierung.

Das Konzept der Containerisierung ist gar nicht neu: Schon zu Mainframe-Zeiten wurden entsprechende Konzepte eingesetzt. Container ermöglichen es Anwendungen in einer isolierten Umgebung auszuführen. Sie kapseln Dateien, Bibliotheken und weitere Bestandteile einer Anwendung und erwarten Konfigurationsparameter, welche „von außen" gesetzt werden.

Container eines Servers teilen sich denselben Betriebssystem-Kernel und verwenden dessen Isolations-Features. Damit sind Container kleiner, leichtgewichtiger und schneller als virtuelle Maschinen - beispielsweise können sie innerhalb von Sekunden-Bruchteilen gestartet werden.

Das Portieren von Applikationen ist damit deutlich einfacher und schneller möglich. Weite Verbreitung fand das Thema Containerisierung aber erst durch das Open Source-Projekt Docker.

Container: Dank Docker aus der Nische

Die Einführung von Containerisierung stellt außerdem eine gute Vorbereitung für die nächsten Evolutionsstufen des Container-Ökosystems dar: Container-Orchestrierung (Kubernetes) und Cluster-Orchestrierung (SAP Gardener).

Containerisierung vs. Virtualisierung

Mit dem Konzept der Virtualisierung gibt es bereits eine weitere Möglichkeit, virtuelle Ressourcen zur Verfügung zu stellen.

Bei der Virtualisierung sorgt ein sogenannter Hypervisor für die Partitionierung des Servers unterhalb der Ebene des Betriebssystems und erzeugt virtuelle Maschinen, die ausschließlich die physische Hardware

TO GO!

CONTAINER ERMÖGLICHEN ES ANWENDUNGEN IN EINER ISOLIERTEN UMGEBUNG AUSZUFÜHREN. SIE KAPSELN DATEIEN, BIBLIOTHEKEN UND WEITERE BESTANDTEILE EINER ANWENDUNG UND ERWARTEN KONFIGURATIONSPARAMETER, WELCHE „VON AUSSEN" GESETZT WERDEN.

Markus Fensterer, DevOps Consultant, x-cellent technologies GmbH | www.x-cellent.com

miteinander teilen. Bei Containern erfolgt die Virtualisierung auf der Ebene des Betriebssystems, wodurch sich Anwendungen das Betriebssystem teilen.

Im Gegensatz zu Containern benötigen virtuelle Maschinen (VM) sowohl einen Hypervisor als auch ein Gast-Betriebssystem. Dies beeinträchtigt die Portabilität von Anwendungen, verlangsamt den gesamten Prozess und benötigt darüber hinaus mehr Ressourcen (zum Beispiel Speicherplatz). So ist es nicht verwunderlich, dass anfänglich bereits von einer Ablösung des VM-Ansatzes durch die Containerisierung gesprochen wurde. Auf der anderen Seite sind virtuelle Maschinen unter Umständen flexibler und strenger isoliert, da Betriebssystem und Middleware bei jeder Maschine individuell wählbar sind. Bei der Containerisierung dagegen teilen sich mehrere Container die gleiche Serverplattform und müssen deshalb auch auf das gleiche Betriebssystem zurückgreifen.

Mittlerweile hat sich deshalb die Ansicht durchgesetzt, die – in Abhängigkeit vom Anwendungsszenario – von einer Koexistenz der beiden Konzepte ausgeht.

Container und Sicherheit

Betrachtet man die Sicherheitsaspekte im Zusammenhang mit Containern, so stößt man zuerst auf die in der Entwicklung von Softwareanwendungen gängigen Sicherheitsrisiken. So können sich Schwachstellen beispielsweise schnell vom Server-Kernel auf die Container, die diesen Kernel nutzen, ausbreiten. Nicht vertrauenswürdiger Code ist dann in der Lage, diese Schwachstelle auszunutzen und das Gesamtsystem zu kompromittieren.

Ein weiteres Sicherheitsrisiko beim Einsatz von Containern besteht darin, dass Container-Systeme oft Root-Rechte benötigen, um funktionsfähig zu sein. Dies gilt beispielsweise für den Docker-Daemon. Es ist zwar möglich, die Verwendung von Docker auf „vertrauenswürdige Benutzer" zu begrenzen, dennoch besteht die Gefahr, dass der Daemon oder REST-basierende Anwendungen im Container dazu ausgenutzt werden, um Schwachstellen für Hacker zu eröffnen. Grundlage für einen sicheren Einsatz von Containern ist auch hier Software im Container ohne bösartigen Code.

Darüber hinaus muss ein besonderes Augenmerk auf die Richtlinien gelegt werden, die die Interaktion zwischen Container und Host beeinflussen. Wird eine Anwendung in einen Container gepackt, ist sie weiter von den Diensten des Betriebssystems abhängig. Dieses wird allerdings häufig in einer virtuellen Hostumgebung ausgeführt, Die Applikation liegt im Container. An der Schnittstelle zwischen Container und Host-Betriebssystem kann es zu Sicherheitsproblemen kom-

men, wenn die entsprechenden Security Policies nicht verwendet werden oder Leitlinien aus Security Benchmarks verletzt werden. Auch hierbei geht es wieder um die Vertrauenswürdigkeit. Die Repositories, mit denen den Entwicklungsteams Code zur Verfügung gestellt wird, um daraus Container Images zu erstellen, sind nur dann sicher, wenn sie vertrauenswürdig sind. Sie müssen mit Vorsicht behandelt werden.

Continuous Integration, Delivery, Deployment

Der Integrationsaspekt von Containern wird am besten mit den drei „C"s beschrieben: Continuous Delivery, -Integration und -Deployment. In Zeiten der digitalen Transformation stellen die drei „C"s eine zentrale Voraussetzung für eine leistungsfähige und flexible IT dar, die die Geschäftsprozesse eines Unternehmens möglichst optimal unterstützt und umgehend auf Veränderungen und neue Anforderungen von Seiten des Business reagieren kann.

Continuous Delivery steht dabei für Verfahren, Tools und Konzepte mit dem Ziel, qualitativ hochwertige Software zu entwickeln und bereitzustellen. Dank Automatisierung sind schnelle, zuverlässige und wiederholbare Deployments möglich. Erweiterungen und Bug Fixes können rasch und ohne großen manuellen Aufwand an den Anwender ausgerollt werden.

Die Continuous Integration unterstützt den Continuous Delivery-Prozess, denn sie ermöglicht das fortlaufende Zusammenfügen von Komponenten zu einer Anwendung.

Continuous Deployment ist eine Weiterentwicklung von Continuous Delivery. Während bei der Continous Delivery eine neue Softwareanwendung oder -Erweiterung lediglich in eine Staging Area ausgeliefert wird, von wo sie dann manuell in die Produktivumgebung übernommen werden muss, automatisiert Continuous Deployment auch den Übergang in den Produktivbetrieb. Für alle drei „C"s stellen Container-Technologien eine wichtige Grundlage zur Umsetzung dar.

Migration von Legacy-Anwendungen

Jedes Unternehmen, das heute vor der Herausforderung steht, Container im Unternehmen einzusetzen, muss sich die Frage stellen, ob und wie es die bereits im Unternehmen verwendeten Software-Anwendungen in die neue Technologie integriert, beziehungsweise auf diese migriert. Experten raten dabei dazu, die bestehende IT-Infrastruktur zuerst einmal zu standardisieren und auf eine einheitliche – in der Regel heute cloudbasierte – Plattform zu transformieren. Danach besteht die Möglichkeit, diese neu geschaffene IT-Umgebung mit Containern leistungsfähiger und flexibler zu gestalten.

Containerisierung im Unternehmen

Wie eingangs beschrieben führt die Digitalisierung zu einem völlig neuen Verständnis für die Bedeutung von Softwareentwicklung. Der Kunde – extern wie intern – erwartet dabei eine immer kürzere Time-to-Market und sofort funktionstüchtige Anwendungen. Container sind ein zentraler Ansatz, um diese Anforderungen von Seiten der IT-Abteilung erfüllen zu können. Denn nur so ist sie in der Lage, schneller, effizienter und

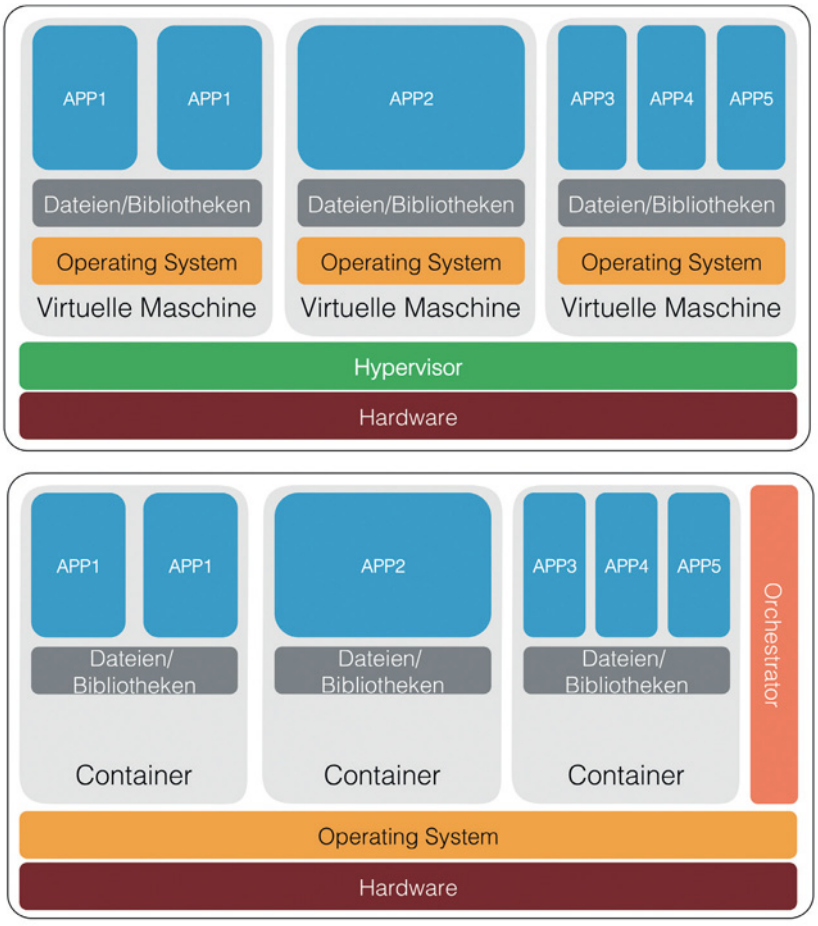


Bild 2: Unterschiede zwischen Container und virtueller Maschine.

Darüber hinaus bietet Docker Inc. bereits seit 2017 das „Modernize Traditional Applications"-Programm. Gegen eine Pauschalgebühr erhalten Anwenderunternehmen einen Migrationsservice und ein darauf folgendes „Hilfe-zur-Selbsthilfe"-Programm, bei dem Spezialisten im Unternehmen geschult werden, damit sie dann die weitere Containerisierung ihrer Legacy-Anwendungen durchführen können.

kostengünstiger neue Anwendungen und IT-Services anzubieten.

Die spezifischen Vorteile von Containern liegen dabei insbesondere in ihrer geringen Größe, Wiederverwendbarkeit sowie sicheren und leichten Verwaltung. Weitere Vorteile sind eine bessere Ausnutzung von Ressourcen und eine höhere Agilität.

Markus Fensterer

AACHENER ERP-TAGE 2019

VORDENKEN, GESTALTEN, UMSETZEN.

„Smart Operations – Vordenken. Gestalten. Umsetzen." So lautet der Titel der 26. Aachener ERP-Tage, die vom 4. bis 6. Juni 2019 in Aachen stattfinden. Seit über einem Vierteljahrhundert bieten die ERP-Tage ein wichtiges Forum für unabhängige ERP-Informationen und den Austausch zwischen Anbietern und Anwendern.

Die Grundidee der Veranstaltung existiert schon lange, aber die jährlich neuen Inhalte sind den realen Anwendungen immer um eine Nasenlänge voraus. Schließlich ist es das Ziel der Organisatoren vom FIR, IT-gestützte Betriebsorganisation für zukünftige Unternehmensentwicklung zu betreiben. Das gibt auch der aktuelle Titel wieder: die diesjährigen ERP-Tage stehen unter dem Motto „Smart Operations – Vordenken. Gestalten. Umsetzen."

Smart Operations

Unter Smart Operations verstehen wir die Digitalisierung der Auftragsabwicklung mithilfe umfangreicher Informationstechnologien und aller benötigten Tools und Methoden, um die Effizienz eines Unternehmens zu verbessern.

Die im Unternehmen anfallenden Prozessdaten werden so zu wertvollen Informationen, die eine qualitativ höherwertige Auftragsabwicklung ermöglichen. Um die Transparenz und Prognosefähigkeit der Wertschöpfungssysteme mithilfe von Smart Operations durch die Nutzung von ERP- und ME-Systemen zu verbessern, werden wir mit Ihnen Lösungsstrategien vordenken und innovative Prozesse für zuvor identifizierte Handlungsbedarfe gestalten, damit Sie diese für eine optimierte Auftragsabwicklung zukünftig umsetzen können.

Dabei klären wir, wie sich innovative Technologien wie Blockchain, Data Analytics und KI auf betriebliche Anwendungssysteme auswirken und ob sich die Systeme zu Kollaborationsplattformen entwickeln.

Theorie und Praxis treffen aufeinander

Die Aachener ERP-Tage nehmen diese Idee auf. In zwei Vortragssträngen werden innovative Ideen und praktische Beispiele aus ERP-, ME- und angrenzenden betrieblichen Systemwelten vorgestellt. Parallel dazu zeigen verschiedene Anbieter auf dem Ausstellerforum ihre Lösungen. Der Besucher erhält anschauliche Informationen und gewinnt einen Überblick aus der Welt der betrieblichen Anwendungssysteme. In den Pausenzeiten gibt es ausreichend Raum für den Austausch zwischen Anwendern und Anbietern. Bei noch spezifischerem Interesse vermittelt der vorgelagerte Praxistag in Workshops detailliertere Informationen zu gegenwärtigen und zukünftigen Anwendungsoptionen.

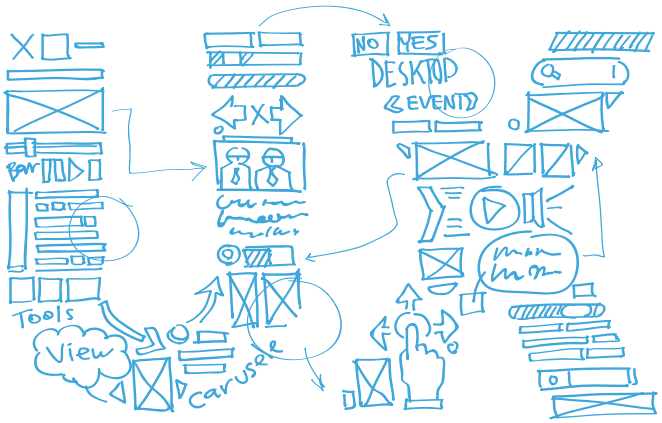
www.erp-tage.de

26. Aachener ERP-Tage
04. + 05.–06.06.2019

Digitale Services sind heutzutage maßgeblich am Erfolg eines Unternehmens beteiligt. Häufig scheitern gleichwohl die Anwendungen im großen Stil. Da hilft es, UX Designer einzuschalten, die von Anfang an die erkunden, für die das Unternehmen den Service entwickelt: User und Mitarbeiter. Mit User Experience Design gelingt es, die wirklichen Bedürfnisse der Menschen zu erkennen und genau dafür innovative Lösungen zu entwickeln, die begeistern.

Für jede Lebenslage gibt es eine App. Sei es die Zeitung am Morgen, der Fitness-Tracker oder etwa auch die Apps, die über das Wohl und Wehe des Online-Bankings entscheiden. Bei der Vielzahl an Angeboten steht jederzeit die App zur Verfügung, die man sich wünscht. Doch mittlerweile entscheiden gerade bei der Masse an Angeboten ausschließlich die User, welche Angebote sie nutzen wollen. Und dies gilt besonders für sensible Apps wie zum Beispiel die bereits genannten sicherheitsrelevanten Anwendungen bei Finanzgeschäften. Denn das Überangebot auf dem Markt sorgt dafür, dass stets eine passende Alternative zur Verfügung steht, die besser gefällt. Schnelligkeit und Bedienerfreundlichkeit bilden dabei die Grundvoraussetzung für die Entscheidung der Nutzer. Zeigt eine App nicht schnell genug und kommod die gewünschten Ergebnisse an, ist die Gefahr groß, dass der User einfach zum nächsten Anbieter wechselt.

Der Unternehmenserfolg von digitalen Service-Anbietern hängt allerdings nicht nur von der Akzeptanz der Kunden gegenüber Produkten und Services ab. Auch wie Mitarbeiter digitale Unternehmensanwendungen nutzen, spielt eine entscheidende Rolle. Wo der Wettbewerb auf Kundenseite nur einen Klick entfernt ist, sabotieren in Unternehmen selbstgestrickte Sonderlösungen die internen Prozesse. Zu häufig kommen ganze Abteilungen mit den digitalen Anwendungen im Unternehmen, die ihnen vorgesetzt werden, nicht zurecht. Das ist der Punkt, an dem Mitarbeiter die berüchtigten „work-arounds" erfinden. Solche schaffen scheinbar eigene Lösungen, die die für schlecht befundenen Unternehmensanwendungen ersetzen sollen. Doch diese Sonderlösungen gefährden die internen Arbeitsprozesse mehr als gedacht. Wenn sich ein Kunde beispielsweise nach dem Bearbeitungsstand seines Anliegens erkundigt, der Mitarbeiter aber nicht schnell genug an die relevanten Daten herankommt, weil seine Kollegen diese in einem eigenen Work-Around-Programm abspeichern, sinkt die Servicequalität dem Kunden gegenüber, da es im Unternehmen Insel-Lösungen gibt. Das Unternehmen ist in der Folge nicht mehr ganzheitlich auskunftsfähig, besonders im bedeutsamen Schadenmanagement ist so etwas ein absolutes No-Go. Kann ein Mitarbeiter einem Kunden nicht schnell genug helfen, wirft das Unternehmen am Ende Geld aus dem Fenster hinaus. Denn nicht nur schlechter Service ist ein Grund für den Kunden, die Konkurrenz zu wählen. Das Unternehmen hat zudem sehr viel Geld in eine Unternehmensanwendung investiert, die die Mitarbeiter schlussendlich gar nicht passend einsetzen und nur ungenügend nutzen. Im schlimmsten Fall wechselt der Kunde zur Konkurrenz – und die eigenen Mitarbeiter auch. Es kann ein immer wiederkehrender Teufelskreis für solche Unternehmen sein, die die Anwendungen nicht auf ihre User und Mitarbeiterschaft abstimmen und deren Bedürfnisse nicht erfüllen, weil sie sie nicht erkennen.



Innovation durch Nähe

Aber wie entwickeln Unternehmen Services, die sowohl Kunden als auch Mitarbeiter begeistern? User Experience Design (UX) bietet die passenden Werkzeuge und Strategien, die die Beziehung zwischen Kunden, Mitarbeitern und Unternehmen nachhaltig und sachgerecht-modern gestalten. Dafür betrachtet UX den User und die Mitarbeiter

USER EXPERIENCE DESIGN

GELUNGENES RENDEZVOUS MIT USER UND MITARBEITER.

in deren Umgebung und konkreter Lebenssituation. UX hat dabei eine klare Aufgabe: Herausfinden, was die Kunden und Mitarbeiter tatsächlich wollen. Intensive User Research und Empathie helfen bei der Beantwortung dieser Frage.

Ein UX Designer muss mit seinem Team nah an User und Mitarbeiter herangehen. Ein Beispiel: Entwickelt ein UX Designer eine Fahrkarten-App, muss er den User zunächst in seinem Umfeld, dem Bahnhof, beobachten. Doch das erfordert Nähe und Empathie. Steht der User mit klammen Fingern bei fünf Grad Celsius und „Schietwetter" am S-Bahnsteig in Hamburg, muss der Designer es ihm gleichtun, um die Bedürfnisse des Users zu erspüren und zu erkennen. Die App müsste somit zum Beispiel vielleicht große Schaltflächen haben, die auch mit klammen Fingern nutzbar sind, und den User in so wenigen Schritten wie möglich zum Kauf der Fahrkarte führen. Würde der UX Designer für die App-Entwicklung in einem beheizten Büro bei einem Cappuccino sitzen, würde das Ergebnis anders aussehen. Nur wenn der Designer selbst am kalten Bahnhof steht, begreift er, welche Lösungen der User benötigt.

Personas schaffen heißt verstehen lernen

Durch Einfühlungsvermögen kann das Team also Innovationen entwickeln, die zum Ziel einer gut umgesetzten Service-Lösung führen: mehr Erfolg für alle Beteiligten, für Kunden, Mitarbeiter und das Unternehmen. Und noch viel wichtiger: Lösungen, die die User und die Mitarbeiter auch wirklich benötigen. Oft passiert es, dass Unternehmen Services entwickeln, bei denen sie meinen zu wissen, was diese brauchen. Erst im Nachhinein, wenn das Produkt bereits programmiert ist und das Unternehmen reichlich Geld dafür ausgegeben hat, stellt sich heraus, dass die User und die Mitarbeiter die Anwendung gar nicht fachgerecht einsetzen und demnach auch nicht gewinnbringend nutzen. Wo liegt der Fehler? Nicht am Ende des Prozesses, nicht in der Entwicklungsphase allein, sondern ganz einfach am Anfang von allem: Das Unternehmen kannte seine User und seine Mitarbeiter schlicht und einfach nicht. Diesen Fehler können UX Designer allerdings vermeiden helfen, wenn ihnen von Anfang an Verantwortung übertragen wird. Dann definiert das gesamte, fachübergreifende Team das Problem. Dort stellt es heraus, was es durch die User Research gelernt hat. Aufbauend auf den Beobachtungen entwickelt das Team sogenannte Personas. Dies sind rhetorisch leicht überspitzte Personen, die die Usermerkmale als Konzentrat widerspiegeln. Dabei handelt es sich nicht allein um statistische Größen, die beschreiben, ob die gesuchte Zielgruppe etwa 20 bis 30 Jahre alte Frauen oder Männer in einem sehr allgemeinen Sinne betrifft. Personas repräsentieren im Gegenteil konkrete, einzelne Personen. Der Designer entwickelt zum Beispiel eine App für Larissa, die im wohlhabenden Hamburger Viertel Blankenese wohnt und ihre Freizeit im Segelclub verbringt. Larissa hat aber einen anderen Hintergrund als Pascal, der im alternativen Schanzenviertel wohnt und in seiner Freizeit gerne Poetry Slams besucht. Damit wird schnell deutlich, dass soziale Gegebenheiten die Entwicklung von digitalen Services maßgeblich und entscheidend beeinflussen. Personas erleichtern somit die Kommunikation im Designprozess und helfen Unternehmen bei der passgenauen Entwicklung innovativer Services.

> USER EXPERIENCE DESIGN (UX) BIETET DIE PASSENDEN WERKZEUGE UND STRATEGIEN, DIE DIE BEZIEHUNG ZWISCHEN KUNDEN, MITARBEITERN UND UNTERNEHMEN NACHHALTIG UND SACHGERECHT-MODERN GESTALTEN.
>
> Bernd Lohmeyer, Inhaber lohmeyer, Business UX | www.lohmy.de

Endlich Schluss mit dem Guesswork

Die Entwickler definieren zumeist vier bis fünf Personas, für die sie im Anschluss Lösungsansätze sammeln. Dort gilt: Keine Idee zur Lösung ist zu absurd, als dass sie nicht durchgespielt wird. Nachdem das Team auf Basis ausgewählter Ideen Prototypen entwickelt hat, testen reale User und Mitarbeiter die Anwendung auf ihre Tauglichkeit. Denn ob ein Lösungsansatz geeignet ist oder nicht, zeigt sich erst durch praktische, wirkliche Testverfahren. Die Designer lernen aus dem Nutzerfeedback, beheben Fehler und verbessern ihre Lösungen. Der Designprozess ist also iterativ und wiederholt sich so lange, bis die Services tatsächlich passen. Bisher haben die IT-Entwickler noch keine Zeile Code geschrieben. Jedoch haben Designer mit ihnen gemeinsam jetzt eine passende Lösung für ihre User und Kollegen gefunden. Dieses strategische Vorgehen von UX Designern verhindert also, einen teuren Fehler zu verursachen durch alleiniges Guessworks. Denn nun wissen alle Bescheid, wie die App sein muss und wirklich Anwendung findet.

Bernd Lohmeyer

NEUE WEGE GEHEN

TOOLS UND BEWERTUNGSKRITERIEN FÜR DIE WEBSITERECHERCHE.

Sie haben einen interessanten Content erstellt und möchten diesen nun bekannter machen. Bei diesem handelt es sich zum Beispiel um ein E-Book, ein Online-Tool oder eine Infografik. Um themenrelevante Websites zu finden und zu bewerten, haben Sie verschiedene Möglichkeiten und sollten sich immer wieder neue suchen. Ein paar Recherchemethoden und Bewertungskriterien lernen Sie in diesem Artikel kennen. Neben der klassischen Google-Suche gibt es diverse Tools auf dem Markt, von denen in diesem Beitrag ein paar vorgestellt werden.

Doch wozu sollten Sie überhaupt neue Websites suchen? Es ist zwar möglich, dass Sie immer wieder denselben Webmaster kontaktieren und ihr bestehendes Kontaktnetzwerk nutzen. Sie sollten jedoch stetig nach neuen Websites Ausschau halten. Die erste Anlaufstelle ist wie so oft im täglichen Leben die Google-Suche, bei der Sie nicht nur nach einfachen Phrasen oder Keywords suchen können. Was viele nicht wissen: Google kann mit Suchparametern arbeiten.

1. Tools und Tipps zur Websiterecherche

1.1 Google-Suche mit Parametern

Neben den erweiterten Sucheinstellungen (Einstellungen -> Erweiterte Suche), bei denen Sie unter anderem die Sprache, die Domainendung und die Aktualität eines Suchergebnisses einstellen können, sollten Sie mit Suchparametern arbeiten. Dadurch lässt sich die Recherche präzisieren und die Ergebnisse sind genauer auf Ihre Anfrage zugeschnitten. Dass Sie bei Google nach Phrasen suchen können, ist den meisten sicherlich bekannt. Sucheingaben wie „Trat ich heute vor die Türe“ oder „Wer reitet so spät durch Nacht und Wind?“ hat jeder schon einmal eingegeben. Ebenso bekannt ist das Minus, mit dem bestimmte Begriffe ausgeschlossen werden können. Neben dem „-“-Symbol können Sie noch weitere Symbole und Parameter nutzen:

Wildcard-Suche: Mit dem Sternchen (*) können Sie sich alle Suchergebnisse ausgeben lassen, bei denen der Anfang einer Phrase vorkommt. Zum Beispiel: „Spaghetti mit *“. Hierbei werden alle Ergebnisse ausgegeben, die mit „Spaghetti mit“ in Verbindung stehen, also Spaghetti mit Tomatensoße, mit Hackfleischsoße, mit Käsesoße und so weiter.

Oder-Suche: Mit dem Pipe-Symbol (|) können Sie bei der Suche verschiedene Begriffe trennen, was Google als „oder“ interpretiert. Ein Beispiel wäre „do it yourself | diy regal“. Google zeigt hier Ergebnisse, die entweder do it yourself und diy enthalten.

Synonym-Suche: Mit dem Tilde-Symbol (~) können Sie nach Synonymen oder ähnlichen Begriffen suchen. Hierdurch kommen Sie auf neue Ideen und Suchansätze. Die Eingabe von „~pkw geringer verbrauch“ liefert ebenfalls Ergebnisse die Begriffe wie „Auto, verbrauchsgünstig, Kraftstoffverbrauch, Verbrauchswerte“ enthalten.

intitle, intext, inurl: Kombiniert mit einem Keyword liefern Ihnen diese Parameter Ergebnisse, bei denen das Keyword im Text, im Titel oder in der URL vorkommt. Die Ergebnisse unterscheiden sich von der regulären Google-Suche, da hierbei weiter eingegrenzt wird. Dadurch können Sie viel gezielter nach Websites suchen.

Suchparameter lassen sich übrigens auch kombinieren. Übersichtliche und vollständige Listen mit Anwendungsbeispielen finden sich auf verschiedenen Blogs und Portalen.

1.2 Google Alerts

Mit den Google Alerts können Sie sich automatisch tagesaktuelle Veröffentlichungen per Mail zuschicken lassen. Sie geben hierzu ganz einfach die Phrasen oder Keywords ein, zu denen Sie thematisch passende Artikel zugesendet bekommen möchten. Sie können auch hier mit den Suchparametern arbeiten und gewisse Kriterien ein- oder ausschließen.

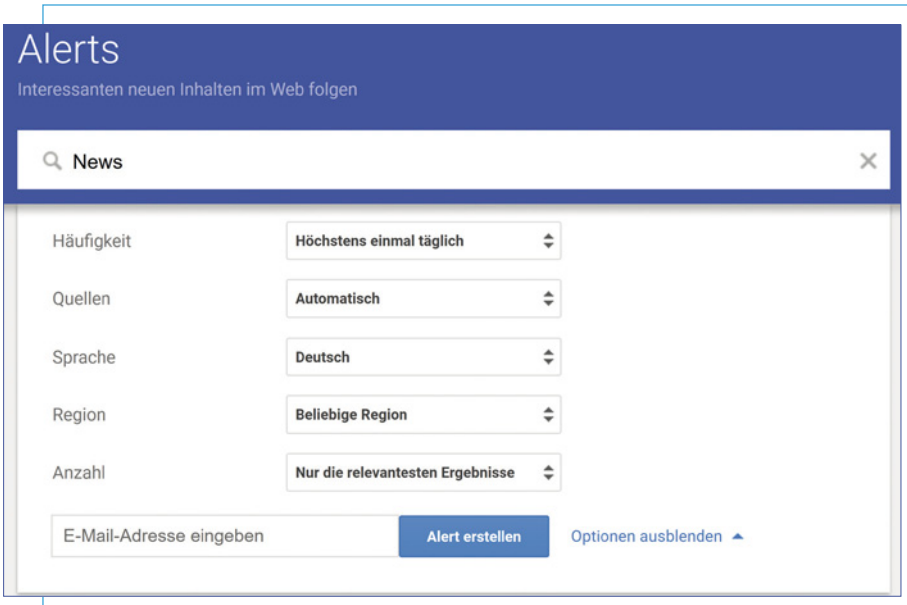


Bild 1: Google Alerts Einstelllungen.

Es empfiehlt sich, verschiedene Alerts mit unterschiedlichen Keywords und Kombinationen zu erstellen. Dadurch erhalten Sie ein viel größeres Angebot an Websites, die zu Ihrer Suchanfrage passen. Außerdem sollten Sie die Suchergebnisse eingrenzen. Unter den Optionen können Sie einstellen, wie oft Sie die entsprechende Mail erhalten möchten und welche Sprache oder welche

LESEN SIE MEHR ÜBER

Linkmarketing-Kampagnen in folgendem Whitepaper: https://www.eology.de/modernes-linkmarketing-fuer-ihren-seo-erfolg/

Region für Sie relevant sind. Suchen Sie beispielweise nur nach Seiten aus Österreich, bietet es sich an, diese Region auszuwählen. Andernfalls werden Ihnen sämtliche Ergebnisse zu den entsprechenden Sucheingaben ausgegeben. Hierbei bekommen Sie mitunter eine sehr große und nicht mehr überschaubare Menge geliefert. Sollten Sie allerdings international tätig sein und sämtliche Websites als relevant betrachten und jede einzeln untersuchen wollen, verzichten Sie auf die Filter.

Durch die Google Alerts werden Ihnen alle möglichen, neu veröffentlichten Beiträge in übersichtlicher Form zugesendet. Hierbei handelt es sich zum einen um Beiträge auf bekannten Seiten, aber zum anderen auch um Blogs und kleinere Magazine. So decken Sie eine große Bandbreite ab und können ohne großen Aufwand schnell an eine Menge themenrelevanter Websites kommen.

Die Google Alerts sind sehr einfach und benutzerfreundlich aufgebaut. Sie können hier nichts „kaputt machen". Testen Sie sich einfach durch und spielen Sie ein bisschen mit den Keywords, Phrasen und Einstellungen. Sollte ein Alert nicht das gewünschte Ergebnis liefern oder nicht zielführend sein, können Sie diesen ganz einfach wieder löschen.

1.3 ahrefs.com

Natürlich gibt es auch abseits von Google die Möglichkeit, nach Websites zu suchen. Neben der fast schon abwegig erscheinenden Idee, andere Suchmaschinen wie zum Beispiel bing oder Yahoo zu nutzen, können Sie auf Tools zurückgreifen.

Ein solches und zugleich benutzerfreundliches Onlinetool finden Sie unter der gleichnamigen URL ahrefs.com. Hier können Sie zum einen den Stand Ihrer eigenen Backlinks ermitteln, wenn Sie herausfinden möchten, wo Ihre Website bisher alles verlinkt wurde. Zum anderen können Sie hierüber auch sehr schnell an neue potenzielle linkgebende Seiten kommen. Das geschieht ganz einfach dadurch, indem Sie hier einen Ihrer Mitbewerber oder eine bekannte thematisch relevante Website untersuchen lassen und sich im Anschluss daran die bestehenden Backlinks näher anschauen. Sie gehen hier am besten von den aktuellsten Veröffentlichungen aus und prüfen jedes Ergebnis. Über den Reiter Backlinks -> Neu gelangen Sie zur Übersicht. Über einen Klick auf „Export" können Sie sich die Ergebnisse als Excel-Datei herunterladen und nach Belieben bearbeiten und filtern. Damit Sie nicht jeden Link, der als einfacher Text vorliegt, einzeln kopieren und einfügen müssen, nutzen Sie am besten die Funktion, einen Hyperlink zu kreieren. Das funktioniert bei Excel ganz einfach: =Hyperlink(das Feld, in dem die URL als Text steht, zum Beispiel A2). Daraufhin wird das entsprechende Feld in einen Hyperlink umgewandelt und Sie können es direkt aus dem Dokument heraus anklicken.

Wie schon bei den Google Alerts empfiehlt es sich auch bei ahrefs.com, die Ergebnisse einzugrenzen. Lassen Sie sich zum Beispiel nur einen Link pro Domain anzeigen oder grenzen Sie den Zeitraum ein. Zudem können Sie auch den Linktyp, die Sprache und den Traffic einstellen, wenn Sie nur bestimmte Ergebnisse vorliegen haben möchten.

1.4 SISTRIX

SISTRIX können Sie in zweierlei Hinsicht nutzen: Zum einen können Sie hierüber an

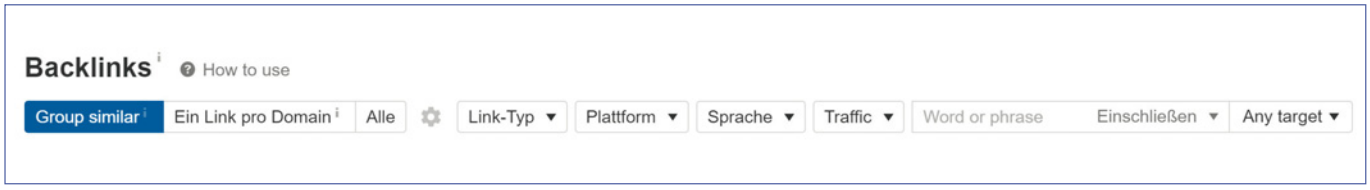


Bild 2: Backlink-Menü ahrefs.com.

neue Rechercheergebnisse kommen und zum anderen Websites bewerten. In diesem Abschnitt geht es zunächst um die Recherchemöglichkeiten, die das Tool bietet. Ähnlich wie bei der Google-Suche können Sie mit Keywords arbeiten. Empfehlenswert ist es, immer zuerst die eigene Website zu checken. Anhand dieser Ergebnisse können Sie ermitteln, welche Keywords für Sie bisher bei Google für das Ranking relevant sind. Basierend darauf starten Sie am besten eine Google-Recherche. Dadurch finden Sie Websites, die mit den für Sie relevanten Keywords ranken und mit einer hohen Wahrscheinlichkeit stimmen diese mit dem Thema Ihres Anliegens (Webshop oder zum Beispiel E-Book) überein. Behalten Sie dabei stets die Themenrelevanz und Nutzerintention im Blick.

Über die Funktion Chancen (Keywords -> Chancen) schlägt Ihnen das Tool die Keywords vor, die auf Seite zwei von Google gelistet werden. Diese werden eher weniger geklickt und Sie sehen auf einen Blick, welche Keywords Sie bei Ihrer Recherche in den Fokus stellen sollten, um damit auf Seite eins bei Google zu kommen.

Eine weitere nützliche Funktion finden Sie unter Links -> Links. Mit dieser können Sie sich – wie bei ahrefs.com – Seiten ausgeben lassen, welche die Website verlinkt haben und hiermit thematisch relevante Ergebnisse finden. Ein wichtiger Hinweis, um bei SISTRIX noch mehr Daten zu erhalten: Aktiveren Sie immer die Funktion LinkPlus! Übrigens können Sie SISTRIX nicht nur in Deutschland nutzen. Das Tool wird stetig um neue Länder und Keyword-Pools erweitert. Dadurch eignet sich das Tool nicht nur zur Recherche und Analyse in der deutschsprachigen DACH-Region, sondern auch für internationale Recherchen und Projekte. In manchen Ländern ist eine größere Datenmenge vorhanden als in anderen. Im Blog des Toolbetreibers werden Sie über alle Änderungen jederzeit informiert.

1.5 searchmetrics

Auch dieses Tool eignet sich für den internationalen Markt. Analog zu SISTRIX können Sie bei searchmetrics unter anderem Daten zu Keywords, Rankings und Backlinks erhalten. Das Tool ist ebenso übersichtlich und benutzerfreundlich gestaltet und baut den Support für weitere Länder stetig aus.

Wenn Sie eine Website in die Suchmaske eingeben, erhalten Sie auf einen Blick relevante Geodaten und können herausfinden, ob die Website von den Nutzern im Zielland aufgerufen wird. Sie können sich unter dem Reiter Backlinks die bereits bestehen Links einer Domain ausgeben lassen.

Sie haben verschiedene Möglichkeiten, die Suche einzugrenzen und sich zum Beispiel nur die neuesten Links anzeigen zu lassen. Das ist dann ratsam, wenn Sie auf Aktualität Wert legen und möglicherweise eine Artikelergänzung vorschlagen möchten. In diesem Fall würden Sie sich einen passenden aktuellen Beitrag heraussuchen und den Webmaster oder Redakteur direkt kontaktieren. Wenn Ihr Content überzeugen kann und den Artikel sinnvoll ergänzt, wird der zuständige Redakteur bereitwillig eine Artikelergänzung vornehmen.

Die meisten Redakteure freuen sich über Input oder schreiben vielleicht sogar direkt noch einen Artikel zu der Thematik.

Da searchmetrics den Fokus unter anderem auf die Internationalisierung legt, sehen Sie direkt, aus welchem Land die jeweilige Website stammt, auf die verlinkt wurde. Das erleichtert Ihnen die Auswahl der potenziellen Linkgeber.

1.6 SimilarWeb

Ein englischsprachiges Tool (das zudem noch auf Japanisch und Französisch verfügbar ist), das Sie sowohl für den Traffic als auch für Geodaten nutzen können, ist SimilarWeb.

Eine für den Zweck der Website-Recherche allerdings deutlich nützlichere Funktion stellt Similar Sites dar. Hierbei sucht das Tool automatisch nach ähnlichen Seiten, ausgehend von der Website, die Sie aktuell untersuchen. Neben der Website von SimilarWeb gibt es noch eine Chrome-Erweiterung. Die Website liefert Ihnen zwar mehr Daten, für den schnellen Überblick ist das Browser-Addon allerdings eine gute Wahl.

1.7 SEMrush

SEMrush ist ein Tool, bei dem Sie zunächst eine eigene Kampagne pro Website anlegen und sich daraufhin Daten ausgeben lassen. Ähnlich wie bereits vorgestellte Tools, crawlt SEMrush die Backlinks der zu untersuchenden Website und gibt diese aus. Hierbei werden Links, die inzwischen offline sind, nicht angezeigt, sodass Sie sich hierum nicht kümmern müssen. Bei anderen Tools werden auch die offline-Links angezeigt.

Das kann in anderen Anwendungsfällen durchaus nützlich sein, für die Website-Recherche liefert dies nur bedingt einen Anhaltspunkt.

Nachdem Sie nun ein paar Tools kennengelernt haben, sollten Sie sich noch etwas mit der Qualität Ihrer Rechercheergebnisse befassen. Auf welche Kriterien Sie hierbei besonders achten sollten und welche Tools Ihnen bei der Bewertung potenzieller Linkpartner helfen, behandelt der folgende Abschnitt.

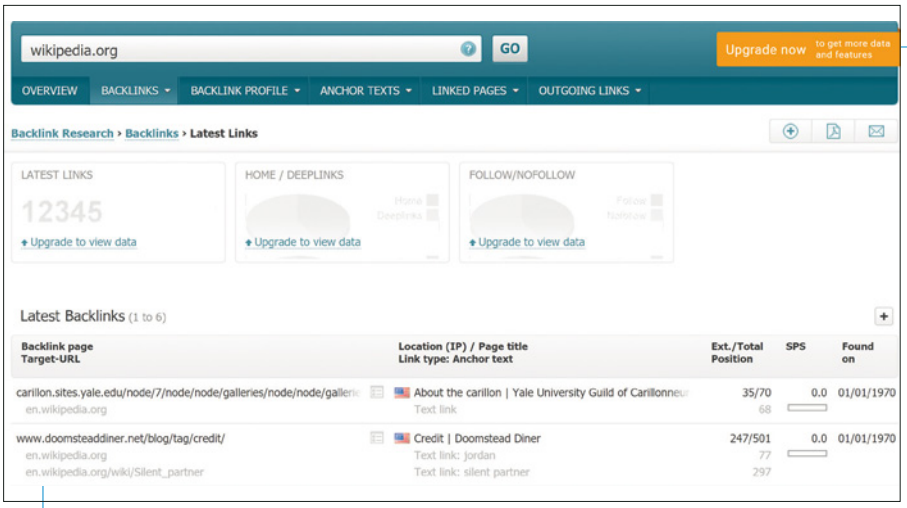


Bild 3: searchmetrics Backlinks, Beispiel wikipedia.org.

2. Bewertungskriterien

Um eine Website zu bewerten, können Sie mit und ohne Tools vorgehen. Es bietet sich jedoch immer eine Kombination aus beidem an, da Sie vieles nicht ohne Tools überprüfen können.

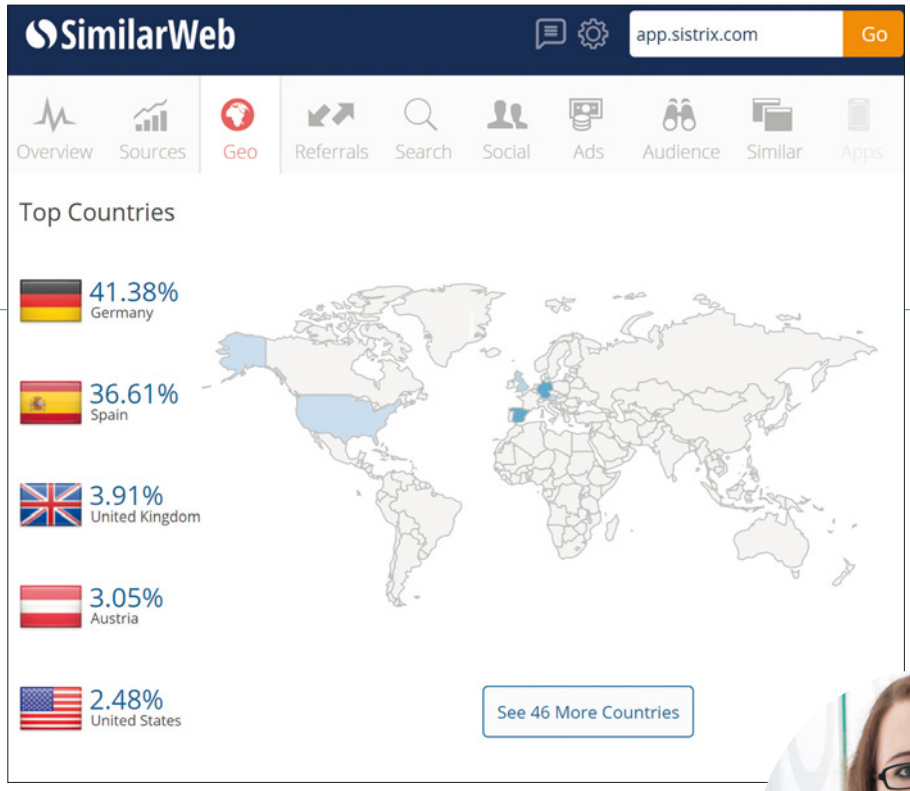


Bild 4: Geodaten in SimilarWeb, Beispiel de.sistrix.com.

2.1 Bewertungskriterien ohne Tools

Bei vielen Websites können Sie auf den ersten Blick erkennen, ob die Seite einer näheren Untersuchung bedarf oder ob Sie sich die Mühe sparen können und diese direkt aussortieren.

Negative Merkmale einer Website können sein:

- Das Layout ist nicht ansprechend gestaltet oder veraltet.
- Eine Website besteht nur aus Artikeln, die in fast jedem Beitrag einen Link zu einer kommerziellen externen Website haben.
- Das Impressum ist nicht gepflegt oder liegt nur als Bilddatei vor. (Tipp: Websitebetreiber können sich auch anders vor Spam schützen, indem Sie die E-Mail-Adresse zum Beispiel so hinterlegen, dass Sie nicht automatisch als solche erkannt wird.)
- Wenn eine Website sehr viele Themen bedient, kann das ein Hinweis auf eine Seite sein, die nur dazu da ist, um Artikelplätze zu verkaufen und damit Geld zu verdienen. Sie müssen hier abwägen, ob es sich um einen Blog mit entsprechend weitem Interessengebiet des Bloggers handelt oder ob der kommerzielle Gedanke vorliegt.
- Neben den Themenbereichen ist die Aktualität ein wichtiger Punkt. Es hilft Ihnen nichts, wenn eine Seite sehr viele Beiträge am selben Tag veröffentlicht und Ihrer dabei untergeht. Es ist ebenso nicht zielführend, wenn Sie eine Website finden, die kaum Beiträge veröffentlicht. Wurde dort seit mehreren Monaten nichts mehr veröffentlicht, können Sie davon ausgehen, dass die Seite nicht aktiv betreut wird. Möglicherweise hat bereits ein starker Trafficverlust stattgefunden und kaum jemand würde Ihren Beitrag lesen.

Die Websites, die nach dieser Vorauswahl noch vorhanden sind, untersuchen Sie mit entsprechenden Tools.

2.2 Bewertungskriterien mit Tools

Damit Sie bei Websites hinter die Fassade blicken können, benötigen Sie die Hilfe von ein paar Tools.

SISTRIX: Mit dem bereits erwähnten SISTRIX untersuchen Sie die Seite auf ihre Keywords und nehmen den Sichtbarkeitsverlauf unter die Lupe. Das liefert Ihnen einen Anhaltspunkt, wie gut die Seite besucht wird. SISTRIX gibt die Sichtbarkeit zum einen als Zahl, zum anderen als Verlaufskurve aus. Wenn der Verlauf nach oben geht, können Sie die Website in die engere Auswahl aufnehmen. Geht es hingegen stetig bergab, ist es besser, von der Seite Abstand zu nehmen.

SearchMetrics: Ähnlich wie bei SISTRIX, gibt auch SearchMetrics einen Wert aus, der als SEO Visibility bezeichnet wird. Dieser liefert wie der Sichtbarkeitsindex einen guten Vergleichswert mit anderen Websites und bietet dadurch eine Grundlage für die Kategorisierung.

NEUE WEBSITES ZU FINDEN, IST MANCHMAL GAR NICHT SO EINFACH. MIT NEUEN DENKANSÄTZEN UND DER NUTZUNG VON TOOLS KÖNNEN SIE SICH ALLERDINGS IMMER INSPIRATIONSQUELLEN SUCHEN.

Patricia Unfried, Content Marketing Manager, eology GmbH, | www.eology.de

Moz: Bei Moz können Sie vor allem zwei Werte nutzen – nämlich die Domain Authority (kurz DA) und den Spam-Score. Beide

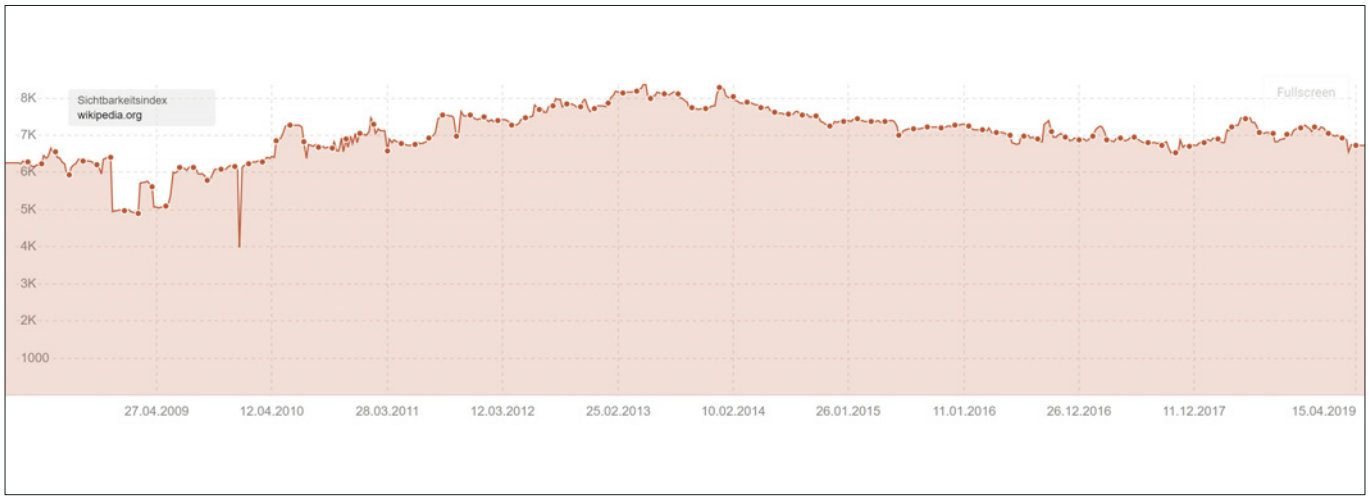


Bild 5: Sichtbarkeitsindex SISTRIX, Beispiel wikipedia.org.

Werte liefern Ihnen eine Einschätzung über die Vertrauenswürdigkeit einer Seite. Liegt ein hoher Spam-Score vor (dieser Wert wird in Prozent angegeben), nehmen Sie davon Abstand. Die Domain Authority (wird in einer Zahl von 1-100 angegeben) ist der Ranking-Score von Moz und liefert Aufschluss über die Qualität einer Seite. Je höher der Wert, desto besser bewertet Moz die Seite.

SimilarWeb: Wenn Sie sich für den Traffic einer Website interessieren und nicht nur wissen möchten, wie oft eine Seite aufgerufen wird, sondern sich im internationalen Umfeld bewegen, können Sie mit SimilarWeb die Geodaten ermitteln. Dadurch sehen Sie auf einen Blick, aus welchem Land eine Website die meisten Zugriffe hat.

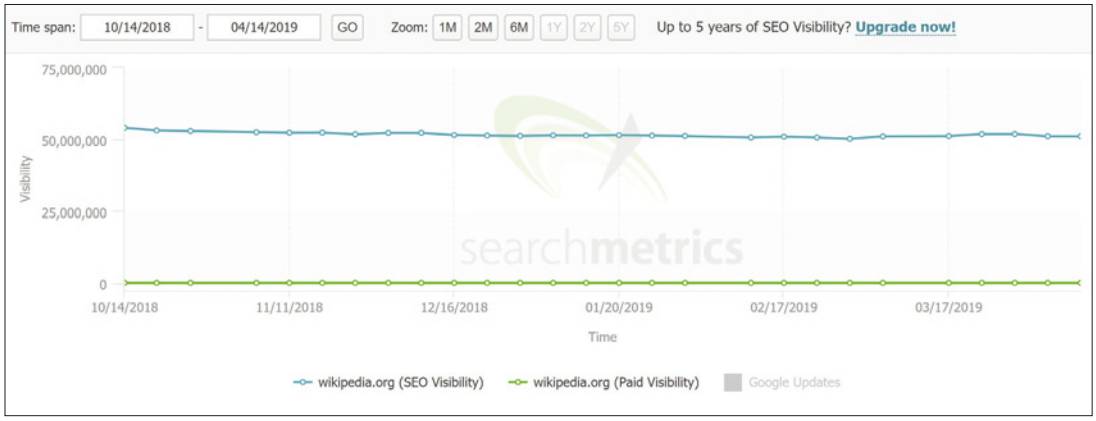


Bild 6:
SEO Visibility
searchmetrics,
Beispiel wikipedia.org.

Fazit

Neue Websites zu finden, ist manchmal gar nicht so einfach. Je nach Themengebiet und eigenen Vorstellungen kann eine Recherche mehrere Stunden in Anspruch nehmen, bis brauchbare Ergebnisse vorliegen. Mit neuen Denkansätzen und der Nutzung von Tools können Sie sich allerdings immer Inspirationsquellen suchen. Neben den hier vorgestellten Tools gibt es noch zahlreiche andere Anbieter und Möglichkeiten, um potenzielle Linkgeber zu finden. Man darf sich wie so oft nicht auf gewohnten Mustern ausruhen und muss bereit sein, neue Wege zu gehen.

Patricia Unfried

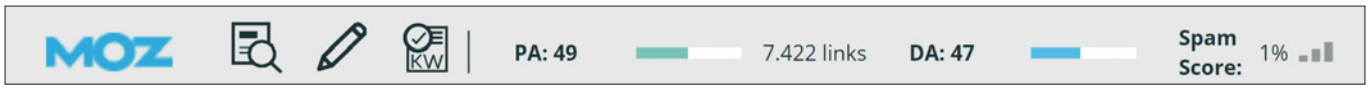


Bild 7: Moz Toolbar, Google Chrome Browser-Addon.

DIGITALE SPRACHASSISTENTEN

IMMER BELIEBTER.

Das Hamburger Marktforschungsinstitut Splendid Research hat im Januar 2019 im Rahmen einer repräsentativen Umfrage 1.006 Deutsche zwischen 18 und 69 Jahren online zur Nutzung digitaler Sprachassistenten und Smartspeaker befragt. Untersucht wurde, wofür digitale Sprachassistenten verwendet werden und welche Ablehnungsgründe bei Nicht-Nutzern bestehen. Daneben wurde das Kaufpotenzial für Smartspeaker ermittelt.

Alexa vor Siri

Sechs von zehn Bundesbürgern haben bereits einen digitalen Sprachassistenten genutzt. Dabei sind Amazons Alexa, der Google Assistant und Apples Siri die meist genutzten Tools. Vergleicht man die Nutzerbewertungen, stechen die jeweiligen Assistenten mit unterschiedlichen Stärken hervor: Für 81 Prozent der Nutzer hat Alexa eine angenehme Stimme. Der Google Assistant hat wiederum für drei Viertel der Nutzer eine Menge praktische Funktionen. Siri liegt bei allen Eigenschaften hinter den Assistenten von Amazon und Google. Nur für neun Prozent der Nutzer gehört Siri zur Familie (Alexa 33 Prozent). Fast jedem Fünften macht Siri gar manchmal Angst.

„Offenbar ersparen sich die Deutschen mit den intelligenten Lautsprechern wie Amazons Echo oder Google Home vor allem Mühe und Zeitaufwand beim Lesen", so Carina Krämer, Studienleiterin von Splendid Research. 53 Prozent der Nutzer verwenden den Smartspeaker, um das aktuelle Nachrichtengeschehen zu verfolgen. Mehr als die Hälfte der Nutzer streamen Musik und Hörspiele mit dem Gerät, gefolgt von Suchmaschinennutzung (51 Prozent) sowie Radio hören (50 Prozent).

Datenschutzbedenken als Hindernisgrund

Ungehobenes Potenzial besteht insbesondere bei Nicht-Nutzern mit Datenschutzbedenken: 35 Prozent der Nicht-Nutzer - und damit zehn Prozentpunkte mehr als noch 2017 – verwenden aufgrund von Datenschutzbedenken keinen Sprachassistenten.

Ferner sieht die Mehrheit der bisherigen Ablehner schlichtweg keine sinnvolle Verwendungsmöglichkeit für einen digitalen Sprachassistenten. „Insofern gilt es für Unternehmen entsprechende Anwendungen zu entwickeln", führt Krämer weiter aus.

Smartspeaker

Nach wie vor interessiert sich lediglich ein kleiner Teil der Bundesbürger für die Verwendung von Smartspeakern wie Amazon Echo, Google Home oder Apples HomePod. Zwar hat sich die Kaufwahrscheinlichkeit für Smartspeaker seit 2017 von zwei auf fünf Prozent mehr als verdoppelt, allerdings ist diese Gruppe immer noch viel zu klein im Vergleich zu den Nicht-Interessierten.

Die Preisbereitschaft für die Anschaffung von Smartspeakern liegt bei Interessierten bei durchschnittlich 115 Euro (+37 Euro im Vergleich zu 2017).

Amazons Echo hat bei Kaufinteressenten von Smartspeakern klar die höchste Präferenz: 69 Prozent können sich vorstellen, das Gerät zu kaufen, 28 Prozent ziehen Google Home in Betracht, Apples HomePod kommt hingegen nur für 16 Prozent infrage.

www.splendid-research.com

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
28. JUNI 2019.

BIMODALE IT

Traditionell versus modern?

SERVICE MESH

Mehrwert für die Cloud

BIG DATA

KI für APM: Hype oder Hot?

DIE NÄCHSTE AUSGABE ERSCHEINT AM 31. MAI 2019.

INSERENTENVERZEICHNIS

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren: Martin Besemann, Thomas Eimecke, Simon Federle, Markus Fensterer, Pierre Gronau, Jens Harms, Alexander Haugk, Dr. Patrick Hedfeld, Markus Kahmen, Christian Koch, Jürgen Kolb, Anton Kreuzer, Bernd Lohmeyer, Carina Mitzschke, Dr. Ulrich Müller, Björn Orth, Silvia Parthier, Ulrich Parthier, Prof. Dr. Dr. Gerd Rossa, Christine Schuhmacher, Nisanth Thangarajah, Prof. Dr. Bernd Ulmann, Patricia Unfried, André Vogt

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH,
Rudolf-Diesel-Ring 21, D-82054 Sauerlach
Tel: 08104-6494-0, Fax: 08104-6494-22
E-Mail für Leserbriefe: info@it-verlag.de
Homepage: www.it-daily.net

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

Manuskripteinsendungen:
Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift 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:
Rebecca Kömm

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 26
Preisliste gültig ab 1. Oktober 2018

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

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

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

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

Erscheinungsweise:
10x pro Jahr

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

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

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

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

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

Das E-3 Magazin

Information und Bildungsarbeit von und für die SAP-Community

Man kann versuchen, SAP®-Probleme durch Meditieren zu lösen. Einfacher ist es jedoch, das E-3 Magazin zu abonnieren. e-3.de/abo

e-3.de | e3zine.com

THOUGHT LEADERSHIP

DIE NEUE DIMENSION DES IT-WISSENS.

Jetzt neu auf www.it-daily.net

it-daily.net

itsecurity
MAI 2019

DAS SPEZIAL

SCHUTZ VON VIRTUALISIERTEN INFRASTRUKTUREN

FLUCH UND SEGEN NEUER TECHNOLOGIEN

Uwe Gries, Stormshield

RISK ADAPTIVE PROTECTION
THOUGHT LEADERSHIP

SCHWACHSTELLEN-MANAGEMENT

Unternehmens-IT – lieber lückenlos

RISIKO DROHNEN

Der Spion, der aus der Luft kam

APTs

Permanente Gefahr

www.it-daily.net

4

COVERSTORY

10

INHALT

SCHUTZ VON VIRTUALIS

FLUCH UND SEGEN NEUER TECHNOLOGIEN.

Die Einführung neuer Technologien wird von ITlern meist freudig begrüßt. Leider wird der Sicherheitsaspekt dabei oft vergessen. Über dieses Thema sprach Ulrich Parthier, Publisher it sexurity mit Uwe Gries, Country Manager bei Stormshield.
Ulrich Parthier: Die ersten Produkte für die Virtualisierung sind nunmehr rund 20 Jahre auf dem Markt. Man sollte meinen, sie seien ausgereift. Warum wird dem Security-Aspekt bei Innovationen immer zu wenig Aufmerksamkeit geschenkt?

Uwe Gries: Viele Anwender sind sich der Sicherheitsrisiken von virtualisierten Umgebungen erst gar nicht bewusst und meinen deshalb, sie seien auf der sicheren Seite. Hinzu kommt, dass sich die Lösungen häufig in der Cloud befinden. Der Anwender kann mit seinem Smartphone, Tablet oder PC von überall auf seine gespeicherten Daten zugreifen; trotzdem ist die Cloud für ihn nicht wirklich greifbar und somit „außer Reichweite". Oftmals steht einzig und allein der Nutzen und der Service von Cloud-Diensten im Vordergrund – der Sicherheitsaspekt wird vernachlässigt oder sogar gänzlich ignoriert.

Das machen sich Cyberkriminelle zunutze und verschaffen sich Zugang zu ganzen Cloud-Datenbanken. Ist das Tor zur Datenwolke einmal geöffnet, steht ihnen der Zugriff zu sämtlichen persönlichen Daten und vertraulichen Inhalten offen. Werden diese sensiblen Unternehmensinformationen entwendet oder für die kriminellen Machenschaften der Hacker missbraucht, kann ein solcher Angriff für ein Unternehmen schwerwiegende Folgen haben. Um solchen Szenarien geeignet zu begegnen, gilt es, bei der firmeninternen IT-Sicherheitsstrategie alle Bereiche mit einzubeziehen – sowohl On-Premises als auch virtualisierte Infrastrukturen.

? **Ulrich Parthier:** *Es gibt wenige Produkte auf dem Markt, die sich mit dem Thema Virtualisierung und IT-Sicherheit beschäftigen. Sehen Sie das ähnlich?*

Uwe Gries: Ja, da stimme ich Ihnen zu. Allerdings lässt sich seit geraumer Zeit ein Wandel des Marktes beobachten. Grund dafür ist sicherlich die enorme Zunahme von Cyberattacken. In den Medien hört man regelmäßig von neuen Hackerangriffen. Davon sind längst nicht mehr nur Großunternehmen betroffen, sondern auch immer öfter kleine und mittelständische Unternehmen. Diese Entwicklung führt den Unternehmen deutlich vor Augen, dass das Thema IT-Sicherheit unbedingt berücksichtigt und als ganzheitlicher Prozess betrachtet werden muss. Wird der Sicherheitsaspekt nur teilweise und lückenhaft umgesetzt, bedeutet dies letztlich, dass die firmeninterne IT-Infrastruktur nicht ausreichend geschützt ist.

? **Ulrich Parthier:** *Sie haben gerade Ihre neue Elastic Virtual Appliance-Lösung vorgestellt. Wo liegen die Vorteile für den Anwender?*

Uwe Gries: Die Lösungen von Stormshield – so auch die Elastic Virtual Appliances – sind hochskalierbar. Dabei passen sich die Leistungsniveaus der EVA-Lösungen automatisch an die vRAM- und vCPU-Kapazitäten an, die dem Hypervisor zugewiesen sind. Mit dieser automatischen Anpassung an die zugewiesenen Ressourcen ist ein optimaler Rollout gewährleistet. Das Sicherheitsmodul lässt sich zudem einfach in den Aufbau eines neuen virtualisierten Service integrieren und an zukünftige Entwicklungen der Cloud-Infrastruktur des Unternehmens anpassen.

? **Ulrich Parthier:** *Das neue Produkt sorgt auch für eine sichere Unterstützung bei der Bereitstellung von Cloud-Services. Womit wir wieder beim Ausgangspunkt wären: neue Technologien, neue Angriffsvektoren.*

Uwe Gries: Heutzutage verlagern Unternehmen ihre Daten sowie die auf herkömmlicher Infrastruktur gehosteten Dienste zunehmend in öffentliche oder private Cloud-Plattformen. Mit der Stormshield Elastic Virtual Appliance reagieren wir auf den zunehmenden Virtualisierungstrend der IT-Infrastrukturen. Die Lösung schützt virtuelle Umgebungen proaktiv vor internen und externen Bedrohungen.

? **Ulrich Parthier:** *Viele Unternehmen hosten Anwendungen oder Daten mittlerweile bei AWS oder Azure. Können Sie auch hier den Schutz von virtuellen Servern und virtuellen Netzwerken garantieren?*

Uwe Gries: Die Appliance unterstützt diverse Umgebungen wie zum Beispiel Citrix, VMware, KVM und Hyper-V. IT-Abteilungen sind damit in der Lage, die Wahl ihrer Infrastruktur flexibel zu gestalten. So besteht die Möglichkeit, die Cloud-Plattformen wie etwa Amazon Web Services oder Microsoft Azure zu wechseln und die Sicherheitslösung gleichzeitig mit den Services zu migrieren.

? **Ulrich Parthier:** *Die Integration in die bestehende IT-Infrastruktur ist immer ein Diskussionsthema in den Unternehmen. Wie haben Sie es bei Ihrer neuen Appliance gelöst?*

Uwe Gries: Unsere neuen virtuellen Appliances fügen sich nahtlos in die IT-Infrastruktur ein. Sie lassen sich mit dem bisherigen aktuellen Stormshield Management Center genauso verwalten wie eine herkömmliche physische Appliance. Der Systemadministrator benötigt dafür keine intensive Einweisung oder zusätzliche Ausbildung. Das Management der IT-Infrastruktur bleibt weiterhin zentral und transparent.

? **Ulrich Parthier:** *Gibt es Zertifizierungen für das neue System?*

Uwe Gries: Die Elastic Virtual Appliance wurde, wie die anderen Stormshield-Lösungen, nach den Vorgaben der ANSSI EAL4+ zertifiziert.

IERTEN INFRASTRUKTUREN

LÄNGST SIND NICHT NUR GROSSUNTERNEHMEN VON HACKERANGRIFFEN BETROFFEN, SONDERN AUCH IMMER ÖFTER KMU. DIESE ENTWICKLUNG FÜHRT DEN UNTERNEHMEN DEUTLICH VOR AUGEN, DASS DAS THEMA IT-SICHERHEIT UNBEDINGT BERÜCKSICHTIGT UND ALS GANZHEITLICHER PROZESS BETRACHTET WERDEN MUSS.

Uwe Gries, Country Manager, Stormshield, www.stormshield.dee

Ulrich Parthier: *Reden wir übers Geld. Sie versprechen Kostenreduktionen beim Einsatz Ihrer Lösung. Wie stellt sich das Szenario betriebswirtschaftlich dar?*

Uwe Gries: Die zunehmende Nutzung der Cloud führt zu Änderungen der IT-Budgets sowie der Investitionskosten, die zu Betriebskosten werden. Im Wesentlichen arbeiten neue Cloud-Praktiken mit elastischen Angeboten, die an die Menge der Ressourcen gebunden sind. Deshalb besteht die neue Herausforderung für IT-Abteilungen darin, Betriebskosten durch eine bessere Verwaltung dieser Ressourcen zu optimieren, das heißt virtuelle CPU und RAM oder das Speichervolumen. Mit der Stormshield Elastic Virtual Appliance lassen sich Änderungen an zugewiesenen Ressourcen je nach Anforderung und dem erforderlichen Leistungsniveau sehr schnell und einfach vornehmen, um einen angemessenen Verbrauch von Cloud-Ressourcen sicherzustellen.

Ulrich Parthier: *Sie bieten einen kostenlosen Test auf der Microsoft Azure-Plattform. Dort wird die Lösung innerhalb von fünf Minuten bereitgestellt, und Anwender können ihre Umgebung dann mit einer virtuellen Appliance, einem Honeypot-Server oder einem Angriffsclient testen. Dazu gibt es eine Dokumentation, wie man die Konfiguration einfach einrichten und die Sicherheitsrichtlinien im virtuellen Netzwerk verwalten kann. Klingt gut. Wird der Service in Anspruch genommen, oder fordern die Anwender ein ausführlicheres Testszenario?*

Uwe Gries: Wir haben die Erfahrung gemacht, dass dieser Service gerne und häufig in Anspruch genommen wird. Der Anwender kann sich mit dem Test schnell und einfach einen ersten Überblick verschaffen. In der Regel wird das Tool von erfahrenen IT-Spezialisten genutzt. Selbstverständlich stehen wir auch persönlich zur Verfügung, um die Fragen der Nutzer zu beantworten und komplexe Szenarien zu diskutieren.

Ulrich Parthier: *Letzte Frage. Gibt es spezielle Branchen, die besonders im Fokus der Cyberkriminellen stehen, und was raten Sie Anwendern, die virtualisierte Infrastrukturen im Einsatz haben?*

Uwe Gries: Industrieunternehmen oder Betreiber kritischer Infrastrukturen wie zum Beispiel Energieversorger oder Krankenhäuser sind für Angreifer besonders attraktiv, da sie hier höchstvertrauliche Betriebsgeheimnisse abgreifen und damit auf dem Schwarzmarkt horrende Summen erzielen können. Grundsätzlich sind aber alle Branchen und Unternehmen jeder Größenordnung von den Attacken der Hacker betroffen – niemand ist davor gefeit. Nahezu jedes Unternehmen arbeitet mit virtualisierten Infrastrukturen, was vielen Verantwortlichen aber oft gar nicht bewusst ist. Eine ganzheitliche IT-Sicherheitsstrategie ist daher unerlässlich, um Cyberkriminellen keine Angriffsfläche zu bieten und alle Bereiche im Unternehmen vollumfassend zu schützen.

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

THANK YOU


Remote Admin
Malware
Identity Theft
Phishing
Hacker
Password
Backdoors
Crime
Virus Computer
Firewall
Spam
Botnet
Social Network
E-Commerce
Worms
Internet Scam
Username
Skimming
RISK ADAPTIVE PROTECTION
THOUGHT LEADERSHIP

THREAT INTELLIGENCE: ALLES ODER NICHTS?

VON THREAT INTELLIGENCE ZU RISK ADAPTIVE PROTECTION.

Als der Begriff vor einigen Jahren erstmals auftauchte, markierte er so etwas wie den Wendepunkte im IT-Sicherheitsdenken. Weg von der Reaktion hin zu proaktiven Denken und Handeln. Start ups entstanden und schnell merkten die großen Player, das dort ein Hype entstehen könnte, den man auch bespielen müsste.

So kam es aus Marketinggründen schnell zu einer Verwässerung des Begriffs. Inzwischen ist die Begriffbezeichnung eher banal, denn wenn Threat Intelligence als aufbereitete und in den Kontext gesetzte Informationen über Bedrohungen für die Informationssicherheit bezeichnet wird, ist das alles wie auch nichts.

So listet der eSecurity Planet beispielsweise 10 Hersteller auf, die auch genauso gut beim Thema SIEM stehen könnten:

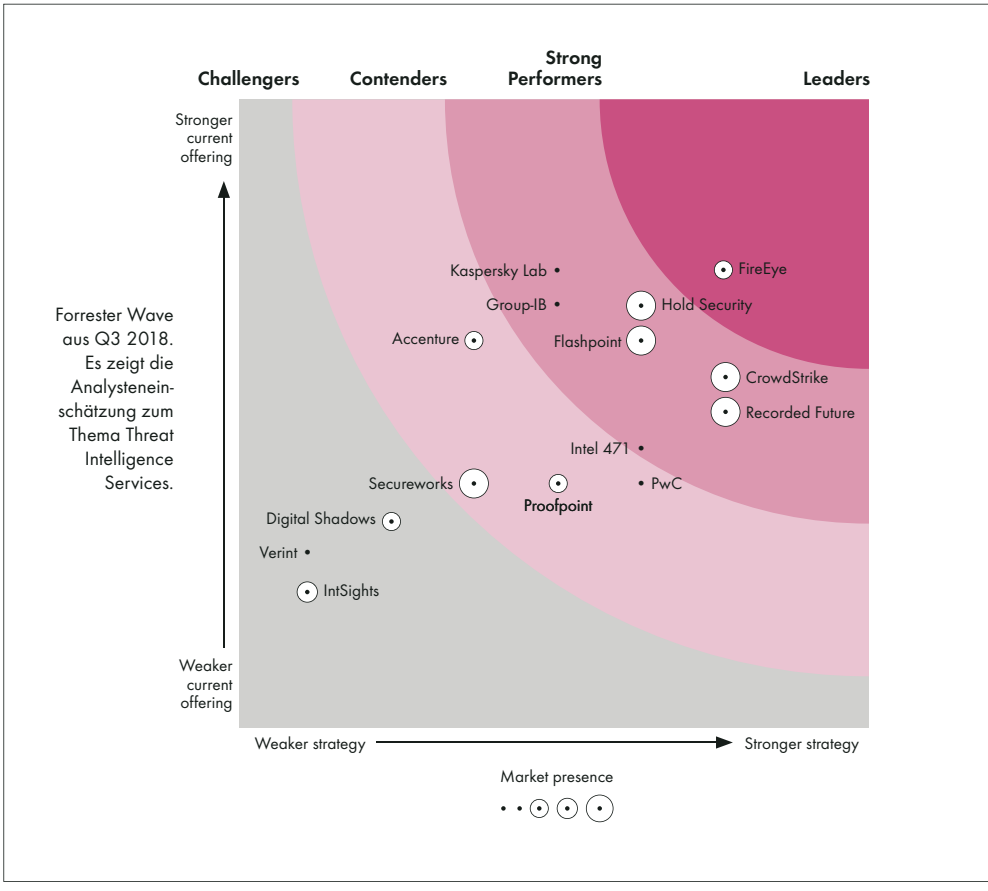
- IBM X-Force Exchange
- Anomali ThreatStream
- Palo Alto Networks AutoFocus
- RSA NetWitness Suite
- LogRhythm Threat Lifecycle Management (TLM) Platform
- FireEye iSIGHT Threat Intelligence
- LookingGlass Cyber Solutions
- AlienVault Unified Security Management (USM)

Andere Beispiele wären eset oder Kaspersky, typische AV-Anbieter, die ihr Wissen nun, na sagen wir mal, „veredeln". Die Liste könnte man noch beliebig fortsetzen und mit anderen Begriffen variieren.

Rufen wir uns noch mal kurz den Ursprung der Threat Intelligence-Welle ins Gedächtnis: Das waren komplexe und zielgerichtete Angriffe, die meist von staatlichen Hacker-Gruppen begangen wurden und werden, die sogenannten Advanced Persistent Threats (APT). Sie sind schwer zu erkennen und abzuwehren. Threat Intelligence sollte hier das Allheilmittel sein. War es natürlich nicht. Bestenfalls leidensmindernd. Nach den Produkten kamen die Services und Provider: Services konnte und kann man gut im Abo verkaufen, für Hersteller ein kontinuierlicher Revenue Stream.

Beispiele für Threat Intelligence Provider wären: Crowdstrike, Proofpoint, Team Cymru, Recorded Future, Clearsky, BAE Systems, Fox IT, Symantec, eset und Kaspersky. Die große Frage aber ist: Wo geht die Reise hin? Ich denke, der nächste große Schritt muss durch KI kommen und mehr in Richtung proaktives Handeln gehen. Und da bietet Forcepoint mit seinen X-Labs einen möglichen, richtungsweisenden Ansatz. Mehr dazu im Interview auf den kommenden Seiten.

Ulrich Parthier
Publisher – Analyst - Influencer



CYBERSECURITY @WORK

X-LABS: FORSCHUNGSLABOR FÜR VERHALTENSBASIERTE CYBERSECURITY ETABLIERT.

In Zeiten ständig wachsender Sicherheitsrisiken gilt es neue Wege zu gehen. Darüber sprach Ulrich Parthier, Herausgeber it security, mit Nicolas Fischbach, CTO bei Forcepoint.

Ulrich Parthier: *Der Kampf Angreifer versus Verteidiger geht in der Kategorie Cybersecurity in eine neue Runde. Forcepoint hat die X-Labs gegründet. Was steckt hinter diesen Labs?*

Nicolas Fischbach: Mit X-Labs hat Forcepoint eine weltweit einzigartige Forschungseinrichtung und globales Kompetenzzentrum für IT-Sicherheit und Verhaltenswissenschaft gegründet. Dort arbeiten Sicherheitsforscher, Datenwissenschaftler, Psychologen und Spionageabwehrspezialisten zum ersten Mal zusammen, um verhaltensbasierte Sicherheitslösungen rund um den Faktor Mensch und Maschine zu entwickeln.

Dabei nutzen die X-Labs-Spezialisten Daten und Erkenntnisse aus dem Forcepoint-Produktportfolio sowie Informationen und Feeds von Drittanbietern.

Ulrich Parthier: *Thought Leadership verlangt nach neuen Denk- und Lösungsansätzen. Wie sieht ihre Ausprägung aus?*

Nicolas Fischbach: Nicht die Infrastruktur, sondern der Mitarbeiter ist die Konstante in einer sich ständig wandelnden Bedrohungslandschaft. Wichtige Fragen, die sich Sicherheitsexperten zum Beispiel stellen müssen, sind: Wie interagieren Mensch und Maschine mit Daten? Wann, wo und warum wird auf Daten zugegriffen? Wie werden diese verarbeitet oder analysiert? Wir entwickeln daher Cybersecurity-Lösungen mit klassischer Threat Intelligence und neuen, patentierten Behaviour-Analytics.

Ulrich Parthier: *Wie würden Sie das Ziel definieren?*

Nicolas Fischbach: Das Ziel der X-Labs ist es, digitale Identitäten und deren Cyberverhalten besser zu verstehen, insbesondere dann, wenn sie mit sensiblen Daten und geistigem Eigentum interagieren. Unsere Forschung liefert Einblicke in das Verhalten von Mensch und Maschine. Verbunden mit einem Privacy-by-Design-Ansatz für einen umfassenden Schutz der Privatsphäre wurden diese Erkenntnisse noch nie zuvor in Sicherheitsprodukte integriert. Unsere Innovationen im Bereich Risk Adaptive Protection prüfen Risiken kontinuierlich, passen das Sicherheitslevel individuell an und verhindern dadurch, dass sensible Daten abfließen.

Ulrich Parthier: *Die X-Labs setzen also auf einen neuen Sicherheitsansatz?*

Nicolas Fischbach: Unternehmen und Behörden sind Millionen von Sicherheitsereignissen ausgesetzt. Sie sind nahezu

gezwungen Schwarz-Weiß-Entscheidungen zu treffen: zulassen oder blockieren. Das gefährdet die Produktivität. Menschen und Maschinen, sogenannte „Entities" in einem Netzwerk, stellen vielmehr ein dynamisches Risiko für Unternehmen dar, das sich innerhalb Sekunden verändern kann. Unsere X-Labs-Spezialisten nutzen daher das Adaptive Trust Profile (ATP).

Ulrich Parthier: *Was genau verbirgt sich hinter dem Begriff Adaptive Trust Profile (ATP)?*

Nicolas Fischbach: Das ATP ist eine Sammlung von Eigenschaften, Mustern und Schlussfolgerungen einzelner Entities. Es arbeitet mit Forcepoints Analytik-Algorithmen, die Daten von Sensoren sammeln: seien es Cloud-, Endpoint-, Drittanbieteranwendungen oder Services (einschließlich SaaS-Applikationen). KI-Modelle innerhalb des ATP setzen die Ereignisse in Kontext und berechnen einen Risikowert für jede Einheit auf Basis eines umfangreichen Verhaltenskatalogs. Greift ein bestimmter Account etwa von einem anderen Ort als üblich auf Daten zu, oder möchte er Daten nutzen,

die nicht in seinen Aufgabenbereich fallen, wird ein erhöhtes Risiko festgestellt und es kann entsprechend gehandelt werden.

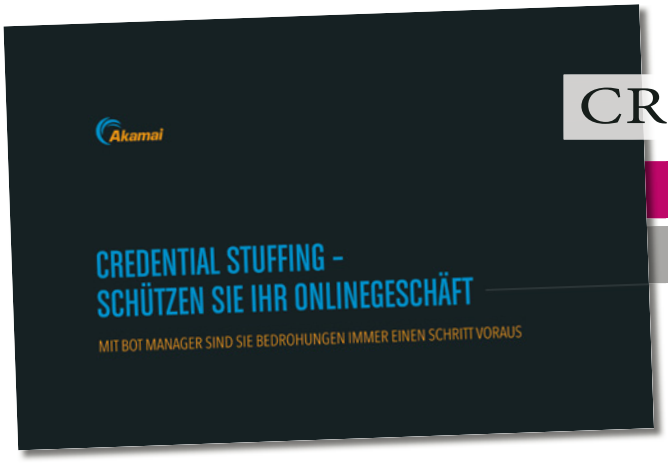
? **Ulrich Parthier:** *Ändert sich damit auch das Profil und die Arbeitsweise der Security-Experten?*

Nicolas Fischbach: Sicher. Die Security-Experten können sich voll und ganz auf relevante, auffällige Entities und Aktivitäten konzentrieren – ohne Rückstau von Warnmeldungen wie bei herkömmlichen Sicherheitstools. Gleichzeitig minimieren CISOs und CIOs so klassische Security-Reibungspunkte, was unterbesetzte Sicherheitsteams entlastet. Darüber hinaus lässt sich die Zeit, die benötigt wird, um Risiken zu erkennen. stark reduzieren. Wir bewegen uns also weg von reaktiven Ja- und Nein-Sicherheitsentscheidungen hin zu dynamisch bewerteten, risikobasierten Entscheidungen. Ein Security-Ansatz, zu dem die meisten CISOs heute übergehen.

? **Ulrich Parthier:** *Sie haben weltweit verteilte Teams. Wie gelingt der Know-how Transfer in künftige Produkte?*

Nicolas Fischbach: Die Spezialisten von X-Labs sind weltweit verteilt, darunter Teams mit Sitz in Austin, Baltimore, San Diego, Cork, Dublin, Reading und Helsinki. Künftig fließen die Erkenntnisse der X-Labs auch in die neue Cloud-basierte Forcepoint Converged Security Platform mit ein, um Risk Adaptive Protection auf die gesamte On-Premise- und Cloud-Infrastruktur eines Unternehmens auszuweiten.

! **Ulrich Parthier:** *Herr Fischbach, vielen Dank für das Gespräch.*



CREDENTIAL STUFFING

SCHÜTZEN SIE IHR ONLINE GESCHÄFT

Credential Stuffing ist auf dem Vormarsch. Es beginnt damit, dass ein Angreifer versucht, gestohlene Nutzerinformationen zur Anmeldung auf Ihrer Website zu verwenden. Sobald eine Reihe erfolgreicher Anmeldungen bestätigt wurde, verkauft der Angreifer die Liste entweder an andere Betrüger oder führt die Kontoübernahme direkt durch – und erleichtert dabei Onlinekonten um alle Assets, die irgendwie Geld einbringen können.

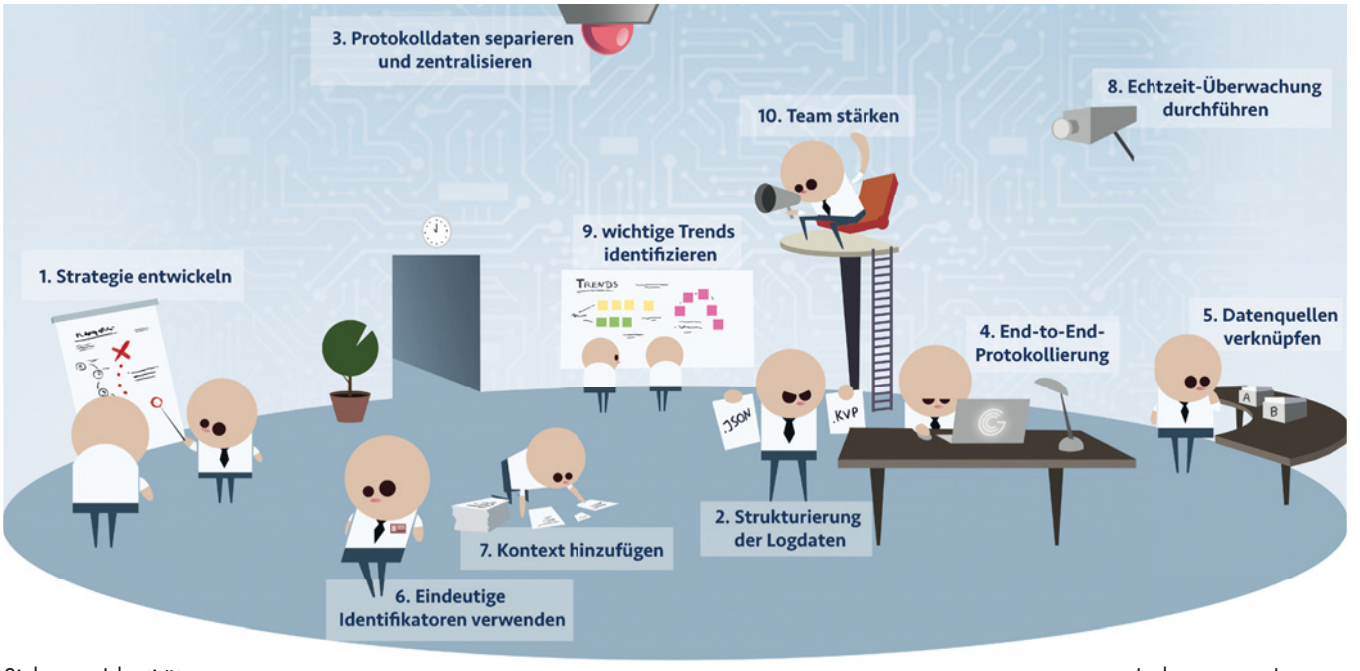
Im Gegensatz zu Angriffen auf Webanwendungen, wie zum Beispiel SQL Injection, weisen Anmeldeanfragen, die aus Credential Stuffing entstehen, keine besonderen Muster auf, die sich leicht erkennen und blockieren lassen. Verifizierte Anmeldedaten führen zu gültigen Anfragen: Die Anmeldeinformationen sind legitim, selbst wenn die sich anmeldende Person kriminell ist. So sind entsprechende Anfragen nahezu unmöglich zu erkennen.

Glücklicherweise erfolgen die Verifizierung gestohlener Anmeldedaten und Credential Stuffing meist nicht manuell. Und genau hier haben Sie die Möglichkeit, einzuschreiten. Die Validierung erfolgt für gewöhnlich automatisiert, sodass es sich bei Credential Stuffing eigentlich um ein Bot-Problem handelt.

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

AUS PROTOKOLLDATEN

DER SCHLÜSSEL ZUR ABSICHERUNG VON IT-STRUKTUREN.



© Illustration: Lukas Liebhold | Gronau IT Cloud Computing

Sichere Identitäten bilden die Voraussetzung für weitere Schutzmaßnahmen, die Unternehmen in puncto Datensicherheit ergreifen sollten, um sich compliant und wettbewerbsfähig aufzustellen.

Mit der Einführung eines Sicherheitsprozesses leiten IT-Verantwortliche notwendige organisatorische Veränderungen ein, definieren eine Strategie und nutzen Hilfsmittel zur Erreichung ihrer Schutzziele.

Logmanagement priorisieren

Logmanagement ist ein wesentlicher Bestandteil des Managementsystems für Informationssicherheit. Die Sicherstellung der Authentizität jedes Nutzers von ITK-Systemen genießt daher oberste Priorität. Wenn es zu Unregelmäßigkeiten oder offensichtlich missbräuchlicher Nutzung von Programmen und Applikationen kommt, müssen Administratoren detailliert nachverfolgen können, wer, wann, wo zugegriffen und welche Änderungen vorgenommen hat. Dies setzt voraus, dass Anwendungen entsprechend detaillierte, möglichst allgemein verständliche Logmeldungen erzeugen, diese speichern und sie auch über längere Zeitfenster unveränderbar zentral vorhalten. Im Sinne einer in der IT üblichen Log-Zentralisierung erweisen sich Funktionen zur direkten, zugriffgeschützten Speicherung der Protokolldaten auf einem zumindest logisch abgesicherten Logmanagement-Server als sinnvoll. Dazu gehört auch die Alarmierung der IT-Sicherheit, falls mit einem Benutzerkonto mehrfach innerhalb kurzer Zeit an diversen Geräten erfolglose Zugriffsversuche unternommen werden. In diesem Zusammenhang sollten Entscheider eine skalierbare Lösung wählen, da zum einen wirklich umfangreiche Datensammlungen entstehen können und Angreifer zum anderen mit DDoS-Attacken bewusst die Grenzen solcher Systeme ausloten, um unprotokollierten Schabernack zu treiben.

Security-Dreiklang

Die Notwendigkeit von Logmanagement ergibt sich aus dem Dreiklang aus gesetzlichen Auflagen, notwendiger Analyse von Sicherheitsvorfällen und kontinuierlichen Analyseprozessen. Dabei folgt effizientes Logmanagement stets diesem Prozess: Annahme ➤ Verarbeitung ➤ Auswertung ➤ Visualisierung

Jeder am Logmanagement Beteiligte sollte verstehen, dass sich hinter dem Begriff ein Prozess und kein Produkt verbirgt. Dementsprechend liegt im internen Aufbau von Logging-Know-how, der wahre Benefit. Dazu gehören zwangsläufig der Aufbau von Strukturen, die Definition aller personenbezogenen Daten, eine sinnhafte Archivierung der Protokolle sowie eine übergreifende Konzernbetriebsvereinbarung (KBV).

Vom Log- zum Protokollmanagement

Mit der raschen Entstehung und Dominanz von Cloud-basierten Systemen erleben wir ein explosionsartiges Wachstum maschinell generierter Protokolldaten. Infolgedessen ist das Protokollmanagement zu einem Grundpfeiler eines modernen IT-Betriebes geworden und unterstützt eine Reihe von Anwendungsfällen wie Debugging, Produktionsüberwachung, oder Support.

Während verteilte Systeme eine hohe Effizienz in Bezug auf die Skalierbarkeit bieten, stellen sie Teams, die sich auf Protokolldaten beziehen, vor Herausforderungen: Wo sollen sie anfangen und welchen Aufwand benötigen sie, um die benötigten

LERNEN

Protokolldateien zu finden? IT-Administratoren, DevOps-Profis und Mitarbeiter, die den protokollerstellenden Systemen am nächsten stehen, haben die Aufgabe, dezentrale Protokolldateien unter Einhaltung von Sicherheits- und Compliance-Protokollen zu verwalten. Entwickler und Ingenieure, die Probleme auf Anwendungsebene beheben müssen, könnten sich durch den Zugriff auf Protokolldateien auf Produktionsniveau eingeschränkt fühlen. Betriebs-, Entwicklungs-, Datenwissenschaftler- und Support-Teams, die Einblicke in das Benutzerverhalten für Trendanalysen und Fehlerbehebungen benötigen, fehlt oft das technische Fachwissen, das erforderlich ist, um Protokolldaten effizient zu nutzen. Angesichts dieser Herausforderungen ist es wichtig, bei der Implementierung einer Protokollierungslösung Best Practices zu berücksichtigen:

1. Festlegung der Strategie

Protokollierung muss eine Strategie verfolgen. Schon bei der Strukturierung des DevOps-Aufbaus und der Veröffentlichung jeder neuen Funktion achten IT-Administratoren im Idealfall darauf, dass sie einen organisierten Protokollierungsplan beifügen. Dieser Plan sollte auch Hinweise beinhalten, ob personenbezogene Daten und Archivierungsanforderungen vorliegen.

2. Strukturierung der Logdaten

Das Protokoll-Format muss berücksichtigt werden. Wer effektive Protokollierungsformate nicht versteht, kann aus den hinterlegten Informationen keine Erkenntnisse gewinnen. Lesbare Protokolle erleichtern Fehlerbehebungen.

3. Protokolldaten separieren und zentralisieren

Protokolle sollten immer automatisch gesammelt und an einen zentralen Ort geschickt werden. Dies erleichtert die organisierte Verwaltung und erweitert die Analysefunktionen, sodass Verantwortliche Cross-Analysen effizient durchführen und Korrelationen zwischen verschiedenen Datenquellen identifizieren können.

4. Anwendung von End-to-End-Protokollierung

Systemadministratoren sollten alle Systemkomponenten überwachen und protokollieren. Dazu gehören auch Windows-Sicherheitsprotokolle, relevante Metriken und Ereignisse aus der zugrunde liegenden Infrastruktur, den Anwendungsschichten und den Endbenutzer-Arbeitsplätzen.

5. Datenquellen verknüpfen

End-to-End-Protokollierung an einem zentralen Ort ermöglicht es Verantwortlichen, Datenströme aus diversen Quellen dynamisch zu aggregieren, um die wichtigsten Trends und Kennzahlen in Beziehung zueinander zu setzen.

> KLAR IST: SOBALD ES EINEM ANGREIFER GELINGT, SICH UNBERECHTIGT EINER IDENTITÄT ZU BEMÄCHTIGEN, LAUFEN ALLE DARAUF AUFBAUENDEN MASSNAHMEN INS LEERE.
>
> Pierre Gronau, Geschäftsführer, Gronau IT Cloud Computing www.gronau-it-cloud-computing.de

Die Korrelation von Daten unterstützt dabei, Ereignisse, die Systemstörungen verursachen, schnell und sicher zu identifizieren.

6. Eindeutige Identifikatoren verwenden

Eindeutige Identifikatoren erlauben es, komplette Benutzersitzungen und Aktionen einzelner Benutzer genau zu verfolgen. Wenn IT-Mitarbeiter die eindeutige ID eines Benutzers kennen, können sie die Suche nach allen Aktionen filtern, die dieser Benutzer in einem bestimmten Zeitraum durchgeführt hat. Hier ist jedoch dem Datenschutz gemäß EU-DSGVO und der Betriebsvereinbarung Vorrang einzuräumen.

7. Kontext hinzufügen

Sobald Protokolle als Daten verwendet werden, ist es wichtig, den Kontext jedes Datenpunkts zu berücksichtigen. Zu wissen, dass ein Mitarbeiter auf eine Schaltfläche geklickt hat, ist möglicherweise nicht so nützlich, wie zu wissen, dass er beispielsweise gezielt auf die Schaltfläche „Verbrauchsmaterial bestellen" geklickt hat.

8. Echtzeit-Überwachung durchführen

Eine „Live-Tail"-Sicht auf Protokolldaten kann Entwickler und Administratoren befähigen, Protokollereignisse nahezu in Echtzeit zu analysieren, wenn Anwender mit ihren Anwendungen oder Systemen interagieren. Die Live-Tail-Suche und Berichterstattung ermöglicht es zudem den Support-Teams, Kundenprobleme zu untersuchen und zu lösen, sobald sie auftreten.

9. Protokolle nutzen, um Trends zu identifizieren

Die Behandlung von Protokollereignissen als Daten schafft die Möglichkeit, statistische Analysen, zukünftig auch mit KI auf Benutzerereignisse und Systemaktivitäten anzuwenden. Diese Einblicke öffnen die Tür zu fundierten Geschäftsentscheidungen auf der Grundlage von Daten, die außerhalb der Protokolle oft nicht verfügbar sind.

10. Teamprofit

Ein Protokollverwaltungs- und Analysedienst, der nur einem hochtechnisierten Team zugänglich ist, schränkt die Möglichkeiten des Unternehmens, von Protokolldaten zu profitieren, erheblich ein. Die Werkzeuge sollten Entwicklern Live-Tail-Debugging, Administratoren Echtzeitalarmierung, Datenwissenschaftlern aggregierte Datenvisualisierungen und Support-Teams Live-Such- und Filterfunktionen bieten.

Pierre Gronau

UNTERNEHMENS-IT: LIEBER LÜCKENLOS

AUTOMATISIERTES SCHWACHSTELLENMANAGEMENT.

Die Hacker-Angriffe der letzten Zeit haben es einmal mehr eindrucksvoll demonstriert: Die IT eines Unternehmens ist ständigen Attacken ausgesetzt. Darunter ist Vielen sicherlich die WannaCry-Attacke noch prägend in Erinnerung – der bislang größte Angriff durch Ransomware, der im Mai 2017 zahlreiche Unternehmen lahmlegte und damit prominent in der Berichterstattung der Medien erschien. Er befiel damals Windows-Betriebssysteme und verschlüsselte sofort bestimmte Nutzerdaten, die sich nur gegen Zahlung eines Lösegelds in der Kryptowährung Bitcoin wiederherstellen ließen. Erfolgte diese Zahlung nicht in einer vorgegebenen Zeit, waren die Daten verloren – eine klassische Erpressung. Darüber hinaus versuchte der WannaCry-Wurm auch weitere Windows-Systeme zu infizieren und beispielsweise die Backdoor „DoublePulsar" zu installieren.

Einfallstor Schwachstellen

Doch warum war der WannaCry-Angriff überhaupt so erfolgreich? Wie so oft nutzten die Cyberkriminellen im Betriebssystem bereits vorhandene Schwachstellen. Sicherheitslücken sind tatsächlich recht normal – Software-Codes sind meist viel zu komplex, um wirklich alle Eventualitäten bis ins Letzte durchzutesten. Meist bleiben sie längere Zeit auch unentdeckt. Erst bei Identifizierung werden sie plötzlich zum großen Risiko.

Um solche Schwachstellen auszunutzen, braucht es dabei zumeist keine genialen Informatiker mit Detail-Kenntnissen des Betriebssystems. Ein Angriff ist mit einfachsten Mitteln möglich. Im Internet kursieren Exploits zu unzähligen Schwachstellen. Firewalls und Virenscanner bieten dagegen keinen zuverlässigen Schutz. Im Fall von WannaCry zum Beispiel konnte sich die Attacke deshalb so schnell ausbreiten, weil viele Systeme der betroffenen Unternehmen nicht auf dem neuesten Stand waren – es fehlten Updates. Befallen wurden daher ausschließlich ältere Windows-Betriebssystemversionen, die nicht über die neuesten Patches verfügten.

Basisbausteine für mehr IT-Sicherheit

Auf den ersten Blick scheinen fehlende Updates ein leicht zu behebender Fehler – dabei geht es schließlich um bekannte Sicherheitslücken. Wo liegt also der Grund, dass viele Systemadministratoren anscheinend nicht vorbereitet waren? Warum waren so viele Betriebssysteme nicht auf dem neuesten Stand? Der Grund ist einfach: Die eigenen Mittel der Administratoren bei der Schwachstellenbekämpfung sind vor allem zeitlich begrenzt. Denn um Sicherheitslücken zuverlässig aufzuspüren, müssen nicht nur Betriebssystem und Anwendungen beständig gepatcht werden, Administratoren müssen sich außerdem in regelmäßigen Abständen über neu veröffentlichte Lücken und Patches informieren.

Für typische IT-Teams mit klar begrenzten Ressourcen ist das in der Regel nicht leistbar. Unternehmen müssten dafür eigene Schwachstellen-Teams einrichten, die zusätzliche Kosten verursachen.

Gefahr nicht nur für das eigene Unternehmen

Ohne geeignete Hilfsmittel ist dieser Prozess in der Praxis bei der hohen und ständig wachsenden Anzahl der Sicherheitslücken manuell nicht mehr zu bewerkstelligen. Konzentrieren sich Administratoren etwa auf die ihrer Meinung nach gefährlichsten Angriffsvektoren, nutzen Cyberkriminelle für ihre nächste Malware-Attacke vielleicht schon längst eine bisher als nicht so gefährlich eingestufte, untergeordnete Schwachstelle aus. Mittlerweile bestehen die Konsequenzen eines erfolgreichen Angriffs nicht mehr alleine darin, dass der Betriebsablauf im eigenen Unternehmen gestört wird. Gelangen über so einen Angriff vertrauliche Daten an die Öffentlichkeit, können auf Unternehmen zum Beispiel nach der seit letztem Jahr in Kraft getretenen DSGVO auch empfindliche Strafzahlungen zukommen, wenn keine geeigneten Maßnahmen zum Schutz personenbezogener Daten nachgewiesen werden können. Dies gilt auch, wenn gekaperte Rechner in einem Botnet zusammengeschaltet werden und über dieses weitere Cyberangriffe gegen Dritte durchführen.

Automatisierung ist der Schlüssel

Eine wirkliche Abhilfe schafft hier nur ein automatisiertes Schwachstellenmanagement, – ein Schwachstellenscanner überprüft periodisch und automatisch sämtliche PCs und Server eines Unternehmens auf Schwachstellen oder unsichere Konfigurationen. Jedes Gerät wird dabei anhand kontinuierlich aktualisierter Datenbanken renommierter Sicherheitsorganisationen mit mehr als 20.000 hinterlegten Einträgen auf Risiken abgeglichen – eine Arbeit, die kein Systemadministrator manuell leisten könnte. Gleichzeitig können Unternehmen die Konfiguration ihrer Geräte mittels eines vorbereiteten und den eigenen Anforderungen anpassbaren Regelsatzes jederzeit überprüfen – einfach und schnell kontrollierbar per übersichtlichem Dashboard. Administratoren haben damit den Zustand ihrer Unternehmens-IT immerzu im im Blick und können schnell und flexibel auf unerwartete Ereignisse oder Probleme reagieren.

Sind mögliche Schwachstellen identifiziert, lassen sie sich mit einem Patch Manager beheben. Administratoren können damit Sicherheitslücken schließen, Fehler korrigieren und Funktionen erweitern. Durch die regelbasierte Freigabe von Patches können diese Maßnahmen problemlos auch unternehmensweit implementiert werden, ohne dass sich Systemverantwortliche manuell um jeden einzelnen PC oder Server kümmern müssen. Im Idealfall wird dabei auch der Status der erfolgten Jobs unmittelbar erfasst.

Als dritte Komponente einer umfassenden Unternehmenssicherheit müssen die Betriebssysteme auf dem neuesten Stand gehalten werden. Auch dafür empfiehlt sich ein automatisierter Prozess, da sich die Updatezyklen selbst von Standardsoftware mittlerweile stark verkürzt haben und ein manuelles Update einen zu großen Zeitaufwand erfordern würde.

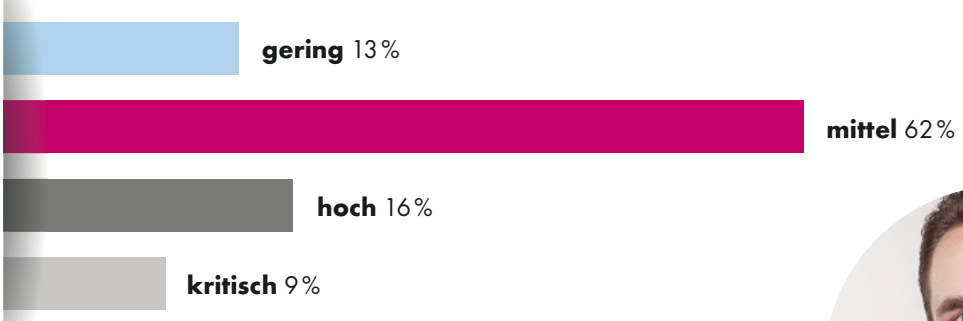
Unternehmen können nur gewinnen

Der Einsatz eines automatisierten Schwachstellenmanagements garantiert Unternehmen einen wirklichen Mehrwert an Sicherheit. Sie können auf potenzielle Bedrohungen schnell und gezielt reagieren und haben jederzeit eine Übersicht über mögliche Schwachstellen. Updates und Patches lassen sich zentral und automatisiert verteilen und die Unternehmen können sich darauf verlassen, dass jeder Arbeitsplatz und jeder Server sicher konfiguriert ist. Einer der größten Vorteile: Durch die Entlastung der eigenen Systemadministratoren von diesen, manuell kaum mehr mit der gleichen Qualität leistbaren Routineaufgaben, haben diese den Kopf frei, sich den Aufgaben zu widmen, die für die Zukunft des Unternehmens strategisch wirklich wichtig sind.

Alexander Haugk

BRISANTE SCHWACHSTELLEN 2018

Rund ein Viertel aller Schwachstellen in 2018 wurden mit hoher oder kritischer Priorität eingestuft.



ttps://www.cvedetails.com/cvss-score-charts.php

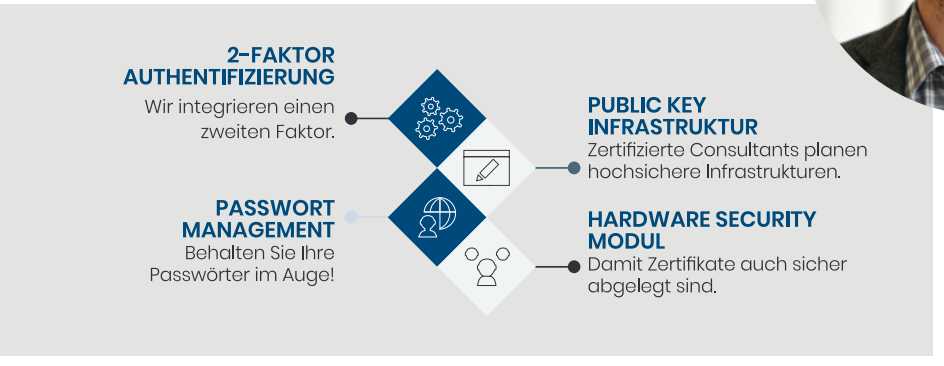
IM INTERNET KURSIEREN EXPLOITS ZU UNZÄHLIGEN SCHWACHSTELLEN. FIREWALLS UND VIRENSCANNER BIETEN DAGEGEN KEINEN ZUVERLÄSSIGEN SCHUTZ.

Alexander Haugk, Produkt Manager, baramundi software AG | www.baramundi.de

EU-DSGVO DIGITAL

DAS PASSWORD-MANAGEMENT BOOMT.

Was kann an einem Passwort so schwer sein? Vieles! Die EU-DSGVO gibt klar vor, dass Zugriffe geregelt und dokumentiert sein müssen. Auch deswegen gewinnt das toolbasierte Password Lifecycle Management immer mehr Zuspruch. Ein Passwort für alle Anwendungen und Plattformen ist bei vielen Usern noch immer Standard. Unternehmen wissen um dieses Sicherheitsrisiko und arbeiten mit Hochdruck an einem Konzept. Schnell ist vielen Administratoren klar, dass mit Excel-Listen und gängigen Freeware-Tools kein Weiterkommen ist. Die Knackpunkte sind unter anderem die Active-Directory-Integration, aber auch die Client-Server-Architektur, Browser-Add-ons für den Single-Sign-On-Zugriff oder die Durchsetzung von Richtlinien.



Passwort Lifecycle Management greift weiter

Ein toolbasiertes Passwort Lifecycle Management löst diese Punkte ebenso wie weitere Mehrwerte generiert werden. So können auch Pins, Tans und Codes aller Art sicher abgelegt, mit einem Backup versehen und bei Bedarf von einer zentralen Stelle bereitgestellt werden. Zudem werden die Passwörter regelmäßig geändert und Personen können auf Knopfdruck gesperrt werden. Weitere Aspekte eines datenschutzkonformen „Privacy-by-Design"-Ansatzes sind das angewandte Vier-Augen-Prinzip, eine rollenbasierte Zugriffskontrolle oder verschiedene zeit- und kostensparende Auditierungsmöglichkeiten. Um die Sicherheit weiter zu erhöhen, ist es außerdem sinnvoll, sehr starke Passwörter automatisch generieren zu lassen. Diese können einfach mit Copy & Paste oder gar via Single-Sign-On automatisiert eingefügt werden – ohne Browser-Merkfunktion. Voraussetzung dafür ist eine sinnvolle Variante der 2-Faktor-Authentifizierung. Im Sinne des Datenschutzes ist die Wahl eines europäischen Herstellers grundsätzlich ratsam, da sie selbst in der Cloud hohe Rechtssicherheit, schnellere Supportantworten und meist die bessere Anwendbarkeit für mittelständische Umgebungen gewährleisten.

Ganze IT-Security betroffen

Mit der Passwort-Thematik treten weitere Security-Aspekte auf die Agenda, die bereits geklärt sein sollten oder in dem Zuge erledigt werden. Dazu zählen:

- Single-Sign-On
- 2-Faktor-Authentifizierung
- PKI-Integration
- HSM-Integration
- Prozesse hinsichtlich Notfall-Passwort-Vergabe oder bei Verstößen (Siegelbruch)

Immer wichtiger werden zudem „Session Recording" und „Privilegierte Accounts", bei denen Administratoren oder externe Servicetechniker mit temporären Accounts ebenfalls überwacht und gemonitort werden. Natürlich gibt es für jedes dieser Themen eigene Speziallösungen renommierter Hersteller; ein gutes Passwort-Management-Tool ist jedoch ebenfalls in der Lage, die Anforderungen abzubilden.

Faktoren für ein erfolgreiches Projekt

Die Komplexität erfolgreicher Lösungen kann so umfangreich sein, dass einige wenige Consulting-Tage für die Implementierung empfehlenswert erscheinen. Dafür sollte ein Partner gewählt werden, der entsprechende Zertifizierungen und Referenzen mitbringt. In Sachen Software-Anbieter müssen die offene Architektur und erfolgreiche Kooperationen mit anderen Security-Vendoren gegeben sein, um Insellösungen zu verhindern und möglichst viele Synergien zu nutzen. Mateso, Yubico und Antares NetlogiX sind drei der wenigen Anbieter, die diese Kriterien erfüllen.

Jürgen Kolb

> UM DIE SICHERHEIT WEITER ZU ERHÖHEN, IST ES SINNVOLL, SEHR STARKE PASSWÖRTER AUTOMATISCH GENERIEREN ZU LASSEN.
>
> Jürgen Kolb, Managing Partner, Antares-NetlogiX Netzwerkberatung GmbH www.netlogix.at

ES GIBT KEINE 100 % ABSICHERUNG GEGEN CYBERATTACKEN, ABER EINE VERSICHERUNG.

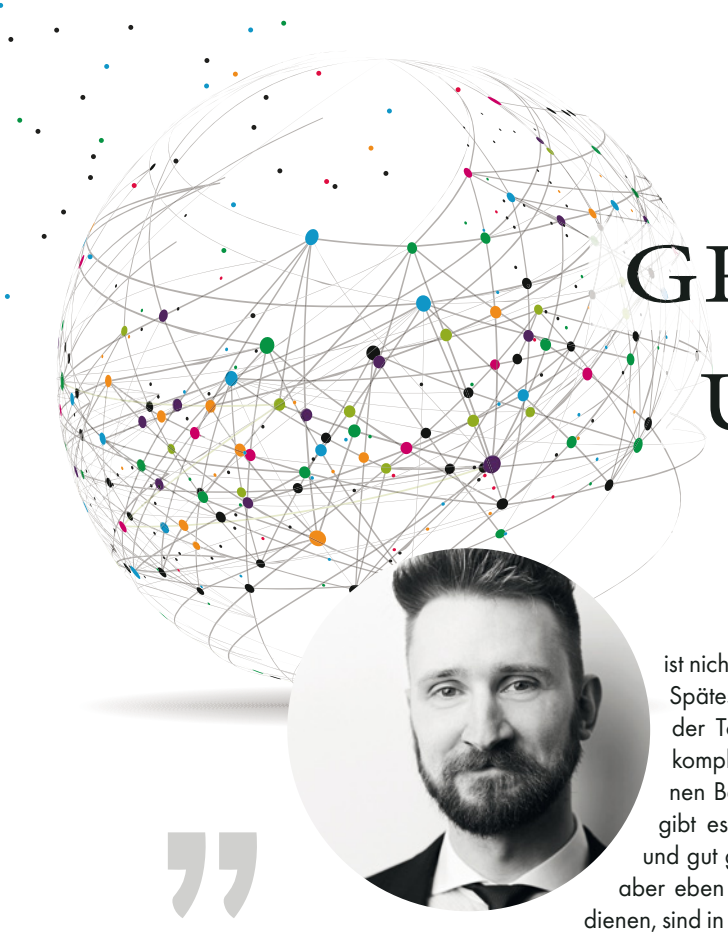
Hiscox CyberClear – die Cyberversicherung für kleine und mittelständische Unternehmen und Freelancer.

Hiscox weiß, wie schwerwiegend Schäden durch Systemausfall, Datenverlust oder Schadprogramme sind. Mit maßgeschneiderten Versicherungslösungen schützen wir Sie vor Digitalrisiken und unterstützen Sie bei der Prävention.

Mehr erfahren: hiscox.de/cyber

HISCOX

WISSEN VERSICHERT.



GRUNDSCHUTZ UND ISO 27001

VERNETZUNG VON BAUSTEINEN UND GEFÄHRDUNGEN.

> INSGESAMT LÄSST SICH FESTSTELLEN, DASS SICH DIE GRUNDSCHUTZ-VORGEHENSWEISE DURCH DIE ANNÄHRUNGEN AN DIE ISO 2700X NORMENREIHE ZU EINEM IMMER KOMPLETTER WERDENDEN STANDARD ENTWICKELT HAT.
>
> Thomas Eimecke, Senior Consultant, HiScout GmbH | www.hiscout.com

Mit seinen 200-x Standards hat sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) weiter der ISO 2700x Normenreihe angenähert. So haben zum Beispiel die Anforderungen des IT-Grundschutz-Kompendiums jetzt einen ähnlichen Charakter wie die Controls der ISO Standards.

Für viele Unternehmen und Behörden ist die Einführung und Etablierung eines ISMS eine der größten Herausforderungen denen sie sich bislang stellen mussten. Das Ziel, ein integriertes GRC-Managementsystem zu etablieren, scheint daher oft unerreichbar.

Oftmals sind allein schon die organisatorischen Hürden unüberwindbar und eine Zusammenarbeit der jeweiligen Fachbereiche ist nicht immer selbstverständlich. Spätestens aber bei der Frage der Tool-Unterstützung wird es kompliziert. Denn für die einzelnen Bereiche des GRC-Umfelds gibt es viele hoch spezialisierte und gut geeignete Tools. Da diese aber eben nur einen Teilbereich bedienen, sind in den meisten Unternehmen mehrere parallel im Einsatz.

Diese komplexen Strukturen können über ein geeignetes, integratives GRC-Tool vermieden werden. Hierfür sollten im Tool die einzelnen Anwendungsgebiete zwar separat darstellbar sein, aber eben auf eine gemeinsame Datenbasis zugreifen.
Die HiScout GmbH verfolgt mit Ihrer Plattform genau diesen Ansatz. Die einzelnen Module sind dabei speziell für ihr Anwendungsgebiet gestaltet, aber immer über die gemeinsame Datenbasis miteinander verbunden.

Bausteine als Risikoprofile

Ein Vorteil den die Grundschutz-Vorgehensweise seit jeher bietet, ist die Vernetzung von Bausteinen und Gefährdungen. Schon für die alte Grundschutz-Vorgehensweise war im „HiScout Grundschutz" eine automatisierte Übernahme der, aus der Modellierung mit Bausteinen resultierenden, Gefährdungen möglich. Auch für das neue Vorgehen ist diese Übernahme möglich und schafft somit eine wesentliche Erleichterung für den jeweiligen Risikomanager.

Diese Erleichterung kann auch im „HiScout ISM" genutzt werden. Hierbei dienen die Bausteine als eine Art Risikoprofil für die Assets. Bei der Erstellung einer Risikoanalyse kann so über die zugeordneten Profile ein Vorschlag für möglicherweise relevante Gefährdungen direkt an die Risikoanalyse übernommen werden.

Die im Vorfeld durchzuführende Zuordnung zu den Profilen kann dabei, in Anlehnung an die Modellierung des Grundschutzes, auf Einzel-Asset-Ebene durchgeführt werden aber ebenso auch auf der Basis von Asset-Typen erfolgen. Die Zuordnung der Grundschutzbausteine zu einzelnen Asset-Typen bildet im „HiScout Grundschutz" auch die Grundlage für die automatisierte Modellierung und wird vom Unternehmen mitgeliefert.

Die Nutzung der neuen Grundschutzbausteine als Risikoprofile bietet eine fachlich fundierte Basis und kann natürlich durch eigene Profile erweitert werden. Diese können dann wiederum im „HiScout Grundschutz" als benutzerdefinierte Bausteine genutzt werden.

Annäherung schafft Synergieeffekte

Insgesamt lässt sich feststellen, dass sich die Grundschutz-Vorgehensweise durch die Annährungen an die ISO 2700x Normenreihe zu einem immer kompletter werdenden Standard entwickelt hat. Während in der alten Vorgehensweise noch die umfänglichen Kataloge und die darin enthaltenen Verknüpfungen der Hauptvorteil waren, verbindet die aktuelle Vorgehensweise nun die guten Ansätze der ISO 2700x Normenreihe mit einem umfangreichen Kompendium.

Des Weiteren ist festzustellen, dass sich die, über diese Annäherungen entstandenen Synergieeffekte durch ein Tool mit einem integrativen Ansatz sehr gut nutzen lassen.

Thomas Eimecke

5 HERAUSFORDERUNGEN FÜR DEN CIO SAP SICHERHEIT HEUTE.

Die Bedeutung von SAP-Sicherheit ist eine von vielen Herausforderungen mit denen ein CIO konfrontiert ist. Dies kommt besonders durch den enormen Anstieg von Cyberkriminalität.

Laut einer Studie von Accenture finden jährlich durchschnittlich 130 Angriffe auf jedes Unternehmen statt. Das entsprach zuletzt einem Anstieg von nahezu 30 Prozent zum Vorjahr. Hinzu kommt, dass Angriffe häufig intern ausgeübt werden und es durchschnittlich 80 Tage dauert, diese zu entdecken.

Weitere 50 Tage werden benötigt, um den Vorfall zu beheben und die Sicherheitslücke zu schließen.Eine ganzheitliche Sicherheitsstrategie ist demnach kein „nice-to-have", sondern von grundlegender Relevanz. Der Schutz der SAP-Landschaft muss eine wichtige Rolle spielen. Auch wenn die SAP-Systeme in vielen Unternehmen lediglich 5 bis 10 Prozent der IT ausmachen, ist SAP bei weitem mehr als nur eine Anwendung. Die SAP-Systeme verfügen über eine eigene IT-Infrastruktur und sind somit hochkomplex. Als Herzstück des Unternehmens ist es fatal, SAP als Blackbox zu betrachten. Die Systeme beinhalten personenbezogene Daten von Kunden, Mitarbeitern und Partnern und bilden kritische Unternehmensprozesse ab.

Ein Angriff auf die SAP-Landschaft hat gravierende Folgen für das Unternehmen. Um dem entgegenzuwirken sollten alle Maßnahmen, die für IT-Security im Allgemeinen wichtig sind, auch für die SAP-Landschaft umgesetzt werden.
Erfahren Sie in unserm eBook, welchen Herausforderungen sich der CIO darüber hinaus stellen muss und welche Maßnahmen ihm dabei helfen diese zu meistern.

www.virtualforge.com/de/5-herausforderungen

VIRTUALFORGE

KOSTEN VON DOS-ATTACKEN UND ANGRIFFEN AUF WEBANWENDUNGEN

Das Ponemon Institut hat die Veränderungen in den Kosten und Folgen von Denial of Service (DoS)- und Webanwendungsangriffen im EMEA-Raum untersucht und die Ergebnisse in dem Bericht „Die Kosten von DoS-Attacken und Angriffen auf Webanwendungen: EMEA" zusammengefasst.

Für diese Studie befragte das Ponemon Institut 517 Personen in den Bereichen IT-Betrieb, IT-Sicherheit, IT-Compliance oder Verwaltung von Rechenzentren im EMEA-Raum (Europa, Naher Osten und Afrika). Das im Oktober 2018 veröffentlichte Whitepaper ist in zwei Abschnitte unterteilt: Der erste Abschnitt befasst sich mit der Sicherheit von Webanwendungen. Im zweiten Abschnitt geht es um DoS-Angriffe. Die Ergebnisse sind in 23 Abbildungen veranschaulicht.

Für diese Studie befragte das Ponemon Institut 517 Personen in den Bereichen IT-Betrieb, IT-Sicherheit, IT-Compliance oder Verwaltung von Rechenzentren im EMEA-Raum (Europa, Naher Osten und Afrika). Das im Oktober 2018 veröffentlichte Whitepaper ist in zwei Abschnitte unterteilt: Der erste Abschnitt befasst sich mit der Sicherheit von Webanwendungen. Im zweiten Abschnitt geht es um DoS-Angriffe. Die Ergebnisse sind in 23 Abbildungen veranschaulicht.

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

ADVANCED PERSISTENT THREATS

SECURITY INFORMATION AND EVENT MANAGEMENT ALS SCHUTZ VOR ANGRIFFEN.

Nachdem heute kein Wirtschaftszweig mehr auf den Einsatz moderner Informationstechnologien verzichten kann, kommt dem Thema „Cyberkriminalität" entsprechend hohe Bedeutung zu. Allein in den Jahren 2016 und 2017 wurden nach Angaben von Bitcom 53 Prozent der deutschen Unternehmen Opfer von Angriffen auf ihre IT-Infrastruktur, wobei ein geschätzter Sachschaden von circa 55 Milliarden EUR pro Jahr entstand. Neben einfachen Angriffen, wie sogenannten „Denial of Service Attacken", wurden in den vergangenen Jahren Tendenzen offenkundig, nach denen Angriffe beispielsweise zur Ausspähung von Betriebsgeheimnissen über einen langen Zeitraum vorbereitet und mitunter auch durchgeführt werden, ein Phänomen, das als „Advanced Persistent Threat", kurz „APT", bezeichnet wird.

Ziel derartiger APTs sind nicht nur staatliche Einrichtungen beziehungsweise kritische Infrastruktursysteme wie Strom-, Wasser- und Gasversorgung, sondern nicht zuletzt auch Unternehmen des Mittelstandes, deren zentraler Erfolgsfaktor spezifisches Spezialwissen darstellt, das entsprechend auch für Mitbewerber von hohem Interesse ist. Der Verlust solchen Wissens kann die Existenz solcher KMU direkt und innerhalb kurzer Zeitspannen gefährden. Neben einer solchen Form der Ausspähung, das heißt dem „Vertraulichkeitsverlust", gilt es auch die „Datenintegrität" zu gewährleisten, das heißt Unternehmensdaten dürfen nicht unberechtigt manipuliert, eingespielt oder gelöscht werden. Zu guter Letzt ist die „Verfügbarkeit" der IT-Systeme sicherzustellen. Diese drei zentralen Anforderungen wer-

den als die „primären IT-Schutzziele" bezeichnet. Diesen zur Seite werden in der Regel „sekundäre" Schutzziele gestellt, zu denen die „Authentizität", die „Verbindlichkeit" sowie die „Privatsphäre" gehören. Unter Authentizität versteht man, dass die Glaubwürdigkeit von Benutzern beziehungsweise Daten in einem System gewährleistet wird, während die Nichtabstreitbarkeit beispielsweise von

Änderungen an Datenbeständen unter die Verbindlichkeit fällt.

Erkennung dauert zu lange

Das Perfide an APT-Angriffen ist, dass sie für jedes angegriffene Unternehmen sozusagen maßgeschneidert werden, um die individuellen Eigenschaften der IT-Landschaft des Zielunternehmens auszunutzen, wozu auch das Ausnutzen bislang nicht publizierter beziehungsweise gar bekannter Schwachstellen, sogenannter „Zero Day Exploits" zählt. Dies macht das Erkennen derartiger Angriffe ausgesprochen schwierig, da sie in der Regel keinem bekannten Muster folgen und allein aufgrund dieser Tatsache häufig lange Zeit unbemerkt bleiben. Nach einer Studie des Sicherheitsunternehmens „FireEye" verstreichen im europäischen Raum zwischen 99 und 175 Tagen, bis ein APT-Angriff innerhalb des betroffenen Unternehmens erkannt wird. Innerhalb einer solchen Zeitspanne können Daten (Konstruktionszeichnungen, Unternehmensstrategieplanungen) in großem Umfang ausgespäht werden.

Ziel eines jeden Unternehmens muss also eine möglichst schnelle Erkennung solcher und anderer Angriffe sein. Diesem geht selbstverständlich eine rigide Patchpolitik voraus, um sicherzustellen, dass alle IT-Systeme auf dem jeweils aktuellen Patchlevel sind, um zumindest bekannte Sicherheitslücken als Einfallstore für Angriffe auszuschließen.

SIEM

Zentrales Element zur frühzeitigen Erkennung von APT-Angriffen ist ein sogenanntes „SIEM"-System, kurz für „Security Information and Event Management", das heißt ein System, mit dessen Hilfe die gesamte IT-Infrastruktur eines Unternehmens überwacht werden kann, wobei in Echtzeit Ereignisse gesammelt, überwacht und analysiert werden. Neben der zentralen Frage, welche Ereignisse, meist als „Events" bezeichnet, überhaupt in das SIEM-System fließen sollen, stellt die Analyse die zentrale Herausforderung dar, da bei einer hinreichend komplexen überwachten Infrastruktur viele tausend, mitunter auch Millionen von Ereignissen pro Tag anfallen können, die in der Regel für sich alleine genommen wenig bis gar nicht aussagekräftig sind.

Beispielsweise ist ein einziger Login-Fehlversuch für sich genommen nicht verdächtig, handelt es sich jedoch um einen Fehlversuch in einer ganzen Reihe von Versuchen, die vielleicht noch dazu außerhalb der Geschäftszeiten oder in urlaubs- oder krankheitsbedingter Abwesenheit des zugeordneten Users stattfinden, so kann dies ein Zeichen für einen Angriffsversuch sein. Zunächst einmal ist es also erforderlich, alle, wirklich alle Systeme der IT-Landschaft eines Unternehmens an das genutzte SIEM-System anzubinden, was allein für sich gesehen keine kleine Herausforderung darstellt, müssen doch in der Regel Systeme einer sehr heterogenen Landschaft mit Schnittstellen versehen werden, um Daten anliefern zu können. Ist diese Hürde erfolgreich genommen, stellt sich die Frage, wie mit den derart gesammelten Datenmengen verfahren wird. In einfachen Fällen kann mit mehr oder weniger komplexen Regeln gearbeitet werden, um beispielsweise Vertipper bei der Passworteingabe durch einen legitimen Benutzer von einem Angriffsversuch zu unterscheiden. Im Falle von APTs

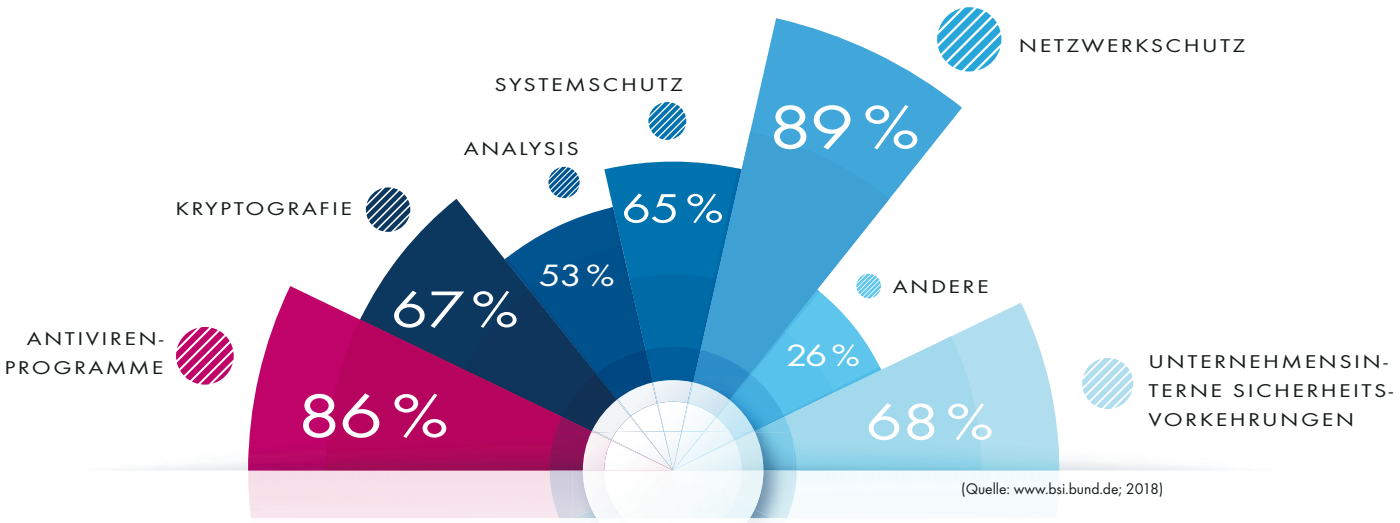
BIG DATA UND ARTIFICIAL INTELLIGENCE WERDEN NICHT ZULETZT IM SIEM-UMFELD IN ZUKUNFT EINE ZENTRALE ROLLE SPIELEN.

Prof. Dr. Bernd Ulmann
Professor für Ökonomie und Management; FOM

sind derartige Regeln jedoch typischerweise nicht ausreichend, da ein „guter" Angreifer eventuell auch Kenntnis dieses Regelwerkes besitzt und entsprechend Angriffsvarianten anwenden wird, für welche diese Regeln blind sind.

Hinterfragen, analysieren, anpassen

Der Einsatz von SIEM-Systemen an sich ist also noch kein Garant für die zeitnahe Erkennung von APTs. Wichtig ist vor allem, dass ein solches System „lebt", das heißt nicht als statische Einrichtung betrachtet



Welche Maßnahmen werden derzeit in Ihrer Einrichtung zum Schutz vor Cyber-Angriffen durchgeführt?

und betrieben wird, sondern Tag für Tag an die sich ändernden Rahmenbedingungen angepasst wird. Hierzu gehört vor allem, dass das zur Anwendung gelangende Regelwerk kontinuierlich hinterfragt, analysiert und angepasst wird. Ein statisches System ist gefährlicher als gar kein System, da es das Unternehmen in trügerischer Sicherheit wiegt, vermutlich aber längst blind für eine Vielzahl von Angriffsszenarien ist.

Ein weiterer Punkt von zentraler Bedeutung neben der Einrichtung eines SIEM-Systems, der Anbindung der einzelnen Infrastrukturkomponenten (sowohl Hard- als auch Software) sowie der Pflege und Weiterentwicklung des Regelwerkes ist das Aufstellen von Reaktionsplänen. Wurde eine Bedrohung erkannt, muss auf bereits im Vorfeld definierte und kommunizierte Maßnahmen zurückgegriffen werden können, um den erkannten Angriff abzuwehren. Ohne eine solche Sammlung möglicher Reaktionen geht im Falle eines Angriffes zu viel wertvolle Zeit verloren, was dem Angreifer in die Hände spielt. Für die Pflege und Weiterentwicklung dieses Maßnahmenkataloges gilt das Gleiche wie das für das Regelwerk gesagte – ein über längere Zeit hinweg statischer Maßnahmenkatalog büßt nicht nur zusehends an Wirkungskraft ein, sondern vermittelt einen falschen und eventuell fatalen Eindruck, dass man Bedrohungen gezielt beantworten könne, was sich dann im Krisenfall angesichts der rasch fortschreitenden Entwicklung von APT-Angriffen als falsch herausstellt.

Der Maßnahmenkatalog

Zu einem solchen Maßnahmenkatalog gehört auch die Definition von Ansprechpersonen sowie deren Verantwortlichkeiten im Falle eines Angriffes. Hierzu gehört beispielsweise die Entscheidungsgewalt, Verbindungen zu unterbrechen oder ganze Server herunter zu fahren – auch, wenn hierdurch laufenden Produktionsprozesse beeinträchtigt oder unterbrochen werden. Die Abwägung, wie stark beispielsweise Produktionsausfälle beziehungsweise Datenverluste zu gewichten sind, sollte lange im Vorfeld im Maßnahmenkatalog festgelegt worden sein, um zeitraubende Kompetenzsrangeleien zu vermeiden und entsprechend schnell reagieren zu können („Incident Response Orchestration").

Eine zentrale Rolle in diesem Zusammenhang ist die des „Incident Coordinators". Neben diesen Maßnahmen sollten auch in regelmäßigen Abständen, idealerweise jedoch zu unbekannten Terminen „Alarmübungen" wie beim Militär durchgeführt werden, um sicherzustellen, dass alle relevanten Personen wissen, wie im Falle eines erkannten APTs vorzugehen ist und nicht in Panik Fehlentscheidungen treffen. Dies lässt sich mitunter und idealerweise mit sogenannten „Penetrationstests" kombinieren. Ein solcher Test wird mit den Methoden, die auch reale Angreifer aller Wahrscheinlichkeit nach anwenden würden, auf die reale Infrastruktur eines Unternehmens durchgeführt, um Schwachstellen aufzudecken.

Beispiele für APT Angriffe

Opfer von APT-Angriffen wurden bereits eine Vielzahl von namhaften Unternehmen wie zum Beispiel Sony Entertainment, Adobe, Google oder Yahoo. Bei Yahoo gelang es den APT-Angreifern, in den Besitz von circa 1,5 Milliarden Benutzerdaten zu gelangen. Die Benutzerdaten umfassten unter anderem E-Mail-Adressen, Telefonnummern und Passwörter. Gemessen an der Anzahl der betroffenen Personen stellt der Cyberangriff auf Yahoo einen der größten Datendiebstähle der Geschichte dar. Yahoo erkannte erste Anzeichen für den Angriff im Jahr 2014 und konnte den vollen Umfang des Datendiebstahls erst im Jahr 2016 feststellen. Die Angreifer erlangten aber bereits im Jahr 2013 Zugriff auf die Nutzerdaten und blieben über viele Monate weitestgehend unentdeckt. Ziel von APT-Angriffen sind aber nicht nur Unternehmen, sondern auch Regierungsnetze und deren IT-Systeme. Das zeigt der Angriff auf den Deutschen Bundestag im Jahr 2015. Die eindeutige Identifizierung der Angreifer ist bis heute nicht möglich, aber die Spuren weisen auf die Hacker-Gruppe APT28 hin. Diese wird in Verbindung mit der russischen Regierung gebracht.

Die Täter infiltrierten das Netz über den Laptop eines Abgeordneten, auf dem sie Malware einschleusten. Danach gelang es den Angreifern mithilfe verschiedener Hacker-Tools, weitere Zugangsdaten mit den dazugehörigen Passwörtern von Nutzer-Accounts und sogar von IT-Administratoren zu erlangen. Dadurch konnten Sie sich innerhalb kürzester Zeit im Netzwerk des Bundestages ausbreiten und blieben zu Beginn weitestgehend unentdeckt. Welche Daten genau durch die Täter entwendet wurden, ist nicht veröffentlicht worden. Der BSI bestätigt aber in seinem Abschlussbericht, dass etwa 16 GB an Daten gestohlen wurden, die E-Mails von Abgeordneten, Dateien und Bildschirmfotos umfassten. Ein weiteres Beispiel dafür, dass es Angreifer nicht nur ausschließlich darauf abzielen, sensible Informationen zu erlangen, zeigt der Cyberangriff auf eine iranische Nuklearanlage im Jahr 2010. Die Angreifer entwickelten eine sehr fortschrittliche Form von Malware namens Stuxnet. Diese war speziell an den technischen Steuerungsgeräten der Firma Siemens angepasst. Stuxnet war auf tausenden IT-Systemen weltweit verbreitet, richtete dort aber keinen Schaden an, sondern nur wenn es auf einem IT-System eingeschleust wurde, das den Siemens Steuerungsgeräten des iranischen Atomkraftwerkes entsprach. Dies zeigt, wie zielgerichtet die Angreifer die Malware konzipiert hatten. Das Ziel der Angreifer war es, die iranische Nuklearanlage zu sabotieren und damit die komplette Anlage zu zerstören. Stuxnet gelang es circa 1000 Uran-Zentrifugen zu zerstören und damit das Atomprogramm Irans, um mehrere Jahre zurückzuwerfen. Die erforderliche Expertise, die erheblichen finanziellen Ressourcen und der hohe personelle Aufwand deuteten darauf hin, dass hinter dem Angriff eine staatliche Institution stehen musste. Es wird vermutet, dass es sich dabei um die USA und Israel handelte, die das Aufsteigen des Irans zu einer Atommacht verhindern wollten. Stuxnet zeigt, dass APT-Angriffe das Potenzial bieten, konventionelle Militärschläge zu ersetzen.

Diese Beispiele verdeutlichen das große Schadenspotenzial, das von APT-Angriffen ausgeht und damit auch die Wichtigkeit, sich gegen diese effektiv zu schützen.

Die zentrale Fragestellung

Durch welche Maßnahmen kann beim Einsatz eines SIEM-Systems der Schutz vor APT-Angriffen verbessert werden?

Zusammenfassend konnte mithilfe von Experteninterviews in verschiedene Bereiche der Technologiebranche folgende Maßnahmen identifiziert werden, die beim Einsatz eines SIEM-Systems den Schutz vor APT-Angriffen verbessern

- Sandboxing und Implementierung von Honeypots,
- Orientierung an der Cyber Kill Chain von APT-Angriffen,
- Nutzung von Threat Intelligence Services,
- Mehrstufige Analyse und Priorisierung der Incidents,
- Qualifizierung der Mitarbeiter,
- Proaktives Threat Hunting,
- Regelmäßige Durchführung von Penetrationstests.

Diese Ergebnisse zeigen, dass für einen effektiven Schutz vor APT-Angriffen beim Einsatz eines SIEM-Systems neben der technischen Leistungsfähigkeit eines SIEM-Systems auch prozessuale, organisatorische und personelle Maßnahmen erforderlich sind.

GERADE DIE VERBINDUNG VON SIEM UND KI BIETET EIN GROSSES POTENZIAL.

Dr. Patrick Hedfeld, Senior Projektleiter, Deutsche Leasing AG, FOM Hochschuldozent
www.deutsche-leasing.com

Ein Vergleich der Ergebnisse dieser Befragungen mit bereits existierenden Sammlungen von allgemeinen Best-Practice-Tipps und Empfehlungen für den Einsatz von SIEM-Systemen zeigt, dass die identifizierten Maßnahmen sich zum Teil überschneiden.

Die Untersuchung verdeutlicht jedoch, dass für den effektiven Schutz vor APT-Angriffen beim Einsatz von SIEM-Systemen weitaus mehr spezifische Maßnahmen erforderlich sind, als derzeit in existierenden Sammlungen von Best-Practice-Tipps zu finden sind.

Dr. Patrick Hedfeld, Prof. Dr. Bernd Ulmann

DIE FÜNF STUFEN EINES APT-ANGRIFFS

(Quelle: www.hometsecurity.com)

SICHERES PASSWORTMAN

AUF DEM WEG IN DIE ZUKUNFT.

Die Zahl der Passwörter, die in Unternehmen aber auch privat verwaltet werden müssen, steigt stetig. Mit jeder neuen Anwendung, jedem neuen Dienst oder Gerät kommen neue Kennwörter und Berechtigungsnachweise dazu. Gerade für Unternehmen bedeutet die wachsende Zahl an Passwörtern eine große Herausforderung, da sie den Spagat zwischen hoher Verfügbarkeit und hoher Sicherheit meistern müssen, insbesondere bei kritischen und privilegierten Zugangsdaten.

Was es bedeutet, wenn dies nicht gelingt, zeigte jüngst der Vorfall bei einer kanadischen Kryptogeld-Börse. Die Geschäftsführer von QuadrigaCX mussten gestehen, nicht mehr an die Kundeneinlagen in Höhe von 190 Millionen US-Dollar heranzukommen, da nur der Firmengründer in Besitz des Passwortes gewesen ist, dieser aber unerwartet verstorben sei. Mag dieses drastische Beispiel eher die Ausnahme sein, so sind schlecht geschützte Passwörter jedoch an der Tagesordnung. Der Diebstahl und das Knacken unsicherer Passwörter ist für Unternehmen eines des größten Cyberrisiken, das existenzgefährdende Auswirkungen nach sich ziehen kann.

Passwortschutz wie in den 90ern

Obwohl die Anforderungen an den Datenschutz seit Jahren steigen und die Einführung der EU-DSGVO von vielen begrüßt wurde, sind die Auswirkungen auf das eigene Sicherheitsverhalten eher gering – gerade in Sachen Passwortschutz. Erst kürzlich hat das Hasso-Plattner-Institut aus Potsdam basierend auf einer Analyse von rund 60 Millionen geleakter Identitätsinformationen die beliebtesten Passwörter der Deutschen veröffentlicht. Das Ergebnis ist ernüchternd, denn wie in den Vorjahren stehen bei den Deutschen vor allem unsichere Zahlenreihen wie „123456" sowie unkreative Einfälle wie „passwort" oder „hallo" hoch im Kurs. Hinzukommt, dass ein Passwort meist für eine Vielzahl von Accounts eingesetzt wird.

> PRIVILEGED ACCOUNT MANAGEMENT-TECHNOLOGIEN WERDEN IMMER WEITER AN BEDEUTUNG GEWINNEN, WENN ES DARUM GEHT, PASSWÖRTER UND ZUGRIFFSDATEN SICHER UND INSBESONDERE AUCH EFFEKTIV ZU VERWALTEN.
>
> Markus Kahmen, Regional Director CE, Thycotic | https://thycotic.com/

Dabei beschränkt sich schlechter Passwortschutz längst nicht nur auf Privatnutzer, wie man vielleicht denken könnte. Denn wem es privat am Bewusstsein für sichere Kennwörter mangelt, der wird höchstwahrscheinlich auch im beruflichen Umfeld hin und wieder nachlässig handeln. Begünstigt wird dies durch das Fehlen von Sicherheitsrichtlinien und Passwortmanagement-Technologien in den Unternehmen.

Dabei sind schlechte, leicht zu merkende Passwörter bei weitem nicht die einzige Nachlässigkeit in Sachen Passwortmanagement. So ist es in vielen Unternehmen nach wie vor an der Tagesordnung, Passwörter unkontrolliert über E-Mail, SMS oder soziale Netzwerke mit anderen Abteilungen oder Kollegen zu teilen, und auch das traditionelle und höchst unsichere Verwalten von Kennwörtern auf Excellisten ist noch weiterverbreitet als gedacht. Überdies ist es für viele IT-Administratoren zudem nach wie vor keine Selbstverständlichkeit, beim Installieren neuer Hard- oder Software die Standard-Kennwörter der Hersteller abzuändern. Kein Wunder also, dass für Hacker das Ausnutzen von nicht geänderten Standardkennwörtern eine der beliebtesten und schnellsten Methoden darstellt, um privilegierte Konten zu kapern, wie der BlackHat Hacker Report 2018 gezeigt hat.

Passwortsicherheit automatisieren

Bei all den negativen Beispielen darf man jedoch nicht übersehen, dass sich in Sachen sicherer Passwortverwaltung in den letzten Jahren auch viel getan hat. Immer mehr Unternehmen setzen auf Privileged Account Management (PAM)-Lösungen und forcieren Best-Practices, um ihre Zugangsdaten (vor allem die für privilegierte Accounts) unter Kontrolle zu bringen. Tatsache ist, dass Passwörter auch in Zukunft die Basis für den sicheren Zugriff auf Konten und sensible Informationen bleiben werden. Zwar entwickeln sich gerade biometrische Authentifizierungsme-

22 %

der Hacker greifen ihre Opfer regelmäßig über nicht geänderte Hersteller- und Standardkennwörter an.

AGEMENT

thoden rasant weiter, dennoch ist davon auszugehen, dass sie weiterhin lediglich als eine Ergänzung zu regulären Zugriffskontrollen fungieren werden.

Deshalb werden Privileged Account Management-Technologien immer weiter an Bedeutung gewinnen, wenn es darum geht, Passwörter und Zugriffsdaten sicher und insbesondere auch effektiv zu verwalten. Denn ihr Einsatz vereinfacht nicht nur die Einführung von Richtlinien, sondern macht einen nachlässigen Umgang mit Passwörtern so gut wie unmöglich. Moderne PAM-Lösungen bieten automatisierte Prozesse, die das sichere Erstellen und Rotieren starker Passwörter ermöglicht und sie zudem in die Lage versetzt, unkompliziert und schnell auf Ereignisse, etwa das Ausscheiden eines Mitarbeiters oder Sicherheitsvorfälle, zu reagieren. Ausführliche Zugriffsanalysen und Sitzungsüberwachungen privilegierter Konten helfen, Anomalien und möglichen Missbrauch frühzeitig zu identifizieren und unterstützen IT-Abteilungen zudem, die Einhaltung von Compliance- und Datenschutzanforderungen zu dokumentieren. Sicherheitsverantwortliche haben so alle sensiblen Zugriffsdaten im Blick und Mitarbeiter kommen nicht mehr in die Situation, Passwörter zu teilen oder zu verlieren.

Die Zukunft liegt in der Cloud

Dabei liegt die Zukunft von Privileged Account Management ganz klar in der Cloud. Mit PAM-as-a-Software-Services profitieren Unternehmen von skalierbaren, Hard- und Infrastruktur-unabhängigen Lösungen, die sofort einsatzbereit sind. Weil sich IT-Abteilungen hier nicht mit aufwendigen Installationen und vor allem nicht mit zeitaufwendigen Updates konfrontiert sehen, ist die Entlastung der Teams bei Cloud-Lösungen meist noch größer und die langfristigen Einsparungen noch höher.

Waren es bisher vor allem Großunternehmen, die auf Enterprise-PAM-Lösungen zurückgegriffen haben, so investieren nun auch KMUs verstärkt in PAM. Steigende Angriffszahlen – insbesondere bei Mittelständlern – und nutzerfreundliche Lösungen haben auch bei ihnen zu einem Umdenken und dem Zurücklassen herkömmlicher Passwortsicherheitspraktiken geführt.

Markus Kahmen

DROHNEN: RISIKO FÜR DIE IT-SICHERHEIT

DER SPION, DER AUS DER LUFT KAM.

> MITARBEITER MÜSSEN VERSTEHEN, DASS EIN ANGRIFF NICHT NUR ÜBER DAS INTERNET DROHT, SONDERN AUCH AUS DER LUFT. UNTERNEHMEN SOLLTEN DAS ENTSPRECHENDE RISIKOBEWUSSTSEIN SCHAFFEN UND DIE GEFAHR DURCH DROHNEN IN IHRER SICHERHEITSSTRATEGIE BERÜCKSICHTIGEN.
>
> Christian Koch, Senior Manager GRC & IoT/OT, NTT Security, www.nttsecurity.com/de-ch

Datendiebe haben längst neue Wege gefunden, in Firmengelände und -netzwerke einzudringen: Mit Hilfe von Drohnen greifen Cyber-Kriminelle inzwischen aus der Luft an. Um die unerwünschten Spione vom Himmel zu holen, hat sich die Industrie mit akustischen Signalen, Störsendern oder Laserkanonen einiges einfallen lassen. Vieles davon ist nicht erlaubt – umso wichtiger ist es, das Bewusstsein der eigenen Mitarbeiter für die neue Bedrohung zu schärfen.

Sicherheitsmaßnahmen

Keine Frage: Eine verlässliche Freigeländesicherung beginnt mit Mauern und Zaunsystemen, mit adäquater Video- sowie Tür- und Tortechnik. Doch gegen die Gefahr von oben helfen diese Maßnahmen wenig, immer öfter werden Unternehmen mit Drohnen aus der Luft angegriffen. Die unbemannten Flugobjekte nähern sich dem Gelände fürs bloße Auge kaum beziehungsweise nur sehr spät sichtbar. Der große Vorteil für die Cyber-Kriminellen: Sie kommen mit der Drohne näher an das interne Funknetz heran, dessen Reichweite normalweise nicht über das Betriebsgelände hinausgeht.

Das kleine Fluggerät wird sozusagen zum verlängerten Arm – sei es auf das WLAN, auf kabellose Verbindungen zu Peripheriegeräten wie Tastaturen, auf IoT-Systeme, die per Funk kommunizieren, und natürlich auf kabellose Systeme zur Gebäudesteuerung. Einmal platziert in luftiger Höhe, können Drohnen dann beispielsweise die Kommunikation zwischen Industriesystemen und dem MES (Manufacturing Execution System) mitschneiden oder manipulieren. Sie können mittels hochauflösender Kamera durch das Bürofenster Bildschirme abfilmen oder die Eingabe von PIN-Codes bei Zugangssystemen erfassen. Angreifer können zudem USB-Sticks mit Malware auf dem Firmengelände fallen lassen. Die Chance oder besser gesagt die Gefahr, dass Mitarbeiter diesen USB-Stick mitnehmen und an einem Rechner einstecken, ist sehr hoch. Interessantes zu entdecken gibt es dabei auf fast jedem Betriebsgelände. Für manche Branche ist die Spionage von oben zu einem richtigen Problem geworden: Wenn in der Automobilbranche ein „Erlkönig" auf die Teststrecke geschickt wird, landen Drohnen-Fotos schnell bei der Konkurrenz. Wie stark das Thema die Sicherheitsbranche beschäftigt, konnte man auch auf der letzten Messe, der „Perimeter Protection", in Nürnberg sehen. Dort machten sich Fachleute aus Industrie, Verkehr, Energie und Freizeit eigentlich über Neuerungen rund um Zaunsysteme, Zutrittskontrollen und Videoüberwachung schlau. Erstmals widmeten die Messeveranstalter der Drohnenerkennung und -abwehr eine Sonderfläche.

Spionage für ein paar Hundert Euro

Drohnen, die man bereits für ein paar Hundert Euro bekommt, sind inzwischen zu einem Massenprodukt geworden: Sie sind klein, leicht zu bedienen, überaus leistungsfähig und je nach Propellermodell relativ leise. Auf einem geschäftigen Betriebsgelände werden die Geräusche nicht wahrgenommen. Selbst günstigere Drohnen verfügen meist über hochauflösende Kameras, die mit einer speziellen Vorrichtung befestigt sind, um trotz Turbulenzen in luftiger Höhe möglichst verwacklungsfreie Aufnahmen zu bekommen. Je nach Bauart können die unbemannten Flugobjektive darüber hinaus Nutzlasten bis zu zwei Kilogramm aufnehmen. Wird beispielsweise ein scheckkartengroßer Minirechner wie der Raspberry Pi mit Funkempfänger, Interfacekarte und entsprechender Software an die Drohne gepackt, können Kriminelle ohne weiteres die Kommunikation einer drahtlos angebundenen Tastatur und damit die Eingabe von Passwörtern „abhören".

Auf dem Papier ist die Nutzung von Drohnen in Deutschland rechtlich geregelt. Die-

jenige Person, die eine Drohne betreibt, ist Nutzer des Luftraums und muss daher die geltenden luftrechtlichen Bestimmungen befolgen. Hat die Drohne eine Kamera an Bord, muss jederzeit die Privatsphäre anderer Personen respektiert und bei der Erfassung personenbezogener Daten die gesetzlich geltenden Vorschriften beachtet werden. Für Drohnen mit einem Gewicht über zwei Kilogramm – inklusive Zuladung – ist zudem ein Drohnen-Führerschein verpflichtend. All diese Vorgaben werden allerdings keinen Hacker davon abhalten, die kleinen Fluggeräte als Angriffsobjekte einzusetzen.

Gefahr aus der Luft - Cyber-Kriminelle nutzen Drohnen für ihren Angriff auf Firmennetzwerke.

© Fotolia

Fehlende Abwehr gegen Drohnen

Was können Unternehmen nun gegen die Bedrohung aus der Luft machen? Für das Erkennen und Identifizieren von Drohnen kommen akustische, optische und elektronische Verfahren zum Einsatz. Akustiksensoren erfassen die spezifischen Schallwellen, die jede Drohne emittiert, und werten diese aus. In einer nicht zu stark „lärmverschmutzten" Umgebung lassen sich damit die unbemannten Flugobjekte grob orten. Entsprechende Kamerasysteme arbeiten sowohl im sichtbaren Spektrum als auch im nahen Infrarotbereich.

Mit entsprechender Bildauswertungssoftware sollen falsche Alarme, durch zum Beispiel eines vorbeifliegenden Vogels, vermieden werden. Kameras und Akustiksensoren decken aber nur vergleichsweise geringe Distanzen ab, so dass zwischen dem Eindringen in den Luftraum und dem Erkennen des Flugobjekts eine sehr kurze Zeitspanne verbleibt, um adäquate Gegenmaßnahmen zu ergreifen. Für elektronische Erkennungsverfahren werden spezielle Antennen genutzt, die das Funkspektrum nach Signalen von Drohnen absuchen.

Detektieren ist der eine Aspekt in der Drohnen-Abwehr, der andere das Abfangen. Spezielle Störsender unterbinden die Kommunikation zwischen der Drohne und ihrem Piloten und zwingen das Flugobjekt damit zur Landung. Mit Lasertechnik oder EMP (Elektromagnetische Pulse) lassen sich Drohnen zudem direkt unter Beschuss nehmen, eine andere Möglichkeit sind Fangnetze, die vom Boden oder einer anderen Drohne aus über das unerwünschte Fluggerät geschossen werden. Alle Maßnahmen sind prinzipiell Polizei und Militär vorbehalten, der Betrieb von Störsendern durch Privatpersonen oder Unternehmen ist wie auch das Abschießen in Deutschland verboten und nur in Ausnahmefällen nach einer aufwändigen behördlichen Genehmigung erlaubt.

Das Bewusstsein fürs Risiko stärken

Die Abwehrmöglichkeiten gegen Drohnen sind damit begrenzt. Unternehmen sollten deshalb zuallererst sämtliche Funkverbindungen sichern, besonders durch konsequentes Verschlüsseln. Wird beispielsweise durch die Analyse der Funkkommunikation eine Drohne erkannt, können die Jalousien heruntergelassen werden. Werden Fenster vorbeugend verspiegelt, ist es nicht mehr möglich, Bildschirme abzufotografieren.

Zudem sollten Tastenfelder für PIN-Eingabegeräte so angebracht werden, dass sie nicht von oben ausspioniert werden können. Die wichtigste Maßnahme betrifft aber die Mitarbeiter: Sie müssen verstehen, dass ein Angriff nicht nur über das Internet droht, sondern auch aus der Luft. Unternehmen sollten das entsprechende Risikobewusstsein schaffen und die Gefahr durch Drohnen in ihrer Sicherheitsstrategie berücksichtigen.

Störsender und Abschießen verboten: Die Abwehrmöglichkeiten gegen Drohnen sind begrenzt.

© Pixabay

Christian Koch

DSGVO, CYBER & GESCHÄFTS

SMART CARDS MIT ZWEI-FAKTOR-AUTHENTISIERUNG BILDEN EINE FUNDAMENTALE SCHUTZSCHICHT UND SICHERN KRITISCHE UNTERNEHMENSWERTE EFFEKTIV UND KOSTENEFFIZIENT AB.

Anton Kreuzer, CEO, Drivelock SE | www.drivelock.de

IT-Sicherheit wird für Unternehmen und Organisation immer umfangreicher und komplizierter. Zum einen müssen Unternehmen seit der DSGVO kontrollieren, wer Zugang zu personenbezogenen Daten erhält. Auf der anderen Seite ist mittlerweile allgemein bekannt, wie schnell Cyberkriminalität wächst und wieviel Schaden sie verursacht.

WannaCry und Emotet sind nur zwei Schadprogramme, die weltweit immense Verluste unter ihren Opfern verursacht haben. Hinzu kommen immer raffiniertere und realistischere Phishing-Mails und Social-Engineering-Methoden. Seit dem 21. März 2019 gelten auch neue Bestimmungen beim Geschäftsgeheimnisgesetz. Bisher reichte es aus, wenn Unternehmen nach außen dokumentierten, dass sie eine Information geheim halten wollen. Jetzt müssen sie proaktiv technische und organisatorische Schutzmaßnahmen ergreifen, ähnlich wie bei der DSGVO. Erst dann greift der Geheimnisschutz auch rechtlich. Der Umfang der Maßnahmen muss sich zudem am jeweiligen Inhalt ausrichten: je schützenswerter das Geheimnis, umso umfassender der Schutz. Der Prototyp eines Produkts muss beispielsweise besser geschützt werden als das neue Design einer Verpackung.

Smart Cards – die Wachposten für Unternehmenswerte

Einen grundlegenden Schritt, um die Sicherheit sowie die Einhaltung aller gesetzlichen Vorgaben zu gewährleisten, stellen Smart Cards dar. Es gibt sie in verschiedenen Formen: virtuell und physikalisch als Security Token mit integriertem Lesegerät sowie als Chipkarte.

Ihr Zweck ist einfach: die Kontrolle von Zugängen zu Unternehmenswerten jeglicher Art. Dazu zählen sowohl das Firmengelände, Abteilungen, Laptops und weitere Endgeräte, wie auch Anwendungen und Dateien.

Mit dem dazugehörigen Passwort beziehungsweise der PIN wird die Sicherheit zusätzlich durch Zwei-Faktor-Authentisierung erhöht. Generell sollte in so vielen Fällen wie möglich diese Art von Login verwendet werden. Dazu rät auch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Über die Middleware der Smart Cards, der Software auf den Karten, können die Zugriffsrechte und Befugnisse des jeweiligen Mitarbeiters eingerichtet werden. Dadurch erhalten nur die Personen den Zugang zu Abteilungen oder die Erlaubnis zur Ausführung bestimmter Programme, die auch tatsächlich dafür berechtigt sind.

Smart Cards mit Zwei-Faktor-Authentisierung sichern somit effektiv den Zugang zu geschäftskritischen Unternehmenswerten und stellen eine aktive Schutzmaßnahme im Sinne der DSGVO und des

Geschäftsgeheimnisgesetzes dar. Zusätzlich erschweren sie Cyberkriminellen, auf die Unternehmenssysteme zuzugreifen. Denn selbst falls die Hacker durch Social Engineering Passwörter abgreifen, hilft es ihnen nichts ohne das physikalische Gegenstück.

In der Praxis

Für die verschiedenen Typen von Smart Cards gibt es unterschiedliche Einsatzszenarien. Große Unternehmen verwenden häufig physikalische Smart Cards. Zum Beispiel bezahlen Mitarbeiter auch das Essen in der Kantine über diese Karten

KRIMINALITÄT GEHEIMNISSE

WIE SMART CARDS UNTERNEHMEN BEI DER SICHERHEIT UNTERSTÜTZEN.

oder kommen erst durch Vorhalten der Karte auf das Firmengelände oder in die Forschungsabteilung. Wenn die Unternehmen keine Security Token mit integriertem Lesegerät verwenden, dann stellen sie die entsprechende Infrastruktur separat bereit. Das erfolgt durch Lesegeräte, die an Türen angebracht oder in Laptops für mobiles Arbeiten eingebaut sind. Mit physikalischen Karten gehen jedoch laufende Kosten einher. Etwa 10 Prozent der Karten müssen pro Jahr erneuert werden aufgrund von Verlust, Diebstahl oder Abnutzung. Außerdem sind die Organisationen häufig an den Kartenhersteller gebunden. Beendet dieser den Support der bestehenden Karten und ersetzt sie durch neue, sind die Unternehmen gezwungen, mitzuziehen.

Aufgrund dieser Abhängigkeit sind sie zusätzlich in einer schlechteren Verhandlungsposition. Alternativ können sie zwar den Anbieter wechseln, aber so oder so müssen sie zusätzliche Käufe tätigen. Abhilfe schafft hier eine Middleware, die auf jeder Karte läuft – unabhängig vom Hersteller. So können Unternehmen, statt neue Karten zu kaufen, lediglich eine neue Software erwerben und die bestehenden Smart Cards weiterhin nutzen.

Physikalische Karten haben einen Nachteil, der nicht auf den ersten Blick ersichtlich ist: Bei Verlust oder Diebstahl muss der Mitarbeiter eine gewisse Zeit warten, bis die neue Karte sowie die PIN ankommen – aus Sicherheitsgründen meist getrennt voneinander. Befindet sich die Person gerade wegen einer Messe oder ähnlichem im Ausland, macht es ihr das Arbeiten unmöglich. Aus diesem Grund setzen Unternehmen oft auf virtuelle Smart Cards als Backup.

Die virtuelle Karte nutzt den sicheren Speicher im PC. Dieser Secure Enclave funktioniert kryptografisch wie der physikalische Part einer Smart Card. Der größte Vorteil von virtuellen Smart Cards liegt vor allem darin, dass keine Kosten für den Erwerb von Karten oder die Bereitstellung der Infrastruktur anfallen – allein die Middleware ist von Bedeutung. Das macht virtuelle Smart Cards zu einer wichtigen Schutzmaßnahme für kleinere Unternehmen. Diese geraten immer mehr ins Visier von Hackern, verfügen aber häufig nicht über vergleichbare Ressourcen wie Großunternehmen.

Fazit

Ob strengere Richtlinien, raffiniertere Cyberbedrohungen oder mobiles Arbeiten, angesichts der zunehmenden Komplexität in der IT-Sicherheit müssen Organisationen zusätzliche Maßnahmen ergreifen. Smart Cards mit Zwei-Faktor-Authentisierung bilden hier eine fundamentale Schutzschicht und sichern kritische Unternehmenswerte effektiv und kosteneffizient ab.

Anton Kreuzer

EIN CUSTOMER IAM IST

GLEITENDE GRENZEN ZWISCHEN DEN USERKATEGORIEN SIND VON ZENTRALER BEDEUTUNG.

Schwerpunkt einer Customer IAM-Lösung (C-IAM) ist die Verwaltung einer hohen Anzahl von Identitäten, verbunden mit relativ einfachen Transaktionen.

Dies sind im Wesentlichen:

1. Eine Person wird sicher (erstmalig) identifiziert und in das System übernommen.
2. Ein User wird ebenfalls sicher gegen eine Identität im System authentifiziert.

(Mitarbeitern) eher prozessual und bei Externen (Kunden) eher einfach und transaktional sind. Außerdem sind zwischen diesen beiden Kategorien diverse Zwischenkategorien zu verwalten.

Zu berücksichtigen ist auch, dass es User in Doppelfunktionen gibt: Ein Mitarbeiter kann gleichzeitig Kunde seines Unternehmens sein, wie bei Herstellern, Banken und Versicherungen üblich.

Wenn es zwei getrennte IAM-Systeme gibt, entsteht zusätzlich das Problem der Synchronisation des User-Life-Cycle, welches in einem zentralen IAM selbstverständlich entfällt. Außerdem ist das zentrale Management der Anforderungen der DSGVO eindeutig einfacher und sicherer. Selbstverständlich lassen sich Übergänge zwischen den einzelnen Kategorien in einem zentralen System besser verwalten. So kann zum Beispiel eine Person ein

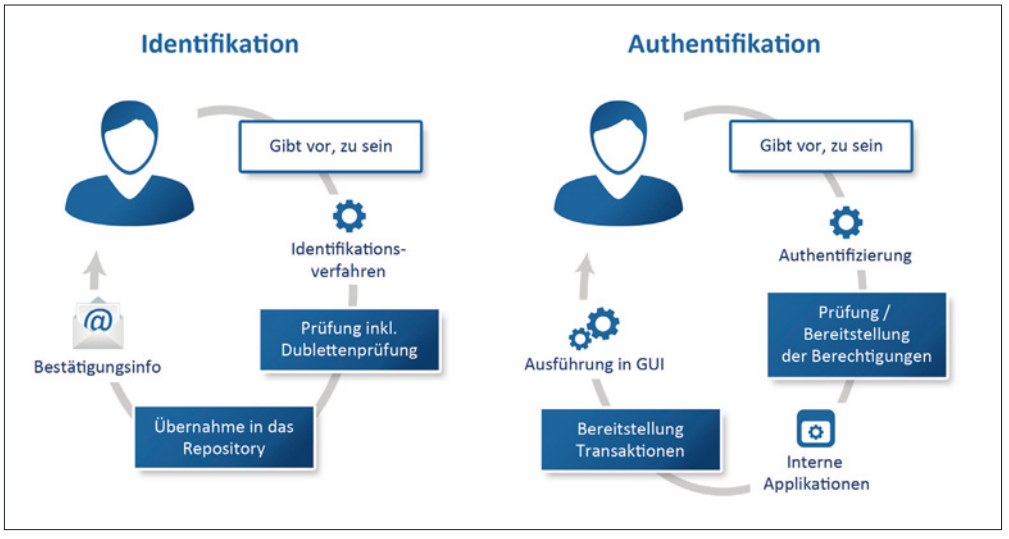


Bild 1:
Abläufe bei Identifikation und Authentifikation.

3. Der Identität werden die berechtigten Ressourcen bereitgestellt.

Deren Bereitstellung richtet sich nach der Risikoklasse des Users (basic, substantial, high / Security Classification = 3,4,5).

Zwischen den Userkategorien bestehen gleitende Grenzen

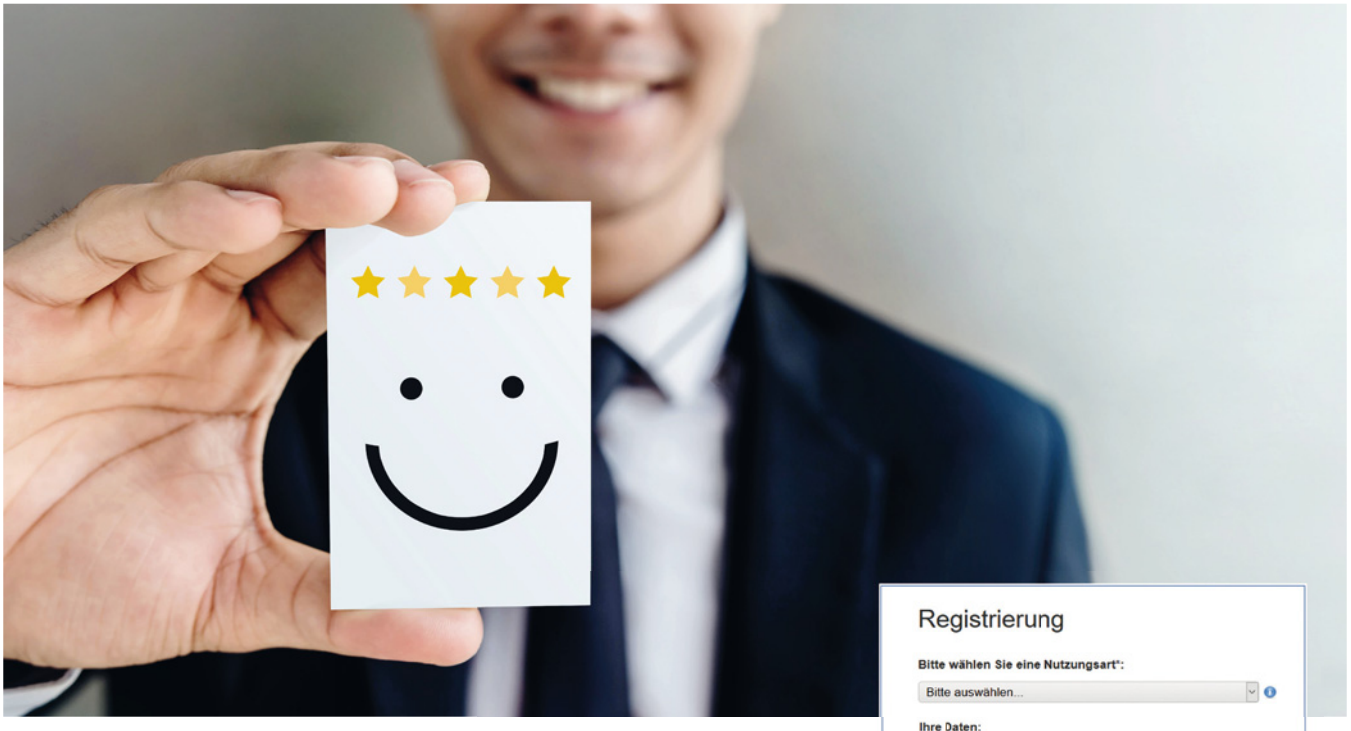
Der Ansatz, dass es ein separates C-IAM geben muss, ist aktuell zwar oft zu finden aber irreführend, da es genau genommen keine strenge Grenze zwischen internen und externen Usern gibt.

Unterschiedlich ist nur die Art der Übernahme in ein IAM sowie die userspezifischen Transaktionen, die bei Internen

	Usergruppe	Verwaltung in bi-Cube
intern	Interne User	Vertragsverhältnis mit dem Unternehmen – voll im Berechtigungsmodell verwaltet
	Externe User (direkt)	Vertragsverhältnis mit dem Unternehmen – voll im Berechtigungsmodell verwaltet
extern	Externe User (indirekt)	Juristisch eigenständige Einheiten – aber mit Berechtigungen in bi-Cube
	Kunden aus Vertrieb	Übernahme der User in bi-Cube
	Externe im Portalzugang (Kunden)	User mit Selbstregistrierung
	Regelmäßige Gäste	Beispiel: registrierte Gäste in der Kantine
	Temporäre Gäste	Kurzfristige Erfassung (Zutritt, WLAN, ...) – Beispiel: Schulungsteilnehmer

Bild 2: Klassifikation von Usern.

KEIN ANDERES IAM



Unternehmen als Besucher betreten und es dann als Bewerber oder Mitarbeiter wieder verlassen.

Trotz der gleitenden Übergänge zwischen den Userkategorien werden also grundsätzlich zwei Hauptgruppen unterschieden: interne und externe User.

Diese Userkategorien werden im IAM-Repository gleichwertig behandelt, unterscheiden sich aber in der Art ihrer Berechtigungen und der Komplexität der Transaktionen sehr deutlich.

Möglichkeiten des User-Managements

Im Kontext der C-IAM-Komponente eines IAM sind Kunden als Repräsentanten des „C" auf zwei Arten zu verwalten:

1. Sie sind als Identität im Unternehmen bereits bekannt (Kunden einer Bank) und wollen jetzt einen Portalzugang. In dieser Variante ist die Prüfung gegen die Bestandsdaten entscheidend.
2. Eine Person aus dem anonymen Raum meldet sich an. Dies sind dann in der Regel Kunden eines Online-Vertriebsportals.

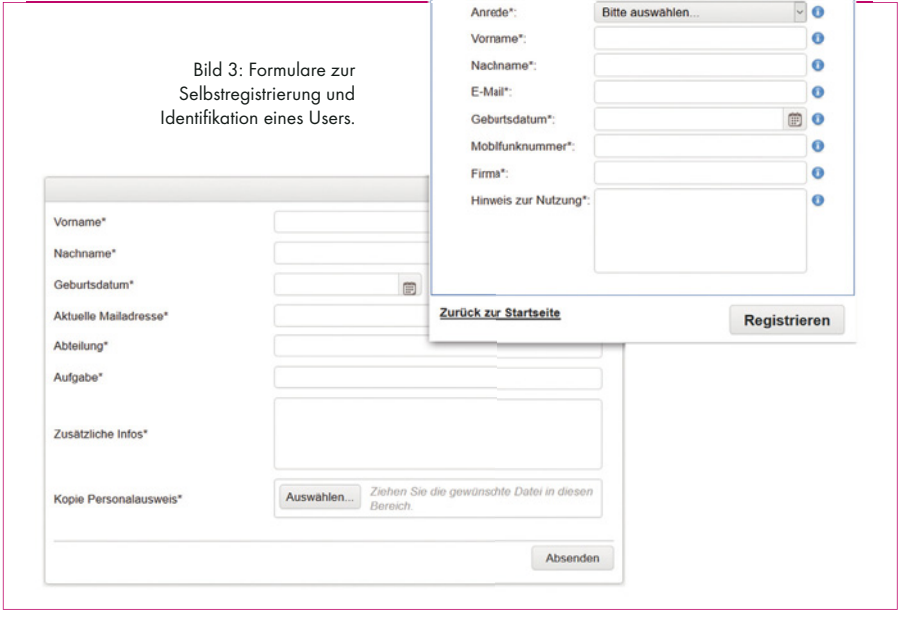


Bild 3: Formulare zur Selbstregistrierung und Identifikation eines Users.

Auch hier kann es Überdeckungen geben, die eine gemeinsame Verwaltung mit den internen Usern rechtfertigt. Solange ein Kunde auch Mitarbeiter ist, hat er im Vertriebsportal zum Beispiel einen Mitarbeiter-Rabatt, den er verliert, wenn er das Unternehmen verlässt, aber trotzdem Kunde bleibt. Der allgemeine Fall ist, dass sich eine Person der Selbstregistrierung bedient. Die Art der weiteren Verarbeitung ist dann unterschiedlich und abhängig vom gesamten Kontext der Verarbeitung der externen User.

Zu beachten ist auch, dass bestimmte Anwendungsrichtungen eines Kundenportals weitere Datenobjekte am User benötigen, die für interne User nicht erforderlich sind, zum Beispiel Rechnungs- und Lieferadressen.

Identifikation und Autorisierung

Die Komplexe „Identifikation" und „Autorisierung" sind in den C-IAM die im Schwerpunkt bereitgestellten Funktionen. Aus dem Bankenbereich kommen sehr sichere Verfahren wie Post-Ident, Video-Ident oder auch der Aktivierungsbrief.

In bi-Cube werden die drei Risikoklassen des Users (basic, substantial, high) mit leichter handhabbaren Verfahren abgebildet.

Je nach ausgewählter Nutzungsart und der damit verbundenen Risikoklasse wird das entsprechende Verfahren der Identifikation angewendet.

In der Authentisierung muss er entweder den Mobile Token oder den SMS-Token für die TFA nutzen.

Das Betreuungsteam der Externen im Unternehmen muss einen User der Klasse „substantial" explizit freigeben und ihm dann in der Regel eine Rolle zuordnen, die ihm die gewünschten Zugänge mit dedizierten Berechtigungen zu internen Funktionen freigibt.

Je nach Kontext und Anforderung kann dies auch automatisch erfolgen. Manuell ist aber in jedem Fall ein Externer der Klasse „high" zu bearbeiten (Prüfung der Identität anhand des Ausweises und Bereitstellung weiterer Informationen für den User).

thentifizierung ganz zu erlassen. User der beiden anderen Stufen werden dann beispielsweise zusätzlich aufgefordert, einen zweiten Faktor einzugeben.

Mengengerüst

Die beiden Hauptgruppen der User unterscheiden sich somit im Wesentlichen nur in der Anzahl zu verwaltender Identitäten, was ein leistungsfähiges IAM mit einer entsprechend skalierbaren System-Architektur beherrschen muss. Wesentlich ist dabei die effektive Verwendung der In-Memory-Technik. bi-Cube ist aktuell bei internen Usern bis in den Bereich von 0,5 Mio. praktisch im Einsatz und für bis zu 1 Mio. interner User im Test freigegeben. Für den Bereich der externen User (C-IAM) ist bi-Cube bis 10 Mio. freigegeben. Da in bi-Cube die beiden Usergruppen nur formal getrennt sind, ist bi-Cube ein sogenanntes globales oder generelles IAM (G-IAM). Das Attribut „generell" ist erst dann angebracht, wenn wie in bi Cube die Breite der Funktionalität bis in den Bereich Enterprise Service Management (ESM) ausgedehnt ist.

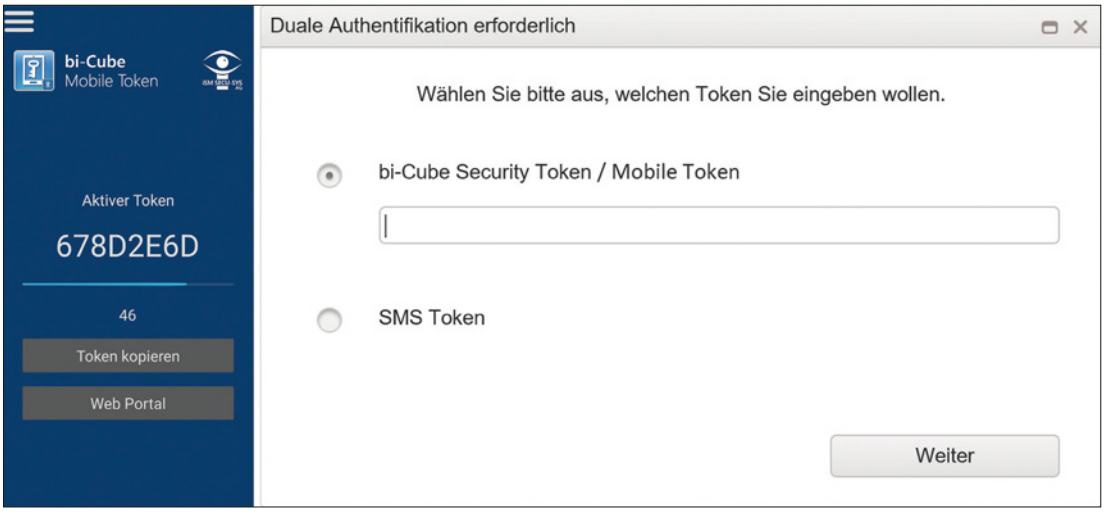


Bild 4: Duale Authentifikation in bi-Cube.

§ basic
Hier ist es ausreichend, dass der User die Selbstregistrierung nutzt. Er wird dann automatisch in einer speziellen Organisationseinheit angelegt, erhält seine Zugangsdaten per Mail oder SMS.

§ substantial
Bei dieser Einordnung erhält der User eine Bestätigungsinfo auch per Mail oder SMS. Die Aktivierung des Links wird als Bestätigung der Identität gewertet.

§ high
Hier muss der externe User die Kopie seines Ausweises beifügen. Nach Prüfung der Namensangaben, wird der User übernommen.

Verdeckte Two-Factor-Authentication (TFA)

bi-Cube ermöglicht dem User nach Einrichtung des Mobile Token für den Aufruf der App bi-Cube GO eine verdeckte TFA, da er nur noch seine Credentials (UserID /PW) eingeben muss und dann durch bi Cube im Hintergrund die registrierte Geräte-ID abgefragt wird. In dieser Konstellation ist die Geräte-ID der zweite Faktor.

Integration des ID-Providers

Der bi-Cube interne ID-Provider kann genutzt werden, um dem Basic-User die Au-

Zusammenfassung

Die Analyse der Produkte, die unter dem Begriff C-IAM firmieren, hat ergeben, dass diese nur eine spezifische Ausprägung (Teilmenge) der Funktionalitäten eines leistungsfähigen IAM bereitstellen.

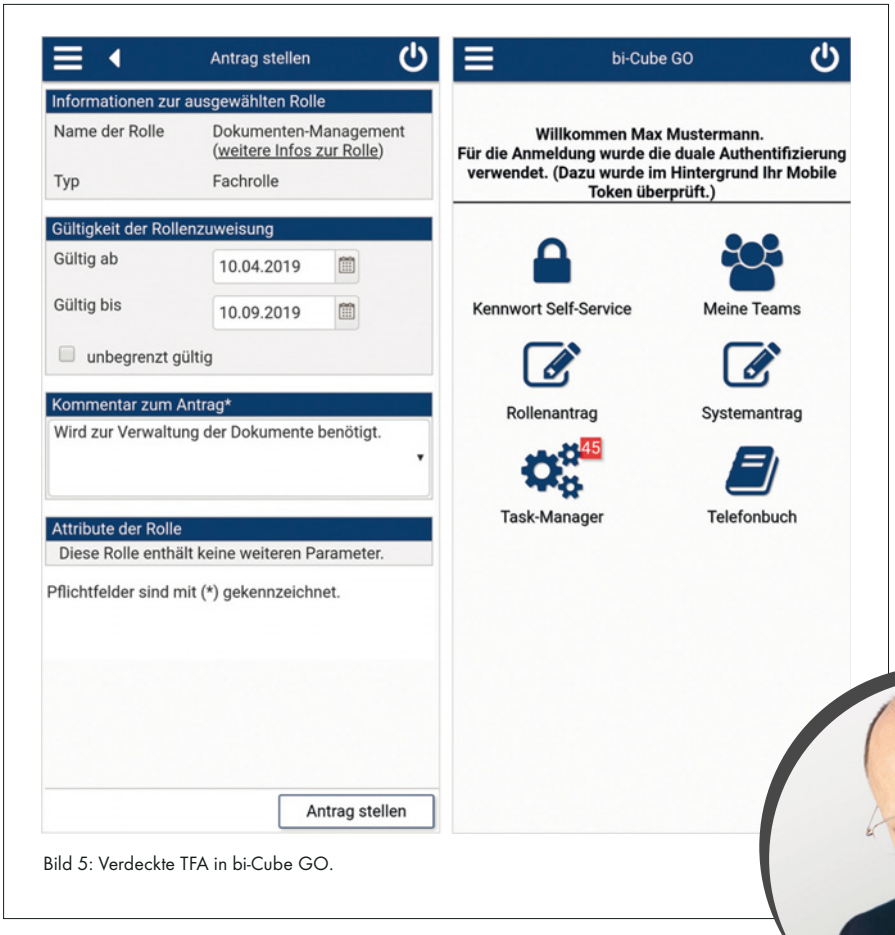


Bild 5: Verdeckte TFA in bi-Cube GO.

Es ist wenig sinnvoll, neben einem IAM für die internen Mitarbeiter ein zweites zu etablieren, das beispielsweise die Kunden verwaltet. Dieses C-IAM muss dann natürlich auch viele interne Mitarbeiter kennen, was eine doppelte Verwaltung dieser Personen sowie parallele Schnittstellen (Connectoren) zu Applikationen der Kunden bedingt.

Ein übergreifendes Reporting ist bei zwei IAM-Lösungen ebenfalls deutlich erschwert. Demnach ist es unbedingt empfehlenswert, bei der Auswahl eines IAM auch dessen C-IAM-Fähigkeiten in die Prüfung miteinzubeziehen.

Prof. Dr. Dr. Gerd Rossa

> ES IST WENIG SINNVOLL, NEBEN EINEM IAM FÜR DIE INTERNEN MITARBEITER EIN ZWEITES ZU ETABLIEREN, DAS BEISPIELSWEISE DIE KUNDEN VERWALTET.
>
> Prof. Dr. Dr. Gerd Rossa,
> CEO iSM Secu-Sys AG
> www.secu-sys.de

LOGICALIS
Business and technology working as one

Die Angreifer lauern schon

Schützen Sie jetzt Ihre Endgeräte!

- » Intelligentes Erkennen und Beseitigen
- » Komplett plattformunabhängig
- » Keine Installation notwendig

Kostenloser Ratgeber auf www.logicalis.de