itmanagement

MÄRZ 2019

MAGAZIN FÜR DIE ENTERPRISE IT

SERVICE MESH THOUGHT LEADERSHIP

SERVICEZENTRIERTE ORGANISATION

SO GELINGT DAS PROJEKT

José Silva, Hamburg Süd Group

\+

INKLUSIVE 32 SEITEN
IT SECURITY SPEZIAL

AGILES ENTERPRISE ARCHITECTURE MANAGEMENT

Katalysator für die Digitale Transformation

25 JAHRE IT MANAGEMENT

Visionen, Utopie oder Realität?

NACH DEN DEVOPS KOMMEN DIE DATAOPS

Sicherheit und Datenmodernisierung

www.it-daily.net

LOGICALIS
Business and technology working as one

Ihr digitaler Wegbereiter

- Clevere Lösungen für IT-Sicherheit, Netzwerke & Collaboration
- Modernes Datenmanagement und Business Intelligence
- Zukunftsweisende Data Center Technologien & nahtlose Cloud Integration

www.logicalis.de

25 JAHRE IT MANAGEMENT – HAPPY BIRTHDAY

Liebe LeserInnen,
wie die Zeit vergeht. Im März 1994, pünktlich zur damaligen Welt-Leitmesse CeBIT, kam die erste Ausgabe von it management auf den Markt. Die CeBIT ist mittlerweile Vergangenheit, aber die it management erfreut sich nach wie vor Ihrer Gunst und das nach wie vor auch als Printmagazin.

Als wir seinerzeit auf den Markt kamen, wurden wir von vielen müde belächelt, war es doch das erste Magazin, das ein „IT" im Titel führte. Ein Novum für die damalige EDV-Welt und, auch das neu, das Informationen für die erste Ebene der IT/EDV-Entscheider lieferte.

Im Heft finden sie einen Rückblick auf die letzten 25 Jahre und einen Ausblick was IT-Hersteller die nächsten 25 Jahre erwarten. Wird es eine Vision, Utopie oder Realität? Und wird die Innovationsgeschwindigkeit anhalten? Wie meistern wir den Personalmangel, Stichwort Generationenwechsel? Was wird mit den Kosten? Und wie entwickelt sich die Cyber Security? Darüber berichten wir, dann retrospektiv, in 25 Jahren.

Was unser Magazin betrifft, so gibt es heute nicht nur ein breiteres Themenspektrum, sondern zusätzlich zur Evolution im Druckereigewerbe (Fotosatz, Belichtung, DTP, Computer-to-plate) die digitalen Medien (Website, eBooks, Newsletter). Diese finden sie bei uns gebündelt auf https://www.it-daily.net/ .

Im Vorjahr haben wir mit einem neuen Layout, der Adaption unseres CIs, einer verbesserten Papierqualität und einem erweiterten Umfang Maßstäbe gesetzt. 2019 haben wir mit der Ausgabe 1/2 neu die Rubrik „Thought Leadership" eingeführt und begonnen, Print & Online unsere Content-Strategie konsequent umzusetzen. Bleiben sie uns also treu, denn eines kann ich Ihnen schon heute versprechen: Der Innovationsschub wir sich auch 2020 weiter fortsetzen!

Herzlichst Ihr

Ulrich Parthier
Publisher it management

INHALT

IT MANAGEMENT

eBUSINESS

THOUGHT LEADERSHIP

IT INFRASTRUKTUR

Inklusive
32 Seiten

IT SECURITY SPEZIAL

ERP UND INDUSTRIE 4.0.

HERAUSFORDERUNGEN UND LÖSUNGEN.

Die einen vergleichen Industrie 4.0-Projekte mit einem Marathon, für andere Unternehmen gestaltet sich die Digitalisierung eher als Hindernislauf. Dabei bewertet jeder Betrieb die Anforderungen ganz unterschiedlich. Das Analystenhaus PAC befragte dazu im Sommer 2018 über 100 IT-, Produktions-, Fertigungs- und Einkaufsleiter.

1 Mit SOA gegen Silos
Als besonders große Hürde empfinden 68 Prozent der Studienteilnehmer die Integration vieler verschiedener Systeme und Daten. Um diese Hürde zu nehmen, bringen moderne ERP-Systeme zahlreiche Ansatzpunkte mit – allen voran die Integrationsmöglichkeiten über einen Enterprise Service Bus. Eine solche serviceorientierte Architektur (SOA) macht den mandanten-, system- und sogar unternehmensübergreifenden Datenaustausch spürbar effizienter.

2 Von Hand zu Hand zu Hand
Manuelle Arbeitsgänge sind sowohl in der Produktion wie im kaufmännischen Bereich oft immer noch die Norm. Die durchgängige Digitalisierung von Abläufen stellt daher 67 Prozent der Unternehmen vor eine große Herausforderung. Ein Workflow-Management kann hier helfen.

3 Alteisen smart gemacht
Viele IT-Leiter zerbrechen sich den Kopf, wie sie ältere Maschinen und Anlagen mit dem ERP-System als Steuerzentrale vernetzen. Knapp die Hälfte der Teilnehmer an der PAC-Studie sah dies als große Herausforderungen für sich. Dabei gibt es bereits erste, vielversprechende Pilotlösungen: etwa, indem ein Minirechner zwischen Maschine und ERP geschaltet wird.

4 Wer rastet, der rostet
Jeder Manager weiß, dass er seinen Bereich, und damit die Abläufe, ständig weiterentwickeln muss. Für 42 Prozent der Unternehmen sind jedoch die Neukonfiguration der bestehenden Prozesse oder die Entwicklung neuer Abläufe ein Spießrutenlauf. Branchenspezifische ERP-Lösungen und leicht konfigurierbare Anwendungen schaffen hier Abhilfe.

5 Mitarbeiter zu Leistungsträgern machen
Das modernste und leistungsstärkste ERP-System ist nur so gut wie das Team, das damit arbeitet. Mangelhafte ERP-Kenntnisse bremsen ihre Digitalisierung. Umfangreiche Schulungen für die verschiedensten Bedarfe, vom Poweruser bis zum Management-Reporting, führen nur eingeschränkt zum Erfolg.

www.proalpha.de

DIGITALISIERUNG

MASSNAHMEN FÜR DEN ERFOLG.

Mit diesen Maßnahmen schaffen viele Unternehmen die Voraussetzung für den Einsatz intelligenter Technologien wie Machine Learning, Bilderkennung oder Natural Language Processing.

Wieder haben 99,4 % aller

ACMP-Kunden ihre Lizenzen verlängert!

Lizenzmanagement - Softwareverteilung - OS Deployment - Inventarisierung - Helpdesk - Patchmanagement - Asset Management - Lizenzmanagement - Softwareverteilung - OS Deployment - Inventarisierung - Helpdesk - Patchmanagement - Asset Management - Lizenzmanagement - Softwareverteilung

Clientmanagement ist Vertrauenssache!

www.aagon.de

Aagon

DATENMANAGEMENT

DER OPTIMALE NUTZEN.

Die Möglichkeit, Daten durch Embedded Analytics zu monetarisieren und neue datenbasierte Dienstleistungen anzubieten, steigert die Wertschöpfung deutlich und ermöglicht, das enorme Potenzial von Data Analytics besser zu erschließen. Einige der aktuellen Technologien kommen erst nach und nach in verschiedenen Anwendungsszenarien in den Bereichen Analytik und Datenmanagement zum Einsatz.

1. Umfassende unternehmensweite Analytik. Die Nachfrage aus den Fachabteilungen nach einem effizienteren Datenmanagement und einer Data Value Chain, die entscheidungsrelevante Informationen bereitstellt, steigt weiter rasant an. Erfolgreiche Unternehmen kombinieren Aktivitäten und Komponenten in einer abteilungsübergreifenden und unternehmensweit skalierbaren Analytics-Strategie.

2. Es stehen immer mehr Daten für Analysen bereit. Mit dem zunehmenden Einsatz von intelligenten Wearables, beispielsweise im Gesundheitswesen oder für den persönlichen Gebrauch, entstehen umfangreiche Ökosysteme, die Verbrauchern, aber auch spezialisierten Dienstleistungsunternehmen wichtige Erkenntnisse über Zuverlässigkeit, Sicherheit und Gesundheit liefern.

3. Konvergenz von Technologien. Unternehmen können immer größeren Datenmengen erschließen, analysieren und aufbereiten. Damit schaffen sie eine leistungsstarke Grundlage, um von hier aus weiteren Benutzergruppen innerhalb sowie außerhalb der eigenen Organisation einen sicheren Zugriff zu gewähren und neue handlungsrelevante Einblicke zu ermöglichen.

4. Ausbau von Embedded Analytics. Der Einsatz von Embedded Analytics wird sich an der Konvergenz anderer Schlüsseltechnologien für Datenanalysen ausrichten, da mehr Unternehmen KI und Machine Learning einsetzen, um auf Basis einer fundierten Data Value Chain ihre Prozesse zu optimieren und effizienter zu steuern.

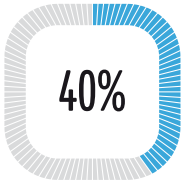
5. Verbesserter Datenschutz und höhere Datensicherheit. Regierungen und Unternehmen werden noch stärker als bislang gefordert sein, persönliche und vertrauliche Daten vor unbefugtem Zugriff zu schützen und zu definieren, was öffentlich zugänglich sein darf.

www.informationbuilders.de

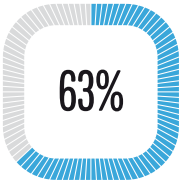
HERAUSFORDERUNG

IT-SICHERHEIT

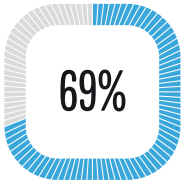
Befragung von deutschen IT- und Sicherheitsentscheidern.



fühlen sich innerhalb ihres eigenen Unternehmens isoliert.



nennen interne Kommunikation als größte Herausforderung für die Cybersicherheit.



erleben, dass die interne Kommunikation nach Vorfällen, wie WannaCry für sie einfacher wird.


WE LEAD
TRANSFORMATION
Unlock the Power of SAP® S/4HANA with SNP´s BLUEFIELD™ Approach.
BLUEFIELD™
25
YEARS
www.snpgroup.com
SNP

SERVICEZENTRIERTE ORGANISATION

SO GELINGT DAS PROJEKT.

Die Digitalisierung von Services ist eine große Herausforderung für alle Unternehmen. Traditionelle Strukturen müssen dabei oft neuen, fortschrittlichen Ansätzen weichen. Über die Erfahrungen bei der Entwicklung der IT hin zu einer servicezentrierten Organisation sprach it management-Herausgeber Ulrich Parthier mit Jose Silva, Manager Service Portfolio & Catalogue Management bei der Hamburg Süd Group.

? **Ulrich Parthier:** *Mehr Serviceorientierung ist ja an sich ein positives Ziel, scheitert aber oft. Können sie uns an einem positiven Beispiel zeigen, wie man strategisch vorgehen muss?*

Jose Silva: Die Schifffahrt ist ein persönliches Geschäft und die Hamburg Süd steht für den Personal Touch in der Containerschifffahrt. Gleichzeitig ist das Geschäft ohne IT nicht denkbar. Angesichts veränderter Märkte und der Digitalisierung in der Schifffahrt sehen wir es als erforderlich an, die IT in eine serviceorientierte Organisation zu transformieren. Dazu ist es nötig, IT-Dienstleistungen transparent zu machen und Services bedarfsgerecht anzubieten. Damit einher geht unter anderem die Entwicklung und Etablierung neuer Rollen (Service- Portfolio Manager/Service-Owner) und die Standardisierung von Servicemanagement-Prozessen mit Hilfe einer zentralen ITSM-Lösung.

? **Ulrich Parthier:** *Die IT-Prozessautomatisierung ist ein Schlüssel beim Aufbruch hin zu einer serviceorientierten Organisation. Können Sie etwas zur IT-Infrastruktur sagen, die Sie vorgefunden haben? Über wie viele Services und Softwarepakete sprechen wir?*

Jose Silva: Die IT-Landschaft ist wie bei vielen Unternehmen dieser Größenordnung komplex. Insgesamt haben wir aktuell 55 Services, bestehend aus circa 180 technischen Services und etwa 380 Software-Paketen untersucht und transformiert. Und wir sind noch lange nicht am Ziel! Dies ist erst der Anfang.

? **Ulrich Parthier:** *Es war hier bereits der dritte Anlauf. Ein solches Projekt ist ja kein Selbstläufer. Was waren Fehler bei den ersten Versuchen und wie setzt man erfolgreich ein kundenzentriertes Geschäftsmodell um?*

Jose Silva: Der Aufbau einer serviceorientierten Organisation gelingt nicht allein durch Strategie und Technik. Das musste die IT der Hamburg Süd erfahren, die bereits 2008 versuchte, Services zu definieren und bedarfsgerecht anzubieten. Die Analyse ergab, dass nicht nur eine vollständige Beschreibung der einzelnen Services fehlte, sondern auch das aktive Einbinden aller Stakeholder nicht erfolgt war. Mit einem neuen Team und einem neuen Ansatz wurde ab 2014 ein weiterer Anlauf unternommen, das „Service-Gen" innerhalb der Organisation zu aktivieren und jenseits von Silos und Hierarchien neue Rollen und Prozesse zu etablieren. Hierzu verfeinerte das Projektteam das bestehende Service-Modell und detaillierte Service-Beschreibungen und Abhängigkeiten. Parallel dazu arbeitete man die Rollen „Service Owner" und „Service Element Owner" weiter aus. Ein wichtiges Erfolgskriterium hierbei war, dass die betroffenen Kollegen an der Gestaltung aktiv beteiligt waren und ihre Hinweise und Bedürfnisse weitestgehend berücksichtigt wurden.

? **Ulrich Parthier:** *Auf welche Herausforderungen sind Sie bei dem Projekt gestoßen?*

Jose Silva: Als größte Herausforderung erwies sich die Akzeptanz der Führungskräfte, die in der klassischen Organisationsstruktur bislang Verantwortung trugen. Denn die neuen Querschnittsrollen verfügen über umfangreiche Befugnisse zur Durchsetzung ihrer Services, die mit den Interessen der bisherigen Linienorganisationen in der IT unter Umständen kollidierten.

Aktuell liegt die Budgethoheit noch in der Linie – sie wird von den Service Ownern aber immer stärker eingefordert. Für die Beschreibung der Rollen nutzte man zunächst die Darstellungen bei ITIL und formte diese nach Interviews mit den internen Kunden, allen betroffenen Mitarbeitern und den künftigen Service-Ownern so, dass es für die spezifische Situation bei Hamburg Süd passte. Zur optimalen, kundenzentrierten Bereitstellung eines Service waren abteilungsübergreifende Kompetenzen und das Führen interdisziplinärer Teams erforderlich. Durch flankierende Marketingaktivitäten und dem ständigen Dialog mit allen Beteiligten gelang es sukzessive, die benötigten Services konkret zu definieren und die Rolle des Service-Owners zu etablieren.

? **Ulrich Parthier:** *Welche Projekt-Meilensteine haben sie festgelegt?*

Jose Silva: Wir haben sieben Punkte bei der Hamburg Süd definiert:

1. Die Entwicklung eines Service-Modells.
2. Die Tool-Evaluierung, die zugunsten von USU Valuemation entschieden wurde.
3. Die Situationsanalyse und das Beschreiben der Services für den Service-Katalog.
4. Die Implementierung des Tools Valuemation.
5. Die Inbetriebnahme des Online-Service-Katalogs und das zeitnahe Bereitstellen von Services im Service Shop für den Nutzer (Mehrwert).
6. Die Einführung von Querschnittsrollen für einzelne Services (Service Portfolio Manager, Service Owner und Service Element Owner).

7. Der sukzessive Aufbau weiterer Disziplinen, etwa Service Portfolio Management oder SLA- Management.

Ulrich Parthier: *Welchen Nutzen hat das Unternehmen von der Einführung erwartet?*

Jose Silva: Hier waren für Hamburg Süd fünf Kernziele von Bedeutung:

1. Die IT wird als Treiber für den „Mind Change" in Richtung einer serviceorientierten Organisation sichtbar.
2. Die Transparenz über die Vielfalt vorhandener Software und deren Einsatz spart Betriebsmittel und Lizenzkosten, unter anderem durch die Abschaffung redundanter Software.
3. Minimierte Durchlaufzeiten durch (teil-)automatisierte, benutzerfreundliche Bestellvorgänge
4. Höhere Kundenzufriedenheit mit dem IT-Service
5. Effiziente IT-Services wirken als Blaupause für Enterprise-Services für HR und Facility Management.

Ulrich Parthier: *Warum wurde gerade USU Valuemation für das Projekt ausgewählt?*

Jose Silva: Das USU-Produkt Valuemation wurde ausgewählt, weil es sämtliche ITIL-Prozesse abbildet und über eine hohe Flexibilität sowie Integrationsfähigkeit verfügt.

Die erfolgreiche Realisierung vieler ähnlich komplexer Kundenprojekte beweist die Leistungsfähigkeit des Unternehmens. Neben der Technologie überzeugt USU durch Flexibilität, Servicebereitschaft und umfassende Beratungsexpertise.

Ulrich Parthier: *Welches war in diesem Fall das richtige Erfolgsrezept bei der Umsetzung?*

Jose Silva: Unser Ansatz lautete, einen Servicekatalog als Basis der Service-Orientierung einzuführen. Transparenz zu schaffen, war ein zentrales Ziel aller Projektbeteiligten. Dem zuvor vorhandenen Wildwuchs wurde „der Kampf angesagt". Durch die aktive Einbindung von HR und Betriebsrat gelang es, eine Betriebsvereinbarung zur Nutzung von Software abzuschließen, die in den Anforderungs- und Bestellprozess integriert ist. Durch die Abschaffung redundanter Software spart Hamburg Süd heute hohe Software-Lizenzkosten.

Nachdem alle derzeit ermittelten 55 Services aus der Perspektive des Endkunden in einer einheitlichen Struktur beschrieben waren, konnten Optionen über einen Online-Service-Katalog auf Basis von Valuemation bereitgestellt werden. Durch den Service-Katalog werden heute etwa 70 Prozent aller Service Requests abgedeckt. Bei der Bestellung kostenpflichtiger Produkte ist ein automatisierter Genehmigungsprozess zwischengeschaltet. Lizenzpflichtige Software wird in circa 72 Stunden geliefert. Bei Software, die nicht lizenzpflichtig ist, beginnt die Installation innerhalb von 24 Stunden. Unser nächstes Ziel (Projekt bereits gestartet) ist eine vollautomatisierte Umsetzung der Auslieferung von Software.

Ulrich Parthier: *Was konnten sie in puncto Kundezufriedenheit erleben?*

Jose Silva: Durch die kollaborative Vorgehensweise, den bedarfsgerechten Aufbau und die nutzerfreundliche Bedienung des IT-Shops sowie die beschleunigten Bestellprozesse stieg die Kundenzufriedenheit in den Fachabteilungen signifikant. Damit ist die Basis für die Umsetzung weiterführender Prozesse geschaffen, etwa den Aufbau eines Service-Portfolio-Managements oder die Einführung von SLA-Management.

> DER AUFBAU EINER SERVICEORIENTIERTEN ORGANISATION GELINGT NICHT ALLEIN DURCH STRATEGIE UND TECHNIK. ALS GRÖSSTE HERAUSFORDERUNG ERWIES SICH DIE AKZEPTANZ DER FÜHRUNGSKRÄFTE, DIE IN DER KLASSISCHEN ORGANISATIONSSTRUKTUR BISLANG VERANTWORTUNG TRUGEN.
>
> Jose Silva, Manager Service Portfolio & Catalogue Management bei der Hamburg Süd Group

Ulrich Parthier: *Herr Silva wir danken für dieses Gespräch.*

ORGANISATORISCHE HERAUSFORDERUNGEN

ENTWICKLUNG EINER SERVICEZENTRIERTEN IT-ORGANISATION.

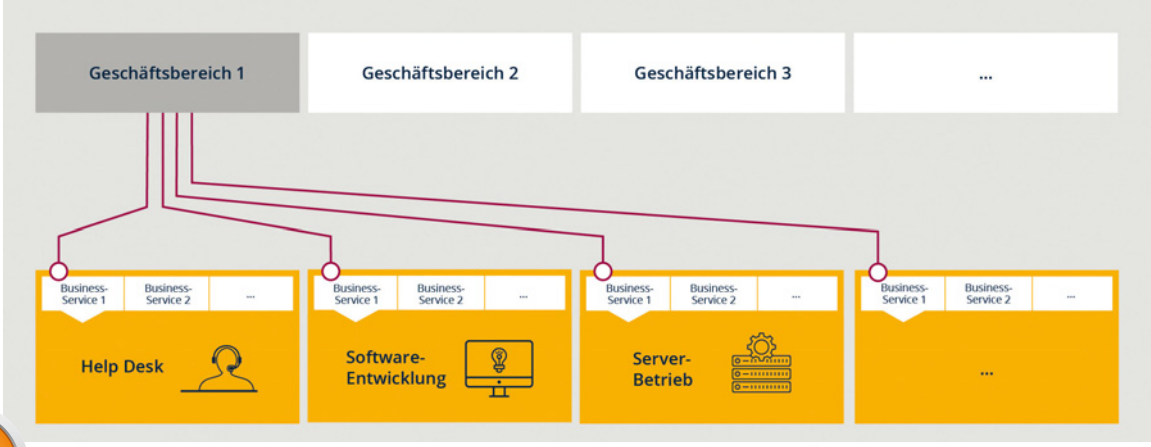


Bild 1: Aufbau einer traditionellen IT-Organisation.

Whitepaper:
Dieser Artikel ist ein Auszug aus einem umfangreichen Whitepaper, das hier heruntergeladen werden kann: http://bit.ly/serv_zent_orga_itm

Bei vielen IT-Organisationen steht der „Service" als zentrales Objekt zur Definition und Strukturierung ihres Angebots noch nicht im Mittelpunkt. Der Aufbau eines Servicekatalogs ist dann ein erster Schritt in diese Richtung. Der Übergang von einer infrastrukturgetriebenen zu einer servicezentrierten IT-Organisation ist aber ein längerer Prozess, der nicht nur Änderungen bei den eingesetzten Tools mit sich bringt, sondern auch Veränderungen in der Aufbau- und Ablauforganisation erfordert.

Dieser Fachartikel ist ein Auszug aus einem umfangreichen Whitepaper des Geschäftsbereichs Valuemation der USU GmbH. Er beschreibt die notwendigen organisatorischen Veränderungen und auch Erfolgsfaktoren, die in praktischen Projekten bei der Einführung einer servicezentrierten IT-Organisation gewonnen wurden.

Die traditionelle IT-Organisation

In traditionellen IT-Organisationen steht die eingesetzte Infrastruktur im Mittelpunkt, nicht der Business-Service für die Kunden. Dabei beziehen die Kunden aus den Geschäftsbereichen keine vereinbarten Business-Services von der IT, sondern einzelne Leistungskomponenten (siehe Bild 1).

So kauft zum Beispiel der Kunde für den Betrieb einer Business-Applikation den Applikations-Server, die Datenbank, den Storage-Bereich und Help-Desk-/Support-Leistungen bei den jeweiligen IT-Abteilungen ein. Notwendige funktionale Änderungen bespricht und plant er mit der Entwicklungsabteilung. Der Betrieb der Infrastrukturkomponenten erfolgt häufig nach dem „Best Effort"-Prinzip, das heißt die IT liefert nach bestem Bemühen, aber ohne garantierte Liefer- oder Verfügbarkeitszeiten. Diese Vorgehensweise erfordert einen großen IT-Sachverstand auf Seiten der Geschäftsbereiche, um im Dialog mit der IT deren Sprache zu verstehen und die benötigte Infrastruktur gemäß den eigenen Business-Anforderungen auswählen zu können. Die Verrechnung der IT-Kosten an die Geschäftsbereiche erfolgt häufig in vielen technischen Einzelpositionen, die nicht einer Applikation oder einem Service zugeordnet werden. Der Vergleich von Leistung und Preis der intern bezogenen Services mit dem Angebot externer Service-Provider ist für die Geschäftsbereiche somit erschwert.

Die servicezentrierte IT-Organisation

Bei einer servicezentrierten IT-Organisation steht der zu erbringende Service an der direkten Schnittstelle zum Kunden im Mittelpunkt der Betrachtung (siehe Bild 2).

Die Dienstleistungen der IT werden in sogenannten „Business-Services" gebündelt, bei denen die qualitativen und quantitativen Leistungsversprechen (SLAs) in der Sprache der Geschäftskunden beschrieben sind. Der Business-Service beschreibt also eine Leistung, ohne auf die dafür notwendige Infrastruktur einzugehen – er wird somit zum Vermittler zwischen Kunde und Dienstleister. Für die Geschäftskunden hat diese Organisation den großen Vorteil, dass sie sich auf ihre Business-Anforderungen konzentrieren können und sich nicht mehr mit den für einen Service notwendigen technischen Komponenten beschäftigten müssen. Die Servicekosten variieren mit Abnahmemengen und Qualitätsansprüchen. Die Geschäftsbereiche haben somit die Möglichkeit, Ihre IT-Kosten gemäß betriebswirtschaftlicher

Randbedingungen zu steuern. Das führt grundsätzlich zu einer Erhöhung der Kundenzufriedenheit im Verhältnis von Business und IT.

Für die IT hat diese Serviceorientierung den großen Vorteil, dass alle ihre Leistungen unmittelbar einem oder mehreren Business-Services und damit einem Geschäftszweck zugeordnet werden. Dies unterstützt die Motivation der IT-Mitarbeiter, die hier ihren persönlichen Beitrag am Geschäftserfolg erkennen können. Außerdem wird alles, was nicht wirtschaftlich notwendig ist, künftig unterlassen. Mittelfristig ist die Standardisierung von Business-Services häufig der Anstoß, auch die (internen) technischen Services erst zu standardisieren und dann zu automatisieren.

Die so entstehenden Einsparpotenziale schaffen den dringend benötigten Freiraum für die IT, um sich proaktiv mit neuen Serviceideen als Innovator bei den Geschäftsbereichen zu positionieren. Der Übergang von einer infrastrukturgesteuerten hin zu einer servicezentrierten IT-Organisation ist mit organisatorischen Änderungen verbunden. Zentrale Rollen sind dabei der Service-Manager, der Service-Owner und das Service-Team.

- **Die Rolle des Service-Managers**
  Die Aufgaben des Service-Managers umfassen die Pflege der Kundenbeziehung (Business Relationship Management) und die Steuerung der Service-Level. Er ist der erste Ansprechpartner für den Kunden in der Serviceorganisation und vertritt dessen Interessen im Zusammenhang mit den vereinbarten Service Level Agreements. Außerdem steuert er das Service-Portfolio.

- **Die Rolle des Service-Owners**
  Neben dem Service Manager ist der Service-Owner eine der wichtigsten Rollen in einer servicezentrierten Organisation. Er ist verantwortlich die Services und stimmt sich dabei eng mit dem Service Manager und dem Service-Team ab.

- **Die Rolle des Service-Teams**
  Das Service-Team wird interdisziplinär zusammengestellt und vom Service-Owner gesteuert. In dem Team arbeiten sowohl direkt mit der Service-Erbringung betraute Rollen als auch – ggfs. temporär – Mitarbeiter aus unterschiedlichen Bereichen. Es ergibt sich eine Matrix-Organisation, in der z. B. eine für den Serverbetrieb verantwortliche Personen sowohl einem Service-Team zugeordnet ist (vertikale Zuordnung) also auch der für den Serverbetrieb verantwortlichen IT-Abteilung (horizontale Zuordnung).

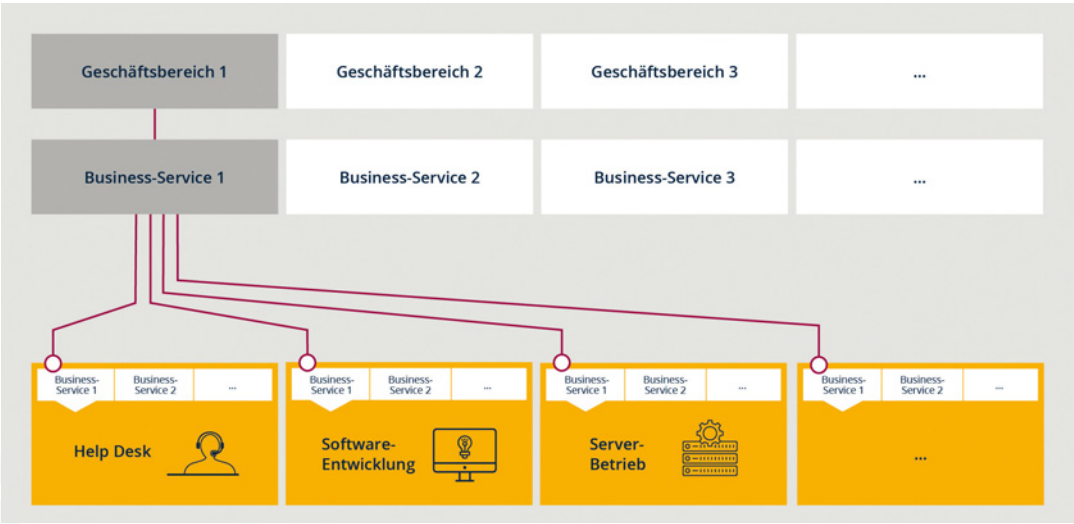


Bild 2: Aufbau einer servicezentrierten IT-Organisation.

Zehn Erfolgsfaktoren für den erfolgreichen Übergang

Aus verschiedenen Projekten und Interviews mit Experten ergeben sich zehn Erfolgsfaktoren zur Einführung einer servicezentrierten Organisation:

1. Die Kunden und deren Services in den Mittelpunkt alle Aktivitäten stellen
2. Messbare Ziele für das Change-Projekt definieren
3. Die Unterstützung des Managements sicherstellen
4. Standards für Begriffe, Abstimmungen und Prozesse definieren
5. Eine anerkannte Leitfigur als Projektleiter einsetzen
6. Leuchtturmprojekte anstoßen und Erfolge feiern
7. Den Change-Prozess aktiv managen
8. Lessons-learned-Prozess aufsetzen
9. Das Service-Portfolio unter Einbeziehung von IT und Business managen
10. Wissensaustausch horizontal und vertikal organisieren

Fazit

Zur Einführung einer servicezentrierten IT-Organisation ist die Bereitstellung eines Servicekatalogs häufig der erste Schritt. Man wird dann aber sehr schnell feststellen, dass zur konsequenten Umsetzung der Serviceorientierung auch die Organisationsform innerhalb der IT verändert werden muss. Verantwortlichkeiten müssen aus den horizontalen Technologie-Silos der IT in die vertikalen Servicestrukturen verlagert werden. Neue Rollen wie zum Beispiel Service-Manager und Service-Owner entstehen und werden mit umfangreichen Kompetenzen ausgestattet. Dieser Prozess dauert mehrere Jahre. Wichtig dabei ist die schrittweise Umsetzung in Leuchtturmprojekten, das Vermarkten von Erfolgen und das Treiben durch eine im Unternehmen anerkannte Leitfigur. Letztlich gewinnen mit dieser Entwicklung beide Seiten – sowohl die Geschäftskunden als auch die IT selbst.

Stefan Kuhardt, José Silva, Dr. Horst Tisson
www.usu.de

DIE SERVICE MESHS SIND DA

2015 PROGNOSTIZIERT, HEUTE IM KOMMEN.

Die Service Meshs sind da. Gartner hatte sie bereits 2015 auf seinem Radar; als neunten von 10 Trends nannten die Analysten seinerzeit Mesh App and Service Architecture.

Auch in einer weiteren Prognose für 2018 taucht der Begriff Mesh wieder auf, wenn auch in einem anderen Kontext. Seitdem hat sich schrittweise eine Community in diesem Marktsegment entwickelt. Einen Thought Leader kann man hier noch nicht sehen, jedoch bilden sich technologische Plattformen heraus, die marktführend sind.

Unternehmen wie Buyoyant oder Istio treiben das Konzept der Service Meshs in einem entstehenden Ecosystem voran. Gerade im Open-Source-Bereich ist Kubernetes zwar zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von Container-Anwendungen eine feste Größe. Aber wenn es beispielsweise um komplexe Websites geht, stellt Kubernetes zwar einige wichtige Ressourcen zur Verfügung. Sie sind trotz allem nur eine Grundlage. Denn für komplexere, über einen längeren Zeitraum laufende Webportale, reicht das heute nicht mehr aus. Service Meshs liefern, was den Kubernetes-Bordmitteln fehlt. Und das liefern Plattform wie etwa Istio. Mehr zu dem Thema und übergreifende Ideen wie sie Service Meshs in ihrem Unternehmen nutzbringend finden können, finden sie auf den folgenden Seiten.

Ulrich Parthier
Publisher – Analyst - Influencer

PROBLEMLÖSER SERVICE MESH?

VON SOA ÜBER ESB ZUM SERVICE MESH.

Die meisten IT-Architekten gehen derzeit davon aus, dass Microservices die Antwort auf all die Probleme sind, die sie mit früheren Architekturen wie serviceorientierten Architekturen (SOA) und Enterprise Service Bus (ESB) hatten. Wenn man sich jedoch die aktuellen Microservices-Implementierungen in der Praxis anschaut, stellt man fest, dass auf der Ebene der Microservices häufig nichts anderes als die Funktionalität eines zentralen ESB implementiert wird. Gelöst werden also mehr oder weniger die gleichen grundlegenden Probleme, nur in diesem Fall mit Microservices in verschiedenen Dimensionen. Hier kommt das Konzept des ´Service Mesh´ ins Spiel, das wichtige und oft genutzte Funktionalitäten bündelt und für die einzelnen Microservices bereitstellt.

Microservices-Architekturen im Wandel – Entwicklung und Herausforderungen

Eine Microservices-Architektur ist ein verteiltes System, in dem unterschiedliche Bauteile über das Netzwerk miteinander sprechen. In einem verteilten System kann der Ausfall eines fremden Computers den eigenen Computer lahmlegen. Es sind große Anstrengungen notwendig, um das Risiko für ein solches Ausfall-Szenario im Vorfeld zu minimieren und damit die Vorteile einer Microservices-Architektur nutzbar zu machen. Die Lösung könnte eine technologische Strategie sein, mit der wir die Irrtürmer der verteilten Datenverarbeitung adressieren können. [1]

In der ersten Generation von Microservices-Architekturen wurden die notwendigen Muster zur Adressierung der Probleme in Frameworks in der jeweiligen Programmiersprache umgesetzt. Bekannt wurde der sogenannte „Netflix-Stack“, eine Sammlung von Java Libraries, die Netflix in seiner Architektur einsetzt und Open Source stellte. Mittels der Tools Eureka, Zuul und Hystrix werden dabei die Themen Service Discovery (Eureka: Wie finden sich Services bei einer sich dauernd ändernden Netzwerktopologie?, Hystrix: Wie verhindere ich, dass der Ausfall eines Services durch das Netzwerk kaskadiert?) und Sicherheit adressiert.

Microservices versus ESB

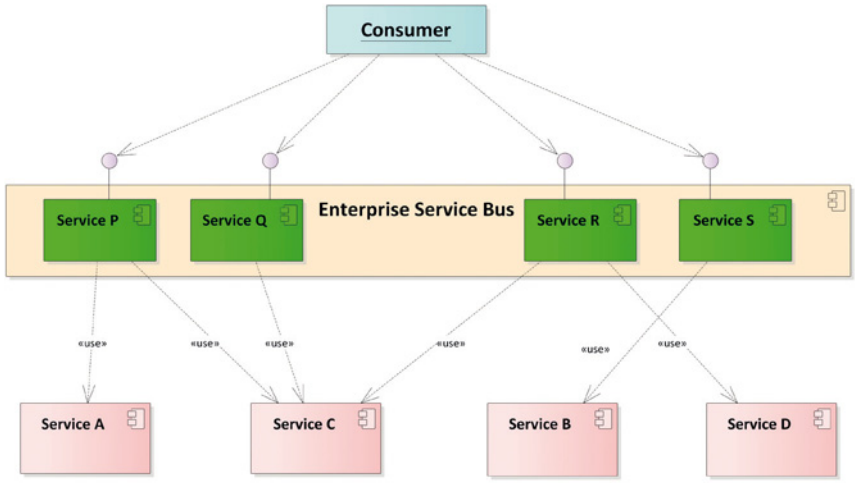
Die Themen Service Discovery und Sicherheit gelten auch als typische Aufgaben eines ESB. Für einen ESB gibt es keine eindeutige Definition, aber häufig wird er mit einer zentralen Komponente gleichgesetzt. Und darin liegt der wesentliche Unterschied. Microservices setzen auf Dezentralität und autonome Entscheidungen, ein ESB wird in Unternehmen häufig von einer zentralen Einheit verwaltet. Daher widerspricht der ESB einigen Architekturtreibern, welche die Wahl für eine Microservices-Architektur beeinflussen.

Sidecars und Service Mesh

Mit der nächsten Generation von Microservices-Architekturen änderte sich die Situation etwas. Das Ökosystem, insbesondere

um Kubernetes herum, war reifer geworden, und man erkannte, dass man bestimmte Aspekte, die jedem Microservice an die Seite gestellt werden, als Dienste anbieten kann. Dieses Muster nennt sich Sidecar Pattern. Die Kommunikation zwischen den unterschiedlichen Services erfolgt dabei immer über die Sidecars. Diese kümmern sich um alle kommunikationsrelevanten Themen und entlasten so den Anwendungsentwickler bei der korrekten Behandlung dieser Themen und ermöglichen gleichzeitig eine bessere zentrale Durchsetzung von bestimmten Policys und Nachvollziehbarkeitsanforderungen. Die Sidecars und deren Steuerung als Gesamtheit bezeichnet man als „Service Mesh".

1 ENTERPRISE SERVICE BUS ARCHITECTURE



Ein Blick unter die Haube

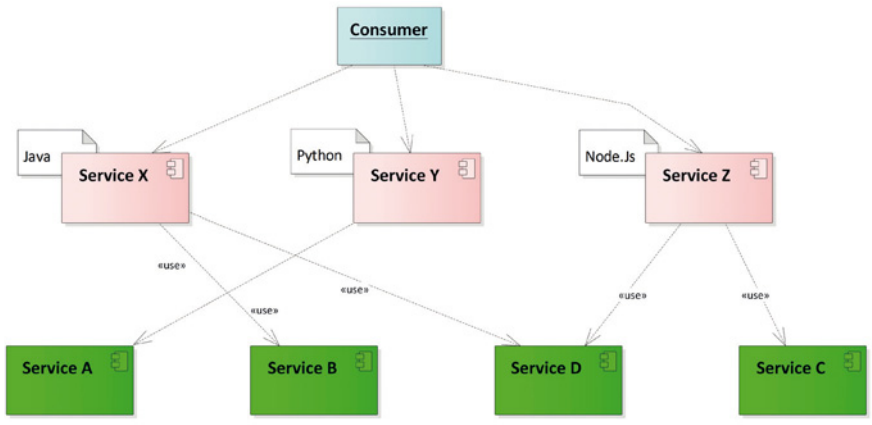
Schauen wir uns Sidecars und Service Mesh einmal genauer an: Nehmen wir zum Beispiel ein Szenario, in dem wir mehrere nachgelagerte Dienste belastbar aufrufen und die Funktionalität als einen weiteren (zusammengesetzten) Dienst darstellen müssen. Wie in Bild 1 dargestellt, können wir mit einer ESB-Architektur die in ESB integrierten Funktionen leicht nutzen, um Funktionalitäten aufzubauen, die für die Inter-Service-Kommunikation nützlich sind, wie Leistungsausfall, Timeouts, Service-Erkennung und so weiter.

Wenn wir das gleiche Szenario mit Microservices implementieren, dann haben wir es nicht mehr mit einer zentralisierte Integrations-/ESB-Schicht zu tun, sondern mit einer Reihe von zusammengesetzten und atomaren Microservices. Daher ist es wichtig, alle diese Funktionalitäten auf der Ebene der Microservices zu implementieren. Doch könnte die Kommunikation nicht einfach weiterhin über einen ESB laufen?

Dagegen spricht der Wunsch der Entwicklerteams nach Autonomie. Die Loslösung von einem zentralen Team und von den mit diesem verbundenen Abhängigkeiten und Bottlenecks führt unvermeidlich zu einem dezentralen Architekturansatz wie Microservices.

Daher umfasst ein bestimmter Microservice, der mit anderen Diensten kommuniziert, auch a) die eigentliche Geschäftslogik und b) die Netzwerkfunktionen, die sich um die Kommunikationsmechanismen zwischen den Diensten kümmern (Bild 3).

2 MICROSERVICES-ARCHITECTURE



Babylonische Sprachverwirrung

Der Aufwand für die Implementierung eines Microservice, der die funktionalitätsbezogenen Service-zu-Service-Kommunikation enthält, ist für viele Architekten ein Alptraum. Anstatt sich auf die Geschäftslogik zu konzentrieren, verbringen sie viel Zeit damit, die Funktionen für die Inter-Service-Kommunikation aufzubauen. Noch aufwändiger wird es, wenn mehrere Technologien zum Aufbau von Microservices verwendet werden, zum Beispiel mehrere Programmiersprachen wie in Bild 2 dargestellt. Dann fällt der gleiche Aufwand in verschiedenen Sprachen an. Zwar gibt es für die einzelnen Programmiersprachen Bibliotheken, die diese Netzwerkfunktionalitäten bereitstellen, doch diese müssen aus Sicherheitsgründen regelmäßig aktualisiert werden, was einen hohen administrativen Aufwand bedeutet.

Protokollierung und Tracing

Eine wichtige Frage, die sich bei verteilten Systemen aus Entwicklersicht stellt, lautet: Wie lassen sich Service-Aufrufe im Fehlerfall debuggen, loggen oder verfolgen? Dies war und ist trotz einer zentralen Instanz wie einem ESB auch in SOA eine Herausforderung. Verteilte Protokollierung über Services hinweg ist auch heute nur mit Diensten wie Graylog[2]

oder Splunk[3] möglich. Für verteiltes Tracing werden sehr oft APM-Tools wie AppDynamics[4] verwendet, da diese von Haus aus Traces aufzeichnen können.

Die komplexeste Herausforderung bei der Realisierung von Microservices-Architekturen besteht tatsächlich nicht im Aufbau der Dienste selbst, sondern in der Kommunikation zwischen den Diensten.

Inter-Service-Kommunikation
Die meisten Anforderungen an die Inter-Service-Kommunikation für die Microservices sind recht allgemein. So besteht meist der Wunsch, dass all diese Aufgaben in eine Komponente verlagert werden, damit sich die Microservices-Implementierungen auf die Geschäftslogik konzentrieren können.

In diesem Fall kommuniziert ein bestimmter Microservice nicht direkt mit den anderen Microservices. Vielmehr findet die gesamte Service-zu-Service-Kommunikation über eine Softwarekomponente statt: das Service Mesh.

Service Mesh – Hilfe für verteilte Systeme
Ein Service Mesh bietet integriert die Unterstützung für einige Netzwerkfunktionen wie Ausfallsicherheit oder Dienst-erkennung (Bild 4). So wird der größte Teil der Arbeit im Zusammenhang mit der Netzwerkkommunikation auf das Service Mesh übertragen und die Entwickler können sich stärker als bisher auf die Geschäftslogik konzentrieren.

Das Service Mesh ist sprachunabhängig: Da die Kommunikation der Microservices über den Service Mesh Proxy immer mithilfe von Standardprotokollen wie HTTP1.x/2.x oder gRPC abläuft, funktionieren die Microservices mit dem Service Mesh in jeder Technologie.

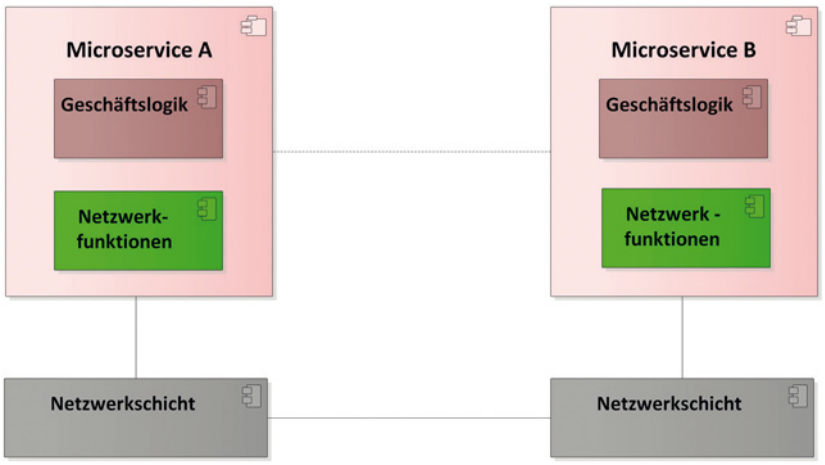
Wie sehen nun die Verantwortlichkeiten innerhalb der Service-Interaktionen aus:

1. Geschäftslogik
Die Service-Implementierung sollte die Realisierung der Geschäftsfunktionalitäten beinhalten. Dazu gehören die Logik für Geschäftsfunktionen, Berechnungen, Integration mit anderen Diensten/Systemen (einschließlich Legacy, proprietär und SaaS) sowie Service-Kompositionen, komplexe Routing-Logik, Mapping-Logik zwischen verschiedenen Nachrichtentypen und so weiter.

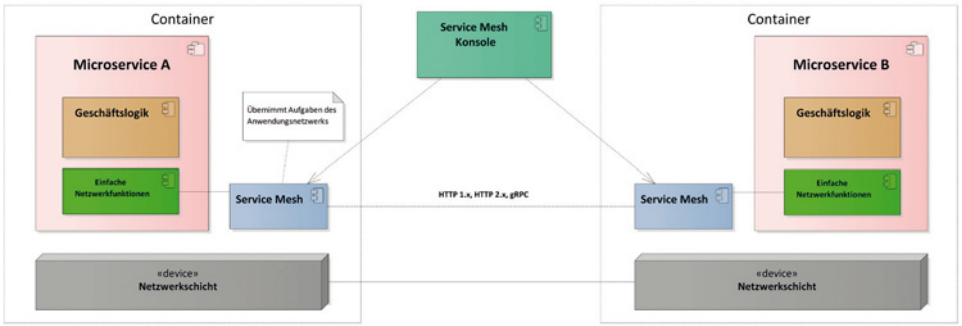
2. Einfache Netzwerkfunktionen
Obwohl wir die meisten Netzwerkfunktionen ins Service Mesh auslagern, muss ein bestimmter Dienst die grundlegenden High-Level-Netzwerkinteraktionen enthalten, um eine Verbindung mit dem Service Mesh herzustellen. Daher muss eine bestimmte Service-Implementierung eine bestimmte Netzwerkbibliothek verwenden. In den meisten Fällen bettet das Microservices Development Framework die erforderlichen Netzwerkbibliotheken ein, die für diese Funktionen verwendet werden sollen. Anders als in der ESB-Welt verwendet man hier eine sehr einfache Abstraktion, um auf Services zuzugreifen.

3. Aufgaben des Anwendungsnetzwerks
Es gibt Anwendungsfunktionalitäten, die eng mit dem Netzwerk verbunden sind, wie Leistungsausfall, Timeouts, Serviceerkennung und so weiter. Diese sind explizit von der Service-Code/Business-Logik getrennt und werden vom Service Mesh übernommen, das diese Funktionalitäten sofort nach

3 MICROSERVICES MIT SERVICE-ZU-SERVICE-KOMMUNIKATION



4 SERVICE-ZU-SERVICE-KOMMUNIKATION MIT DEM SERVICE MESH



> DER AUFWAND FÜR DIE IMPLEMENTIERUNG EINES MICROSERVICE, DER DIE FUNKTIONALITÄTSBEZOGENEN SERVICE-ZU-SERVICE-KOMMUNIKATION ENTHÄLT, IST FÜR VIELE ARCHITEKTEN EIN ALPTRAUM.
>
> Klaus Kramer, Senior Consultant, Opitz Consulting, www.opitz-consulting.com

der Installation bereitstellt. Microservice-Implementierungen haben die Komplexität der Netzwerkfunktionen, die von einer zentralen ESB-Schicht angeboten werden, zu Beginn häufig noch unterschätzt. Sie implementierten diese Funktionalitäten auf jeder Mikroservice-Ebene von Grund auf neu. Mittlerweile hat man erkannt, dass gemeinsam genutzte Funktionalitäten hier ähnlich wichtig sind, wie bei einem verteilten Netz.

4. Steuerebene

Alle Service Mesh Proxys werden zentral über eine Konsole verwaltet. Das ist sehr sinnvoll, wenn es darum geht, Service-Mesh-Funktionen wie Zugriffskontrolle, Beobachtungsfähigkeit oder Serviceerkennung zu unterstützen.

Funktionalitäten eines Service Mesh

Wie wir bereits gesehen haben, bietet das Service Mesh eine Reihe von Anwendungsnetzwerkfunktionen, während einige (primitive) Netzwerkfunktionen noch auf Microservices-Ebene implementiert sind. Die Funktionalitäten eines Service Mesh sind nicht fest definiert. Häufig bietet es diese Funktionen:

- Ausfallsicherheit für die dienstübergreifende Kommunikation: Leistungsunterbrechung, Wiederholungen und Timeouts, Fehlerinjektion, Fehlerbehandlung, Lastausgleich und Ausfallsicherung
- Service-Erkennung: Erkennung von Service-Endpunkten durch eine dedizierte Service-Registrierung
- Beobachtbarkeit: Metriken, Überwachung, verteilte Protokollierung, verteiltes Tracing
- Sicherheit: Transport Level Security (TLS)
- Zugangskontrolle: Listen-basierte Zugriffskontrolle
- Bereitstellung: Native Unterstützung für Container. Docker und Kubernetes
- Kommunikationsprotokolle zwischen den Diensten: HTTP1.x, HTTP2, gRPC

+ Vorteile

Die allgemeinen Netzwerkfunktionen werden außerhalb des Microservice-Codes implementiert und sind so wiederverwendbar. Ein Service Mesh behebt die meisten Probleme in der Microservices-Architektur, die wir früher mit Ad-hoc-Lösungen hatten wie Verteilte Verfolgung, Protokollierung, Sicherheit, Zutrittskontrolle und so weiter. Zusätzlich bekommen wir mehr Freiheit bei der Auswahl einer Implementierungssprache für die Microservices, das heißt, wir müssen uns keine Gedanken mehr darüber machen, ob eine bestimmte Sprache Bibliotheken besitzt, um Funktionen für die Netzwerkkommunikation zu erstellen oder die Funktionen von Grund auf neu zu implementieren.

– Nachteile

Da wir mehr Laufzeitkomponenten in unserem System benötigen, wird es insgesamt komplexer. Des Weiteren fügen wir eine weitere Komponente in unsere Netzkommunikation hinzu: Jeder Service-Aufruf durchläuft nun zusätzlichen einen Service Mesh.

Der Service Mesh adressiert nur eine Teilmenge von Kommunikationsproblemen zwischen den Diensten. Viele umfängliche Probleme wie komplexes Routing, Transformation/Typ-Mapping, Integration mit anderen Diensten und Systemen, müssen weiterhin in der Geschäftslogik der Microservices gelöst werden.

Service-Mesh-Implementierungen

Die bekanntesten Service-Mesh-Implementierungen sind Envoy[5] oder das darauf basierende Istio-Framework[6] sowie Linkerd[7] und consul-connect[8]. Bei diesen handelt es sich um Open-Source-Projekte, die sich mit dem Thema Service Mesh beschäftigen. Alle Service-Mesh-Technologien sind relativ neu und werden aber bereits für voll produktiv erklärt.

Fazit

Zusammenfassend lässt sich sagen, dass die Service-Mesh-Technologie einige der wichtigsten Herausforderungen bei der Realisierung von Microservices-Architekturen angeht. Architekten profitieren damit von einer größeren Freiheit bei der Auswahl von Technologien zur Implementierung von Microservices. Außerdem benötigen sie weniger Zeit für Netzwerkfunktionen zwischen den Services und können sich mehr auf die Geschäftslogik konzentrieren. Allerdings löst das Service Mesh keine Probleme, die mit der Geschäftslogik oder mit der Service-Integration oder -Komposition verbunden sind.

Klaus Kramer

Quellen:
1 https://de.wikipedia.org/wiki/Fallacies_of_Distributed_Computing
2 https://www.graylog.org/overview
3 https://www.splunk.com/en_us/solutions/solution-areas/log-management.html
4 https://www.appdynamics.de/
5 https://www.envoyproxy.io/
6 https://istio.io/
7 https://linkerd.io/
8 https://www.consul.io/docs/connect/index.html

Daten intelligent schützen

mit Endpoint Security Lösungen von DriveLock

30 Tage kostenfrei testen

bit.ly/demo_drivelock

Effiziente Cyber Security

- Application Control
- Device Control
- Security Awareness
- Verschlüsselung
- Smart Card Management

www.drivelock.de

SERVICE MESH

KONSEQUENZEN BEI MICROSERVICE-ARCHITEKTUREN.

Michael Hofmann im Interview mit Ulrich Parthier über die Vorteile, den Nutzen und die Kosten für IT-Abteilungen in Unternehmen.

Bild 1: Die Death Star-Architektur bei Netflix.
Quelle: Adrian Cockcroft (Netflix) / Martin Fowler

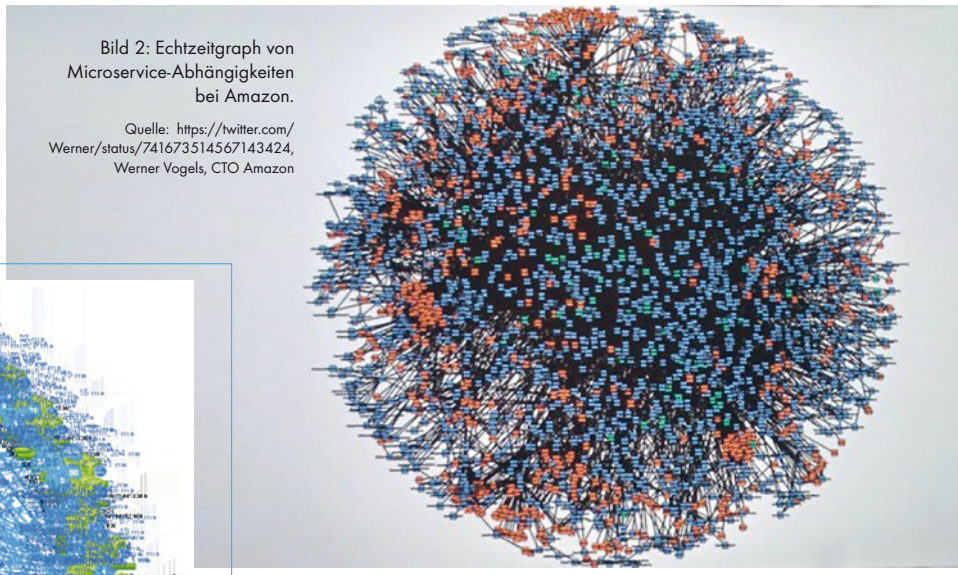


Bild 2: Echtzeitgraph von Microservice-Abhängigkeiten bei Amazon.

Quelle: https://twitter.com/Werner/status/741673514567143424, Werner Vogels, CTO Amazon

Ulrich Parthier: *Der Begriff der Microservice-Architektur ist in den letzten Monaten verstärkt in den Fokus von IT-Abteilungen geraten. Wie kann diesen Begriff am besten beschreiben?*

Michael Hofmann: Der aktuelle Architektur-Trend geht weg von monolithischen Systemen hin zu kleineren Anwendungen (Microservices), die in sich fachlich abgeschlossen sind und über definierte Schnittstellen mit anderen Anwendungen kommunizieren. Diese fachliche Abgeschlossenheit geht sogar so weit, dass diese Anwendungen ihre eigene Persistierung besitzen und direkte Zugriffe anderer Services auf diese Datenbanken verboten sind. Somit werden Anwendungslandschaften geschaffen, die unabhängig voneinander entwickelt und released werden können, was insgesamt zu mehr Flexibilität führt.

Änderungen an den kleineren Anwendungen können schneller erfolgen, wodurch rascher auf neue Anforderungen reagiert werden kann.

Ulrich Parthier: *Neuerdings taucht im Zusammenhang mit Microservice-Architekturen der Begriff „Service Mesh" auf. Was verbirgt sich dahinter?*

Michael Hofmann: Derzeit existieren zwei Definitionen des Begriffs Service Mesh. Die erste Definition bezeichnet einen Service Mesh als das Zusammenspiel von vielen kleineren Anwendungen, welche in der Regel als Microservices implementiert werden. Durch die Interaktion der Microservices kann dabei ein Kommunikations-Geflecht entstehen, das nur schwer ohne Werkzeuge zu betreuen und zu verwalten ist. Hier kommt jetzt die zweite Definition ins Spiel. In dieser erweiterten Form wird auch das Werkzeug zur Verwaltung eines Services Meshs mit in die Definition integriert.

Ulrich Parthier: *Gibt es Tools, die dabei helfen, die Übersicht zu behalten?*

Michael Hofmann: Aktuell führend sind derzeit zwei Werkzeuge, die zur Verwaltung des Service Mesh entwickelt werden: Istio und Linkerd.

Ulrich Parthier: *Können Sie ein Beispiel für eine Microservice-Anwendung und Service Meshs nennen?*

Michael Hofmann: Die bekanntesten Beispiele hierfür sind Anwendungen bei Netflix (Bild 1) oder Amazon (Bild 2). In beiden Fäl-

> FRÜHER ODER SPÄTER WERDEN SIE SICH MIT DEM THEMA SERVICE MESH IN IHREM MICROSERVICE-PROJEKT AUSEINANDER SETZEN MÜSSEN.
>
> Michael Hofmann, Software Architekt | www.hofmann-itconsulting.de

len interagieren mehr als hundert Services miteinander und bilden somit eine komplexe Fachlichkeit ab. Abhängigkeitsgraphen, welche zur Laufzeit erstellt wurden, zeigen eindrucksvoll wie Komplex diese Kommunikations-Beziehungen sein können.

Ulrich Parthier: *Was wird gerne bei der Betrachtung der Services vernachlässigt oder gar vergessen?*

Michael Hofmann: Durch die Möglichkeit einzelne Services voneinander unabhängig zu releasen existieren in Produktionsumgebungen neue Versionen von Services oft neben älteren Versionen des selben Services. Der Grund für diese Koexistenz liegt darin, dass aufrufende Services noch abhängig sind von der Vorgänger-Version des aufgerufenen Services. Parallel dazu befinden sich aber schon Services in Produktion, die von den neuen Funktionalitäten des Partner-Services profitieren. Damit entsteht ein Mix an alten und neuen Versionen von Services, die gleichzeitig verwendet werden. Multipliziert man die Anzahl an unterschiedlichen Versionen mit der Anzahl an Services kommt man schnell in einen zweistelligen oder sogar dreistelligen Bereich an Services die verwaltet werden müssen.

Ulrich Parthier: *Was kann beim Beherrschen eines Service Mesh helfen?*

Michael Hofmann: Notwendige Funktionalitäten um einen Service Mesh in den Griff zu bekommen sind beispielsweise Traffic-Management, Security bei der Service-Kommunikation, Policies wie zum Beispiel Rate Limiting und Sammlung von Telemetrie-Daten zur Überwachung des Service Mesh. Dabei verbirgt sich hinter dem Begriff Traffic-Management der umfangreichste Teil der Funktionalität. Neben einer parametrisierten Festlegung von Request-Routings (Service A ruft bei gewissen Vorbedingungen Service B in unterschiedlichen Versionen auf) sollten auch Möglichkeiten zum Testen von neuen Services existieren.

Ein Service Mesh Werkzeug sollte so etwas wie Blue-Green-Deployment oder Canary-Releasing bieten, um den Übergang zwischen den Versionen eines Services möglichst reibungslos zu gestalten. Da es bei verteilten Systemen naturgemäß auch zu Fehlern in der Kommunikation kommen kann, bieten Service Mesh Tools Funktionalitäten zur Erhöhung der Resilienz an. So kann man beispielsweise bei Istio neben Request-Timeouts auch verschiedene Circuit-Breaker definieren. Das ganze erfolgt ohne Eingriff in den Source-Code des Services, was wiederum einen großen Vorteil darstellt. Oft werden die notwendigen Resilienz-Patterns erst im produktiven Umfeld erkannt. Sollen diese Patterns nun im Source-Code umgesetzt werden, so kann dies nicht ohne ein erneutes Deployment erfolgen.

Ulrich Parthier: *Wodurch unterscheiden sich Service-Mesh-Werkzeuge wie etwa Istio oder Linkerd. Gibt es ein herausragendes Tool oder so etwas wie eine Stärken/Schwächen-Matrix?*

Michael Hofmann: Beide Tools Istio und Linkerd unterscheiden sich kaum in deren Funktionalität. Von daher ist es eher eine Frage der persönlichen Präferenzen für welches Werkzeug man sich entscheidet. Einen detaillierten Vergleich bietet folgender Beitrag: https://abhishek-tiwari.com/a-sidecar-for-your-service-mesh/

Ulrich Parthier: *Wo es Vorteile gibt, lauern meist auch Risiken. Hier auch?*

Michael Hofmann: Ein Service Mesh besitzt an sich schon eine gewisse Komplexität und auch das Tool zur Verwaltung des Service Mesh muss erstmal beherrscht werden. Von daher geht die Empfehlung ganz klar in die Richtung sich möglichst frühzeitig mit dem Service Mesh Tool zu beschäftigen. Auch wenn aktuell nur wenige Services zu verwalten sind sollte man dafür ein Tool einsetzen, da davon auszugehen ist, dass die Anzahl der Services sehr schnell steigen wird und sei es nur über die unterschiedlichen Versionen eines Services.

In der Regel findet die Service zu Service Kommunikation abgesichert statt. Eine der Mindestvoraussetzungen ist TLS aber auch mutual TLS kann notwendig sein. Der zugehörige Austausch von SSL-Zertifikaten kann dabei schnell eine umfangreichere Aufgabe werden. Hierbei kann das Service Mesh Werkzeug helfen indem es diese Aufgabe selbständig übernimmt. Aus Sicherheitsgründen ist eine automatisierte Verteilung der Zertifikate gegenüber einer manuellen Administration vorzuziehen. Wer schon mal abgelaufene Zertifikate von Hand in Produktion tauschen musste will so etwas nicht nochmal erleben.

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

EINE INFRASTRUKTUREBE

SIND SIE SCHON AN BORD DES SERVICE-MESH-ZUGS?

Jedes Unternehmen hegt heute den Wunsch, als Technologieunternehmen wahrgenommen zu werden. Innerhalb dieser Philosophie hilft der Einsatz von Software bei der Weiterentwicklung des Unternehmens mit dem Ziel einen Wettbewerbsvorteil zu erzielen. Die Umsetzung der digitalen Transformationsstrategie führt darüber hinaus dazu, dass Legacy-Applikationen modernisiert werden müssen, um sich von traditionellen monolithischen Anwendungen zu lösen.

Das Ergebnis? Microservices boomen und neue Technologien werden entwickelt, um ihre Leistung zu verbessern. Ein solches Werkzeug ist das Service Mesh. Tatsächlich wird es als einer der großen Cloud-Computing Trends von 2019 angesehen, allerdings bestehen Zweifel, ob die Mehrheit der Unternehmen schon bereit dafür ist.

Warum benötigen Sie ein Service Mesh?

Zuerst zum Wesentlichen: Sie sind sich immer noch nicht ganz sicher, was ein Service Mesh ist? Einfach ausgedrückt, ist ein Service Mesh eine einfache, konfigurierbare Infrastrukturebene für Microservices. Während Microservices eine weitaus höhere Flexibilität für Applikationsentwicklern und Architekten bieten, steigt damit auch die Komplexität, weshalb das Service Mesh aufgrund seiner Fähigkeit, die Interaktionen zwischen den verschiedenen Microservices zu sichern, zu überwachen und zu steuern, immer mehr an Bedeutung gewinnt.

Die Haupteigenschaft eines Service Mesh ist das Traffic-Management, das die Kommunikation zwischen einzelnen Services, die von der Applikation erstellt oder sich innerhalb dieser befinden, unterstützt und erleichtert sowie ihnen dabei hilft schneller, flexibler und zuverlässiger zu sein. Mit diesen Funktionen bietet ein Service Mesh Service Discovery, Load Balancing, Verschlüsselung für Antworten und Anfragen, Authentifizierung und Autorisierung innerhalb und außerhalb der Applikation.
Hinzu kommt Unterstützung beim Auffinden und Verhindern von Fehlern durch die Verwendung eines Trennschalter-Musters, das jedes „Durchsickern" in andere Services verhindert. Dies sind nur einige wenige der Funktionalitäten, die Unternehmen dabei helfen die Produktivität von Entwicklern zu verbessern, eine höhere Skalierbarkeit, Verfügbarkeit und Sicherheit ihrer Services zu gewährleisten sowie die Sichtbarkeit und Übersicht mithilfe von Überwachungs-, Tracking- und Analysetools zu sichern.

Diese Vorteile, vor allem die Fähigkeit zu höherer Belastbarkeit und Sicherheit, führt dazu, dass das Service Mesh als ein entscheidender Bestandteil jeder Microservice-Infrastruktur angesehen wird und die Zukunft der Applikationsbereitstellung darstellt. Dabei ist Zukunft hier das Schlüsselwort. Es ist eine Fehlannahme, dass Sie bei der Arbeit mit Containern direkt zur Implementierung von einem Service Mesh übergehen sollten. Wenn Sie noch nicht bereit dafür sind, könnte es mehr Probleme als Lösungen geben. Deshalb sollten Sie nicht einfach auf den Service-Mesh-Zug aufspringen.

Ist Service Mesh das Richtige für Sie?

In der IT-Branche glauben viele, einschließlich Gartner, dass Service Mesh nicht eine Frage des „Ob", sondern des „Wann" ist, und das für jeden, der Microservices nutzt. Das Team von Gartner hat eine genaue Definition von Service Mesh und macht dies zu einer äußerst vertretbaren Position – allerdings werden viele Unternehmen dem nicht zustimmen.

Vor der Implementierung von Service Mesh, ist es wichtig, sich in aller Ruhe über seine aktuelle Situation Gedanken zu machen: Wo befinden Sie sich? Und welche Vorteile versprechen Sie sich? Schließlich ist es keine schnelle Einmallösung, sondern ein Lösungsweg. Wo befinden Sie sich also derzeit auf Ihrem Weg zu containerisierten Applikationen? Untersuchen, entwerfen und führen Sie erste Machbarkeitsstudien durch oder befinden Sie sich im produktiven Einsatz? Noch wichtiger ist, was erwarten Sie von einem Service Mesh und haben Sie andere, ausgereiftere Ansätze evaluiert?

Schauen Sie sich zunächst Ihre bestehende Technologie an. Welche Probleme wollen Sie lösen? In Anbetracht der angestrebten Verbesserungen und der von wichtigsten von Ihnen benötigten Funktionen, könnten Sie diese vielleicht mit einigen Optimierungen und einfachen Ergänzungen zu Ihrem vorhandenen System erreichen? Es hat keinen Zweck, ein Projekt um seiner selbst willen komplizierter zu gestalten oder sich ein brandneues System zuzulegen. Obwohl Service Mesh eine Vielzahl an Vorteilen

NE FÜR MICROSERVICES

> ES HAT KEINEN ZWECK, EIN PROJEKT UM SEINER SELBST WILLEN KOMPLIZIERTER ZU GESTALTEN ODER SICH EIN BRANDNEUES SYSTEM ZUZULEGEN. OBWOHL SERVICE MESH EINE VIELZAHL AN VORTEILEN BIETET, DÜRFEN DIE NACHTEILE NICHT UNTERSCHÄTZT WERDEN, INSBESONDERE FÜR KLEINERE UMGEBUNGEN.
>
> Owen Garrett, Sr. Director Product Management, NGINX | www.nginx.com

bietet, dürfen die Nachteile nicht unterschätzt werden, insbesondere für kleinere Umgebungen.

Wohin führt ihr Weg?

Der sich abzeichnende universelle Ansatz für Service Mesh sind Sidecar-Proxys. Wie der Name schon sagt, können diese Sidecar-Proxys mit dem Beiwagen eines Motorrads verglichen werden und sind speziell mit einer bestimmten Service-Instanz als „Utility Pod" verbunden, der diesen Service unterstützen soll. Das bedeutet, dass immer ein zusätzlicher Proxy neben jeder Service-Instanz bereitgestellt wird. Obwohl es die Verwaltung des gesamten Netzwerk-Traffics und zusätzliche Funktionen ermöglicht, bringt es dennoch auch eine erhöhte architektonische Komplexität mit sich.

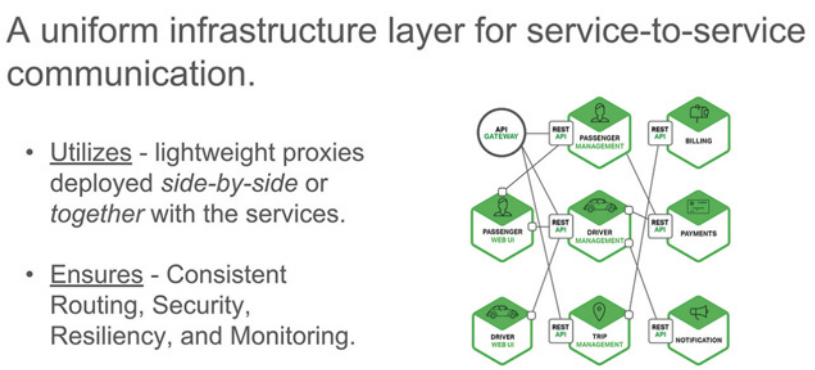
Hinterfragen Sie daher, ob Ihre Umgebung groß und Ihre Servertopologie komplex genug sind, um diese Implementierung zu gewährleisten! Service Mesh benötigen Sie nur, sobald Sie einen bestimmten Level an Komplexität erreichen. Bis dahin ist es am besten, Fundamente zu legen und sich damit vertraut zu machen, worauf ein Service Mesh aufbauen würde sowie andere Optionen zu prüfen, die besser zu Ihren aktuellen Anforderungen und Ihrer Infrastruktur passen.

Für Container gibt es bereits heute Kubernetes, das beliebte Orchestrierungssystem für containerisierte Applikationen, dessen

Fähigkeit, Container-Applikationen bereitzustellen, bewährt ist. Kubernetes bietet bereits eine umfangreiche Netzwerkstruktur, die Service Discovery, Lastausgleich, Health Checks und Zugriffskontrolle bereitstellt. Auch das Einbetten ist einfach und es gibt eine große Auswahl an zusätzlichen Diensten, die Sie problemlos hinzufügen können.

Die Orchestrierungsfrage

Sie haben sich die Zeit genommen und festgestellt, an welchem Haltepunkt Sie sich befinden und dass Kubernetes nicht ganz Ihren Anforderungen entspricht? Dann sollten Sie trotzdem nicht zu schnell vorwärts springen und stattdessen überlegen, ob beispielsweise ein einfacher Load Balancer oder ein API-Gateway Ihre Anforderungen erfüllen würden? Ein API-Gateway bietet zusätzlich die Möglichkeit der Authentifizierung und Überwachung des Request Routings. Es ist wesentlich besser geeignet, wenn Sie beispielsweise nur wenige Microservices mit einer bestehenden monolithischen Applikation verknüpft haben. In diesem Fall wäre ein Service Mesh schlichtweg überflüssig.



Der Service Mesh bietet die Gelegenheit eines einheitlichen Infrastruktur-Layers für service-to- service Kommunikation.

Dabei ist anzumerken, dass während Anbieter und Open-Source-Projekte in hohem Tempo daran arbeiten Service Mesh stabiler und funktionaler zu machen sowie die Implementierung zu vereinfachen, sich die Technologie weiterentwickelt und eventuell in den Aufgabenbereich und die Funktionalitäten eines API-Gateways eingreifen wird. Wenn Sie jedoch eine kleinere containerisierte Umgebung mit geringer Komplexität und wenigen Microservices haben, ist dies die richtige Option für Sie.

Sind Sie jetzt bereit?

Möglicherweise sind Sie noch nicht bereit für ein Service Mesh, dennoch wird wahrscheinlich der Zeitpunkt kommen, an dem Sie einen Wendepunkt erreichen und die Größe und Komplexität erreichen, die es zu einem essentiellen Bestandteil macht. Wenn Ihre Teams eine größere Transparenz im Netzwerk benötigen, müssen sie etwa eine Durchsatzratenbegrenzung oder eine zusätzliche Zugriffskontrolle hinzufügen. Dies wird Ihre Applikationsentwickler und Ihr operatives Team stark belasten. In diesem fortgeschrittenen Stadium können und sollten Sie sich nun auf ein Service Mesh konzentrieren.

Wenn Ihr System größer wird, sich entwickelt und die Anforderungen steigen, ermöglicht Ihnen ein Service Mesh, diese Einschränkungen zu überwinden und Ihre Applikationen für Microservices weiter auszubauen. Wobei diese konfigurierbare Struktur die nun benötigte Kommunikation zwischen Microservices unterstützt und erleichtert. Wenn Ihre containerisierte Applikationsverfügbarkeit an Fahrt verliert, kann ein Service Mesh den Treibstoff darstellen.

Allerdings bedeutet das immer noch nicht mit Volldampf voraus. Service-Mesh entwickelt sich vielleicht weiter und ist einfacher zu implementieren, aber es gibt eine Reihe von Hindernissen und Herausforderungen, die es zu beachten gilt.

Der richtige Zeitpunkt

Auch wenn Netflix und Twitter die Implementierung von Service Mesh vorantreiben, ist es immer noch eine junge Technologie, deren viele Lösungen sich entweder in der Entwicklungsphase befinden oder umfangreiches Wissen erfordern, um ein Service Mesh in der Betriebsphase zuverlässig zu pflegen. Die große Mehrheit der Unternehmen dürfte daher nicht über das Know-how oder die Fähigkeiten verfügen, die für die Implementierung von Service

Mesh in der Anfangsphase erforderlich sind. Um dies richtig umzusetzen, müssen sie erst die Defizite an Qualifikationen beheben – und das braucht Zeit. Hinzu kommt das zusätzliche Problem, inwieweit Sie wirklich den gesuchten na sagen wir mal Treibstoffschub erhalten.

Mit der schnellen Entwicklung von Service Mesh und der zunehmenden Attraktivität, werden einige der ersten Lösungen nicht gut strukturiert oder auf Ihre langfristigen Bedürfnisse ausgerichtet sein. „Service-Mesh-Washing" wird eine beliebte Marketing-Taktik sein, ebenso wie viele Produkte in „software-basiert" oder „virtualisiert" umbenannt wurden, um den Hype des bisherigen Technologiewandels zu nutzen.

Istio hat sicherlich den Vorteil, als Erster auf diesem Gebiet zu operieren, aber das bedeutet nicht, dass in den kommenden Jahren keine anderen tragfähigen Optionen zur Verfügung stehen werden. Derzeit besteht keinerlei Gewissheit darüber, wer sich als führender Anbieter und Vorreiter dieser Technologie entwickeln wird.

Vorarbeit und Umsetzung

Wenn Sie die genannten Faktoren bei Ihrer Vorbereitung beachten, sollte sich ihr Implementierungsprozess erleichtern und einen Erfolg garantieren. Wie schön wäre es, wenn man sagen könnte, dass es jetzt Zeit ist, sich zurückzulehnen und zu entspannen, aber selbst wenn das Service Mesh einen bestimmten Entwicklungsstand erreicht hat, wird es sich kontinuierlich weiterentwickeln. Wenn neue Technologien aufkommen, die in den Bereich der Service Mesh eintreten, muss sich das Service Mesh anpassen und verändern; und was würde passieren, wenn wir beispielsweise damit aufhören, Kubernetes als containerisierte Umgebung zu nutzen?

Trial & Error

Ist Service Mesh also die richtige Wahl für Sie? Die wahrscheinlichste Antwort: ja, aber möglicherweise noch nicht jetzt. Auch wenn Sie eventuell noch nicht bereit sind, die Umsetzung von Service Mesh jetzt durchzuführen, stellen Sie dennoch sicher, dass Sie keine der Maßnahmen versäumen, die Sie auf diesen Weg führen könnten.

Das Jahr 2019 könnte das Jahr des Service Mesh werden. Allerdings sollten Sie erst dann einsteigen, wenn Sie an der richtigen Haltestelle sind. Selbst wenn Sie das Ziel erreichen, wird dies sicherlich nicht Ihr letztes sein, doch wird Service Mesh für eine einfachere Fahrt sorgen.

Owen Garrett

25 JAHRE IT

DIE NÄCHSTEN 25 JAHRE: 6 EXPERTEN – 6 MEINUNGEN.

Ja, wer hätte das gedacht. 1991 ging es mit dem Magazin DATENBANK FOKUS los, 1994 zur CeBIT folgte die it managment. Seit wann gibt es sie? Wird es sie morgen noch geben? Das waren nur zwei der damals oft gestellten Fragen. Wie man sieht, es gibt uns noch immer. Das Zauberwort heißt Evolution und gemäß Darwin überleben nur die, die sich neuen Situationen schnell anpassen. Und deren gab es genug. Neue Technologien, immer schneller werdende Innovationszyklen, Internetblase, Finanzkrise und so weiter.

LAN-Manager und NT. Mitte der 90er Jahre hatten die PC-Durchdringung und die Netzwerke, die Ära des Client-Server Computings begünstigt.

Mitte der 90er Jahre war gerade das Desktop Publishing entstanden und läutete das abrupte Ende von Setzmaschinen ein, weniger als ein Jahrzehnt später kam das Ende der Belichtungsmaschinen und wir waren bei Computer-to-Plate. Und wir: immer mittendrin im technologischen Wandel an vorderster Front.

behalten. Der Hang aller Regierungen zur totalen Überwachung, immer mit dem Scheinargument des Terrorismus begrün-

Gestartet sind wir just zu Beginn des Siegeszuges der relationalen Datenbanken. Heute sind das schon Legacy-Systeme und sie werden uns noch viele Jahre begleiten. Anfangs wurden sie belächelt, von den Großrechner-Gurus, die mit IMS arbeiteten und den PC-Fuzzys, deren Heiligtum dBase III und Clipper waren. Eine krasse Fehleinschätzung nach dem dBASE IV Flop folgten Access für die Home User und Oracle, Informix und Ingres für die Profis.Es dauerte nicht lange und dann begann der Niedergang von Novells Netware und der Aufstieg von Microsofts

Wer erinnert sich noch an die Hardware: PCs mit Festplatten von 20 Mbyte, den Umstieg von 5 ¼ auf 3 ½ Zoll Floppy Disk? Hat einer von Ihnen etwas von der Gigabyte- und nun Terabyte-Welle geahnt? Router, Switches, WiFi, Hotspots, das Ende der Modems?

Aber was war das alles gegen das Internet und die Mobiltelefone? Nicht einmal im Traum konnten wir Mitte der 90er ahnen, was uns alles erwartet und damit ist nicht nur das Positive gemeint. Auch die Negativerfahrungen müssen wir im Blick

det. Die Cyberkriminalität, die Industriespionage aus Russland und China. All das sind Situationen, gegen die wir uns wehren müssen.

Letzter Punkt bei der Hardware: Die Erfindung des Mobiltelefons. Aber: Wer hat's erfunden? Apple! Falsch! Martin Copper gilt als der Erfinder und der Name Motorola ist eng damit verbunden. Nokia jedoch macht das Handy populär, bevor der Quantensprung in der Mobilfunkära begann: Apples iPhone. Es war das Ergebnis nach dem ersten Fehlschlag, dem

MANAGEMENT

ROKR, einer Kooperation Motorola/ Apple. Wie tief muss da der Schmerz von Steven Jobs gewesen sein, als er das Ergebnis gesehen hat? Die Folgen waren radikal und heraus kam das iPhone. Wie naiv mussten die Manager der anderen Mobilfunkmitbewerber sein, um nicht zu erkennen, dass sie sofort alle eigenen Arbeiten hätten maximieren müssen, um eine ähnliche Benutzeroberfläche zu bauen? Und Software-technisch? Viele Themen von damals sind Dauerbrenner, Beispiel Projektmanagement. Andere Themen kamen und gingen wie das Client/Server Computing, andere entwickeln sich dynamisch weiter wie das Internet, Computerleistung, Speicher, Datenübertragungsraten wachsen linear und neue Themen wie das Quantencomputing werden kommen.

Fakt heute ist, jedes Jahr lernen wir zwei bis drei neue Programme. Waren wir anfangs mit Apple II und Visicalc gestartet, kamen bald Wordperfect, Euroscript und MS-Word sowie Lotus1-2-3 oder Excel hinzu. Und heute: Neben Office oder den Google Apps, nutzen wir jede Menge weiterer Apps. Ich schätze mal, dass jeder von uns so 20 bis 30 heruntergeladen hat, auch wenn wir dies Apps nicht alle regelmäßig nutzen. Datenanalyseprogramme, Upload- und Datenübertragungsprogramme, Grafik- und CRM-Tools und und und... Ich kann Ihnen versprechen, es wird nicht weniger, mit dem wir uns beschäftigen müssen. Und da erinnere ich mich an einen der wenigen richtigen Sätze aus meiner Schulzeit: „Non vitae sed scholae discimus“, zu deutsch: „nicht für die Schule, sondern für das Leben lernen wir“. In diesem Sinn, viel Spaß beim Blick auf unsere VORSCHAU. Lesen Sie was ausgewählte Experten uns für das nächste Vierteljahrhundert voraussagen.

1 | Startschuss CeBIT 1994
Anzug und Krawatte war in der Ära des Client-Server-Computing noch das angesagte Outfit für CIOs und IT-Leiter. Der herbe Schlagabtausch fand zum Glück nur zwischen der neuen Technologie und dem alten Mainframe statt. Aber totgesagte leben bekanntlich länger und sollen aktuell sogar zum digitalen Geschäftswachstum beitragen.

2 | Die Gelbe Phase
Sehr gewagt: Knallrot auf sonnengelbem Hintergrund. Das waren die 90er! Die Themen allerdings waren zeitlos: Analysen, Business Reengineering, ISO-Standard und Speicher. Aktuell kämpfen Unternehmen mit der Einführung des ISO 27001.

3 |Graue Zeiten - DOT.COM
Mit dem grauen Erscheinungsbild stellte die it management ihre Leser schon mal auf die harten Zeiten ein, die auf das Platzen der Dot-Com-Blase im Jahr 2000 folgten. Workflows bewegen uns noch immer. „Smart Agents" sind als digitale Kollegen dazugekommen. Wie die Zukunft des Arbeitens mit KI-basierten Workflows aussieht, lesen Sie heute auf it-daily.

4 | SOA und Data Warehouse
Mit serviceorientierte Architektur (SOA) wird erstmals versucht, Dienste bzw. Services von IT-Systemen zu strukturieren und zu nutzen. Zudem nehmen die Datenmengen rasch zu und werden in Data Warehouses gemanagt. Inzwischen sprechen wir von Big Data und denken darüber nach, in der smarten Datenflut Kurs zu halten.

5 | What you model is what you get
Mitte des ersten 2000er Jahrzehnts haben Unternehmen noch mit ihrem eigenen Grips über Geschäftsprozesse nachgedacht. Es wurde modelliert und der Geschäftserfolg hing von der Qualität des Geschäftsmodells ab. Lohnt es sich heute mit Künstlicher Intelligenz Geschäftsprozesse zu transformieren?

6 | Das aktuelle Layout
Nach zehn Jahren wurde es im Januar 2018 höchste Zeit für ein Facelifting der it management. it-daily.net und it management sieht man nun die Verwandtschaft an. Trotz viel schnellerer IT-Systeme schreien die Anwender auch heute noch nach SPEED! Vor allem jedoch bei Internet-Verbindungen und Cloud Apps.

TRANSFORMATION IN PROGRESS

Paola Krauss,
Corporate Communications,
SNP SE | www.snpgroup.com/de

In den kommenden Jahren stehen Unternehmen weltweit vor gewaltigen Herausforderungen: Neue Technologien, disruptive Geschäftsmodelle, Digitalisierung und sich wandelnde Kundenanforderungen zwingen Unternehmen, ihre IT- und Geschäftslandschaften kontinuierlich anzupassen, um sich dauerhaft schnell und agil im Markt bewegen zu können. Wenn sie der globalen Konkurrenz weiterhin wettbewerbsfähig gegenübertreten wollen, müssen sie auf technische sowie prozessuale Veränderungen zügig reagieren und dafür IT- und Geschäftslandschaften zeitnah und sicher transformieren können. Hierfür die Voraussetzungen zu schaffen, bedeutet tiefgreifende Veränderungen in den Systemen vorzunehmen. Diese Projekte bergen viele Risiken. Entscheider tun sich daher mit Einführungen neuer Technologien und Eingriffen in Systeme schwer.

Schon vor 25 Jahren begann die Schneider-Neureither & Partner SE, sich mit den drängenden Fragen bei Veränderungen in SAP ERP-Landschaften zu beschäftigen und unterstützt heute Kunden weltweit mit hochautomatisierten Softwarelösungen bei komplexen Datenmigrationen. Doch der Blick geht schon lange über die reine Datenmigration hinaus. Denn zukünftig warten neben M&As, Carve-out & Co. nicht nur der schwierige Wechsel nach SAP S/4HANA auf Unternehmen, sondern Herausforderungen, für die schon heute Lösungen gefunden werden müssen. Schlüsselthemen sind zum Beispiel Data Analytics und Künstliche Intelligenz. Daten und ihre sinnvolle Verwertung werden in Zukunft neben der Frage, wer sich schneller und flexibler als der Wettbewerber auf neue Anforderungen ein- und seine IT-und Geschäftsprozesse umstellen kann, entscheidend sein, denn: Die Regeln, auf die sich etablierte Globalplayer in der Vergangenheit geeinigt hatten und nach denen bisher gespielt wurde, können schon morgen von den „jungen Wilden", den trotzigen Aufsteigern, die sich um Ordnungen nicht scheren, außer Kraft gesetzt werden. Unsere Antwort können nur visionäre Ideen und Lösungen mit Weitblick sein, die Unternehmen befähigen, stets einen Schritt voraus zu sein.

KEINE KLUFT ZWISCHEN PLANUNG UND UMSETZUNG DIGITALER TRANSFORMATION

Anton Kreuzer,
CEO, DriveLock SE
www.drivelock.de

Meine Vision für eine zukunftsorientierte IT in Deutschland ist eine schnelle Realisierung der digitalen Transformation. Viele Unternehmen streben diese an. Oft mangelt es jedoch an ganzheitlichen Konzepten und Investitionen. Wichtig ist ein übergreifender Ansatz für alle Felder der Unternehmens-IT. Dieser macht Unternehmen nicht nur effizienter, sondern auch weniger angreifbar als isolierte Insellösungen.

Im Kontext einer wachsenden Vernetzung von Prozessen, Geräten und Systemen muss auch die Cyber Security stark ausgebaut werden. Spionage und Sabotage bedienen sich stets neuester Methoden. Eine umfassende Cyber-Security-Strategie sollte daher ein Muss für jedes Unternehmen sein. Dabei geht es nicht mehr nur um die Abwehr von Cyberattacken, sondern zunehmend auch um das schnelle Erkennen und Reagieren auf Anomalien im System. Hierfür bedarf es der richtigen Tools: Intuitive IT-Werkzeuge auf Basis Künstlicher Intelligenz werden immer wichtiger, um die großen Datenmengen der vernetzten Systeme nutz- und analysierbar zu machen.

Und last but not least: Bei allen Initiativen und Innovationen für eine erfolgreiche digitale Zukunft darf auch die kontinuierliche Bildung und „Mitnahme" der Menschen nicht vergessen werden. Digitale Vernetzung ist nicht alleinige Aufgabe von IT-Managern, sondern muss unternehmensweit, bereichs- und abteilungsübergreifend gedacht und umgesetzt werden.

API ECONOMY READY TO GO

Rolf Scheuch, Chief Strategy Officer, Opitz Consulting GmbH
www.opitz-consulting.com

Die Verteilung von Systemen durch Cloud Computing und Microservices nimmt in unserem alltäglichen Umfeld täglich zu. Meinte man vor Jahren mit Systemintegration noch entfernte Funktionsaufrufe oder den Datenaustausch zwischen mehreren Softwaresystemen, so verschiebt sich der Umfang heute mehr und mehr. Integration umfasst zunehmend auch Dinge, Devices und Maschinen. Vielmehr noch: Der Mensch und seine Interaktionen mit Softwaresystemen rücken stärker in den Blick und Usability beeinflusst das Schnittstellen- und Kommunikationsdesign.

Bereits 2015 hat der Harvard Business Review aufgeführt, dass der Umsatz bei Unternehmen mit einem rein digitalen Geschäftsmodell zu einem großen Teil auf der Monetarisierung von APIs beruht. So generiere Expedia.de circa 90 Prozent seines Umsatzes über APIs. eBay generiert über 60 Prozent Umsatz über Transaktionen und Auktionen, die von fremden Web-Seiten initiiert werden. Die API-Economy ist also angekommen und ready-to-go für (fast) alle Unternehmen. Doch was bringt die Zukunft? Wie wird sich dieser Trend für die Unternehmen weiterentwickeln?

1. **Die Welle der Open (Public) APIs wird abnehmen, da mehr und mehr Firmen aus einer API-Nutzung monetäre Vorteile ziehen wollen.**
   Die Entwicklung im eGovernment Bereich wird gegenläufig sein, da die OpenData-Policy der Länder und Gemeinden zu einer verbreiteten Nutzung öffentlich zugängigen Daten führen wird. Ansonsten werden kostenfreie Public-API mehr und mehr Freemium Modellen weichen und über eine Basisfunktionalität hinaus werden additive Mehrwert-Dienste vertrieben.

2. **Die Digitalisierung und der Wunsch neue digitale Produkte zu generieren wird die API-Economy antreiben.**
   Hierbei ist uns noch unklar, ob es in Zukunft eine Vielzahl an unabhängigen API-Marktplätzen als Aggregatoren und Broker geben wird oder wegen der Netzwerkeffekte doch nur wenige, aber sehr umfangreiche, API-Marktplätze sich durchsetzen werden. Insbesondere werden viel Unternehmen über einen branchenbezogenen Marktplatz versuchen, Kontrolle über ein Marktsegment oder Nische zu erhalten und an den Mehrwerten der Teilnehmer zu verdienen.

3. **Conversational APIs werden immer wichtiger werden.**
   Mit dem Aufkommen von Chatbots werden APIs, die natürliche Sprache verarbeiten interessant, um automatisierte Systeme zu erstellen. Hierbei werden diese Systeme wegen den eingesetzten KI-Komponenten wahrscheinlich eher auf einem Cloud Liefer- und Servicemodell basieren somit ein Baustein einer hybriden Architektur einer API-Economy werden.

4. **APIs werden die Microservices und SaaS Nutzung verstärken.**
   Neben der verstärkten Nutzung von APIs als transparenter Zugriff auf Legacy Systeme im Zuge einer Applikationsmodernisierung, werden APIs als Tür zu Microservices sowie als Methode zur Applikationsintegration zur Verbindung von Saas-Lösungen an Bedeutung gewinnen. Insbesondere wird die Integrationslandschaft um ein Netzwerk an API-Aufrufen bereichert werden.

5. **APIs als Backbone einer hyper-connected world**
   Mit dem Internet of Everything und den deutschen Industrie 4.0-Bestrebungen wird der Informationsaustausch von Systemen und Dingen untereinander zu einem Zuwachs an APIs führen. Diese API-Welt muss kontrolliert und gesteuert werden. Insbesondere wird das Thema der API-Lineage, dem Verwendungsnachweisen der API-Nutzung, eine besondere Bedeutung zukommen, da Unternehmen ein Meta-Daten Repository benötigen, um die Vielzahl an API automatisiert zu verwalten und deren Beziehungen analysieren zu können.

Ingo Kraupa,
Vorstand,
noris network AG
www.noris.de

DIE ZUKUNFT AUS SICHT VON NORIS NETWORKS

Die Digitalisierung steht erst am Anfang. Deutschland hat mutig den Ausstieg aus Atomkraft und Kohle beschlossen, aber den Einstieg in die Digitalisierung bislang verschlafen. Die Energiewende ist ohne dem Smart-Grid, also dezentralen Erzeugern, Verbrauchern und Energiespeichern, verbunden über ein intelligentes Verteilnetz, nicht zu schaffen. Nicht nur hier sehen wir immensen (Nachhol-)Bedarf, der sich auch in einem weiter wachsenden Verbrauch an Rechenzentrumskapazitäten spiegeln wird. Weshalb noris network auch künftig besonders sichere und energieeffiziente Rechenzentren bauen und möglichst viele IT-Fachkräfte ausbilden wird.

Der aktuelle Cloud-Trend, das „Edge-Computing", wird eine Spielart bleiben. Da, wo es sinnvoll und notwendig ist, wird man Compute-Leistung auf die Fläche verteilen, aber die Mega-Datacenter werden erhalten bleiben, insbesondere für die zentrale Datenhaltung. Denn überall dort, wo auch physischer Schutz notwendig und sinnvoll ist, ist Dezentralisierung schwierig. Noch mehr Workloads als heute werden in die Cloud wandern, welche durch ihre unbestrittenen Vorteile bei Standardisierung, Skalierung und Automatisierung nicht mehr wegzudenken ist. Die großen Anbieter werden noch stärker werden, aber auch die kleineren Anbieter werden sich verbreitern, da die Eintrittshürden, um in einer Nische Cloud-Provider zu werden, sinken. Gerade die produzierenden und entwickelnden Unternehmen haben ihre Sicherheitsvorbehalte.

noris network bietet Kunden verschiedenste Public-Cloud-, Private-Cloud- und Hybrid-Lösungen mit flexiblen, skalierbaren Services – alles, um die Sicherheits-und Qualitätsbedürfnisse von Banken, Versicherungen und innovativen Mittelständlern zu erfüllen. Es ist selbst für uns sehr schwer, mit den technischen Entwicklungen Schritt zu halten. Für unsere Kunden ist es quasi unmöglich. Neben der modernen „Cloud Native"-Architektur muss auch die klassische IT noch viele Jahre zuverlässig funktionieren. In Zeiten des Fachkräftemangels keine einfache Aufgabe. Ein Einbremsen dieser Dynamik ist derzeit noch nicht zu erkennen, weshalb der IT-Sektor selbst bei einer sich eintrübenden Gesamtwirtschaftslage keinen massiven Einbruch erleben wird – Veränderungen wird es aber geben.

FLEXIBLERE MÖGLICHKEITEN FÜR DEN ZUKÜNFTIGEN ARBEITSPLATZ

„Unternehmen, die heute Webseiten benutzen um zu informieren, werden morgen diese Webseiten auch nutzen um zu kommunizieren", das ist die Vision von estos. Mit dem LiveChat legt der Starnberger Softwaresteller die Grundlage, diese Vision zu verwirklichen: Unternehmen können Webseitenbesuchern den direkten Kontakt zu einem geeigneten Experten anbieten. Interaktive Touchpoints wie das Webseiten Widget, das Kontaktportal oder die elektronische Visitenkarte zeigen geeignete Ansprechpartner aus dem Unternehmen mit Kontaktmöglichkeiten wie Text- oder Video-Chat. Der Kunde oder Interessent tritt dadurch früher als bisher in Kontakt mit dem Unternehmen, wichtige Fragen können zu einem deutlich früheren Zeitpunkt geklärt werden. Die Entscheidungszeiten verkürzen sich. Gerade die Beratung per Video, von Angesicht zu Angesicht, erlaubt den persönlichen Kontakt. Die Webseitenbesucher benötigen weder eine zusätzliche Software oder ein Plug-In. Stärkere Kundenbindung und -zufriedenheit, höhere Produktivität, verbesserte Customer Journey und höhere Conversion-Rate sind die wesentlichen Vorteile.

LiveChat bietet nicht nur einen weiteren Kommunikationskanal, sondern für Unternehmen auch die Möglichkeit, Berater automatisiert sinnvoll auf Webseitenbesucher zu verteilen. Grundlage hierfür ist das Präsenz-Management-System, in dem alle Informationen über die Verfügbarkeit von Mitarbeiterinnen und Mitarbeitern gebündelt werden. Unternehmensexperten stehen so entsprechend ihrer aktuellen Erreichbarkeit für Kunden und Interessenten digital zur Verfügung. In der Unified Communications & CTI Software Suite ProCall Enterprise Software sorgt das Präsenz-Management-System für Transparenz über die Erreichbarkeit von Kolleginnen und Kollegen: Unabhängig von Zeit und Ort können die Benutzer mit einem Endgerät wie PC, Laptop, Tablet oder Smartphone sehen, welcher ihrer Kontakte gerade auf welchem Weg erreichbar ist und eine der Situation angepasste Kommunikationsart wählen. Diese Transparenz der Erreichbarkeiten eröffnet neue und flexiblere Möglichkeiten für künftige Arbeitsplatz- und Arbeitszeitmodelle.

Sibylle Klein, Content Production Manager, estos | www.estos.de

Alexander Stühl,
Director Sales und Marketing,
Aagon GmbH | www.aagon.de

CLIENT MANAGEMENT UND DIE AUTOMATION DER UNTERNEHMENS-IT

Je schneller die IT eines Unternehmens wächst, desto eher stoßen auch Administratoren an ihre Belastungsgrenzen. Jeder neue Rechner im System, jede neue Softwareinstallation ist mit erheblichem Mehraufwand verbunden. Eine mögliche Antwort auf diese rasante Entwicklung ist Automation mit einer Clientmanagement-Lösung. Wie sonst soll die IT-Abteilung mit zunehmenden Arbeitsaufgaben Schritt halten?

In absehbarer Zeit wird vor allem die reine Arbeitsbelastung für IT-Abteilungen zunehmen. Nicht alle dieser Mehranforderungen sind hausgemacht, sondern kommen hauptsächlich von den Anforderungen der zunehmenden Digitalisierung. Fehlendes Werkzeug, Wissen oder Lösungsansätze können die Situation noch verschärfen. So bleibt wenig Zeit für die Einführung neuer Prozesse und kaum Spielraum für die Rolle, in der sich viele Beschäftigte der IT-Abteilungen gerne sähen: Als Innovatoren und digitale Wegweiser für ihr Unternehmen. Vor dem Hintergrund dieser Misere kommen IT-Verantwortliche nicht um das Thema Automation herum.

Zukünftig ist zusätzlich zu den üblichen Themen wie Migration und Softwareverteilung auch ein radikales Umdenken im Bereich der Sicherheitskonzepte gefordert. Diese Herausforderungen zwingen Unternehmen jeder Größe dazu, ihre IT zukunftsfähig und langfristig flexibel aufzustellen. Spätestens, wenn die Arbeitsbelastung der IT-Abteilung dauerhaft an die absolute Obergrenze stößt, kommen häufig ernsthafte Überlegungen ins Gespräch regelmäßig anfallende Aufgaben per Automation zu erledigen.

Klassische IT war bisher darauf ausgelegt „die Unternehmensmaschine" am Laufen zu halten. Zukünftig wird sich diese Rolle ändern – auch dank Automation, die viele Aufgaben des üblichen Tagesgeschäfts übernehmen wird. Ziel muss es sein eine einheitliche Softwarelandschaft und einen gleichen Stand aller Clients und ihrer Betriebssysteme zu erreichen. Besonders beim Betriebssystem gilt es für viele Unternehmen eine gewaltige Aufgabe zu stemmen, denn mit dem endenden Support für Windows 7 im Januar 2020 wird die Migration auf Windows 10 unumgänglich.

Die Vorteile liegen klar auf der Hand: Automatisierte Arbeitsprozesse in der IT schaffen transparente Prozesse und für das Unternehmen selbst wirtschaftliche Vorteile. Das brennende Problem vieler IT-Abteilungen, nur begrenzte Ressourcen zur Verfügung zu haben, ist damit zwar noch nicht gelöst, diese haben aber nun genug Freiräume, auch andere als wirtschaftliche Ansätze zu verfolgen.

Automation ist auch im Bereich der IT-Sicherheit ein wichtiger Aspekt. Vordefinierte Maßnahmen, die standardisiert auf Security-Breaches und Angriffe reagieren, entlasten IT-Abteilungen im Ernstfall enorm. Sie bieten genügend Spielraum um Entscheidungen überlegt und mit kühlem Kopf auf Bedrohungen auf das Unternehmens-Netzwerk und unternehmenskritische Daten zu reagieren.

Moderne Automations-Lösungen kombinieren Antivirus-Produkte mit Clientmanagement-Aufgaben und bieten damit ein hervorragendes Werkzeug für Administratoren zur Abwehr und Schutz der eigenen IT-Landschaft. Automation ist der richtige Schritt die IT-Abteilung eines Unternehmens zukunftsfähig aufzustellen. Effektive Kostensenkung, eine allgemeine Entlastung der Mitarbeiter und volle Kontrolle über die Unternehmens-IT wirken sich positiv auf die Produktivität des Unternehmens aus und sparen bares Geld. Wer das große Potenzial von Automation erkennt und Clientmanagement als echte Chance für die eigene Unternehmens-IT begreift, baut an deren Zukunft.

OPITZ CONSULTING

Überraschend mehr Möglichkeiten

> DIGITALE
> SERVICE
> MANUFAKTUR

Changeability & Innovationen als Schlüssel der Digitalisierung

Geschwindigkeit und Continuity durch Services

Individuelle & passgenaue Lösungen mit flexibler Architektur

Sprechen Sie uns an:
Telefon: +49 2261 6001-0 · E-Mail: info@opitz-consulting.com

TEIL

2

Eine Content-Strategie ist die Basis für langfristigen Online-Erfolg. Denn sie hilft Ihnen dabei, Ihre Aktivitäten strategisch auszurichten, effizient zu planen und sich auf Ihre Ziele zu fokussieren. So können Sie sich zum einen von Ihren Mitbewerbern absetzen und zum anderen die Suchmaschinen und die Nutzer von sich überzeugen. In Teil 1 wir Ihnen die theoretischen Hintergründe einer Content-Strategie erläutert. Im 2. Teil zeigen wir Ihnen nun, wie Sie diese praktisch umsetzen.

1. Schritt: Ziel-Definition

Die Content-Erstellung ist immer Mittel zum Zweck, egal ob Sie einen Online-Unternehmensauftritt pflegen, einen Shop oder Blog betreiben. Online-Inhalte sind kein Selbstzweck, sondern wollen gelesen werden und beim Nutzer eine Handlung auslösen (und sei es nur ein weiterer Besuch der Website, weil die Texte so schön waren). Ihre Content-Strategie richten Sie danach aus, was Sie erreichen möchten. Legen Sie im ersten Schritt daher Ihre Ziele fest. Sofern nicht bereits, beispielsweise unternehmensseitig, Zielvorgaben gesetzt sind, haben Sie diese Möglichkeiten:

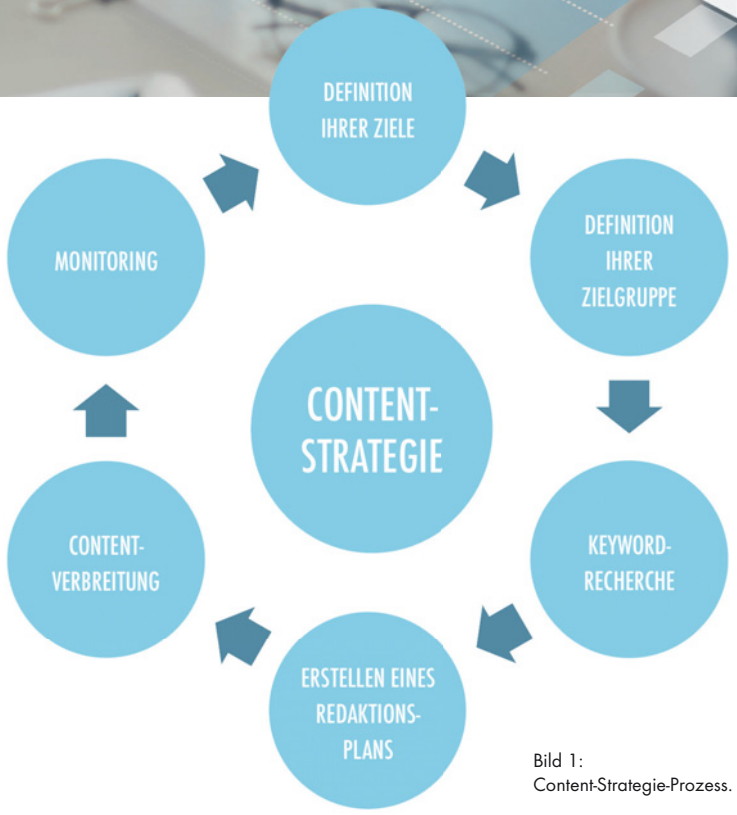


Bild 1: Content-Strategie-Prozess.

- Beim **Marketingansatz** analysieren Sie marketingrelevante Kennzahlen und stellen sich folgende Fragen: Wie hat sich Ihr Umsatz im letzten halben Jahr/Jahr entwickelt? Wie viele Abonnenten Ihres Blogs begiehungsweise Follower Ihrer Social-Media-Kanäle haben Sie in diesem Zeitraum gewonnen? Konnten Sie eine Steigerung Ihrer Bekanntheit erzielen? Sind Sie mit diesen Kennzahlen unzufrieden, können Sie diese mithilfe des Contents optimieren.

STRATEGISCH UND DURCHDACHT

UMSETZUNG EINER ERFOLGREICHEN CONTENT-STRATEGIE.

Sie erstellen dann Inhalte, mit denen Sie Ihren Umsatz und Ihre Markenbekanntheit verbessern können, und Sie verstärken Ihre Social-Media-Aktivitäten durch gezielte Kampagnen.

- Beim **SEO-Ansatz** analysieren Sie die Content-Performance Ihrer Website: Wie haben sich die Keyword-Rankings im letzten halben Jahr/Jahr entwickelt? Wie viele neue Besucher kamen auf Ihre Website? Wie lange haben sich die Nutzer durchschnittlich auf Ihren Seiten aufgehalten? Wenn diese Kennzahlen nicht das gewünschte Bild ergeben, haben Sie mit dem Content Ansatzpunkte, um diese zu verbessern. Sie sollten dann Inhalte erstellen, die gezielt auf die Suchanfragen der Nutzer ausgerichtet sind. Damit sind Sie zum einen besser bei Google & Co. auffindbar, zum anderen können Sie die Suchanfragen der Nutzer so optimaler befriedigen.

2. Schritt: Zielgruppen-Definition

Sie sollten für Ihre Content-Strategie festlegen, für welche Zielgruppe/n Sie Inhalte produzieren. Wenn Sie auf deren Wünsche und Bedürfnisse eingehen, können diese direkter ansprechen und damit auch Ihre Ziele einfacher erreichen. Es gibt zwei verschiedene Ansätze:

- Wenn Sie Zugriff auf Daten haben, die Ihnen bereits etwas über Ihre Fans oder Kunden sagen, wie Alter und Geschlecht, können Sie daraus Ihre Zielgruppe entwickeln. So wissen Sie schließlich schon, wer Ihnen folgt oder gerne bei Ihnen kauft, und können passende Inhalte bieten. Neben den Kundendaten aus Bestellungen liefern solche Informationen auch Social-Media-Portale.

- Alternativ können Sie von Ihren Produkten, Dienstleistungen oder bestehenden Inhalten ausgehen. Für wen sind diese interessant? Legen Sie Personas fest, welche die Zielgruppen beschreiben.

Achten Sie bei der Content-Erstellung darauf, dass Sie sich in die Zielgruppe/n hineinversetzen: Welche Fragen haben sie? Welche Bedürfnisse und Probleme beschäftigen sie? Auf diese Weise produzieren Sie Inhalte, die echten Mehrwert bieten.

3. Schritt: Keyword-Recherche

Für die Keyword-Recherche stehen verschiedene Tools zur Verfügung:

- Google AdWords Keyword Planner – ist die erste Anlaufstelle, da er Suchvolumina angibt. Alternativen hierzu: Searchmetrics und searchvolume.io. Er dient dazu, das Fokuskeyword zu finden, auf das Sie den Inhalt primär ausrichten.

  Dieses ist in der Regel der Begriff unter Synonymen mit dem höchsten Suchvolumen. Sie können mit diesem Tool aber auch recherchieren, welche Suchanfragen aus einem Themengebiet für die Nutzer interessant sind und diese dann mit passenden Inhalten bedienen.

- Mit Longtail-Keywordtools wie keywordtool.io oder answerthepublic finden Sie verwandte Suchbegriffe zum Fokuskeyword und können Ihre Inhalte mit diesen noch relevanter machen.

- W-Fragen-Tools wie HyperSuggest oder termlabs Questionfinder dienen dazu, konkrete Nutzerfragen zu recherchieren. Diese zeigen Ihnen, was die Nutzer wissen möchten. Sie dienen als Grundlage bzw. Gliederung für neue Inhalte und helfen Ihnen, den Content auf Ihre Zielgruppe auszurichten.

Nutzen Sie möglichst viele Tools, denn so entsteht ein deutlicheres Bild des Nutzerinteresses. Umso besser Sie dieses bedienen, umso relevanter werden die Inhalte für die

	Fokus-Keyword	Synonyme & neue Themen	Suchvolumina	Longtail-Keywords	W-Fragen	WDF*IDF Keywords
Google AdWords Keyword Planner	x	x	x	x		
searchmetrics	x	x	x	x	x	
searchvolume.io	x		x			
Keyword Tool				x	x	
ANSWER THE PUBLIC				x	x	
HYPERSUGGEST					x	
TermLabs.io					x	x

Bild 2: Keyword-Recherche-Tools im Überblick.

Nutzer und damit auch für die Suchmaschinen. Fassen Sie semantisch zusammengehörende Keywords zu Themen zusammen. So bauen Sie sich ein Keyword-Set pro Text auf mit

- ein bis drei Fokuskeywords
- Synonymen und verwandten Wörtern
- Thematisch relevanten Phrasen und Fragen

- **Seite rankt zwischen Position 11 und 20:** Sie sollten mit einem WDF*IDF-Tool wie Content Succes von Ryte oder termlabs TF*IDF Data prüfen, ob Ihrem Text relevanzschaffende Wörter fehlen.

- **Seite rankt schlechter als Position 20:** Sie sollten den Text umfassend überarbeiten.

Um den Redaktionsplan zu erstellen, gehen Sie folgendermaßen vor:

- Beschriften Sie die Spalten mit diesen Informationen:
  - **Monat**, in dem der Text erstellt werden soll; alternativ können Sie hier auch ein exaktes Datum als Deadline festlegen.
  - **Thema des Contents beziehungsweise Arbeitstitel für den Text.**
  - **To-do:** Neuerstellung, Überarbeitung etc.
  - **Content-Art:** Ist der Text für eine Shopkategorie, eine Produktseite oder einen informationalen Content-Bereich wie Ratgeber, Magazin, Blog?

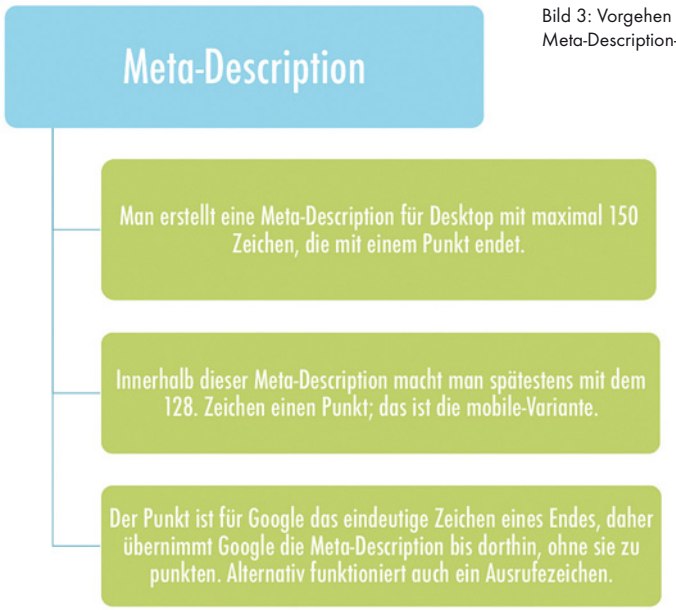


Bild 3: Vorgehen Meta-Description-Erstellung.

Teil der Keyword-Recherche sollte unbedingt eine Ranking-Abfrage sein. Denn so sehen Sie, ob Sie mit einer Seite für ein Keyword bereits ranken. Bestehen Rankings, müssen Sie entscheiden, was Sie tun:

- **Seite rankt unter den Top-3:** Sie sollten keinen neuen Content für dieses Keyword erstellen.

- **Seite rankt zwischen Position 4 und 10:** Sie sollten prüfen, wie Sie diese weiter nach oben bekommen. Mögliche Maßnahmen sind die Optimierung von Title-Tag und Meta-Description. Die Überarbeitung des Inhalts, wenn dieser veraltet ist beziehungsweise nicht so gut oder so ausführlich, wie der Inhalt der Besser-Rankenden.

- **Es gibt keine Rankings:** Sie erstellen eine komplett neue Seite.

4. Schritt: Der Redaktionsplan

Es gibt verschiedene Tools, die es Ihnen ermöglichen, einen Redaktionsplan zu erstellen. Meistens ist aber eine Excel-Liste (beispielsweise eine Online-Liste in Google Drive) ausreichend.

- Keywords
- Keywordfunktion: Fokuskeyword, Nebenkeyword, W-Frage oder relevanzschaffendes Wort
- Suchvolumen für jedes Keyword
- Inhalte: Hier können Sie den Inhalt des Textes konkretisieren; dies bietet sich vor allem an, wenn der Redaktionsplan als Texter-Briefing dient.

- Legen Sie Filter an; so können Sie später, wenn der Plan gut gefüllt ist, bequem nach Daten suchen wie bestimmte Keywords oder Themen – so vermeiden Sie zudem Überschneidungen.

5. Schritt: Texterstellung

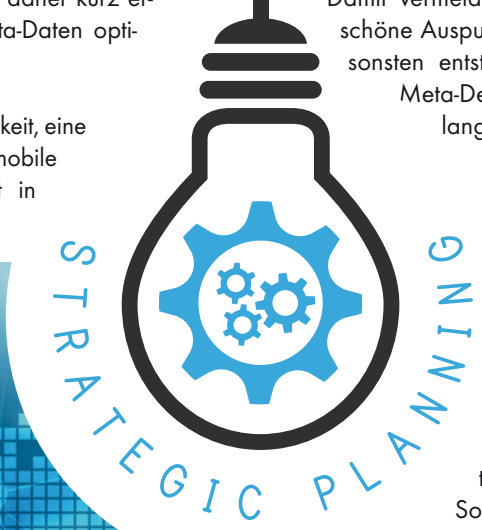
Wie in Teil 1 beschrieben, sollten Sie Ihre Inhalte für Suchmaschinen optimieren. In Teil 2 möchten wir Ihnen daher kurz erklären, wie Sie Ihre Meta-Daten optimal erstellen.

Denn es gibt eine Möglichkeit, eine Meta-Description für die mobile und die Desktop-Ansicht in einem zu erstellen:

- Schreiben Sie für die Desktop-Ansicht eine Meta-Description mit maximal 150 Zeichen. Das 150. Zeichen sollte ein Punkt oder ein Ausrufezeichen sein.

- Für die mobile Ansicht schreiben Sie diese Description so, dass Sie innerhalb der 150 Zeichen einen Satzteil bereits mit spätestens dem 128. Zeichen mit einem Punkt oder Ausrufezeichen enden lassen.

Punkt und Ausrufezeichen markieren für Google ein exaktes Ende. Damit haben Sie die Chance, dass Google für die mobile Ansicht nur den Teil der Description ausspielt, der vor dem 128. Zeichen steht. Damit vermeiden Sie die unschöne Auspunktung, die ansonsten entsteht, wenn die Meta-Description zu lang ist.



6. Schritt: Verbreitung

Nutzen Sie hierfür erst einmal Ihre eigenen Netzwerke. Teilen Sie Ihren Content auf Ihren Sozialen Medien und machen Sie in Ihrem Newsletter darauf aufmerksam. Der zweite Schritt ist dann die Kooperation mit möglichen Partnern. Das klappt aber nur erfolgreich und googlekonform, wenn Sie wirklich verlinkungswürdige Inhalte anzubieten haben.

Der Content muss Mehrwert haben und einzigartig sein wie bei einem E-Book oder Whitepaper, einer Infografik oder einem umfassenden Ratgeber.

Recherchieren Sie mithilfe der Google-Suche Webseiten wie Blogs oder Portale, die thematisch zu Ihrer Webseite passen. Kontaktieren Sie den Ansprechpartner der Webseite, bitten Sie ihn über Ihre Inhalte in einem Beitrag zu berichten und dann auf Ihre Webseite zu verlinken. Dessen Leser werden so auf Ihre Inhalte aufmerksam und können durch den Link direkt zu Ihrer Seite gelangen. Und nicht zu vergessen: Links sind ein wichtiges Ranking-Kriterium für die Suchmaschinen!

7. Schritt: Monitoring

Um das Monitoring einzurichten, gehen Sie wieder ähnlich vor wie bei der Erstellung des Redaktionsplans:

- Beschriften Sie die Spalten mit den Kennzahlen, die Sie monitoren möchten. Zu empfehlen sind: Rankings, Backlinks, Social Signals, Verweildauer, Klickrate und neue Besucher.

- Reservieren Sie die erste Spalte für die URL.

- Tragen Sie die Kennzahlen jeweils pro URL ein.

- Nutzen Sie auch hier die Filter, damit Sie sich später beispielsweise die Rankings für eine URL bequem ansehen zu können.

Fazit

Wenn Sie bei der Content-Erstellung strategisch und durchdacht vorgehen, werden Sie schon bald erste Erfolge sehen. Aus dem Monitoring ziehen Sie sich beständig Erkenntnisse, mit denen Sie Ihre Inhalte weiter optimieren können. So ist die Content-Produktion keine einmalige Geschichte, sondern ein fortlaufender erfolgreicher Prozess.

Dr. Beatrice Eiring

DIE CONTENT-ERSTELLUNG IST IMMER MITTEL ZUM ZWECK, EGAL OB SIE EINEN ONLINE-UNTERNEHMENSAUFTRITT PFLEGEN, EINEN SHOP ODER BLOG BETREIBEN.

Dr. Beatrice Eiring, Head of Content Creation, eology GmbH | www.eology.de

IAM CONNECT 2019

Die Brücke zu neuen Geschäftsmodellen

Die IAM CONNECT, die größte deutschsprachige Konferenz zum Thema Identity & Access Management vom 18. bis 20. März in Berlin, bietet Ihnen auch 2019 wieder ein praxisnahes Programm: hochkarätige Sprecher großer Unternehmen teilen ihre Erfahrungen und Visionen mit Ihnen. Freuen Sie sich auf konstruktive Gespräche mit Kollegen auf hohem fachlichen Niveau.

Konferenz
18. bis 20. März 2019
in Berlin

Agenda und Anmeldung unter

www.iamconnect.de

Hauptsponsor

ipg
EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Speed Demo Sessions

AIRLOCK by ergon
BeyondTrust
DIERICHSWEILER Unternehmens- und Prozessberatung
iSM SECU-SYS AG
welcome

Eine Veranstaltung von itmanagement & itsecurity

Highlights aus der Agenda

Vorträge

Sichere Identitätsmanagement-system (FIDES)

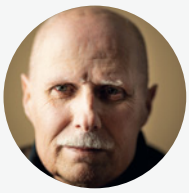
Dr. Manfred Paeschke, Chief Visionary Officer, Bundesdruckerei GmbH

Schrittweise ein rollenbasiertes IAM in einem compliance-getriebenen Unternehmen etablieren

Dominik Schönwetter, A1 Telekom Austria AG

Einführung eines IAM in 20 Tagen bei der Krankenkasse IKK classic

Stefan Schellberg, IKK classic



Privilegierte Accounts mit IdM-Bordmitteln managen

Peter Will, Bundesamt für Justiz

IAM ganzheitlich: Die Herausforderungen einer Spitalgruppe

Michael Geisser, Spital Thurgau AG

Hier geht´s zur aktuellen Agenda:
www.iamconnect.de

Workshops

DSGVO - Fazit nach 10 Monaten

Ralf Schulten, Rechtsanwalt, avocado rechtsanwälte

IAM & API-Sicherheit

Karsten Müller-Corbach, CISSP, Ping Identity Regional Solutions Architect

Privileged Access Management als Erweiterung des IAM

Dennis Weyel, Senior Technology Consultant, BeyondTrust

NEVIS MAKE SECURITY AN ASSET · NEXIS · OGITIX Einfach schneller am Ziel! · ONE IDENTITY · Ping Identity. · WALLIX CYBERSECURITY SIMPLIFIED

HANNOVER MESSE 2019

WIE DIE INDUSTRIE NOCH INTELLIGENTER WIRD.

In der Industrie ist heute eines klar: ohne IT läuft nichts. Ob in der Produktion, der Energiebranche oder der Logistik, Themen wie Blockchain, Cybersicherheit, Künstliche Intelligenz und Plattformökonomien stehen an vorderster Front. Nur damit können Unternehmen ihre Wettbewerbsfähigkeit erhalten. Auf der HANNOVER MESSE zeigen Aussteller wie man Fabriken, Lagerhallen oder dezentrale Kraftwerke intelligent vernetzt.

In der Industrie ermöglicht erst die Digitalisierung effizientere, nachhaltigere Prozesse sowie die Entwicklung neuer Geschäftsmodelle. Dies gilt nicht nur für Produktionsverfahren, sondern auch für die Energie- oder Logistikbranche. Mithilfe Industrie 4.0-Technologien vernetzen Unternehmen ihre Lieferanten, Kunden und Partner entlang der gesamten Wertschöpfungskette. Aus dieser Form der Zusammenarbeit entstehen nicht nur einzelne Bauteile, sondern ganzheitliche Lösungen.

Industrial Intelligence

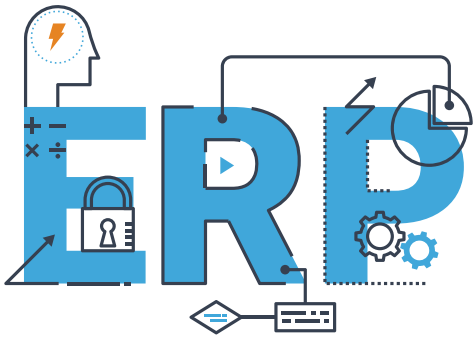
Vom 1. bis zum 5. April 2019 öffnet die HANNOVER MESSE erneut ihre Tore. Rund 6 500 Aussteller präsentieren sich auf der Weltleitmesse der Industrie. Das Leitthema lautet „Integrated Industry – Industrial Intelligence" und unterstreicht die zunehmende Bedeutung von maschinellem Lernen. Der Mensch nutzt künftig künstliche Intelligenz, damit Maschinen und Fabriken sich selber steuern. Dabei geht es nicht nur um Prozessoptimierung oder Energieeffizienz, sondern auch um Schnittstellen, Protokolle und Sicherheit.

Im Hinblick auf die Digitalisierung sind neue Sofware- und IT-Entwicklungen für Firmen im verarbeitenden Gewerbe besonders entscheidend. Daher ist der entsprechende Bereich auf der HANNOVER MESSE wieder gewachsen. Zu den Top-Themen zählen künstliche Intelligenz und Plattformökonomien sowie hybride Clouds, Augmented und Virtual Reality, 5G, Blockchain oder Digital Twin. Bisher dabei sind traditionelle Softwarehäuser und Cloudkonzerne wie etwa Amazon Web Services, Atos, Dassault Systems, EPLAN, Huawei, IBM, Konica Minolta, Microsoft, Oracle, SAP, Siemens PLM und Software AG. Insgesamt zeigen mehr als 600 Aussteller ihre Lösungen für integrierte Prozesse zur industriellen Anwendung.

Wissenstransfer

Die Digitalisierung hat globale Auswirkungen auf Industrie, Mitarbeiter und Gesellschaft. Die HANNOVER MESSE zeigt die aktuellen Chancen und Stolpersteine nicht nur auf den Ständen der Austeller, sondern auch in den mehr als 90 Konferenzen und Foren. Damit schafft die Weltleitmesse der Industrie einen einzigartigen Wissenstransfer zwischen der Industrie, Wirtschaft und Politik. Das Partnerland Schweden passt perfekt in das Programm, denn die schwedische Regierung setzt stark auf eine intelligente Industrie. Dabei fokussiert sich das Land auf schwedisch-deutsche Innovationspartnerschaften unter anderem in den Bereichen Mobilität, Testumfelder und Digitalisierung von KMUs. In Hannover präsentieren sich mehr als 100 schwedische Aussteller inmitten der Weltmarktführer in Sachen Industrie 4.0.

www.hannovermesse.de



INDIVIDUELL BETRACHTET

DIE MODERNE ARCHITEKTUR IN ERP-SYSTEMEN.

Wie ein Bauherr beim Eigenheim müssen auch IT-Verantwortliche bei einem ERP auf eine solide und tragfähige Architektur achten. ERP-Systeme (Enterprise-Ressource-Planning-Systeme) umfassen die Durchführung von weitestgehend allen Geschäftsprozessen, um die Ressourcen, wie Material, Personal, Finanzen, Information, unternehmensweit verwalten zu können. Ein ERP-System baut auf einer Datenbank auf und deckt diverse Funktionen aus mehreren Anwendungsbereichen ab.

Die klassische Architektur eines ERP-Systems besitzt eine Multi-Tier-Architektur, bestehend aus einer Drei-Schichten-Architektur: Client, Server und Datenbank.

Der Rechner, welcher Anforderungen stellt, wird als Client definiert und das System, welches jene Anforderungen ausführt und die Ergebnisse zurücksendet, als Server. Die Kommunikation zwischen Client und Server erfolgt durch Transaktionen: Der Client generiert die Transaktion und der Server verarbeitet diese. Alle Geschäftsaktivitäten werden mithilfe solcher Transaktionen durchgeführt. Diese Art von Architektur kann in 3 Teile/ Schichten untergliedert werden:

Die Präsentationsschicht (sog. client / „Front-End'') bildet die Benutzeroberfläche. Sie stellt die Schnittstelle zwischen Benutzer und Anwendungssystem dar. Die Eingaben auf der Benutzeroberfläche werden an die Anwendungsschicht/Logikschicht weitergegeben.

Die Anwendungsschicht (sog. server) besteht aus der Applikation selbst und ist das Kernstück der Software. Hier werden die eingegebenen Daten verarbeitet.

In der Datenschicht (sog. Back-End) werden alle Klassen und Dialoge in Tabellen verwaltet. Der Server schickt SQL-Anfragen an die Datenbank, diese sucht in den definierten Tabellen nach dem Ergebnis und schickt eine Antwort zurück.

Interoperabilität

Dieses Client-Server-Architekturmodell ermöglicht eine Aufteilung von Programmen, sodass diese auf verschiedenen Systemen funktionieren können. Dadurch kann eine Verteilung der Verarbeitung oder Datenhaltung erzielt werden. Durch die Verteilung der Verarbeitung ist es möglich, mehrere Funktionen unabhängig voneinander und parallel zu verwenden.

Die neueren ERP-Systeme basieren zumeist auf einer Java-Architektur. Viele Anbieter verwenden heutzutage die Architektur der „Java Enterprise Edition" (Java EE). Diese Architektur ermöglicht eine Interoperabilität, Wiederverwendbarkeit und Erweiterbarkeit von ERP-Systemen. Damit ist es möglich die Anforderungen, die an moderne Businessanwendungen gestellt werden, zu erfüllen. Das Merkmal einer javabasierten Architektur ist insbesondere die Persistenz der Datenhaltung. Das heißt die sichere Durchführung von Transaktionen kann gewährleistet und die Verbindung zwischen Server und Client kann verschlüsselt werden. Ein weiteres Merkmal ist auch die Wiederverwendung der in Java geschriebenen Serverkomponenten. Durch dessen Interoperabilität ist die Anpassung an die sich verändernden Anforderungen erheblich leichter umzusetzen.

Wie die Architektur eines Bauwerks ist auch die Systemarchitektur flexibel in ihrer Gestaltung, solange diese auf ein beständiges Fundament aufbaut. Zu beachten ist vorwiegend, was genau benötigt und damit den Anforderungen gerecht wird. Eine vierköpfige Familie – um die Eingangsparallele zum Bauherrn wieder aufzugreifen – benötigt keine architektonische Ausnahmeerscheinung eines Opernhauses. Es lässt sich daher nicht pauschal beantworten, welche Architektur zu welchem Unternehmen passt. Der Einzelfall sollte stets individuell betrachtet werden.

Tülin Duman, Christine Schuhmacher
www.caniaserp.de

AGILES EAM IST

KATALYSATOR FÜR DIE DIGITALE TRANSFORMATION.

Die Rolle des Enterprise-Architekten muss erweitert werden, um mit den neuen Entwicklungen in Unternehmen Schritt halten zu können. Die Grundwerte Stabilität und Nachhaltigkeit sind zwar weiterhin gültig, jedoch kommen neue Anforderungen hinzu – und dazu zählt unter anderem Tempo. Erst dann wird Enterprise Architecture zum Enabler und nicht zum Verhinderer.
In der Arbeitsgruppe „Angewandtes agiles EAM" untersuchte das Cross-Business-Architecture Lab die Zukunft des Enterprise Architecture Management. Das traditionelle Mandat der Architekten lautet für Struktur, Stabilität, Standards, Methoden und ihre Einhaltung zu sorgen. Allerdings muss es nun ergänzt werden, um dem Wandel der Unternehmen hin zu mehr Initiative, Dynamik, Kreativität und Innovation besser gerecht zu werden.

Dieses neue, erweiterte Mandat basiert auf der Einsicht, dass Architektur in einer Welt, die geprägt ist von rasanten Veränderungen, Unsicherheit, zunehmender Komplexität und Ungewissheit immer nur temporär – phasenbezogen – Klarheit und Verständnis schaffen kann. Dieses Verstehen ist Grundlage für die Entwicklung agiler Prozesse, die Unternehmen in einer volatilen Welt handlungsfähig machen. Aber da Architektur immer nur zeitweise stabile Plattformen herstellen kann, muss sie auch selbst beweglicher und schneller werden und sich selbst der agilen Methoden bedienen, die zum Beispiel in der IT-Entwicklung genutzt werden.

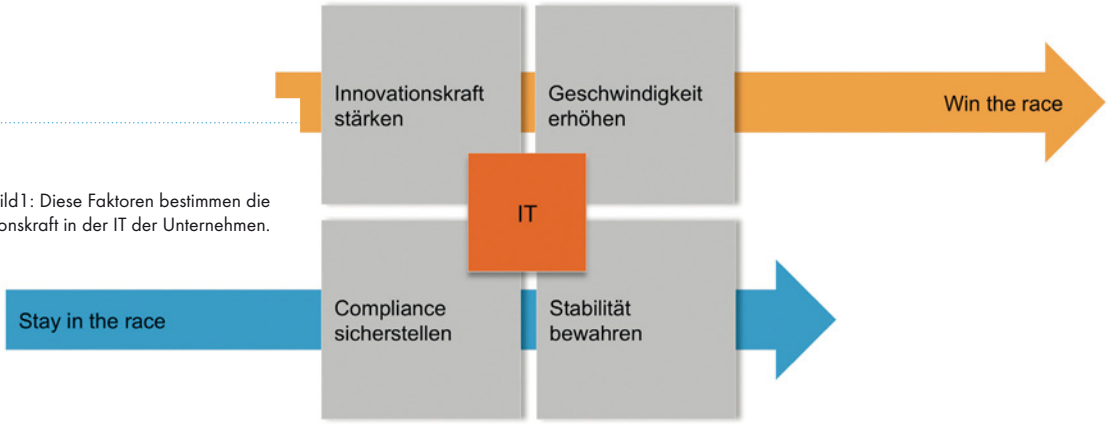


Bild1: Diese Faktoren bestimmen die Innovationskraft in der IT der Unternehmen.

Whitepaper:
Das Whitepaper „EA goes agile":
https://bit.ly/2N3bqRJ

Enterprise-Architekten müssen ins Feld

Je mehr agile Methoden im Unternehmen Einzug halten, desto größer wird die Diskrepanz zum traditionellen Enterprise Architecture Management (EAM). Es entsteht ein Spannungsfeld zwischen Bewahren und Verändern. Denn das klassische EAM beschäftigt sich mit der zukünftigen Ausrichtung der IT-Landschaft – der Soll-Architektur. Aktuelle Probleme lassen sich damit kaum lösen, denn es ist zu unflexibel.

Agiles EAM dagegen ist auf die Lösung konkreter Probleme gerichtet und kann flexibel auf Veränderung reagieren. „Enterprise-Architekten werden einfach Teil der Teams. Sie gehen ins Feld, sie haben häufigen Kundenkontakt und sie verarbeiten die Inputs aus regelmäßigen Feedbackrunden schnell", betont CBA-Lab-Workstreamleiter Marc Gorges, der als Enterprise-Architekt bei Bosch arbeitet. Denn Enterprise Architecture soll kein „Show Stopper" sein, sondern aktiver Teambestandteil, der Chancen realisiert, zu besseren Services und Produkten beiträgt und letztlich zu mehr Einnahmen des Unternehmens führt.
Gorges Kollege Bernhard Lerch, ebenfalls bei Bosch, ergänzt: „Die Unternehmen wandeln sich zurzeit rasant, diesen Wandel gestaltet die Enterprise Architecture aktiv mit. Sie erweitert ihre Ziele und ihren Satz an agilen Methoden erheblich."

Drei Anforderungen an das neue EAM

Ein verändertes Selbstverständnis und Wertesystem gepaart mit einem zeitgemäßen Mandat führt zu einer gewandelten Zielsetzung der Unternehmensarchitektur im digitalen und agilen Umfeld.

Drei Kriterien kennzeichnen ein Unternehmensarchitekturmanagement, das den Zielen gerecht wird:

1. Es ist fokussiert und auf Wirksamkeit und Wertschöpfung ausgerichtet. Es ist lösungsorientiert, sieht Enabling und

UNVERZICHTBAR

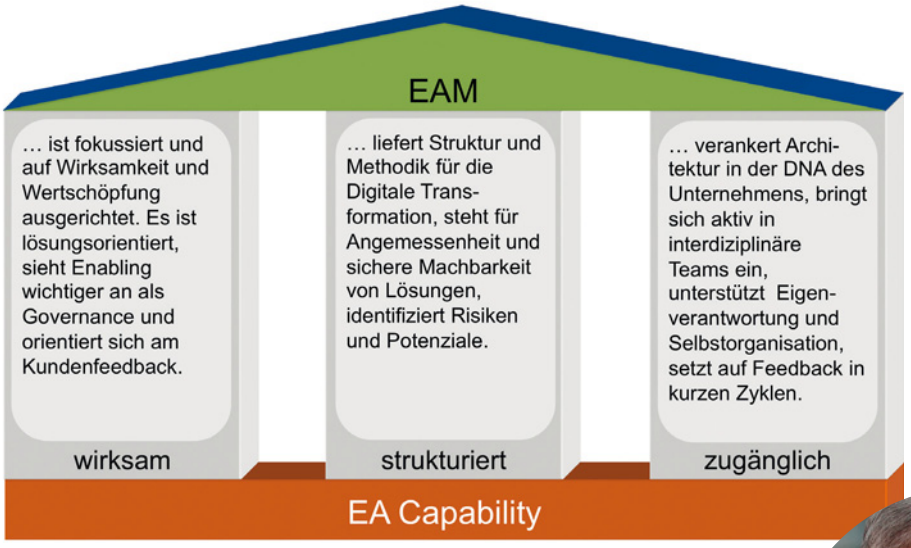


Bild 2: Der Aufbau eines Enterprise Architecture Managements (EAM).

das Setzen von Leitplanken wichtiger an als strikte Governance und orientiert sich immer am Kundenfeedback.

2. Es liefert Struktur und Methodik für die Digitale Transformation, steht für Angemessenheit und sichere Machbarkeit von Lösungen, identifiziert Risiken und Potenziale.

3. Es verankert Architektur in der DNA des Unternehmens, bringt sich aktiv in interdisziplinäre Teams ein, unterstützt Eigenverantwortlichkeit und Selbstorganisation und setzt auf Feedback in kurzen Zyklen.

Diese Ziele lassen sich nicht mit einem zentralen Enterprise-Architektur-Ansatz realisieren, der nur von einigen Personen aktiv betrieben wird. Dazu braucht es einen breiteren Ansatz, den zum Beispiel das „Architectural Thinking" darstellt. Architectural Thinking zielt auf die Etablierung eines kollektiven Verständnisses von „exzellenten Produkten und Services" und fördert eine „diesem Zweck dienende Architektur".

Der Ansatz geht von einer breiten Verankerung eines Architekturverständnisses im Unternehmen aus, sodass Unternehmensarchitektur nicht mehr vorgeschrieben werden und durchgesetzt werden muss, sondern in der DNA des Unternehmens verankert und gelebt werden kann. In etwa ist das vergleichbar mit dem Verständnis von Haus- und Stadtarchitektur. Heute haben viel Menschen ein Gefühl dafür, was ein „schönes" Haus oder ein „guter" Stadtteil ist.

Gorges verdeutlicht den Anspruch an zwei Beispielen: „Es besteht ein kollektives Verständnis zur Sinnhaftigkeit der Mülltrennung sowie zur Anschnallpflicht. Ähnlich strebt Architectural Thinking als Zielbild ein kollektives Verständnis von guter, richtiger/falscher Architektur an. Und interessanterweise ist beiden Beispielen gemeinsam, dass die Gesetzgebung hier der gemeinschaftlichen Wertevorstellung zeitlich nachgelagert und nicht etwa die Umsetzung beider „Richtlinien" durch entsprechende Gesetze erzwungen worden ist."

Methoden für mehr Tempo

Damit die Enterprise Architecture schneller agieren kann, empfiehlt der Workstream weiterhin die Nutzung von Methoden des Architectural Engineering, die den Prinzipien der Ingenieurwissenschaften folgen. Dabei werden Ergebnisse der Grundlagenforschung, Erfahrungswissen und Erkenntnisse aus der Erprobung anwendungsnah aufbereitet, um damit ein leichtgewichtiges, praxisnahes Instrumentarium zur Entwicklung der „Minimum Viable Architecture" zu realisieren. Dabei geht es um ein schrittweises Vorgehen. Das heißt, die finale Architektur entwickelt sich Schritt für Schritt. Sie wird im Laufe mehrerer Arbeitssitzungen erarbeitet. Final entschieden wird darüber erst ganz am Ende. Das lässt Raum zum Ausprobieren und zum Lernen.

Weitere Möglichkeiten, EAM zu beschleunigen, ergeben sich durch die frühe und enge Zusammenarbeit mit anderen Bereichen, mit neuen

> DER ANSATZ DES ARCHITECTURAL THINKING GEHT VON EINER BREITEN VERANKERUNG EINES ARCHITEKTURVERSTÄNDNISSES IM UNTERNEHMEN AUS, SODASS UNTERNEHMENSARCHITEKTUR NICHT MEHR VORGESCHRIEBEN WERDEN UND DURCHGESETZT WERDEN MUSS, SONDERN IN DER DNA DES UNTERNEHMENS VERANKERT UND GELEBT WERDEN KANN.
>
> Dr. Karsten Schweichhart, Vorstand F+E im CBA Lab www.cba-lab.de

Partnern außerhalb der IT-Organisation, etwa dem Business Development. Die EAM-Funktion sollte am gesamten sogenannten Imipo-Zyklus mitwirken. Dieser Kreislauf setzt sich zusammen aus den Elementen: Ideation, Modeling, Implementation, Proving und Operation. Je früher sich EAM in diese Elemente einbringt, desto schneller verbreitet sich das allgemeine Architekturverständnis und desto eher wird Architektur nicht als etwas Fremdes betrachtet, sondern als integrales Element bei der Entwicklung und Umsetzung neuer Geschäftsideen.

Ebenfalls ein wichtiger Beschleuniger für EAM ist die Nutzung von EAM-Erfahrungswerten aus früheren Projekten („Harvesting"), die zum Beispiel in einem Architecture Repository zusammengefasst werden. Ein solches Repository hilft, die Architekturanforderungen eines neuen Projektes schneller zu definieren oder sogar bestehende Standards wiederzuverwenden.

Das Architekturmanagement der Zukunft

Unternehmen sind mit hohem Tempo in einer sich ständig verändernden, komplexen Welt mit ungewisser Zukunft unterwegs. Als Leitplanke dient dabei ein agiles EAM: Es ermöglicht die strategiekonforme Verknüpfung zwischen Geschäftsprozessen und IT und bringt dieses komplexe Gebilde von lebenszyklusabhängigen Bebauungsobjekten in einen planbaren sowie systematisch steuerbaren und kontrollierbaren Prozess. Ein gut justiertes EAM unterstützt Transformationsprozesse und zugehörige Projekte mit wiederverwendbaren Architekturelementen und abgesicherten Referenzarchitekturen.

Man kann die Aufgabe eines agilen EAM wie folgt formulieren: Es muss Sicherheit und Stabilität in Ihre Digitale Transformation bringen, ähnlich wie ein Elektronisches Stabilitätsprogramm (ESP) im Auto darauf achtet, dass es nicht aus der Kurve fliegt.

Dr. Karsten Schweichhart

Cross-Business-Architecture Lab:

Das Cross-Business-Architecture Lab (CBA Lab) ist ein Verband von Anwendern für Anwender. Das CBA Lab steht für modulare Bausteine, für modulare, flexible Architekturen und übergreifende Interoperabilität – die Fundamente der Digitalen Transformation. Es erarbeitet mit und für seine Mitgliedsunternehmen innovative „Bausteine", die die Architektur prägen und organisieren. Seine Themen sind: Standardsoftware, Governance, EAM, Cloud, Mobility, Industrial Analytics, Microservices, APIs und Blockchain.

10 JAHRE E-COMMERCE DAY

GEBURTSTAGSJUBILÄUM IM RHEINENERGIESTADION, KÖLN.

Am Freitag, den 17.05.2019 bietet der e-Commerce Day – made by real.de, Onlinehändlern, Herstellern und Interessierten die Möglichkeit neue Features zu entdecken und sich über die aktuellen Trends im e-Commerce zu informieren. Mehr als 100 Aussteller präsentieren ihre Dienstleistungen und bieten die Möglichkeit zum Kennenlernen.

Informieren, Kennenlernen, Austauschen

Onlinehändler, Hersteller mit eigenem Onlinevertrieb und Brancheninteressierte haben am 17. Mai 2019 die Möglichkeit sich von 9 bis 18 Uhr zu informieren: Für die Besucher sprechen mehr als 30 Referenten über neue Erkenntnisse und aktuelle Trends im e-Commerce-Business, und stellen praktische Lösungen für den Alltag im Onlinehandel vor.

Über 100 Aussteller präsentieren zudem auf der über 4000 qm² großen Fläche im Kölner RheinEnergieSTADION ihre Dienstleistungen und bieten die Möglichkeit zum Austausch und Kennenlernen. Unter den Aussteller sind auch 15 junge Start Up Unternehmen vertreten.

Spannendes Rahmenprogramm & Vorabend-Veranstaltung

Ein Rahmenprogramm mit spannenden Stadionführungen, tollen Geburtstagsaktionen und der legendären After-Show Party im Anschluss an den Messetag runden den 10. e-Commerce Day ab.

Am Vorabend dem 16. Mai findet zum zweiten Mal das e-Commerce Day Beach BBQ statt. Hier können sich alle Teilnehmer in lockerer Atmosphäre und mit einem leckeren Grill-Buffet auf den e-Commerce Day einstimmen. Wer möchte kann sich zudem bei einer Partie Beach-Volleyball mit seinen Mitstreitern messen.

www.ecommerceday.de

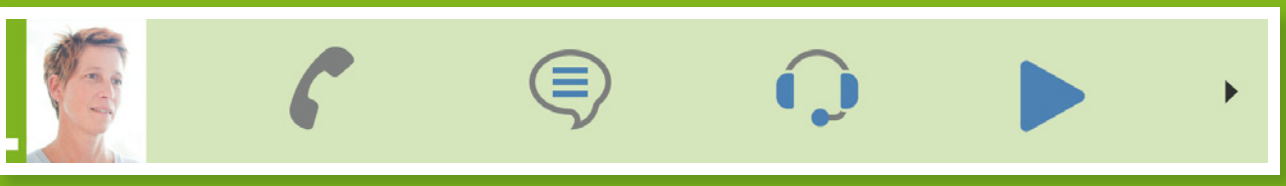
e-Commerce Day
made by real.de

estos
enables easy communication

Ausgezeichnet: ProCall 6 Enterprise

Präsenz-Management als Grundlage für flexible Arbeitsplatz- und Arbeitszeitmodelle von morgen

Das Präsenz-Management-System von ProCall 6 Enterprise ermöglicht eine nie dagewesene Transparenz über die Erreichbarkeit eines Kollegen. So kann einer, der Situation ideal angepasster Kommunikationsweg gewählt werden, um diese Person zu kontaktieren.



ProCall 6 Enterprise ist eine Unified Communications & CTI Software Suite, die alle wichtigen Kommunikationswege in einer einzigen Anwendung vereint.

Mehr erfahren
estos.de/praesenzmanagement

GERMAN INNOVATION AWARD '18 WINNER

NACH DEVOPS KOMMEN

SICHERHEIT UND DATENMODERNISIERUNG HABEN DIE HÖCHSTE PRIORITÄT.

Laut dem Forschungs- und Beratungsunternehmen 451 Research, planen Unternehmen auf der ganzen Welt bedeutende Investitionen im Bereich DataOps. Diese und weitere wichtige Erkenntnisse gehen aus der neuen Studie „DataOps Lays the Foundations for Agility, Security and Transformational Change" hervor, die sich mit den Strategien zur digitalen Transformation 2019 befasst. In der Umfrage gaben 86 Prozent der Teilnehmer an, ihre Investitionen in DataOps-Strategien und -Plattformen innerhalb der nächsten 12 Monate zu erhöhen. 92 Prozent erwarten, dass die DataOps-Technologie einen nachhaltig positiven Einfluss auf den Geschäftserfolg ihres Unternehmens haben wird.

Matt Aslett, Research Vice President, Data, AI und Analytics bei 451 Research, beschreibt DataOps als „die Koordination von Menschen, Prozessen und Technologien, um agile und automatisierte Ansätze für das Datenmanagement in Unternehmen zu fördern und so Geschäftsziele zu erreichen. Das Ziel ist, den Zugriff auf Unternehmensdaten zu erleichtern, um die Anforderungen der beteiligten Interessengruppen in der Datenlieferkette (Entwickler, Datenwissenschaftler, Business-Analysten, DevOps-Experten usw.) zu erfüllen und eine breite Palette von Anwendungsfällen zu unterstützen."

Praktisch alle Branchen stehen vor ähnlichen Herausforderungen: Zum einen steht Innovation ganz oben auf der Tagesordnung, um jederzeit schnell auf Kundenwünsche reagieren zu können und um im globalen Wettbewerb nicht das Nachsehen zu haben. Zum anderen muss die Einhaltung der neuen, geografisch unterschiedlichen Datenschutzbestimmungen jederzeit gewährleistet sein. Aus der Studie geht hervor, dass die befragten Führungskräfte auf DataOps-Strategien setzen, um diese Herausforderungen zu meistern und um der Konkurrenz immer einen Schritt voraus zu sein.

Datenbezogene Herausforderungen meistern

Die Ergebnisse zeigen auch, dass globale Unternehmen davon ausgehen, dass DataOps zur Lösung von Compliance- und regulatorischen Herausforderungen, der Beschleunigung entscheidender Initiativen zur digitalen Transformation, sowie zur Steigerung ihres Wettbewerbsvorteils in der heutigen, digitalen Wirtschaft beitragen wird.

Die Herausforderung, Daten gleichzeitig sicher und zugänglich zu machen, erweist sich als größte Hürde im digitalen Zeitalter.

> DIE HERAUSFORDERUNG, DATEN GLEICHZEITIG SICHER UND ZUGÄNGLICH ZU MACHEN, ERWEIST SICH ALS GRÖSSTE HÜRDE IM DIGITALEN ZEITALTER.
>
> Minas Botzoglou,
> Regional Sales Director DACH, Delphix
> www. delphix.com

Der kleinste gemeinsame Nenner ist wenigstens, dass viele Unternehmen der unterschiedlichsten Branchen glauben, mit einem DataOps-Ansatz datenbezogene Herausforderungen meistern zu können und das in einer Geschwindigkeit, die wettbewerbsfähig ist.

Die Studie identifiziert die wichtigsten datenbezogenen Herausforderungen von Unternehmen:

- Lange Wartezeiten bei exponentiell wachsenden Datenmengen
- Steigende Komplexität bei der Verwaltung unterschiedlicher Datenquellen
- Langsame und riskante Cloud-Migrationen
- Zunehmende Sicherheits- und Compliance-Bedenken

In der Befragung ergaben sich insbesondere die Schwerpunkte Compliance und Sicherheit: Fast drei Viertel der Befragten gaben diese als wichtigste Vorteile von DataOps an. Die Teilnehmer erwarten, dass neue DataOps-Technologien die Brücke zwischen dem Innovationsdruck auf der einen und den Anforderungen durch die DSGVO, CCPA oder anderen Datenschutzbestimmungen auf der anderen Seite, schlagen können.

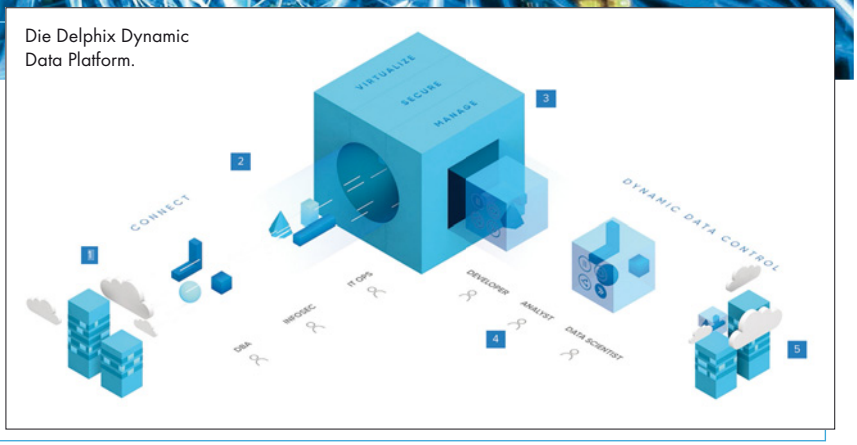
Die Datenmodernisierung vorantreiben

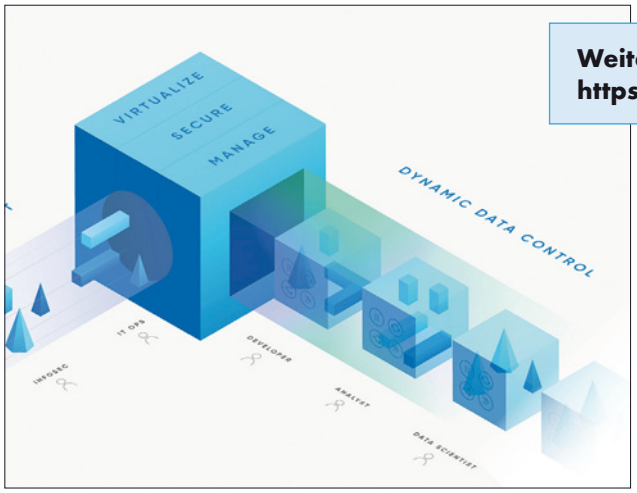
Das 451 Research Team resümiert, dass DataOps fester Bestandteil einer modernen Datenstrategie sein muss. Wenn Unternehmen mittels der Entwicklung und Bereitstellung datenbasierter Anwendungen oder -Entscheidungsfindung einen Business-Nutzen schaffen wollen, werden agilere und automatisierte Herangehensweisen an die Provisionierung von Datenbanken sowie das Datenmanagement benötigt. Diese Lösungsansätze müssen schnell auf die Geschäftsanforderungen von Unternehmen anpassbar sein.

Warum? „Jedes Unternehmen ist heute ein Datenunternehmen. Die Fähigkeit, mit den sich ständig ändernden Kundenanforderungen Schritt zu halten, ist der Schlüssel, um auf dem Markt zu bestehen", erklärt Chris Cook, CEO von Delphix. Es gibt eine steigende Nachfrage nach DataOps-Plattformen von einigen der größten Unternehmen der Welt, um die Bereitstellung von Daten

DIE DATAOPS

Die Delphix Dynamic Data Platform.





Weitere Infos:
https://bit.ly/2GaESof

Bild 2: DataOps – Entwicklungshilfe für Apps.

schnell und sicher gewährleisten zu können und so kontinuierliche Innovationen und Erfolge in der digitalen Wirtschaft zu fördern. Mit dem fortschreitenden Reifegrad von DataOps werden Unternehmen zusätzliche Vorteile nutzen können. Diese ergeben sich aus der Fähigkeit ihrer Entwicklerteams, Reibungsverluste im Datentransfer zu vermeiden und die von der digitalen Wirtschaft geforderte Agilität für Innovationen zu erreichen. Durch die Nutzung der Delphix-Plattform und den Angeboten von Partnern wie Amazon, Microsoft, Oracle und vielen anderen können IT-Verantwortliche die Cloud-Migration verbessern, Sicherheitsrisiken umgehen und die Datenmodernisierung vorantreiben.

Minas Botzoglou

© www.pexels.com

WETTBEWERBSFÄHIG

CLOUD- UND EDGE-RECHENZENTREN WERDEN ZUM KRITISCHEN WIRTSCHAFTSFAKTOR.

Das Voranschreiten der digitalen Transformation hat in den vergangenen Jahren eindrucksvoll das disruptive Potenzial Internet-basierter Geschäftsmodelle gezeigt. AirBnB schreckte die Hotellerie auf, Streaming-Dienste wie Spotify oder Netflix die Multimedia-Branche, E-Commerce-Plattformen wie Amazon verlocken die Kunden, vom heimischen Sofa aus zu shoppen, statt in regionalen Läden einzukaufen. Diese Unternehmen haben ihre jeweiligen Branchen durch den Einsatz neuer Internet-Technologien innerhalb kürzester Zeit verändert und Wettbewerber unter Zugzwang gesetzt, sich weiterzuentwickeln. Mittlerweile haben die meisten Unternehmen über alle Branchen hinweg die Chancen, die sich durch die Digitalisierung ergeben, erkannt und arbeiten daran, innovative digitale Strategien umzusetzen.

Die Folge dieser Entwicklung: Es basieren immer mehr Abläufe in der Wirtschaft und in unserem täglichen Leben darauf, dass irgendwo in einem entfernten Rechenzentrum ein Server reibungslos funktioniert. Von Flugausfällen bis zur Unterbrechung der Stromversorgung reichen heute die Auswirkungen, wenn es im Rechenzentrum zu einer Störung kommt. Auch erwarten die Anwender heute, dass Online-Anwendungen schnell reagieren und dass Informationen ohne Verzögerungen abrufbar sind.

Ein Blick auf die Datacenter-Industrie belegt, dass rund um den Aufbau und Betrieb von IT-Infrastrukturen ein rasantes Wachstum stattfindet. Die Marktexperten von 451 Research erwarten, dass Rechenzentren weltweit von 2015 bis 2020 um 2,8 Prozent jährlich in der Fläche wachsen. Gleichzeitig erleben Anbieter von Colocation-Zentren im gleichen Zeitraum ein Flächenwachstum von knapp zehn Prozent jährlich. Die Analysten der Synergy Research Group zählten Ende 2018 weltweit 430 große Cloud-Rechenzentren und prognostizieren, dass im Jahr 2019 weitere 130 Hyperscale-Datacenter entstehen werden. Auch in Deutschland nimmt die Akzeptanz der Cloud-Rechenzentren weiter zu. Vorreiter dieser Entwicklung: der Maschinen- und Anlagenbau. Hier nutzt bereits jedes zweite Unternehmen die Cloud, so der ITK-Industrieverband Bitkom. Insgesamt setzen laut Bitkom bereits mehr als zwei Drittel der deutschen Unternehmen auf Cloud Services.

Echtzeitverarbeitung mit Edge Computing

Das hohe Wachstumstempo der RZ-Industrie könnte in 2019 weiter anziehen. Grund dafür ist die Entwicklung, dass Unternehmen neben der Nutzung von zentralen Cloud-Ressourcen verstärkt eigene dezentrale Rechenzentren aufbauen. So wird in Deutschland in der zweiten Jahreshälfte 2019 mit dem Start des 5G-Mobilfunknetzes gerechnet. Die Vielzahl der für 5G notwendigen Sendemasten macht den Ausbau der Mobilfunkinfrastruktur mit Edge Datacentern notwendig, da nur so eine Verarbeitung der großen Datenmengen mit niedrigen Latenzen erreicht werden kann. Außerdem erhöhen sich durch 5G die Datenmengen dramatisch, die Netzbetreiber und andere Unternehmen verarbeiten müssen. Die Folge ist, dass auch Endanwender immer mehr Daten auf mobilen Geräten verarbeiten werden. Die Analysten von CB Insights gehen beispielsweise davon aus, dass im Jahr 2020 Anwender im Schnitt täglich 1,5 GByte an Daten mit einem Internet-fähigen Gerät erzeugen.

BLEIBEN

Durch einen dezentralen Ausbau der IT-Infrastruktur mit Edge-Rechenzentren lassen sich Daten schon an der Quelle erstverarbeiten. Damit wird die bei 5G geforderte geringe Latenz in der Datenverarbeitung erreicht, sodass Echtzeitapplikationen für eine Steuerung von Industrierobotern oder autonome Fahrzeugsysteme möglich werden. Für weitergehende Datenanalysen sind Edge-Rechenzentren mit der Cloud verbunden.

Mit der Digitalisierung steigt die Nachfrage nach schnell verfügbaren Daten nahe dem Entstehungsort. Dies erfordert zusätzliche Rechenleistung, kurze Latenzzeiten, unterbrechungsfreie Datenverfügbarkeit und systemweite Sicherheit. Für diese und weitere Anforderungen entwickelte Rittal beispielsweise Container-basierte Edge-Rechenzentren. Edge-Rechenzentren.

Bessere Datenverfügbarkeit benötigt

Viele neue digitale Geschäftsmodelle basieren auf der zunehmenden Vernetzung von Endgeräten oder Maschinen. Heute gibt es etwa intelligente Systeme in Fahrzeugen, die nicht nur Verkehrsdaten übermitteln, sondern auch assistierend in die Fahrt eingreifen – oder das Auto komplett autonom steuern. Ein weiteres Szenario sind Smart Cities, in denen beispielsweise Kommunen in Echtzeit die Luftqualität in Wohnvierteln mit hohem Verkehrsaufkommen überwachen. Werden Grenzwerte erreicht, erfolgt eine automatisierte Umleitung des Verkehrs.

Echtzeit bedeutet hier konkret Latenzen von unter einer Millisekunde. Der Research-Spezialist IDC hat in seinem Analyse-Paper „Data Age 2025" ermittelt, dass bis 2025 über ein Viertel der erzeugten Daten aus Echtzeitdaten bestehen werden. Die Anwendungsfälle erfordern physische Infrastrukturressourcen im näheren Umfeld der Systeme, um die Latenz so gering und die Datenverfügbarkeit so hoch wie möglich zu halten – also Lösungen für das Edge Computing.

Standardisierung erlaubt schnellen Aufbau

Der Bedarf nach immer mehr IT-Ressourcen verlangt aber auch von den RZ-Anbietern neue Konzepte. Dazu zählen modulare und standardisierte Lösungspakete, die den schnellen Aufbau von Rechenzentren ermöglichen, wie beispielsweise in Rechenzentrumscontainern. Die neueste Generation solcher RZ-Lösungen basiert auf einer stringenten Standardisierung der darin verbauten Hardware und Software. Sie bringen zudem von Haus aus sowohl die passende Operational Technology (OT) als auch die Information Technology (IT) als Basis für moderne Infrastrukturkonzepte mit. Dadurch eignen sie sich für eine Vielzahl unterschiedlicher Szenarien, die auf innovativen, datengetriebenen Technologien innerhalb des Internet of Things und Industrie 4.0 beruhen. Modulare Rechenzentren, integrierbar in ISO- oder Non-ISO-genormte Container, werden noch vor der Auslieferung an den Kunden vom Anbieter komplett nach dessen Anforderungen montiert und vorab getestet.

> WIR WERDEN IM JAHR 2019 ERLEBEN, DASS UNTERNEHMEN IHRE IT-INFRASTRUKTUR VERSTÄRKT DEZENTRAL AUSBAUEN. EIN MITTEL DAFÜR SIND EDGE-DATACENTER. RITTAL BIETET HIER EINE REIHE VON LÖSUNGEN.
>
> Andreas Keiger, Executive Vice President Global Business Unit IT, Rittal www.rittal.de

Zentrale Elemente sind bei diesem Konzept die standardisierten Komponenten, die der Anbieter entsprechend des Anforderungsprofils des Kunden zusammenstellt. Das minimiert den Aufwand auf Anwenderseite.

Die RZ-Lösung umfasst etwa neben dem Container als Außenhülle die IT-Racks, Stromversorgung, Klimatechnik sowie Server, Netzwerksysteme, Storage und eine passende Managementsoftware als vorkonfigurierte Cloud-Komponenten. Diese sind im Idealfall entsprechend der anvisierten Einsatzszenarien auswählbar und bilden die Basis für zusätzlich erhältliche cloud-basierte Dienste (XaaS). Der Vorteil solcher Konzepte: Unternehmen erhalten von der OT über die IT bis hin zu spezifischen Softwarelösungen alle Bausteine aus einer Hand. Diese sind durchgängig maximal standardisiert. Das ermöglicht eine geringere Time-to-Market sowie deutlich reduzierte Kosten.

Die IT als Innovationstreiber

Wer als Unternehmer auch künftig wettbewerbsfähig bleiben möchte, sollte jetzt prüfen, wie sich die bestehende IT-Landschaft modernisieren lässt. Der weltweite Ausbau von Rechenzentren belegt, dass Unternehmen erkannt haben, welche Chancen die Digitalisierung bietet. Edge-Rechenzentren sowie die Nutzung von Cloud-Ressourcen gehören also ganz oben auf die Liste der Innovationen, mit denen sich Unternehmenslenker beschäftigen sollten.

Andreas Keiger

DAS NÄCHSTE
SPEZIAL
itsecurity
ERSCHEINT AM
30. APRIL 2019.

KI IM ECM-UMFELD

Chancen und Grenzen

INDUSTRIE 4.0

Die Autonomie der Systeme

MULTIFUNKTIONS-DRUCKER

Die unterschätzte Gefahr

DIE NÄCHSTE AUSGABE ERSCHEINT AM 27. MÄRZ 2019.

INSERENTENVERZEICHNIS

IMPRESSUM

Chefredakteur:
Ulrich Parthier (-14)

Redaktion:
Silvia Parthier (-26), Carina Mitzschke

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren: Thomas Boele, Minas Botzoglou, Tülin Duman, Dr. Beatrice Eiring, Owen Garrett, Jochen Griebel, Andreas Keiger, Sibylle Klein, Klaus Kramer, Ingo Kraupa, Paola Krauss, Anton Kreuzer, Stefan Kuhardt, Carina Mitzschke, Stefan Mulder, Silvia Parthier, Ulrich Parthier, Prof. Dr. Dr. Gerd Rossa, Rolf Scheuch, Christine Schuhmacher, Dr. Karsten Schweichhart, José Silva, Alexander Stühl, Dr. Horst Tisson, Raphael Vallazza, Peter Weierich, Elmar Witte

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

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

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

Herausgeberin:
Dipl.-Volkswirtin Silvia Parthier

Layout und Umsetzung:
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

Wir waren zwar nicht die Ersten auf dem Mond, dafür sind wir die Ersten, die unabhängig über SAP® berichten.

e-3.de | e3zine.com

noris network

- IT-Outsourcing
- Managed Services
- Cloud Services
- Colocation

IT-Sicherheit
Made in Germany

RECHENZENTREN IN MÜNCHEN, NÜRNBERG UND HOF (NEUERÖFFNUNG)

noris.de

itsecurity
MÄRZ 2019

DAS SPEZIAL

IDENTITY & ACCESS MANAGEMENT THOUGHT LEADERSHIP

SURVIVAL KIT FÜR DIE IT-SECURITY

SEAL KIT-SUITE

Pierre Gronau, Gronau IT Cloud Computing GmbH

www.it-daily.net

secIT by Heise

HANNOVER 2019

13. – 14. März 2019
Hannover

Der Treffpunkt für Security-Anwender und -Anbieter!

Seien Sie dabei und profitieren Sie als Besucher von neuesten IT-Security Trends, Produkten oder Software-Lösungen.

- **16 vertiefende Workshops** zu aktuellen IT-Sicherheits-themen
- Bis zu **40 Expert Talks**
- Wichtige **Unternehmen** aus der **IT-Sicherheits-branche**
- Netzwerken und feiern auf der großen secIT-Party
- Mehr als **40 Vorträge führender IT-Experten auf 2 Bühnen**
- **Hochkarätige Sprecher,** ausgewählt von unseren Redaktionen

Auszug aus dem Vortragsprogramm

- **Ihre Sicherheit ist unsere Aufgabe! Das kann die Zentrale Ansprechstelle Cybercrime (ZAC) für Sie tun!**
  // Christian Pursche, Zentrale Ansprechstelle Cybercrime (ZAC) LKA Niedersachsen
- **Cyberangriffe verstehen, Bedrohungslage richtig einordnen!**
  // Holger Unterbrink, Sicherheitsforscher Cisco Threat Research Group Talos
- **Spionage 4.0: Ihre Daten sind bestimmt sicher, oder?**
  // Jörg Peine-Paulsen, Wirtschaftsschutz, Verfassungsschutzbehörde, MI Niedersachsen
- **IT-Security Hypes – eine Polemik**
  // Tobias Glemser, Geschäftsführer der secuvera GmbH und BSI-zertifizierter Penetrationstester
- **Mythos Blockchain**
  // Dr. Reinhard Wobst, Autor von „Abenteuer Kryptologie", selbständiger Softwareentwickler

Veranstalter Heise Medien

organisiert von heise Events Conferences, Seminars, Workshops

Eventpartner itsa 2019 Die IT-Security Messe und Kongress

26

INHALT

SEAL KIT-SUITE

EIN SURVIVAL KIT FÜR DIE IT-SECURITY.

Die Gronau IT Cloud Computing GmbH hat sich im Security-Umfeld einen Namen gemacht. Über den Status Quo und die Zukunft sprachen wir mit Pierre Gronau, dem Geschäftsführer des Berliner Unternehmens.

it security: *Sie schreiben auf Ihrer Website „IT-Probleme sind für uns willkommene Herausforderungen, denen wir uns mit Herzblut und Innovationsfreude stellen." Was hat sich in den vergangenen Jahren am meisten verändert und welchen Herausforderungen mussten sich Ihre Kunden und Sie stellen?*

Pierre Gronau: Die vergangenen Jahre haben gezeigt, wie verwundbar IT-Systeme in unserer vernetzten Welt sind und wie hilflos Unternehmen teils dastehen, wenn es darum geht, geeignete Schutzwälle zu errichten. Auch die rasant ansteigende Zahl an internetfähigen Geräten, die miteinander verbunden sind, und an Daten, die hier ausgetauscht werden, bergen enorme Risiken. Parallel entwickeln sich Hackerangriffe zum zentralen Geschäftsrisiko bis hin zur Existenzbedrohung in der vernetzten Weltwirtschaft. Gott sei Dank hob der Gesetzgeber die Anforderungen an die IT-Sicherheit erheblich an – insbesondere für Unternehmen mit kritischen Infrastrukturen. Die neuen Auflagen erschweren es Unternehmen, Verantwortung auszulagern. Sie sind angehalten, Verantwortung für die eigene IT-Sicherheit zu übernehmen und sich den Cyberangriffen eigenhändig zu stellen. In diesem Spannungsfeld liegt meine Hauptaufgabe darin, meine Kunden durch Beratung auf mögliche Szenarien vorzubereiten und sie mit wirtschaftlichen Lösungen zu unterstützen.

it security: *Was würden Sie als Ihre Kernkompetenzen bezeichnen und wie sieht ihr Leistungsportfolio aus?*

Pierre Gronau: Ich blicke auf jahrzehntelange Erfahrung im IT-Sicherheits- und IT- Compliance Umfeld zurück, bin also alles andere als ein Newbie. Dabei ist es mir und meinem Team einerseits wichtig, sehr eng an den Themen der Hacker und Security-Experten dran zu sein. So war es für mich selbstverständlich und ein Anliegen, Ende des Jahres auch wieder am Kongress des Chaos Computer Clubs teilzunehmen. Schließlich bedeutet Wissen Zeitvorteil und Sicherheit! Zum anderen spreche ich als Berater vieler Enterprise-Unternehmen auch die Sprache der Manager, argumentiere und implementiere Software nach wirtschaftlichen Kriterien. Zu guter Letzt verstehe ich die Herausforderungen, mit denen Entwickler und Administratoren heute konfrontiert sind. In dieser Kombination sehe ich meine Kernkompetenz.

it security: *Wie würden sie Ihre Mission beschreiben?*

Pierre Gronau: Meine Mission ist es, Unternehmen davon zu überzeugen, dass Privacy, Compliance, Security by Design und Security by Default selbstverständlich sein müssen. Die Kultur, die mein Team und ich leben, um diese Mission umzusetzen, ist geprägt von Wissensvorsprung und Wissenstransfer, solider Handwerkskunst sowie agiler Selbsterneuerung bei Technologien und Organisationsstrukturen. Kurz: Wir wissen, was Unternehmen jetzt brauchen, und bieten nichttechnokratische Lösungen an.

it security: *Eine Ihrer selbstentwickelten Lösungen ist die Security Suite SEAL Kit. Das klingt ein bisschen nach Survival Kit. Was hat Sie zu dieser Entwicklung veranlasst?*

Pierre Gronau: Der wirtschaftliche Schaden, der durch Cyberkriminalität entsteht, wächst jährlich weltweit an. Um der Ge-

> MIT UNSEREM WISSEN ÜBER DIE SPEZIELLE DNA ERFOLGREICHER UNTERNEHMEN UND DER MECHANIK DER VERNETZTEN WELT VON MORGEN GEBEN WIR DIE ENTSCHEIDENDEN DENKANSTÖSSE, WIE FIRMEN IHREN DIGITALEN WANDEL MODELLIEREN KÖNNEN.
>
> Pierre Gronau, Geschäftsführer,
> Gronau IT Cloud Computing
> www.gronau-it-cloud-computing.de

fahrensituation effizient einen Riegel vorzuschieben, muss die Wirtschaft schnell reagieren und höhere Investitionen für IT-Sicherheit tätigen. Ich traf als Berater in großen Unternehmen immer wieder auf die gleiche Mangellage und vergleichbare Aufgabenstellungen. Trotz der Vergleichbarkeit musste ich das Rad auf Kundenwunsch mehr oder weniger jedes Mal neu erfinden, Projekte neu starten. Dieser Aufwand belastet die Mitarbeiter-Ressourcen in Enterprise-Umgebungen enorm. Zumeist haben die Firmen darüber hinaus mit Personalreduktion zu kämpfen, was die IT-Sicherheit zusätzlich gefährdet. Auf Basis dieser Situation startete ich mit meinem Team die Entwicklung des SEAL Kits. Hinter der Entwicklung steht der Anspruch, Sicherheitslücken in IT-Systemen aufzudecken, Hackerangriffe zu erkennen und Datenschutzkonformität sicherzustellen.

it security: *Seit Ende letzten Jahres gibt es ein neues Hauptrelease der Security-Suite SEAL Kit. Damit wollen Sie Anwendern helfen, die Klippen aus DSGVO, KRITIS und Co. zu umschiffen. Das ist kein typisches SIEM-Szenario, oder?*

Pierre Gronau: Ich hatte das SEAL Kit auf der it-sa 2018 erstmals offiziell vorgestellt und den Anwendernutzen in vielen Gesprächen deutlich gemacht. Die Software ermöglicht es der Industrie, sich leichter, beziehungsweise überhaupt, in einem wirtschaftlich tragbaren Rahmen an die neuen gesetzlichen Vorgaben zu halten, die Sie in Ihrer Frage erwähnen. Meine Entwickler-Teams betrachten IT-Sicherheit als großes Ganzes, in dem Logmanagement, insbesondere SIEM, einen Teil abbilden. Gronau besetzt ganzheitlich die Spezialgebiete Penetrations-Tests, Sicherheitsberatung, Kritische Infrastruktur, Härtungskonzepte, Linux, Cloud Computing, Big Data, Automation, Rechenzentrum-Infrastruktur. Ich denke, damit sind wir gut aufgestellt. In Einzeldisziplinen ist IT-Security heute nicht mehr beherrschbar.

it security: *Ist die Lösung modular aufgebaut und welche Module beinhaltet sie?*

Pierre Gronau:. Ja, die Werkzeuge sind modular beliebig zusammenstellbar sowie erweiterungsfähig und bieten für jeden wichtigen Anwendungsfall das richtige Instrument. Insgesamt sind es aktuell sechs Tools, die IT-Sicherheit in Unternehmen verankern: SEAL SIMP ist eine Open Source Management-Plattform für Linux-Strukturen und Cloud Computing. Dahinter steht ein voll automatisiertes und ausgiebig getestetes Framework, mit dem entweder bestehende Infrastrukturen erweitert oder neue aufgebaut werden können. SEAL SIMP basiert auf dem Konfigurations-Management-Werkzeug Puppet und ist auf Skalierbarkeit, Flexibilität und Compliance ausgelegt. Das von Ihnen schon erwähnte SEAL SIEM Monster ist eine auf ELK Stack aufsetzende Open Source-Anwendung, die Protokolle wie beispielsweise Logs analysiert. Das Tool erkennt Anomalien sowie Muster und identifiziert daraufhin Hackerangriffe. Es lässt sich zügig in bestehende IT-Unternehmensstrukturen ausrollen und kommt mit einer unterstützenden Build- und Wartungsdokumentation daher, die anderen Open Source-Lösungen fehlt. SEAL Pen Test ist ein automatischer Penetrationstest, der Sicherheitsschwächen in der Implementierung oder Softwareentwicklung aufzeigt. In der Regel deckt er nicht nur einzelne Schwachstellen auf, sondern auch deren Ursache. SEAL Vul

Scan ist ein Tool zur Schwachstellenanalyse von Applikationen, die auf Linux oder Cloud Computing laufen – zum Beispiel Web-Produkte wie WordPress oder Apache. Die Anwendung erkennt den Einsatz von unsicheren Geräten oder Diensten, Fehler in deren Konfiguration oder fehlerhafte Anwendung von Passwortrichtlinien. SEAL GDPR ist ein Datenschutz-Modul, das auf Basis technischer Maßnahmen beispielsweise Informationen zur Passwort-Policy ausliest und auditiert. Zu guter Letzt haben wir mit SEAL Container Sec eine Anwendung im Gepäck, die Docker Container auf Sicherheit, Compliance und Malware überprüft.

it security: *Wie unterschiedet sich Ihre Lösung SEAL SIEM Monster von traditionellen SIEM-Lösungen?*

Pierre Gronau: Unser SIEM Monster ist im Vergleich zu konventionellen SIEM-Lösungen erheblich schlanker. Damit meine ich, dass die Software unnötiger Komplexität beraubt und so verständlich konzipiert ist, dass sie auch vom Management, nicht nur vom IT-Sicherheitsleiter, verstanden wird. Wir können sie flink als „Out-of-The-Box"-Software in Unternehmensstrukturen verankern - auch in IT-Mischstrukturen aus Cloud und Rechenzentrum. Durch dieses Tempo und die Simplizität schonen wir personelle Ressourcen und IT-Budgets. Das Tool ist dabei so flexibel, dass der Einsatz in vermeintlichen Spezialumgebungen wie Industrie oder Medizintechnik mühelos gelingt. Unsere Kunden schätzen an der SIEM-Lösung zudem, dass sie Bedrohungen klar einschätzt, ohne mit einer Alarm-Hypersensibilität Betriebsabläufe zu stören.

it security: *Auf welche Zielgruppen fokussieren Sie mit Ihrer SIEM-Lösung und wie schätzen Sie den Bedarf für die nächsten Jahre ein?*

Pierre Gronau: Der Analyst Gartner definiert den SIEM-Markt als unternehmerische Notwendigkeit, Ereignisdaten in Echtzeit zu analysieren, um Angriffe und Datenschutzverletzungen frühzeitig zu erkennen, auszuwerten und zu melden. Die betriebliche Realität jedoch sieht anders aus und der Bedarf an Lösungen ist international enorm. So soll der globale Logmanagement-Markt bis Ende 2022 zweistellig wachsen. Europa ist in diesem Segment der zweitgrößte Weltmarkt mit über 26 Prozent Marktanteil. Wir fokussieren hier große mittelständische Unternehmen, Enterprise-Unternehmen und Unternehmen mit kritischen Infrastrukturen. Sie alle brauchen wirtschaftliche Logmanagement- und SIEM-Lösungen als Antwort auf Treiber wie KRITIS, BaFIN oder das Medizinproduktegesetz.

Das SEAL-Kit

SEAL Pen Test
Dieser Pen Test ist ein automatischer Penetrationstest, der Sicherheitsschwächen in der Implementierung oder Softwareentwicklung aufzeigt.

SEAL Vul Scan
Der Vul Scan ist ein Tool zur Schwachstellenanalyse von Applikationen, die auf Linux oder Cloud Computing laufen.

SEAL SIMP
SEAL SIMP ist eine Open Source Management-Plattform für Linux-Strukturen und Cloud Computing.

SEAL GDPR
SEAL GDPR ist ein Datenschutz-Modul, das auf Basis technischer Maßnahmen beispielsweise Informationen zur Passwort-Policy ausliest und auditiert.

SEAL Container Sec
SEAL Container Sec überprüft Docker Container auf Sicherheit, Compliance und Malware.

SEAL SIEM Monster
SEAL SIEM Monster ist eine Open Source Anwendungssammlung, die Protokolle, wie beispielsweise Logs analysiert. Das Tool erkennt Anomalien sowie Muster und identifiziert daraufhin Hackerangriffe.

it security: *Herr Gronau, wir danken für das Gespräch!*

IT & BUSINESS STETS IM BLICK

Tägliche News für die Enterprise IT finden Sie auf www.it-daily.net

it-daily.net

Das Online-Portal von
itmanagement & itsecurity


IDENTITY & ACCESS MANAGEMENT
THOUGHT LEADERSHIP

IAM – EIN THEMA IM WANDEL

VOM STATISCHEN ZUM DYNAMISCHEN THEMA IN DER IT.

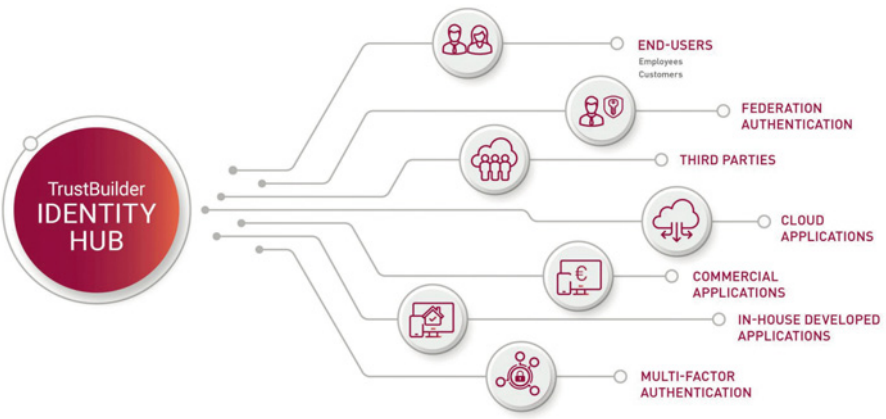
Ab 2005, als sich das IAM entwickelte, waren Themen wie Passwortmanagement, Single Sign-on oder Provisioning die beherrschenden Problematiken. Dem folgten die Identity Federation-Thematik und das PIM Privileged Identity Management. Man sollte meinen, dass nicht nur der Sinn, sondern die Vorzüge der Automatisierung von großen wie mittelständischen Unternehmen schnell erkannt wurden. Doch weit gefehlt. Es gibt immer noch wahnsinnig viele Unternehmen, die ihre IT-Mitarbeiter diese Arbeiten manuell erledigen lassen. In Zeiten von DSGVO ein trügerisches Verhalten, das sich letztendlich das C-Level Management ankreiden lassen muss. Dass nicht genug davor gewarnt worden ist, darauf kann sich heute kein Manager mehr berufen.

Was wir jedoch sehen, sind neue Themen, die auf dem Radar auftauchen. Zum einen sind das cIAM, die API-Thematik, aber auch Identity Analytics, die attributbasierte Zugriffssteuerung (ABAC) und der Vorstoß in angrenzende IT-Fachbereiche, wie dem IT Service Management, sind Topthemen. Schaut man sich traditionelle ITSM-Anbieter an, dann sieht man dort jetzt Module für Rollen- und Berechtigungsmanagement, bei ServiceNow ist es sogar nur noch ein Teil einer gesamten IT Operations-Plattform, die entsteht. ITSM und IAM verbinden die Prozesse, immer geht es um Genehmigungsprozesse. Und das kann man in einem IAM einfach über ein Standardmodell in Form eines modellierbaren Objektmodells abbilden.

Und IoT-Sicherheit? Wird noch von vielen Unternehmen geradezu ignoriert. Doch wer mit einem IAM die Kontrolle über Devices aller Art hat, hat auch die Kontrolle über die Zugänge und damit ein zusätzliches Level an Sicherheit. Das gilt nicht nur für mobile Devices aus der Office-Welt, sondern auch für Geräte in der Produktion.

Im Mittelpunkt steht immer die Identität als Hub wie unsere Grafik zeigt. Darum herum gruppieren sich die Services, die man beliebig erweitern kann. Jeder Anbieter sieht den Markt dabei natürlich anders. Wichtig ist, wer heute den Weitblick für morgen hat und möglichst viele dieser Strömungen integrieren kann, zählt zu den Gewinnern. Denn zum einen muss man über ein starkes Prozess Know-how verfügen und zum zweiten über die richtige Priorisierung. Das cIAM Thema zum Beispiel erfordert eine modifiziertere Architektur als traditionelle IAMs es benötigen.Denn während etablierte IAMs vor allem transaktionssicher sein müssen und eher langsam sind, lautet eine Anforderung an cIAM hohe Transaktionsraten schnell zu verarbeiten, was wiederum an der Datenstruktur liegt. Sehr, sehr viele kleine, unstrukturierte Daten sind im Consumerbereich nicht unüblich. Im Businessbereich hingegen treffen wir auf weniger, dafür aber gut strukturierte Daten.

Und die Anwender müssen Prioriäten setzen: Welche Module, welche Betriebsform und welcher Anbieter? Gartner als Beispiel mit seinem IAM 2018 Planing Guide wie auch Forrester in seiner Forrester Wave Identity Management and Governance aus Q3 2018 sind wenig hilfreich, weil viele Anbieter einfach fehlen oder hierzulande überhaupt keine Präsenz haben und deshalb durch das Raster fallen und hinsichtlich der Bewertung kann man auch geteilter Meinung sein!



© TrustBuilder

Zusammenfassend ergibt sich also ein sehr fragmentierter Markt mit vielen Anbietern, die technologisch im Ansatz Hervorragendes bieten, wie Ping Identitiy, One Identity, bi-cube (ISM) oder Nexis, aber ein Thought Leadership bisher nicht nachweisen konnten.

Ulrich Parthier
Publisher – Analyst - Influencer

EIN IAM IN 20 TAGEN

GEHT DOCH! EIN PROJEKTBERICHT.

Eine Krankenkasse mit etwa 9.000 Usern hat sich entschlossen, ein IAM in Nutzung zu nehmen. Um das Ziel, eine erste Phase des IAM kurzfristig produktiv setzen zu können, wurde eine Reihe notwendiger Voraussetzungen erkannt und akzeptiert. Das Projekt ist in mindestens zwei Phasen zu splitten. In der ersten Phase wird sich auf den Schwerpunkt AD und dessen Ressourcen konzentriert.

Kurzfristig wirksam sollten auch die Automatisierungsmöglichkeiten der Zuordnung der AD-Ressourcen Exchange und Filespace genutzt werden. Einverständnis musste auch in der weitgehenden Nutzung der Standards des IAM mit dessen Modellierungsmöglichkeiten bestehen, womit dann keinerlei Anpassungsprogrammierungen erforderlich sind, die immer einen Zeitverzug bewirken.

Um die Automatisierungsmöglichkeiten von bi-Cube voll nutzen zu können, bestand auch die Bereitschaft dem End-User im Service-Portal eine Eigenverantwortung in der Beantragung von Ressourcen zuzumuten und zuzutrauen. Letztlich sollte der technische Implementierungsaufwand durch die Nutzung aus der iSM-Cloud vermieden werden. Möglich wird die Nutzung aus der Cloud durch das duale Cloud-Konzept von bi-Cube, das durch die Kommunikation mit einem bi-Cube Hub in der Infrastruktur des Kunden praktisch wie eine On-Premises-Installation mit allen Cloud-Vorteilen wirkt (siehe Bild 1). Durch das Mietmodell des IAM aus der Cloud entfällt auch eine aufwendige Investitionsphase.

Um einen schnellen Einsatz zu erreichen, wurde das standardisierte IAM-Einführungskonzept der iSM Secu-Sys AG genutzt. Dieses Konzept ermöglicht es, das IAM-System beim Kunden mit einem Auf-

wand von nicht mehr als 30 (Werk-)Tagen und circa 20 Tagen internem Aufwand so weit zu bringen, dass es aus der Cloud in einer ersten Phase produktiv einsetzbar ist.

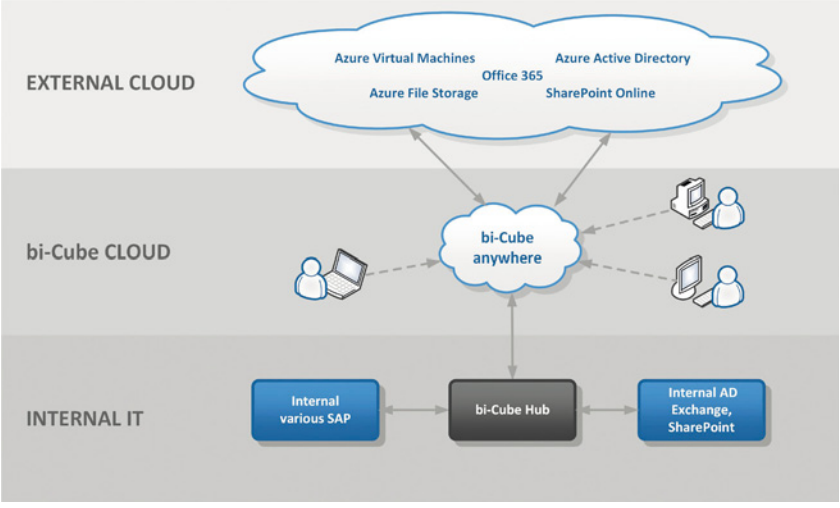
Projekt und Ergebnis Phase

Das Projekt startete am 29.11.2018 mit einem Kick-Off-Meeting beim Kunden. Bereits zum 04.01.2019 konnte die Phase 1 mit den wichtigsten Funktionen produktiv gesetzt werden. Die User- und Organisations-Daten sowie die Leiter der Bereiche werden regelmäßig mit bi-Cube synchronisiert. Die Migration von zwei AD-Domänen wurde erforderlich, da der Einsatz von bi-Cube auch ein Mittel zur Konsolidierung des AD ist. Die ersten fachlichen Basisrollen konnten modelliert und regelbasiert zugeordnet werden. Neue Mitarbeiter werden nur noch in bi-Cube aufgenommen und über die automatisch zugeordnete Basisrolle im AD angelegt, erhalten ein Postfach und die Rechte zur Nutzung des bi-Cube Workplace. bi-Cube erzeugt auch das HomeDir des Users über eine Basisrolle.

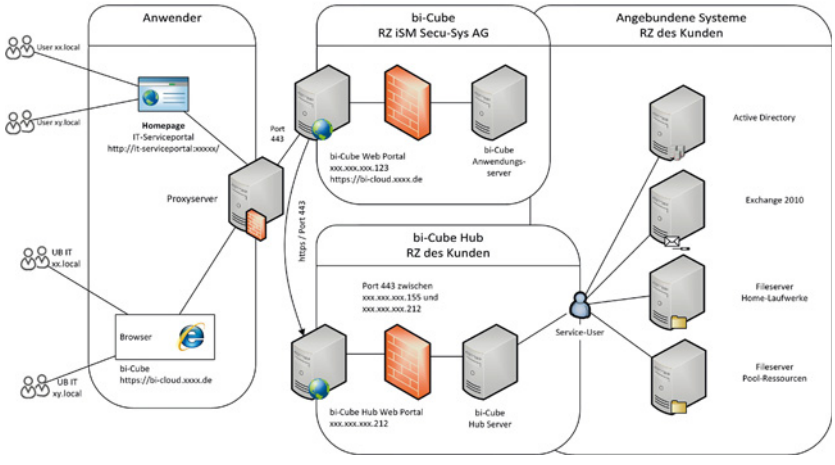
Neben der Automatisierung der bisherigen Prozesse erwartet man von einem IAM auch einige weitere Funktionen. Mit der Dubletten-Kontrolle und -Auflösung und der Bereitstellung der ersten Antragsprozesse im Self-Service für jeden User, wird auch eine deutliche Entlastung des UHD erreicht.

Diese automatisierten Ressourcenprozesse ermöglichen einen Password Self-Service sowie zwei Antragsprozesse (Antrag auf Pool-Ressource, Allg. dokumentenbasierter Antragsprozess).

1 DIE BI-DIREKTIONALE ARCHITEKTUR DER BI-CUBE CLOUD



BI-CUBE CLOUD ARCHITEKTUR



Wenn in der Aufbauorganisation in bi-Cube ein neues Element (Abteilung) generiert wird, erfolgt eine automatische Anlage von Filespace sowie die Berechtigung der Mitarbeiter dieser Organisationseinheit an diesem Abteilungs-Filespace.

Dieses Ziel wurde auch ohne direkten Aufenthalt der iSM-Experten beim Kunden erreicht. Ein wesentliches Automatisierungsmittel ist damit der Self-Service durch die Mitarbeiter. Über den bi-Cube Workplace kann der berechtigte User u.a. eine sogenannte Pool-Ressource (Filespace oder Mailgruppe) beantragen (siehe Bild 2). Nach Freigabe durch den Leiter wird diese Ressource inklusive der erforderlichen Gruppen im AD durch bi-Cube automatisch angelegt und der Antragsteller als Owner definiert. Dieser kann dann im Self-Service weitere User an dieser Ressource berechtigen. Andere User können diese Pool-Ressource sehen und eine Teilnahme bei deren Owner beantragen. Alle diese Operationen laufen unter Regie von bi-Cube und vollkommen ohne die Mitarbeit eines AD-Admins ab.

Einstieg in das Rollenmodell

Durch die iSM Secu-Sys AG wird ein Rollen-Referenz-Modell (RRM) vorinstalliert. Zweck dieses RRM ist es, dem Kunden eine Grundstruktur des Rollenmodells vorzugeben und ihm die Einstiegsebenen für die konkreten eigenen Fachrollen vorzubereiten (siehe Bild 3).

Die erste Ebene enthält nur die vier branchenunabhängigen Hauptgruppen. Das eigentliche Fachrollenmodell (FRM) wird unter dem Container „Unternehmens-Fachrollen" entwickelt. Im Fall einer Krankenversicherung beginnt hier die Spezifik des Unternehmens mit Branchen-Fachrollen. In diesen Containern werden dann die konkreten Fachrollen vom Kunden weitgehend eigenständig modelliert.

Neben den rollenbasierten Berechtigungen wird es aber immer einen gewissen Anteil von durch bi-Cube direkt zugeordneten, individuellen Berechtigungen geben, womit das IAM alle User-Berechtigungen „kennt".

Sicherheitsmaßnahmen

Eine weitere wichtige Vorgabe ist das Admin-Rollenmodell (Bild 4), wodurch das für ein IAM wichtige Sicherheitsniveau einzuhalten ist. Durch die Rollen der Job-Family ‚IT-Admin' sind die einzelnen Admin-Bereiche streng in die Modellierer und Operatoren getrennt, womit sich die auch für diesen Bereich wichtigen SoD-Regeln sicherstellen lassen.

Die Cloud-Installation von bi-Cube ist verpflichtend mit dem Managed-Service der iSM Secu-Sys AG verbunden. Das bedingt eine saubere Trennung der Berechtigungen des Kunden und des Managed-Service-Teams im Kundensystem. Um den zukünftigen Anforderungen des IT-Sicherheitsgesetzes zu KRITIS zu entsprechen, erfolgt eine technische Trennung der Möglichkeiten der Rechtezuordnung. Die Mitarbeiter der iSM Secu-Sys AG können sich keine Rechte in den Kundensystemen zuordnen. Berechtigungen der User des Kunden an bi-Cube selbst bedürfen der Freigabe der iSM Secu-Sys AG. Diese Trennung ist zeitlich variabel. In der Einstiegsphase haben die Mitarbeiter des Kunden in der Regel noch nicht die erforderlichen Zertifikate, um etwa als Rollen-Modellierer tätig zu sein. Schrittweise kann dann je nach personellen Möglichkeiten des Kunden die Modellierung durch den Kunden übernommen werden.

> DAS IAM BENÖTIGT DURCH DEN HOHEN GRAD AN STANDARDISIERUNG BEI GLEICHZEITIGER GENERIK KEINE KUNDENSPEZIFISCHE ANPASSUNGSPROGRAMMIERUNG. EIN WEICHER ABER EXTREM WICHTIGER FAKTOR WAR DIE HOHE PRIORISIERUNG BEIM KUNDEN UND DESSEN EFFEKTIVE MITARBEIT.
>
> Prof. Dr. Dr. Gerd Rossa, CEO iSM Secu-Sys AG
> www.secu-sys.de

Wodurch war dieses Ergebnis möglich?

bi-Cube steht kurzfristig als Systembasis aus der Cloud zur Verfügung. Der in der Infrastruktur des Kunden erforderliche Hub (bi-Cube Gateway) ist remote schnell aufgesetzt. Die modulare Struktur von bi-Cube ermöglicht es, die Funktionalität für die geforderte Phase 1 zielgenau bereitzustellen.

Das IAM benötigt durch den hohen Grad an Standardisierung bei gleichzeitiger Generik keine kundenspezifische Anpassungsprogrammierung. Ein extrem wichtiger Faktor war die hohe Priorisierung beim Kunden und dessen effektive Mit-

arbeit. Auf eine aufwendige Projektorganisation und zeitraubende Meetings beim Kunden wurde verzichtet und die (agile) Steuerung wurde dem verantwortlichen iSM-Team überlassen.

Also ist zu konstatieren: Nur wenn alle Beteiligten (und das dürfen beim Kunden nicht zu viele sein) extrem kooperativ arbeiten und die weitgehenden Möglichkeiten von bi-Cube und die Erfahrung des iSM-Teams bereitwillig nutzen, ist ein solches Ergebnis zu erreichen!

Ein partieller Showstopper war auch hier die etwas mühselige, kurzfristige Bereitstellung der erforderlichen Systemberechtigungen des bi-Cube System-Accounts im AD sowie die etwas schwierige Lösung der technischen Zertifikatsprobleme. In dem Bewusstsein der AD-Admins ist es nicht einfach zu akzeptieren, dass ein Automat, der Admin-Funktionen ausführt, auch Admin-Berechtigungen benötigt.

Dieses Ergebnis widerlegt die allgemeine Ansicht, dass ein IAM immer teuer und langwierig sein muss, in sehr eindeutiger und überzeugender Art und Weise.

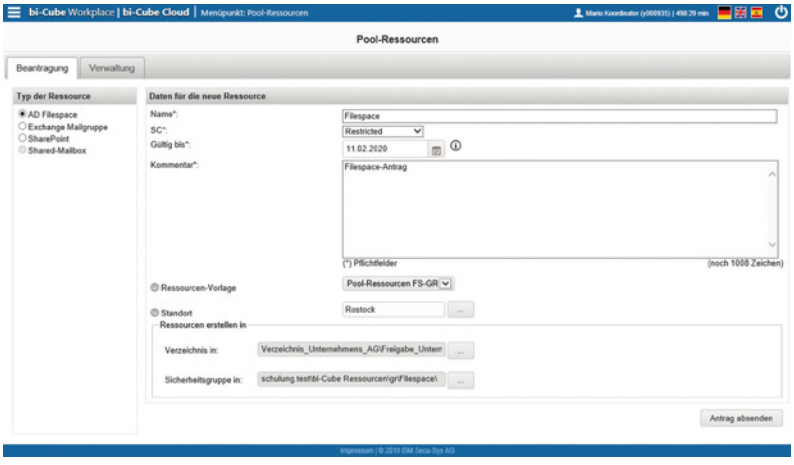
Weitere Planung für Phase 2

Die Planung der Phase 2 sieht vor, dass diese Ende Mai abgeschlossen ist. Damit wäre dann ein komplettes IAM innerhalb von sechs Monaten eingeführt. Eine gewisse Zeit dient jetzt der Konsolidierung der Funktionen der Phase 1. Dies geht aber mit gleichzeitiger Einführung weiterer Prozesse wie dem OE-Wechsel, Team-Funktionen und der Compliance-Funktionen ‚Re-Zertifizierung' und ‚Reconciliation' einher.

Besonders wichtig für die Phase 2 ist die Modellierung des Kernsystems mit anschließender Migration und Übernahme der Verwaltung des Kernsystems durch bi-Cube. Die Modellierung der AD-geführter Applikationen und der schrittweise Ausbau des Rollenmodells sind ebenfalls in Phase 2 vorgesehen. Um der zunehmenden übergreifenden Digitalisierung zu entsprechen, werden weitere User-Kategorien wie Externe und Praktikanten in die zentrale Verwaltung übernommen.

Prof. Dr. Dr. Gerd Rossa

2 POOL-RESSOURCEN-ANTRAG



3 EBENEN DES FACHROLLENMODELLS

1. und 2. Ebene des Fachrollenmodells

- Externe Partner
- Sonderrollen
- Team-Rollen
- Unternehmens-Fachrollen
  - _Branchen-Fachrollen
  - Allgemein verfügbare Rollen
  - Basisrollen
  - Job Family IT-Admin / Klasse bi-Cube
  - Stellenbezogene Rollen
  - Z_Referenzierbare Systemrollen

Teil der 3. Ebene des Fachrollenmodells

- _Branchen-Fachrollen
  - Fachbereiche
    - Leistung
    - Marketing
    - Prävention
    - Versicherung
    - Vertrieb
    - Widerspruchsstelle
  - Landesdirektionen
  - Regionaldirektionen
  - Stabsorgane
  - Unternehmensbereiche
  - Vorstand

4 DAS STANDARD-ROLLENMODELL

(GETRENNT NACH MODELLIERERN UND OPERATOREN)

- Job Family IT-Admin / Klasse bi-Cube
  - bi-Cube Operating
    - bi-Cube Modellierer
      - Aufbauorganisations-Modellierer
      - Ausstattungs-Modellierer
      - bi-Cube Customizing
      - Kostenstellen-Modellierer
      - Prozess-Modellierer
      - Role-Miner / Life-Cycle
      - Rollen-Modellierer
      - Standort-Modellierer
      - Teamrollen-Modellierer
      - Zielsystem-Modellierer

- bi-Cube Operatoren
  - BA / Berechtigungs-Operator
  - bi-Cube All +++++
  - Finaler Prozess-Aktor
  - PA / erweiterter User-Admin (ITC+)
  - RO / Rollen-Operator (ITC++)
  - Team-Koordinator
  - UA / User-Admin (ITC)

IAM FÜR INTERNET-DINGER (IOT)

IOT-PROJEKTE UND IHRE AUSWIRKUNGEN AUF IAM-PROZESSE.

Ist ein moderner PKW noch ein „Auto" wie wir es früher kannten? Oder ist es ein komplexes Internet-Ding mit ein wenig Physik zur Fortbewegung? In jedem Fall ist das ein gutes Beispiel, um auch folgende Fragen zu anzugehen: Welche Auswirkungen haben Internet of Things-Projekte auf die IAM-Prozesse? Sind oder haben IoT Devices eine Identität? In diesem Artikel versuchen wir auf diese Fragen eine Antwort zu geben, indem wir eine Systematik für IoT Einsatzfälle einführen. Daraus können wir dann Anforderungen an IAM Projekte ableiten.

Von „dumm" bis intelligent und autonom

Zuerst muss geklärt werden, welche Typen von IoT-Devices im Fokus stehen:

- Einfache Geräte, beispielsweise Sensoren (Temperatur, Bewegungsdetektion, Geschwindigkeitsmesser).
- Komplexe Devices, die typischerweise eine Komposition einfacher Geräte sind.
- Intelligente Geräte, bis hin zu autonomen Plattformen: beispielsweise Serviceroboter, autonome Fahrzeuge.

Tatsächlich läuft es darauf hinaus: Je intelligenter und autonomer die „Internet-Dinger" werden, desto mehr müssen sie aus der Sicht des Identity- und Accessmanagement wie menschliche Identitäten behandelt werden: Ihre Rechte zum Zugriff auf Daten und Ressourcen müssen unter Umständen genauso gemanagt werden, wie die natürlicher Personen.

Dabei ist eine wichtige Randbedingung zu beachten: Die Steuerung und Kommunikation sehr komplexer Geräte erfolgt nicht direkt, sondern in der Regel über IoT-Plattformen, in denen ein „digital twin" abgebildet ist. Das heißt: Die Interaktion findet primär mit dem digitalen Zwilling statt. Die IoT-Plattform ist – nicht zuletzt aus Sicherheitsgründen – der exklusive Kommunikationspartner des Geräts. Insofern hängt die Umsetzung von IAM-Prozessen davon ab, welche Mechanismen die IoT-Plattform bereitstellt. Die heute weit verbreiteten Produkte agieren noch weitgehend IAM-agnostisch. Einige wenige bieten immerhin LDAP-basierende Zugriffsteuerungen zur Verfügung.

Benötige ich überhaupt IAM für Internet-Dinge?

Bevor die Frage beantwortet wird, ob und welche IAM Prozesse benötigt werden müssen neben der Klassifizierung der Geräte selbst noch weitere Dimensionen unterschieden werden:

- Welche Personen beziehungsweise Interaktionspartner sind involviert?
- Welche Geschäftsprozesse werden abgedeckt?

Daraus ist eine Risiko-Einschätzung abzuleiten, die dann die Notwendigkeit und den Umfang der IAM Prozesse begründet.

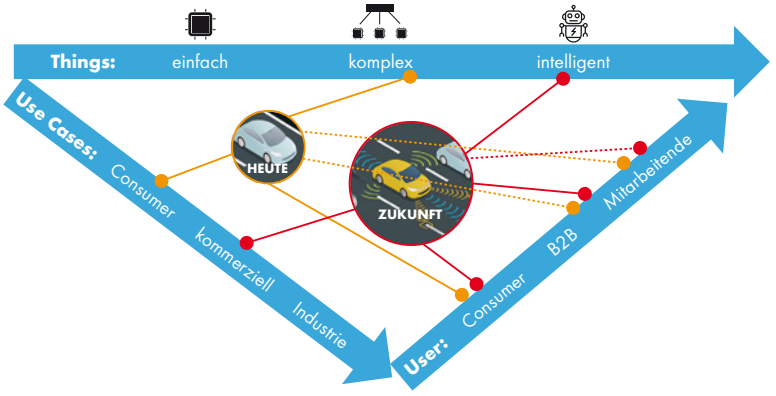
Interaktionspartner:

Hier kommen die klassischen IAM-Einstufungen zum Tragen, das bedeutet, wir unterscheiden zwischen Mitarbeitenden im Unternehmen, Business-to-Business und Business-to-Consumer Szenarien. Zusätzlich können auch die IoT-Devices miteinander interagieren. Im Au-tomobilbereich werden beispielsweise die folgenden Interaktionsformen betrachtet:

SEHR HÄUFIG ERLEBEN WIR IM RAHMEN VON IAM-STRATEGIE-PROJEKTEN, DASS NUR DIFFUSE IDEEN EXISTIEREN, WELCHE IOT-SZENARIEN IN ZUKUNFT RELEVANT WERDEN.

Peter Weierich, Managing Director, ipg Deutschland GmbH | www.ipg-group.com

KLASSIFIZIERUNG VON IOT-SZENARIEN



BEISPIEL FÜR IOT-SZENARIEN

	Heute	Morgen
Szenario	1. Assistenzfunktionen im „eigenen" PKW 2. Abfrage von Fahrzeugdaten	Mobilitätsdienstleistungen mit autonomen Fahrzeugen
IoT-Klassifikation	komplex, zum Teil intelligent (Mustererkennung, Spurhalteassistent, Abstandsregelung)	Intelligent, autonom
Use Cases	Consumer	Consumer und kommerziell (Mobilitätsverträge auch mit-Unternehmen)
Interaktion	In-vehicle, Consumer- mit rein physischer Zugangskontrolle V2E für Fahrzeugdaten (zum Beispiel Online-Abfrage von Tankfüllung, GPS Position, Servicestatus)	• C-IAM für Bestell- und Abrechnungsvorgänge • Vehicle-to-Enterprise für die Flottenplanung und -steuerung • Vehicle-to-vehicle für Optimierung der Fahrten
Geschäftsprozessell	Consumer mit bzw. ohne „digitale Identität"	Consumer, B2B
IAM Anforderungen	Für 1: Praktisch nicht vorhanden, nur für zentrale Assistenzfunktionen erforderlich Für 2: C-IAM für Benutzerregistrierung, Login etc.	Hoch, insbesondere um Fremdeingriffe in das System zu verhindern

- In-Vehicle: User (Fahrer) beziehungsweise Fahrgäste kommunizieren mit dem Fahrzeug
- Vehicle-to-Vehicle: Fahrzeuge interagieren miteinander
- Vehicle-to-Enterprise: Die Fahrzeuge interagieren mit dem Hersteller bzw. einer anderen Partei, etwa einem Mobilitätsdienstleister

Art der Geschäftsprozesse:

- Consumer-Prozesse haben häufig sehr niedrige Sicherheitsanforderungen oder Anforderungen an IAM Prozesse – es sei denn, es handelt sich um Finanztransaktionen oder um Szenarien, bei denen es um die Gesundheit von Menschen geht: Beispielsweise bei digitalen und vernetzen Blutzuckermessgeräten oder Insulinpumpen.
- „Commercial"-Prozesse, bei denen typischerweise Unternehmen involviert sind.
- Industrie-Prozesse: Hierunter werden die klassische „Industrie 4.0" Prozesse in der Produktion subsummiert, die oft besonders hohe Sicherheitsanforderungen haben.

Beispiel: Motorisierter Individualverkehr

Die heutigen Nutzungsszenarien erfordern oft keine IAM-Mechanismen, allerdings bieten die Hersteller häufig digitale Dienste (Connected Drive, Audi Connect, me connect, OnStar etc.) an, die folgende IAM Basisprozesse erfordern:

- Registrierung als User (typischerweise über die Homepage des Herstellers),
- Herstellen der logischen Verbindung zum PKW
- Anmeldevorgänge im PKW / per App.

Zukünftig bedarf es detaillierter Konzepte für die folgenden Fragen: Welcher Prozessbeteiligter darf welche Daten von welchen Fahrzeugen wissen (Position, Route, Auslastung, Ladezustand)? Wie darf wer steuernd eingreifen, auch beispielsweise für Umfahrungsrouten etc.? Wer darf wissen welche Person in welchem Fahrzeug wo unterwegs ist? Eine Gegenüberstellung wesentlicher Punkte findet sich in der Tabelle.

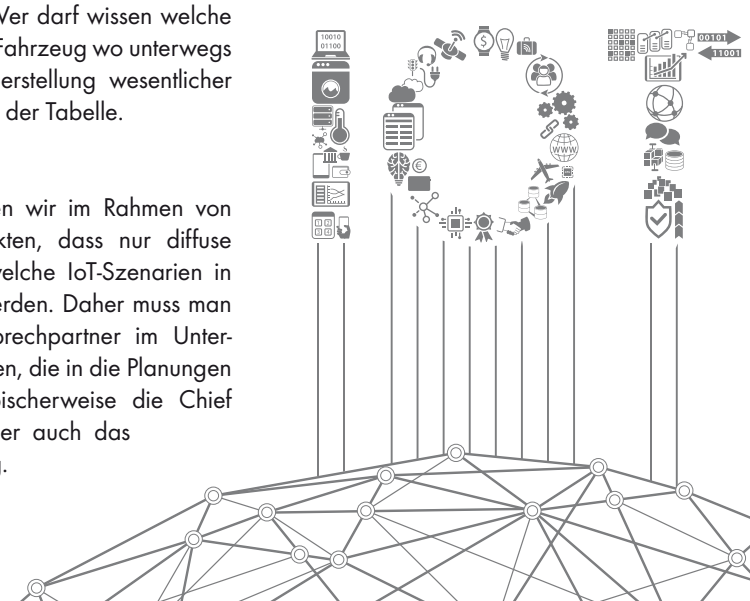
Was ist zu tun?

Sehr häufig erleben wir im Rahmen von IAM-Strategieprojekten, dass nur diffuse Ideen existieren, welche IoT-Szenarien in Zukunft relevant werden. Daher muss man zunächst die Ansprechpartner im Unternehmen identifizieren, die in die Planungen involviert sind, typischerweise die Chief Digital Officers oder auch das (Produkt-)Marketing.

Allerdings passiert es regelmäßig, dass aus der Produktentwicklung heraus eine Entscheidung für die Einführung einer IoT-Plattform von einem strategischen Lieferanten, etwa von Microsoft (Azure IoT) fällt, ohne vorher die User Journeys zu entwickeln, die bedient werden sollen.

Daher ist es erforderlich, möglichst früh auch IAM Spezialisten bei der Entwicklung der IoT-Szenarien zu involvieren, um im Vorfeld „die richtigen Fragen" zu stellen. Unter anderem können dann IAM-Anforderungen an eine zu beschaffende (oder zu mietende) IoT-Plattform abgeleitet werden, da etliche Produkte nur marginale oder gar keine IAM-Prozessunterstützung leisten können.

Peter Weierich



EDGE PLATFORM

AUF DEM WEG ZUR SICHEREN MULTI-CLOUD.

Im Zuge der Digitalisierung entscheiden sich immer mehr Unternehmen dazu, Daten, Prozesse und Anwendungen in die Cloud zu verlagern. Dafür stehen ihnen mit Private, Public und Hybrid Cloud verschiedene Modelle zur Verfügung, die sich je nach Bedarf individuell anpassen lassen. Wer Anwendungen verschiedener Cloud-Anbieter parallel nutzen möchte, für den ist das Modell der Multi-Cloud perfekt geeignet. Diese Bündelung unterschiedlicher Cloud-Dienste innerhalb einer Cloud-Architektur bietet zahlreiche Vorteile, birgt aber gleichzeitig aufgrund ihrer Komplexität gewisse Risiken. So können einheitliche Compliance-Richtlinien und Sicherheitskonzepte meist nur mit hohem Aufwand bereitgestellt werden. An dieser Stelle tritt Akamai auf den Plan: Die Akamai Intelligent Edge Platform ebnet Unternehmen den Weg zur Multi-Cloud Strategie. Compliance, Sicherheit, Performance und Stabilität sind dann nicht mehr optional, sondern Standard.

Für Firmen drängt sich der Schritt in die Cloud nahezu auf: Ob Datenspeicherung, Softwarenutzung oder IT-Leistungen – Cloud-Computing bringt zunächst vor allem Vorteile. Kosten für Software und Hardware sinken und Abläufe lassen sich effizienter gestalten. Abhängig von den Anforderungen eines Unternehmens besteht die Wahl zwischen der Nutzung einer Private Cloud, einer Public Cloud oder einer Hybrid Cloud. Bei der Private Cloud werden Services exklusiv für Firmen, Konzerne oder Behörden bereitgestellt. Der Zugriff darauf ist nur intern über ein separates Intranet oder über ein abgeschlossenes Virtual Private Network (VPN) möglich. Zudem wird die Private Cloud auf firmeneigenen Rechnern oder über entsprechende Dienstleister gehostet. Bei strengen Sicherheitsauflagen ist dieses Modell ideal.

Die Dienste der Public Cloud sind hingegen über das öffentliche Internet zugänglich. Services wie Rechenleistung, Speicherplatz oder Anwendungen können hier bezogen werden. Eine Mischform dieser beiden Cloud-Modelle ist die Hybrid Cloud: Dabei wird die Private um eine Public Cloud ergänzt. Dadurch ist sie auch bei datenschutzkritischen Anwendungen einsetzbar, während Unternehmen gleichzeitig von der Flexibilität und den Kosteneinsparungen von Public Cloud-Lösungen profitieren.

Passgenaue Lösungen dank Multi-Cloud

Bei der Multi-Cloud werden die Services mehrerer Anbieter miteinander kombiniert – unter dem Dach einer einzigen großen Cloud. Das Konzept ist also eine Erweiterung des Hybrid-Cloud-Modells: So kann zum Beispiel eine Private Cloud mit unterschiedlichen Services diverser Public Clouds ergänzt werden. Die Organisation und Verwaltung der Cloud-Services und IT-Infrastruktur kann über Cloud-Management-Plattformen (CMP) erfolgen. Ziel ist es, Services, Anwendungen und Infrastrukturen verschiedener Anbieter parallel zu nutzen und dadurch unabhängig zu bleiben. Bei der Auswahl des jeweils passendsten Providers orientieren sich Firmen daran, welche Services sie benötigen, wie die Kosten ausfallen und welche Leistung erbracht wird.

Die Vorteile einer solchen IT-Architektur: Firmen bewahren ihre Unabhängigkeit, indem sie Services von mehreren Dienstleistern verwenden. Zudem können sie schnell und flexibel zwischen den Angeboten wechseln, wenn sich Bedarf, Prei-

> DIE AKAMAI INTELLIGENT EDGE PLATFORM UND IHRE CLOUD SECURITY-LÖSUNGEN BIETEN FÜR HYBRID CLOUD-INFRASTRUKTUR UMFASSENDEN SCHUTZ GEGEN WEB-, DDOS-, DNS- UND BOT-ATTACKEN.
>
> Elmar Witte, Product Marketing Manager Security, Akamai Technologies
> www.akamai.com/de

se oder Leistungen ändern. Mithilfe der Multi-Cloud können Unternehmen genau die Services auswählen und zusammenstellen, die ihren individuellen Anforderungen entsprechen. Auch für Firmen, die strenge Sicherheits- und Datenschutzauflagen beachten müssen, ist das Konzept ideal: Sie organisieren sensible Daten in einer Private Cloud und nutzen für alle anderen Bereiche die Services aus der Public Cloud. Der Servicemix innerhalb der Multi-Cloud sorgt für Kosteneffizienz und wirkt sich positiv auf die Leistungsfähigkeit der Anwendungen aus.

Multi-Cloud: Top oder Flop?

Setzt ein Unternehmen auf verschiedene Services, zum Beispiel von Amazon Web Services (AWS), Microsoft Azure oder Google Cloud, bringt ihm dieser Mix allerdings nicht nur Vorteile. Denn je mehr Dienste innerhalb der Multi-Cloud genutzt werden, desto komplexer werden Management und Sicherheitsanforderungen an die IT.

Oftmals fehlt nämlich die entsprechende Cloud-Security und muss zusätzlich gekauft werden. Selbst wenn eine Sicherheitslösung integriert ist, ist sie mitunter nicht mit anderen Systemen kompatibel, sodass für jeden Cloud-Service eine eigene Security-Lösung benötigt wird. Da es kein einheitliches Datensicherheitskonzept gibt, entstehen Inkonsistenzen. Ist eine Multi-Cloud-Strategie für Unternehmen also doch nicht die passende Option?

Doch! Denn zunächst löst die Multi-Cloud das Problem, dass es keinen Dienst gibt, der alle Einsatzszenarien optimal abdeckt. Die Multi-Cloud bietet das ideale Konzept, um den individuellen Bedarf an Cloud-Services einer Firma passgenau abzudecken, und hilft dabei unabhängig und flexibel zu bleiben. Unternehmen fehlt also lediglich ein Partner, der mit ihnen ein ganzheitliches Sicherheitskonzept erarbeitet und umsetzt, über alle Cloud-Dienste und -Anbieter hinweg.

Die Intelligent Edge Platform

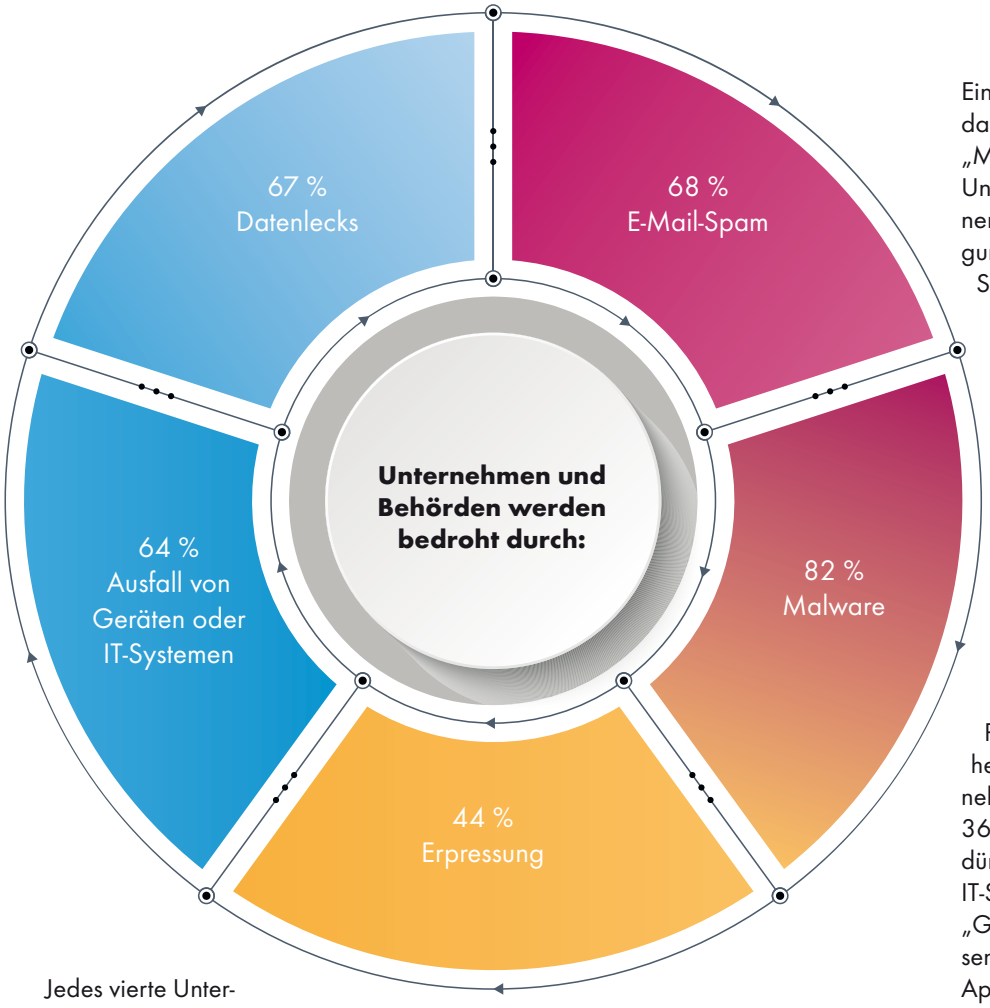
Genau hierfür hat Akamai eine Lösung entwickelt: Die Akamai Intelligent Edge Platform und ihre Cloud Security-Lösungen bieten für Hybrid Cloud-Infrastruktur umfassenden Schutz gegen Web-, DDoS, DNS- und Bot-Attacken. Dabei wird dafür gesorgt, dass individuelle Services gegen die verschiedenen Angriffe aus dem Internet geschützt werden können, ob sie nun auf AWS, Azure oder der Google Cloud bereitgestellt werden. Zudem werden über das Akamai Content Delivery Network (CDN) mit über 240.000 Servern weltweit sämtliche Cloud-Applikationen und digitalen Inhalte beschleunigt ausgeliefert, das heißt die Anwendungen werden schneller und die Nutzerakzeptanz steigt.

Wie die Intelligent Edge Platform funktioniert, zeigt ein Kundenbeispiel: Ein großes globales Finanzdienstleistungsunternehmen, bestehend aus unabhängigen Geschäftsbereichen, folgt strikt der Maxime „Cloud-first". Um stets die beste Nutzererfahrung zu gewährleisten, entwickelt das Unternehmen Anwendungen auf AWS, Azure und Google Cloud. Um trotz dieser Komplexität einheitliche Sicherheitsstandards über alle Dienste hinweg zu etablieren, hat das Unternehmen eine Cloud-unabhängige Sicherheitsebene integriert, die allen Webanwendungen vorangestellt ist (Schutz gegen Web- und DDoS-Attacken sowie Bot Management). Darüber hinaus nutzt der Finanzdienstleister auch die Web-Performance-Lösungen, um seine Webseiten und Webanwendungen zu beschleunigen. So gewährleistet das Unternehmen ein hervorragendes Nutzungserlebnis für die Endanwender und eine optimierte IT-Sicherheit.

Elmar Witte

IT-SICHERHEIT

BUDGETOFFENSIVE GEGEN DIGITALE SORGLOSIGKEIT.



Jedes vierte Unternehmen in Deutschland kämpft mit dem Problem knapp bemessener Budgets für IT-Sicherheit. Bedarf besteht bei der Sensibilisierung der Mitarbeiter und bei der Rekrutierung von IT-Sicherheitsspezialisten.

Das soll sich bis 2021 ändern. Mehr als die Hälfte der Entscheider (56 Prozent) erwarten für die kommenden drei Jahre eine Steigerung des Budgets. Jeder vierte Manager geht von konstanten Ausgaben für den Kampf gegen potenzielle Cyberattacken und für den Schutz von Kunden- und Unternehmensdaten aus. Das ergibt die Studie „Potenzialanalyse Unternehmen schützen, Risiken minimieren" von Sopra Steria Consulting und dem F.A.Z.-Institut.

Digitale Sorglosigkeit und wie ihr zu begegnen ist, bleibt für viele Geschäftsleitungen auf der Themenagenda 2019. 34 Prozent der befragten Unternehmen schätzen das Risiko, Opfer einer schwerwiegenden Cyber-Attacke zu werden, als sehr gering beziehungsweise gering ein.

59 Prozent haben zwar eine IT-Sicherheitsstrategie formuliert, dokumentiert und verabschiedet. 25 Prozent der befragten Manager beklagen allerdings finanzielle Schwierigkeiten bei der Umsetzung.

50 Prozent finden beispielsweise keine passenden IT-Sicherheitsspezialisten, auch weil zu wenig Budget für Rekrutierungskampagnen eingeplant ist.

Ein großer Investitionsbedarf besteht darüber hinaus beim Sicherheitsrisiko „Mensch". In 57 Prozent der befragten Unternehmen wurde in den vergangenen drei Jahren ein zentrales Berechtigungsmanagement eingeführt, so die Studie. Gut ein Drittel setzt mittlerweile auf regelmäßige Sensibilisierungskampagnen für Mitarbeiter. Angesichts der wachsenden Zahl schwerwiegender Sicherheitsvorfälle ist allerdings davon auszugehen, dass die Anteile künftig steigen werden. Unerwünschte E-Mails sind für 68 Prozent der befragten Entscheider die Top-Bedrohung, die sie bis 2021 deutlich besser im Griff haben wollen.

Security-Awareness nimmt zu

Parallel dazu soll das Thema IT-Sicherheit stärker als bislang in die Unternehmensprozesse verankert werden. In 36 Prozent der befragten Unternehmen dürfen IT-Projekte nur bei Vorliegen eines IT-Sicherheitskonzepts gestartet werden. „Genauso wie ein Auto nicht ohne Bremsen vom Band läuft, sollten auch kritische Apps und digitalisierte Abläufe in einem Unternehmen nicht ohne Sicherheitskonzept live gehen", sagt Dr. Gerald Spiegel, Leiter Information Security Solutions, von Sopra Steria Consulting. „Nötig hierfür sind allerdings abgestufte Konzepte je nach Risikolage, damit unkritische Projekte nicht durch unnötig scharfe Kontrollen zu teuer werden oder zu lange dauern", so Spiegel.

Das Inkrafttreten der EU-DSGVO im Mai 2018 haben immerhin 72 Prozent der Unternehmen genutzt und ihre unternehmensinternen Strategien und Maßnahmen professionalisiert. Verstöße wie in Portugal – dort soll ein Krankenhaus jetzt aufgrund von Verstößen 400.000 Euro Strafe zahlen – rütteln auf.

www.soprasteria.de

CYBERSECURITY FÜR DIE INDUSTRIE

Wer auf dem neuen digitalen Markt erfolgreich sein will, muss seine Daten bestmöglich nutzen. Für Industrieunternehmen ist es daher heute unverzichtbar, die traditionell isolierte Operational Technology (OT) mit der IT zu verbinden. Wie aber sichert man solche Umgebungen richtig ab?

Fast alle Industrieunternehmen haben bereits damit begonnen, ihre OT- und IT-Netze zu verbinden. Doch bei der Absicherung sind sie mit zahlreichen Problemen konfrontiert. IT- und OT-Teams sprechen einfach unterschiedliche Sprachen. Viele Industriesteuerungs- und SCADA-Systeme sind seit langer Zeit in Betrieb. So kann selbst ein harmloser Malware-Scan zu Fehlfunktionen führen. Gleichzeitig steigt die Gefahr für Cyber-Angriffe. Wie eine Studie von Fortinet und Forrester Research ergab, haben 88 Prozent der Unternehmen schon einmal einen Sicherheitsvorfall bei ihren SCADA/ICS-Architekturen erlebt.

Integrierter Cybersecurity-Schutz

Um die Geschäftsziele zu erreichen, ohne die OT zu kompromittieren, empfiehlt es sich, auf einen erfahrenen Anbieter für SCADA/ICS-Security zu setzen. Genau das ist Fortinet mit dem Security Fabric- und Fabric-Ready-Partner-Ansatz. Fortinet ist einer der wenigen Sicherheitsanbieter, die auf den Schutz und die Absicherung von OT-Operationen spezialisiert sind, insbesondere solche, die zu den kritischen Infrastrukturen gehören. Fortinets robuste Firewall-, Switching- und Wireless-Access-Point-Appliances, kombiniert mit FortiGuard Industrial Threat Intelligence, bieten integrierten Cybersecurity-Schutz für Industriesteuerungs- und SCADA-Systeme. Die FortiGuard Industrial Security Services (ISS) schützen die am weitesten verbreiteten ICS- und SCADA-Geräte und -Anwendungen. Sie bieten Schwachstellenschutz, umfassende Transparenz und granulare Kontrolle.

www.fortinet.com

FORTINET®

GEFÄHRLICHER TREND

DDOS-ATTACKEN WERDEN QUALITATIV HOCHWERTIGER.

Für DDoS-Angriffe gibt es eine Art Miet-Modell inklusive Preisstaffelung, bei dem Käufer sekundenweise die Leistungsstärke eines Botnetzes mieten können. Auch wenn die Anzahl von DDoS-Angriffen im Jahr 2018 gegenüber 2017 um 13 Prozentpunkte leicht rückläufig war, sehen die Experten von Kaspersky Lab einen gefährlichen Trend in der Qualität solcher Angriffe. Der Grund: Bessere Schutzmaßnahmen seitens Unternehmen führen dazu, dass Cyberkriminelle in diesem Jahr ihre Expertise weiter ausbauen werden, um erfolgreicher zu sein.

„Wenn die meisten einfachen DDoS-Angriffe ihr Ziel nicht erreichen, haben die Personen, die durch solche Angriffe Geld verdienen, zwei Möglichkeiten", so Alexey Kiselev, Business Development Manager im Kaspersky DDoS Protection Team. „Sie können entweder die für DDoS-Angriffe erforderlichen Kapazitäten für andere Einnahmequellen wie Krypto-Mining verwenden oder aber sie müssen ihre technischen Fähigkeiten verbessern, da ihre Kunden nach erfahreneren Angreifern suchen. Vor diesem Hintergrund können wir davon ausgehen, dass sich die DDoS-Angriffe im Jahr 2019 weiter entwickeln werden und es für Unternehmen schwieriger wird, sie zu erkennen und sich zu schützen."

www.kaspersky.de

ERGEBNISSE Q4 2018

- **Der längste Angriff dauerte 329 Minuten, also fast 14 Tage.**
- **Die meisten Botnet-Angriffe fanden im Oktober statt.**
- **China (50,43%), USA (24,90%)und Australien (4,5%) waren am häufigsten von DDoS-Angriffen betroffen.**

CLOUDSZENARIO

BEST PRACTICES FÜR MITTELSTÄNDISCHE UNTERNEHMEN MIT MEHREREN STANDORTEN.

Wachsende, mittelständische Unternehmen mit vielen Standorten stehen häufig vor der Herausforderung, die IT-Grundausstattung für neue Standorte und Mitarbeiter schnell und flexibel bereitstellen zu müssen. Verzögerungen und technische Probleme können zu geschäftsschädigenden Ausfällen führen. Darüber hinaus sind Aufbau, Betrieb, Wartung und Support einer „realen" lokalen Infrastruktur in standortreichen Unternehmen personell oder finanziell oft nicht umsetzbar. Eine Lösung liegt daher immer öfter im kompletten Outsourcing der IT-Infrastruktur in die Cloud.

Was bringt das Outsourcing der Infrastruktur?

Das Auslagern der IT-Infrastruktur bietet besonders mittelständischen Unternehmen große Vorteile. Durch die Cloudlösung werden keine eigenen IT-Abteilungen an den Standorten benötigt, da der Administrationsaufwand für lokale Systeme entfällt und technische Probleme remote gelöst werden können. Das versetzt die Unternehmen in die Lage, User weitgehend ortsunabhängig zu betreuen. Durch die Zusammenarbeit mit dem Cloudanbieter lassen sich zudem viele Rollout-Prozesse standardisieren, die den Aufwand für die Einrichtung neuer Standorte deutlich verringern. Auch zeitintensive Aufgaben für Betrieb, Verfügbarkeit und Weiterentwicklung der Infrastruktur entfallen. Diese liegen nun komplett im Verantwortungsbereich des Cloudanbieters.

Entscheiden Unternehmen sich für einen Provider mit Rechenzentrum in Deutschland, profitieren sie von der räumlichen Nähe zu ihren Standorten sowie hohen Standards in den Bereichen Datenschutz und -sicherheit. Bei professionellen Cloudanbietern stehen außerdem individuelle Beratungsmöglichkeiten, weitere Services und persönlicher Support zur Verfügung.

Wie finden Unternehmen den richtigen Cloudanbieter?

Üblicherweise stellt der Cloudanbieter die virtuellen Instanzen aus Rechenleistung, Arbeitsspeicher und Storage sowie Domänen-, File- und Printdienste zur Verfügung. Außerdem besteht eine typische IT-Infrastruktur in der Cloud aus einem standortübergreifenden Netzwerk über VPN und einer VPN-Verbindung zur Firewall einschließlich der nötigen Firewallregeln. Die Erweiterung um die neuen IP-Adressbereiche sowie ein ausführlicher Funktionstest

Outsourcing-Vorteile im Überblick:

- Einsparen von Ressourcen in lokalen IT-Teams
- kein lokales IT-Team an jedem Standort nötig
- Wartungstätigkeiten rund um die lokale Infrastruktur entfallen
- Standardisieren von Rollout-Prozessen
- Auslagern der Verantwortung für Betrieb und Verfügbarkeit der Infrastruktur
- Auslagern von Entwicklungsarbeiten, um die Zukunftssicherheit der Infrastruktur zu gewährleisten
- Remote-Support für technische Probleme, da sich die Systeme nicht nur lokal befinden
- persönlicher Support und Beratung
- lokale Nähe durch Rechenzentrum und Standort in Deutschland

runden das Paket ab. Auch Standorte im Ausland lassen sich so weltweit anbinden.

Nach der erfolgreichen Bereitstellung der gewünschten IaaS-Komponenten liegen Einrichtung und Betrieb der Umgebung jedoch beim Unternehmen selbst. Hier kommen lokale IT-Dienstleister mit eigener Cloudplattform ins Spiel: Anders als viele große Cloudanbieter sind sie mit persönlichen Ansprechpartnern für ihre Kunden da und können individuelle Anforderungen flexibler umsetzen.

Zudem garantieren lokale Cloudanbieter mit Zusatzangeboten wie Managed Services und Remote-Support eine Komplettbetreuung. Dabei übernehmen sie zum Beispiel die Verwaltung von Security-Infrastrukturen, eine kontinuierliche Überwachung, das Einspielen von Updates und Patches oder regelmäßige Datensicherungen.

Schneller Einstieg in die Cloud mit Warm Migration

Ist die Entscheidung für die Cloud und den Anbieter gefallen, muss die Migration der Daten organisiert werden. Auch für ein Problem, das dabei regelmäßig für Bedenken sorgt, gibt es bei ausgewählten lokalen Cloudanbietern seit Kurzem revolutionäre Lösungen: Normalerweise müssen Daten, die ausgelagert werden, kopiert und im Rechenzentrum des Cloudanbieters wieder eingespielt werden. Neben dem Zeitaufwand und komplexen Netzwerkanpassungen bedeutet dies ein hohes Risiko für die Daten, die per Festplatte zum Rechenzentrum des Providers transportiert werden müssen – möglicherweise quer durch ganz Deutschland. Bei der „warmen" Migration werden virtuelle Maschinen im laufenden Betrieb HTTPS-verschlüsselt in die Cloud repliziert. Möglich macht dies der vCloud Director Extender von VMware, der eine direkte Verbindung zwischen der Umgebung des Cloudproviders und dem On-premises-Rechenzentrum des Unternehmens herstellt. Egal ob die Infrastruktur komplett in die Cloud verlagert oder als hybride Umgebung betrieben werden soll – Unternehmen profitieren von einer schnellen, reibungslosen Migration und einer persönlichen Beratung und Betreuung durch den lokalen Cloudanbieter.

Viele Vorteile durch lokale Dienstleister

Grundsätzlich bringt eine Migration in die Cloud deutliche Verbesserungen im Bereich Performance und Sicherheit der IT-Systeme, da professionelle Cloudanbieter neueste Speicher- und Sicherheitstechnologien einsetzen. Zudem ist es gerade für standortreiche Unternehmen von Vorteil, dass sich die Systeme so verhalten, als würden sie am jeweiligen Standort stehen. Ein Aufbau neuer Standorte bei wachsenden Unternehmen ist so schnell und einfach möglich.

Speziell lokale Cloudanbieter punkten außerdem mit persönlicher Betreuung und Support als Qualitätsmerkmal und schaffen so das notwendige Vertrauen für Outsourcing-Projekte, denn das Unternehmen muss sich auf den Partner, der sein gesamtes System betreut, hundertprozentig verlassen können. Insbesondere mittelständischen Unternehmen mit vielen Niederlassungen kommt diese Zusammenarbeit zugute, da zahlreiche Möglichkeiten für Managed Services, individuelle Beratung und ausreichend Flexibilität bei der Umsetzung bestehen.

Jochen Griebel

DAS AUSLAGERN DER IT-INFRASTRUKTUR BIETET BESONDERS MITTELSTÄNDISCHEN UNTERNEHMEN GROSSE VORTEILE.

Jochen Griebel, Vertriebsleiter, netlogix IT-Services | www.netlogix.de

INDUSTRIAL CONTROL SYSTEMS

IM VISIER VON CYBERKRIMINELLEN.

Industrial Control Systems (ICS) beziehungsweise Betriebstechnik (Operational Technology, OT) bilden den Motor von Schlüsselindustrien und kritischen Infrastrukturen wie Energie, Wasser, Transport, Produktion und Chemie. Da die OT in der Vergangenheit sowohl digital als auch physisch abgeschottet war, galt sie als hacksicher und es gab keine Notwendigkeit für entsprechende Sicherheitsmaßnahmen. Doch mit der Konvergenz und zunehmenden Vernetzung von IT- und ICS/OT-Architekturen steigt nun die Gefahr von Cyberangriffen auf kritische Infrastrukturen durch computergestützte Exploits. Klassische IT-Security Ansätze aus der Office-IT greifen hier jedoch oft zu kurz und berücksichtigen beispielsweise nicht die lange Lebensdauer der ICS, bedingt durch die Betriebsdauer von Produktionsanlagen. In vielen Fällen hindern zudem Herstellervorgaben die Betreiber daran, eingesetzte zertifizierte Versionen zu aktualisieren oder zu verändern. So können bereits regelmäßige Updates oder Patches eine große Hürde für die Sicherheit der Produktionssysteme darstellen. Verschärft wird die Situation, da Wartungsarbeiten die Produktion in der Regel nicht einschränken oder gefährden dürfen. Aus diesen Gründen können klassische Best Practices und Technologielösungen aus der Office-IT nicht automatisch in der Industrial Security mit ihren hochkomplexen, herstellergebundenen und individuellen Systemen eingesetzt werden. Hier bedarf es eines neuen und mehrschichtigen Sicherheitsansatzes.

Ausgangslage für die Cybersicherheit in der Industrie

Cyberangriffe erfolgen häufig dreistufig: Dem Ausspähen folgen der Angriff und das Eindringen und Ausbeuten/Manipulieren der Systeme. Hacker spähen die Umgebung auf potentielle Schwachstellen in Hard- und Software aus und versuchen, über alle gefährdeten Personen, Prozesse oder Komponenten Zugang zu erhalten. Ein mehrschichtiger Sicherheitsansatz – Defense in Depth (DiD) – ist nötig, um physische und digitale Assets in zunehmend vernetzten ICS/OT-Umgebungen effektiv zu schützen.

DiD-Strategien hindern Eindringlinge mit so vielen und effektiven Hürden wie möglich daran, ihr Ziel zu erreichen. Gleichzeitig wird der Fortschritt des Angriffs überwacht sowie entsprechende Abwehrmaßnahmen entwickelt und umgesetzt. Mit dieser Strategie wird im ICS-Umfeld das unbefugte Eindringen frühzeitig erkannt, verhindert und eingedämmt. Eine Liste priorisierter Abwehrmaßnahmen stellt beispielsweise das Department of Homeland Security zur Verfügung.

Sicherheitskontrollen und Richtlinien

DiD-Praktiken reduzieren Risiken im Unternehmen auf ein akzeptables Maß. Ihre Einführung in die ICS sollte mit den kritischsten (höchste Auswirkung) und anfälligsten (höchste Wahrscheinlichkeit) Systemen beginnen. Sofern Mitarbeiter in Prozesse involviert sind, sind regelmäßige Cybersicherheits-Trainings sinnvoll. Zudem können mit intelligenten Zugangsdaten (Smart Cards) bereits Zugriffsrechte verwaltet werden. Unabhängig vom System, zum Beispiel Human Machine Interface (HMI) oder Supervisory Control and Data Acquisition (SCADA), können ICS-Hosts und Geräte im OT-Netzwerk mit mehreren Schritten gesperrt werden: Host-basierte Firewalls, starke Kennwörter, konsequentes Installieren von Patches und Updates

oder Entfernen vorinstallierter, nicht genutzter Software.

Unternehmen sollten proaktiv Schwachstellen suchen und beheben, um das Zeitfenster für Angreifer zu minimieren. Dazu müs-

sen sie ununterbrochen neue Informationen erfassen und bewerten sowie Maßnahmen ergreifen, um mögliche Einfallstore zu identifizieren und zu eliminieren. Mit jeder neu erkannten Schwachstelle beginnt ein Wettlauf gegen die Zeit. Im ICS-Umfeld können automatisierte Software-Update-Tools helfen, Betriebssysteme und installierte Software auf dem aktuellsten Stand zu halten. Hersteller oder Computer Emergency Response Teams (CERTs) informieren ergänzend über Schwachstellen.

Einfallstore reduzieren

Zu den größten Einfallstoren von Cyberattacken zählen USB-Sticks oder Service-Laptops. Sie können für den Transport von Schadsoftware hinein (bewusst wie unbewusst) oder von sensiblen Informationen hinaus missbraucht werden. Private Wechseldatenträger und andere mobile Endgeräte sollten daher im ICS-Umfeld entsprechend überwacht und reglementiert werden. Einen wirksamen Schutz vor der Ausführung schadhafter Programme bilden Applikations- und Schnittstellenkontrolle sowie Whitelisting mit Machine Learning. Während der Erst-Einrichtung dieser Endpoint Protection wird ein Hardware- und Applikations-Scan durchgeführt. Die Scan-Ergebnisse bilden dann die sogenannte Whitelist, für die Applikations- wie auch Geräte-Kontrolle. Nachträglich angeschlossene Datenträger werden zunächst blockiert, um vor zum Beispiel Bad-USB und dem unerlaubten Kopieren sensibler Daten zu schützen. Ebenso können keine Schadprogramme ausgeführt werden. Erlaubt ist ausschließlich die Ausführung erwünschter Programme; alle nicht explizit freigegebenen Anwendungen werden automatisch blockiert.

> MIT DER KONVERGENZ UND ZUNEHMENDEN VERNETZUNG VON IT- UND ICS/OT-ARCHITEKTUREN STEIGT DIE GEFAHR VON CYBERANGRIFFEN AUF KRITISCHE INFRASTRUKTUREN DURCH COMPUTERGESTÜTZTE EXPLOITS.
>
> Anton Kreuzer, CEO, DriveLock SE
> www.drivelock.de

Datenschutz und der Faktor Mensch

Der Schutz von Daten wird am besten durch eine Kombination aus Verschlüsselung, Integritätsschutz und Data Loss Prevention (DLP) erreicht. Durch die zunehmende Vernetzung von ICS und Office-IT, Cloud-Nutzung und mobilem Zugriff ist es entscheidend, die Datenexfiltration zu begrenzen, zu dokumentieren und Folgen abzuschwächen. Angreifer, die in solche Netzwerke eindringen, können leicht wichtige Informationen extrahieren, den Betrieb stören oder andere Schäden verursachen. Daher sollten externe Speichermedien verschlüsselt und das Kopieren von Daten stark eingeschränkt werden. Sensible Informationen mit Multi Factor Authentication zu sichern, bildet eine zusätzliche Schutzschicht.

Ein Security Awareness- und Trainingsprogramm für Mitarbeiter ist essentiell, weil große und komplexe Systeme anfällig für die Fehler ungeschulter Mitarbeiter sind – auch für die Aktivitäten bösartiger Insider. Neue Mitarbeiter sollten schnell hinsichtlich aller erforderlichen Vorschriften und Standards für das gesamte ICS/OT geschult werden. Ein solches Security-Awareness-Programm sollte unter anderem umfassen, Social Engineering zu erkennen und richtig mit sensiblen Informationen umzugehen von ihrer Identifizierung bis hin zur Vernichtung.

Industrial Security in fünf Schritten

Zusammenfassend können Industrieunternehmen mit diesen Schritten ihre Sicherheit maßgeblich erhöhen:

1. Identifizieren, Reduzieren und Sichern aller Netzwerkverbindungen zum ICS.
2. Ständige Überwachung und Bewertung der Sicherheit von ICS, Netzwerken und Verbindungen.
3. Härtung des ICS und der unterstützenden Systeme, indem nicht genutzte Anwendungen und Endgeräte deaktiviert, verfügbare Sicherheitsfunktionen aktiviert und robuste Konfigurations-Management-Verfahren eingesetzt werden.
4. Einführung eines risikobasierten Ansatzes zur Absicherung von ICS und Netzwerken.
5. Verwalten der Anforderungen an das ICS hinsichtlich Leistung, Verantwortlichkeiten, Richtlinien und Sicherheitsschulungen.

Anton Kreuzer

HERAUSFORDERUNG ENDPOINT SECURITY

ENDGERÄTE VOR CYBERATTACKEN SCHÜTZEN.

Mobile Endgeräte sind bei Mitarbeitern und Cyberkriminellen gleichermaßen beliebt: Den einen bieten sie die notwendige Flexibilität, für die anderen sind sie ein beliebtes Einfallstor für gezielte Attacken. Endpoint Security rückt damit zunehmend in den Fokus der Unternehmen. Für den CIO gilt es, die richtige Strategie zu finden, um das Unternehmensnetzwerk bestmöglich abzusichern.

EXTERNE IT-DIENSTLEISTER WIE LOGICALIS KÖNNEN HELFEN, DIE SICHERHEITSLAGE IM UNTERNEHMEN ZU BEWERTEN UND ENTSPRECHENDE IT-SICHERHEITSKONZEPTE ZU IMPLEMENTIEREN.

Stefan Mulder, Client Solution Director Cyber Security, Logicalis GmbH
www.logicalis.de

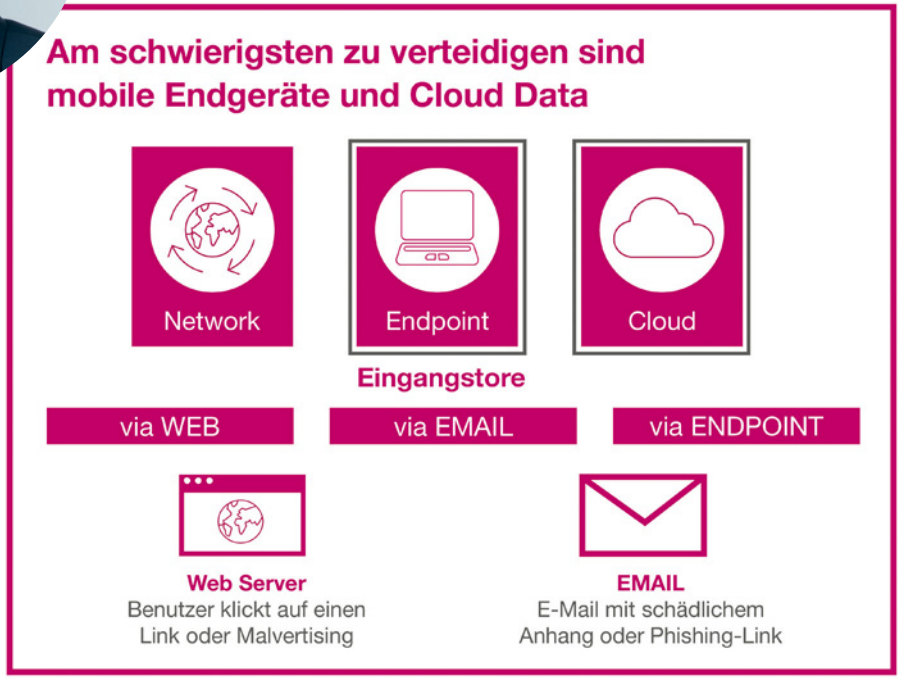
Unternehmen und ihre Mitarbeiter müssen immer flexibler sein. Sie sind zunehmend im In- und Ausland unterwegs, arbeiten von zu Hause aus, beim Kunden vor Ort oder abends im Hotel. Dabei surfen sie im Internet und nutzen soziale Netzwerke. Ob PC, Smartphone oder Laptop, ob Windows, Linux oder MacOS: Mobile Endgeräte bieten eine gute Angriffsfläche für Cyberkriminelle, die immer schneller, immer effektivere Malware-Arten entwickeln. Diese bringen klassische Sicherheitslösungen an den Rand des Machbaren. Weniger als 25 Prozent der Antiviren-Scanner können solche Attacken noch abwehren. Polymorphe Malware beispielsweise verändert sich permanent und macht es den Schutzlösungen dadurch schwer sie zu entdecken und zuzuordnen.

Die Brisanz der Lage ist den Unternehmen bekannt. Laut jüngster CIO-Studie von Logicalis widmen 54 Prozent der CIOs mindestens 30 Prozent ihrer Zeit der Informationssicherheit. Die Hälfte der CIOs wird am Faktor Risikominimierung sogar gemessen. Um in diesem Bereich bestehen zu können, müssen CIOs das Thema Endpoint Security mehr denn je auf ihre Agenda setzen.

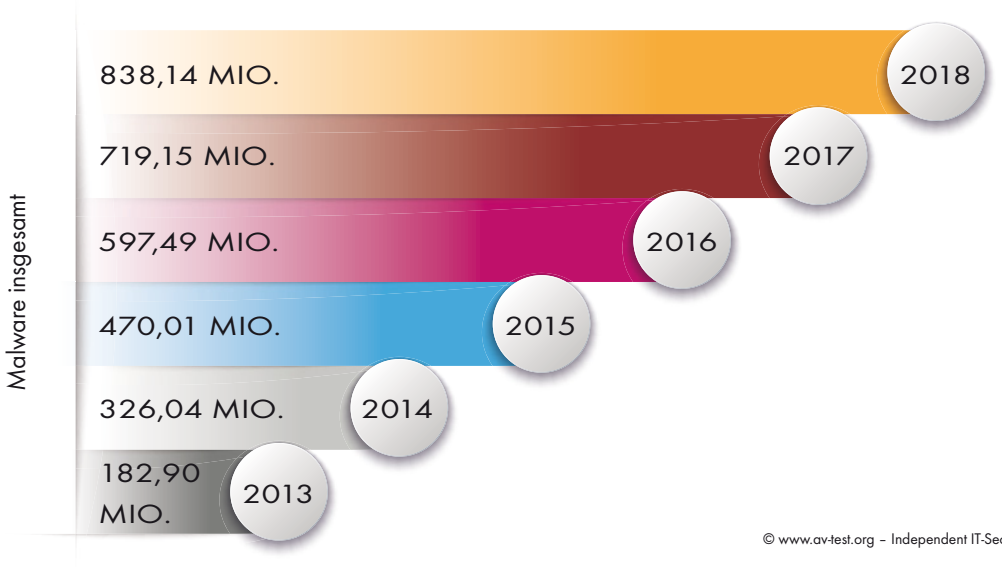
Umfassender Schutz

Fakt ist: Eine einmalige Prüfung auf potentielle Malware reicht heutzutage nicht mehr aus, um moderne Attacken auf Endgeräte abzuwehren. Die entsprechenden Tools werden durch Cyberkriminelle oft überlistet. So ist es zwar nach wie vor wesentlich, Dateien direkt beim Eintritt in das Netzwerk mittels erprobter Verfahren wie Viren-Scanner und Mustererkennung auf bekannte und unbekannte Malware zu untersuchen. Darüber hinaus gilt es aber, die weiteren Aktivitäten der Dateien zu überwachen, zu analysieren und zu dokumentieren.

Zeigen sie zu einem späteren Zeitpunkt ein schädliches Verhalten, muss nachvollziehbar sein, von wo sie ins Netzwerk einge-



Geschwindigkeit, Komplexität und Ausmaß von Cyber-Angriffen nehmen zu.



drungen sind, wo sie sich bewegt und was sie „im Sinn" haben. Mit diesem Wissen können sie identifiziert und ausgeschaltet werden. Stichwort: Retrospective Security oder auch Forensik. Sie schafft umfassende Transparenz und auch das notwendige Verständnis, um zukünftigen Attacken besser vorzubeugen. Auf diese Weise sparen Unternehmen auch Zeit und Kosten beim Schutz ihrer Endpoints.

Abwehr von Cyberattacken

Es kommt auf die richtige Mischung. Für die gesamte IT-Security gilt: Eine rein defensive Haltung bei der Cyberabwehr reicht nicht mehr aus. Mehr als ein Drittel der CIOs weltweit ist sich einig, dass Sicherheit heute eine Kombination von Erkennen, Abwehren, Standhalten und Vorbeugen sein muss. Eine solche Strategie basiert auf der Erkenntnis, dass es heutzutage unmöglich ist, alles Schädliche draußen zu halten.

Externe IT-Dienstleister wie Logicalis können helfen, die Sicherheitslage im Unternehmen zu bewerten und entsprechende IT-Sicherheitskonzepte zu implementieren. Diese umfassen beispielsweise Präventionsmaßnahmen zur Früherkennung von Angriffen, die Absicherung der Infrastruktur mit Firewalls und auch Endpoint Protection.

Das von Logicalis betriebene Security Operation Center bietet die notwendige Expertise und stellt die benötigte Palette an Lösungen und Services bereit. Kunden erhalten so einen effektiven Rundumschutz, ohne selbst in diesen Bereich investieren zu müssen.

Stefan Mulder

SICHER DURCH DEN CLOUD-DSCHUNGEL

Rolf Haas, Enterprise Technology Specialist von McAfee, hat Tipps den Überblick über komplexe Cloud-Strukturen zu behalten:

1. **Welche Daten liegen in der Cloud?**
   Wenn man nicht weiß, was man eigentlich schützen möchte, nutzen auch die besten Sicherheits-Tools wenig.

2. **Data Loss Prevention (DLP) reicht nicht mehr aus**
   Unternehmen müssen Cloud-native Lösungen installieren, um Cloud-Anwendungen gleichermaßen zu schützen und Sicherheitsregeln lückenlos durchzusetzen.

3. **Nutzerverhalten analysieren**
   CASB-Lösungen ermöglichen es, das Verhalten von Nutzern genauer zu überwachen.

4. **Automatisierung für mehr Sicherheit**
   Um eine sichere Cloud-Umgebung bereitzustellen kommt es darauf an, immer über die neuesten Versionen mit allen Patches zu verfügen.

www.mcafee.com/de

GEGENANGRIFF:

Daten sind der wichtigste Bestandteil in der digitalen Wirtschaft. Aus diesem Grund wurden Daten gleichzeitig zum wertvollsten und meist angegriffenen Wirtschaftsgut. Diesem Aspekt müssen Unternehmen also besondere Aufmerksamkeit schenken.

> COHESITY FINDET UND LÖSCHT INFIZIERTE DATEIEN IN GLOBALEN DATENSPEICHERN UND BRINGT ALLE ANWENDUNGEN UND DATEN MIT EINZIGARTIGEN FUNKTIONEN FÜR DIE SCHNELLE MASSENWIEDERHERSTELLUNG SOFORT ZURÜCK.
>
> Thomas Boele, Senior Director Systems Engineering EMEA. Cohesity
> www.cohesity.com

Ein wirksames Gegenmittel ist die Cohesity Platform-Lösung. Sie wirkt Ransomware-Angriffen effektiv entgegen und hilft Unternehmen, die Zahlung von Lösegeld zu vermeiden. Die umfassende End-to-End-Lösung bietet einen vielschichtigen Ansatz, um einen Ransomware-Angriff zu verhindern, zu erkennen und darauf zu reagieren. Die diversen Funktionen verhindern, dass das Backup zum Angriffsziel wird. Durch maschinelles Lernen bietet sie Transparenz und überwacht kontinuierlich alle Anomalien in den Daten. Im schlimmsten Fall hilft Cohesity dabei, infizierte Daten in globalen Speicherorten, einschließlich öffentlicher Clouds, aufzuspüren und anschließend zu löschen, um unternehmenseigen Daten und Apps sofort wiederherzustellen und die Geschäftskontinuität zu gewährleisten.

Die wichtigsten Vorteile:

- Verhindert, dass Backups zu einem Angriffsziel werden.
- Schnelle Erkennung von Anomalien durch kontinuierliche maschinengesteuerte Überwachung der Primärquellen
- Schnelle Wiederherstellung durch sofortige Massen-Restore vor Ort und über mehrere Clouds

Das geschieht wie folgt:

Verhindern

Eine dreifache Verteidigung: Das unveränderliche Dateisystem, DataLock und die Multi-Faktor-Authentifizierung verhindern, dass Backup-Daten zum Ziel werden

Erkennen

Maschinengesteuerte Intelligenz ermittelt Muster und erkennt und meldet automatisch Anomalien

Reagieren

Einfache Suche und sofortige Wiederherstellung zu jedem Zeitpunkt ermöglicht eine rasche Wiederaufnahme des Geschäftsbetriebs. Der einzigartige sofortige Massen-Restore von Cohesity stellt Hunderte von virtuellen Maschinen (VMs) schnell wieder her.

Angriffe verhindern

Hochentwickelte Ransomware, wie Locky und Crypto, wurde kürzlich zum Zerstören von Shadow Datenkopien und zum Wiederherstellen von Punktdaten verwendet. Damit wird die Backup-Infrastruktur von Unternehmen zum erstklassigen Ziel von Cyberkriminellen, obwohl diese eigentlich ein Teil der Verteidigung eines Unternehmens sein soll. Cohesity stoppt Eindringlinge, indem verhindert

RANSOMWARE STOPPEN!

EIN BLICK AUF DIE COHESITY-PLATFORM.

wird, dass das Backup zum Angriffsziel wird. Die Plattform mit seinem komplett neuen, speziell entwickelten Dateisystem - dem Cohesity SpanFS - für sekundäre Daten- und Anwendungs-Workloads, bietet auf einzigartige Weise einen mehrschichtigen Schutz vor einem Ransomware-Angriff. Unter anderem gewährleistet Cohesity den höchsten Schutz vor Ransomware-Angriffen, weil ein unveränderliches Dateisystem mit schreibgeschützten Status-Momentaufnahmen als Basis dient. Die folgenden Funktionen verbessern den Schutz:

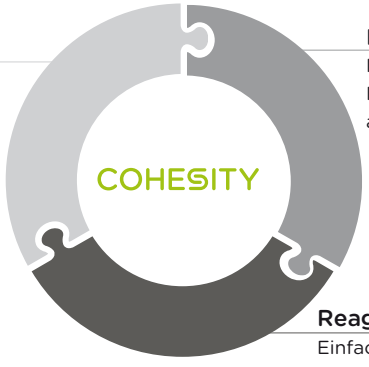
- Das unveränderliche Dateisystem kann sehr häufige, unbegrenzte schreibgeschützte Status-Snapshots machen und wird. Obwohl Ransomware Dateien in der gemounteten (Lese-/Schreib-) Sicherung löschen könnte, kann sie den unveränderlichen Snapshot nicht beeinflussen.

- Das Dateisystem SpanFS von Cohesity ermöglicht es eine sehr große Anzahl von Views zu erstellen und diese sofort zu kopieren, was so gut wie keine Kosten in Bezug auf den Speicherplatzverbrauch verursacht. Der Schutz vor unbefugten Zugriffen auf sensible Daten ist ein zentrales Anliegen von Cohesity.

Deshalb bietet die Lösung im Bereich Ransomware-Schutz neben dem unveränderlichen Dateisystem weitere innovative Funktionen:

- DataLock-Richtlinien – WORM-ähnliche Backup-Funktionen ermöglichen die rollenbasierte Erstellung und Anwendung einer DataLock-Richtlinie auf ausgewählte Backup-Snaps. Die Rolle des Sicherheitsbeauftragten im Unternehmen kann diese Funktion nutzen, um Snaps im WORM-Format zu speichern. Das zeitabhängige Setting, das bestimmte Zeitspannen festlegt, kann auch von der Rolle des Administrators oder Sicherheitsbeauftragten nicht gelöscht werden und bietet einen zusätzlichen Schutz vor Ransomware-Angriffen.

- Multi-Faktor-Authentifizierung (MFA) – Sollte ein Angreifer Zugriff auf das Systempasswort erhalten, kann diese Person nicht auf das Cohesity-Backup zugreifen, ohne eine zusätzliche Sicherheitsebene in Form von MFA oder mehrstufiger Verifizierung überwinden zu müssen. Die Plattform unterstützt eine Vielzahl von Authentifizierungs- und Autorisierungsfunktionen, darunter eine starke Active Directory-Integration, MFA, Zugriffskontrolllisten, Mixed-Mode rollenbasierte Zugriffskontrolle (RBAC) und umfassende Audits auf System- und Produktebene.



Verhindern
Eine dreifache Verteidigung: Das unveränderliche Dateisystem, DataLock und die Multi-Faktor-Authentifizierung verhindern, dass Ihre Backup-Daten zum Ziel werden

Erkennen
Maschinengesteuerte Intelligenz ermittelt Muster und erkennt und meldet automatisch Anomalien

Reagieren
Einfache Suche und sofortige Wiederherstellung zu jedem Zeitpunkt ermöglicht eine rasche Wiederaufnahme des Geschäftsbetriebs. Der einzigartige sofortige Massen-Restore von Cohesity stellt Hunderte von virtuellen Maschinen (VMs) schnell wieder her.

Bild 1: Cohesity bietet umfassende Funktionen zum Schutz, zur Erkennung und Reaktion auf Ransomware-Angriffe.

mit extrem geringem Aufwand speichern. Die ursprüngliche Backupdatei wird unveränderlich gespeichert und kann nie von einem externen System gemountet werden. Die einzige Möglichkeit, den Backup im Lese-/Schreibmodus zu mounten, besteht darin, das ursprüngliche Backup zu klonen, was vom System automatisch durchgeführt

Cohesity ist derzeit die einzige Plattform, die diese einzigartige Kombination aus

einem unveränderlichen Dateisystem mit DataLock-Funktionen und MFA bietet, um zu verhindern, dass Backup-Daten Teil eines Ransomware-Angriffs werden.

Angreifer entdecken

Da Cyberkriminelle ihre Methoden weiter verstärken und modifizieren, erleichtert Cohesity es Unternehmen, Einbrüche mit einer globalen, unternehmensweiten SaaS-basierten Managementlösung zu erkennen. Unternehmen, die Cohesity Helios nutzen, verfügen über ein einziges Dashboard, um ihre sekundären Daten und Anwendungen weltweit anzuzeigen, zu verwalten und schnell einzugreifen. Im Kampf gegen Ransomware liefert Helios Machine Learning (ML) Erkenntnisse, die Menschen übersehen könnten, weil es die Daten automatisch und kontinuierlich überwacht und benachrichtigt, wenn eine Anomalie erkannt wird.

Die hochmodernen ML-Algorithmen von Helios bewerten proaktiv die IT-Anforderungen und automatisieren regelmäßig Infrastrukturressourcen. Wenn die Datenänderungsrate des Unternehmens, einschließlich der Speicherung neuer Daten, außerhalb des normalen Bereichs liegt – basierend auf den täglichen Änderungsraten für logische Daten, gespeicherte Daten nach globaler Deduplizierung oder historische Datenspeicherung – sendet die maschinell gesteuerte Anomalieerkennung von HELIOS eine Benachrichtigung an die zuständige IT-Administratoren. Die IT-Abteilung wird sofort darüber informiert, dass Datenänderungen nicht den normalen Mustern entsprechen.

Da das maschinengesteuerte Lernen von Helios Muster erstellt und automatisch nach Anomalien der Datenspeicherungs- und -änderungsrate sucht, markiert es einen möglichen Ransomware-Angriff. Sollte eine Anomalie festgestellt werden, alarmiert Helios gleichzeitig das IT- und Support-Team von Cohesity und beschleunigt so die Abwehrmaßnahmen.

Neben der Überwachung der Änderungsrate von Backup-Daten, um einen potenziellen Ransomware-Angriff zu erkennen, erkennt und warnt die Plattform – und das ist einzigartig –vor Anomalien auf Dateiebene in unstrukturierten Datei-

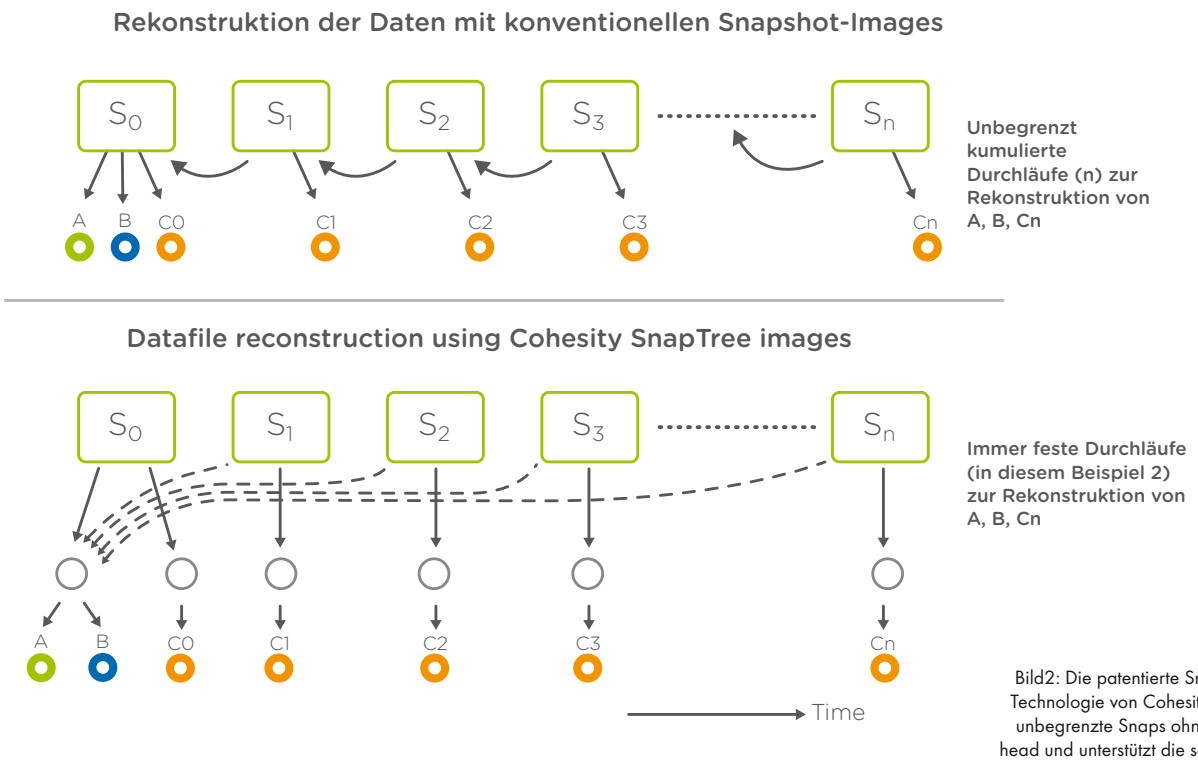


Bild2: Die patentierte SnapTree Technologie von Cohesity liefert unbegrenzte Snaps ohne Overhead und unterstützt die sofortige Wiederherstellung im großen Stil.

zu beschleunigen, führt die Plattform einfach eine schnelle Wiederherstellung des neuesten intakten Snapshots durch. Einzigartig ist, dass Cohesity Hunderte von VMs zu jedem Zeitpunkt sofort wiederherstellen kann. Die patentierte Cohesity SnapTree-Technologie speichert jedes Backup als vollständig hydratisierten Snapshot und unterstützt die sofortige Wiederherstellung zu jedem Zeitpunkt.

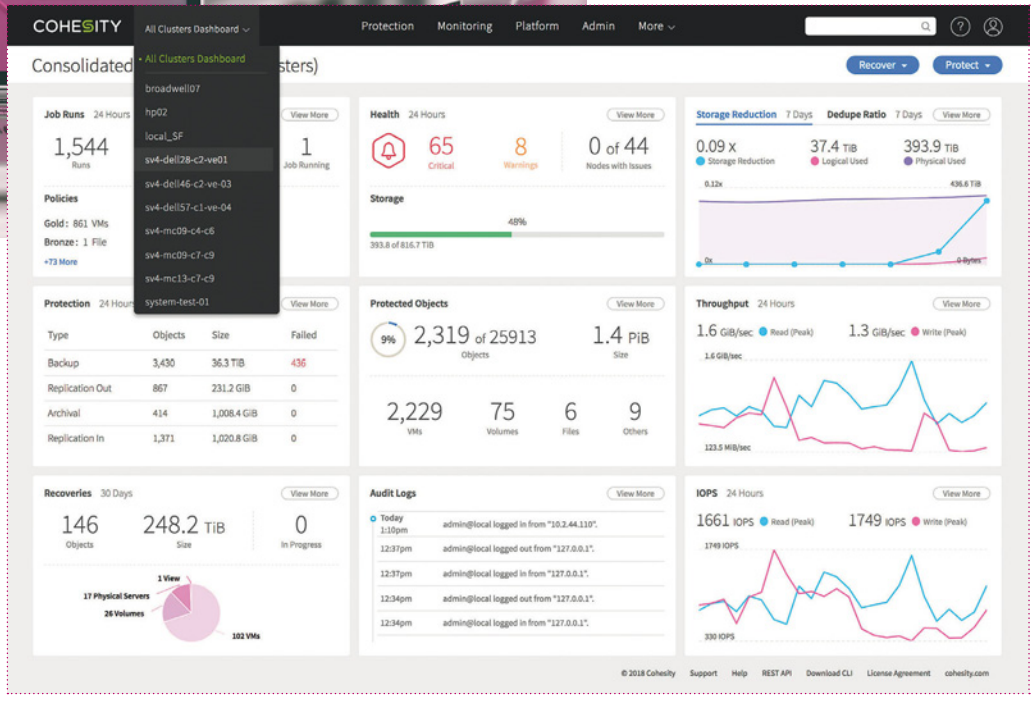


Bild 3: Mit Cohesity Helios erkennen Unternehmen Ransomware-Angriffe.

en und Objektdaten. Dazu gehört die Analyse der Zugriffshäufigkeit auf Dateien, die Anzahl der Dateien, die von einem bestimmten Benutzer oder einer Anwendung geändert, hinzugefügt oder gelöscht werden, und mehr, um sicherzustellen, dass ein Ransomware-Angriff schnell erkannt wird.

Rasch reagieren

Angriffe passieren, und zwar schnell. Deshalb muss auch die Wiederherstellung schnell erfolgen. Cohesity beschleunigt den Prozess, freigekaufte Unternehmensdaten und Anwendungen wiederzuerlangen - und zwar in großem Umfang. Die Plattform findet und löscht infizierte Dateien in globalen Datenspeichern - einschließlich Public Clouds wie Amazon Web Services, Microsoft Azure und der Google Cloud Platform - und bringt alle Anwendungen und Daten mit einzigartigen Funktionen für die schnelle Massenwiederherstellung sofort zurück. Sie durchsucht Helios und ermöglicht es, Korrekturmaßnahmen zu ergreifen, um eine reibungslosen Geschäftsbetrieb zu gewährleisten.

Die skalierbare DataPlatform speichert Backup-Daten mit den Speicherzyklen, die das Unternehmen festlegt – Wochen, Monate und Jahre – damit diese kurz nach ihrer Entstehung wiederhergestellt werden können. IT-Teams können die Google-ähnlichen, globalen Suchfunktionen der Plattform nutzen, um die Daten und infizierten Dateien schnell zu finden, bevor sie geeignete Korrekturmaßnahmen einleiten. Dazu gehört auch, eine verseuchte Datei nicht nur in einem, sondern in allen Workloads zu finden und zu löschen, für deren schnelle und gezielte Bereinigung.

Neben der beschleunigten Reaktion hat die spezielle, sofortige Massenwiederherstellung von Cohesity einen weiteren Vorteil der darin besteht, dass eine beliebige Anzahl von Virtuellen Maschinen (VMs) auf einen beliebigen früheren Zeitpunkt zurückgesetzt wird, um einen reibungslosen Geschäftsbetrieb zu gewährleisten. Cohesity kann einzelne VMs, Dateien auf Quell-VMs und einzelne Anwendungsobjekte wiederherstellen.Um die Wiederherstellung von Ransomware

Ransomware-Angriffe abwehren

Durch den umfassenden Ansatz Ransomware-Angriffe zu verhindern, zu erkennen und darauf zu reagieren, vermeiden Nutzer jeglichen Datenverlust und können deshalb eine Ransomware-Zahlung jederzeit verweigern. Bei einer Attacke, einer Katastrophe oder einem Ransomware-Angriff, ist Cohesity die einzige Lösung, die die sofortige Wiederherstellung von Hunderten von VMs unterstützt, um Unternehmen wieder online zu bringen. Durchgehend geschützte Backups sind lokal oder in der Cloud verfügbar, damit Unternehmen den Geschäftsbetrieb schnell wiederaufnehmen kann.

Thomas Boele

IT-SICHERHEIT FÜR IOT-PLATTFORMEN

DATEN UND ANLAGEN OPTIMAL SCHÜTZEN.

Endian Connect: Sicherer und hoch skalierbarer Zugriff auf Endpunkte.

IoT-Plattformen sind der Dreh- und Angelpunkt für digitale Geschäftsmodelle: Sie bieten die notwendige Infrastruktur, um Daten von allen angebundenen Geräten und Prozessen zu sammeln und zu analysieren. In der Industrie gibt es mittlerweile eine ganze Reihe von Erfolgsbeispielen: So können Unternehmen beispielsweise durch die Analyse von Maschinendaten und Predictive Maintenance ihre Effizienz erheblich steigern. Doch trotz all der Chancen haben viele Unternehmen Vorbehalte gegen den Einsatz von IoT-Plattformen: Bei einer Befragung des Branchenverbands Bitkom aus dem Jahr 2018, sprachen sich 18,9 Prozent der Unternehmen klar gegen eine Nutzung von IoT-Plattformen aus. Bedenken hinsichtlich der Datensicherheit und Datenintegrität rangieren bei den Gründen dafür mit 57,7 Prozent an vorderster Stelle.

1. IoT-Security-Gateways

Die Verbindung von Maschinen und Anlagen mit einer übergeordneten Plattform erfolgt idealerweise über ein IoT-Gateway. Diese Gateways sind in der Lage, unterschiedliche Industrie-Protokolle auszulesen und sie anschließend in ein einheitliches Kommunikations-Protokoll für die Übertragung an die IoT-Plattform zu übersetzen. Innovative Gateways sind mit einem Unified Threat Management (UTM) ausgestattet. Gateways wie das Endian 4i Edge 515 enthalten mehrere Sicherheitsfunktionen wie beispielsweise Anti-Virus, Intrusion Prevention System (IPS), Intrusion Detection System (IDS) und eine Firewall. Dadurch sind Maschinen und Anlagen vor Angriffen optimal geschützt. Ein Gateway sollte dabei die Auswahlmöglichkeiten bei IoT-Plattformen nicht einschränken.

2. Netzwerksegmentierung

Die ständig wachsende Zahl von vernetzten Endpunkten bietet Hackern eine immer breitere Angriffsfläche. Schadsoftware wird deshalb zunehmend so konzipiert, dass sie sich schnell von einem System auf ein anderes ausbreiten kann. Hinzu kommt, dass Unternehmen ihre IT-Sicherheitsmaßnahmen meist gegen Bedrohungen von außen konzipieren. Hat ein Angreifer diese Hürde genommen, kann er sich rasch innerhalb eines Netzwerks ausbreiten. Netzwerksegmentierung bietet hier eine Möglichkeit, Cyberangriffe abzuschwächen und zu verlangsamen. Dafür werden Zonen mit vergleichbarem Schutzbedarf definiert und über IoT-Security Gateways voneinander abgegrenzt.

3. Verschlüsselung

Jeder Datenaustausch sollte über VPN-Verschlüsselung erfolgen. Damit lässt sich sicherstellen, dass Daten während der Übertragung nicht entwendet oder manipuliert werden. Auch hier ist es vorteilhaft, Gateways vor die Infrastruktur zu schalten: Der laufende Betrieb wird damit nicht unterbrochen und die Verschlüsselung kann entsprechend schnell implementiert werden.

NUR EINE INTUITIV ZU NUTZENDE IOT-PLATTFORM WIRD DIE AKZEPTANZ DER MITARBEITER FINDEN.

Raphael Vallazza, CEO, Endian
www.endian.com

4. Mandantenfähigkeit

Eine mandantenfähige IoT-Plattform kann Daten innerhalb der Datenbank logisch voneinander abtrennen und verwalten. In der Praxis wird es damit möglich, die Datensicherheit zu erhöhen. Anwender erhalten nur Einblick in die Daten, die für die Erfüllung ihrer Aufgaben von Bedeutung sind. Wenn beispielsweise ein Maschinenhersteller für Wartungszwecke Zugriff auf eine Maschine beim Kunden hat, muss er nicht gleichzeitig die genauen Nutzungsdaten einsehen können.

5. Berechtigungsmanagement

Wird eine IoT-Plattform auch für den Remotezugriff und die Fernwartung genutzt, so ist ein granulares Berechtigungsmanagement unverzichtbar, um die Sicherheit von Maschinen und Anlagen zu gewährleisten. Einzelne Nutzer oder Nutzergruppen erhalten nur Zugriff auf die Funktionen, für die sie zuvor eine Berechtigung erhalten haben. Verlässt ein Anwender das Unternehmen oder wechselt er die Abteilung, können seine Berechtigungen angepasst oder gelöscht werden. Über die Protokollierung aller Zugriffe ist jederzeit nachvollziehbar, wer wann auf einer Maschine eingeloggt war und welche Maßnahmen er dort durchgeführt hat.

6. Skalierbarkeit und Open Source

Die sehr kurzen Innovationszyklen in der IT lassen keine genauen Prognosen darüber zu, welche Neuigkeiten der Markt in den nächsten fünf bis zehn Jahren hervorbringen wird. Eine IoT-Plattform muss daher so ausgestaltet sein, dass sie auch zukünftige technologische Entwicklungen reibungslos integrieren kann. Open Source basierende Plattformen bieten für die unvorhersehbaren Zukunftsszenarien die notwendige Flexibilität. Architektur- und Quelloffenheit machen sie anpassungsfähig und herstellerunabhängig. Außerdem bieten sie die Möglichkeit für individuelle Erweiterungen.

7. Usability

Erfolgreiche digitale Lösungen und Erfindungen der letzten Jahre zeichnen sich durch eine besonders hohe Anwenderfreundlichkeit aus. Durch den Consumer-Bereich sind Anwender an ansprechende und einfache Benutzeroberflächen gewöhnt.

Deshalb wird auch nur eine intuitiv zu nutzende IoT-Plattform die Akzeptanz der Mitarbeiter finden. Durch eine hohe Anwenderfreundlichkeit lässt sich verhindern, dass einfachere Lösungen um die Plattform herum gebaut werden, die dann wiederum das Sicherheitskonzept aushebeln.

Fazit

Das Vertrauen aller Partner in die zunehmende Vernetzung ist die Voraussetzung für eine erfolgreiche Digitalisierung. Bei der Einführung einer IoT-Plattform sollte deshalb die Funktionalität und die IT-Sicherheit gleichwertig betrachtet werden.

Raphael Vallazza

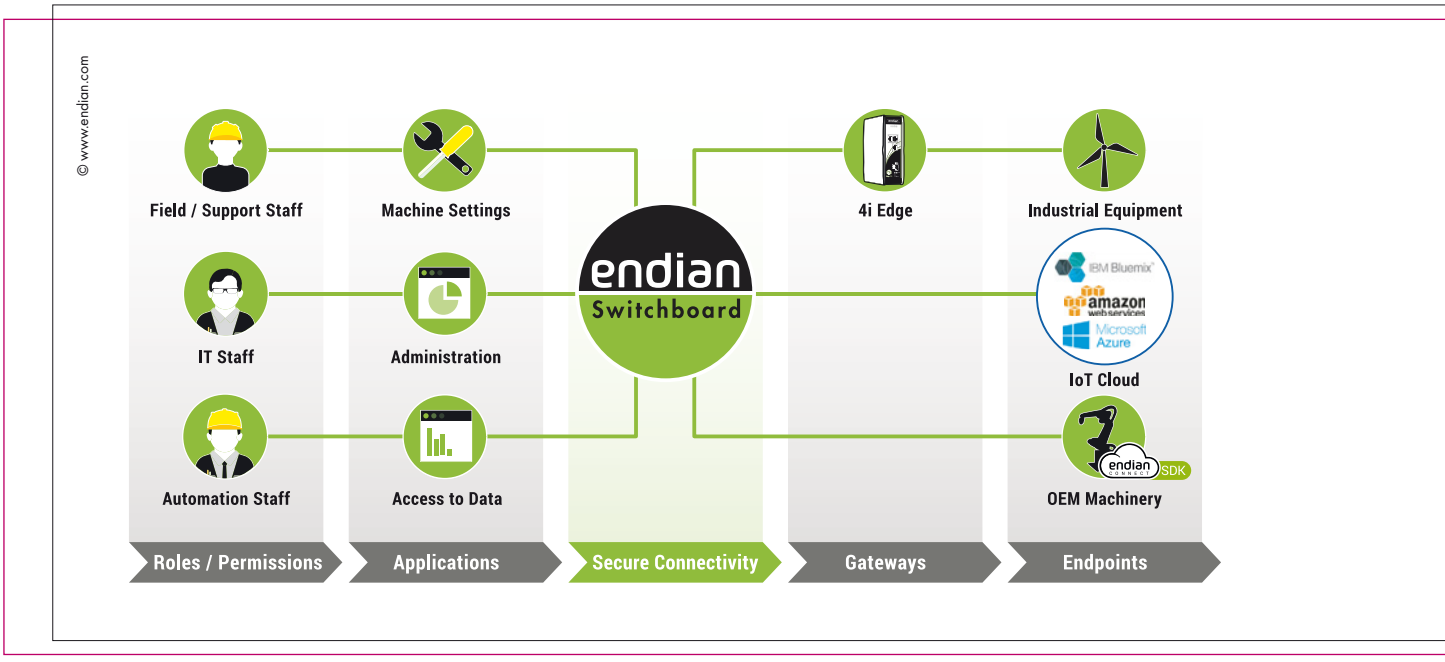


Bild: Sicher und flexibel: Endian Connect erfüllt alle Anforderungen an Industrie 4.0.

IAM CONNECT 2019

Die Brücke zu neuen Geschäftsmodellen

18. bis 20. März 2019
Berlin Marriott Hotel – Potsdamer Platz

www.iamconnect.de

Save the Date!

Eine Veranstaltung von itmanagement & itsecurity