DAS WIRTSCHAFTSMAGAZIN ZUR DIGITALISIERUNG

DIGITALE WELT

ZUKUNFT | EINFACH | ENTDECKEN

Ausgabe 2 ▪ April ▪ Mai ▪ Juni ▪ **2018**

Cyber Security – Von digitalem Datenmissbrauch bis Passwort-Hacks

Digitale Identität

Authentifizierung und Schlüsselmanagement

Use Cases

Strategien für mehr Informationssicherheit

Datenschutz

Sicherheitsempfehlungen für BYOD und Cloud

BLOCKCHAIN

Technik, Features, Anwendungen

Der Nunatak-Gründer über den Unternehmenswandel durch die Digitalisierung

Robert Jacobi

8,50 EUR
9,50 EUR
13,90 CHF

DIGITALE WELT AUSGABE 2 | 2018

18 **HINTER DEN KULISSEN**
AIDA – Kreuzfahrt von morgen

62 **BLOCKCHAIN**
Technik, Features, Use-Cases

Die nächste DIGITALE WELT erscheint am 06.06.2018

Titel: iStock, Oliver Nieder Fotos: AIDA, Shutterstock, iStock, Oliver Nieder

MICHAELA HARLANDER
Dr. Michaela Harlander gründete nach ihrer Forschungstätigkeit in der Physik 1992 das IT-Sicherheitsunternehmen genua gmbh, das sie bis Ende 2016 leitete. Seit 2015 ist sie Vorstand der gemeinnützigen Harlander-Stiftung, die sich u. a. um die Förderung der MINT-Ausbildung bei Kindern und Jugendlichen bemüht. Seit 2017 ist sie zudem als Unternehmensberaterin für Strategie- und Führungskräfteentwicklung tätig.

Cyber Security – Weckruf

Die Sicherheitsprobleme „Spectre“ und „Meltdown“ halten uns in Atem. Noch können die Folgen nur ungefähr abgeschätzt werden, und die Behebung der Probleme könnte Jahre dauern. Der Vorfall ist ein Musterbeispiel dafür, wie Krisenmanagement nicht ablaufen sollte und wie Vertrauen in unsere digitale Zukunft unterminiert wird.

Es dürfte um 2009 herum gewesen sein, als ich das erste Mal mit konkreten Überlegungen konfrontiert wurde, man könne die Integrität eines Computersystems durch einen Angriff auf die Hardware aushebeln. Das Szenario damals ging von einer Manipulation des Prozessors selbst während der Produktion aus – ein äußerst aufwändiger, aber praktisch nicht zu entdeckender Angriffsvektor. Mir war klar: Würde das jemals Realität, wären die Folgen dramatisch, denn alle Systeme mit den betroffenen Prozessoren müssten aktualisiert werden.

Die jetzt unter den Namen „Meltdown“ und „Spectre“ bekannt gewordenen Sicherheitslücken sind nicht ganz so tief in den Prozessoren verortet. Sie stecken nicht in den Halbleitern selbst, sondern in der CPU-Programmierung. Code, der für die Beschleunigung der CPU-Leistung gedacht ist, kann durch geschickte Angriffe dazu genutzt werden, Speicherbereiche auszulesen, auf die man eigentlich keinen Zugriff haben sollte. So könnten dann Passwörter oder andere sensible Informationen abgegriffen werden [1].

Mehrere voneinander unabhängige Forscherteams haben die Probleme gefunden und Mitte 2017 den Herstellern gemeldet. Erst im Januar 2018 wurde die Öffentlichkeit informiert, um so den Herstellern Zeit zu geben, Patches zu entwickeln und Abläufe zu planen.

Betroffen sind dabei die meisten neueren Intel-CPUs, AMD-Prozessoren sowie einige Prozessoren anderer Architekturen, z. B. ARM. Updates werden für die auf diesen Prozessoren aufbauenden Betriebssysteme notwendig, aber auch für Firmware, diverse Treiber, Browser und andere Anwendungen. Derart umfassend war zuvor kaum eine Sicherheitslücke.

Das Grundproblem der Angriffe ist, dass sie eben auf Code zur Prozessorbeschleunigung beruhen. Würde man diesen Code einfach vollständig abschalten, hätte dies eine deutliche Absenkung der Rechengeschwindigkeit zur Folge. Je nach Einsatzgebiet eines Rechnersystems könnte dieses damit seinen Zweck nur noch eingeschränkt oder vielleicht auch gar nicht mehr erfüllen. Die heute verfügbaren Patches versuchen daher, die Probleme zu umgehen. Entsprechend gering sind die Leistungseinbußen [1].

Doch leider erweist sich die Fehlerbehebung dieser Lücken als Desaster – zumindest kommunikativ.

Am 23. Januar warnte Intel davor, bestimmte Updates zu nutzen, da diese zu vermehrten Neustarts und unberechenbarem Verhalten der betroffenen Systeme führen könnten. Ganz offensichtlich waren die Updates nicht umfassend genug getestet worden, sodass diese Probleme nicht zuvor aufgefallen waren. Die Meldung sorgte für viel Aufsehen, vor allem aber für große Verwirrung. Anwender spielen in der Regel nicht die Updates von Intel ein, sondern z. B. die von Microsoft, Apple oder ihrer Linux-Distribution. Ihr Anbieter verarbeitet dann die Intel-Updates entsprechend. Der Linux-Distributor RedHat stellte beispielsweise ein Update zur Verfügung, das den problematischen Intel-Code wieder beseitigte.

Doch diese Feinheiten sind nicht jedem Anwender klar. Immer wieder war zu hören und zu lesen, dass Anwender nach der Intel-Information über das problematische Update alle automatischen Update-Funktionen stoppten – die schlechteste aller Lösungen.

Anwender älterer Geräte oder Betriebssystemversionen fühlen sich ohnehin schlecht über ihre Handlungsmöglichkeiten informiert, denn für ihre Systeme gibt es häufig überhaupt keine Updates. Doch nicht jeder Anwender hat die Möglichkeit, mal schnell Hardware oder Betriebssystem zu wechseln, um dann die notwendigen Updates einzuspielen. Durch die weite Verbreitung der betroffenen Prozessoren wird uns die Abwehr von Spectre und Meltdown noch Jahre beschäftigen.

Darüber hinaus reicht es nicht immer aus, einfach einen Patch einzuspielen. Für einen der Angriffe – die zweite Variante von Spectre – ist es (Stand Ende Januar) zusätzlich notwendig, neben dem Betriebssystemupgrade ein Upgrade des BIOS durchzuführen [2]. Microsoft weist darauf in einem Artikel zu den Sicherheitsproblemen auch hin [3]. Hand aufs Herz: Hätten Sie gewusst, dass es nicht reicht, das Update des Betriebssystems auszuführen? Und falls Sie von einem Systemadministrator betreut werden: Wurde bei Ihren PCs wegen Spectre das BIOS aktualisiert?

Zudem ist es nicht immer einfach, für alle Anwender verständliche Informationen zu den schwerwiegenden Sicherheitslücken zu finden. Auf der Website von Intel werden Sie auf die Intel-Partner verwiesen. Nur hilft Ihnen das nicht weiter, wenn sie gar nicht wissen, bei welchen Partnern man nachsehen muss – reichen die Hersteller der Betriebssysteme? Muss jedes einzelne Programm aktualisiert werden? Offenbar schaffen es nur einschlägige Medien und Behörden, hier für Klarheit und Überblick zu sorgen [4, 5].

Natürlich sind sofort die Trittbrettfahrer zur Stelle. Da werden mit vorgeblichen Sicherheits-Updates Schadprogramme verteilt oder Benutzer mit gefälschten Mails, die angeblich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) kommen, auf Phishing-Seiten gelockt.

Und so bleiben auf Seite der Anwender oft nur Ratlosigkeit und Unsicherheit, wo solides Krisenmanagement und strukturierte Kommunikation Handlungssicherheit und Vertrauen hätten schaffen können.

Wie groß die Unsicherheit wirklich ist, wurde mir klar, als ich in diversen Diskussionen gefragt wurde, ob man nun IT-Investitionen zurückstellen sollte, bis die Lage rund um Spectre und Meltdown geklärt sei – was immerhin Monate dauern könnte, wenn nicht länger. In diversen Plattformen wird das Konzept von Clouds infrage gestellt. Vollends zur Farce wird das Ganze, wenn Nutzer – durchaus berechtigt – Angst davor haben, Analysetools zu installieren, weil sie damit statt Aufklärung zu erhalten Schadcode einschleusen könnten. Über allem thront schlussendlich die ultimative Weltuntergangsstimmung, die wahlweise in der Forderung „alle weg vom Netz“ oder „Schluss mit der Digitalisierung“ gipfelt. Was für ein Alptraum!

Während wir noch auf eine übersichtliche Darstellung der Handlungsoptionen und vor allem auch auf eine Strategie für die Aktualisierung all jener Prozessoren warten, die nicht von den bislang erhältlichen Updates erreicht werden, bietet es sich an, einige erste Lehren aus dem Vorfall zu ziehen.

An erster Stelle steht für mich die Erkenntnis: Sicherheit bekommen wir nur, wenn wir von vorneherein, von Grund auf, unsere Produkte auf Sicherheit hin konzipieren. Sie muss bereits Teil des Grunddesigns sein. Wenn wir Sicherheit weiterhin nur als das notwendige, aber lästige Anhängsel betrachten, das es mehr oder weniger rechtzeitig nachzurüsten gilt, nehmen wir die Nachfolger von Meltdown und Spectre billigend in Kauf.

Sicherheit ist aber nicht nur eine technische Frage, sondern auch eine Frage der Organisation. In den Unternehmen müssen Notfallpläne bereitliegen, die bei Bekanntwerden schwerwiegender Sicherheitslücken einfach aktiviert werden können.

Die großen Hersteller verfügen mit Sicherheit bereits über Notfallpläne, doch scheint mir die Kommunikation zu den Anwendern eine viel zu geringe Rolle zu spielen, ebenso wie ein Notfallszenario für die vielen Anwender älterer Systeme. Dass man durch Abkündigung der Systeme juristisch auf sicherem Boden steht, wenn man keine Patches anbietet, verkennt, dass diese Systeme häufig noch im Einsatz sind und reale Probleme verursachen. Hier braucht es Lösungen, die jenseits juristischer Herangehensweisen die praktischen Probleme lösen können.

Die nächste große Sicherheitslücke wird kommen. Das kommunikative Chaos, das wir jetzt erleben, unterminiert das Vertrauen in digitale Technik mindestens genauso wie die eigentliche Sicherheitslücke und darf nicht toleriert werden.

Es ist an der Zeit, endlich aufzuwachen.

Literatur:

[1] Christof Windeck, Die Riesenlücken – Überblick, c't 3/2018.

[2] https://www.administrator.de/wissen/meltdown-spectre-machen-361578.html

[3] https://support.microsoft.com/de-de/help/4073229/windows-protect-device-against-chip-related-security-vulnerability

[4] Zum Beispiel: Die Riesenlücken, Artikelserie in der c't 3/2018

[5] BSI für Bürger: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Meltdown_Spectre_Sicherheitsluecke_10012018.html

DIGITALE WELT News & Trends

Highspeed-Mobilfunknetz 5G kommt in 2018

Die Mobilfunkbranche arbeitet eifrig an dem weltweiten Einstieg in das neue 5G-Highspeed-Netz. Für die Mobilfunk-Generation 5G wird ein weltweit einheitlicher Standard angestrebt, wie auf der Konferenz 5G Summit im September 2017 in Dresden diskutiert wurde. Vorreiter in Sachen 5G sind die USA. Die Mobilfunkriesen AT&T und Verizon wollen noch in 2018 diverse US-Städte mit ihren 5G-Mobilfunknetzen ausstatten. Der neue Funkstandard soll bei der Datenübertragung mit sehr geringen Latenzen und effizienterer Ausnutzung des Funkspektrums punkten. Pro Sekunde sollen mehrere Gigabit übertragen werden können.

Dogecoin: Bitcoin-Parodie ist zwei Milliarden US-Dollar wert

Die Programmierer Billy Markus und Jackson Palmer entwickelten in 2013 die Spaßwährung Dogecoin als Reaktion auf den Hype um die Kryptowährungen. Die auf Litecoin basierende Währung mit Hundekopf-Design wurde für scherzhafte Fundraising-Aktionen eingesetzt. Obwohl die echte und nutzbare Kryptowährung ab 2014 nicht mehr weiterentwickelt wurde, wird sie mittlerweile mit einem Umtauschkurs von 0,018 US-Dollar gehandelt. Bei rund 112 Milliarden im Umlauf befindlichen Dogecoins ergibt das einen Wert von rund zwei Milliarden US-Dollar.

Amazons Sprachassistentin Alexa soll zukünftig aus Backöfen sprechen

Alexa ist den meisten als Amazons smarter Assistent in Form der bekannten Echo-Boxen bekannt. Doch mit der Öffnung für Drittanbieter seit Mitte 2015 ist das Interesse vieler Hersteller an Alexa stetig gewachsen. So gibt es heute bereits rund 50 verschiedene Alexa-Geräte von Drittanbietern auf dem Markt: General Electric baute den Sprachassistenten in eine Lampe ein, Huawei integrierte ihn ins Handy und LG brachte einen smarten Kühlschrank mit integriertem Alexa auf den Markt. Damit nicht genug: Mit der Veröffentlichung des Alexa Mobile Accessory Kit kann Alexa nun auch in Kopfhörer, Smartwatches, Fitnessarmbänder, Mikrowellen und Backöfen integriert werden. Gerätehersteller wie Bose, Beyerdynamic, Whirlpool, Samsung und LG arbeiten derzeit bereits an der entsprechenden Produktintegration.

Bosch setzt auf das Geschäft mit der smarten Stadt

Immer mehr Menschen zieht es in die Stadt: Bis 2050 werden laut den Vereinten Nationen rund zwei Drittel der Weltbevölkerung in urbanen Zentren leben – 2014 war es noch etwa die Hälfte. Mit der fortschreitenden Urbanisierung steigen auch die Herausforderungen an das städtische Leben. Entsprechend hoch ist schon heute der Bedarf an intelligenten Lösungen. Bosch arbeitet daran, Städte und Gemeinden für die Zukunft zu rüsten und ist aktuell bereits an 14 umfassenden Smart-City-Projekten weltweit beteiligt. Getüftelt wird an intelligenten Mobilitätslösungen, besserer Luft, mehr Komfort und höherer Sicherheit sowie an viele neuen Dienstleistungen; kurz: deutlich mehr Lebensqualität in Stadt und Nachbarschaft ist das Ziel.

Smartes Betriebssystem in der neuen A-Klasse

Auf der diesjährigen Consumer Electronics Show in Las Vegas hat Mercedes-Benz ein neues Betriebssystem für seine Fahrzeuge vorgestellt. Das neue 3-D-Betriebssystem mit dem Namen Mercedes-Benz User Experience (MBUX) überzeugt mit 3-D-Grafik, Sprachsteuerung und künstlicher Intelligenz: Durch MBUX wird das gesamte Auto zur Bedienoberfläche. Die Features von MBUX sollen vor allem die junge Generation begeistern. Das System wird daher erstmals im Mai 2018 in der neuen A-Klasse auf den Markt kommen.

Fotos: Bosch, Daimler, pixabay

KÜNSTLICHE INTELLIGENZ REVOLUTIONIERT DAS AUTO

Aktuell existiert nur ein Prototyp des neuen Volkswagens I.D. BUZZ. Doch Volkswagen arbeitet bereits an der Serienproduktion für den in 2022 geplanten Markteintritt des elektrischen VW-Busses. In der Neuauflage des VW-Klassikers wird KI-Technologie des strategischen Partners NVIDIA zum Einsatz kommen. Komplett autonomes Fahren soll mit dem VW Buzz zum Marktstart noch nicht möglich sein. Stattdessen liegen die Funktionen der KI-Unterstützung vorerst eher im Bereich des intelligenten Co-Piloten.

Dank der KI-Plattform Drive IX von NVIDIA sind Funktionen wie die Gesichtserkennung zum Entriegeln des Fahrzeugs von außen, ein Warnsignal für Fahrräder, Gestenerkennung für Bedienelemente, natürliche Spracherkennung für eine einwandfreie Sprachsteuerung und Blickverfolgung für Warnungen bei Ablenkung des Fahrers möglich. Weiterhin soll das smarte System die Aufmerksamkeit des Fahrers kontrollieren und bei erkannten Ablenkungen dafür sorgen, dass er sich wieder auf den Straßenverkehr konzentriert. Die NVIDIA-Drive-AR-Plattform ermöglicht zudem den Einsatz von Augmented-Reality-Funktionen im Cockpit und erlaubt so Informationen über die Beschaffenheit der Straße oder interessante Wegpunkte in die reale Welt zu projizieren.

Anna-Sophie Rauschenbach

Der I.D. BUZZ ist Bestandteil der I.D. Familie, mit der Volkswagen im Jahr 2020 seine Elektro-Offensive starten und das autonome Fahren schrittweise einführen will. Ab 2025 soll dann nach und nach komplett autonomes Fahren möglich sein.

Fotos: Volkswagen

Very Digital Person: ROBERT JACOBI

Der Firmenname „Nunatak“ bedeutet in einer Inuit-Sprache Wegweiser. Denn die Gruppe will für ihre Kunden ein Wegweiser in einem digitalen Umfeld sein.

Die Medienbranche war eine der ersten Industrien, die die Auswirkungen der Digitalisierung zu spüren bekam. Selbst aus diesem Feld kommend, war Robert Jacobi klar, dass die Digitalisierung hier nicht enden und in naher Zukunft andere Branchen treffen würde. Diese Erkenntnis führte zur Gründung der Nunatak Group: ein Consultant-Unternehmen der „digitalen Enthusiasten“, welches seine Kunden bei der digitalen Transformation unterstützt. Im Interview mit dem DIGITALE-WELT-Magazin verrät Robert Jacobi die Geheimnisse seines Erfolgs.

Was ist wichtig, um im Zeitalter der Digitalisierung ein Unternehmen langfristig zum Erfolg zu führen?
Ich muss meine Organisation so aufbauen und meine Mitarbeiter so incentivieren, dass Veränderung, Ausprobieren und Kreativität belohnt werden – natürlich ohne dass das bestehende Erfolgs- und Kerngeschäfts dadurch zu sehr aus dem Blick gerät.

Viele Firmen wissen gar nicht, was sie digitalisieren wollen. Sie wissen nur, dass sie jetzt auch etwas tun müssen. Was wäre Ihr Rat? Wie fängt man am besten mit der digitalen Transformation an?
Das hängt stark von der Branche ab. Digitalisierung ist für mich nicht ein Segment einer Unternehmensstrategie. Vielmehr müssen alle Teile des Unternehmens digitalisiert werden und das hat auch schon begonnen: nicht nur bei Marketing und Vertrieb, sondern auch bei Finanzen und Controlling, Personal- oder Rechtsabteilung. Auch diese müssen sich mit digitalen Tools und Techniken auseinandersetzen. Wenn ich Digitalisierung nur als ein To-Do anrechne oder nur einer Abteilung zuweise, dann unterlaufe ich die Relevanz, die das Ganze haben muss – auch wenn die Koordination an einer Stelle vorübergehend sinnvoll sein kann. Für einen Unternehmer in der Digitalisierung ist es aber wie für einen Landwirt, für den sich das Klima ändert. Die Frage, die aufkommt, ist grundsätzlich: Kann ich noch die Früchte anbauen, die ich immer angebaut habe? Sind die Instrumente und Werkzeuge von früher noch die richtigen? Ist die einzige Gemeinsamkeit zwischen heute und früher, dass mir dieses Stück Land gehört, welches ich bewirtschaften möchte? Denn die Bedürfnisse der Nutzer bzw. der Abnehmer, die ja ebenso in dieser Welt leben, verändern sich ja genauso. Dann muss der Landwirt eben etwas anderes anbauen – man braucht also ein neues Produkt.

Die Nunatak Group ist beratend tätig, hilft aber teils auch bei der Umsetzung. Dementsprechend haben Sie Einsicht in die Firmenstrukturen ganz unterschiedlicher Unternehmen. Was sind Ihrer Meinung nach die größten Hürden, auf welche die meisten Unternehmen in der digitalen Transformation stoßen?
Wenn ich die digitale Strategie formuliere, muss ich die Umsetzung immer schon mitdenken und auch frühzeitig Ressourcen dafür einplanen. Wenn ich erst einen langen strategischen Prozess habe, welcher Monate oder gar Jahre dauert und welcher dann erst implementiert wird, hat sich die Welt fünfmal gedreht und ich kann von vorne anfangen. Das gilt erst recht vor dem Hintergrund, dass für viele Umsetzungsthemen Ressourcen schwer zu bekommen sind. Dafür ist auch wichtig, dass ich die Strategie so schnell wie möglich transparent mache und die Mitarbeiter auf die Veränderung vorbereite und trainiere. Es ist falsch zu glauben, dass Digitalisierung nur durch High-end-Silicon-Valley-Personal bewältigt werden kann. Entscheidend ist, den bestehenden Kern mitzunehmen. Führungskräfte müssen die Leute mitnehmen und brauchen, genauso wie ihre Mitarbeiter, die Motivation, Neues zu lernen. Aber vor allem muss man allen Mut für Experimente beibringen und in sichtbaren Ergebnissen zu denken, anstatt in internen Strukturen, Zahlen und Firmenpolitik. Und wenn mal etwas nicht gleich funktioniert, hat man zumindest etwas gelernt.

„Digitalisierung ist für mich nicht ein Segment einer Unternehmensstrategie. Vielmehr müssen alle Teile des Unternehmens digitalisiert werden.“

Wie würden Sie den Umbruch der Medienindustrie im Zeitalter der Digitalisierung beschreiben?
Neben IT und Telekommunikation war die Medienindustrie sicher mit als Erste von der Digitalisierung betroffen. Durch die digitale Vernetzung hat sie das Monopol über ihre Verbreitungswege verloren. Es hat länger gedauert, bis das von der Branche realisiert wurde und die schmerzhaften Folgen verdaut waren, doch nach einer längeren Durststrecke kommt die Industrie jetzt langsam aus dem Tal der Tränen heraus. Denn es wurde erkannt, dass eine gewisse Zahlungsbereitschaft besteht, wenn ich hochwertige Inhalte produziere und verkaufe. Spotify und Netflix gehören ja de facto zur Medienindustrie. Die haben genau das geschafft: nämlich Bezahlmodelle. Im einen Fall mit Musik, im anderen Fall mit Video. Genau diese Logik des Abos funktioniert im digitalen Bereich also auch. Doch dafür brauche ich einerseits ständige Verfügbarkeit, die dem Nutzer erlaubt, immer und überall darauf zuzugreifen, und andererseits Premiuminhalte. Natürlich ist dieses Modell bei exklusivem Entertainment einfacher als im Informationssektor. Doch auch hier ist durch die Fake-News-Debatte eine Hinwendung zu qualitativen Inhalten zu bemerken.

Was halten Sie von Content Marketing, das ja durch digitale Kanäle boomt und für Medienhäuser eventuell eine Konkurrenz darstellt?
Ja, Konkurrenz, aber durchaus auch Geschäft in der Beratung und Umsetzung. Relevante Inhalte sind heute aus keiner Marketingabteilung – egal welcher Branche – mehr wegzudenken. Ich kann nicht mehr einfach mein Produkt hinstellen und darauf warten, dass die Leute es kaufen. Man muss immer eine Geschichte mitliefern. Das Thema Inhalt und dessen digitale Verbreitung sind einfach in jeder Branche wichtig geworden. Deshalb ist es auch so essenziell, dass große Unternehmen hier Kompetenz aufbauen. Jedes Unternehmen sollte sich zu einem kleinen Medienhaus entwickeln. Ein gutes Beispiel hierfür ist Red Bull. Red Bull produziert das Getränk gar nicht selbst. Diese Firma ist im Prinzip nur ein riesiges Medienunternehmen. Vor allem wenn ich Premium-Produkte anbiete, ist die Geschichte dahinter so wichtig: Die Marke muss aufgeladen sein. Ich zahle mehr, weil ich ein Lebensgefühl mitkaufe. Red Bull hat hierbei digitale Kanäle gut genutzt. Der Baumgartner-Sprung lief natürlich auch über klassisches TV, aber gerade für speziellere, jüngere Zielgruppen ist die digitale Reichweite entscheidend. Es geht also auch immer um die Frage: Wie kann ich digitale Tools nutzen, um mit weniger Geld größere Reichweite zu erzielen?

Sie waren früher auch als Journalist tätig. In welcher Weise hat Sie Ihre frühere Tätigkeit dazu bewogen, die Nunatak-Group zu gründen?
Nach dem Platzen der Dotcom-Blase und der Rezession im Jahr 2001 habe ich gemerkt, dass das klassische Mediengeschäft unter Druck gerät und dass neue Plattformen entstehen, die die Bedürfnisse von Anzeigenkunden und Lesern auf andere Weise befriedigen. Das hat in den Medienhäusern erst zu einer Krise und dann zu einem Umdenken geführt. Deshalb habe ich begonnen, mich intensiv mit der Digitalisierung zu beschäftigen. Ich habe gemerkt, dass diese Veränderung im Medienbereich nicht Halt machen würde, nur war eben hier der Veränderungsdruck durch die Digitalisierung früher da. Als Journalist habe ich das natürlich hautnah miterlebt. So waren wir dann als Firma bereit, als anderen Industrien klar wurde, dass sie sich nun auch mit diesem Thema auseinandersetzen müssen.

Aktuell unterstützten Sie vom kleinen Betrieb bis zum DAX-Konzern die Unternehmen bei der digitalen Transformation. Was unterscheidet Sie von den vielen anderen Anbietern. Was ist das Geheimnis Ihres Erfolgs?
Es ist die authentische Digitalkompetenz. Wir haben unternehmerische Digitalerfahrung und unsere Mitarbeiter haben in Start-ups, im Venture-Capital-Bereich oder in Digitalabteilungen gearbeitet. Wir haben uns Digitalisierung nicht angelesen, sondern live mitgestaltet. Das haben wir in der Medienindustrie früh getan und das machen wir jetzt in anderen Branchen. Bei uns steht die Machbarkeit viel eher im Vordergrund als bei anderen Anbietern. Wir helfen unseren Kunden dabei, die Bedürfnisse ihrer Zielgruppen besser zu verstehen und sich danach auszurichten. Jeder muss für sich eine branchen- und produktabhängige Antwort auf die Digitalisierung finden: Für jeden ist diese anders. Standardansätze helfen da nicht weiter.

Auf Ihrer Website bezeichnen Sie Ihre Mitarbeiter als digitale Enthusiasten. Welche Kernkompetenzen werden in den nächsten zehn Jahren generell und in jedem Arbeitsfeld unabdingbar werden?
Das kommt auf die Ebene an. Für Führungskräfte und Entscheidungsträger ist es wichtig, Know-how aufzubauen und sich möglichst auch ein gewisses Technikverständnis anzueignen. Eine motivierende und aktivierende Grundhaltung ist essenziell, anstatt durch Kontrollen und Vorgaben zum Erfolg zu kommen. Lernwille und Neugier sind auf allen Ebenen entscheidend.

Wieso heißt Ihr Unternehmen „Nunatak“? Hat der Name

etwas mit Ihrer digitalen Vision zu tun?
Ich war in Alaska, dort steht der Begriff für bestimmte Bergformationen. In einer Inuit-Sprache bedeutet „Nunatak“ Wegweiser und wir sehen uns als Wegweiser für unsere Kunden in einem digitalen Umfeld, einem geschäftlichen Klimawandel, der substanziell ist.

Wie viel ist Nunatak aktuell wert?
Der Wert von Beratungen und Agenturen lässt sich schwer bemessen, da wir projektorientiert arbeiten und nicht mit einem festen Produkt. Im Tagesgeschäft spielt die Kategorie Unternehmenswert gar keine Rolle.

„Die Wirtschaft in der Digitalisierung ist wie die Landwirtschaft unter neuen Klimabedingungen.“

Sie bieten Start-ups aus dem Bereich Internet und Telekommunikation Ihre Dienstleistungen zu besonderen Tarifen an. Auch haben Sie in mehre Start-ups investiert bzw. diese auch erfolgreich mitgegründet. Was sind Ihre größten Erfolge? Was war Ihr Beitrag?
Der Hauptfokus liegt natürlich auf Nunatak selbst, wir sind ja auch ein Start-up. Researchgate habe ich anfangs im Bereich Marketing und Kommunikation unterstützt; Harvard-Kommilitonen von mir haben diese Wissenschaftsplattform gegründet. Abgesehen davon habe ich noch eine Bergsport-Plattform aufgebaut und erfolgreich an einen Verlag verkauft. Doch auch über meine Misserfolge bin ich froh, denn gerade im digitalen Bereich lernt man besonders viel aus den Fehlern, die man gemacht hat. Mein letztes Investment ging an eine Art digitale Hausverwaltung namens vermietet.de.

Wieso dieses Engagement? Bedeuten Firmenneugründungen heute etwas anderes als vor 20 Jahren? Wieso sind Start-ups für unsere Wirtschaft wichtig? Welches Potenzial bringen Sie mit, das andere Firmen nicht mitbringen?
Ich glaube, dass es eine Phase gab im Zeitraum zwischen den Siebzigerjahren und den Neunzigerjahren, in welcher unsere Wirtschaft sehr stark von den bestehenden großen Firmen dominiert war. Aber auch Linde oder Siemens waren einmal Start-ups. Warum gab es diese damals? Wegen eines technischen Quantensprungs durch Elektroantriebe und andere Innovationen. Dadurch sind neue Unternehmensstrukturen entstanden. Seit den Neunzigerjahren ist wieder ein Umfeld entstanden, in dem komplett neue Unternehmen bestehen. Wieder durch einen digitalen Quantensprung. Für ein Unternehmen, welches die letzten 30 oder 40 Jahre schon erfolgreich war und jetzt versuchen muss, das Geschäftsmodell anzupassen, ist die aktuelle Situation natürlich anders, als für Firmen, die jetzt neu beginnen und sich von vornherein mit der Digitalisierung beschäftigt haben. Um wieder auf die Landwirtschafts-Analogie zurückzukommen: Der neue Landwirt, der sozusagen gleich im neuen Klima beginnt, hat die Lage wahrscheinlich besser im Griff, weil er von Anfang an das richtige Saatgut und die passenden Werkzeuge hat. Bei Nunatak geht es uns darum, dass unsere Kunden sich rechtzeitig an diese Veränderungen anpassen und nicht erst dann, wenn die Ernte keine Abnehmer mehr findet und verdorrt . Landwirtschaft unter neuen Klimabedingungen ist die Wirtschaft in der Digitalisierung. Es handelt sich um einen Faktor von außen, den ich nicht selbst beherrschen kann, auch wenn ich das gerne möchte. Und wenn ich darauf nicht reagiere, bin ich ein Verlierer dieser Evolution.

Florentina Hofbauer

Foto: Oliver Nieder

Wohlbefinden und Arbeit – wie soll das zusammenpassen?

„Ich brauche keine Mitarbeiter, die sich tiefenentspannt wohlfühlen, ich brauche welche, die was wegschaffen!“, so die Aussage eines Geschäftsführers. *„Dieses ganze Gerede über Corporate Happiness, Feelgood-Manager, Mindfulness-Circles oder Balance mit Wohlbefinden geht mir auf die Nerven. Arbeit ist anstrengend und notwendig für das Überleben. Unter Druck entstehen Diamanten!“* Dieser Geschäftsführer steht mit dieser Meinung nicht alleine da! Es ist Zeit für eine Klärung.

Die Neurobiologie beschreibt Wohlbefinden als einen Stoffwechselzustand im Mittelhirn wie folgt: Stellen Sie sich vor, Sie wachen morgens fröhlich auf und freuen sich auf den Tag, der vor Ihnen liegt. In Gedanken gehen Sie die anstehenden Themen des Tages durch und fühlen sich beschwingt. Sie fühlen sich geborgen in einem Netz von Menschen, die Sie lieben und mögen. Sorgen und Nöte sind nicht greifbar. Sie nehmen diese Stimmung mit in den Tag, lösen knifflige Themen, haben positive Kontakte und kommen abends mit der Gewissheit nach Hause, etwas geschafft zu haben. Das ist Wohlbefinden bzw. psychische Gesundheit nach der Definition der Weltgesundheitsorganisation. Die Erfahrung, leistungsstark und kreativ zu sein, erhöht das Wohlbefinden, ist also ein sich selbst verstärkender Kreis in die richtige Richtung.

Auch wenn es in der Vergangenheit anders funktioniert hat: Das erhöhte Tempo und die stetig steigende Komplexität schaffen ein Arbeitsumfeld, in dem „Zähne zusammenbeißen und weiterarbeiten“ langfristig nicht mehr tragfähig ist.

Denn was erleben wir aktuell bereits? Die Anzahl der überlasteten oder kranken Mitarbeiter nimmt dramatisch zu. Ergebnis einer fundierten Studie ist: 25 % der Erwerbstätigen leiden einmal pro Jahr unter einer psychischen Überlastung oder Störung, davon suchen und erhalten nur 30 % professionelle Hilfe“. [1]

Was also können Unternehmen tun? Tabus rund um die Psyche auflösen und mögliche Einflussfaktoren auf das Wohlbefinden nutzen. Was genau zeigt ein Modell mit drei Säulen:

In der **ersten Säule** ist jede Person aufgefordert, ihre Gesundheitskompetenz aufzubauen und damit die Verantwortung für ihre persönliche Stabilität zu tragen. Viele Menschen sind in diesem Themenbereich sehr effektiv aktiv, bei anderen gibt es Verbesserungspotenziale. Die betriebliche Gesundheitsförderung vonseiten der Unternehmen kann viel Sinnvolles beisteuern. Eine der einfachsten Maßnahmen ist die „aktive Pause“: Der mögliche Stresspegel wird gesenkt, neue Energien werden freigesetzt, und alles das budgetneutral.

In der **zweiten Säule** geht es um die soziale Interaktion zwischen der Führung und dem Team. Dass Führungskräfte großen Einfluss auf das Wohlbefinden und damit auf die bestmögliche Leistung jedes Einzelnen haben, ist nicht wirklich neu. Im Trubel des Alltags verschwinden manche guten Absichten aus dem Fokus. Ein kleines, einfaches Ritual ist aus neurobiologischer Sicht hochwirksam: Teambesprechungen mit der Frage zu beginnen: „Was haben wir seit unserem letzten Treffen erledigt“, anstelle gleich auf die offenen Punkte einzugehen. Denn Kopfarbeiter brauchen für sich selbst ein Häkchen-Ritual. Anders als Handwerker sehen sie nicht, was sie geschafft haben, und das wiederum führt auf Dauer zu Schlafstörungen.

In der **dritten Säule** finden sich die wichtigsten Maßnahmen und Systeme, die eine Organisation braucht, um bestmöglich gerüstet zu sein. Das reicht von einer effektiven Bewertung möglicher Gefährdungen psychischer Belastung bis hin zu einem barrierefreien Zugang zu Expertenberatung.

[1] Wittchen, H-U. et.al. (2011). The size and burden of mental disorders and other disorders of the brain in Europe 2010. European Neuropsychopharmacology 21, 655–679.

Viel Erfolg!

Dr. Petra Bernatzeder,
Diplom-Psychologin, Geschäftsführung
upgrade human resources GmbH

Praxisbeispiele aus Unternehmen finden Sie dazu im hochaktuellen Buch „Erfolgsfaktor Wohlbefinden am Arbeitsplatz“: http://www.springer.com/de/book/9783662552483

Foto: Privat

DIGITALISIERUNG *in Zahlen*

Im Laufe des **Jahres 2017** *stieg der* **Wert eines Bitcoins** *um mehr als* **900 %.**

Das **Bitcoin-Netzwerk** *war damit* **2017** *für den Ausstoß von über* **17.000.000 Tonnen CO_2** *verantwortlich.*

Fast **90 %** *der* **Mitarbeiter in Kliniken** *sind aufgeschlossen gegenüber* **technischen Neuerungen** *an ihrem Arbeitsplatz.*

Dennoch ist **jeder dritte** *Klinikmitarbeiter der Meinung, Digitalisierung trägt aktuell eher zur* **Arbeitsverdichtung** *bei.*

53 % **der Unternehmen** *gaben in einer Studie an,* **der Politik** *fehle das Verständnis für das* **Thema Digitalisierung.**

Über **70 %** *der* **deutschen Kinder** *im KiTa-Alter nutzen das Smartphone ihrer Eltern im Schnitt* **mehr als eine halbe Stunde pro Tag.**

Schätzungen *zufolge gibt es mehr als* **400 Blockchain-Start-ups,** *die sich auf das* Segment der Finanzdienstleistungen *spezialisiert haben.*

40 % **aller Firmen** *geben an, ihre Ausgaben für Innovationen in diesem Jahr zu erhöhen.*

Bis **2025** *könnte* **Automatisierung** *die* **Stellen** *von* **7,7 Millionen** *Beschäftigten in Deutschland ersetzen.*

Eine Studie schätzt, **über 60 %** *der im* **Zuge der Digitalisierung** *ersetzten Stellen sind* **Fachkräfte.**

Eine Studie schätzt, **deutsche Unternehmen** *haben* **2017** *rund* **540 Millionen Euro** *durch eine* **unzureichende Automatisierung** *ihrer digitalen* **Strukturen** *verloren.*

81 % *der deutschen* **Marketingverantwortlichen** *geben an, die* **Budgets** *für mobile* **Werbung 2018** *zu erhöhen.*

Foto: 123RF

AIDA Cruises – Kreuzfahrt von morgen

Hochmoderne Motorentechnik oder eine verbesserte Rumpfgestaltung sind nur einige von vielen Maßnahmen, mit welchen das Unternehmen bewusst versucht, seine Schiffe umweltfreundlicher zu gestalten. Die Fortschritte werden jährlich in dem Nachhaltigkeitsbericht „AIDA cares“ festgehalten.

Von digitaler Schiffstechnik über RFID-Chips in den Uniformen der Crew-Mitglieder hin zum Seamless Check-in: Es ist eine Unternehmensphilosophie bei AIDA Cruises, die neuesten Technologien zu implementieren. Das Motto des Kreuzfahrtunternehmens ist dabei: digitalisieren dort, wo es Sinn macht.

AIDA Cruises beschäftigt Mitarbeiter aus 40 unterschiedlichen Ländern; davon 8.000 an Bord und 1.000 an Land. Auf den zwölf Schiffen begrüßt das Unternehmen im Jahr mehr als eine Million Gäste. Ohne die intensive Zuhilfenahme digitaler Techniken wären all die damit verbundenen Prozesse nicht zu schaffen. Ein Gespräch mit **Steffi Heinicke**, Vice President Guest Service bei AIDA Cruises, gibt Einblick in die digitalen Entwicklungen des Kreuzfahrtunternehmens.

Würden Sie sich als digitale Flotte bezeichnen?

Die Kreuzfahrt an sich ist ein sehr mensch-

Das Markenzeichen der Flotte ist der Kussmund. Denn für das Kreuzfahrtunternehmen steht das Lächeln seiner Gäste an erster Stelle.

Steffi Heinicke
Steffi Heinicke (37) leitet seit Juni 2016 in der Position Vice President Guest Services bei AIDA Cruises die Bereiche Culinary, Entertainment, F&B Services, Guest Services und Product Development. Sie ist Mitglied des Executive Teams von AIDA Cruises. Ihre Karriere beim Kreuzfahrtunternehmen begann Steffi Heinicke 2006 im Personalbereich. Als Director HR Development hatte die diplomierte Betriebswirtin und MBA die Verantwortung für die unternehmensweiten Trainingsaktivitäten, das Talent-Management und die Unternehmenskultur.

Der AIDA-Roboter namens „Pepper“ ist speziell für die jüngeren Gäste ein beliebtes Selfie-Motiv und dient – wie so vieles an Bord – vor allem der Unterhaltung der Passagiere.

Um sich für die Reise zu registrieren, können sich Gäste über das MyAIDA-Portal mit ihren persönlichen Daten online anmelden. Eine Anmeldung mit Papierformularen ist aber noch immer eine Option.

liches Produkt. Aber: Wir sind ein Kreuzfahrtunternehmen, das auf Digitalisierung setzt. Sie beginnt bei der Buchungsstrecke, bei welcher wir mit unseren Gästen digital in Kontakt treten, und erstreckt sich hin bis zur Schiffstechnik. Wir haben als Unternehmen den großen Anspruch, immer neue Technologien auszuprobieren: Technologien, die uns weiterbringen. Wie etwa bei den beiden Schiffen mit den emissionsarmen Flüssigerdgas-Antrieben, welche sich gerade im Bau befinden. Wir treiben also durchaus die Gesamtentwicklung voran. Durch die neuen Schiffe haben wir zudem die Chance, technologisch immer weiter voranzukommen. Bei älteren Schiffen rüsten wir nach. Die Digitalisierung macht bei uns eben nicht Halt.

„Wir sind ein Kreuzfahrtunternehmen, das auf Digitalisierung setzt.“

Ihr erstes Bauchgefühl, wenn Sie an den Begriff Digitalisierung denken: Fluch oder Segen für die Kreuzfahrtbranche?
Die Digitalisierung ist ein Teil des Lebens von mittlerweile fast allen Menschen, mich selbst miteingeschlossen. Somit ist sie auch Teil der ganzen Wertschöpfungskette. Wenn man die Digitalisierung klug einsetzt, kann sie zur Arbeitserleichterung, Lebensqualitätssteigerung und letztendlich auch zu neuen Urlaubserlebnissen führen.

In welchen Business-Bereichen wird für AIDA Cruises sowohl an Land als auch auf See die Digitalisierung am deutlichsten sichtbar?
Grundsätzlich betrifft die Digitalisierung bei uns alle Bereiche: Von der Reservierung über eine virtuelle Suchmaschine über Servicebereiche bis hin zu den Maschinen. Auch sind wir sehr aktiv in den sozialen Netzwerken – überhaupt sind wir online sehr stark: Das MyAIDA-Portal ist dabei unsere wichtigste Plattform. Hier meldet sich der Gast mit seinen persönlichen Daten online an. Für viele unserer Passagiere ist gar nicht mehr der Wunsch da, die Anmeldung via Papier zu schicken. So kann der Gast auf dem MyAIDA-Portal für die Reise individuelle Ausflüge buchen, sodass an Bord bereits alles organisiert ist.

Über welche Vertriebswege kommen heutzutage die meisten Buchungen zu Stande?
Es gibt viele Möglichkeiten, eine AIDA – Reise zu buchen und wir bieten unseren Gästen die verschiedensten Kanäle dafür an. Auch wenn sich die digitalen Buchungen als Vertriebsweg gut entwickeln, gehen Kunden immer noch gern ins Reisebüro; das gibt es natürlich auch noch. Die persönliche Beratung dort schätzen viele unserer Gäste sehr. Beliebt ist es auch, sich vorher online zu informieren, aber die Buchung selbst dann über das Reisebüro abzuwickeln. Daher ist auch das Reisebüro bis heute unser stärkster Vertriebsweg.

Wie wirkt sich die Digitalisierung auf das Kundenerlebnis an Bord aus?
Die Gäste merken die Auswirkungen der Digitalisierung natürlich stark, da der gesamte Prozessablauf der Passagiere davon betroffen ist. Wir haben die Vorgänge so gestaltet, dass es der Gast leicht hat, durch diese Prozesse zu gehen. Das gelingt uns mittlerweile sehr gut, denn was Buchung und Check-in betrifft, haben wir uns in den letzten Jahren enorm weiterentwickelt: Wir haben die Buchungsschritte vereinfacht und sie auch auf mobile Endgeräte ausgerichtet.

Bleiben wir beim digitalen Check-in: Wie gestaltet er sich?
Für das Einchecken an Bord haben wir einen Prozess entwickelt, der dem Gast einen stressfreien Beginn seiner Reise ermöglicht. Daher nennen wir unser Modell auch Seamless Check-in. Dabei brauchen wir nichts weiter als ein Smartphone und einen Hochtisch. Der Check-in-Prozess beginnt damit, dass der Gast sich registrieren lässt, wenn er an Bord kommt: Es werden alle Reisedokumente eingescannt und ein Crew-Mitglied wirft einen Blick auf den Pass. Im Anschluss bekommt der Gast seine Bordkarte ausgehändigt. Diese gleicht dann während der gesamten Reise einem Ausweis an Bord und funktioniert mit RFID-Technologie. Der Prozess der Registrierung dauert nicht länger als eine Minute. Durch das Seamless Check-in haben wir die Wartezeiten extrem reduziert und sind viel schneller als früher. Auf AIDAprima können wir zum Beispiel 1.200 Gäste innerhalb von nur einer Stunde einchecken. In den Bewertungen sind wir dadurch extrem bei den Passagieren gestiegen, weil diese das natürlich angenehm finden; sie bekommen ohne die langen administrativen Angelegenheiten sozusagen zusätzliche Urlaubszeit geschenkt. Ist der Gast dann an Bord, bekommt er eine SMS, wenn seine Kabine frei ist. Diese digitale Experience ist ein echter Mehrwert für den Gast und passt zu unserem Motto: digitalisieren dort, wo es sinnvoll ist, dort, wo es wirklich etwas für den Gast oder die Crew verbessert.

Wie äußert sich die Digitalisierung im Recruiting-Bereich?
2016 haben wir etwa 1.000 Crew-Mitglieder eingestellt. Gerade beim Recruiting sind digitale Technologien unerlässlich. Sie sind auch der einzig mögliche Weg, um so viel Personal im Jahr einstellen und

Das Show-Programm der AIDA-Flotte ist einzigartig: Musical-Einlagen, Artistik-Performance, Mitmach- und Familienshows sowie Rockspektakel wechseln einander ab. Ferner werden an Bord Fernsehsendungen produziert, welche beliebten TV-Formaten nachempfunden sind und die im hauseigenen Fernsehprogramm an Bord gesendet werden.

koordinieren zu können. Wir haben hierfür auch eigens digitale Tools eingerichtet. So gibt es etwa Video-Tools für Bewerbungsgespräche, damit die Recruiter die Bewerber und Bewerberinnen besser kennenlernen können. Jedoch gilt natürlich: Wer seine Bewerbungsunterlagen lieber in Papierform schickt, kann das natürlich auch gerne machen.

In Norwegen wird 2018 das erste autonome Containerschiff in Betrieb genommen. Ist eine solche Entwicklung auch für die Kreuzfahrtbranche vorstellbar?

Ich glaube nicht, dass das vorstellbar ist. Die Crew spielt eine entscheidende Rolle für die Kreuzfahrt, ganz besonders der Kapitän. Daher wird gerade für die Kreuzfahrt der Faktor Mensch nach wie vor im Mittelpunkt stehen. Denn die Crew transportiert das Lächeln: Der Kussmund steht nicht umsonst für AIDA. Unseren Crew-Mitgliedern geht es immer darum, ein ehrliches Lächeln zu transportieren und stets eine gute Atmosphäre aufzubauen.

Wenn man die Digitalisierung klug einsetzt, kann sie zur Arbeitserleichterung, Lebensqualitätssteigerung und letztendlich auch zu neuen Urlaubserlebnissen führen.

Stichwort Robotik: In China gibt es bereits seit einigen Jahren Restaurants, die ausschließlich mit Hilfe von Robotern funktionieren. Ist so etwas auch für die Kreuzfahrtbranche vorstellbar? Beispielsweise auch als Ersatz für das Reinigungspersonal?

Das kommt ganz stark auf den jeweiligen operativen Prozess an. Wir haben momentan noch keine Putz-Roboter im Einsatz, aber wir haben Augen und Ohren offen. Jedoch im Service wären Roboter bestimmt der falsche Weg. Wie gesagt: Roboter und digitale Technologien wären niemals ein Ersatz für unsere Crew, nur ihre Ergänzung.

Dabei haben Sie einen Roboter zur Unterhaltung der Gäste mit an Bord.

Das ist richtig. Wir haben einen kleinen Roboter namens „Pepper“ mit an Bord. Dieser Roboter gibt Informationen und unterhält die Gäste. Speziell die jüngeren Passagiere machen auch gerne Fotos mit Pepper. Daher bauen wir ihn bei Entertainment-Angeboten und Workshops mit ein. So kommen die Passagiere unterhaltsam mit dem Roboter in Berührung. Eine wirklich praktische Funktion – etwa zur Kaffeeausgabe – hat er aber nicht.

Sie haben RFID-Chips für Uniformen und Tischwäsche. Weshalb?

Wäre unsere Wäsche nicht in diesem Ausmaß digitalisiert, wären die derartig vielfältigen Prozesse in der bordeigenen Wäscherei nicht zu schaffen. Denn durch RFID-Chips können wir das Wäschesystem besser kontrollieren. Wir können mit den Chips also Einzelteile tracken: Bei ca. 9.000 Uniformteilen unserer Crew und 9.000 Kostümteilen unserer Bühnenartisten wäre das gar nicht anders möglich. Durch die in die Uniformen integrierten Chips bekommt jedes Crew-Mitglied exakt die von ihm benötigten Kleidungsstücke automatisch ausgegeben.

Dringt die Digitalisierung auch bis in die analogen Gefilde der Küchen vor?

Die Küche schließt oft nicht direkt an die Buffet-Fläche an. Daher ist jede Speise am Buffet mit einem kleinen Kärtchen ausgestattet. Wenn nun ein Gericht ausgeht, kann ein Service-Mitglied das dazuge-

Über das bordeigene WLAN können Gäste kostenlos auf die AIDA-App zugreifen. Mit dieser App können sich die Gäste über das Ausflugsangebot informieren, die Wetterlage checken, den Tisch im gewünschten Restaurant reservieren sowie mit Familienmitgliedern, Freunden oder neuen Reisebekanntschaften an Bord chatten.

Das neueste Schiff ist die AIDAnova und dieses wird im Dezember 2018 in See stechen. Es wird das bisher größte AIDA Schiff werden und das erste der Helios-Klasse. Das ist eine völlig neue Schiffsgeneration. Unter dem Motto „Green Cruising" werden Schiffe der Helios-Klasse zu hundert Prozent mit nachhaltigem Flüssigerdgas betrieben werden können. Geplant ist, dass insgesamt sieben Kreuzfahrtschiffe dieser Art für die Carnival Corporation gebaut werden.

hörige Kärtchen scannen. Die Information wird dann in Echtzeit an die Küche übertragen, welche sogleich Nachschub vorbereiten kann. Natürlich kommen noch viele weitere digitale Technologien im Küchenbereich zum Einsatz.

Wie erfolgt der Internetanschluss für die Gäste?
Wir haben hierfür eine eigene Satelliten-Verbindung auf jedem Schiff. An Bord bieten wir verschiedene Internetpakete an. Beispielsweise das Social-Media-Paket oder auch größere Pakete, etwa für jene Gäste, die mehr Zeit online verbringen wollen. Man kann diese Pakete auch schon vor der Reise buchen. Darüber hinaus kann man sich auch über die App und das Bord-Portal über die Produkte informieren. Außerdem haben wir ein bordeigenes WLAN, über das Gäste kostenlos auf die bordeigene App zugreifen können. Das funktioniert dann wie eine Art Intranet an Bord. Auf der App kann man Wetterinformationen erhalten oder das Ausflugsangebot durchstöbern. Doch man kann auch mit seiner Familie oder seinem Freundeskreis an Bord chatten, Tische reservieren und vieles mehr.

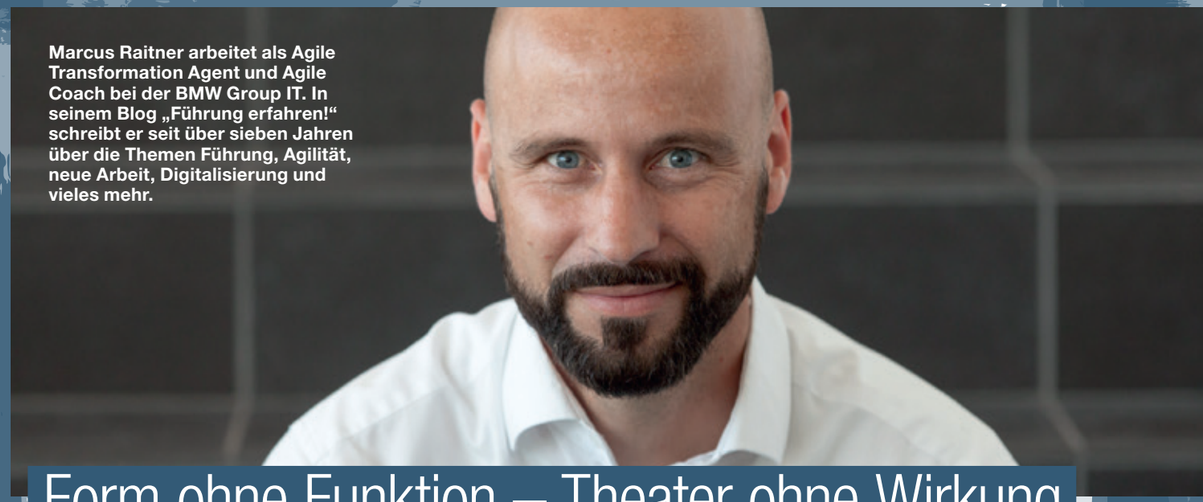
Diese digitale Experience ist ein echter Mehrwert für den Gast und passt zu unserem Motto: digitalisieren dort, wo es sinnvoll ist, dort, wo es wirklich etwas für den Gast oder die Crew verbessert.

Wie modern sind die Studios ausgestattet, die die bordeigenen Sendungen produzieren?
Unsere Studios an Bord sind hochdigital und haben die beste Ausstattung. Denn wir produzieren wirklich alles inhouse: eigene Fernsehshows, Filme für Gäste, Videos für Social-Media-Kanäle und vieles mehr. Wir senden exklusiv für unsere Gäste an Bord. Jede Art von Sendung wird hier produziert: von Gameshows über Comedy bis zu Kochsendungen. Wenn es neue Standards gibt, dann ziehen wir mit, wie beispielsweise bei der Umstellung von SD zu HD. Außerdem arbeiten wir im Videobereich sehr stark mit Drohnen. So können wir Luftaufnahmen machen, die vor ein paar Jahren noch nicht möglich waren. Wir sind also immer am Puls der Zeit. Unsere Expertinnen und Experten sind hierfür eigens auf Medienmessen unterwegs und integrieren dann die neuesten technischen Errungenschaften in unsere Medienprodukte.

Wird es irgendwann eine Technologie geben, die Kreuzfahrtschiffe ersetzt?
Ein Urlaubserlebnis kann nie durch ein digitales Erlebnis ersetzt werden. Ich kann mir nicht vorstellen, dass es eine Technik gibt, die diese Urlaubsform ersetzen kann. Natürlich entwickelt sich der Reisemarkt weiter; so wird es immer einfacher zu reisen. Aber dadurch, dass wir mit unserer Flotte mobil sind und auch Reiserouten ändern können, werden wir diesen Puls der Zeit immer aufgreifen können. Auch in der Zukunft wollen wir neue Technologien integrieren. Wir bleiben immer am Ball und schauen, dass wir uns stets weiterentwickeln.

Interview/Text: Claudia Linnhoff-Popien/ Florentina Hofbauer

Fotos: AIDA



Marcus Raitner arbeitet als Agile Transformation Agent und Agile Coach bei der BMW Group IT. In seinem Blog „Führung erfahren!" schreibt er seit über sieben Jahren über die Themen Führung, Agilität, neue Arbeit, Digitalisierung und vieles mehr.

Form ohne Funktion – Theater ohne Wirkung

Sie müssen jetzt stark sein. Ein paar User-Storys und Daily Stand-ups machen noch lange nicht agil. Es ist sinnlos, Spotify zu kopieren. Die Form, die Rituale und die Praktiken zu imitieren, ohne die Essenz darin und die Logik dahinter zu begreifen, ist wirkungsloser Cargo-Kult. So, jetzt ist es raus.

In seiner Rede auf der Abschlussfeier des California Institute of Technology benutzte der Physiker Richard Feynman 1974 den aus der Anthropologie stammenden Begriff des Cargo-Kults erstmals im übertragenen Sinne. Er bezeichnete damit Pseudowissenschaft, die sinnlos die Formen und Praktiken echter Wissenschaft imitiert: „In der Südsee vollführen die Menschen einen Cargo-Kult. Während des Krieges sahen sie Flugzeuge mit begehrenswerten Gütern landen und jetzt wollen sie, dass das wieder passiert. Also bauen sie Landebahnen, entzünden Leuchtfeuer entlang der Landebahnen, bauen hölzerne Hütten, in denen ein Mann sitzt mit zwei Holzstücken auf dem Kopf wie mit Kopfhörern mit Bambusstäben als Antennen (…) und dann warten sie bis die Flugzeuge landen. Sie machen alles richtig. Die Form ist perfekt. Es sieht genau so aus, wie sie es beobachtet hatten. Aber es funktioniert nicht. Die Flugzeuge landen nicht."

Agile Methoden und insbesondere Scrum haben ein ungeheures Cargo-Kult-Potenzial. Wegen der Einfachheit der agilen Praktiken einerseits, denn schließlich war das agile Manifest als Gegenbewegung zu schwergewichtigen Software-Entwicklungsmodellen entstanden. Andererseits wegen der für hierarchisch-tayloristische Organisationen nicht umsetzbaren und teilweise gar nicht denkbaren dahinter liegenden Prinzipien.

Selbstorganisierte Teams, die autonom volle Verantwortung für ihr Produkt übernehmen und entsprechend auch weitgehende Entscheidungsmacht erhalten? So agil dann doch lieber nicht. Teams, die alle unterschiedlich arbeiten und wo niemand zentral eine einheitliche Arbeitsweise vorgibt? Wo kämen wir da hin! Der Unsicherheit ins Auge sehen und entsprechend lieber auf Sicht segeln anstatt Großprogramme im Detail für drei Jahre ausplanen – wohlgemerkt: zur Genehmigung? Schwierig, wenn der einzige Karrierepfad über Projekte und Programme ins Linienmanagment führt.

Dennoch – oder gerade deswegen – wirken die Ergebnisse agiler Unternehmen verführerisch auf klassische Industrieunternehmen, insbesondere wenn sie sich aufgrund neuer Technologien mit enormem disruptivem Potenzial mit neuen und meist agileren Konkurrenten messen müssen. So anpassungsfähig und innovativ will man freilich auch werden. Also keine dicken Konzepte mehr, sondern nur noch User-Storys. Und flugs die Arbeitspakete im Großprogramm umbenannt in Epics. Ein bisschen Planning Poker zum Schätzen und jeden Tag ein Daily Stand-up. Ein paar Kicker noch und fertig ist der Cargo-Kult: Form ohne Funktion – Theater ohne Wirkung.

Agilität bedeutet im Kern Anpassungsfähigkeit. Es geht darum, in kurzen Abständen etwas Benutzbares zu liefern, Feedback dazu einzuholen und aufgrund dieser Erkenntnis die Strategie anzupassen und die nächsten Schritte zu planen. Agilität bedeutet in unbekanntem Gewässer als Team auf Sicht zu segeln, statt der Unsicherheit mit detaillierten Plänen zu begegnen und diese dann in tayloristischer Arbeitsteiligkeit mit vielen Übergaben schwerfällig umzusetzen. Voruntersuchungen in epischer Breite, um den Scope bis in den letzten Winkel zu klären, sind wenig agil, sondern zeugen von altem Denken. Natürlich kann man die vollständigen Anforderungen für die nächsten drei Jahre User-Storys und die Arbeitspakete des zugehörigen Großprogramms Epics nennen und im Detail planen, aber agil wird das trotz Kicker dann eben doch nicht.

Form folgt Funktion. Nicht umgekehrt. Agilität beruht auf Prinzipien. Die bekannten Praktiken und Methoden sind nur Phänomene der Prinzipien und nicht die Essenz von Agilität. Dass Spotify und andere agile Organisationen ähnliche Praktiken aufweisen, liegt an den gemeinsamen agilen Prinzipien. Die Praktiken allein machen aber nicht agil. Auch hier gilt es, wie so oft, Korrelation nicht mit Kausalität zu verwechseln.

Dr. Marcus Raitner

Foto: privat

1. CYBER SECURITY

Cyber Security ist eines der meist behandelten Themen im Geschäftsumfeld; und das seit Jahren. Diese Attraktion ist leicht zu begründen, schließlich geht es bei dem Thema Sicherheit um nicht weniger als Angst, Vertrauen und eben auch um Geld. Bei einem solchen Thema wird der Mensch schnell aufmerksam. Auch wenn viel von Cyber Security geredet wird, so ist es schwierig, dieses Thema scharf abzugrenzen. Wie ist Cyber Security definiert, wie Internetsicherheit, Informationssicherheit oder Datenschutz?

Cyber Security ist ein so kompliziertes und eben auch interessantes Thema, weil es auf so vielen unterschiedlichen Ebenen behandelt werden kann. So ist Cyber Security selbstverständlich technischer Natur, aber ebenso hat es eine organisatorische Dimension: nur wenn eine Maßnahme auch wirklich in einen Prozess integriert werden kann, wird diese verwendet. Darüber hinaus gibt es eine politische Ebene ("wessen" Datenschutzgesetze werden beispielsweise beim Surfen im Internet angewendet) und eben auch eine menschlich-soziale: der Anwender muss die Maßnahmen wollen, keine Berührungsängste haben und sie insbesondere auch verstehen.

Selbst innerhalb der beispielhaft vorgestellten Ebenen gibt es stets einen schwierigen Kompromiss zu lösen, der mit "Wähle zwei: Sicherheit, Nutzbarkeit, Kosten" umschrieben werden kann. Eine sichere und einfach zu bedienende Lösung ist oft teuer, eine einfach zu bedienende und günstige Lösung oft nicht sicher und schließlich eine günstige und sichere Lösung oft nur schwer zu verwenden. Sowohl für Unternehmen als auch für Privatanwender gilt es nun, einen möglichst passenden Weg zu beschreiten.

Ebenso facettenreich wie das Thema Cyber Sicherheit sind die einzelnen Beiträge dieser Ausgabe selbst. Sie enthalten unter anderem allgemein aufzufassende Themen wie die Sensibilisierung der Gesellschaft, technische Themen wie zukünftige digitale Identitäten, aber auch die Behandlung konkreter Anwendungsfälle wie den mobilen Zugriff auf Unternehmensdaten.

MEIST GEKLICKT – Unsere erfolgreichsten Blog-Beiträge

Unsere Beiträge wurden insgesamt **82.429 Mal** geklickt*

Beiträge zum Thema **CYBER SECURITY** erhielten **21.028** Klicks.

	Autor	Thema
#1	**Dr. Amir Alsbih**	Von Passwort-Hacks bis hin zum Missbrauch digitaler Daten: Es ist höchste Zeit zum Handeln **Seite 48**
#2	**Carl-Sven Kruse**	Cyber Security versus Informationssicherheit versus Netzwerksicherheit **Seite 32**
#3	**Dirk Lieder**	Welche Sicherheitsthemen bewegen aktuell den IT-Markt? **Seite 29**
#4	**Michael Klatte**	Kein Saft in der Leitung: Wenn der Hacker den Strom abdreht **Seite 38**
#5	**Dirk Schlimm**	Dirk Schlimm von Geotab zur Sicherheit von Telematikplattformen **Seite 54**

***Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 1. August 2017 – 14. Februar 2018.**

INHALT

1.1 ALLGEMEIN

1.1.1 Sensibilisierung

Henning Neu, Datenschutz- und IT-Sicherheitsberater, praemandatum GmbH

Better sorry than safe – wir erziehen unsere Gesellschaft zur Unsicherheit

Gigantische Account-Hacks und Datenleaks kommen inzwischen so häufig vor, dass die Aufnahmesolcher Nachrichten in der Öffentlichkeit von Empörung und Sorge übergegangen ist in Gleichgültigkeit. Selbst der Yahoo-Hack, der auf dem Papier quasi die Hälfte der menschlichen Erdbevölkerung betrifft, war auch nur eine Tages-News unter vielen. Hinzu kommt das gesellschaftliche Bild der IT-Sicherheit im Allgemeinen. Die Ende-zu-Ende-Verschlüsselung in WhatsApp wurde als Feature erst nachgeschoben, als das Produkt bereits ein riesiger Erfolg war. Die zusätzliche Sicherheit erscheint somit nicht als notwendig, denn sonst wäre sie ja von Anfang an eingebaut gewesen.

Hieraus ergibt sich ein großes Problem. Sicherheitsmängel werden so alltäglich, dass wir damit das Bild erschaffen, dass das in Ordnung ist. Für uns allgemeine Nutzer erscheint es nur natürlich, dass wir alle paar Wochen von einem Service dazu aufgerufen werden, unser Passwort zu ändern. Wir denken teilweise nicht mal mehr darüber nach, welche Implikationen es haben könnte, wenn mal unser Account gehackt wurde. Klartext-Passwort geleakt? Ich ändere einfach die letzte Stelle. Mail-Adresse geleakt? Das bisschen extra Spam ist doch auch nicht schlimm. – Aber das stimmt nicht. Es ist schlimm. Lassen wir mal die offensichtlichen, potenziell fatalen Folgen dieser Denkweise beiseite und konzentrieren uns auf die Ursache: Die IT-Industrie. Spätestens mit der Erfindung des Internets sind unsere Fortschritte in der Technologie und grenzenlosen Konnektivität gerade zu explodiert. Die Konkurrenz unter den IT-Giganten hat uns so wunderbare Produkte wie das Smartphone gebracht, oder das vernetzte Haus, das uns hoffentlich irgendwann mal dahin bringen wird, dass wir unsere Türklingel mit „JARVIS“ ansprechen können. Doch leider ist häufig bei diesem rapiden Fortschritt die Sicherheit auf der Strecke geblieben. Und zwar, weil sie in vielerlei Hinsicht nebensächlich ist.

IT-Sicherheit ist einer dieser Bereiche, die für die meisten Menschen schlichtweg ungreifbar sind. Von Experten und manchen interessierten Technikern abgesehen, gibt es wohl wenige Menschen, die ein solides Grundverständnis von Sicherheit haben, selbst auf rein theoretischer Ebene. Jeder Mensch kann nachvollziehen, dass ein Zahlenschloss mit drei Ziffern keine solide Methode ist, um sein Fahrrad über Nacht am Bahnhof stehen zu lassen. Doch nur wenige wissen, warum wir nicht „JesusFart“ als Passwort für Facebook, unsere zwei E-Mail Konten, sowie unser Online-Banking nutzen sollten.

Aus Sicht eines Unternehmens ist die Sicherheit ebenso schwammig. Klar könnten wir viele Millionen Dollar in die sichere Systementwicklung stecken, doch wir könnten auch einfach darauf spekulieren, dass wir in der Laufzeit eines Unternehmens nur zwei, oder vielleicht drei große Systemhacks mitmachen müssen. Da sind die Kosten für die Schadensbegrenzung immer noch geringer, vor allem, wenn das Geschäft schon boomt. Und funktionierende Sicherheit bekommt eh niemand mit. Da sparen wir uns lieber das Geld und stecken es in die Produktentwicklung, denn neue Features bringen Geld, im Gegensatz zur Sicherheit. Und hier liegt der Knackpunkt. Sowohl für den Konsumenten, als auch für den Hersteller ist Sicherheit in der Regel kein Muss. Sie ist ein Gimmick. Wir wollen manchmal gar nicht erst darüber nachdenken, welche Folgen unsere neue Technologie für uns und unsere Umwelt haben kann. Wir ziehen in der Industrie Fatalismus der Verantwortung vor, sei es aus Bequemlichkeit, Konkurrenzdruck, Kostensenkung oder purer Naivität.

Unsere IT-Industrie spiegelt nicht das wider, was uns Sicherheitsexperten seit Jahrzehnten einprügeln wollen. Wir lehren unsere Kinder nur selten den verantwortungsvollen Umgang im Internet, wir unterrichten unsere IT-Studenten nicht die Grundlagen der Sicherheit vom ersten Semester an. Wir wollen keine sicheren Software- und Systementwickler, weil sie langsamer sind und uns Grenzen aufzeigen, anstatt uns grenzenlose Möglichkeiten zu bieten. Wir wollen nicht planen und vorausschauen. Wir wollen unser Leben hacken und uns um Konsequenzen keine Sorgen machen.

Und dieses Bild der verschwindenden Grenzen suggerieren wir auch unserer Gesellschaft. Es ist für uns Nutzer in Ordnung, dass Industriegiganten wie Microsoft und Facebook unsere Daten sammeln, dass Behörden aufgrund von mangelnder Sicherheit demokratische Grundwerte mit ihrer neuen Wahlsoftware riskieren. Das gehört heutzutage dazu. So ist unsere Welt, und wir können als Nutzer daran nichts ändern. Und deswegen regen wir uns auch gar nicht mehr so sehr darüber auf, wenn wir mal wieder von einem Hack oder Leak betroffen sind. Wir sind es gewohnt.

Natürlich haben wir trotzdem die Möglichkeit, uns zu informieren, Produkte nicht kaufen, Services zu ignorieren und uns aus aller Technik herauszuhalten, die uns suspekt vorkommt. Doch mit zunehmender Digitalisierung wird dies immer schwerer. Und genau hier sollten wir unser Verhalten als Industrie verändern. Wir können nicht darauf spekulieren, dass unsere gesamte Gesellschaft eine Fachlektüre in die Hand nimmt und plötzlich Enigmail installiert und E-Mails verschlüsselt. Usability ist hier das große Schlagwort und das heißt vor allem im Sicherheitsbereich, dass sich Nutzer nicht mit der Sicherheit selbst auseinandersetzen müssen, um sie zu nutzen und zu verstehen.

Ausnahmsweise ist in diesem Fall WhatsApp sogar ein gutes Beispiel. Ein einfaches, automatisches Update hat für uns Nutzer gereicht, um Nachrichten verschlüsselt zu übertragen. Keine Schlüsselpaarerzeugung, kein manueller Schlüsselaustausch, kein 15-Schritte-Installationsassistent, keine technische Blockade. Es war nicht nur einfach so da, sondern es wurde auch noch automatisch aktiviert. Gut, es kam deutlich zu spät, aber die Einführung selbst konnte aus Nutzersicht nicht komfortabler sein. Und genau so muss gute Usability im Sicherheitsbereich aussehen. Selbst die Information über die Verschlüsselung ist knackig: „Weder Dritte, noch WhatsApp können deine Nachrichten lesen oder hören.“

Sicherheit muss nicht nur implizit vorhanden sein, sie muss auch noch prägnant ausgewiesen sein. Erst dann können wir als Industrie der Gesellschaft auch das Bild vermitteln, das uns in eine sichere Zukunft führt. Das benötigt vor allem echte Verantwortung. Wir dürfen Sicherheit nicht als Feature ansehen. Sie muss ein Grundbaustein in jedem Projekt sein und sich durch alle Bereiche ziehen. Nur so können wir Expertenwissen auch an unsere Nutzer weitergeben. Das heißt, wir müssen auch unsere Fachleute aus allen beteiligten Bereichen in Sicherheitsaspekten unterweisen. Jeder Programmierer sollte wissen, welche Risiken ein Datenbankzugriff haben kann. Jeder Geschäftsführer sollte wissen, dass Sicherheit nicht nur das eigene Unternehmen betrifft und sich manchmal gar nicht in Zahlen ausdrücken lässt. Jeder UX-Designer sollte wissen, wie man Nutzer mit Sicherheit konfrontiert, ohne dass es abschreckend wirkt.

Dies sind alles Punkte, die uns unangenehm sein können, weil sie uns zwingen, einen Moment inne zu halten und über unsere Taten nachzudenken. Wir müssen weg vom fatalistischen Denken, damit wir uns nicht irgendwann selbst zum Verhängnis werden. Es ist an der Zeit Verantwortung zu übernehmen und die regelmäßigen Hacks und Leaks wieder als Skandale anzusehen. Nur so können wir unserer Gesellschaft beibringen, dass Sicherheit wichtig und richtig ist, und vor allem, dass Sicherheit immer implizit sein sollte.

Henning Neu

Welche Sicherheitsthemen bewegen aktuell den IT-Markt?

Mit der PITS – Public IT Security und der it-sa liegen zwei Messeflaggschiffe des Jahres hinter den Anbietern und Anwendern von Cyber-Security-Lösungen. Die Nachfrage nach Antworten auf sicherheitsrelevante IT-Fragestellungen bleibt auf erwartet hohem Niveau – aber welche Themen sorgen aktuell bei den IT-Verantwortlichen für die meiste Bewegung?

Im Zuge der weiter fortschreitenden Digitalisierung der Arbeitswelt und des Privatlebens rückt interessanterweise der Mensch wieder immer stärker in den Fokus. Mitarbeiter arbeiten oft über ihre Smartphones und Tablets auch von unterwegs. Gleichzeitig werden immer mehr Anwendungen und Daten über interne oder externe Cloud-Anwendungen und das Internet zur Verfügung gestellt, die wichtigen Unternehmensdaten sind also auch „unterwegs“. Da wird es naturgemäß eine immer komplexere Aufgabe, Datenflüsse und Zugriffe im Sinne einer integrierten Cyber Security abzusichern.

Wer darf wann von wo über welche Geräte auf was zugreifen – und wie kann ich das wirkungsvoll kontrollieren? Das ist derzeit die Kernfrage, die sich IT-Verantwortliche stellen müssen. So gibt es zum Beispiel Informationen, die ein Mitarbeiter auch per WLAN im Café aufrufen darf, andere aber nur von seinem Arbeitsplatz im Firmennetz aus. Oder der Geschäftsführer hat beispielsweise Zugriff auf andere Informationen und Anwendungen als der Service-Techniker.

Die Schlagworte auf der Lösungsseite sind hier Access Management zur Steuerung von Zugriffen und Identity Management zur Verwaltung von Rechten und Rollen. Damit lassen sich unabsichtliche Datenverluste oder Informationslecks wirkungsvoll vermeiden und die Chancen für absichtliche Angriffe minimieren.

Übergreifende Überwachung und umfangreichere Steuerung können auch über ein so genanntes Security Information & Event Management (SIEM) realisiert werden. Als sehr leistungsstarkes und umfangreiches Hilfsmittel wird SIEM derzeit insbesondere von größeren Unternehmen verstärkt nachgefragt. SIEM-Systeme überwachen den kompletten Datenfluss und Zugriffe auf Daten und Anwendungen und sind in der Lage, Unregelmäßigkeiten zu erkennen und automatisch Gegenmaßnahmen zu ergreifen und vereinen damit gleich mehrere Aspekte der Cyber Security wie Kontrolle, Analyse, Maßnahmen und Optimierungsansätze.
Wenn beispielsweise über die Zugangsdaten eines Mitarbeiters, der sonst stets nur zu Bürozeiten von seinem Schreibtisch in Hamburg aus auf eine Anwendung zugreift, plötzlich mitten in der Nacht ein Zugriffsversuch aus Sao Paolo erfolgt, ist hier aller Wahrscheinlichkeit nach etwas im Argen und der Zugang kann vorsorglich gesperrt werden. Gleichzeitig ermöglichen die durch das SIEM gesammelten Daten grundsätzliche Optimierungen der eigenen Schutzmaßnahmen und Arbeitsabläufe.

Zur Unterstützung besonders berechtigter Benutzergruppen wie etwa Administratoren oder tech-

Dirk Lieder, Geschäftsführer, CONET Solutions GmbH

nischen Mitarbeiten stehen aktuell vor allem auch Lösungen für ein Privileged User Management, das für die Kontrolle von kritischen Rechten und Konten zuständig ist, auf der Wunschliste vieler IT-Verantwortlichen. Privileged User Management schützt Organisationen vor vorsätzlichem aber auch unbewusstem Missbrauch privilegierter Berechtigungen.

Neben diesen operativen „Dauerbrennern" sorgen rechtliche Aspekte wie die anstehende Datenschutzgrundverordnung der EU (EU-DSGVO) mit erweiterten gesetzlichen Anforderungen für viel Gesprächsbedarf. Ab Mai 2018 müssen alle Unternehmen, die mit Kundendaten jeglicher Art arbeiten – also eigentlich alle – viel genauer überwachen und dokumentieren, wie sie Kundendaten speichern, nutzen und löschen. In diesem Zusammenhang reichen die aktuell noch offenen Punkte in vielen Organisationen und Unternehmen von grundlegenden Verständnisfragen zu den gesetzlichen Vorgaben bis zu technischen Einzelheiten. Oftmals besteht beispielsweise in historisch gewachsenen Systemwelten und angesichts zahlreicher beteiligter Abteilungen und Prozesse noch nicht einmal ausreichende Klarheit darüber, welche Daten überhaupt von den neuen Vorgaben betroffen sind, wo, von wem und wie diese gespeichert und verarbeitet werden, wie diese sich identifizieren lassen und welche Maßnahmen notwendig sind, um hier zukünftig rechtssicher zu agieren.

Udo Schneider, Security Evangelist DACH, Trend Micro

Um hier verlässliche Klarheit zu erlangen und systematisch vorgehen zu können, hilft eine bewusst prozessorientierte Methodik, wie sie CONET in enger Zusammenarbeit mit einem Kunden entwickelt hat. Diese stellt sicher, dass alle betroffenen Prozesse zuverlässig identifiziert, analysiert und im Bedarfsfall angepasst oder neu aufgesetzt werden können. Dabei werden schnell erste Ergebnisse erzielt, die ebenso schnell in erste Maßnahmen münden und schrittweise umgesetzt werden können.

Kern der Lösungen ist dabei die Erweiterung des Geschäftsprozessmanagements um die Inhalte des Datenschutzes. Dazu gehören die Prozessanalyse und Identifikation der personenbezogenen Daten, die Abgrenzung sowie Abbildung der Verarbeitungstätigkeiten auf Basis der identifizierten Prozesse und die anschließende Ableitung und Initiierung notwendiger technisch-organisatorischer Maßnahmen (TOM). Darauf folgen die Durchführung einer Datenschutzfolgeabschätzung und Risikobewertung, wobei je Verfahren die Notwendigkeit, die Verhältnismäßigkeit sowie die Risiken für die Rechte und Freiheiten des betroffenen Individuums zu bewerten sind. Schließlich leiten sich daraus die Definition der Prozessabläufe zur Einführung der Lösch- und Sperrkonzepte (inklusive Rollen- und Berechtigungskonzepte) und die Erstellung eines Konzepts zur technischen Umsetzung der Informations- und Dokumentationspflichten zur Auftragsverarbeitung nach § 28f DSGVO und § 26 DSGVO sowie Einzeldokumentationspflichten nach § 7 und § 8 DSGVO und § 33f DSGVO ab.

Letztlich führen alle diese Maßnahmen gemeinsam dazu, dass die vorhandenen Prozesse und Systeme in definierten Einzelschritten überschaubar und effizient so angepasst werden können, dass sie den neuen Anforderungen wie Dokumentation und Datensparsamkeit gerecht werden. Dies verursacht trotz iterativen Vorgehens natürlich entsprechende Aufwände, denen sich Unternehmen – nicht nur in regulierten Märkten – und auch gerade der öffentliche Sektor aber zügig werden stellen und für die entsprechende personelle und finanzielle Ressourcen eingeplant werden müssen.

Dirk Lieder

1.1.2 Sicherheitssäulen

IoT & Smart-Devices im Heimnetz – „Adé Security!" oder lösbare Herausforderung?

Heimnetz vs. Firmennetzwerk

Heutige Heimnetzwerke sind alles andere als „klein": Häufig findet man ein buntes Sammelsurium an verschiedenen PCs, Druckern, NAS-Systemen, Tablets und Smartphones. Flankiert werden diese offensichtlichen Geräte oftmals noch durch zahlreiche Smart Devices: Darunter Fernseher, TV-Sticks, Radio- und Streaming-Geräte, Überwachungskameras, Wetterstationen, Heizungssteuerungen oder was sonst noch an internetfähigen Geräten angeboten wird. Willkommen in der wunderbaren Welt des IoT – oder in diesem Kontext besser des IoE – des Internet of Everything!

Diese Komplexität war man bis vor einigen Jahren nur aus dem professionellen Firmenumfeld gewohnt. Doch dort wuchs diese Komplexität der Infrastruktur nicht über Nacht und im Gegensatz zu Heimnetzwerken war und ist das Thema „Security" dabei immer im Fokus.

Sicherheit im Heimnetzwerk?

Wenn also moderne Heimnetzwerke in ihrer Komplexität früheren Firmennetzwerken in nichts nachstehen – woher kommen dann die massiven Diskrepanzen beim Thema Security?

Auf der einen Seite steht sicherlich die Kritikalität der bereitgestellten Dienste und Daten. Im geschäftlichen Umfeld gefährdet der Ausfall von Servern (beispielsweise E-Mail oder Datenbank) oder der Verlust von Daten nicht selten das Fortbestehen der Unternehmung. Im privaten Umfeld hingegen sind viele Daten, so wichtig sie für den Nutzer im Moment auch sein mögen, entweder wiederbeschaffbar oder ohnehin nur vorübergehend von Bedeutung.

Auf der anderen Seite ist aber auch die Art der Internetnutzung zu betrachten. Nicht umsonst spricht man häufig vom „Internet-Zugang". Damit einher geht auch die Vorstellung, dass der eigene Router den Zugang zum großen Netz bereitstellt. Als Einbahnstraße vom heimischen Netz ins Internet – die Gegenrichtung bleibt vermeintlich verschlossen. Frei nach Aschenputtel: „Die Guten im Heimnetz, die Bösen im Internet" – Zumindest glauben das die meisten.

Home-IoT-Geräte untergraben (traditionelle) Heimnetzsicherheit

Spätestens mit dem Aufkommen von „Home-IoT"-Geräten ist diese Einbahnstraße jedoch endgültig durchbrochen. Das smarte Gerät zuhause macht nämlich nur halb so viel Spaß, wenn man es ausschließlich aus dem heimischen Netz mit der schicken App fernsteuern kann. Daher erwarten die meisten Kunden nahezu selbstverständlich den Zugriff aus dem Internet. Ob die Kommunikation über manuell bzw. via UPnP (Universal Plug and Play) geöffnete Ports oder „über Bande", also einen Server im Internet, stattfindet, ist dabei egal. Der Effekt ist stets der Gleiche: Ein Gerät im heimischen Netz ist von außen steuerbar.

Hinzu kommen oft noch Lücken im Gerät selbst oder im damit verbundenen Cloud-Dienst. In beiden Fällen ist der User auf den guten Willen des Herstellers angewiesen – sei es für Firmware-Updates oder die Pflege der Cloud-Dienste.

Aus dem Firmen-Umfeld lernen

Kombiniert bedeutet dies, dass wir uns geistig vom Konzept der Einbahnstraße lösen müssen – „Kommst du ins Internet, kommt das Internet auch zu dir". Das heißt aber auch, dass man bekannte Sicherheitsprinzipien im Heimnetz unbedingt auf den Prüfstand stellen muss. Die simple Annahme, dass keiner reinkommt, ist schlicht nicht mehr haltbar. Das Risikoprofil für das normale Heimnetz ist damit aus Security-Sicht gar nicht mehr so weit von einem normalen Firmennetz entfernt. Das muss aber nicht unbedingt negativ sein, bedeutet es doch auch, dass man Security-Lektionen aus dem Firmenumfeld jetzt auch auf den Heimanwender übertragen kann und dieser sie nicht erst schmerzhaft selbst lernen muss.

Dies heißt jedoch nicht, dass ein Heimanwender jetzt die gleichen Security Lösungen wie ein DAX-30-Unternehmen betreiben muss. Aber es bestehen durchaus Ähnlichkeiten: Lösungen wie Firewalls, Reputationsdienste, Intrusion Detection/Prevention, Content Security oder auch Breach Detection assoziiert man ad hoc zunächst mit großen Unternehmen. Funktional haben diese im modernen Heimnetz aber ebenso ihre Berechtigung:

- Eine Firewall reglementiert den ein- und ausgehenden Netzwerkverkehr am Router. Und vielleicht noch wichtiger – sie führt auch Protokoll über angenommene oder abgewiesene Verbindungen. Die bisher übliche Vorgehensweise „alles darf raus und nichts darf rein" ist einfach nicht mehr zeitgemäß.
- Reputationsdienste verhindern den Zugriff auf gefährliche Inhalte (z.B. Exploit Kits). Sie schließen damit ein Haupteinfallstor für Schadsoftware jeder Art. Auch versuchte oder erfolgreiche Kommunikation mit Command- und Control-Servern wird darüber erkannt und verhindert. Funktionell sind diese Dienste häufig in Kombination mit Kinderschutz-Filtern zu finden.
- Intrusion-Detection- und Intrusion-Prevention-Systeme bieten in Zusammenarbeit mit Firewalls oft deutlich bessere Informationen über die tatsächlich erfolgten Angriffe und benutzten Werkzeuge bzw. Lücken. Sieht man beispielsweise hunderte von Angriffen auf Lücken in Windows XP, so sollte man sich vielleicht doch überlegen, das Schätzchen mit den alten Spielen entsprechend zu schützen…
- Content Security wiederum betrachtet nicht nur die Verbindungen selbst, sondern auch deren Inhalte. Typische Beispiele hierfür sind Spam- und Phishing-Mails aber auch Schadsoftware oder andere schädliche Inhalte.
- Breach Detection erkennt, vereinfacht gesprochen, kompromittierte Geräte. Dies kann der heimische PC sein, der doch irgendwie befallen wurde. Genauso kann es sich dabei aber auch um den Heizungsthermostat handeln, der sich komisch verhält oder das Babyfon mit Kamera im Kinderzimmer, dessen gehackte Firmware den Livestream auf diversen Seiten im Internet bereitstellt.

Firmen-Security-Lösungen im Heimnetz?

All das bedeutet nicht, dass jeder Heimnutzer das Wissen und die Erfahrung eines dedizierten IT-Sicherheitsadministrators aufbauen muss. Viele dieser Funktionen werden heute bereits von am PC installierbaren Sicherheitslösungen abgedeckt.

Aber in Zeiten von Handy, Tablet und anderen smarten Devices muss man sich zwangsläufig auch die Frage der Sicherung dieser Geräte stellen. Wer schon einmal versucht hat, auf einer WLAN-Kamera eine Firewall oder einen Virenscanner zu installieren, kennt das Problem.

Daher sind hier primär die Hersteller von Heimroutern aufgefordert, die bereitgestellten Sicherheitsfunktionen den aktuellen Anforderungen anzupassen. Die Router stellen den zentralen Übergabepunkt zum Internet dar und sind darüber hinaus als Ethernet-Switch bzw. WLAN Access Point die sprichwörtliche Spinne im (Heim-)Netz, die in der

Carl-Sven Kruse, stellvertretender Vorsitzender, Networx Security e.V.

Lage ist, jeglichen internen und externen Verkehr zu sehen, zu untersuchen und bei Bedarf auch zu unterbinden. Sie sind somit eine optimale Plattform, um diese Sicherheitsfunktionen bereitzustellen.

Stand der Technik sind solche Lösungen im Firmenumfeld seit Langem. Was im Heimumfeld oft fehlt, ist eine adäquate Umsetzung dieser Anforderungen mit einer für den Heimbenutzer verständlichen Verwaltung. Trend Micro arbeitet deshalb mit verschiedenen Router-Herstellern zusammen, um den Nutzern genau diese einfach zu verwaltende Sicherheit im Heimnetzwerk zu ermöglichen.

Die bisher weit verbreitete Strategie „viel Geschwindigkeit, viele Ports, viele Antennen und ein bisschen Sicherheit, Modell Einbahnstraße“ ist einfach nicht mehr zeitgemäß.

Zusammenfassung

Wir müssen uns darüber klarwerden, dass spätestens mit dem massiven Aufkommen von Home-IoT-Geräten die klaren Grenzen zwischen „drinnen“ und „draußen“, „gut“ und „böse“ auch bei normalen Heimnetzwerken gesprengt sind.

Dies ist zunächst neutral zu betrachten: „Einfache“ Sicherheitsmaßnahmen sind zwar nicht mehr ausreichend effizient, auf der anderen Seite ist der Funktionalitäts- und Komfortgewinn durch solche Geräte natürlich enorm. Ähnlich wie schon im Firmenumfeld handelt es sich dabei um ein lösbares Problem – nur erfordert dies auch entsprechend angepasste Funktionalitäten. Das simple Einbahnstraßenmodell reicht hier nicht mehr aus.

Optimalerweise werden solche Funktionen zentral auf der Schalzentrale im Heimnetz, dem Router, bereitgestellt. Damit profitieren auch Geräte, auf denen keine Sicherheitssoftware installiert werden kann, automatisch von diesen Sicherheitsfunktionen. Dies bedeutet letztendlich natürlich auch, dass die Router-Hersteller hier in der Pflicht stehen, entsprechende Funktionen anzubieten und mit einer für „Otto-Normal-User“ verständlichen Verwaltung auszustatten.

Einige Hersteller haben diesen Trend bereits erkannt und ihre Produkte mit einem deutlichen Mehr an Sicherheit ausgestattet. Interessanterweise haben sich zuerst die Gamer auf diese Router gestürzt, versprechen sie doch eine Verlagerung der Sicherheitsfunktionen, weg vom PC auf den Router, und damit mehr freie Ressourcen für Spiele. Dies ist aber auch eine Chance, Unterscheidungsmerkmale jenseits von „mehr & billiger“ zu schaffen – eine Entwicklung, die letztendlich uns allen zugutekommt.

Udo Schneider

Cyber Security versus Informationssicherheit versus Netzwerksicherheit

In unserer heutigen Zeit, in der Unternehmen digitaler sind als je zuvor und mit immer neu aufkommenden Technologien muss auch die Sicherheitsinfrastruktur der Unternehmen verbessert werden, um die Sicherheit zu erhöhen. Andernfalls könnte es zu kostspieligen Systemangriffen kommen, wie wir dies bei vielen Unternehmen mit WannaCry und Petya Attacken erlebt haben.

Um Geschäftsdaten, Geld und Ihre Reputation zu schützen, ist es notwendig in fortschrittliche Sicherheitssysteme zu investieren. Bevor Sie jedoch ein Sicherheitskonzept für Ihr Unternehmen entwickeln, ist es essentiell die Unterschiede der verschiedenen Sicherheitslevel zu verstehen und zu wissen wie diese zusammenhängen.

Was ist Cyber Security?

Cyber Security bzw. Computer Sicherheit ist ein Oberbegriff und umfasst den Schutz von Computer Systemen, Daten und Netzwerken. Dazu gehört unter anderem der physische Schutz von Hardware und Serverräumen, sowie Netzwerksicherheit und Schutzmaßnahmen gegen Malware. Des Weiteren kann man die Sicherung von Cloud-Infrastrukturen, mobilen Szenarien und dem Internet der Dinge (IoT) dazuzählen.

Cyber Security schützt Computer, Daten und Netzwerke Ihres Unternehmens vor unautorisiertem Zugriff, Angriffen oder Beschädigungen durch die Implementierung diverser Prozesse, Technologien und Praktiken. Angesichts der zahllosen Bedrohungen, die auf alle Arten von Unternehmen abzielen, ist es entscheidend, dass Ihre IT-Infrastruktur davor geschützt ist und einen vollständigen Angriff auf Ihr Netzwerk abwehren kann, um zu verhindern, dass beispielsweise Unbefugte auf Ihre Daten zugreifen bzw. der Ruf Ihres Unternehmens geschädigt wird.

Social Engineering

Cyber Angriffe richten sich nicht nur gegen ihre Organisation und deren Daten, sondern können auch dazu dienen Ihre Mitarbeiter auszuspionieren. Angreifer nutzen es aus, dass viele Mitarbeiter, außerhalb der IT Sicherheitsbranche, Cyber Bedrohungen nicht erkennen, um somit leicht in ihr Unternehmen eindringen zu können. Durch effektive Cyber Security kann dem vorgebeugt werden.

Der Prozess des Social Engineering bedeutet, dass Angreifer Wissen- und Systemlücken ausnutzen, um so durch den Mitarbeiter Zugang zu sensiblen Informationen zu erhalten. Die häufigsten Social Engineering Angriffe umfassen:

- Phishing: Normalerweise in Form von E-Mails oder Chats, bei denen Angreifer sich als echte Organisation ausgeben, um Informationen und Zugang zum System zu erlangen.
- Pretexting: Wenn ein Angreifer eine Autoritätsperson oder eine Person imitiert, der die Zielperson vertraut, um Informationen zu erhalten.
- Baiting: Wenn Angreifer ein Malware-infiziertes Gerät, wie z.B einen USB Stick oder eine CD, an einem Ort liegen lassen, an dem es leicht von jemandem gefunden werden kann, sodass jemand dann das infizierte Gerät auf seinem Computer verwendet und versehentlich die Malware installiert.
- Quid pro quo: Wenn ein Angreifer persönliche Informationen im Austausch für eine Form von Belohnung wie z.B. Geld, ein Geschenk oder einen kostenlosen Service, anfordert.

Als Unternehmensführer liegt es in Ihrer Verantwortung, eine Kultur des Sicherheitsbewusstseins aufzubauen und Lücken im Cyber Sicherheitswissen und Cyber Verständnis Ihres Teams zu schließen. Es ist wichtig, dass Ihre Mitarbeiter über Cyber Security Risiken informiert werden, damit die Wahrscheinlichkeit sinkt, dass ein Mitarbeiter Opfer eines Angriffs wird. Bieten Sie Ihren Mitarbeitern die erforderlichen Schulungen und Technologien an, um die menschliche Firewall Ihres Unternehmens zu stärken und die Möglichkeit eines Cyberangriffs zu verringern.

Was ist Informationssicherheit?

Informationssicherheit bzw. InfoSec stellt sicher, dass Daten vor unbefugten Zugriffen, Verwendungen, Offenlegungen, Störungen, Änderungen, Aufzeichnungen oder Zerstörungen geschützt sind.

Schutzziele

Wenn InfoSec Experten Richtlinien und Verfahren für ein effektives Informationssicherheitssystem entwickeln, verwenden sie die CIA Schutzziele. CIA hat dabei nichts mit der Central Intelligence Agency zu tun, sondern steht als Abkürzung für:

- Confidentiality – Vertraulichkeit gewährleistet, dass Informationen für unbefugte Personen unzugänglich sind. Dies wird häufig durch Verschlüsselung erreicht.
- Integrity – Integrität schützt Informationen und Systeme vor Änderungen durch nicht autorisierte Personen und stellt sicher, dass die Daten genau und vertrauenswürdig sind.
- Availability – Verfügbarkeit stellt sicher, dass autorisierte Personen bei Bedarf auf die Informationen zugreifen können und dass die Hardware und Software ordnungsgemäß gewartet und bei Bedarf aktualisiert wird

Die CIA Schutzziele sind zum de facto Standardmodell geworden, um ein Unternehmen sicher zu halten. Die drei grundlegenden Prinzipien helfen beim Aufbau einer Reihe von Sicherheitskontrollen, um Ihre Daten zu schützen.

Was ist Netzwerksicherheit?

Netzwerksicherheit umfasst alle Maßnahmen zur Planung, Ausführung und Überwachung der Sicherheit in Netzwerken. Netzwerksicherheit zielt darauf ab die Daten zu schützen, die über Netzwerke transportiert werden, um sicherzustellen, dass Informationen nicht geändert oder abgefangen werden. Des Weiteren soll die Netzwerksicherheit jeden Zugriff, von außen oder innen, eines Systems auf nicht autorisierte Bereiche verhindern.

Die Aufgabe der Netzwerksicherheit besteht darin, die IT-Infrastruktur des Unternehmens vor Bedrohungen zu schützen wie z.B.

- Viren, Würmer und Trojaner
- Zero-Day-Angriffe
- Hackerangriffe
- Denial-of-Service Angriffe
- Adware und Spyware

Netzwerksicherheitsexperten implementieren die Hardware und Software, die zum Schutz erforderlich sind. Mit der richtigen Netzwerksicherheit werden aufkommende Bedrohungen erkannt, bevor diese in Ihr Netzwerk eindringen und Ihre Daten gefährden.

Zu den wichtigsten Netzwerksicherheitskomponenten gehören:

- Firewalls
- Antiviren Software
- Intrusion Detection und Präventionssysteme (IDS / IPS)
- Virtuelle private Netzwerke (VPNs)
- Show Tech Analyzer

Carl-Sven Kruse

Wie Unternehmen Daten vor Cyberangriffen schützen

Michael Nuncic, Marketing Communications Manager, Kroll Ontrack GmbH

WannaCry, Petya und Bad Rabbit haben gezeigt: Unternehmen sind gegen Cyberattacken unzureichend abgesichert. Immer häufiger machen Erpressungstrojaner Schlagzeilen, indem sie zahlreiche Firmendaten beschlagnahmen und Prozesse lahmlegen. Um sich vor finanziellem Schaden zu bewahren, sollten Unternehmen bewusster mit Daten umgehen und sie besser schützen.

Mehr als jedem zweiten Unternehmen in Deutschland wurden schon mal durch eine Cyberattacke Daten gestohlen, das ergab eine repräsentative Studie des Digitalverbandes Bitkom aus dem Juli 2017. Der Schaden, den die deutsche Wirtschaft dadurch erleidet, ist groß: Rund 55 Milliarden Euro kosten Hackerangriffe jährlich. Und auch die kleinen Unternehmen kann ein Datenverlust hart treffen. Denn zwei von drei Kleinunternehmen können ohne ihre Daten nicht arbeiten – das zeigt eine aktuelle Studie des Datenrettungsspezialisten Kroll Ontrack. Ein Cyberangriff, bei dem systemrelevante Daten beschlagnahmt und verschlüsselt werden, kann daher bei vielen zu Ausfällen und finanziellem Schaden führen.

Kleinunternehmen schützen Daten nicht genug

Wer glaubt, dass Kleinunternehmen daher alles tun, um ihre Daten zu schützen, der irrt: Nur jedes

zweite prüft, ob verlorene Daten im Ernstfall wieder herstellbar sind. Ein so leichtsinniger Umgang mit dem Risiko eines möglichen Datenverlusts kann jedoch schwerwiegende Folgen haben. Gehen Daten von einem wichtigen Projekt verloren, kann das den Verlust eines Kunden bedeuten. Sind jedoch systemrelevante Dateien verloren oder korrumpiert, führt das schlimmstenfalls zu finanziellem Ruin. Nämlich dann, wenn die Wiederherstellung der Daten länger dauert als die Zeit, die das Unternehmen ohne Daten überbrücken kann. Laut der Umfrage können nur 17 Prozent länger als eine Woche ohne Daten weiterarbeiten.

Neben wirtschaftlichen Konsequenzen kommen außerdem rechtliche Folgen hinzu. Denn auch für Kleinunternehmen gelten hierzulande einige gesetzlichen Aufbewahrungspflichten für elektronische Unterlagen, dazu zählt das Steuer- und Handelsrecht. „Unternehmen haben danach ihre DV-Systeme gegen Verlust – etwa Unauffindbarkeit, Vernichtung, Untergang und Diebstahl – zu sichern und gegen unberechtigte Eingaben und Veränderungen – beispielsweise durch Zugangs- und Zugriffskontrollen – zu schützen. Werden die entsprechenden Unterlagen nicht ausreichend geschützt und können deswegen nicht mehr vorgelegt werden, ist die Buchführung formell nicht mehr ordnungsmäßig“, weiß Lennart Schüßler, Partner und Datenschutzexperte bei der Kanzlei Bird & Bird. „Die Unterlagen müssen zudem über den gesamten Aufbewahrungszeitraum von bis zu zehn Jahren lesbar bleiben.“

Backup aufsetzen und regelmäßig überprüfen

Damit Unternehmen rechtliche und wirtschaftliche Folgeschäden eines Datenverlusts – sei es durch eine Cyberattacke, aber auch durch Stromausfall, Software- oder Hardwareschäden – umgehen können, sollten sie ihre Daten richtig sichern und dafür sorgen, dass sie im Notfall schnell wieder hergestellt werden können. Nur so können Ausfallzeiten minimiert und der Schaden begrenzt werden. Denn jede Minute Datenverlust kostet. Am einfachsten ist es daher, ein oder besser mehrere Backups aufzusetzen. Ein gutes Backup ist das A und O, denn so lassen sich verlorene Daten einfach ersetzen und neu ins System einspielen. Am geeignetsten dafür sind traditionelle Festplatten, also HDDs, statt schnellere und Chip-basierte SSD-Festplatten. Der Grund ist einfach: Im Falle eines Datenverlusts können Backup-Daten von SSDs nur sehr schwierig, zeitaufwendig oder überhaupt nicht gerettet werden. Außerdem empfiehlt sich ein zusätzliches Backup in der Cloud.

Denn auch Backup-Systeme können mit der Zeit kaputtgehen. Daher sollten Kleinunternehmen Hardware und Software der Speichermedien immer wieder auf Funktionstüchtigkeit prüfen, indem sie zum Beispiel bereits erstellte Backups aufrufen und kontrollieren. Zudem sollten sie mindestens einmal in drei Monaten Tests durchführen, ob es möglich ist, ein Backup in das interne IT-System einzuspielen. Das kann zum Beispiel auf einem dezidierten Testserver oder auf einem ausrangierten Altserver geschehen.

Disaster-Recovery-Plan definieren und auf den Ernstfall vorbereiten

Besser ist es jedoch, wenn das Backup gar nicht erst benötigt wird. So gehört das Erstellen eines Disaster-Recovery-Plans, einem Plan für die Notfallwiederherstellung der gesamten IT-Infrastruktur, unbedingt zur Vorbereitung auf Cyberangriffe dazu. Für den Fall einer Hackerattacke sollte ein separater Absatz definiert werden. Unternehmen sollten Schutzmaßnahmen aufsetzen, damit die Ransomware sich nicht im gesamten Netzwerk ausbreitet, sobald ein Gerät infiziert wurde. Der Plan sollte regelmäßige Sicherheitsupdates beinhalten und vor allem den Mitarbeitern als Anleitung dienen. Denn gerade hier kann menschliches Fehlverhalten Probleme verschlimmern – oder erst verursachen. Ein falscher Klick auf einen Link oder E-Mail-Anhang, und schon beginnt die Schadsoftware mit der Verschlüsselung geschäftskritischer Daten.

Tipps für ein sicheres Verhalten im Netz können leichtsinnigem Umgang mit Daten vorbeugen. Das kann zwar die Wahrscheinlichkeit, Opfer eines Cyberangriffs zu werden, etwas senken – ganz verhindern lässt sich das natürlich nicht. Doch selbst, wenn es zu spät ist, kann eine richtige Reaktion den Schaden minimieren. Bemerkt ein Mitarbeiter den Angriff, sollte er den Computer sofort vom Netz trennen, ansonsten droht der Verlust der gesamten Firmendaten. Allerdings bedeutet das nicht, panisch den Stecker ziehen, sondern zu versuchen, das System so normal wie möglich herunterzufahren. Denn bei hochkomplexen virtualisierten Speichersystemen kann es in Folge eines plötzlichen Shutdowns zu zusätzlichen Problemen kommen, die es schwieriger und aufwendiger machen, die infizierten und verschlüsselten Daten wiederherzustellen. Ein Zusammenbruch bewirkt hier, dass die Dateistruktur beschädigt wird. Oft müssen viele kleine Datenfragmente von mehreren verschiedenen Systemen auf einem Gerät rekonstruiert werden. Das macht eine Datenrettung aufwendiger und teurer und hat einige Unternehmen bereits finanziell ruiniert. Um die Wiederherstellung zu vereinfachen, sollte die IT so einfach wie möglich gehalten und Server in punkto Speicherkapazität nicht überreizt werden.

Eskalationsstufen festhalten und Datenrettungsspezialist kontaktieren

Auch sollten in dem Disaster-Recovery-Plan verschiedene Eskalationsstufen festgeschrieben werden: Wann werden die Kosten eines Systemausfalls und damit einhergehend eines Datenverlusts existenzbedrohend für die Firma? Wie hoch ist der Wert der korrumpierten und verschlüsselten Daten? Welche Daten sind wichtiger als andere und wo drängt die Wiederherstellung mehr? Ebenso sollte dort stehen, welche Dienstleister und Lieferanten die Mitarbeiter im Notfall informiert werden müssen. In diesem Zusammenhang empfiehlt es sich auch, einen vertrauenswürdigen externen Datenrettungsspezialisten an der Hand zu haben. Denn Daten lassen sich meist nicht inhouse wiederherstellen. Und gerade Kleinunternehmen können sich keine eigene IT-Abteilung leisten. Ein Spezialist jedoch kennt viele verschiedene Arten von Ransomware und weiß, wie die Daten zu entschlüsseln und in den Originalzustand zu bringen sind. Dieser sollte frühzeitig zu Rate gezogen werden, sobald das infizierte Gerät ausgeschaltet ist. Denn ein neues Einschalten kann dazu führen, dass sich die Schadsoftware ausbreitet und wichtige Informationen schlimmstenfalls für immer verschwunden bleiben. Außerdem sollte auf keinen Fall gefordertes Lösegeld bezahlt werden.

Vor Cyberangriffen wirklich sicher sein kann niemand, nicht einmal mit den besten Sicherheitsmaßnahmen. Doch mit den richtigen Verhaltensregeln können Unternehmen den Schaden der Angriffe minimieren. Zum Beispiel, indem sie regelmäßig Backups anlegen, einen Notfallplan definieren und dafür sorgen, dass sich Daten so schnell und kostengünstig wie möglich wiederbeschaffen lassen. Auf diese Weise machen sie sich weniger abhängig von ihren Daten und können auch mal den ein oder anderen kleinen Ausfall verschmerzen.

Michael Nuncic

1.1.3 Kritische Infrastrukturen

SAP-Sicherheit im E-Government und im Umfeld kritischer Infrastrukturen

Jörg Schneider-Simon, Chief Technology Officer, Bowbridge Software

„E-Government“ ist in Deutschland bereits seit dem Jahr 2000 eine zentrale Regierungsaufgabe, im Zuge derer den Bürgern immer mehr Verwaltungsangebote auch online zugängig gemacht werden und Prozesse in den Verwaltungsbehörden digitalisiert werden. Der Bereich „Staat und Verwaltung“ ist dabei einer der Sektoren der vom Bundesministerium des Inneren definierten, sogenannten „Kritischen Infrastrukturen“(1), bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe,

erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Aus Cyber-Security Sicht bedeutet dies, dass E-Government Anwendungen für Hacker jeglicher Couleur sehr attraktiv sind und leider auch vermehrt zum Ziel von Angriffen werden.
Bei E-Government, ähnlich wie in Unternehmen, übernehmen auch Lösungen der Walldorfer Software-Schmiede SAP die Digitalisierung und IT-gestützte Abbildung zahlreicher Abläufe. Insbesondere seit Einführung der neuen SAP UI5 Benutzerschnittstellen, die auch für die einfache Verwendung von mobilen Endgeräten aus optimiert sind, interagieren Bürger und Geschäftspartner der öffentlichen Verwaltungen – oft unbewusst – unmittelbar mit einer SAP Anwendung. Für Angreifer bedeuten diese exponierten Benutzerschnittstellen, zu Beispiel Eingabemasken oder Upload-Funktionen, einen möglichen Angriffspunkt.

SAP FIORI basiert auf SAP UI5 Bildquelle: SAP
IT-Insider wissen, bei SAP-Anwendungen gelten zahlreiche Besonderheiten. So auch beim Schutz gegen Cyber-Angriffe. Zwar stellt SAP monatlich Security Fixes – im SAP-Jargon „Security-Hinweise“ genannt – zur Verfügung. Allerdings sind die meisten SAP Anwendungen stark modifiziert und auf die individuellen Bedürfnisse des jeweiligen Kunden angepasst. Die Fixes von SAP betreffen aber immer nur den Auslieferungsstand der Anwendungen – ohne eben diese Anpassungen, in denen oftmals ähnliche oder weitere Sicherheitslücken existieren. SAP-Kunden und öffentliche Verwaltungen sind daher angehalten, Ihre Anwendungen durch den Einsatz geeigneter Produkte zusätzlich abzusichern. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in diesem Zusammenhang in den sogenannten Grundschutzkatalogen auch eindeutige Handlungsempfehlungen zum Schutz von SAP Anwendungen ausgesprochen.

Die Angriffsvektoren, die SAP Cybersecurity-Verantwortliche im Blick haben sollten teilen sich dabei in zwei große Kategorien auf: Angriffe über Formular-Eingaben, also sogenannte „strukturierten Daten“ und Angriffe über Datei-Uploads, mit sogenannte „unstrukturierten Daten“.

Angriffe mit strukturierten Daten:

Cross-Site-Scripting (XSS)
Cross-Site Scripting gehört zu den gängigsten Angriffen auf Web-Anwendungen. Das gilt auch bei SAP- Anwendungen. Etwa 25% aller jemals veröffentlichten SAP Security Hinweise betreffen diesen Angriffsvektor. Mit Cross-Site Scripting gelingt es Angreifern im einfachsten Falle über die Eingabemasken der Anwendung, HTML oder gar JavaScript Code in die Anwendung einzuschleusen. Bei nachfolgenden Benutzern interpretiert der Web-Browser diesen eingeschleusten Code als legitimen Bestandteil der Anwendung und führt ihn mit denselben Sicherheitsprivilegien aus wie die Anwendung. Auf diese Art und Weise können Angreifer das Erscheinungsbild der Anwendung verändern (sog. Defacing), oder subtiler vorgehen und beispielsweise vermeintliche Login-Pop-Ups einblenden, um Zugangsdaten zu erhalten. Auch das Auslesen der SessionID, um die authentifizierte Sitzungen zu übernehmen, ist ebenso möglich wie die Installation von Keyloggern oder anderer Malware über sogenannte Drive-By-Dowbloads.

SQL-Injections
SAP Anwendungen basieren auf leistungsfähigen Datenbanken. Ganz gleich ob Oracle, Microsoft oder die SAP-eigene HANA in-memory Datenbank, werden diese über SQL-Statements abgefragt oder Daten eingepflegt oder bearbeitet. Im Falle einer SAP Anwendung kommt bereits eine unter Sicherheitsgesichtspunkten optimierte Variante (OpenSQL) zum Einsatz. Dennoch kann es Angreifern mit Kenntnis der internen Tabellenstrukturen von SAP-Anwendungen möglich sein, die generierten SQL Statements so zu beeinflussen, dass sie unautorisierten Zugriff auf Datensätze erlangen, oder diese zu modifizieren.

Directory Traversal
Wie auch andere Anwendungen, verwenden SAP-basierte Lösungen URL-Pfade zur Navigation und zur Parameterübergabe innerhalb der Anwendung, oder auch um auf Dateien zuzugreifen, die im Datei-System des Servers liegen. Angreifern kann es gelingen, diese URLs so zu manipulieren, dass der unerlaubte Zugriff auf Dateien (z.B. Konfigurations-Dateien) möglich wird, oder dass Anwendungsbereiche angezeigt werden, auf die der User normalerweise keinen Zugriff hätte.

OS-Command Injections
SAP Anwendungen greifen in vielen Fällen auf Funktionen des darunterliegenden Betriebssystems zurück. In Fällen, in denen es Angreifern gelingt, anstelle des SAP-seitig aufgerufenen Kommandos – oder zusätzlich dazu – eigene Befehle auf Betriebssystem-Ebene auszuführen, kann die vollständige Übernahme des Servers die Folge sein.

Angriffe mit unstrukturierten Daten (Dateien)
Generell ist eine ungesicherte Möglichkeit, Dateien in eine Web-Anwendung hochzuladen als Sicherheitslücke zu bewerten. Dies geht aus der Risikobewertung des Open Web Application Security Projects, aber auch aus den Grundschutzkatalogen des BSI eindeutig hervor.

Viren, Malware, Ransomware
Das Prinzip, Dritt-Anwendungen als Verteiler für Malware zu nutzen ist natürlich nicht neu, und auch nicht auf SAP Anwendungen beschränkt. Eine besondere Herausforderung ergibt sich aber daraus, dass SAP Anwendungen hochgeladene Dateien in der Regel in der Datenbank oder einem proprietären Content Server ablegen. In diese können Anti-Viren Lösungen, die auf Betriebssystem-Ebene installiert sind nicht hereinschauen. SAP selbst empfiehlt sogar, SAP Programm-Verzeichnisse und die Datenbank vom Virenscan vollständig auszuschließen. Unternehmen und Behörden wägen sich daher oft in einem trügerischen Gefühl falscher Sicherheit, wenn Sie davon ausgehen, dass eine aktuelle Virenschutz-Lösung auf Betriebssystem-Ebene auch Uploads in die SAP Anwendung absichert.

Das Bundesamt für Sicherheit in der Informationstechnik hat bereits vor 10 Jahren bei SAP Systemen, die aus dem Internet erreichbar sind, die Implementierung von Virenschutz und Content-Scan auf Anwendungsebene zur Anforderung deklariert (S. BSI Grundschutzkatalog, M4.271 und M2.343).

Umgehung von Dateityp-Filter
Web Anwendungen sollten generell nur den Upload solcher Datei-Typen zulassen, die für den Business-Zweck der Anwendung notwendig sind. Die Filter-Möglichkeiten, die SAP in das Basis-Produkt integriert hat, sind aber bestenfalls als rudimentär zu bezeichnen, denn einfaches Umbenennen von Dateien, bzw. das Ändern der Erweiterung trickst diese Filter bereits aus. Es können z.B. ausführbare Dateien hochgeladen werden, wo nur PDFs erlaubt sein sollten.

Aktive Inhalte
Viele Dateiformate unterstützen die Einbindung von aktiven Inhalten. Diese werden oftmals zur Automatisierung wiederkehrender Aufgaben, zur Validierung von Eingaben und für weitere sinnvolle Maßnahmen verwendet. Aus einer Web-Anwendung heraus aufgerufen, können solche aktiven Inhalte (z.B. JavaScript in SVG Grafiken oder in PDF-Dateien), die Session-Privilegien der Web-Sitzung verwenden, über die sie geladen wurden. Browser sehen diese daher als Bestandteil der Anwendung und führen solche Inhalte oftmals unter Umgehung der „Same Origin“ Sicherheitsrichtlinie aus.

Hybride Dateiformate
Solche, auch Chameleon- oder Polyglot-Dateien genannte, Dateien erfüllen die Erkennungsmerkmale mehrerer Dateitypen gleichzeitig. So kann beispielsweise aus einem GIF-Bild und einem Java-Archiv (Endung .JAR) eine „GIFAR“ Datei erzeugt werden. Eine solche Datei wird von einem Browser als normales Bild angezeigt und kann möglicherweise als Profilbild oder Avatar hochgeladen werden. Wenn diese GIFAR-Datei allerdings wie ein Java-Archiv angesprochen wird (z.B. durch Einbettung als APPLET oder OBJECT) werden die Java-Klassen aus dem Java-Archiv ausgeführt – und zwar wiederum im Sicherheitskontext der Web-Anwendung.

Wie öffentliche Verwaltungen und SAP-Kunden sich schützen können.
Die hier angesprochenen Angriffsszenarien sind weder neu, noch besonders raffiniert. Unter Security-Experten sind dies bekannte und unter Hackern bewährte Techniken. Marktführende Unternehmen, wie SAP, haben diese Risiken bereits erkannt und Ihren Kunden Möglichkeiten an die Hand gegeben, die Risiken zu minimieren. Diese erfordern aber oft den Einsatz von Drittanbieter-Produkten.

So hat SAP beispielsweise bereits 2004 in die gängigen Application-Server Varianten (ABAP und Java) eine Virenscanschnittstelle (NW-VSI) integriert. Diese wurde seither erweitert und ist in der Lage, mit einem angeschlossenen, von SAP zertifizierten Scanner-Produkt Angriffe in Dateien beim Upload und Download zu erkennen und zu blocken, die über die Erkennung von Malware hinausgehen.

Auch für den Scan von Formulardaten hat SAP eine Schnittstelle in den Internet Connection Manager (ICM/icman) integriert. Neben grundlegenden Filtermöglichkeit, die von SAP ausgeliefert wird, können auch hier Produkte von Drittanbietern den Scan der Daten übernehmen und somit ohne Änderungen am SAP Programmcode die Angriffsfläche der SAP-basierten Web-Anwendung erheblich reduzieren.

Jörg Schneider-Simon

(1) http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html

Michael Klatte, PR Manager, ESET Deutschland GmbH

Kein Saft in der Leitung: Wenn der Hacker den Strom abdreht

Angriffe von Hackern auf Kritische Infrastrukturen wie das Stromversorgungsnetz häufen sich – und sie werden immer gefährlicher. So können Cyberattacken Generatoren und Transformatoren massiv beschädigen. Stromversorgungsunternehmen und Stadtwerke müssen daher Vorkehrungen treffen.

Ohne Strom nichts los. Diese unerfreuliche Erfahrung mussten Einwohner der Ukraine bereits zwei Mal machen: Am 23. Dezember 2015 und ein Jahr später, 17. Dezember 2016. Allerdings waren in beiden Fällen nicht technische Probleme die Ursache, dass Hunderttausende von Menschen im Dunkeln saßen, Heizungen ausfielen und weder Fernsehen noch das Telekommunikationsnetz funktionierten. Vielmehr hatten sich Hacker Zugang zu Rechnern von Energieversorgungsunternehmen verschafft und über diesen Weg SCADA-Systeme (Supervisory Control and Data Acquisition) lahmgelegt.

Vom Angriff im Jahr 2015 waren mehr als 220.000 Bürger der Ukraine betroffen. In diesem Fall gelang es den Angreifern, die Workstations des Betriebspersonals zu kapern und 27 Substationen von drei Energieversorgungsunternehmen vom Netz zu nehmen. Die Attacke vom Dezember 2016 zielte dagegen auf die Hauptstadt Kiew und einen dort ansässigen Stromversorger. Die Hacker verschafften sich Zugang zu den Fernbedienungsterminals, über die das Bedienpersonal die Trennschalter steuert. Durch die Abschaltung der Terminals verursachten die Angreifer einen einstündigen Stromausfall.

Profis am Werk

IT-Sicherheitsfachleute gehen davon aus, dass in beiden Fällen Profis am Werk waren, keine Gelegenheitshacker. Denn es bedurfte einer monatelangen Vorbereitung, um Sicherheitsschwachstellen in den IT- und SCADA-Systemen sowie der Netzwerk-Infrastruktur der Stromversorger zu finden. Die Anzeichen deuten daher auf professionelle Hacker hin, die möglicherweise sogar auf die Hilfe von Geheimdiensten und staatlichen Stellen zurückgreifen konnten.

Angriffsfläche wird größer

Solche oder ähnliche Angriffe auf Stromversorgungseinrichtungen und andere „Kritische Infrastrukturen“(Kritis) wie die Wasserversorgung, wichtige Industrieunternehmen, Kliniken, den Finanzsektor, das Telekommunikationsnetz und öffentliche Verkehrssysteme fanden in den vergangenen Jahren mehrfach statt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt in seinem „Bericht zur Lage der IT-Sicherheit in Deutschland 2016“ unter anderem das Beispiel eines Atomkraftwerks an. Während der Vorbereitungen zu Revisionsarbeiten wurden dort Schadprogramme auf einem Rechner zur Darstellung und Aufzeichnung von Handhabungsvorgängen an der Brennelement-Lademaschine (Visualisierungsrechner) entdeckt. Vermutlich gelangte die Malware über einen infizierten USB-Stick auf das System. Zwar entstand dadurch im AKW kein Schaden, doch musste der Betreiber Zeit und Geld in die Analyse des Vorfalls investieren sowie die betroffenen Systeme und Datenträger reinigen.

Maßgeschneiderte Werkzeuge für Attacken auf Energieversorger

Doch die Aktivitäten von Cyberkriminellen zielen nicht nur auf die IT-Infrastruktur in den Büros von Stromversorgungsunternehmen ab. Erst vor wenigen Monaten ging den Sicherheitsforschern des europäischen Security-Software-Herstellers ESET ein Trojaner ins Netz, der es speziell auf Industrieanlagen und die Systeme von Energieversorgern abgesehen hat. Die Schadsoftware mit dem Namen „Industroyer“ (eine Kombination aus „Industry“ und „Destroyer“, also „Zerstörer“) ermöglicht es Cyberkriminellen, industrielle Steuerungssoftware (SCADA) von Umspannwerken anzugreifen.

Die Auswirkungen können beträchtlich sein: von der Unterbrechung der Stromversorgung bis hin zu physischen Schäden an Komponenten. Die Malware ist beispielsweise in der Lage, Schalter in Umspannwerken und Überstromschutzeinrichtungen zu beeinflussen. Dafür werden Kommunikationsprotokolle verwendet, die in Steuerungs- und Kontrollsystemen genutzt werden. Diese Protokolle sind nicht nur in der Stromversorgungsinfrastruktur im Einsatz, sondern auch in Verkehrskontrollsystemen und in anderen Kritischen Infrastrukturen.

Die Schalter und Schutzeinrichtungen sind digitale Äquivalente von analogen Schaltern. Eine Störung solcher Systeme und Komponenten kann weitreichende Folgen haben – vom Abschalten der Stromverteilung über kaskadenförmige Netzzusammenbrüche bis hin zu Schäden an der Hardware. Der Schweregrad der Schäden kann zudem je nach Umspannstation unterschiedlich ausfallen.

Alte Protokolle treffen auf junge Hacker

Ein Problem ist, dass die Protokolle, auf die Industroyer zurückgreift, vor Jahrzehnten entwickelt wurden. Damals waren industrielle Systeme weitgehend von der Außenwelt abgeschnitten. Konzepte wie Industrie 4.0 und Smart Metering, bei denen Maschinen, Stromzähler und Steuerungen über das Internet miteinander „sprechen“, existierten bestenfalls in den Köpfen von Forschern. Cyberkriminelle müssen also gar nicht nach Sicherheitslücken in einem Protokoll suchen, sondern ihrer Malware lediglich die Protokollsprache beibringen. Angreifer könnten die Malware außerdem mit geringem Aufwand an jede Umgebung anpassen – und das macht sie extrem bedrohlich.

Es ist unwahrscheinlich, dass eine solche Malware ohne Zugriff auf die Steuerungen oder SCADA-Komponenten geschrieben und getestet werden kann, die in einem Kraftwerk oder einer Fabrik verwendet werden. Die Autoren von Industroyer mussten demnach über spezielle Kenntnisse der industriellen Kontrollsysteme verfügen. Die ESET Forscher gehen davon aus, dass im Fall des Angriffs auf die Ukraine Ende 2016 das Netzwerk des Energieversorgers Ukrenergo infiltriert wurde. Die Hacker sammelten anschließend monatelang Daten über die Anlagen des Unternehmens. Diese Informationen übermittelte Industroyer anschließend über das Tor-Netzwerk an die Cyberkriminellen. Tor ist ein spezielles Netz, mit dem sich Nutzer anonym im Internet bewegen können.

Die Fähigkeit, sich unbemerkt über Wochen und Monate hinweg in einem System einzunisten und den Betrieb von Industrie-Hardware direkt zu stören, macht Industroyer nach Einschätzung von ESET zur gefährlichsten Bedrohung für die industrielle Infrastruktur seit Auftreten des berüchtigten Computerwurms Stuxnet. Dieser manipulierte ab 2007 unter anderem die Steuerungssysteme von Uranmühlen im Iran. Im Gegensatz zu Stuxnet lässt sich Industroyer jedoch flexibel an unterschiedliche Kritische Infrastrukturen anpassen, etwa an Steuerungsanlagen, die in Kraftwerken eingesetzt werden.

Übliche Schutzmechanismen sind nicht genug

Die große Herausforderung im digitalen Zeitalter besteht darin, dass es nur eingeschränkt möglich ist, Steuerungssysteme und Rechner in Kritis zu schützen. Viele dieser Komponenten verfügen über zu wenig Rechenleistung und Arbeitsspeicher oder veraltete Betriebssysteme, um eine Schutzsoftware einsetzen zu können. Deshalb gilt es, die Netzwerke besser gegen Angriffe zu sichern.

Im ersten Schritt ist es wichtig, das Büronetzwerk und die darin integrierten Server, PCs, Notebooks und Smartphones vor Angriffen zu schützen. Das heißt beispielsweise, solche Systeme mit einer umfassenden Endpoint-Lösung, die über einen klassischen Virenscanner hinausgeht, auszustatten und regelmäßig Updates von Betriebssystemen und Applikationen durchzuführen. So lief auf dem Visualisierungsrechner im deutschen AKW, das laut dem Bericht des BSI Opfer eines Angriffs wurde, eine veraltete Betriebssystem-Version. Nur aus diesem Grund konnte er mit einer ebenfalls veralteten Schadsoftware infiziert werden.

Daher ist es entscheidend, die Mitarbeiter für die Gefahr durch Cyberangriffe zu sensibilisieren. Denn als „Türöffner“ nutzen Hacker häufig Phishing-E-Mails mit manipulierten Anhängen. Öffnet der Empfänger eine solche Nachricht, infiziert er seinen Rechner. Wichtig ist daher neben einer effektiven Schutzsoftware ein gesundes Maß an Misstrauen, wenn eigenartige E-Mails von Kollegen im Postfach landen.

Gemeinsame Schutzkonzepte notwendig

Die größte Herausforderung stellt allerdings die unterschiedliche Ausgangslage der einzelnen Kritischen Infrastrukturen dar: Bisher verfügbare Lösungen zur IT-Sicherheit sind oftmals unzureichend auf die Bedürfnisse der Betreiber zugeschnitten. Das heißt, eine spezielle Sicherheitslösung für Energieversorger gibt es noch nicht. Daran arbeiten derzeit das BSI und UP KRITIS – eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen.

In Branchen- (BAK) und Themenarbeitskreisen (TAK) erstellen Kritis-Betreiber, Behörden und Verbände seit 2007 gemeinsame Schutzkonzepte. Der erste Sicherheitsstandard für den Sektor Wasser wurde vom BSI im August 2017 zertifiziert. Weitere Normen, etwa im Bereich „Strom“, werden folgen.

Michael Klatte

1.2 DIGITALE IDENTITÄT

1.2.1 Authentifizierung

Der Aufstieg der smarten Authentifizierung

David Vergara, Head of Global Marketing, VASCO Data Security

Unterschätze niemals die Macht von „smart“ – Das ist das Marketing-Mantra des 21. Jahrhunderts. Wir haben Smartphones, Smart TV, eine smarte Türklingel und sogar eine smarte Waschmaschine. Lassen wir den Einzelhandel aber mal beiseite und betrachten die wirklich wichtigen Dinge, wie private Informationen vertraulich zu halten, dann kommt die Frage auf: Was ist mit smarter Authentifizierung?

Smarte Authentifizierung muss einfach, bequem und sicher sein

Obwohl die Strategien für Multifaktor-Authentifizierung immer populärer werden, sind sie ein Kompromiss aus Benutzerfreundlichkeit und Sicherheit. Anders gesagt, wenn Authentifizierungslösungen nicht einfach und bequem sind, werden sie von den Usern nicht angenommen. Wenn die Lösungen allerdings nicht sicher sind, werden sie von Hackern ins Visier genommen und schaden den Nutzern.

Das ist weitestgehend der Grund, warum sogenannte smarte Authentifizierungsstrategien aufge-

Newsletter und mehr Beiträge: www.digitaleweltmagazin.de/blog

kommen sind, um sicherere und benutzerfreundliche Erfahrungen zu machen. Sie kontextualisieren das Nutzerverhalten, indem sie Verhaltensmuster vergleichen, die von ausgeklügelten Algorithmen interpoliert werden. Dazu gehören die kontinuierliche Echtzeit-Überwachung und Bewertung der Art und Weise, wie User mit ihren Computern und mobilen Geräten über Mausbewegungen, Tastenanschläge und Gesten interagieren.

Darüber hinaus, seitdem die Authentifizierung transparent abläuft, sind sich weder User noch Hacker bewusst, dass sie, nennen wir es, „forensisch überwacht“ werden und dass es nicht möglich ist, das System auszutricksen.

Kontextbasierte Authentifizierung erkennt unübliche Transaktionen anhand eines Verhaltensprofils
Die Nutzung dieser kontextuellen Daten zur Authentifizierung eines Benutzers erfordert die Analyse von Mustern, um zu bewerten, ob sie Handlungsweisen entsprechen, die der Benutzer oder Kontoinhaber in der Vergangenheit bereits gezeigt hat oder ob diese Handlungen direkt mit bekannten Hackeraktivitäten in Verbindung gebracht werden können.

So kann zum Beispiel, wenn mit dem Gerät eines Benutzers eine App an einem Ort geöffnet wird, der für Hackeraktivitäten bekannt ist, anstelle des Heimat- oder Bürostandorts des Users oder Kontoinhabers, der Zugang blockiert oder eine Step-Up-Authentifizierung vorgenommen werden. Außerdem kann der Zugriff auf ein Konto zusätzlich eingeschränkt werden, wenn die Anforderung nicht von dem Telefongerät stammt, das bereits mit der Telefonnummer des Benutzers verknüpft ist.

Das heißt nicht, dass Multifaktor-Authentifizierung letztendlich zu abnehmendem Ertrag führt. Ganz im Gegenteil. Wenn das System eine Unregelmäßigkeit in den Mustern des Userverhaltens feststellt, könnten zusätzliche Authentifizierungen (z.B. das Benutzen eines Einmalpassworts, kurz OTP für One Time Pad, das per SMS versendet wird) angefordert werden, bevor der Zugriff gewährt wird. Dadurch authentifizieren sich User nur selbst, wenn sich ihr erwartetes Verhaltensmuster ändert. Gleichzeitig wird das Nutzungserlebnis verbessert und der Wert der Sicherheitsstrategie verstärkt, was nicht nur praktisch, sondern auch benutzerfreundlich ist.

Man kann festhalten, dass sich das Verhalten eines Nutzers zwar ändern kann, er aber immer noch dieselbe Person bleibt.

Sind kontextbasierte Authentifizierung und verhaltensbezogene biometrische Daten nun die ersten smarten Lösungen, an der Schwelle zu einer weiten Verbreitung oder befinden sie sich doch noch irgendwo dazwischen?

Während es sicherlich eher darum geht, in ausgewählten industriellen Nischen Fuß zu fassen, wird der globale Markt für verhaltensbezogene biometrische Daten laut Branchenanalysten im Zeitraum 2016-2020 jährlich um 17,34% wachsen.

Erste Umfrageergebnisse: Biometrische Sicherheit vor Passwörtern
Es gibt bereits erste Studienergebnisse zu der Frage, wie smarte Authentifizierung in der realen Welt angenommen wird.

Eine vom Marktforschungsinstitut YouGov durchgeführte Online-Umfrage hat herausgefunden, dass 56% der Konsumenten im Vereinigten Königreich biometrische Sicherheit gegenüber traditionellen Lösungen wie Passwörtern, vorziehen, um sich online in ihr Bankkonto einzuloggen. In der Tat bevorzugen 33% der Befragten die Fingerabdruckerkennung, um Zugang zu ihren Konten zu erhalten, gefolgt von Irisscanner und Gesichts- und Stimmerkennung. Es überrascht nicht, dass nur 19% der Umfrageteilnehmer Passwörter und sogar noch weniger selbst gewählte Sicherheitsfragen benutzen. Beide Möglichkeiten werden durch den Komfort und die Sicherheit, die biometrische Authentifizierung bietet, verdrängt.

Für die Nutzer von mobilen Banklösungen ist das eine besonders wichtige Entwicklung, da Passwörter die Vorstufe für eine völlig neue Generation von Authentifizierungsmöglichkeiten sind. Das gilt insbesondere, wenn sich Mobiltechnologie weiterentwickelt und Banken und weitere Finanzinstitute versuchen, Verbrauchernachfragen nach biometrischen Sicherheitslösungen mit ihrer Verfügbarkeit zu vereinbaren.

In diesem neuen „Zeitalter des Kunden“ kann es sehr gut sein, dass ein mehrschichtiger Ansatz, einschließlich verhaltensbezogener biometrischer Daten und Geräteerkennung, die sicherste Grundlage darstellt, auf der positive Kundenerfahrungen aufgebaut werden kann.
Kurz gesagt, smarte Geräte sind gut und schön und sie werden in absehbarer Zeit sicher nicht verschwinden. Dennoch werden sie, wenn sie durch smarte Authentifizierung ergänzt werden, Benutzerfreundlichkeit und Sicherheit gleichermaßen erreichen. Und das hält letztendlich eine produktive, sichere und langlebige Kundenbeziehung aufrecht.

David Vergara

Schlüsselmanagement als zentrale Herausforderung der IoT-Security

Eine Vielzahl erfolgreicher Angriffe auf IoT-Geräte nutzen Schwachstellen im Schlüsselmanagement aus und ermöglichen so eine Skalierung dieser Angriffe auf ganze Produktserien oder –chargen. Im Laufe der Zeit kommen immer mehr vernetzte Produkte auf den Markt, wodurch sich der Anspruch an die security und privacy erhöhen sollten. Es ist aber zu beobachten, dass die Hersteller der verschiedensten IoT-Devices nicht einmal die Basics der kryptographischen Sicherheit sauber umsetzen und somit fahrlässig für die Sicherheit des gesamten Internets handeln. Die kompromittierten Geräte werden häufig für Bot-Netze und Distributed Denied of Service (DDOS) genutzt, wodurch die Stabilität des Internets gefährdet wird. Ein DDoS-Angriff ist eine spezielle Art der Cyber-Kriminalität, welcher oft genutzt wird, um Lösegelder zu erpressen. Die Angreifer rufen eine Nichtverfügbarkeit eines Dienstes oder Servers herbei. Die schlecht geschützten IoT Geräte werden missbraucht, um von dort aus die Infrastruktur des Unternehmens mit hohen Mengen an Anfragen zu überladen. Das Netz ist als Folge dessen überlastet und Internetleitungen sind kaum noch nutzbar. (DDoS-Attacken: Wenn Angreifer die Webseite lahmlegen, 2011)

Viele große Konzerne sind immer wieder von DDOS-Attacken betroffen. So beispielsweise DHL, Ebay, Hermes und Alditalk. Diese Unternehmen wurden im Jahr 2017 von einer Gruppe jugendlicher, welche sich die „XMR-Squad“ nennt, angegriffen. Diese verlangten Lösegelder, für das Entlasten der Websites. DDoS Attacken sind nur ein Beispiel, weshalb die Sicherheit der IoT Geräte so wichtig ist. Angriffe wie die DDOS-Attacken sind vor allem deshalb so gefährlich, weil sie mit geringem Aufwand, meist unbemerkt und von überall aus der Welt ausgeführt werden können. Selbst große Websitebetreiber wie Google gehen vor den Attacken in die Knie. (DDoS-Erpresser: XMR-Squad greift deutsche Unternehmensseiten an, 2017) Im Jahr 2016 gaben rund 35% aller deutschen Unternehmen an Probleme mit DDoS Attacken gehabt zu haben. Somit wurde jedes dritte deutsche Unternehmen im vergangenen Jahr Opfer eines solchen Angriffs. Obwohl ein weiteres Drittel dieser Betroffenen angibt, dass es in der Summe mehr als zehn registrierte Angriffe waren, werden nur 28% aller deutschen Unternehmen aktiv im Schutz gegen Cyber-Kriminalität (Miridakis, 2017). Die Vorkommnisse reichen so weit, dass Begrifflichkeiten wie „Internet of evil things“ auftauchen und unterstreichen sollen, wie fahrlässig mit dem Aspekt der Sicherheit umgegangen wird. (‘IoT Hall-of-Shame’, 2017)

Die Physec GmbH, gegründet im April 2016, stellt sich dieser Problematik und offeriert maßgeschneiderte Lösungen für IoT-Devices. Ihre Ursprünge liegen an dem Horst Görtz Institut für IT-Sicherheit (HGI) in Bochum, als eines der weltweit führenden Forschungseinrichtungen im Bereich der IT-Sicherheit mit aktuell fast 20 Professoren und dem größten Bachelor/Master-Programm in Europa.

Heiko Koepke, Mitgründer, Geschäftsführer, Physec GmbH

Die Forschungsergebnisse von Dr. Christian Zenger und die Teilnahme am EXIST-Forschungstransfer des BMWi ermöglicht die Weiterentwicklung der Produkte auf Grundlage der PHYSEC-Technologie. Die zentrale Motivation für unsere Arbeit ist die digitale Selbstbestimmung unserer Kunden, durch die erfolgreiche Umsetzung digitaler Geschäftsmodelle mit höchster IT-Sicherheit und einfacher Anwendung. Der Kontext der cyber security ist somit das Kerngeschäft der Physec GmbH. Durch den Lösungsansatz der Security Middleware IoTree wird Sicherheit für ressourcenschwache Kleinstgeräte der im IoT ermöglicht.

In der Zeit der dritten Welle der Digitalisierung, ist das Internet of Things ein all gegenwärtiges Thema. Sowohl in den großen Industrien, als auch im privaten Kontext werden sämtliche Maschinen und Nutzgegenstände „smart“. Sie kommunizieren mit der Umwelt. Das Problem dabei ist, dass die neuen Geräte häufig an den Markt gebracht werden, ohne ausreichend hohe cyber security gewährleisten zu können. Ein solch schwaches Glied in der Kette kann und wird von Kriminellen für bereits besprochene Aktivitäten genutzt. Bisher bot der Markt zwei Lösungsansätze für das Sichern von IoT-Devices, wobei keine der Lösungen final für Sicherheit sorgen konnte. Dadurch eingeläutet, lässt sich der IoTree-Lösungsansatz klar von der Konkurrenz abgrenzen. Bisher gab es zwei Ansätze der Schlüsseletablierung und des –managements, die einfache aber mit Sicherheitsproblemen behaftete „Factory default Key“ (PSK) und die sicheren aber sehr komplexen „Public-key Infrastructur“ (PKI). Bezüglich des PSK Ansatzes erkennt man eklatante Schwachstellen, die eine starke Motivation für Angreifer begründen. Dabei ist nicht nur der Angriff an sich das Problem, sondern die Skalierbarkeit dessen und die damit verbundenen Implikationen. Auf Grund von einheitlicher Identifikationen und Schlüsseln, skalierte ein etwaiger Angriff schnell und wenig kontrollierbar. Das Ziel einer einfach integrierbaren Lösung funktionierte nur auf Kosten der Sicherheit. Der Ansatz der PKI ist deutlich sicherer, da hierbei individuelle Schlüssel für jedes Gerät verwendet werden. Dabei wird aber das Problem aufgeworfen, dass in den Produktionsprozess eingegriffen werden muss, und somit hoher Aufwand und Risiken für die Supply Chain entstehen. Hohe Anforderungen an die Infrastruktur einer PKI sorgen für hohe Kapitalbindungen, Verzahnung von IT und Produktion sowie hohen administrativen Aufwand. Unternehmen, die vernetzte Produkte anbieten scheuen hohe Aufwendungen der PKI und die Notwendigkeit des Eingriffes in den Produktionsprozess, weshalb häufig PSK verwendet werden.

Die Problematiken der beiden Ansätze auszumerzen war die Zielsetzung des Projektes IoTree. Das Ergebnis ist eine Lösung des Problems, die sowohl sicher, als auch einfach anwendbar und kostengünstig ist. Die Security Middleware IoTree ist eine branchenunabhängige Lösung, die eine digitale Datenerfassung und Geschäftsmodelle schnell, sicher und einfach realisiert. Für die Digitalisierung von Produkten und Prozessen bietet IoTree ein umfassendes und konnektivitätsunabhängiges Sicherheitskonzept von der dezentralen Schlüsseletablierung, über die Authentifizierung bis zur starken Kryptographie. Beginnend beim Produktionsprozess, der durch die einzigartige dezentrale Schlüsseletablierung nicht beeinflusst wird, ermöglicht IoTree durch das Management von Schlüsseln und Identitäten die nötige Sicherheit. Wie bereits erörtert, ist oft die Sensitivität für Sicherheit noch nicht vorhanden oder nur sehr gering. Dies resultiert darin, dass bspw. Industrien die Sicherheitsvorkehrungen nur treffen werden, wenn der Aufwand möglichst gering ist. Dies schafft den perfekten Übergang zu einer weiteren Besonderheit der IoTree. Die Anwendbarkeit des IoTree überzeugt dadurch, dass nur geringes technisches Know-how zur Anwendung notwendig ist. Die Konfiguration geschieht per App, welche auf einem Smartphone zu installieren ist. Nach kurzer Befolgung der App-Anweisungen lässt sich eine Konfiguration in wenigen Minuten abschließen. Die Produkte werden durch den registrierten Anwender intuitiv bspw. in das lokale WLAN integriert und zeitneutral authentifiziert. So erhalten die Produkte ihre individuellen kryptographischen Identitäten, wobei das Smartphone als nicht vertrauenswürdig klassifiziert wird und somit kein privates kryptographisches Material sieht. IoTree besteht aus insgesamt drei Softwarekomponenten (Embedded für Gerät, Smartphone-App, Backend) und erfordern keine Aufrüstung der Hardware. Updates der Software über das Over-the-Air system erfolgen und erfordern keine physikalische Präsenz und Terminvereinbarungen. Die technische Finesse in Form der authentischen Schlüsseletablierung und kryptografischen Featureaktivierungen ist bei Benutzung der IoTree sehr benutzerfreundlich. Durch leichte und schnelle Integration der Middleware IoTree entsteht nur sehr geringer betrieblicher und organisatorischer Aufwand. Die Kombination aus einfacher Integration und starker Sicherheit schafft den Weg zur erfolgreichen, und vor allem sicheren Digitalisierung.

Im B2C Segment des IoT ist vor allem die Smart Home Technologie ein prägnanter Anwendungsbereich. Der Markt wächst schnell an, wobei die IT-Sicherheitskonzepte meist unzureichende Schutzmechanismen benutzen, wodurch Angriffe stark über die gesamte Produktpalette skalieren. IoTrees Sicherheit, durch Schlüsselgenerierung bei Inbetriebnahme, sowie die über Zeit und User wechselnden kryptographischen Schlüssel ermöglichen genügend Sicherheit für neue Geschäftsmodelle wie „remote Control“, „Pay per use“ usw. Ein weiteres Segment mit großem Potential ist die Industrie 4.0. Hierbei handelt es sich um ein Segment, in dem die zu behandelnden Informationen über Industrie- und Produktionsprozesse besonders schützenswert sind. Die Risiken einer Industriespionage gilt es zu minimieren, wobei gleichzeitig alle Vorteile der Digitalisierung geschickt genutzt werden sollen, um Prozesse zu optimieren und Kosten zu senken. Authentisierungslösungen von Physec erlauben das einfache Einrichten von starker Verschlüsselung, sodass potentielle Fehler durch Anwender und Wartungsarbeiter verhindert werden. Zu guter Letzt ist auch der KRITIS (Kritische Infrastruktur) Bereich ein sehr interessanter. Die Gefahren für kritische Infrastrukturen wie Energieversorger, Wasserversorgung und – Entsorgung liegen in der Vernetzung zentraler Kontrollzentren, welche aus der Ferne Funktionen und Prozesse steuern. Vor allem Wasserver- und Entsorger sind oft im Visier von Angreifern, und könnten durch Absicherung der wichtigsten Sensoren, Aktoren, Schieber sowieso Pumpen durch IoTree, mehr Sicherheit erlangen.

Abschließend lässt sich konstatieren, dass die Physec GmbH einen, der Konnektivitäts- und Cyber-Sicherheitswünschen angepassten Schutz für ressourcenbeschränkte Geräte bietet. Bisher angebotene Technologien zum Schutz dieser Geräte sind einfach umzusetzen oder sicher, wobei sich häufig für die geringe Komplexität und damit korrespondierenden geringen Sicherheit entschieden wird. Das Herausbringen unsicherer und somit zweckentfremdeter IoT-Geräte stellt eine ernstzunehmende Bedrohung für das gesamte Internet dar. Die Physec GmbH hat sich zum Ziele gesetzt, durch die Security Middleware IoTree, die Sicherheitslücken dieses Bereichs zu schließen. Kritische Infrastrukturen sollen durch einfach anwendbare Sicherheitslösungen besser geschützt sein. Heiko Koepke

Literaturverzeichnis
DDoS-Attacken: Wenn Angreifer die Webseite lahmlegen (2011) computerbetrug.de – Infos über Gefahren des Internet. Available at: http://www.computerbetrug.de/sicherheit-im-internet/ddos-attacken (Accessed: 11 October 2017).
DDoS-Erpresser: XMR-Squad greift deutsche Unternehmensseiten an (2017). Available at: http://winfuture.de/news,97259.html (Accessed: 11 October 2017).
'IoT Hall-of-Shame' (2017) The Code Curmudgeon. Available at: http://codecurmudgeon.com/wp/iot-hall-shame/ (Accessed: 12 October 2017).
Miridakis, V. (2017) 2016: Mehr als 30.000 DDoS-Attacken in Deutschland, it-daily.net. Available at: https://www.it-daily.net/it-sicherheit/cyber-defence/14158-2016-mehr-als-30-000-ddos-attacken-in-deutschland (Accessed: 12 October 2017).

1.2.2 Visionen

Was man an IAM heute haben muss – und was als Nächstes kommt

Identity und Access Management (IAM) ist mittlerweile eine etablierte Fähigkeit in den IT-Infrastrukturen mittlerer und großer Unternehmen. Allerdings ist es mit grundlegenden Provisioning-Diensten und ein bisschen Access Governance längst nicht mehr getan.

Eine effektive und effiziente Verwaltung von Benutzern und ihren Zugriffsberechtigungen ist für die Benutzerfreundlichkeit, die Administrationseffizienz, die Erfüllung von Compliance-Anforderungen und die Reduktion von IT-Sicherheitsrisiken unverzichtbar. Die Anforderungen wachsen aber stetig, wobei zwei Treiber besonders wichtig sind. Zum einen wachsen die Bedrohungen durch Cyberangriffe stetig. Zum anderen wird mit der zunehmenden Digitalisierung die engere Zusammenarbeit mit Kunden und Geschäftspartnern immer wichtiger, weshalb es beim IAM längst nicht mehr nur um die Verwaltung von Mitarbeitern und ihren Berechtigungen geht.

Die Grundlage: Was man heute an IAM haben muss

Wenn man heute ein gutes Basisniveau, also die „Baseline“, für die erforderliche IAM-Funktionalität definieren möchte, dann gibt es hier fünf Bereiche, die auf einem guten Niveau adressiert sein müssen.

Die Basis bilden Verzeichnisdienste, von denen es wenige zentrale Verzeichnisse mit klar abgegrenzten Funktionen geben sollte, also beispielsweise neben dem meist vorhanden Microsoft Active Directory noch ein zentrales „Corporate Directory“ für die Mitarbeiter und Verzeichnisse für Geschäftspartner und Kunden.

Ein Identity Provisioning, mit dem Benutzer automatisch oder indirekt, über Schnittstellen zum IT Service Management, manuell provisioniert werden mit einer vollständigen Unterstützung der Prozesse ist zwingend. Zu einem Prozess-Framework gehört die detaillierte Beschreibung der Prozesse ebenso wie die Unterstützung beispielsweise von Wechselprozessen im Unternehmen und das Management von verwalteten Anwendungen oder Rollen.

Auch Access Governance-Funktionen sind heute ein Muss. Je nach regulatorischen Anforderungen müssen diese unterschiedlich stark ausgeprägt sein. Eine vollständige Übersicht über den aktuellen Status von Berechtigungen gehört aber in jedem Fall ebenso dazu wie ein regelmäßiger Review oder eine erneute Genehmigung von Zugriffsrechten.

Die wohl häufigste Lücke besteht derzeit immer noch im Bereich des Privilege Management, also bei speziellen Funktionen für die Verwaltung und Kontrolle von privilegierten Benutzern und gemeinsam genutzten Benutzerkonten und deren Kennwörtern. Letztere ist ebenso zwingend wie eine Basisfunktionalität für die Überwachung von privilegierten Zugriffen zur Laufzeit, das Session Management.

Schließlich zählen auch das Web Access Management für die Authentifizierung und Autorisierung von Zugriffen auf Web-Anwendungen, Web Application Firewalls und eine zumindest grundlegende Unterstützung von Identity Federation-Standards zum Muss beim IAM.

Wer in diesen grundlegenden Bereichen noch Lücken oder Schwächen wie beispielsweise eine unkoordinierte Vielzahl von Verzeichnisdiensten oder mangelhafte Prozesse im Provisioning hat, muss handeln.

Martin Kuppinger, Founder and Principal Analyst, KuppingerCole

Die nächsten Schritte: Neue Themen im IAM

Auch das IAM bleibt natürlich nicht von den grundlegenden Entwicklungen in der IT unberührt, mit dem Trend hin zu mobilen Zugriffen, zu flexiblen und in mobile Endgeräte integrierten Authentifizierungsfunktionen oder zu Apps, die über sogenannte APIs (Application Programming Interfaces, Programmierschnittstellen) zugreifen, weshalb man dann wissen muss, wer die Apps nutzt, um die APIs entsprechend absichern zu können.

Darüber hinaus gibt es aber mehrere große Trends im IAM, die für Unternehmen immer wichtiger werden und bei der Strategie und Roadmap für IAM eingeplant und schließlich, soweit für das jeweilige Unternehmen erforderlich, in konkrete Projekte münden müssen.

Die schon angesprochene Verwaltung von Kunden und Geschäftspartnern im Rahmen der Digitalen Transformation ist dabei an erster Stelle zu nennen. IAM ist längst nicht mehr nur auf die Mitarbeiter beschränkt. Es wird immer wichtiger, den Konsumenten zu kennen, seine Identität in den internen Systemen beispielsweise mit der aus sozialen Netzwerken zu verknüpfen und die Schnittstelle bis hin zur Marketing-Automatisierung zu schaffen. CIAM (Consumer IAM) ist eines der dominierenden Themen der aktuellen Entwicklung. Das IAM muss die Flexibilität schaffen, um Kunden, Partner und ihre Zugriffe in neuen Geschäftsmodellen zu unterstützen.

Unverzichtbar und damit zunehmend eine Grundfunktionalität von IAM ist auch die Unterstützung von Cloud-Diensten, also beispielsweise ein Single Sign-On für Benutzer über verschiedene Cloud-Dienste hinweg, die Provisionierung von Benutzern, die Zugriffssteuerung und auch Access Governance-Funktionalität für diese Dienste. Auch das Privilege Management bekommt im Kontext der Cloud nochmal einen neuen Stellenwert, weil es bei vielen Cloud-Diensten nur gemein-

sam genutzte administrative Konten und oft sehr grob-granulare Berechtigungskonzepte gibt, so es andere Ansätze für die Einschränkung und Überwachung solcher Zugriffe – eben das Privilege Management – benötigt.

Auch im Bereich der Access Governance steht die Zeit nicht still. Viele Ansätze sowohl für das Rollenmanagement als auch die regelmäßige Rezertifizierung haben sich als zu ineffizient erwiesen. Die automatische Vergabe von Berechtigungen über Richtlinien, risikogesteuerte und fokussierte Ansätze für die Prüfung von Berechtigungen, leistungsfähigere Analysen über „Access Intelligence“ oder die zeitlich beschränkte Berechtigungsvergabe sind einige der Wege, die aus diesem Dilemma führen. Kurz gesagt: Die Access Governance-Ansätze müssen in praktisch allen Unternehmen daraufhin überprüft werden, ob sie mit vernünftigem Aufwand wirklich das erforderliche Resultat liefern. Ein weiteres, immer wichtigeres Feld ist die sogenannte Data Governance, bei der es um die Steuerung und Kontrolle von Berechtigungen auf unstrukturierten Daten, also beispielsweise auf File-Servern, geht.

Dazu gehört auch die Integration mit dem Privilege Management, um privilegierte Benutzer und beispielsweise die Zuordnung von gemeinsam genutzten Benutzerkonten zu zuständigen „Managern“ im Access Governance, aber auch in den Provisioning-Prozessen, mit berücksichtigen zu können. Darüber hinaus rücken erweiterte Funktionen wie die Überwachung und Analyse der Nutzung von privilegierten Benutzerkonten (Privilege Behavior Analytics) und das Management von privilegierten Zugriffen und Anwendungen auf Endgeräten (Endpoint Privilege Management) zunehmend ins Blickfeld.

Während starke Authentifizierung zumindest in Teilbereichen inzwischen fast in jedem Unternehmen zu finden ist (oder zumindest zu finden sein sollte), geht die Entwicklung hier weiter hin zur adaptiven Authentifizierung. Diese ist gleich in zweierlei Hinsicht anpassungsfähig. Einerseits geht es darum, unterschiedliche Authentifizierungsmechanismen in flexibler Weise zu unterstützen, was insbesondere im Hinblick auf die Vielfalt und ständigen Innovationen bei in mobile Endgeräte integrierter starker Authentifizierung essentiell ist. Zum anderen geht es aber auch darum, dass eine adäquate Authentifizierung abhängig vom Risiko gewählt wird. Wer auf sensitive Informationen zugreift, muss stärkere Authentifizierungsmechanismen nutzen oder mehrere Verfahren kombinieren.

Ein Revival erlebt derzeit das Themenfeld der dynamischen Autorisierung, das oft auch unter dem (viel zu engen) Stichwort ABAC (Attribute Based Access Control) positioniert wird. Dabei geht es darum, Autorisierungsentscheidungen zur Laufzeit auf Basis von Richtlinien durchzuführen, also beispielsweise bestimmte Transaktionen nur Benutzern ab einer definierten Hierarchieebene zu erlauben. Die dynamische Autorisierung ermöglicht es, Autorisierungslogik aus dem Code von Anwendungen hin in zentrale Autorisierungssysteme zu verlagern, was die Sicherheit, die Effizienz in der Anwendungsentwicklung und auch die Prüfbarkeit von Anwendungen erhöht.

Diese Entwicklung steht in engem Zusammenhang mit Anwendungssicherheitsinfrastrukturen, die eigentlich längst gute Praxis sein müssten. Anwendungssicherheitsinfrastrukturen entkoppeln die Anwendungen von den darunterliegenden Sicherheitsdiensten, indem sie Schnittstellen, aber auch vordefinierten Module beispielweise für das Zurücksetzen von Kennwörtern oder die Registrierung von Benutzern bereitstellen, die von Anwendungen und Apps genutzt werden können. Richtig gemacht, kann die darunter liegende Infrastruktur weiterentwickelt werden, ohne dass dies zu Änderungen bei Anwendungen führt, während Anwendungen und Apps einfach ein hohes und einheitliches Maß an Sicherheitsfunktionen – über IAM hinaus bis hin zu Verschlüsselung und anderen Diensten – nutzen können. Auch die API-Sicherheit, also spezielle Funktionen zur Verwaltung und zum Schutz von Zugriffen anderer Anwendungen und Apps über APIs, zählen zu diesem Themenbereich.

Es gibt viel zu tun – Stillstand beim IAM kann man sich nicht leisten

Alle diese Trends und neuen Themenfelder im IAM sind eng verbunden mit den Treibern für das IAM, insbesondere der Reduktion von Risiken beim Zugriff auf Anwendungen und Daten und der Erfüllung regulatorischer Vorgaben. Der so oft geforderte „Stand der Technik“ entwickelt sich. Gleichzeitig verändern sich aber auch die Anforderungen durch mobile Endgeräte und Apps, die Einbindung von Konsumenten, Kunden und Partner in Geschäftsprozesse sowie neue Geschäftsmodelle und durch die vermehrte Nutzung von Cloud-Diensten kontinuierlich. Das IAM muss hier nicht nur Schritt halten, sondern ist immer mehr die Basis dafür, dass man den schnellen Wandel in der Digitalen Transformation bewältigen kann und gleichzeitig ausreichend sicher ist.

Deshalb gilt es, heute die Strategie und Roadmap für die weitere Evolution der IAM-Infrastruktur zu definieren und die Projekte zu budgetieren und umzusetzen. Noch mehr gilt das natürlich, wenn man nicht einmal die grundlegenden Dienste vollständig umgesetzt hat und damit noch nicht den Stand der Technik erreicht hat.

Martin Kuppinger

1.3 ANGEWANDTE SICHERHEIT

1.3.1 Sicherheits-empfehlungen

Sieben Tipps, wie Sie Datenschutzverletzungen vorbeugen können

Zu Datenschutzverletzungen kommt es oft, wenn sich die Netzwerk-Sicherheit auf den Netzwerk-Rand konzentriert, aber im Netzwerk selbst ein gleichwertiger Schutz fehlt. Sicherheitsexperten haben sich lange Zeit nur mit der Security am Perimeter beschäftigt. Ob physischer Randbereich, Rechenzentrum, Web Services, Anwendungen oder Cloud-Umgebungen – geschützt wurde häufig nur vor externen Bedrohungen, während innerhalb des Netzwerks „Tür und Tor“ offenstanden. Die Netzwerk-Sicherheit folgte ganz dem Motto: „Harte Schale mit weichem Kern“. In einem solchen Szenario haben Angreifer, die die harte Schale „knacken“, im Netzwerk leichtes Spiel und können oft unbemerkt wertvolle Daten abgreifen. Was können Unternehmen tun, damit ihnen so etwas nicht passiert?

1. Datendiebstahl durch Sicherheitspraktiken verhindern

Viel zu viele Unternehmen vernachlässigen die Anwendung von Patches und haben keine Sicherheitspraktiken. Zugleich wachsen Netzwerke rasant und umfassen heutzutage unterschiedlichste Ecosystems – vom IoT bis zur Cloud. Die Inventarisierung des Gerätebestands und die Pflege einer solchen Datenbank können dabei zur Herausforderung werden. Trotz des damit verbundenen Aufwands ist die Anwendung von Patches keine Option, sondern ein Muss. Im Idealfall würde dies automatisiert, nachverfolgbar und mit der Möglichkeit einer Erfolgskontrolle stattfinden. Weiter sollte ein Prozess implementiert werden, um die Systeme zu ersetzen oder offline zu nehmen, bei denen keine Patches (mehr) angewendet werden können.

2. Netzwerk-Schutz mit Signaturen

Auch wenn neue Angriffsformen eine echte Gefahr darstellen, erfolgen die meisten Datenschutzverletzungen durch Attacken, die seit Wochen, Monaten oder manchmal sogar Jahren bekannt sind. Tatsächlich nutzen die meisten Angriffe Schwachstellen aus, für die es durchschnittlich seit drei Jahren einen Patch gibt und die in vielen Fällen seit mehr als zehn Jahren existieren. Weil aber diese Schwachstellen bekannt sind, lassen sich Angriffe und Exploits über solche Sicherheitslücken an der Signatur erkennen. Mit signaturbasierten Erkennungstools können Unternehmen schnell nach „versuchten Einbrüchen“ suchen, diesen einen „Riegel vorschieben“ oder die Ausführung eines Exploits blockieren, der bekannte Schwachstellen ausnutzen will.

3. Zero Day Threats mit verhaltensbasierten Analysen eindämmen

Neuartige ausgefeilte Angriffe nutzen zahlreiche Techniken, um Schutzmaßnahmen zu umgehen und unerkannt ins Netzwerk einzudringen. Verhaltensbasierte Security-Tools können unangemessenen oder unerwarteten Traffic sowie „verhaltensauffällige“ Geräte erkennen, Zero-Day-Malware-Varianten mit Detonationskammern oder Sandboxing unschädlich machen und Daten korrelieren, um intelligente Angriffe zu entlarven und abzuwehren. Dank Fortschritten bei der absichtsbasierten Sicherheit („Intent-based Security“) können nicht nur Daten und Anwendungen netzwerkweit auf Malware überprüft, sondern auch umfassend inspiziert werden. Solche Lösungen suchen nach Mustern und überwachen dann kontinuierlich den Traffic, um die Absicht festzustellen. Intelligente Security-Systeme können so einen Angriff proaktiv im Keim ersticken, bevor er überhaupt begonnen hat.

Christian Vogt, Senior Regional Director Germany, Fortinet

4. Web Application Firewalls installieren

Während viele Angriffe weiterhin mit „bewährten“ Methoden – wie Phishing per E-Mail oder über bekannte, ungepatchte Schwachstellen – in Netzwerke eindringen, gehen zahlreiche Bedrohungen mittlerweile auch unkonventionelle Wege. Webbasierte Angriffe werden immer häufiger. Oft wird dabei das exponentielle Wachstum bei Anwendungen ausgenutzt. Besonders im Visier steht Software, die Informationen direkt im Rechenzentrum abfragt und auswertet. Web Application Firewalls (WAF) wurden eigens für eine tiefgehende, leistungsstarke Überprüfung des Datenverkehrs von Web Apps entwickelt und sind der herkömmlichen NGFW-Technologie weit überlegen.

5. Threat Intelligence nutzen

Mit moderner Threat Intelligence können Unternehmen Bedrohungen nicht nur schneller erkennen, sondern auch umgehend darauf reagieren. Es gibt zahlreiche Threat Feeds, die Unternehmen bei Bedrohungstrends und der Erkennung von Exploits auf dem neuesten Stand halten. Die Herausforderung besteht darin, diese Daten in nützliche Informationen umzuwandeln und übergreifende Korrelationen zu lokalen Informationen und zur örtlichen

Christoph Maier, PR & Marketing Manager, Hornetsecurity

Infrastruktur herzustellen. Bereitstellungstools wie SIEM- oder WAF-Technologien können solche Daten konsumieren und daraus umsetzbare Richtlinien ableiten, um das Netzwerk zu schützen. Zugleich sollten Unternehmen den Beitritt zu einem Expertenkreis erwägen und den Erfahrungsaustausch mit Branchenkollegen suchen. So erhalten sie relevante Informationen zu Threat Intelligence und können erkannte Gefahren mit Unternehmen aus der Branche teilen.

6. Keine Punktlösungen

Angesichts der raschen Erweiterung von Netzwerken, deren dynamischer, elastischer Natur und der Verlagerung von einem einzigen Netzwerk-Rand hin zu dutzenden – oder sogar hunderten – potenziellen Punkten für den Netzwerk-Zugang und den Datenaustausch ist eine herkömmliche Sicherheitsstrategie mit Geräten oder Plattformen, die nur an bestimmten Punkten des Randbereichs oder im Rechenzentrum Sicherheit bieten, nicht mehr ausreichend. Heutige raffinierte, hochintelligente Multi-Vektor-Bedrohungen verlangen nach Security-Lösungen, die sich über ein einziges, geschlossenes System vernetzen, sich an elastische Netzwerk-Architekturen anpassen und die gesamte Infrastruktur abdecken können. Diese dynamische Integration bietet Transparenz über das gesamte Netzwerk. Ein integriertes Security-Framework vernetzt Sicherheitstools, damit diese Informationen teilen und in Beziehung setzen können. Auch wird damit eine zentrale Orchestrierung und Verwaltung sowie die einheitliche Verbreitung von Richtlinien möglich. Aber was noch wichtiger ist: Sie verfügen über eine koordinierte Reaktion auf Angriffe.

7. Segmentierung Ihres Netzwerks

Heutige Netzwerke müssen mit dem Zugriff durch wechselnde Geräte sowie unterschiedlichsten Anwendungs- und Datenflüssen klarkommen. Unternehmen können ihre Sicherheit durch die Installation von Internal Segmentation Firewalls (ISFW) enorm stärken. Diese verhindern die Verbreitung von Bedrohungen unabhängig davon, ob der Security-Perimeter durchbrochen, ein Zugriffspunkt kompromittiert oder der Angriff aus dem Inneren des Netzwerks gestartet wurde. ISFWs können vor bestimmte Server geschaltet werden, auf denen sich wertvolle Geschäftsinformationen befinden. Sie können aber auch Geräte von Benutzern oder Web Apps in der Cloud schützen oder den Datenverkehr zwischen unternehmensinternen Funktions- oder Geschäftsbereichen absichern. Ohne Tools für die Segmentierung und Erkennung können Angreifer ungehindert Daten sammeln, zerstören und abgreifen. Eine interne Segmentierung, Mikrosegmentierung und Kontrollen, um z. B. Verhalten oder Workflows zu überwachen, sind für heutige datenzentrierte digitale Unternehmen unverzichtbar.

Zu viele Unternehmen haben zwar moderne Netzwerk-Designs, setzen aber beim Netzwerk-Schutz weiterhin auf isolierte Sicherheitslösungen und -Strategien der zweiten Generation. Doch gerade heutzutage darf die Sicherheit nicht stiefmütterlich behandelt werden. Planung, Mitarbeiter, Prozesse und adaptive Security-Technologien müssen eine Einheit bilden, die sich dynamisch für heutige digitale Netzwerke skalieren lässt und die automatisch als ein einziges, integriertes System raffinierte Cyberbedrohungen effektiv abwehren kann.

Christian Vogt

Machtlos gegen Ransomware & Co.?

Die Deutsche Bahn, die Schiffsreederei Maersk, oder das MDAX-Mitglied Leoni – die Liste an teils prominenten Opfern von Erpressersoftware, der Chefmasche oder anderen Cyberangriffen per E-Mail steigt gefühlt seit einigen Monaten stetig an. Nicht selten erreichen die Schäden bei solchen Angriffen siebenstellige Zahlen. Dadurch stellt sich zwangsläufig die Frage: Wenn selbst globale Unternehmen es nicht schaffen, sich vor solchen Angriffen wirksam zu schützen, wie sollen sich dann kleinere und mittelständische Firmen davor wappnen? Oder sollten sie kapitulieren und fatalistisch darauf warten, dass ein Angreifer die Unternehmensdaten und -netzwerke kapert und lahmlegt?

Sicherlich sind solche Überlegungen wenig hilfreich, dennoch ist eines augenscheinlich: Die Zeiten, in denen ein klassischer Spamfilter ausreichte, um sich vor gefährlichen E-Mails zu schützen, sind vorbei. Lag die Zahl an „normalen“ Spammails auf den gesamten E-Mail-Verkehr betrachtet vor acht Jahren bei nahezu 100 Prozent und waren Virenmails nahezu nicht existent, hat sich diese Zahl nun deutlich verändert. Der Anteil an Spamnachrichten ist auf etwa 60 Prozent gesunken, während sich im gleichen Zeitraum der Anteil an E-Mails mit Schadsoftware etwa verzehnfachte. Das Geschäftsfeld mit betrügerischen E-Mails hat sich also in Richtung von Dateianhängen mit bösartigen Absichten verschoben. Doch was bedeutet das für die Sicherheit von Unternehmen und Konzerne?

Eindringlinge auf dem Rücken der E-Mail

Generell ist die E-Mail nach wie vor der Angriffsvektor Nummer eins für Cyberkriminelle. Der Unterschied ist jedoch, dass hochentwickelte, dynamische und oftmals individualisierte Attacken mittlerweile die breit angelegten, einfach zu erstellenden Massenmailings abgelöst haben. Der Grund hierfür liegt in den Abwehrmaßnahmen, die die Security-Anbieter entwickelt haben. So reichten bisher standardisierte, signatur-basierte Filtersysteme aus, um sich gegen die Spam-Mails zur Wehr zu setzen und diese unwirksam werden zu lassen. Die Cyberkriminellen mussten daher neue Verfahren entwickeln, um ihr Ziel zu erreichen. Die Folge: Ein Katz-und-Maus-Spiel zwischen Malware-Entwicklern und Anbietern von Sicherheits-Lösungen, in dem auch heute noch die Angreifer stets die Nase vorne zu haben scheinen. Denn bei der Evolution von Attacken per E-Mail müssen die Security-Anbieter ihre Filtermethoden auf immer neue Varianten, Versionen und Einfälle anpassen.

Dabei sind die Angriffe der Cyberganoven längst nicht mehr nur auf digitaler Ebene angesiedelt, sie bedienen sich vielmehr auch anderer Mittel. So ist zunehmend zu beobachten, dass insbesondere Führungskräfte zu den von Cyberattacken betroffenen Personengruppen von Unternehmen zählen. Dabei bedienen sich die Angreifer unter anderem einer altbewährten Angriffsform – dem Social Engineering, bei der gezielt nach personenbezogenen Informationen von Mitarbeitern gesucht wird. Eine Möglichkeit: Die klassische Recherche.

Die Angreifer unterziehen unter anderem Profile in sozialen Medien einer aufwendigen Untersuchung, um nähere Details über Unternehmensangehörige in Erfahrung zu bringen mit dem Ziel, Gepflogenheiten der Person im Fokus herauszufinden. Die Auskundschaftung dient primär der Vorbereitung einer digitalen Attacke, bei der die Kontaktaufnahme mit der Zielperson im Vordergrund steht.

Chefmasche: Präzision statt Schrotflinte

So geht das Social Engineering regelmäßig mit der Chefmasche, auch CEO-Fraud genannt, als Angriff einher. Dabei nutzen die Angreifer das vorhandene Wissen über eine Person, die berechtigt ist, zum Beispiel Geldsummen zu transferieren, zielgerichtet aus.

Diese Form der Cyberkriminalität bedient sich vorwiegend eines bereits angesprochenen Angriffsvektors – der E-Mail. E-Mail-Nachrichten werden derart professionell verfasst, dass sie schwer von einer tatsächlichen E-Mail eines Vorgesetzten unterschieden werden können. Zudem greifen keine der üblichen Abwehrmechanismen, da die E-Mails weder Dateianhänge noch Links auf Schadseiten im Internet beinhalten. Den Tätern ist keine Anstrengung zu groß, um den Betroffenen zu einer unbeabsichtigten Handlung zu bewegen. Sie nutzen vielmehr die gewonnenen persönlichen Informationen, um an ihr Ziel zu gelangen.

Wer aufmerksam Medienberichte zum Thema IT-Sicherheit verfolgt, wird bestimmt schon einmal mitbekommen haben, dass ein hochrangiger Mitarbeiter auf Anweisung eines Fremden einen Geldbetrag auf ein Auslandskonto angewiesen hat. Und genau hierum geht es bei einem CEO-Fraud. So

betrug die globale Schadenssumme laut Angaben des Landeskriminalamtes Sachsen-Anhalt, in den vergangenen drei Jahren rund 3,1 Milliarden Euro. Eine enorme Höhe, die dafür spricht, dass CEO-Fraud weiterhin auf dem Vormarsch ist.

Ransomware ist ebenfalls eine populäre Angriffsform. Hierbei handelt es sich um polymorphe, also in verschiedenen ähnlichen Erscheinungsformen daherkommende Viren, mit denen Cyberganoven ganze Unternehmen zum Stillstand bringen können. Dabei verschlüsselt der Schadcode innerhalb weniger Sekunden sämtliche lokale Daten eines Computers, aber auch komplette Netzwerkdaten. Für Unternehmen, aber auch für öffentliche Einrichtungen, wie etwa Krankenhäuser, ein absolutes Horrorszenario. Denn entweder gelangen die Geschädigten erst durch die Zahlung eines Lösegeldes an den Entschlüsselungscode oder sie haben ein funktionierendes Backup-System. Auf eine Garantie – seitens der Erpresser – sollten die Betroffenen jedoch nicht setzen.

Eine weitere Brisanz geht von sogenannten Zero-Day-Angriffen aus. Diese nutzen gezielt frische, den Unternehmen und insbesondere den Herstellern unbekannte Sicherheitslücken aus – und das genau am Tag des Auftretens solcher Sicherheitslücken. Dieser Informationsvorsprung sorgt letztlich dafür, dass Unternehmen gar keine Möglichkeit besitzen, präventive Maßnahmen zu ergreifen, um entsprechende Angriffe abwehren zu können.

Wie Unternehmen mit der Situation umgehen sollten

Wichtig für Unternehmen ist, sich – falls noch nicht vorhanden – ein umfassendes Konzept im Bereich der IT-Sicherheit zu erarbeiten. Das bedeutet, dass Daten vor unautorisierten Zugriffen geschützt werden müssen, die Verfügbarkeit der Daten jederzeit zu gewährleisten ist und die Unveränderbarkeit der Informationen gegeben sein muss. Dies sind drei Grundpfeiler, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) als essenziell erachtet.

Die Aufdeckung potentieller Angriffspunkte steht dabei im Mittelpunkt. Neben der technischen Komponente gilt der Mensch weiterhin als einer der zentralen Einfallsvektoren. Awareness-Trainings für Mitarbeiter sind hierbei eine gute Basis, um sich mit den Angriffsmustern der Täter vertraut zu machen und somit unachtsamen Handlungen vorzubeugen.

Auf technischer Ebene wird es zukünftig nicht mehr ausreichen, lediglich auf eine Firewall oder ein Antivirenprogramm zu vertrauen. Die Angriffe von Cyberkriminellen zeichnen sich immer stärker durch eine stetige Dynamik sowie durch eine Vielzahl an Verschleierungsmechanismen aus. Für die Erkennung und Abwehr solch raffinierter Angriffe sind spezielle Analyse-Engines sowie Real-Time-Alert-Systeme notwendig.

Empfehlenswert ist daher, herkömmliche Tools – wie den Spam- oder Virenfilter – durch professionelle Forensic-Engines zu ergänzen. So werden beispielsweise verdächtige E-Mail-Anhänge auf Malware geprüft und ihr Verhalten über eine Sandbox Engine einer detaillierten Analyse unterzogen. Gleiches gilt für die Überprüfung von Links in E-Mails sowie beiliegenden Dateianhängen.

Finden Angriffe in personalisierter Form statt, können diese anhand von bestimmten Inhaltsmustern entsprechend klassifiziert werden. Dies gilt etwa für gefälschte Absenderadressen und fingierter Benachrichtigungen.

Oberste Priorität hat zudem immer der Schutz von sensiblen Unternehmensdaten. Daher empfiehlt sich die Ausweitung des IT-Schutzes nicht nur auf die Daten selbst, sondern ebenfalls auf die Transportwege. Neben der Integration von Backup-Lösungen, sollte insbesondere die E-Mail-Kommunikation durch Verschlüsselung vor Spionageangriffen oder Manipulation geschützt werden.

Ebenfalls ist die Implementierung eines IT-Notfallplans von Relevanz. Denn hat ein Angriff erst einmal ein Unternehmen infiltriert, müssen innerhalb kürzester Zeit entsprechende Gegenmaßnahmen zur Eingrenzung der Schäden getroffen werden. Gleiches gilt bei einem möglicherweise eintretenden Datenverlust. Auch hier gilt es, Lösungen implementiert zu haben, die die Aufrechterhaltung täglicher Geschäftsprozesse sicherstellen.

Beachten Unternehmen diese Schutzmaßnahmen, sind sie zwar immer noch nicht zu einhundert Prozent geschützt, aber alles andere als machtlos gegen die heutigen Cyberattacken und gut aufgestellt.

Christoph Maier

Dr. Amir Alsbih, CEO, KeyIdentity GmbH

Von Passwort-Hacks bis hin zum Missbrauch digitaler Daten: Es ist höchste Zeit zum Handeln

Kennen Sie haveibeenpwned oder den BreachAlarm? Auf diesen Plattformen können Sie anonym prüfen, ob Ihr Account gehackt wurde. Wir zeigen Ihnen am Ende dieses Beitrags, wie das funktioniert. Viel wichtiger sind die Statistiken, die Sie dort einsehen können: Pro Tag werden über 333.000 Passwörter gestohlen – beim größten bisher erfassten Hack erhielten die Angreifer Zugang zu über 500 Millionen Accounts.

Diese Zahlen potenzieren sich, da Nutzer ihre Passwörter für verschiedene Dienste und Webportale mehrfach verwenden. Wie ein US-amerikanischer Journalist, der durch seinen sorglosen Passwortgebrauch seine gesamte digitale Identität aufs Spiel setzte: Erst wurde sein Google-Konto gelöscht, dann sein Twitter-Account missbraucht, und letztlich hackten die Angreifer auch seine Amazon- und Apple-ID-Accounts.

Komplexere längere Passwörter sind keine Lösung

Trotz des großen Risikos sind Passwörter noch immer die meistgenutzte Authentifizierungslösung. Die technischen Standards sind zwar anspruchsvoller geworden: Passwörter müssen aus drei von vier Merkmalen wie Klein- oder Großbuchstaben, Ziffern und Sonderzeichen bestehen sowie mindestens 10 Zeichen lang sein. Für einen Durchschnittsnutzer erfordert es aber eine außerordentliche Gedächtnisleistung, sich für jeden genutzten Service neue Zugangsdaten von dieser Komplexität zu merken. Um im Passwort-Dschungel noch eine Chance auf Nutzbarkeit zu haben, werden die Hälfte aller Passwörter nach denselben Schemata konstruiert:

- Großbuchstabe – 4x Kleinbuchstabe – 2x Ziffer
- Großbuchstabe – 5x Kleinbuchstabe – 2x Ziffer
- Großbuchstabe – 3x Kleinbuchstabe – 4x Ziffer
- Die vorherigen Kombinationen mit angehängtem Ausrufezeichen

Passwörter lassen sich leicht erraten

Die harte Mathematik verdeutlicht, dass Angreifer nach diesen Schemata schneller an ihr Ziel kommen, da sie weniger Daten durchprobieren müssen. Bei 8 Zeichen reduziert sich die Anzahl der möglichen Varianten von einer Zahl mit 84 Nullen auf eine Zahl mit 6 Nullen. Noch erschreckender werden die Risikoszenarien, wenn man sich Folgendes vor Augen führt: Ein Angreifer kann in der Regel mit 10 Versuchen pro Passwort 1 Prozent aller Accounts übernehmen. Ohne Rate-Limits und unter Einbeziehung von Informationen aus öffentlich zugänglichen Quellen lassen sich mit 100 Versuchen zwischen 32 bis 73 Prozent der Accounts systematisch „erraten".

All diese Beispiele machen eines ganz deutlich: Digitale Identitäten, die heute mit Google, Amazon & Co. sowie zahlreichen sensiblen Transaktionen im Online-Banking zum Alltag gehören, lassen sich auf diese Weise nicht ausreichend schützen. Gestohlene oder schwache Passwörter sind inzwischen in 81 Prozent aller Fälle die Ursache für einen Hack. Das ist laut Verizon ein Anstieg um 20 Prozentpunkte im Vergleich zum Vorjahr.

Mehr Sicherheit per Smartphone-Klick

Um die Herausforderung wirklich sicherer digitaler Identitäten und Transaktionen auf lange Sicht und unter Zuhilfenahme der bestehenden Technologie in den Griff zu bekommen, hilft nur die 2-Faktor- (2FA) bzw. Multi-Faktor-Authentifizierung (MFA) wirklich weiter. Denn sie entlastet den Nutzer von der Verantwortung, für die Passwort-Sicherheit zu sorgen, und gewährleistet gleichzeitig, dass wichtige Arbeitsprozesse ohne Unterbrechung weiterlaufen. Mit modernen Konzepten wie Push-Token lassen sich sogar sicherheitskritische digitale Transaktionen und Genehmigungsprozesse nach dem Mehraugenprinzip oder unter Gewährleistung der Nichtabstreitbarkeit umsetzen. Dabei wird automatisch eine Push-Benachrichtigung ausgesendet, wenn ein Nutzer auf geschützten Content zugreifen oder eine Transaktion auslösen will. Die freigebende Person muss dafür nur „OK" oder „Nicht OK" auf ihrem Smartphone anklicken – einfacher geht es kaum.

Durch Multi-Faktor-Authentifizierungslösungen wie LinOTP lassen sich auch neue Vorgaben wie die gerade veröffentlichten NIST Guidelines aus den USA, die PSD2-Richtlinie im Zahlungsverkehr von Banken oder die EU-Datenschutz-Grundverordnung nachweisbar umsetzen. Denn mittlerweile betrifft die strengere Datenschutz-Compliance alle Branchen weltweit – sowohl im B2B- als auch im B2C-Bereich. So empfiehlt der Bundesverband IT-Sicherheit e.V. (TeleTrusT) in einer aktuellen Handreichung die Technologie. Und auch viele große weltweite Anbieter wie Google, Apple oder Facebook setzen bereits auf diese Lösungen, um die digitalen Identitäten ihrer Kunden zu schützen.

Wer jetzt nicht handelt, verliert

Die aktuellen Bedrohungen und regulatorischen Anforderungen machen eines ganz klar deutlich: Wo ich früher als CEO, CIO oder CISO noch mit einem blauen Auge davongekommen bin, handele ich heute grob fahrlässig, wenn ich nicht die geeigneten Sicherheitsmaßnahmen durchsetze. Denn laut BSI ist jedes zweite Unternehmen von Cyberangriffen betroffen. Es ist höchste Zeit, das Thema anzugehen, um Kunden- und Unternehmensdaten wirklich zu schützen.

Apropos Datenverluste: Ich hatte am Anfang des Beitrags noch Informationen zu haveibeenpawned und BreachAlarm versprochen. Sie können sich im Falle eines Missbrauchs direkt über https://haveibeenpwned.com benachrichtigen lassen. Oder Sie gehen alternativ auf unseren KeyIdentity-Blog und finden heraus, wie Sie sich durch MFA-Lösungen schützen können.

Amir Alsbih

1.3.2 BYOD

BYOD: Container sichern personenbezogene Daten auf mobilen Endgeräten

In einem BYOD (Bring Your Own Device)-Modell nutzen Mitarbeiter ihre privaten Smartphones oder Tablets für berufliche Zwecke. Der Vorteil für Anwender: Sie können mit ihren gewohnten Endgeräten arbeiten. Arbeitgeber müssen allerdings einige rechtliche Anforderungen beachten, um einen gesetzes-

Günter Junk, CEO, Virtual Solution AG

konformen und sicheren Betrieb zu gewährleisten.

In vielen Unternehmen ist BYOD längst Realität. Die Beschäftigten nutzen ihre privaten Endgeräte für berufliche Aufgaben und Außendienstmitarbeiter bearbeiten mit Smartphones oder Tablets unterwegs unternehmensbezogene Dokumente und E-Mails. Sobald es dabei um personenbezogene Daten wie beispielsweise Angaben zu Kunden oder Mitarbeitern eines Unternehmens geht – und das ist fast immer so – wird daraus ein Fall für das Bundesdatenschutzgesetz (BDSG).

Die rechtlichen Vorgaben sind klar: Im Sinne von § 3 Abs. 7 BDSG ist der Arbeitgeber für die Einhaltung des Datenschutzes bezüglich der im Unternehmen verarbeiteten Daten verantwortlich. Das gilt ohne Einschränkung auch dann, wenn die Beschäftigten für berufliche Zwecke auf ihren eigenen Smartphones mit personenbezogenen Daten arbeiten. Der Arbeitgeber ist daher in der Pflicht, dass die notwendigen technischen und organisatorischen Maßnahmen getroffen werden, um den Datenschutz zu gewährleisten. Konkret bedeutet das: Die personenbezogenen Daten auf den Smartphones müssen genauso sicher sein wie im Rechenzentrum des Unternehmens und das obwohl die technischen Voraussetzungen völlig andere sind.

Um BYOD auch im Hinblick auf die 2018 in Kraft tretende europäische Datenschutzgrundverordnung (DSGVO) rechtssicher zu gestalten, gibt es mehrere einander ergänzende Maßnahmen:

- Wichtig – und laut der ab 25. Mai 2018 geltenden europäischen Datenschutzgrundverordnung (DSGVO) auch so vorgesehen – ist zunächst einmal die Verschlüsselung der Daten auf den mobilen Endgeräten. Dabei müssen die Daten nicht nur auf dem mobilen Endgerät, sondern auch während der Übertragung verschlüsselt werden. Die durchgehende Verschlüsselung soll sicherstellen, dass die Daten permanent geschützt sind. Ein Unternehmen kann durch die Verschlüsselung nachweisen, dass man der Sorgfaltspflicht beim Umgang mit personenbezogenen Daten nachkommt.
- Die beruflichen und die privaten Daten auf den Smartphones und Tablets werden durch den Einsatz von Containern strikt getrennt. Dadurch werden sowohl die Firmendaten geschützt als auch die Privatsphäre des Mitarbeiters – ein weiterer wichtiger Grundsatz der DSGVO. Container bieten noch weitere Sicherheitsvorteile Sie verhindern, dass andere Apps (beispielsweise WhatsApp) auf die personenbezogenen Daten im beruflichen Bereich unerlaubterweise zugreifen können. Zudem kann der IT-Administrator unterbinden, dass jemand – bewusst oder aus Nachlässigkeit – personenbezogene Daten oder vertrauliche Firmeninformationen per Copy-and-Paste aus dem Container in den Privatbereich verschiebt. Was ist, wenn ein Mitarbeiter sein beruflich genutztes Endgerät verliert oder es gestohlen wird? Der Arbeitgeber ist dann in der Lage, die beruflichen Daten in dem verschlüsselten Container aus der Ferne sicher zu löschen. Es gibt also eine Reihe von Mechanismen, um Daten auf mobilen Endgeräten zu schützen.
- Die Datenschutzgrundverordnung sieht vor, dass die Sicherheit der Daten bereits bei der Entwicklung neuer Software – also auch bei Apps und mobilen Anwendungen – zu berücksichtigen ist. Im Fachjargon (Art. 25 Abs. 1 und 2 der DSGVO) heißt das: Privacy by Design und Privacy by Default. Dies ist bei einem Container-Ansatz gegeben.

Warum es wichtig ist, sich mit den rechtlichen Herausforderungen des BYOD-Modells zu befassen, zeigt abschließend ein Blick auf die Datenschutzgrundverordnung im Unterschied zum Bundesdatenschutzgesetz (BDSG). Die Aufsichtsbehörden konnten bis heute nur dann ein Bußgeld aussprechen, wenn der Datenverstoß aufgrund unzureichender technischer und organisatorischer Maßnahmen verursacht wurde. Mit der ab Mai nächsten Jahres geltenden Datenschutzgrundverordnung kann bereits ein Bußgeld verhängt werden, wenn ein Unternehmen die Maßnahmen nicht nachweisen kann. Dann können Bußgelder von bis zu zehn Millionen Euro oder von bis zu zwei Prozent des gesamten Jahresumsatzes fällig werden. Noch ist für Unternehmen Zeit, sich intensiv mit der Implementierung wirksamer Maßnahmen zur Einhaltung der Datensicherheit beim BYOD-Modell zu befassen. Der Container-Ansatz ist eine einfache und effiziente Art, die neuen Bestimmungen für mobiles Arbeiten einzuhalten.

Günter Junk

Mathias Widler, Area Director, General Manager EMEA Central, Zscaler

Sicherer Remote Access im Zeitalter der Digitalisierung

Die Megatrends der Cloudifizierung, BYOD, Mitarbeitermobilität, Industrie 4.0 und das Internet der Dinge haben einen gemeinsamen Nenner: Zugriffssicherheit. In der Konsequenz bedeutet dass, dass diese Trends nicht isoliert betrachtet werden dürfen, sondern ihre Verzahnung berücksichtigt werden muss. Gefragt ist ein Lösungsansatz für den sicheren Zugriff auf Anwendungen oder Geräte, der die Umsetzung aller Megatrends im Geschäftsalltag ermöglicht.

Die zu bewältigende Herausforderung liegt dabei im Remote Zugriff: der Mitarbeiter muss sicher und performant auf Anwendungen und Daten in der Cloud zugreifen können, unabhängig von welchem Gerät und auch von unterwegs aus, der Maschinenbauer muss zu Wartungszwecken sicheren Zugang zu der beim Kunden stehenden Produktionseinrichtung erhalten und auch auf jegliches Gerät im Internet of Things soll nur autorisierter Zugriff möglich sein. Der sichere Zugriff ist dementsprechend Dreh- und Angelpunkt der digitalen Transformation.

Durch Remote Access Virtual Private Networks (RAS VPNs) wurde in der Vergangenheit der sichere Zugriff auf das Unternehmensnetz für vertrauenswürdige Anwender gewährleistet. Die VPN-Technologie wurde dabei mit der Vorgabe entwickelt, den Remote-Zugang auf das gesamte Netzwerk zu ermöglichen. War der Anwender einmal eingeloggt, hatte er Zugriff auf alle Anwendungen und Daten im Unternehmensnetz.

Als dieses Modell entstand, hatte das Konzept des vertrauenswürdigen Users noch Bestand. Ein solcher Nutzer war während seines Arbeitstages auf den Zugang zum Firmennetz angewiesen und griff darauf mit einem Gerät in Firmenbesitz zu. Damals war es kein Problem, das Unternehmensnetz auch für Remote-Anwender zu öffnen, die Zugang zu Anwendungen benötigten. In Zeiten zunehmender Mitarbeitermobilität und von allgegenwärtigem Internet-Zugriff von unterschiedlichen Parteien auf unterschiedliche Applikationen oder Geräte gehört das Konzept eines „vertrauten Nutzers“ auf den Prüfstand.

Remote Access VPNs sind veraltet

Dieser Ansatz ist im Zeitalter der Digitalisierung in die Jahre gekommen, denn er wurde lange vor den heutigen Megatrends entwickelt. Die Grenzen zwischen intern und extern vorgehaltenen Daten sind seitdem verschwommen. Applikationen und Daten werden gleichzeitig im Netz und in der Cloud gehostet. Im Zeitalter von Industrie 4.0 müssen externe Partner Zugriff auf dedizierte Anwendungen im Unternehmensnetz oder der Produktionsanlage erhalten – aber nicht auf das gesamte Netz. Ein neuer Remote Access-Ansatz ist gefragt, der auf die Sicherheitsanforderungen des heutigen Geschäftsalltags ausgelegt ist.

Klassische VPNs halten mit diesen Megatrends kaum Schritt aufgrund der statischen Netzwerkverbindungen. Nur mit hoher Komplexität und großem Konfigurationsaufwand kann die nötige Skalierbarkeit erreicht werden. Denn für den mobilen Zugriff via VPN benötigen Unternehmen heute die manuelle Administration von Load Balancern, VPN-Konzentratoren, DDoS-Schutz und nicht zuletzt Firewalls. Statische Konfiguration der Verbindungen und Zugangsberechtigungen sorgen zusätzlich dafür, dass sich Cloud-Applikationen nur mit hohem Aufwand einbinden lassen. Und dann kann der Mitarbeiter entweder remote auf das Unternehmensnetz oder auf die Anwendung in der Cloud zugreifen – aber nicht parallel auf beide Welten.

Heutzutage stehen mobile Geräte durch BYOD einerseits nur mehr eingeschränkt unter Kontrolle der IT-Abteilung, zum anderen kann es auch auf strikt verwalteten Geräten nicht ausgeschlossen werden, dass Anwender unerlaubte Software installieren. Nicht zuletzt öffnet ein RAS-VPN ohne administrationsintensive Einschränkungen oftmals den Zugriff auf das gesamte Netzwerk. Je weiter das Netzwerk also über einen VPN-Tunnel vergrößert wird, desto mehr potenzielle Sicherheitslücken entstehen.

Heute haben Unternehmen auch die Cloud oder Industrie 4.0-Anforderungen in ihr Remote Access Konzept einzubeziehen. Wenn Applikationen zum Teil in die Wolke verlagert werden oder Maschinen über das Internet steuerbar sind, muss auch die Konnektivität vom Gerät oder Unternehmen dorthin berücksichtigt und für Verfügbarkeit gesorgt werden, ohne dass dieser Weg die Anwenderakzeptanz beeinträchtigt oder zu Lasten der Sicherheit geht. Der herkömmliche Weg ist allerdings mit einem Umweg verbunden: Zuerst wird eine Verbindung vom Anwender zum Rechenzentrum aufgebaut und im nächsten Schritt ein weiterer Tunnel vom Rechenzentrum in die Cloud, wodurch sich der Routing-Pfad aufwändiger gestaltet. Die Verwaltung eines solchen Konstrukts wird durch die notwendigen Multipoint-VPNs nicht nur unheimlich langsam, sondern auch sehr komplex.

Remote-Zugriff auf den Anwenderbedarf ausgelegen

Mitarbeiter akzeptieren heute keine Einschränkung bei der Zugriffsgeschwindigkeit für die Nutzung von internen wie externen Cloud-Applikationen. Erst wenn der Traffic auf kürzestem Wege bei der Anwendung ankommt, ohne den Umweg über das unternehmenseigene Rechenzentrum zu nehmen, entsteht die gewünschte und notwenige Performance beim Zugriff auf Applikationen in der Wolke. Eine Lösung für das Dilemma des sicheren Zugriffs im Zeitalter der Digitalisierung lautet, dass dem Ansatz, das gesamte Netzwerk für den externen Benutzer oder Geschäftspartner zu öffnen, der Rücken gekehrt wird. Vielmehr ist es erforderlich, den Remote Zugang lediglich auf der Ebene einer bestimmten Applikation zu ermöglichen durch einen neuen Ansatz der Zugriffsrechteverwaltung.

Mit Hilfe von ZPA – Zscaler Private Access können sich Mitarbeiter oder Drittparteien direkt mit der gewünschten Applikation verbinden. Eine solche Private Access Lösung ermöglicht den Zugriff auf Applikationsebene, egal ob für den Mitarbeiter oder den externen Partner. Im Unterschied zum klassischen VPN wird dabei nicht der Zugriff auf das gesamte Netzwerk geöffnet. Eine transparente Forwarding-Software erkennt anhand des DNS-Namens des Zielsystems, wohin die Verbindung aufgebaut werden soll. Abhängig davon wird ein dynamischer,

Ulrich Hamann, Geschäftsführung, Bundesdruckerei

applikationsspezifischer Tunnel geöffnet, der nur die Verbindung vom Anwender zu einer bestimmten Applikation zulässt. Dabei entscheidet eine zwischengeschaltete Authentisierungs- und Autorisierungskomponente darüber, welcher Anwender auf welche Applikation zugreifen darf und sorgt zudem für das optimale Routing – ganze ohne Loadbalancer.

Für eine solche Lösung ist die Leistungsfähigkeit der Wolke gefragt. Durch eine zentrale, Cloud-basierte Sicherheitsplattform wird das Verwalten und Brokern zwischen den verschiedenen Applikationen, Anwendern und deren Gruppenrechten ermöglicht und dynamisch die Verbindung herstellt. Somit lassen sich auch externe Partner und deren dediziertes Zugriffrecht auf eine Maschine oder Anwendung abbilden.

Für den Anwender erfolgt der Verbindungsaufbau zu seiner gewünschten Applikation im Hintergrund, ohne dass er manuell Eingreifen muss. Es spielt für ihn keine Rolle, wo sich eine Applikation oder ein Service befindet – ob in der Private Cloud einem unternehmenseigenen Rechenzentrum, in der Public Cloud bei Dienstleistern wie AWS oder Azure, oder als Hybrid-Variante mit einem Mix aus allen Modellen. Das Routing erfolgt immer im Private Access Service der Sicherheitsplattform. Da Nutzerakzeptanz im Mittelpunkt steht, entfällt die Aktivierung von VPN-Clients und auch ein VPN-Konzentrator wird obsolet. Der Nutzer bewegt sich nun ganz wie immer im Unternehmensnetz (LAN).

Auf diese Weise lassen sich Angriffsvektoren ausschalten, denn die eingehenden Verbindungen zum Rechenzentrum oder den Cloud-Services – und damit oft auf das ganze Netzwerk – entfallen. Unternehmen erreichen nicht nur eine flexiblere Infrastruktur die die Megatrends der Digitalisierung berücksichtigt, sondern auch einen höheren Grad an Sicherheit. . Kritische Unternehmensapplikationen können untereinander kommunizieren, ohne dass diese Applikationen im Internet in Erscheinung treten. Ein Zero-Trust-Konzept für das Digitalisierungszeitalter ist geboren. Mathias Widler

1.3.3 Cloud und IoT

Sichere Häppchen

CLOUDSPEICHER-LÖSUNG: Virtueller Informationsaustausch über Unternehmensgrenzen hinweg sowie Datensicherheit und -schutz müssen sich nicht widersprechen. Ulrich Hamann, Vorsitzender der Geschäftsführung der Bundesdruckerei, über Speichertechnologien, die Unternehmen einfachen und vor allem sicheren Datenzugriff versprechen.

Herr Hamann, 54 Prozent der deutschen Unternehmen nutzen Cloud-Angebote. Warum sollten es noch mehr werden?

Ulrich Hamann: Unsere Arbeitswelt ist in den vergangenen Jahren nicht nur flexibler geworden, sondern auch vernetzter – und zwar innerhalb von Organisationen und über die Grenzen von Unternehmen hinweg. Wer von überall aus auf Informationen und Daten zugreifen, Projekte gleichzeitig bearbeiten sowie Informationen mit Kollegen und Kunden oder Lieferanten teilen möchte, für den ist ein einfacher und sicherer Datenaustausch unerlässlich. Das ermöglichen Cloud-Speicherdienste. Sie stellen IT-Kapazitäten bei Bedarf schnell und auf Knopfdruck zur Verfügung. Verteiltes Arbeiten an Informationen und Daten bietet große Effizienz- und Produktivitätsvorteile.

Amazon, Google Drive und Dropbox sind nur drei der Big Player der Cloud-Speicherdienste. Sich für einen Anbieter zu entscheiden, fällt nicht leicht. Worauf sollte man bei der Wahl achten?

Hamann: Sicherheitsbedenken und Datenschutzgründe halten insbesondere den deutschen Mittelstand davon ab, Cloud Computing zu nutzen. Sicherheit in der Cloud ist vor allem Vertrauenssache: Anwender müssen darauf vertrauen, dass erstens die eingesetzten Lösungen ihre Daten vor unberechtigten Zugriffen schützen, zweitens der Cloud-Anbieter ihre Daten nicht für eigene Zwecke missbraucht und drittens die Daten jederzeit verfügbar sind.

Unsere neue Speicherlösung BDrive beispielsweise erfüllt diese Voraussetzungen. In Zusammenarbeit mit dem Hasso Plattner Institut in Potsdam und dem Start-up neXenio haben wir diese spezielle Cloud-Speicherlösung entwickelt.

Was genau unterscheidet denn Ihre Lösung von denen anderer Anbieter?

Hamann: BDrive ist eine Plattform; die Daten unserer Kunden werden nicht bei uns gespeichert, sondern bei unseren Partnern. Die zu speichernde Datei wird am Arbeitsplatz des Anwenders verschlüsselt; dann werden einzelne Datenpäckchen erzeugt und in der Regel auf fünf kommerzielle etablierte Cloud-Speicherdienste verteilt. Dabei kann der Kunde immer auswählen, welche Speicherdienste für welche Dokumente genutzt werden.

Was bringt diese „häppchenweise" Vorgehensweise?

Hamann: Sie bietet maximalen Schutz. Denn kein Cloud-Speicherdienst kommt in den vollständigen Besitz aller Daten. Angreifer übrigens auch nicht. Dank Verschlüsselungsverfahren ist es zudem niemandem möglich, die Dateien aus den Fragmenten zusammenzusetzen und auszulesen. Mehrstufige Authentifizierungsmethoden sorgen dafür, dass nur identifizierte und berechtigte Anwender mit ihren dafür freigegebenen Endgeräten auf die Daten zugreifen können. Und sollten ein oder zwei Speicherdienste aus technischen Gründen versagen, hindert das Nutzer nicht an einem sicheren Datenaustausch. Das System ist redundant ausgelegt.

Welche technische Vorrausetzungen brauchen die Kunden?

BDrive ist auf allen gängigen Desktop-Plattformen und mobilen Endgeräten sowie über Standard-Web-Browser einsetzbar. Mehr dazu unter bdr.de/bdrive

- Das Wichtigste im Überblick: Zuverlässiger Datenzugriff: Cloud-Computing wird dank verschlüsselter und verteilter Informationen noch sicherer.
- Sichere Cloud-Speicherdienste wie BDrive eignen sich für Nutzer, die flexibel und zeitsparend mit sensiblen Daten arbeiten möchten.

Ulrich Hamann

Von Schnittstellen zu geplanten Schwachstellen

Mit dem Einzug intelligenter und weniger intelligenter Geräte, von digitalen Sprachassistenten und Set-Top-Boxen bis hin zu Autos, Telefonen, Smart-TVs, Tablets und einer Vielzahl neuer und bislang technisch nicht denkbarer IoT-Produkte verlassen sich immer mehr Bürger auf deren starke informations-technologische Sicherheit. Diese soll Schutz vor Hackern, vor anderen Benutzern, vor den Herstellern und vor dritten Dienstanbieter wie Sozialen Netzwerken oder Suchmaschinen gleichermaßen gewährleisten.

Viele dieser Geräte genügen oft schon aktuellen Sicherheitsanforderungen nicht und geraten deshalb auch immer wieder in die Schlagzeilen. Ursache hierfür ist, dass sie im Einzelfall schon einfachsten Sicherheitsbedrohungen nicht standhalten, indem sie vertrauliche Informationen preisgeben oder – unbemerkt vom Eigentümer – als bösartige Fußsoldaten in den Heeren der unzähligen Bot-Netze agieren.

Ursache und Auslöser sind oft absichtlich vom Hersteller hinterlassene oder nachträglich von Dritten installierte Hintertüren, die an den eigentlichen Sicherheitsmechanismen vorbei Zugriff gewähren. Dies geschieht oft auch unter Erlangung von Administrationsrechten bis hin zum Vollzugriff. Aber auch das Beibehalten von Standardkonfigurationen (Username: „admin" mit identischem Passwort als Paradebeispiel) oder eine unzureichende Härtung des Systems machen IT- und IoT-Systeme anfällig für den Zugriff unerwünschter Dritter.

Kein ernstzunehmender Sicherheitsforscher wird verneinen, dass durch derartige Schwachstellen oder Hintertüren in einem IT-System sich die Chance erhöht, dass diese auch durch Kriminelle, professionelle Hacker, Skript-Kiddies oder durch die Nutzung von extra hierfür entwickelten spezialisierten Toolkits praktisch durch jeden auch nur mäßig IT-begabten Nutzer ausgebeutet werden können. Konkrete Gefahren liegen in den Bereichen Industriespionage, Diese Risiken werden immer noch unterschätzt. Grundlegende technische Ansätze, beispielsweise ein angemessenes und umfassendes Patch-Management (zur Aktualisierung kompromittierter Softwareversionen) wären hier eine Lösung.

Die Tatsache aber, dass IoT-Geräte, aber auch viele SmartPhones oder SmartTVs selten bis nie mit neuen, sichereren Betriebssystem oder Firmware-Versionen aktualisiert werden, zeigt einen wichtigen Aspekt des Dilemmas: Wird eine Schwachstelle bekannt, wird sie nur selten gepatcht werden, bleibt damit offen und dokumentiert. Tritt dieser Fall ein, wird eine solche Schwachstelle dann auch zwangsläufig auch von einer Vielzahl unterschiedlicher Angreifer aktiv ausgenutzt. Ist sie einzelnen bekannt, wird aber nicht dokumentiert, wird oft von einer Zero-Day-Vulnerability gesprochen, die aber oft lange ausgenutzt wird. Sie gefährdet den Bürger als Privatanwender und agiert dieser als Mitarbeiter im Unternehmen, ist dieses folgerichtig zusätzlich ebenfalls potentiell bedroht.

Eine Vielzahl von Herstellern strebt an, ein kontinuierlich steigendes Sicherheitsniveau in ihren Systemen zu implementieren. Hierdurch wird gezielt auf die Verhinderung ungewünschte Zugriffe Dritter auf sensible Systeme hingearbeitet. Der Zugriff vorbei an allen Sicherheitsmechanismen ist folgerichtig eine Begehrlichkeit von einer Vielzahl von interessierten Stellen.

Matthias Reinwarth, Lead Advisor & Senior Analyst, KuppingerCole

Gefahr droht damit zukünftig womöglich auch bei bislang vertrauenswürdigeren Systemen: In einer Vielzahl von Staaten fordern staatliche Stellen, etwa zur Verbrechens- oder Terrorismusbekämpfung genau einen solchen Zugriff auf derartige Systeme. Neben der selbständigen Fahndung nach solchen Schwachstellen durch staatliche Stellen werden diese auch in grauen Märkten gehandelt und bisweilen für staatliche Zwecke aufgekauft.

Der logisch nächste Schritt ist damit die Einflussnahme auf Standards, Protokolle, Hersteller und Produkte und diese Forderung wird heute schon in vielen Ländern erhoben. Aktuell wird das nun auch in der Bundesrepublik Deutschland diskutiert.

Nach Recherchen des RedaktionsNetzwerk Deutschland (RND) strebt das Bundesinnenministerium eine durch rechtliche Verpflichtung unter Strafandrohung erzwungene Offenlegung der Programmierschnittstellen/APIs für alle Hersteller aller oben genannter Produkte und weiterer an. Eine Offenlegung der Schnittstellen und damit der Kommunikation bedeutet folgerichtig die potentielle Einsicht in eigentlich zum Übertragungszeit verschlüsselte Daten und die direkte Nutzung möglicher erkannter Schwachstellen vor Ort. Darüber hinaus wird die technische Fähigkeit gefordert, auch private Rechner im noch näher zu definieren „Krisenfall" abzuschal-

ten zu können. Hierbei sollen vor der Stilllegung der Computer personenbezogene Daten extrahiert werden können.

Die grundlegende Beurteilung der Hintergründe von Terrorismus- und Kriminalitätsbekämpfung ist eine langfristige Aufgabe. Deren Umsetzung in technische und rechtliche Maßnahmen muss aber darüber hinaus allgemeinen Grundsätzen und rechtlichen Anforderungen der IT-Sicherheit, des Datenschutzes und der Wahrung der Privatsphäre Genüge tun. Die derzeit vorliegenden Dokumente beinhalten einen Richtervorbehalt, die Maßnahmen sind damit im Rahmen der Gewaltenteilung formal strengen Beschränkungen unterworfen. Damit dieser Richtvorbehalt jegliche nicht genehmigten Zugriff verlässlich verhindert, ist von klaren Voraussetzungen und Annahmen auszugehen: Die Annahme, dass eine Schwachstelle nur von einer staatlichen Stelle entdeckt und anschließend ausgenutzt wird, ist falsch. Gleiches gilt für die Annahme, dass Backdoors nicht entdeckt und geöffnet werden.

Folgerichtig ist jede nicht behobene Schwachstelle eine Gefährdung für Wirtschaft und Gesellschaft. Die Erfahrung zeigt, dass bei staatliche Stellen bekannte und genutzte Schwachstellen nur eine geringe Halbwertszeit bis zu deren Offenlegung und deren unerwünschte Nutzung durch Dritte haben. Der Wikileaks Vault7 Dump als nur ein sehr prominenter Leak in einer Reihe von Veröffentlichungen beinhaltet staatliche genutzte Schwachstellen, die oft noch langfristig ausnutzbar sind. Die Ransomware-Attacke WannaCry basierte auf einer in Windows erkannten Schwachstelle, die von der NSA aktiv fünf Jahre ausgenutzt wurde und deren Details erst nach Diebstahl von Informationen über die zugrundeliegende Schwachstelle und damit offensichtlich zu spät an Microsoft übermittelt wurden.

Dirk Schlimm, Executive Vice President, Geotab Advisory Boards

Die Entfernung solcher Sicherheitsrisiken zum Schutz der Bürger auch bei allgemeinem Bekanntwerden solcher Gefahren hingegen ist schwierig. Oft ist sie weder technisch noch organisatorisch machbar, da die Nutzungsdauer (und damit die Ausnutzungsdauer von bekannt gewordenen, gewollten wie ungewollten Sicherheitslücken) deutlich länger als der Wartungszeitraum ist, in dem Hersteller Sicherheitsupdates, neue Firmware oder Systemversionen bereitstellen. Nicht zuletzt ist auch der Zugang zu diesen Systemen aus vielen Gründen nicht direkt oder nur mit hohem Aufwand möglich.

Da die geplante Regelung die volle Bandbreite von Geräten umfasst, die der private, aber nicht zuletzt auch der kommerzielle oder staatliche Anwender in praktisch allen Lebens- und Arbeitsbereichen nutzt, sind auch praktisch alle von diesen Systemen verarbeiteten Daten in Gefahr. Zu betrachten sind exemplarisch nur etwa die Informationen, die heute einem typischen Smartphone anvertraut werden, ergänzt um die kleinen und großen Geheimnisse, die ein intelligenter Sprachassistent, das vernetzte Auto und das Smart Home (inklusive der Überwachungskameras) über uns wissen. Eine Beurteilung der oben beschriebenen Initiative mit Blick auf eine Ausspähung dieser Informationen durch unerwünschte Dritte jenseits staatlicher Aktivitäten sollte damit grundlegend auf Basis der Grundsätze, Erkenntnisse und Best Practices von IT-Sicherheit, Compliance und dem Schutz der Privatsphäre der betroffenen Personen erfolgen.

Matthias Reinwarth

1.3.4 Telematik

Dirk Schlimm von Geotab zur Sicherheit von Telematikplattformen

„Vernetzte Autos eröffnen zahlreiche Vorteile wie erhöhte Sicherheit, größere Effizienz und Komfort. Flottenmanager (z.B. Betreiber von Autovermietung, Leasinggesellschaften oder Logistikfirmen) haben anhand unzähliger Daten wie GPS, Benzinverbrauch und Fahrverhalten den Status ihrer Autos immer im Blick. Diese Daten werden auf einem Standard Diagnose-Interface, dem On-Board-Diagnostic (OBD) Port gesammelt und bereitgestellt. Dieser ist somit ein wichtiger Bestandteil des vernetzten Fahrens.

Andererseits führt der Anschluss von Fahrzeugen an das Internet zu industrieweiten Diskussionen über den Aspekt der Cyber-Sicherheit. Betreiber von Telematik-Plattformen müssen bei deren Konfiguration dem Sicherheitsaspekt eine hohe Priorität einräumen, um ihren Kunden Datenschutz gewährleisten zu können. Hierzu empfiehlt es sich, Industrierichtlinien und Standards (wie SAE, ISO, IEEE oder ASAM) einzubeziehen. Des Weiteren müssen die Datenschutzmassnahmen der lokalen Gesetzgebung entsprechen und die Daten der Fahrer ausreichend schützen.

Flottenmanager sind einerseits auf den direkten Zugriff auf die operativen Daten ihrer Fahrzeuge angewiesen, andererseits müssen diese stets sicher sein. Daher sollten sie Datenplattformen nutzen können, die genau die Daten erhebt, die sie auch brauchen und persönliche Daten der Fahrer auf einem Minimum halten. Außerdem empfiehlt sich ein Sicherheitsprogramm mit „Best of Breed"-Lösungen, welche für die einzelnen Bereiche die für sie besten Lösungen beinhalten. Denn datengetriebene Mobilität ist nicht möglich, wenn die Sicherheit der Daten nicht gewährleistet ist."

Dirk Schlimm

1.4 DATENSCHUTZ UND GOVERNANCE

1.4.1 Strategie

E-Privacy – Auswirkung auf die digitale Szene

Jahrelang wurde gearbeitet, getüftelt und wieder geändert, bis im April letzten Jahres schließlich die EU-Datenschutzgrundverordnung (EU-DSGVO) beschlossen wurde. Ab 25. Mai 2018 muss diese Verordnung von allen Unternehmen in der EU eingehalten werden, was die Unternehmen vor eine große Aufgabe stellt – die digitale Werbebranche muss sich dadurch nämlich einer intensiven Vorbereitung stellen, um den Richtlinien der Verordnung gerecht zu werden und mögliche Strafen bei Nichteinhaltung zu vermeiden.

Internationale E-Privacy-Richtlinie will für besseren Datenschutz sorgen

In diesem Zusammenhang liest man nun ständig auch Hinweise auf die E-Privacy-Verordnung. Doch was ist E-Privacy eigentlich? Grundsätzlich lässt sich dazu sagen, dass es um den Schutz persönlicher Daten vorrangig im Internetbereich, aber auch in anderen elektronischen Kommunikationskanälen geht. Die E-Privacy-Richtlinie wurde im Jahr 2002 von der EU eingeführt. Sie gibt die Mindestvorgaben des Datenschutzes, die eingehalten werden müssen, vor. Zusätzlich zur E-Privacy-Richtlinie wurde 2009 auch die Cookie-Richtlinie eingeführt, die unter anderem nach der Aufklärung von Kunden in Bezug auf das Setzen und die Verwendung von Cookies auf Webseiten verlangt.

Bisher wurden Richtlinien wie jene der E-Privacy und der Cookies vor allem national geregelt – ab Mai nächsten Jahres will die EU nun eine einheitliche Datenschutzgrundverordnung geltend machen. Die E-Privacy-Richtlinie, die für einen besseren Schutz vor Tracking sowie verschlüsselter Kommunikation sorgen soll, ist in Zukunft des Weiteren auch für das Abwehren von Cookie Walls und von Offline-Tracking durch Bluetooth und öffentliche Netzwerke verantwortlich. Die Meinungen dazu gehen weit auseinander, weisen etwa Befürworter auf die verbesserten Nutzerrechte hin und Gegner wiederum auf die dadurch entstehenden Probleme für die digitale Wirtschaft Europas. Vor allem betroffen ist unter anderem das Affiliate Marketing, da dieses insbesondere der Provisionierung von Werbeleistungen dient und das dafür genutzte Cooking Tracking extrem eingeschränkt wird.

Die Digitalbranche steht vor massivem Wandel

Die digitale Wirtschaft sieht sich mit der neuen Verordnung maßgeblichen Verschärfungen und schwierigen Veränderungen gegenübergestellt – es lässt sich durchaus auch von Benachteiligung sprechen. Die E-Privacy-Richtlinien wollen einen hohen Standard des Datenschutzes für elektronische Kommunikation garantieren, was sich aber mit der Realität, mit welcher Unternehmen konfrontiert sind, nahezu unmöglich vereinbaren lässt. Von den Änderungen und der Etablierung der neuen Richtlinien ist die gesamte Online-Marketing-Branche betroffen. Dazu zählen nicht nur Tracking-Spezialisten und Targeting-Anbieter, sondern auch Online-Journalismus und Programmatic Advertising.

Alexander Eser, Co-Founder & Managing Director, kaufberater.io

Nutzerdaten, die durch das Cookie Tracking bisher erfahren werden konnten, könnten in Zukunft nur mehr durch die Zustimmung der Nutzer zugänglich sein. Dazu muss die Einwilligung des Kunden vorliegen, die er durch das sogenannte „Opt-in" geben kann. Schon alleine die Alternative, eine Zustimmung oder eben eine Ablehnung zu geben, könnte Kunden in Zukunft abschrecken, was zu einem enormen Datenverlust führen kann. Des Weiteren dürfen Daten nur mehr dann verwendet und verarbeitet werden, wenn sie entweder „streng erforderlich" oder „streng technisch notwendig" sind. Vor allem Cookie Walls und Cookie Banner stehen im Fokus der neuen Verordnung.

Zukünftig könnten Hinweistexte wie „Mit dem Besuch dieser Webseite akzeptieren Sie die Verwendung von Cookies" nicht mehr als ausreichend angesehen werden. Auch der Hinweis darauf, dass der Nutzer selbst in seinem Browser Datenschutzeinstellungen vornehmen kann, könnte in Zukunft nicht mehr ausreichen. Es wird vielmehr so sein, dass der Nutzer beim Aufruf einer Affiliate Seite noch vor der Platzierung von Cookies einen Hinweis auf die Verwendung von Cookies der Webseite bekommt, dem der Kunde entweder zustimmen oder ihn ablehnen kann. Die Zustimmung muss per Opt-in erfolgen, stimmt der Kunde nicht zu, darf er die Webseite aber trotzdem benutzen.

Negative User Experience als mögliche Folge der E-Privacy-Richtlinie

Hier stellt sich wohl die wichtigste Frage: Wie sollen Affiliate Marketing Betreiben in Zukunft Geld verdienen? Vor allem kleinere Betreiber sind auch betroffen, da die Umstellung auf und die Anpassung an die neuen Richtlinien einen großen Aufwand darstellen. Aber nicht nur die Unternehmen selbst, sondern durchaus auch die Nutzer sind betroffen, werden sie doch bei jedem Besuch von Webseiten immer und immer wieder mit Werbeeinverständnissen konfrontiert.

Ein großes Problem durch die neuen Regeln ent-

steht dadurch, dass die Richtlinien Werbung nicht einschränken wird, sondern dass diese Werbung noch unkontrollierter und vermehrt umherschwirrt. Denn durch User Tracking kann relevante Werbung mit wenig Streuverlust ausgespielt werden. Dies wäre gemäß der neuen Richtlinie nicht mehr möglich und Online-Werbung würde weniger zielgerichtet. Das heißt als Vegetarier könnten mir Banner für Fleischprodukte gezeigt werden, denn woher soll der Advertiser wissen, dass ich Vegetarier bin? Die Annahme, dass Werbung verschwindet, ist wohl ein kompletter Trugschluss. Die Gefahr, dass sogar noch mehr Werbung ausgespielt wird, um den Streuverlust auszugleichen ist sehr hoch. Sollte sich die neue E-Privacy-Richtlinie in ihrer jetzigen Form durchsetzen, dann könnten User mit einer deutlich schlechteren Erfahrung im Web konfrontiert werden.

Alexander Eser

Jörg Kranepuhl, Syndikusrechtsanwalt und Senior Legal Counsel, Commvault Systems GmbH

Ordnung ins Chaos bringen – Datenmanagement in der Cloud gemäß DSGVO

Immer mehr Unternehmen verlagern Daten in die Cloud. Dabei ist es wichtig, den Überblick zu behalten, wo personenbezogene Daten gespeichert sind und wer darauf Zugriff hat – sonst kann es teuer werden.

Das Unternehmen steht am Anfang der Digitalisierung? Dann geht der erste Blick Richtung Cloud. Ist es schon mittendrin in der digitalen Transformation? Dann steht die Cloud meistens im Mittelpunkt. Gleich um welche Firmengröße oder Branche es sich handelt, die Akzeptanz der öffentlichen Cloud steigt. Intern müssen immer weniger Zweifler von deren Vorzügen überzeugt werden, etwa von einfachem File-Sharing und von besseren Möglichkeiten der Zusammenarbeit. Begeisterung und Eigeninitiative können mitunter sogar Überhand nehmen.

Einzelne Abteilungen oder Nutzer wenden sich Cloud-Tools und -Diensten zu, die ihnen vertraut, einfach zu bedienen, mit den passenden Features vorkonfiguriert oder schnell verfügbar sind. Unabhängigkeit, Kosteneffizienz und Flexibilität auf der einen Seite stehen dann einem IT-Sicherheitsrisiko und ab Mai nächsten Jahres sogar rechtlichen Herausforderungen auf der anderen Seite gegenüber. Ein Beispiel aus der Praxis: Nutzen Mitarbeiter eines Unternehmens aus Gründen der Bequemlichkeit unbemerkt ein Cloud-Tool wie Dropbox, verlassen Daten die internen, abgesicherten IT-Strukturen des Unternehmens. Das kann interne Compliance-Verstöße zur Folge haben, aber auch einen Verstoß gegen die Regeln der europäischen Datenschutzgrundverordnung (EU-DSGVO, engl. GDPR) nach sich ziehen.

Ab dem 25. Mai 2018 gilt eben diese umfassende Verordnung: Wer ihr nicht nachkommt, hat empfindliche finanzielle Schäden zu erwarten – bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes einer Firmengruppe – und muss mit Reputations- und Vertrauensverlust rechnen. Zu den gestärkten Verbraucherrechten zählen unter anderem das Auskunftsrecht (Art. 15) und das Recht auf Löschen („Recht auf Vergessen werden“) (Art. 17). So können Verbraucher nicht nur die gesamten über sie gespeicherten Informationen anfordern, sondern auch deren Löschung beantragen. Deswegen müssen Zweck, Dauer und Verarbeitung derartiger Informationen transparenter werden, Voreinstellungen verbraucher- und datenschutzfreundlich sein.

Im Mai hatten 57 Prozent der deutschen Unternehmen noch nicht mit der Umsetzung der EU-DSGVO begonnen, ermittelte Commvault in einer repräsentativen Umfrage. Zwei Drittel der Verbraucher gedachten hingegen, ihre Rechte zeitnah nach Inkrafttreten der DSGVO einzufordern. Das Problem dabei: Zum Zeitpunkt der Befragung kannten 53 Prozent der IT-Abteilungen nicht alle Speicherorte von relevanten, personenbezogenen Daten im Unternehmen oder konnten nicht darauf zugreifen.

Ohne eine Cloud-Strategie und gute Data-Governance ist das Auffinden von personenbezogenen Daten nicht zu bewältigen; es muss klar sein, welche Daten es gibt, und wo sie liegen. Wie aber stellt man fest, ob Daten beispielsweise in unbekannten Cloud-Anwendungen liegen? Die effektivste Lösung mutet recht analog an: Die Mitarbeiter werden gefragt. Sollte es nicht genehmigte Anwendungen geben, ist ein bedingungsloses Verbot der Verwendung nicht zielführend. Vielmehr sollten Vorgesetzte und IT-Verantwortliche herausfinden, warum diese Systeme bevorzugt werden und Lösungen zusammen mit den Beteiligten erarbeiten.

Gerade vor dem Hintergrund der EU-DSGVO sollte die Datenintegrität höchste Priorität haben, um Compliance-Verstöße zu vermeiden. Hilfreich hierbei ist der Einsatz von professionellen Management- und File-Sharing-Systemen wie etwa von Commvault, um die stetig wachsenden Datenmengen einfacher zu verwalten. Ein Ziel sollte beispielsweise sein, bei einer Verbraucher-Anfrage innerhalb kürzester Zeit relevante Daten auf Knopfdruck bereitstellen zu können.

Jörg Kranepuhl

DSGVO, KRITIS und Cybercrime – Informationssicherheit ist Chefsache

Informationssicherheit ist einer der wichtigsten Erfolgsfaktoren der Digitalisierung: IT-Infrastrukturen bilden das Rückgrat der digitalen Transformation, Daten sind für Unternehmen der Grundstoff neuer Geschäftsmodelle. Nur wenn gewährleistet ist, dass Infrastrukturen und Daten vor Missbrauch, Angriffen und Diebstahl geschützt sind, werden neue Geschäftsmodelle funktionieren.

Mit Informationssicherheit allein lässt sich kein Geld verdienen – es sei denn, man ist Anbieter von Sicherheitstechnologien. So lautet ein häufiger Einwand. Mag sein: Informationssicherheit muss aber als conditio sine qua non die Grundlage aller digitalen Projekte sein.

DSGVO und KRITIS

Die Gesetzgeber auf nationaler und europäischer Ebene haben das verstanden und mit der EU-Datenschutz-Grundverordnung (DSGVO) sowie dem seit 2015 gültigen IT-Sicherheitsgesetz wichtige Grundlagen für den Schutz von Daten und Infrastrukturen geschaffen. Die DSGVO regelt grenzüberschreitend vor allem den Schutz personenbezogener Daten, während das IT-Sicherheitsgesetz dazu dient, mehr Sicherheit für informationstechnische Systeme zu erreichen, speziell für Unternehmen der so genannten „Kritischen Infrastrukturen“ (KRITIS – Unternehmen aus Branchen wie Energie, Ernährung, Finanzen, Gesundheit, Informationstechnik und Telekommunikation, Medien und Kultur, Transport und Verkehr und Wasser, sofern sie für das Funktionieren von Infrastrukturen und die Versorgung der Bevölkerung unverzichtbar sind.).

Ein zentraler Auftrag an alle betroffenen Unternehmen ist die Einführung eines Information Security Management Systems (ISMS). Das ISMS umfasst dabei nicht nur die „klassische“ IT des Unternehmens, sondern fokussiert speziell auf den Teil der Operational-Technology-Netzwerke (OT-Netzwerke). Hierzu zählen beispielsweise die vernetzten Steuer- und Leitsysteme im Energie- und Transportwesen (Umspannwerke, Sortieranlagen etc.) sowie die gesamte vernetzte Medizintechnik in Krankenhäusern. Damit rücken Systeme in den Fokus, die bislang oft weniger der IT, sondern den Ingenieur- und Fachabteilungen zugeordnet waren.

Die erste Rechtsverordnung vom Mai 2016 betrifft die KRITIS-Sektoren Energie, Informationstechnik und Telekommunikation sowie Ernährung und Wasser. Die zweite Rechtsverordnung betrifft die übrigen KRITIS-Sektoren Finanzen, Transport und Verkehr sowie Gesundheit. Sie wurde am 29. Juni 2017 veröffentlicht. Für die DSGVO gilt noch bis zum 25. Mai 2018 eine Übergangsfrist. Erst dann treten die neuen Regelungen ausnahmslos in Kraft.

Dass die Gesetzgeber DSGVO und IT-Sicherheitsgesetz ernst meinen, lässt sich nicht zuletzt am Strafenkatalog bei Verstößen ablesen: Im Fall der EU-Verordnung können die Strafen bis zu bis zu 300.000 Euro im Einzelfall und in der Summe bis zu 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr betragen. Bei Verstößen gegen die Vorschriften des IT-Sicherheitsgesetzes drohen den Betreibern kritischer Infrastrukturen Bußgelder bis zu 100.000 Euro.

Über die Strenge der Sanktionen lässt sich durchaus streiten. Die Höhe des Bußgeldes und die finanziellen Folgen beim Ausfall kritischer Infrastrukturen stehen oft in keinem vernünftigen Verhältnis, sagen Kritiker. Dennoch sind die neuen Sicherheitsgesetze inhaltlich wichtig und richtig: Die DSGVO ist gesetzlich verankerter Verbraucherschutz. Die Vorschrift schafft damit eine der unverzichtbaren Grundlagen digitaler Geschäftsmodelle auf Basis von Daten. Und KRITIS schützt das wichtigste Kapital der digitalen Transformation, das in den digitalen Infrastrukturen gesellschaftlich unverzichtbarer Branchen liegt und vor Diebstahl und Sabotage geschützt werden muss.

Social Engineering und Cybercrime

Die Gesetzgeber auf europäischer und nationaler Ebene haben ihren Job erledigt, jetzt sind die Unternehmen gefragt, ihrerseits die geeigneten Maßnahmen für den Schutz von Infrastrukturen und Daten zu ergreifen.

Einer der größten Schwachpunkte für Cyberangriffe in Unternehmen sind nach wie vor die eigenen Mitarbeiter. Angriffe finden oft über das private Umfeld von Mitarbeitern mit dem Ziel statt, Zugang zu geschützten Infrastrukturen und sensiblen Daten zu bekommen (oft über „Social Engineering“). Folgerichtig müssen wirksame Maßnahmen auch hier ansetzen. Dazu kommen Sicherheitsmechanismen, die flexibel in der Lage sind, auf sich ständig verändernde Bedrohungsszenarien reagieren zu können.

Mobiles Arbeiten muss geschütztes Arbeiten sein

Zu den schützenswerten Gütern in den Unternehmen gehört auch das mobile Arbeiten, das eine hohe Flexibilität mit sich bringt, von der Mitarbeiter und Unternehmen gleichermaßen profitieren. Aber private Endgeräte für berufliche Zwecke zu verwenden, ist nicht ohne Risiko: Geräte können entwendet werden oder verloren gehen, Daten und Datenzugänge so Dritten offenstehen. Allerdings besitzen einer Studie von Sopra Steria Consulting von Anfang 2017 zufolge immer noch vier von zehn Unternehmen keine Mobilgeräteverwaltung. Das heißt also, dass in diesen Unternehmen Sicherheits-Updates und -einstellungen nicht zentral durchführt werden. Zudem fehlen einem Drittel der Firmen übergreifende Sicherheitsrichtlinien für das mobile Arbeiten und den Gebrauch mobiler Endgeräte. Diese Unternehmen überlassen die Absicherung privater Geräte weitgehend den Anwendern. Da diese nicht notwendigerweise verlässlich Sicherheits-Updates durchführen oder Unternehmensdaten von privaten Daten separieren, droht der Verlust sensibler geschäftlicher Informationen, der den aktuellen Sicherheitsgeset-

Dr. Gerald Spiegel, Leiter Information Security Solutions, Sopra Steria Consulting

zen zufolge mit den oben genannten Sanktionen verbunden sein kann und – schlimmer – die mit der Digitalisierung verbundenen Geschäftsziele und -modelle ad absurdum führt.

Sicherheit ist strategische Unternehmensaufgabe
IT-, Geräte- und Datensicherheit zu gewährleisten und damit die gesetzlichen Bestimmungen einzuhalten, ist kein trivialer Job, der sich mit wenigen technischen Handgriffen erledigen lässt. Es ist vielmehr in der digitalen Transformation eine strategisch wichtige Unternehmensaufgabe, die vom Top-Management getragen sein muss und von qualifizierten Fachkräften ausgeübt wird.

Es sind zuerst die Führungskräfte eines Unternehmens, die Verantwortung für das Risikomanagement und für Notfallpläne tragen. Sie müssen sich wiederum auf den Rat ihrer Fachleute im Unternehmen verlassen können, um Fehlinvestitionen und – angesichts der neuen Bestimmungen – vor allem teures Fehlverhalten zu vermeiden. Dabei sind realistische Einschätzungen wichtig, frei von Befindlichkeiten und Gewohnheiten: Die größte Gefahr für die Sicherheit von Daten sind aus meiner Sicht Selbstzufriedenheit und Selbstüberschätzung in Sachen IT- und Cyber-Security.

Laurens van der Blom, Software Architect, BCT Deutschland

Es gibt diverse Studien, die aber genau das belegen: Gerade Geschäftsführer scheinen oft die Sicherheit ihres Unternehmens durch eine Art rosa Brille zu sehen und glauben, sie seien besser gegen interne Sicherheitsverstöße und externe Angriffe gerüstet, als sie es tatsächlich sind oder wähnen sich als nicht attraktiv für einen Angreifer. Da wundert es nicht, dass in vielen Unternehmen eine breite Lücke zwischen der realen Widerstandsfähigkeit und einer Bedrohungslage klafft, die immer ernster wird.

Awareness für Sicherheit schaffen, die die oberste Führungsebene der Unternehmen nicht ausnimmt, ist hier eine wichtige Aufgabe. Dazu gehören aber auch gezielte Investitionen in intelligente Bedrohungserkennung, prädiktive Datenanalysen und Lösungen für die Früherkennung von Angriffen. 100-prozentige Sicherheit bietet bekanntermaßen keiner dieser Ansätze, aber sie tragen ganz wesentlich zu einer signifikanten Verringerung des Schadensrisikos und der Folgen gravierender Sicherheitsvorfälle bei.

Digitalisierung ist Herausforderung und Lösung in einem
Die zunehmende Digitalisierung bringt nicht nur immer neue Bedrohungsszenarien hervor, sie liefert zugleich auch einen großen Teil der Antwort. Künstliche Intelligenz ist über Mustererkennung in großen Datenmengen in der Lage, untypische Abweichungen und damit potenzielle Angriffe von außen zu erkennen und zunehmend automatisch abzuwehren. Mobile Device Management und Unternehmensrichtlinien für mobiles Arbeiten können Datenklau und -verlust nicht gänzlich verhindern, aber typische Einfallstore für Eindringlinge schließen. Schließlich ist die Digitalisierung auch das Mittel der Wahl, um flexibel auf wechselnde und neue Angriffsszenarien reagieren zu können.

Ziel der Unternehmen muss ein maximal digitalisiertes und dynamisches IT-Sicherheitsmanagement sein, das einer Institution jederzeit eine angemessene Cyber-Security garantiert. Das ist am Ende eine technische Aufgabe der Unternehmens-IT, wird aber ohne die Unterstützung des Top-Managements nicht funktionieren.

Gerald Spiegel

1.4.2 Lösungen

So klappt's mit der Informationssicherheit

Beim Umgang mit Informationen bietet das Thema Sicherheit großes Diskussionspotential, denn die Gefahr für Wirtschaft und Gesellschaft wächst im digitalen Zeitalter stetig. Für Schutz sorgen Entwickler und Nutzer von Softwarelösungen mittels verschiedener Maßnahmen.

Cyberkriminalität ist ein düsteres Anhängsel des digitalen Wandels: Es wird immer einfacher, virtuell in Unternehmen einzubrechen. Meist zielen Kriminelle dabei auf finanziellen Gewinn ab, doch auch das Vertrauen ins Unternehmen leidet. Dass Datenschutz im digitalen Zeitalter höchste Priorität hat, offenbart der Sicherheitsrahmen der EU-Datenschutz-Grundverordnung (EU-DSGVO): Er gibt vor, dass Unternehmen sensible Daten nachweislich schützen müssen. Auch Softwareanbieter stehen in der Verantwortung und müssen bei Verstoß gegen die EU-DSGVO Bußgelder leisten. Zu den relevanten Kriterien des Sicherheitsrahmens zählen Menge und Art der zu verarbeitenden Informationen, deren Speicherfrist sowie die Zugänglichkeit.

Die EU-DSGVO gibt außerdem vor, dass die Hard-und Software bereits während des Entwicklungsprozesses auf Schwachstellen getestet werden sollte, um Sicherheitslücken zu minimieren. Nach den Methoden „Security by Design" und „Privacy by Design" sollten also spezifische Schutzmaßnahmen eingehalten werden, bei denen Vertraulichkeit, Verfügbarkeit und Integrität von Informationen die drei Security-Kernprinzipien bilden. Sensible Daten müssen vor unberechtigten Zugriffen, Manipulation und Löschung genauso geschützt werden wie die eigentlichen Informationssysteme.

Das Layered Security Framework

Um es Hackern schwer zu machen, hat sich bei der Softwareentwicklung das Layered Security Framework von Alex Berson und Larry Dubov bewährt: ein mehrschichtiges Modell für den sicheren Umgang mit Informationen. Dabei gelten für jede Schicht der Softwarearchitektur (Data, Application) und der technischen Infrastruktur (Platform, Network, Perimeter) eigene Sicherheitsmaßnahmen. Von innen nach außen bauen sie aufeinander auf; die jeweils überlagernde Schicht kompensiert die Sicherheitslücken der unteren.

Die Softwarearchitektur
Um Daten (Data) und Anwendungen (Application) als Schichten der Softwarearchitektur zu sichern, ist eine zweistufige Authentifizierung und Autorisierung bedeutsam: Wer ist wozu berechtigt? Dies steuert das Identity Access Management zentral und gibt Unternehmen einen Rahmen, in dem sie geschützt in einer Private- oder Public-Cloud arbeiten können. Wichtig ist zudem der begrenzte Datenzugang durch ein Data-Visibility-Konzept mit entsprechenden Sicherheitszertifikaten. Darüber hinaus sollten Web-Lösungen mithilfe der führenden Sicherheitsrichtlinien des Open Web Application Security Project auf Schwachstellen untersucht worden sein.

Die technische Infrastruktur
Die technische Infrastruktur teilt sich in die internen Schichten Platform und Network sowie in die übergreifende Perimeter-Schicht: Zur Platform zählen Betriebssysteme, Web- bzw. Application-Server sowie Datenbanken und Dateisysteme. Die Verbindungen zu ihnen via Kabel oder WLAN können unterschiedlich geschützt werden: durch verschlüsselte Datenspeicher, die richtige Port-Konfiguration, aktuelle Updates, blockierte Systeminformationen sowie strenge Autorisierungsmaßnahmen.

Weitere Präventivmaßnahmen innerhalb des lokalen Netzwerks (Network) sind die Verschlüsselung der Datenübertragung anhand von Transport Layer Security sowie die sichere Konnektivität durch Firewalls. Diese Perimeter-Schicht ermöglicht die Verbindung zwischen einem geschlossenen und einem öffentlichen Netzwerk und wird etwa durch ein Virtual Private Network (VPN) sowie VPN-fähige Firewalls geschützt. Ein Access Point sorgt wiederum für eine sichere WLAN-Umgebung; ein Security Information Event Management erkennt, wann und wo der Umgang mit Daten von geltenden Compliance-Vorschriften abweicht.

Weitere Sicherheitsmaßnahmen
Für ein ganzheitliches Informationssicherheits-Managementsystem (ISMS) sollten Unternehmen zudem organisatorische und verfahrenstechnische Maßnahmen treffen. Ein ISMS berücksichtigt besonders die Privatsphäre und die drei Security-Kernprinzipien. Obwohl in der ISO-Norm nicht explizit erwähnt, gibt es zudem die physische Sicherheit, die den Zutritt zu Serverräumen, aber auch Netzwerkkabel oder die Reichweite der WLAN-Verbindung betrifft. Für cloudbasierte Arbeitsumgebungen sind Cloud-Provider, deren Rechenzentren nach ISO 27001 zertifiziert sind, die richtigen Sicherheitspartner.

Fazit
Informationssicherheit ist von großer Bedeutung, wollen sich Unternehmen vor unbefugtem Zugriff auf ihre Daten schützen. Diese Sicherheit liegt auch in der Verantwortung der Software- sowie Cloud- Anbieter, mit denen sie zusammenarbeiten. Dabei stehen Vertraulichkeit, Integrität und Verfügbarkeit der Informationen im Fokus. Um finanziellen wie immateriellen Schäden durch Hacker vorzubeugen, bedarf es Zeit und Geld – angesichts des steigenden Sicherheitsbewusstseins von Kunden, Lieferanten und Partnern eine wichtige Investition.

Laurens van der Blom

Cybersicherheit im Mittelstand mit SIEM

IT-Leiter in Deutschland spüren bereits, dass sich die Gefahrenlage grundsätzlich verändert hat. Ransomware-Angriffe und andere ausgefeilte Schädlinge wüten in der Bundesrepublik, zudem gibt es neue Vorgaben wie die EU-Datenschutzgrundverordnung (DSGVO), das IT-Sicherheitsgesetz oder Compliance-Richtlinien. Bei Verstößen dagegen droht die EU oder der Vertragspartner mit harten Strafen.

Die Zeit ist knapp, gerade die DSGVO gilt für fast alle Unternehmen mit Kunden in Europa ab Mai 2018 – dann ist die Schonfrist vorbei. Sogar im Falle, dass Budgetrücklagen für zusätzliches Personal vorhanden wären, ist die Lage auf dem Arbeitsmarkt für IT-Sicherheitsexperten angespannt, sodass Organisationen sich nach anderen Lösungsansätzen umschauen müssen. Eine passende Lösung gerade für den Mittelstand ist der Einsatz einer (SIEM) Security Information and Event Management-Software. Einerseits hilft sie ihnen, die Vorgänge innerhalb des eigenen Netzwerks zu optimieren, andererseits unterstützt sie sie auf dem Weg zur Erfüllung der Vorgaben der DSGVO. Zusätzlich hilft sie bei der Abwehr von Schadsoftware wie Verschlüsselungstrojanern.

Digitale Integration verstehen und richtig absichern
Der digitale Wandel der Herstellungsprozesse und die Vernetzung der Office IT-Welt mit der Produktionswelt stellen viele Branchen vor eine große Herausforderung. Nicht nur, weil immer mehr Prozesse auf eine Fernsteuerung umgestellt werden, sondern auch, weil durch diese zunehmende Vernetzung noch mehr als zuvor die Gefahr von Spionage und Sabotage droht. Cyberattacken in Verbindung mit schlecht abgestimmten IT-Prozessen können Verwaltungs- und Produktionsprozesse empfindlich stören. Eine Lücke im Sicherheitssystem zieht schwerwiegende Folgen nach sich. Dazu gehören

Pascal Cronauer, Country Manager DACH, LogPoint

Tobias Theelen, Head of Marketing & Sales, esatus AG

unter anderem Produktionsstörungen und –ausfälle sowie Datenmanipulation und Datendiebstahl.

Ein weiterer Risikofaktor schlummert in der gängigen Praxis des zunehmenden Outsourcings. Grundsätzlich ist der Einsatz von Service-Providern wichtig, um die eigenen Ressourcen auf die Kernkompetenzen fokussieren zu können, allerdings müssen Schutzmechanismen entsprechend angepasst werden. Gerade Patente und digitale Assets sind für Konkurrenten interessant und daher wertvolle Ziele von Angriffen. Doch die Aktivitäten reichen inzwischen über eine einfache Spionage hinaus. Cyber-Attacken auf Stromversorger in der Ukraine[1] oder der Angriff auf ein deutsches Stahlwerk in Essen[2] haben bereits angedeutet, wozu Cyberkriminelle inzwischen fähig sind. Zudem können durch Malware-as-a-Service Angriffe einfach und schnell auch durch Laien ohne Fachwissen per Mausklick gekauft werden.

Mit SIEM gegen Ransomware

Patch-Management ist ein wichtiger Baustein im Kampf gegen Ransomware. IT-Administratoren sollten die Netzwerkbewegungen und vor allem Log-Einträge innerhalb ihrer Organisation genau beobachten. SIEM nimmt ihnen diese Aufgabe zu einem nicht unerheblichen Teil durch Automatisierung ab. Es sammelt, korreliert und wertet Log-Daten aus und warnt bei sicherheitsrelevanten Zwischenfällen durch vorkonfigurierte Alarme. Zusätzlich reichern Informationen unterschiedlichster Hardware und Software von Switches, Firewalls usw. aber auch von Mail- oder Webservern und spezifischem Equipment die Analysen an. Sensoren für Netzwerkdienste wie Ping, HTTP, SMTP, FTP, POP3 oder verschiedenste Datenbanken dienen ebenfalls als Datenquellen, die über Schnittstellen betrachtet werden können.

Fazit – Mit regelmäßigen Updates Schritt halten

Das Angebot an Security-Lösungen ist riesig, doch die wenigsten Angebote sind für Mittelständler in Deutschland geeignet. Häufig liefern Hersteller nur Teillösungen und die dringendsten Probleme bleiben ungelöst. Noch nie war das Bewusstsein für Cybersicherheit größer und IT-Verantwortliche sind sich des Handlungsbedarfs bewusst, allerdings sollten Entscheidungen wegen der Vielzahl der Herausforderungen mit Bedacht gewählt werden.

Eine SIEM-Lösung eignet sich für Unternehmen, die sich auf die DSGVO, Ransomware und neue Compliance-Anforderung einstellen müssen und dabei keine umfangreichen, neuen Projektbudgets bereitstellen möchten. Pascal Cronauer

[1] FAZ 2016: „Die Hackerdämmerung“ http://www.faz.net/aktuell/wissen/physik-mehr/ukrainischer-stromausfall-war-ein-hacker-angriff-14005472.html
[2] heise 2014: „BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk“ https://www.heise.de/security/meldung/BSI-Sicherheitsbericht-Erfolgreiche-Cyber-Attacke-auf-deutsches-Stahlwerk-2498990.html

IT-Sicherheitsgesetz und EU-Datenschutzgrundverordnung

Effiziente Projektierung zur Erfüllung neuer Anforderungen an den Stand der Technik

Die letzten Jahre waren geprägt von verschiedenen neuen Gesetzgebungen, insbesondere im Bereich des Datenschutzes und der IT-Sicherheit. Die Anforderungen, die aktuell am stärksten in Ihrer Umsetzung in Deutschland diskutiert werden, sind das IT-Sicherheitsgesetz (ITSiG) und die EU-Datenschutzgrundverordnung (EU-DSGVO). Insbesondere die EU-DSGVO, welche am 25.05.2018 den Datenschutz in der gesamten EU neu aufstellen wird, schafft Anforderungen an Prozesse und Sicherungsmaßnahmen für Technologien, die personenbezogene Daten verarbeiten. Werden die neuen Anforderungen nicht erfüllt, so werden Sanktionen in Höhe von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes des Unternehmens fällig, je nachdem welcher Betrag höher ist. Das Thema des technischen Datenschutzes (Data Privacy by Design and by Default) war nie relevanter. Im BDSG (Bundesdatenschutzgesetz) waren Regelungen zur Absicherung von Technologien durch technische und organisatorische Maßnahmen (TOM) noch als „soft law“ definiert, also ohne konkrete Sanktionierung bei Nicht-Erfüllung. Dies ändert sich durch die EU-DSGVO, da nun bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes fällig werden können, wenn Richtlinien des technischen Datenschutzes nicht umgesetzt sind. Darüber hinaus stellt das IT-Sicherheitsgesetz neue Anforderungen an die IT-Sicherheit für Betreiber kritischer Infrastrukturen und Betreiber von Telemedien. Beide Gesetzgebungen haben einen wesentlichen Faktor gemeinsam: Den Stand der Technik.

Der Stand der Technik ist ein bewusst offen definierter Rechtsbegriff. Nach ITSiG und EU-DSGVO sollen IT-Sicherheitsmaßnahmen und der technische Datenschutz in ihren technischen und organisatorischen Maßnahmen den aktuellen Stand der Technik nachweisen. Im Gesetz selbst (EU-DSGVO) ist als Methode gemäß Stand der Technik lediglich die Pseudonymisierung genannt, durch die Datensätze bspw. durch Verschlüsselungen so verändert werden, dass sie keine Identifizierbarkeitsfaktoren für die jeweilige Person beinhalten. Da der Rechtsbegriff sehr offen definiert ist, haben viele Unternehmen keinen klaren Durchblick, was dieser Stand der Technik nun für einen selbst bedeutet. Eine erste Einordnung, was der aktuelle Stand der Technik ist, gibt die Handreichung zum Stand der Technik im Sinne des IT-Sicherheitsgesetzes vom TeleTrusT – Bundesverband IT-Sicherheit e.V. aus dem Jahre 2016. Hier werden Anforderungen an sichere Vernetzung, sichere Internetverbindungen, Digital Enterprise Security, Client- und Serversicherheit, Mobile Security sowie gängige Standards und Normen zur Nachweisung des Stands der Technik von IT-Sicherheitsexperten und Juristen beleuchtet.

Unternehmen, die nicht schon durch das bereits eingetretene ITSiG den Stand der Technik erfüllen müssen, sollten sich priorisiert mit Bestandsanalysen der Sicherungsmaßnahmen von Technologien beschäftigen, die personenbezogene Daten verarbeitet, um zum Stichtag des 25.05.2018 konform zu den neuen Anforderungen der EU-DSGVO zu sein. Für diese Herausforderung ist ein Projektteam aus IT-Sicherheitsexperten und Juristen notwendig, um die juristischen Anforderungen mit wirkungsvollen Methoden der IT-Sicherheit zu kombinieren. Betreiber kritischer Infrastrukturen oder Anbieter von Telemedien, die sich mit noch keiner der beiden neuen Gesetzgebungen beschäftigt haben, sollten eine Kombination beider Problemstellungen anstreben. Im Unternehmensberatungskontext fällt oft auf, dass gerade größere Unternehmen oftmals Projektieren ohne eine Abstimmung mit anderen Fachabteilungen voranzustellen. Als Konsequenz werden die gleichen Problemstellungen individuell von den jeweiligen Fachabteilungen behandelt, mehrere Software-Tools implementiert, welche die gleichen Problemstellungen lösen sollen und Synergieeffekte verschiedener Herausforderungen völlig ausgeblendet. Dies ist ineffizient und erzeugt unnötige Kosten in mehrstelliger Millionenhöhe. Eine effiziente Kombination beider Herausforderungen für Betreiber kritischer Infrastrukturen oder Betreiber von Telemedien könnte wie folgt aussehen:

1. Schnittmengen und GAP-Analyse

Im ersten Schritt sollten Unternehmen Technologien, Prozesse und IT-Infrastrukturkomponenten identifizieren, die sowohl unter den Schutzbedarf des technischen Datenschutzes nach EU-DSGVO fallen, als auch vom ITSiG betroffen sind. Sind diese identifiziert, sollte im Zuge einer GAP-Analyse die Kluft zwischen IST-Zustand und SOLL-Zustand der neuen regulatorischen Anforderungen erörtert werden. Aus dieser Analyse lassen sich Maßnahmen ableiten, die umgesetzt werden müssen, um in Zukunft gesetzeskonform agieren zu können. Eine Betrachtung der Technologien, Prozesse und IT-Infrastrukturkomponenten sollte dabei nicht nur durch Juristen erfolgen, sondern auch durch IT-Sicherheitsspezialisten, die mit „Bits und Bytes“ umgehen können. Die identifizierten GAPs zu beiden neuen regulatorischen Anforderungen sollten priorisiert behandelt werden, da diese mit den höchsten Risiken für Unternehmen einhergehen, wenn die regulatorischen Anforderungen nicht beachtet werden.

2. Technische Nachbesserung

Die identifizierten GAPs aus Schritt 1 sollten im nächsten Schritt eliminiert werden. GAPs mit hohem IT-Impact benötigen eine höhere Vorlaufzeit zur Beseitigung als solche, die reine Dokumentationen voraussetzen. Die Erstellung eines Zeitplans unter Berücksichtigung des IT-Impacts scheint also der effizienteste Weg, um technische Nachbesserungen bis zum Stichtag des 25.05.2018 bewältigen zu können. Wer noch nicht gestartet hat, sollte dies schleunigst tun.

3. Dokumentationen

Sind die technischen Nachbesserungen abgeschlossen, sollten alle fehlenden Dokumentationen erstellt werden und bestehende Dokumentationen nachgebessert bzw. erweitert werden. Im Zuge der Dokumentationserstellung sollte man sich an den Richtlinien der ISO 27001 orientieren. Dadurch ebnet man den Weg zu einer ISO 27001 Zertifizierung, die mit hoher Wahrscheinlichkeit in Zukunft der Maßstab zur Vorweisung der Erfüllung des Stands der Technik werden kann.

4. Kontinuierliches Information Security Management System (ISMS)

Sind technische und dokumentarische Anforderungen bis zum Stichtag umgesetzt, ist das „Projekt“ IT-Sicherheit noch lange nicht abgeschlossen. Angriffsvektoren nehmen von Jahr zu Jahr zu, bewährte Verschlüsselungsverfahren könnten durch steigende Rechenleistung leicht zu entschlüsseln werden und der Stand der Technik ist morgen schon nicht mehr der, welcher er heute ist. Die Implementierung eines kontinuierlichen Information Security Management Systems ist nicht nur Voraussetzung zur Erlangung einer ISO 27001 Zertifizierung. Wenn Unternehmen IT-Sicherheit und Datenschutz wirklich ernst nehmen und ihre Daten umfassend schützen möchten, sollten sie in regelmäßigen Abstände den Stand der Technik in technischen und organisatorischen Maßnahmen zur Absicherung gegen Cyberangriffe und Datenverluste überprüfen.

Eine gemeinsame Betrachtung des ITSiG und der EU-DSGVO im Sinne des Stands der Technik ist kosteneffizient und führt zu einer klaren Definition der IT-Faktoren im Unternehmen, die sich im Falle eines Angriffs am negativsten auf das Unternehmen auswirken könnten. Leider ist der dargestellte Weg der Projektierung in vielen Unternehmen reines Wunschdenken, da Fachabteilungen zu unabhängig voneinander agieren und meist die generelle Aufmerksamkeit für die Thematik nicht vorhanden ist. Zu sehr werden regulatorische Anforderungen, insbesondere im Datenschutz, als notwendige Übel wahrgenommen, welche so lange ignoriert werden, bis Audit-Findings Unternehmen zur Handlung zwingen. Das bis zu diesem Zeitpunkt bereits Gigabytes an kritischen Daten durch Cyberangriffe in falsche Hände geraten können, scheint oftmals nicht in der Aufmerksamkeit zu stehen. Dies bestätigen zuletzt die gezielten Angriffe auf Größen der Unternehmensberatungsbranche. Daher ist zu empfehlen: Projektieren Sie frühzeitig, stärken Sie Ihre Aufmerksamkeit zu Fragestellungen der IT-Compliance und erschließen Sie Synergiepotentiale! Tobias Theelen

2. BLOCKCHAIN

Blockchain – einer der meist gehörten, wenn nicht der meist gehörte technische Begriff des Jahres. Doch wie so oft wenn eine breite Öffentlichkeit beginnt über ein neues Thema zu diskutieren herrscht zunächst Verwirrung. Es gibt viele Stimmen, viele Meinungen und viele eigentlich verschiedene Konzepte, die unter dem Begriff Blockchain verstanden werden. Die Einen meinen die Bitcoin Blockchain, die Anderen digitale Währungen im allgemeinen, wieder andere sogenannte Smart Contracts und Digitale Tokens. Gerade deshalb ist es so wichtig neben der technischen Definition des Begriffs auch die unterschiedlichen Themen zu verstehen, die oft weniger trennscharf unter dem Begriff Blockchain zusammengefasst werden. Was also sind die gemeinsamen Themen, die die unterschiedlichen Diskussionen vereint?

Festhalten lässt sich, dass es eine Vielzahl an Blockchains gibt. Die Prominenteste ist wohl die Bitcoin-Blockchain. Genutzt werden diese Blockchains aktuell meist für finanzielle Transaktionen, doch sind sie keineswegs auf diesen Einsatzbereich beschränkt. Eine Vielzahl an weiteren Einsatzmöglichkeiten wird zum Beispiel mit der Ethereum-Blockchain bereits aktiv erprobt. Ein weiterer Kernaspekt von Blockchains ist, dass es sich um verteilte Systeme handelt, die auf Millionen von Computern ausgeführt werden. Grundlage aller Blockchains bilden Verschlüsselung und digitale Signaturen, die die Fälschungssicherheit der Einträge garantieren. Gebildet wird eine Blockchain dann schlussendlich von einer Liste von Datensätzen, an die nur neu Einträge angehängt, alte Einträge jedoch nicht gelöscht werden können.

Diese neuartige Form der dezentralen Datenhaltung bringt neben einer Vielzahl an Möglichkeiten zunächst auch eine Vielzahl an Herausforderungen mit sich: Wie kann Manipulation verhindert werden? Wie erreicht man Einigkeit? Können sich die Regeln des Systems ändern? Diesen Fragen und Chancen widmen sich die nun folgenden Beiträge und beleuchten das Thema Blockchain aus den unterschiedlichsten Richtungen.

MEIST GEKLICKT –
Unsere erfolgreichsten Blog-Beiträge

Unsere Beiträge wurden insgesamt **82.429 Mal** geklickt*

Beiträge zum Thema **BLOCKCHAIN** erhielten **51.204** Klicks.

	Autor	Thema
#1	**Stefan Zimprich**	Mittelstand plant die Blockchain-Revolution **Seite 73**
#2	**Dr. Stefan Hopf**	Blockchain als Schlüsseltechnologie für das Internet der Dinge? **Seite 67**
#3	**Henning Neu**	Die Blockchain und die Kryptowährungen – das smarte Geld für eine einfache Welt **Seite 74**
#4	**Dr. Axel von Perfall**	Mit der Blockchain die Energiewende meistern? **Seite 77**
#5	**Matthew Key**	Blockchain: the art of the possible **Seite 76**

***Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 01. August 2017 – 14. Februar 2018.**

INHALT

2.1 TECHNIK

2.1.1 Bitcoin

Nikolai Fischer, Medieninformatik-Student im Master, LMU München

Wie funktioniert eigentlich Bitcoin?

Die revolutionäre Technologie Bitcoin existiert mittlerweile seit fast 10 Jahren und trotzdem können sich auch heute viele noch nichts darunter vorstellen. Häufig wird sie mit Begriffen wie “Nerd-Geld” oder “Darknet-Währung” abgewertet und dennoch hätte sie die Voraussetzungen zum Mainstream-Phänomen. Kurz zusammengefasst ist Bitcoin eine dezentrale Online-Währung, die auf der Blockchain Technologie basiert. Alleine der kompliziert klingende Begriff “Blockchain” schreckt bereits viele davon ab, sich weiter mit dem Thema zu beschäftigen. Dabei ist Bitcoin auf einer konzeptuellen Ebene weit verständlicher als einem technische Erklärungen glauben machen wollen:

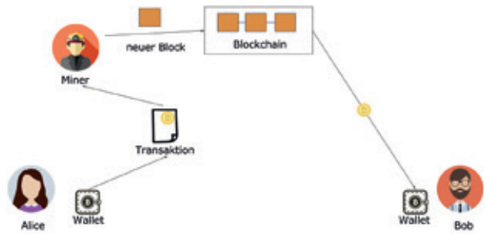


Abbildung: Vereinfachte Darstellung des Bitcoin Systems, Icons designed by Freepik from Flaticon

Transaktionen – Bitcoins Überweisungsträger

Um Bitcoin auf den Grund zu gehen, sehen wir uns im Folgenden an, was passiert, wenn ein Teilnehmer Bitcoin an einen anderen überweist – nach Informatik-Tradition nennen wir sie Alice und Bob. Ein Grundbaustein der Bitcoin-Technologie sind ihre Transaktionen. Diese beinhalten in etwa dieselben Informationen wie ein Überweisungsträger bei der Bank: **Wer** sendet **wie viel** Geld **wohin**? In unserem Beispiel nimmt Alice die gewünschte Menge Bitcoin aus ihrer Wallet (eine digitale Brieftasche für Bitcoin) und erstellt eine neue Transaktion. Als Empfänger trägt sie Bob’s Bitcoin Adresse ein: Eine eindeutige Zeichenfolge, vergleichbar mit einer Kontonummer.

Miner – die Erbauer der Blockchain

Jetzt kann Alice die Transaktion in das Bitcoin Netzwerk senden. Dieses besteht aus vielen miteinander verbundenen Teilnehmern, womit es zu den sog. P2P-Netzen gehört. Durch dieses dezentrale Netzwerk erfahren **Miner** von Alice’s Transaktion. Miner sind User, auf deren Rechner spezielle Mining Software läuft, die mehrere Transaktionen zu einem **Block** zusammenfassen. Der Mining Vorgang besteht aus aufwendigen Rechenoperationen, durch welche die Manipulation eines Blocks erschwert wird. Hat ein Miner einen Block gebildet, bekommt er für die getane Arbeit eine Belohnung in Form von Bitcoin. Diese werden dem System neu hinzugefügt – der Vorgang ist also vergleichbar mit dem Drucken von neuem Bargeld. Nun hängt der Miner den neuen Block an die Blockchain. Wie der Name schon sagt, handelt es sich bei der **Blockchain** um eine Aneinanderreihung von Blöcken. Da diese wiederum Transaktionen beinhalten, fungiert die Blockchain als Grundbuch aller Transaktionen. Bitcoin erlaubt es jedem User, eine Kopie dieses Grundbuchs zu speichern. Dabei sorgen verschiedene Mechanismen dafür, dass alle Benutzer ihre Blockchains untereinander synchronisieren. Somit entsteht keine zentrale Quelle unüberprüfbarer Wahrheit, sondern eine verteilte Datenbank. Bob sieht nun in der Blockchain, dass eine Transaktion an ihn gesendet wurde. Nachdem er seine Identität durch kryptographische Methoden bewiesen hat, kann Bob die Bitcoin in seine Wallet legen und die Überweisung ist abgeschlossen.

Ist Bitcoin sicher?

Die Sicherheit Bitcoins ergibt sich aus dem Mining Vorgang. Will ein Angreifer eine Transaktion verändern, muss er den entsprechenden Block sowie alle Blöcke nach ihm in der Chain neu minen. Da das Mining ein sehr aufwendiges Unterfangen ist, müsste der Angreifer über große Rechenleistung verfügen: Tatsächlich erfordert es mindestens 51% der Rechenpower des Bitcoin Netzwerks, um die Blockchain manipulieren zu können. Durch die große Anzahl von Minern im Netzwerk gestaltet sich dies allerdings so gut wie unmöglich und ist vor allem auch wirtschaftlich uninteressant.

Ist Bitcoin anonym?

Für viele Anwender ist das Versprechen der Anonymität ein bedeutender Vorteil. Interessanterweise gehört diese nicht zu den zentralen Design-Zielen der Bitcoin Technologie. Tatsächlich ist sie eher ein Nebeneffekt des Systems. Die Anonymität ergibt sich daraus, dass aus einer Bitcoin Adresse nicht (wie z.B. bei einer Kontonummer) auf die Identität des Besitzers geschlossen werden kann. Diese Verbindung nicht über andere Kanäle preiszugeben, liegt allerdings in der Verantwortung des Benutzers und wird vom System in keinster Weise erzwungen. Da insbesondere für den Währungstausch in der Regel die eigene Identität nachgewiesen werden muss, kann hierbei theoretisch der Urheber mancher Transaktionen ausfindig gemacht werden. Nichtsdestotrotz bietet Bitcoin einige technische Lösungen, um dies zu erschweren. Ein Beispiel hierfür ist die Verwendung von Einmal-Bitcoin Adressen, die lediglich für eine einzige Transaktion verwendet werden.

Betrachtet man das Bitcoin System in all seinen Facetten, so gestaltet es sich selbstverständlich etwas komplexer als eben dargestellt. Dementsprechend setzt ein vollständiges Verstehen auch Kenntnisse der allgemeinen Informatik-Grundlagen voraus. Fachfremde Verbraucher sollten sich vor dieser Tatsache allerdings nicht abschrecken lassen, denn: Bereits grobe Einblicke in die Thematik reichen aus, um die Bitcoin-Technologie im alltäglichen Gebrauch einzusetzen.

Nikolai Fischer

2.1.2 Funktionsweise Blockchain

Smart Contracts – Coded Computer Programs in the Blockchain Environment

When we take a look at today’s conventional contracts: Our monthly smartphone billings, working employee contracts, insurances, big trade agreements between companies… there is one instant keyword on our mind: **Complexity**.

Contracts are a pattern of profound legal language, rising numbers of paragraphs, covered eventualities and overall lengthy documents. All of this oftentimes makes them difficult to understand for wider audiences and even some more professional user groups. But even more, today’s conventional contracts are a core foundation of our modern society. They build a backbone for agreements on intentions between parties, applying existing laws in practice and are being enforced by supervising institutions.

Our whole life circles around the idea of rights and duties acquired by contractual practices.We expect our banking services to be available since we pay a monthly fee for them. We expect our insurances to address our issues because we have a contract which acquired these rights for paying a regulated yearly insurance fee. The list goes on and on. Conventional contracts, in short, are a last century concept, most times still based on physical paperwork, which was subsequently tried to be updated and improved for the digital age of the 21st century with mixed success so far.

Smart Contracts: Blockchain-executed computer programs

A smart contract is, compared to a conventional contract, at its lowest level: A computer program. It is coded by a developer and stored and deployed on a computational system. The big advantage of smart contracts is that these computational code programs are now stored on a blockchain, utilizing the possibility to be activated or triggered by the blockchain itself or activated from an external call, executing the capability to read and write data in the blockchain database or to interact with the blockchain state in general.

The code itself is not bound to the blockchain. It could be anything from object-oriented programming languages like Java, functional programming languages like Haskell or complex languages like Python, C++ or Pascal. Storing the information database-wise is often achieved by subsidiaries of SQL. Smart contract programs are therefore able to provide novel programming paradigm approaches to conventional contracts while simultaneously utilizing all the core benefits of the blockchain technology like advanced security, anti-fraud mechanisms and public data integrity as well as autonomy.

Ethereum, the leading smart contract blockchain framework as of today, utilizes the smart contract approach by having each user-deployed program being delivered with its own minimized version of a database connected to it. This database can only be modified by the smart contract program that owns it, thus meaning that if a user wants to change the program-connected database and subsequent data that it holds and processes, the user needs to access the program by a digitally signed message that needs to use one of the smart contract’s provided functions.

As an example for a simple smart contract execution to transfer money to another account, and since digital currency is still on of the most important blockchain and payment-related topics, an Ethereum blockchain user now wants to send 2 Ether coins to a another friend’s wallet.

Therefore, he sends a request to his deployed smart contract on the blockchain demanding to send 2 Ether tokens to another smart contract on the blockchain. He would call his smart contract at the blockchain address ‚0x1a2b3c4e5f6g7h‘ and its function ’send2EtherTokensTo(MyFriend)‘. The smart contract would register the request by the user, and since he digitally signed the request with his identifying account, the smart contract knows that he is eligible to use the contract. The smart contract function would now check its database for sufficient funds and triggers the next smart contract on the blockchain located at the address ‚MyFriend‘ with the send funds.

So in theory, the creation and deployment of a

Martin Kraft, M.Sc. student in media informatics, LMU Munich

Newsletter und mehr Beiträge: www.digitaleweltmagazin.de/blog

Dr. Martin Klapdor, Senior Solutions Architect, Netscout

contract has never been this simplified, usable by a wider audience and immediate in its execution on a distributed and fraud-secure ledger architecture.

Strict If-Then Principles barely cover all Contractual Scenarios so far

In reality however, the general use cases for smart contracts, which are ultimately the conventional contracts of today's world, are not that simply mappable to computer program code. Smart contracts generally gain advantages in logic-based scenarios. If ‚A' is called with parameter ‚B', execute ‚C'.

Our understanding of smart contract implementation as of today, which is a Touring-complete high level scripting language executed and validated on a virtual machine and stored and saved on top of a blockchain implementation, creates its own technological and logical limitations and dependencies. A smart contract implementation of a conventional contract is not able to contain any form of unenforceable terms, vaguely written paragraphs or non-deterministic outcomes.

The nature of the blockchain is that a smart contract is deployed once and remains valid forever. Non-alterable, non-removable and without the possibility to non-enforce a contract when demanded. A smart contract gets called and executed with no state possible in between. A party cannot decide if they want to enforce only parts of a contract or none together. The smart contract is called or not with everything else being handled by the smart contract program itself without interference from the outside world. These fundamental principles do not only need to be factored into running a smart contract, but need to be a major factor in the planning and creation of smart contracts early on.

Takeaways

So where do we stand with smart contracts?

Smart contracts are an immensely powerful and new incarnation of conventional contract approaches. They are a young and thriving technology, with the state of the art still being on an early ‚alpha level' status, developed by an active community improving this future technological implementation.

In theory, the application of smart contracts into real-world scenarios and fields does, per se, not include any boundaries. However, today's smart contracts are not yet simply applicable to a scenario without potential problems in terms of technological and logical limitations. Planning and special analysis of use-cases are still necessary to yield the benefits of smart contract implementation and blockchain technology in general. But ultimately, smart contracts show immense promise to improve some of the most business-critical components like transaction speed, anti-fraud methods and overall data accessibility and autonomy with the potential to be universally applicable and easy-to-use in future iterations.

Martin Kraft

2.1.3 Herausforderungen QOS

Chancen und Herausforderungen der Blockchain

Blockchain soll den Austausch von Daten sicherer machen und jede Transaktion fälschungssicher dokumentieren. Doch damit die Technologie halten kann, was sie verspricht, müssen noch einige technische Hürden überwunden werden. Service Assurance bereitet das Netzwerk auf Blockchain vor.

Die Blockchain-Technologie revolutioniere das Internet und verändere die Welt von morgen, da sind sich Experten sicher. So kann über die Blockchain beispielsweise ein vernetztes Auto zur Geldbörse umfunktioniert werden – etwa, indem es automatisch Maut und Parkgebühren bezahlt. Oder im Gesundheitsbereich-Bereich erhalten Ärzte per Blockchain elektronische Patientendaten, die Informationen zu Behandlungen und eingenommenen Medikamenten umfassen.

Geldüberweisungen und Vertragsabschlüsse fälschungssicher dokumentieren

Solche Anwendungsszenarien zeigen: Firmen haben das Potenzial der neuen Technologie erkannt. Laut einer aktuellen Studie der Unternehmensberatung Sopra Steria Consulting erwägt und prüft bereits jedes zweite Unternehmen, Blockchain im eigenen Haus einzusetzen. AXA zum Beispiel plant als erste Versicherung, ihren Kunden Flugversicherungen über die Blockchain anzubieten und auch Schadensfälle darüber abzuwickeln. Und die Schweizer Distributionsplattform Winding Tree will einen Blockchain-basierten digitalen Marktplatz für Reiseleistungen entwickeln – Lufthansa unterstützt dieses Vorhaben. Grundsätzlich ist die Blockchain-Technologie in jedem Bereich einsetzbar, bei dem es darum geht, Verträge oder Objekte zu erfassen, zu bestätigen oder zu transferieren. Und egal, ob Geldüberweisungen, Vertragsabschlüsse oder interne Prozesse – über die Blockchain soll es möglich sein, jede Transaktion fälschungssicher zu dokumentieren.

Blockchain als dezentrale Datenbank

Doch warum gilt die Technologie als so sicher und worin genau liegt das Potenzial? Durch Blockchain werden Transaktionen in einer Art dezentralen Datenbank nach dem Peer-to-Peer-Prinzip übermittelt. Der Datenaustausch erfolgt durch eine Vielzahl von Rechnern (Netzknoten), die im Blockchain-System miteinander verbunden sind. Jeder Rechner speichert jeden Vorgang redundant und teilt ihn mit den anderen Netzknoten. Transaktionen können dabei nur hinzugefügt, nicht aber bearbeitet oder gelöscht werden. Zudem braucht jeder Teilnehmer einen Schlüssel, um auf die Inhalte zurückzugreifen.

Hinzu kommt, dass Transaktionen in der Blockchain nicht von einer einzigen Institution durchgeführt werden. Die Blockchain-Systeme liegen auf vielen Servern weltweit. Damit unterstehen sie keiner Autorität wie etwa einem Kreditinstitut oder einer Behörde. Parteien können also Daten austauschen, ohne die Privatsphäre des Eigentümers zu beeinträchtigen.

Technische Hürden überwinden und Servicequalität erhalten

Doch mit den Vorteilen der Blockchain gehen auch Herausforderungen einher. Auf dem aktuellen Entwicklungsstand verbraucht die Technologie viel Strom und funktioniert als dezentrale Datenbank nur sehr langsam. Lediglich sieben Prozent aller Unternehmen halten Blockchain momentan für marktreif, das ergab die Studie von Sopra Steria Consulting ebenfalls. Um die Technologie massentauglich zu gestalten, müssen also noch technische Hürden überwunden werden. Denn die Blockchain mag vielleicht fälschungssicher sein, ausfallsicher ist sie aber nicht.

Denn die Blockchain bedeutet eine höhere Komplexität für die IT-Infrastruktur. An Transaktionen beteiligte Server, benötigte Middleware für die Verschlüsselung oder virtuelle Maschinen machen die IT unübersichtlicher – und damit auch fehleranfälliger. Dadurch, dass das Blockchain-System auf mehreren Servern verteilt ist, ist es schwieriger, Fehler zu lokalisieren und die Stabilität der Technologie zu gewährleisten. Werden Ursachen von Problemen nicht schnell gefunden, können sie Kettenreaktionen auslösen, die schlimmstenfalls zu einem Ausfall der Blockchain führen.

Blockchain ist abhängig von DNS-Anfragen

Eine weitere Fehlerquelle stellen DNS-Dienste dar. DNS dient dazu, Anfragen zur Namensauflösung in IP-basierten Netzwerken zu beantworten. Die Blockchain ist abhängig vom Kontakt zum DNS-Dienst. Ist er nicht erreichbar, kann die Technologie den nächsten Block in ihrer Kette (Chain) nicht abrufen.

DNS beeinflusst daher die Performance und die Servicebereitstellung der Blockchain. Diese Abhängigkeit sollten Unternehmen kennen, um im Falle einer Störung entsprechend reagieren zu können. Denn schlimmstenfalls können unvollständig ausgeführte Transaktionen oder Ausfälle der ganzen Kette die Folge sein. Und je nachdem, in welchem Bereich Blockchain eingesetzt wird, hat das gravierende Auswirkungen. Im Gesundheitsbereich etwa kann sich jeder Fehler unmittelbar auf Patienten auswirken. Und auch in anderen Branchen wie Energieversorgung oder Versicherungen haben Systemausfälle Auswirkungen auf den Endnutzer.

Service Assurance sorgt für Ende-zu-Ende-Sicht auf das gesamte Netzwerk

Um einen reibungslosen Ablauf innerhalb der Blockchain zu gewährleisten, benötigen Unternehmen eine ganzheitliche Ende-zu-Ende-Sicht auf Paket- und Datenströme, Gateways, Server und das Netzwerk. Wer eine gute Performance der Blockchain sicherstellen will, sollte zudem die DNS-Funktionstüchtigkeit überwachen. Mit entsprechenden Service-Assurance-Plattformen werden mögliche DNS-Fehler frühzeitig erkannt. Doch auch mögliche Cyberattacken auf das Netzwerk können die Blockchain lahmlegen. Auch hier kann eine Monitoring-Lösung helfen, indem sie etwaige Anomalien und Auffälligkeiten sichtbar macht. Service Assurance dient also nicht nur dazu, die IT auf neue Technologien vorzubereiten, sondern auch, diese sicher zu machen.

Unternehmen sollten Service Assurance zu einem zentralen Asset machen, wenn sie über die Einführung einer eigenen Blockchain nachdenken. Denn nur, wenn die Technologie abgesichert ist, lässt sich das volle Potenzial ausschöpfen. Das oberste Ziel bei der Umsetzung sollte sein, Ausfälle der dezentralen Datenbank zu vermeiden und die Performance in Abhängigkeit von DNS-Diensten sicherzustellen. Gelingt es Unternehmen, schnell auf Fehler zu reagieren, haben sie eine erste Hürde der Blockchain gemeistert.

Martin Klapdor

2.2 FEATURES

2.2.1 Vertrauen & Recht

Blockchain als Schlüsseltechnologie für das Internet der Dinge?

Blockchain-Technologie wird inzwischen in zahlreichen Branchen pilotiert und teilweise bereits produktiv eingesetzt. Konsortien in der Finanzbranche haben sich zum Ziel gesetzt, jahrzehntealte Technologie durch Blockchain-basierte Infrastruktur zu ersetzen und damit Finanztransaktionen schneller, effizienter und kostengünstiger abzuwickeln.

Newsletter und mehr Beiträge: www.digitaleweltmagazin.de/blog

Dr. Stefan Hopf, Senior Consultant, The Nunatak Group

Durch ihre Abhängigkeit von bisherigen Strukturen (u.a. existierende Technologien, Prozesse, regulatorische Rahmenbedingungen) werden in diesen Initiativen vor allem sogenannte „Brownfield-Projekte“ verfolgt, die einen hohen Abstimmungsaufwand erfordern und komplizierte Abhängigkeiten berücksichtigen müssen.

Blockchain und das Internet der Dinge

Das Internet der Dinge dagegen stellt ein neues Anwendungsfeld dar, das als sogenanntes „Greenfield“ bisher kaum etablierte Technologien und Standards aufweist. So prognostiziert Gartner, dass bis zum Jahr 2020 über 20 Milliarden Gegenstände mit Konnektivität ausgestattet sein werden und daraus ein Markt von drei Billionen US-Dollar entstehen wird. [1] Blockchain-Technologie und das Internet der Dinge sind dabei hochgradig komplementär. Warum?

Das Internet der Dinge führt zunehmend zu einer Verschmelzung der physischen und virtuellen Welt. Physische Gegenstände erhalten damit ein virtuelles Abbild, das gesichert und durch Verfügungsrechte zugänglich gemacht wird. Um die Rechte der Beteiligten zu wahren sind aufwändige Sicherheitslösungen sowie die Einschaltung vertrauenswürdiger Dritter erforderlich, z.B. in Form eines zentralen Rechtemanagements und spezialisierter Sicherheits- und Vertrauensdienstleister. Diese zentralisierten Ansätze werden insbesondere im Internet der Dinge zunehmend als limitierendes Problem erkannt. Viele der möglichen innovativen Produkte und Geschäftsmodelle benötigen, wenn sie gelingen sollen, autonom abwickelbare, nahtlose und dynamische Transaktionen zwischen heterogenen Partnern in Echtzeit und teilweise in sehr feiner Granularität. Man denke insbesondere an Machine-to-Machine (M2M) Kommunikation, wie sie etwa für autonomes Fahren, Smart Grids oder vernetzte Industrie-4.0-Applikationen erforderlich ist.

Die noch junge Blockchain-Technologie scheint hier einen Lösungsansatz zu bieten. Eine Blockchain erlaubt es, Gegenstände in einem globalen Netzwerk zu registrieren und genau zu verfolgen, wer welche Verfügungsrechte an einem Gegenstand besitzt. Interaktionen erfolgen dabei direkt zwischen den Beteiligten (Peer-to-Peer), ohne eine zentrale Instanz einschalten zu müssen. Diese aus der Theorie des verteilten Rechnens auf Computern sowie aus der Kryptographie hervorgegangene Technologie erzeugt ein Vertrauensnetzwerk, in dem nur der rechtmäßige Eigentümer u.a. Rechte an Gegenständen weitergeben und nur der berechtigte Adressat sie in Empfang nehmen kann; ein Gegenstand und zugehörige Verfügungsrechte existieren nur einmal (sind also nicht duplizierbar), die getätigten Transaktionen und die aktuelle Eigentümersituation sind von Jedermann jederzeit transparent überprüfbar. [2]

Für zahlreiche Anwendungen im Internet der Dinge könnte Blockchain damit eine Schlüsseltechnologie darstellen:

Industrielle Produktion: Bereitstellung von Informationen über den gesamten Produktlebenszyklus hinweg (u.a. Produktentwicklung, Produktion, Wartung) zur Optimierung von Just-in-Time Supply-Chain Prozessen und einer Auslastung von Fertigungskapazitäten

Smart Grids: Management von Peer-to-Peer Energiehandel und Organisation dezentraler erneuerbarer Energiequellen in Microgrids

Vernetzte Mobilitätslösungen: Austausch von individuellen Bewegungsdaten und Bereitstellung sicherer Vehicle-to-Vehicle Kommunikation und Transaktionen für nahtlose Mobilitätsdienstleistungen

Smart Home: Informationsaustausch und Management von vernetzten Gegenständen zur Automatisierung von übergreifenden Smart-Home-Anwendungen (z.B. Energiemanagement)

Einzelhandel: Individuelle Bereitstellung von persönlichen Produktpräferenzen (z.B. Farben und Größen) zur Optimierung des Beratungsangebots, der Kundeninteraktion und weiterer Dienstleistungen (z.B. elektronischer Self-Checkout)

Herausforderungen

Trotz offensichtlicher Vorteile von Blockchain-Technologie existieren auch einige zentrale Herausforderungen. So erfordern viele Anwendungen im Internet der Dinge einen hohen Transaktionsdurchsatz nahezu in Echtzeit. Die Bitcoin-Blockchain dagegen verarbeitet aktuell nur ca. sieben Transaktionen pro Sekunde mit einer bis zu 60-minütigen Wartezeit zur sicheren Bestätigung einer Transaktion. Rechenintensive Kryptographieverfahren verursachen zudem einen hohen Energieaufwand, der eine nachhaltige Skalierung eines öffentlich zugänglichen Blockchain-Netzwerks erschwert.

Für viele Anwendungen im Internet der Dinge ist zudem die Gewährleistung der Privatssphäre von Nutzern (Personen oder Gegenstände) unbedingt notwendig – eine Anforderung, die bisher nur wenige Blockchains erfüllen. Zudem gestaltet sich eine Community-basierte Governance von Blockchain-Protokollen nach wie vor kompliziert, wie die aktuelle Diskussion zur Anpassung der Transaktionskapazität der Bitcoin Blockchain aufzeigt. Um die Anforderung des Internet der Dinge zu erfüllen, müssen ggf. eigens dafür entwickelte Blockchain-Protokolle entstehen (z.B. IOTA). Bis diese reibungslos funktionieren, steht noch ein ganzes Stück Arbeit bevor.

Stefan Hopf

Referenzen: **[1]** http://www.gartner.com/newsroom/id/3598917 **[2]** https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

Alexandros Karakatsis, Consultant, CGI

7 Gründe, wieso sich die Blockchain mittelfristig auch bei Ihrem Unternehmen durchsetzen wird!

Viele Unternehmen und Personen stellen sich folgende Fragen:
Was ist an der Blockchain so besonders?

Warum soll Aufwand betrieben und die bestehenden Systeme, mit bewährten Lösungen, gegen diese neue Technologie ersetzt werden? Lohnt sich das?

7 Punkte, die Sie in Betracht ziehen sollten, wenn Sie sich mit der ersten Frage auseinandersetzen:

1. Datensicherheit

Die Blockchain bietet eine erhöhte Datensicherheit, durch dezentrale Speicherung. In einer klassischen Datenbank können, durch einen Angriff, Daten verändert oder gelöscht werden. Dadurch, dass die Daten jedoch bei vielen Parteien gespeichert werden, sinkt dieses Risiko gegen null. Hierdurch müsste sich ein Angreifer Zugriff auf tausende Rechner verschafft und eine gleichzeitige Datenänderung vornehmen. Dabei muss angemerkt werden, dass nicht jeder Nutzer in Besitz aller Daten sein muss und kann.

Aufgrund der Architektur der Blockchain reichen kleine Datenpakete aus, um den Inhalt der ganzen Kette zu verifizieren. Dies ermöglicht ein schnelles Aufdecken potentieller Manipulationen.

2. Kein Risikomonopol

Durch die Dezentralität verschiebt sich auch das Risiko. Bei einer klassischen zentralen Speicherung trägt derjenige, der den Dienst bereitstellt, das alleinige Risiko für dessen Konsistenz, Verfügbarkeit und Sicherheit. Indem die Daten nicht mehr bei einer Partei liegen, liegt auch das Risiko nicht mehr nur bei einer Partei, sondern wird geteilt. Je mehr Parteien die Daten speichern, desto geringer fällt das gesamte – zu tragende – Risiko aus.

3. Minimierung des Verwaltungsaufwandes

Ein großer Vorteil sind „Smart Contracts“. Hierbei handelt es sich um Verträge, die sich nach dem eintreten bestimmter Parameter selbstständig ausführen. So wird die Zahlung für ein Produkt, nachdem die Lieferung abgenommen wurde, automatisiert durchgeführt – bzw. nach einer vereinbarten Frist angestoßen.

4. Gleichstellung von Vertragspartnern

Falls zwischen zwei Geschäftspartnern Uneinigkeit über eine Forderung herrscht, bekommt nicht immer jener Recht, der tatsächlich das Recht auf seiner Seite hat, sondern vielmehr die Partei, mit der besseren Verhandlungsposition. Ähnlich verhält es sich mit Versicherungen. Melden Sie als Kunde einen Schaden bei Ihrer Versicherung, stehen Sie deutlich besser da, als ein Geschädigter, der bei einer fremden Versicherung einen Anspruch geltend machen möchte. In der Blockchain entsteht eine Entscheidung demokratisch. Das heißt nicht, dass eine Einzelperson entscheiden kann, wer Recht hat.

Vielmehr entscheidet das Netzwerk von Computern, ob die vorher bestimmten Bedingungen erfüllt wurden oder nicht. Das Urteil, dass die Mehrheit im Netzwerk trifft, gilt als „Soll-Wert“ und wird automatisiert durchgeführt.

5. Kostenreduktion

Aus den geringeren Aufwendungen für Risikomanagement, Datensicherheit und Verwaltung sinken auch die finanziellen Belastungen für Unternehmen. Zwar muss zu Beginn in die Technologie investiert und gegebenenfalls die gesamte IT modernisiert werden, dafür sinken aber die laufenden Kosten signifikant.

So schätzt der Thinktank der spanischen Bank Santander, dass Banken damit bis 2022 ein jährliches Einsparpotential in Höhe von 15 bis 20 Milliarden Dollar besitzen.

6. Öffnung des Marktes

Durch die geringen Kosten für Datensicherheit, Erreichbarkeit und Anschaffung erschließt sich auch für viele kleine Anbieter die Gelegenheit, sich dem Wettbewerb großer Anbieter zu stellen.

So können Start-Ups neue Finanzdienstleistungen und Versicherungen, auf Basis von Smart Contracts anbieten, ohne, dass eine Verwaltung benötigt wird. Aus diesem Grund können auch deutlich attraktivere Preise angeboten und eine ernste Konkurrenz zu renommierten Dienstleistern aufgebaut werden.

7. Mehr Kooperation

Die Blockchain findet ebenso oft Erwähnung, wenn Unternehmen untereinander kommunizieren wollen.

Nun stellt sich die Frage, woran die Kommunikation bisher scheiterte? Ein wesentlicher Punkt ist das Machtverhältnis zwischen den Akteuren.

Welcher Teilnehmer verwaltet die Daten und welcher darf diese nutzen? Wer trägt die Kosten? Wer die Verantwortung? Im Zweifel werden sich die Akteure für eine gemeinsame Unternehmung entscheiden, die mit der Verwaltung und Bereitstellung der Daten beauftragt wird. Aber welches Unternehmen entscheidet, wer den Geschäftsführer dieser neuen Firma stellen darf?

Die Blockchain ermöglicht allen Teilnehmern die gleichen Machtverhältnisse über die Daten, da sie jeder speichern kann. Auch können sie durch Verschlüsselung geschützt werden, so dass nicht alle Daten mit jeder Partei geteilt werden müssen. Aus diesem Grund hat die Blockchain, besonders in der Vernetzung von Unternehmen, eine große Zukunft.

Ob die Blockchain in allen Bereichen ihr volles Potential ausschöpfen kann, ist momentan ungewiss. Selten kamen disruptive Innovationen ohne Probleme und Widerstände auf den Markt. Dennoch lohnt sich eine Analyse, ob es für Ihr Unternehmen Bereiche gibt, die Sie optimieren können. Mittelfristig werden Sie sich damit auseinandersetzen müssen.

Alexandros Karakatsis

Lars Göbel, Leiter Strategie & Innovation bei DARZ

Die Blockchain ist kein Selbstläufer

Der Blockchain und den dazugehörigen Technologieaspekten werden in der aktuellen Diskussion viel Potenzial und beinahe heilende Kräfte zugewiesen. Entsprechend hoch gerankt wird das Konzept in allen Formen von Hypecycles, Übersichten und Top-Listen. Vor allem im Hinblick auf die Verhütung von Manipulation und Ausfallsicherheit soll sich ein neues Level an Qualität für Datenbanktechnologien auftun. Der Ansatz beruht darauf, dass kleine, abgeschlossene Elemente, die sogenannten Transaktionen, zusammengefügt, in Blöcken gebündelt, verifiziert, validiert, codiert und schließlich geteilt werden. Damit trägt die Blockchain den Anforderungen der Digitalen Transformation Rechnung, nicht nur permanent mehr Leistung und Effizienz zur Verfügung zu stellen, sondern die in diesem Zusammenhang genutzten Daten auch entsprechend revisionssicher zu strukturieren und permanent verfügbar zu halten.

Eine Vielzahl an Einsatzmöglichkeiten

Die Blockchain verspricht also für Organisationen aus unterschiedlichen Branchen Mehrwerte. Vorreiter in der Ideenfindung war die Finanzwirtschaft. Für das Buzzword und Hype-Thema der Krypto-Wärung Bitcoin bildet Blockchain das technische Rückgrat. Transaktionen können mit ihrer Hilfe verschlüsselt und gleichzeitig transparent abgewickelt werden. In diesem Kontext ist Bitcoin auf der einen Seite Experimentierfeld und gleichzeitig Vorbild für andere Formen von Transaktionen. Die Blockchain Technologie könnte in der Zukunft für zahlreiche Automatisierungsmaßnahmen genutzt werden. Ein denkbares Einsatzgebiet sind Smart Homes. Wenn beispielsweise Sensoren im Haus anschlagen, weil ein Wasserrohr kaputt ist, und aus diesem Grund automatisiert Prozesse ausgelöst werden. Dies kann unter anderem eine digitale Zahlung an den Handwerker umfassen, der direkt vorbeikommt und entsprechende Reparaturen vornimmt. Schäden können auf diese Weise so repariert werden, bevor der Hausbesitzer den Fall selbst überhaupt wahrnimmt. Auch die Musikindustrie könnte durch die Blockchain Technologie stark verändert werden. Künstler und Rechtsinhaber könnten Musiktitel registrieren und ihre Rechtsansprüche in der Blockchain vermerken. Zahlungen würden automatisiert und unmittelbar mit Unterstützung der sogenannten Smart Contract Technologie vorgenommen werden. Zudem könnten die Musiker selbst Richtlinien festlegen, auf welche Art und Weise ihre Werke genutzt werden dürfen.

Komplexer Ansatz, komplexe Umsetzung

Dies sind nur zwei Beispiele für die Vielfalt an Möglichkeiten, die die Blockchain bietet. Es stellt sich jedoch die Frage, wie einzelne Unternehmen vorgehen müssen, um davon zu profitieren. Hier geht es um die technische Etablierung, die aktuell noch einige spannende Herausforderungen formuliert. Hier einige davon:

Die Blockchain ist komplex

Um eine revisionssichere Speicherung von Daten zu gewährleisten, setzt die Blockchain auf Dezentralisierung. So sind sehr viele Kopien der Datenbank im Netzwerk verteilt, sodass mehr als die Hälfte der verfügbaren Elemente gefälscht werden müsste, um einen Datenbankeintrag wirklich zu verändern. Dies bedeutet für den Manipulator, dass eine exorbitant hohe Summe aufgewendet werden muss, um die Manipulation überhaupt herbeiführen zu können. Das lohnt sich für den Angreifer nicht. Nichtsdestotrotz muss auch bei der Blockchaintechnologie auf eine Umgebung gesetzt werden, die eine dauerhafte Speicherung der Informationen an unterschiedlichen Orten vorsieht. In diesem Fall ist das Thema Dezentralisierung nur über die Einbindung von Partnern zu erreichen, die die Nutzung unterschiedlicher Standorte weltweit garantieren, die auch entsprechend performant sind.

Die Sicherheit hängt von der Umgebung ab

Dezentralisierung sorgt für Ausfallsicherheit. Die Sicherheit der Daten per se resultiert auch und vor allem aus der Umgebung. Hier müssen potenzielle Anwender darauf Acht geben, in den einzelnen Standorten sowohl für physische als auch auf logische Sicherheit zu sorgen. Das bedeutet letztendlich, dass die genutzte IT eben nicht mehr im Keller betrieben werden kann, sondern dass die Nutzung von Hochsicherheitsrechenzentren notwendig wird, um den Datenzugriff nur für autorisiertes Personal zu ermöglichen.

Blockchain ist Vertrauenssache

Es zeichnet sich ab, dass die Etablierung der Blockchain für einzelne Unternehmen ein kompliziertes Unterfangen ist. Hier hilft nur die Einbindung von qualifizierten Partnern wie Full IT Service Providern. Hier ist es wiederum notwendig, konsequent auf Zertifizierungen zu achten wie ISO 27001. Auch die Einhaltung der Vorgaben nach der EU Datenschutzgrundverordnung (DSGVO / GDPR) durch den Partner sind essenziell, um wirklich sicher und effizient zusammenarbeiten zu können.

Blockchain betrifft multiple Geschäftsbereiche

Genauso wie unterschiedliche Branchen von der Nutzung der Blockchain profitieren können gilt dies natürlich auch für verschiedene Geschäftsbereiche im Unternehmen. Hier ergeben sich durch die Anwendung von Shared-Ansätzen nicht nur Kostensparpotenziale, sondern auch die Möglichkeit, die Lösung gemeinsam weiterzuentwickeln und Innovationen hervorzubringen. Auch dies bedingt jedoch das Consulting von Partnern aus den unterschiedlichsten Bereichen wie IT Security, Distribution etc. und die Führung durch einen zentralen Partner.

Das Angebot von Blockchain-as-a-Service setzt die Zusammenführung von Services aus den Bereichen Colocation, Managed Services sowie Infrstructure-as-a-Service (IaaS). Organisationen, die sich für die Etablierung einer eigenen Blockchain interessieren, sollten auf entsprechend zertifizierte Partner setzen.

Lars Göbel

2.3 USE-CASES

2.3.1 Lieferketten

Shared-Ledger-Technologie ist mehr als Krypto-Währungen und Finanzdienstleistungen

Manfred Opificius, Vice President DACH Region, Juniper Networks

Bestätigt die Realität den Hype, wird die Blockchain eine neue Disruptionswelle auslösen

Blockchain, der verteilte, dezentralisierte Ledger, gewährleistet die Integrität und Authentizität aller übertragenen Daten. Damit bildet die Technologie eine Vertrauensbasis zwischen Dritten, die digitale Transaktionen durchführen – und eröffnet damit eine Welt neuer Möglichkeiten. Abgesehen von Bitcoin gibt es im Moment wenige umfangreiche Blockchain Anwendungen, das Potenzial der Technologie ist aber enorm. Gartner Analysten schätzen, dass der Mehrwert für Unternehmen, die Blockchain nutzen, bis 2030 satte 3,1 Billionen US-Dollar erreichen wird. Dieser Mehrwert setzt sich aus verschiedenen Komponenten zusammen. Dazu gehören neue Vertriebschancen, höhere Verkäufe und reduzierte Investitions- sowie indirekte Kosten.

Transparent, aber sicher
Die Blockchain ist absichtlich transparent angelegt, gewährleistet aber gleichzeitig Datenintegrität. Eine Blockchain verlinkt elektronisch Transaktionsdatensätze, sogenannte Blöcke. Diese lassen sich nicht manipulieren, da jeder neue Block verschlüsselt an die Informationen des vorherigen gehängt wird. Die Daten können nicht geändert oder gelöscht werden, sobald sie Teil der Blockchain sind – ein wesentliches Design-Merkmal, das die Daten und das Protokoll absichert. In der heutigen Welt mit regelmäßigen Sicherheitsverletzungen, die persönliche Informationen gefährden und ein wachsendes Misstrauen im Zusammenhang auf Nachrichten, Informationen und Dokumentation fördern, ist dies eine willkommene Erleichterung.

Identitäts- und Datenintegrität sind enorm wichtige Probleme, die es zu lösen gilt. Um aber erfolgreich zu sein, benötigt die Blockchain wie jede andere Anwendung ein sicheres Kommunikationsnetzwerk als Basis. Dazu gehört außerdem eine zuverlässige Infrastruktur und eine End-to-End-Cloud-Orchestrierung. Wenn die privaten Schlüssel für den Zugriff auf die Blockchain gestohlen werden oder gefährdet sind, entstehen Sicherheitslücken.

Blockchain in Aktion
Die Technologie ist daher kein Ersatz für eine umfangreiche Netzwerk-Sicherheit. Die sollte die Basis für die Blockchain liefern. Ein Beispiel: Intelligente Verträge – basierend auf der Blockchain – bestätigen die Authentizität von Flugzeug-Bauteilen entlang der gesamten Lieferkette. Das Teil verlässt die Produktion und wird per Container in den nächsten Hafen verschifft. Am Bestimmungsort ausgeladen, transportiert ein Lkw es zum Distributor. Doch wie kann der Flugzeughersteller, der das Bauteil erhält, sicher sein, dass es sich um Original-Bauteil und nicht um eine Fälschung handelt?

Dafür lassen sich der Distributed Ledger und intelligente Verträge nutzen: Sie gewährleisten die Integrität des Prozesses und bestätigen, dass es sich um das Original-Bauteil handelt. Lasert er vor dem Verlassen der Produktionsstätte noch eine Tracking-Nummer auf das Bauteil und scannt es ein, ist dies der erste Eintrag in der Blockchain. An jedem weiteren Kontrollpunkt bestätigen Smart Contracts den Empfang und kümmern sich um die Bezahlung der Lieferanten. Zwischenschritte während der Produktion lassen sich zur Blockchain hinzufügen und lückenlos nachverfolgen. Dem Internet der Dinge (IoT) eröffnet die Blockchain somit zahlreiche neue Chancen. Mit ihr lässt sich auch die Vielzahl der Geräte managen: Der Schiffscontainer mit Flugzeug-Bauteilen kann fast ins Unendliche potenziert oder um Millionen von Sensoren, die Produktionsprozesse kontrollieren, erweitert werden.

Auch bei der Autorisierung der IoT-Endpoint-Identität bietet die Blockchain einen Mehrwert und verbessert die IoT-Sicherheit. Die End- oder Edge-Geräte zu schützen, ist ein relativ neuer Ansatz. Cyber-Kriminelle können über diese Geräte in die Systeme eindringen – auch, da IoT-Security sich momentan noch im Entwicklungsstadium befindet. Mirai nutzte beispielsweise Sicherheitslücken von IoT-Geräten. Blockchains sind in der Lage, Geräte gegen Betrug und Angriffe schützen, sobald sie in der Blockchain registriert sind. Die Blockchain zeichnet dann jede Transaktion und Kommunikation auf, die durch die Devices stattfindet. Ohne die privaten Schlüssel und Prüfung durch das Blockchain-Netzwerk sind Hacker nicht fähig, die hohe Zahl der IoT-Geräte zu kompromittieren um DDoS-Angriffe zu initiieren.

Auch wenn die Blockchain Identitäten ebenso wie die Datenintegrität gewährleistet, löst dies keine Security bezogenen Probleme. Im Gegenteil: Die Blockchain vergrößert die Angriffsfläche und zeigt bislang unbekannte Schwachstellen auf. Je mehr Anwendungen entwickelt werden, desto anfälliger wird die Applikationsebene der Blockchain, die neue Schwachstellen für Cyberkriminelle offenlegen. Niemand weiß, wie lange es dauern wird, bis ein Sicherheitsrisiko innerhalb der Blockchain-Anwendungen entdeckt wird. Die beste Verteidigung ist aber eine holistische Sicherheitsstrategie, bei der alle Elemente des Netzwerks bei Threat Intelligence und ihrer Reaktion auf Bedrohungen zusammenarbeiten.

Gewaltiges Potenzial
Das Potenzial der Blockchain betrifft fast jede Branche. Finanzinstitutionen können Wertpapierdarlehnen in Minuten statt in Tagen abwickeln. Hersteller sind in der Lage, ein Produkt zurückzurufen, indem die Daten der Produktionskontrolle mit den Erstausrüstern (OEMs) und Regulatoren geteilt werden. Die Betreiber von Mobilfunknetzen sind im Stande, Roaming-Betrug zu bekämpfen, indem sie Smart Contracts erstellen. Diese sind zwischen dem Host- und dem besuchten mobilen Netzwerk implementiert. Der Fluss von Gütern und zugehörigen Zahlungen sind einfacher, schneller und risikoärmer als bisher zu kontrollieren. Der Kernfrage ist allerdings: Kann die Blockchain ein Problem beseitigen, das sich auf traditionelle Weise nicht lösen lässt?

Vertrauen wiederherstellen
Regierungen, Unternehmen und Verbraucher werden immer digitaler, der Netzwerk-Verkehr immer dichter. Die Angriffe auf Netzwerke ebenso wie Daten nehmen zu und dies beeinträchtigt das Vertrauen in Technologie – und vor allem in Datenschutz und Authentizität. Kombiniert mit sicheren Netzwerken könnte die Blockchain die Technologie sein, die das Vertrauen wiederherstellt und ein neues Zeitalter an Interaktion und Security einläutet. Manfred Opificius

Wie die Blockchain das Asset Management von Maschinen und Anlagen revolutionieren könnte

Die Blockchain ist derzeit eine der faszinierendsten Technologien. In der Regel wird sie allerdings nur im Zusammenhang mit der Welt der Finanzen diskutiert und aus diesem Bereich stammen meist auch ihre ersten Anwendungsfälle. Dabei bietet ihr Funktionsprinzip auch anderen Branchen große Chancen. Eine Blockchain ist eine Art riesiges weltweites dezentrales Register, auf das alle zugreifen können, die an einer konkreten Blockchain beteiligt sind; und die Einträge in dieses Register erfolgen über ein zu Einhundert Prozent sicheres, verifizierbares und nachverfolgbares Protokoll. Mit diesen Eigenschaften verfügt die Blockchain auch über Potenzial für andere Einsatzgebiete – etwa für das Asset Management von Maschinen und Anlagen.

Diese können je nach Größe aus zigtausenden Einzelteilen bestehen. Um sicherzustellen, dass sie die richtige Spezifikation haben und nicht gefälscht sind, ist es entscheidend, ihre Herkunft genau zu kennen, sprich: ihren Originalhersteller, das genaue Produktmodell und die präzise Version. Darüber hinaus müssen sich viele dieser Teile über ihre gesamte Instandhaltungshistorie hinweg transparent nachverfolgen lassen. Im Moment haben aber sämtliche Parteien, die mit einer Maschine oder Anlage zu tun haben – von den Zulieferern über den Hersteller bis zum Betreiber und den Servicedienstleistern – ihre eigenen, voneinander losgelösten Systeme. Eine einzige „Single Version of Truth" für ihren kompletten Lifecycle zu etablieren und zu pflegen, ist dadurch sehr schwer. Häufig sind derartige Sammlungen deshalb unvollständig oder liegen überhaupt nicht digital vor; und die Kommunikation zwischen den Parteien findet oft nur papierbasiert oder sogar rein verbal statt. Fehlende Standards erschweren außerdem die Nachverfolgbarkeit.

Diese Probleme ließen sich beseitigen, wenn alle Beteiligten aus ihren Systemen heraus Transkripte sämtlicher Transaktionen an ein extra dafür geschaffenes und verteiltes digitales Register senden könnten, auf das ausschließlich autorisierte Teilnehmer Zugriff haben. Der Hersteller könnte die Blockchain für seine Maschine oder Anlage starten und jede weitere Partei könnte weitere relevante Blöcke hinzufügen. Etwa der Betreiber, der die Teilnehmer darüber informiert, wo und wann eine Maschine in Betrieb genommen wurde oder welche Betriebszeiten sie bereits hinter sich hat, oder der Instandhaltungsdienstleister, der seine Wartungsarbeiten dokumentiert. Auf diese Weise würde durch eine Blockchain eine absolut nachprüfbare, nachverfolgbare und vertrauenswürdige Historie über den gesamten Lebenszyklus in Echtzeit entstehen. Und die einzelnen Parteien könnten weiterhin die Vorzüge ihrer eigenen Systeme nutzen, um ihr Geschäft erfolgreich zu betreiben.

Bis es wirklich soweit ist, sind aber noch einige Voraussetzungen zu erfüllen. So müssen zahlreiche Partner zusammenarbeiten und auch Willens sein, Informationen zu teilen, um sie in einer Blockchain integrieren zu können: die Anbieter von Blockchaintechnologien und Unternehmenslösungen, natürlich sämtliche an einer solchen Blockchain direkt beteiligten Parteien und, sofern gesetzliche Vorgaben wie etwa Umweltschutzauflagen zu beachten sind, unter Umständen auch Behörden. Aber auch technische Aspekte wie die Latenz von Transaktionen und die erforderliche Rechenpower könnten der Realisierung noch im Wege stehen. Nicht zuletzt sind außerdem Fragen nach der Sicherheit, Vertraulichkeit und dem Eigentum der Daten zu klären. Trotzdem: Wer bereit ist, sich auf das Thema einzulassen, dem winken große Optimierungspozenziale und Wettbewerbsvorteile. Ata Abdavi Azar

Ata Abdavi Azar, Senior PreSales Consultant, Sales & Marketing, IFS

2.3.2 Geschäftsmodelle

Mittelstand plant die Blockchain-Revolution

Fälschungssichere Transaktionen und Verträge, die sich ganz ohne menschliches Eingreifen erfüllen: Die Blockchain erreicht den Mittelstand als eine der wichtigsten technischen Plattformen für digitale Innovationen.

Die Blockchain steht für dezentrale Datenbanken jeder Art, die Informationen sicher speichern und managen – auch über Kryptowährungen wie Bitcoin und Ethereum hinaus. Das könnte in den nächsten 10 Jahren die deutsche Wirtschaft grundlegend verändern, denkt jeder dritte Mittelständler (32 Prozent) in Deutschland laut einer aktuellen Umfrage des eco – Verbands der Internetwirtschaft e. V. und des Markt- und Meinungsforschungsinstituts YouGov. 266 Entscheider des oberen und mittleren Managements in Unternehmen mit 50 bis 499 Mitarbeitern hatten die Marktforscher befragt. Dabei zeigt sich: Zwei Drittel der Mittelständler kennen die Blockchain noch gar nicht. Um eine große Chance nicht zu verschlafen, ist für sie jetzt die Zeit gekommen, sich mit dem Thema zu beschäftigen.

Transparente Verträge ohne zentrale Instanz
In einer Blockchain festschreiben lassen sich beispielsweise Computeralgorithmen die festlegen, welche Bedingungen zu welcher Handlung führen. Es entstehen sogenannte Smart Contracts – intelligente Verträge, die sich automatisiert erfüllen. Ganz

Stephan Zimprich, Leiter der Kompetenzgruppe Blockchain/ Anwalt & Partner ‚eco – Verband der Internetwirtschaft e. V / Fieldfisher LLP

Henning Neu, Datenschutz- und IT-Sicherheitsberater, praemandatum GmbH

ohne Juristen oder Anwälte überwachen Algorithmen die Verträge in Echtzeit und setzen die Rechte der Vertragspartner automatisch durch. Der Mensch als Fehlerquelle entfällt.

Die Anwendungsmöglichkeiten reichen von Internet of Things (IoT) und Finanzwirtschaft bis in die Branchen E-Commerce und E-Government – beispielsweise fürs Lizenz- oder ID-Management oder in der Logistik. Um Transaktionen lückenlos, fälschungs- und revisionssicher zu erfassen, braucht es damit keiner großen Investitionen in IT und Infrastruktur. Das Blockchain-Netzwerk validiert transparent ohne zentrale Instanz. Die Einträge sind an vielen Orten gleichzeitig manipulationssicher gespeichert.

Grundlagen für Blockchain-Geschäftsmodelle entstehen

Aufgrund der vielfältigen Anwendungsfälle planen neun Prozent der Mittelständler bereits konkret den Einsatz einer Blockchain. 17 Prozent der Befragten denken laut eco-Umfrage immerhin über den Einsatz in ihrem Unternehmen nach. Gemeinsam mit Wissenschaftlern arbeiten sie zurzeit intensiver denn je an Standards, Schnittstellen und Protokollen für die Entwicklung entsprechender Geschäftskonzepte. Diese Entwicklungen machen es sehr wahrscheinlich, dass sich die Blockchain für bestimmte Anwendungsfälle und Branchen in der Breite durchsetzen wird – diese Annahme teilen laut Umfrage 44 Prozent der Mittelständler.

Unternehmen auf der Basis von Algorithmen

Möglich werden auch komplexere Anwendungsfälle ohne menschliches Eingreifen: Decentralized autonomous organizations (DAO) sind auf der Blockchain basierende, autonom handelnde und völlig digitale Unternehmen. Aktionen werden dabei auch ganz ohne menschliches Urteilsvermögen, rein aufgrund von Algorithmen überwacht und durchgeführt. Solche Anwendungen lassen sich beispielsweise mit der Plattform Ethereum entwerfen. Diese Blockchain mit integrierter Programmiersprache stellt Entwicklern ein Werkzeug zur Verfügung, um selbst intelligente Verträge zu entwickeln und in einer Blockchain zu verwenden – sozusagen die „Blockchain 2.0".

Stephan Zimprich

2.3.3 Zahlungsmittel

Die Blockchain und die Kryptowährungen – das smarte Geld für eine einfache Welt

Als die Blockchain das Licht der Welt erblickte, brachte sie eine nicht minder beeindruckende Anwendung auf den Weltmarkt: Die Bitcoin. Eine digitale Münze, die per Design sicher ist. Eine Idee, die inzwischen so erfolgreich ist, dass der Währungskurs der Bitcoin trotz vieler Achterbahnfahrten sich meistens jenseits der 2000 Dollar pro Bitcoin bewegt, also je nach Tagesform locker das Doppelte des Marktwertes einer Feinunze Gold. Auf die Bitcoin folgten inzwischen weit über hundert verschiedene Kryptowährungen, von denen sich einige an einem gewaltigen Aufschwung erfreuen.

Kryptowährungen sind längst kein einfacher Trend mehr und das breite Publikum fängt an zu begreifen, dass das vielleicht auch so bleibt, auch wenn es weiterhin verwunderlich scheint, dass ein gänzlich immaterielles Konstrukt einen so großen Wert haben soll. Natürlich liegt dies größtenteils an der Blockchain selbst, die ein wichtiges Problem in der IT-Sicherheit löst – der sogenannte Byzantinische Fehler. Hierbei wird sichergestellt, dass in einem dezentralen Netzwerk alle Knoten die selben Informationen zur Verfügung haben. Auf Deutsch heißt das: Wenn wir von unserer Mutti 30 Euro für den Einkauf bekommen, dann können wir ihr später nicht erzählen, dass wir das Geld noch gar nicht haben, wenn sie gerade voll im Stress einen Streit zwischen unseren beiden Schwestern lösen muss, weil sie nämlich schlau ist und jede Bargeldtransaktion genau aufschreibt und belegen kann – simplifiziert formuliert. In der Realität ist es etwas komplexer, aber der Kern lässt sich prinzipiell darauf reduzieren, dass das Kryptogeld nicht lügen kann und jede Transaktion buchstäblich bis hin zur allerersten zurückverfolgbar ist.

Doch warum ist dieser Firlefanz nötig? Meine Bank kann doch schon ewig online Überweisungen tätigen.

Das Problem bei Banken liegt im Prinzip an den Banken selbst. Wenn ich meinem Freund das Geld für die Kinotickets überweisen will, dann vertraue ich darauf, dass die Banken sich schon irgendwie darum kümmern, dass das Geld auch wirklich bei meinem Freund ankommt. Die Idee, meine Besitztümer einer verwaltenden Institution in die Hand zu drücken, zeugt von enormem Vertrauen. Ein Vertrauen, an das wir uns schon als kleines Kind mit einem Taschengeldkonto gewöhnen können. Und das ist auch in Ordnung. Sicherheit baut immer irgendwie auf Vertrauen auf. Doch die Frage ist, ob dies irgendwann noch nötig sein wird. Das Bankensystem hat das materielle Geld größtenteils durch virtuelle Repräsentationen ersetzt. Aus geprägten Goldstücken wurden Papierscheine, aus Scheinen wurden Bits. Und seitdem befindet sich das Finanzsystem auf einer abstrakteren Ebene. Die Digitalisierung der Welt hat uns ein Stück der Kontrolle über unser Geld genommen. Und diese Verschiebung der Kontrolle über das Geld hat zwar bisher bis auf wenige Ausnahmen funktioniert, doch das grundlegende Problem bleibt bestehen.

Und genau da setzen Kryptowährungen an. Sie sind der Versuch, die Vorteile aus der physikalischen und der digitalen Welt zu kombinieren. Wir haben eine fest kalkulierbare Schöpfungsrate der digitalen Münzen, die bei manchen sogar auf ein festes, maximales Pensum begrenzt ist. Es gibt zum Beispiel maximal 21 Millionen Bitcoin, die erschlossen werden können. Andererseits lässt sich eine digitale Währung in beliebig kleine Einheiten aufspalten, sodass wir selbst winzige Bruchteile eines Cents ohne Probleme verarbeiten können. Die Währung ist zudem Fälschungssicher, ein Problem, das selbst heutzutage noch mit gewöhnlichem Bargeld besteht. Die Transaktionsverwaltung ist dezentral, wir sind also unabhängig von jeglichen Finanzinstituten. Und dennoch behalten wir die volle Kontrolle über unser Geld, verpackt in einem verschlüsselten, digitalen Geldbeutel, mit Transaktionen, die auf alle Zeit verfolgbar sind. Natürlich kommen mit den ganzen Vorteilen auch gewisse Nachteile. Die versprochene Anonymität ist momentan theoretisch umkehrbar, sofern jemand die Transaktionsadresse seines Partners mit dem dazugehörigen Namen veröffentlicht, also analog zu einer Kontonummer. Außerdem bleibt die Frage, ob sich die Kryptowährungen auch dann noch weiter halten, wenn es für die Transaktionsverarbeitung vielleicht mal keine lohnenswerte Entschädigung mehr gibt.

Die Blockchain selbst ist eine spannende Erfindung mit vielerlei Anwendungsgebieten. Kryptowährungen sind ein Lösungsansatz für eine digitale Zukunft und eine Kritik an einem komplexen Finanzsystem. Ein fälschungssicheres Bargeld wäre zwar die perfekte Sicherheitslösung, doch im globalen Onlinehandel sind Kryptowährungen ein Schritt in die richtige Richtung. Sie sind aber auch noch weit entfernt davon, unser bestehendes System zu ersetzen, doch sie sind ein Richtungsweiser für eine interessante Zukunft, die weniger Vertrauen von uns verlangt und uns ein Stück mehr Kontrolle in unsere eigenen Hände legt.

Henning Neu

Revolutioniert Blockchain das Bezahlen der Zukunft?

Bitcoin & Co werden häufig auch als Digitalisierung des Geldes bezeichnet. Die Begrifflichkeit kann jedoch verwirren, denn Geld war mit das Erste, das in den 1950er Jahren in Form von Buchgeld bzw. Giralgeld digitalisiert wurde. Was genau ist also neu an Bitcoin & Co und wie grenzt es sich von dem Altbekannten ab?

Das etablierte Finanzsystem basiert zu einem großen Teil auf Konten. Sei es auf der Basis von Bankkonten der Kunden bei den Geschäftsbanken oder der Einlagen der Geschäftsbanken bei den Zentralbanken. Teilweise sind die Konten für den Nutzer nicht sichtbar, wie beispielsweise bei der Geldkarte. Der Bezahlvorgang wird zwar über die Karte initiiert, die eigentliche Verrechnung, d.h. der Geldtransfer findet aber über ein Börsenverrechnungskonto im Hintergrund – sogar zeitverzögert – statt, was der Nutzer allerdings nicht merkt.

Revolutionär neu bei dem Gedanken der Blockchain-Technologie ist die Loslösung des Bezahlens von der Struktur des etablierten Finanzsystems. Digital Community Money (Bitcoin & Co) ist der erste selbst-organisierte Versuch ein neues digitales Geld einzuführen. Die Konten werden dabei auf vielen Rechnern repliziert gespeichert. Jede Privatperson kann dabei einen Rechner im Netzwerk betreiben. Diese Innovation war als Antwort auf die Probleme der etablierten Finanzinstitute in der Finanzkrise 2009 entwickelt worden, mit dem Ziel ein freies, von niemandem kontrollierbares Geld einzuführen. Mittlerweile untersuchen aber auch viele Regierungen und Zentralbanken die Einsatzmöglichkeiten von regulierten Versionen einer Blockchain basierten Währung, einer sogenannten Digital Currency. Darüber hinaus evaluieren einige Zentralbanken (z.B. Bank of England, Bank of Canada) die Optimierung der Interbanken-Systeme durch die Blockchain-Technologie.

Digital Community Moneys unterliegen starken Kursschwankungen

Digital Community Moneys feierten in der ersten Jahreshälfte 2017 einen großen Erfolg. Die Marktkapitalisierung der mehr als 800 Digital Community Moneys betrug zur Jahresmitte 2017 fast 100 Milliarden US-Dollar. Bitcoin hat dabei einen Marktanteil von über 40 %. Das ist zwar verschwindend gering im Vergleich zur z.B. M1-Geldmenge in Höhe von 33 Billionen US-Dollar allein im Raum der durch die G20 vertretenen Staaten, aber groß für eine Technologie, die ihren Ursprung in einer pseudonymen neun-seitigen Veröffentlichung aus dem Jahr 2008 hat.

Die Schattenseiten des starken Wachstums sind allerdings stark schwankende Wechselkurse zu regulierten stabilen Währungen wie dem US Dollar oder dem Euro. Was für risikofreudige Investoren interessant sein mag, ist für Bezahlvorgänge normaler Konsumenten, oder gar für eine Volkswirtschaft ungeeignet. Fast alle Angebote mit Digital Community Moneys zu bezahlen verliefen sich nach anfänglicher Euphorie schnell in der Bedeutungslosigkeit. Dies war der Fall als der Internet-Händler Overstock im Jahr 2014 damit begann, Bitcoin als Bezahlmittel zu akzeptieren oder als die Schweizer Stadt Zug im Jahr 2016 Bitcoin als Bezahlmittel für Gebühren einführte. In beiden Fällen war die Resonanz in der Presse groß, aber die Nachfrage nur von kurzer Dauer. Die Tatsache, dass es immer

Dr. Florian Gawlas, Technology Director, G+D Mobile Security GmbH

Matthew Key, Head of Customer Innovation, Global Banking and Financial Market, BT GmbH

noch eine Pressemeldung wert ist, wenn irgendwo Bitcoin als Zahlungsmittel akzeptiert wird, demonstriert, dass diese Verfahren noch nicht etabliert sind.

Sind Digital Currencies die Lösung für das Bezahlen der Zukunft ?
Auch wenn sich die meisten Zentralbanken aktuell mit dem Thema der Digital Currencies beschäftigen, gibt es bis heute wenig konkrete Pläne, ein solches Geld tatsächlich auch einzuführen, da die Komplexität hoch ist und zusätzliche Risiken birgt.

Die Attraktivität einer Digital Currency für eine Zentralbank besteht unter anderem darin, die Bürger auf dem Weg in die Digitalisierung zu begleiten. Eine Digital Currency für die breite Masse wäre eine regulierte Alternative zu einem Digital Community Money und erlaubt zusätzlich Menschen ohne Bankkonto in die Welt der digitalen Dienstleistungen zu integrieren.

Andererseits könnte durch die Einführen einer Digital Currency den Zentralbanken eine neue Rolle zukommen. Entspräche eine Digital Currency einer digitalen Form des Bargelds, könnten sich viele Bürger entscheiden, ihr Geld in Form der Digital Currency direkt bei der Zentralbank zu halten anstatt auf einem Girokonto. Ein ähnliches Verhalten der Bürger sieht man in Krisenzeiten heute auch mit privaten Bargeldreserven. Die Position der Geschäftsbanken würde dadurch geschwächt. Daran hat aber in einer freien Marktwirtschaft der Staat kein Interesse.

Wird Blockchain dann beim Bezahlen der Zukunft keine Rolle spielen ?
Blockchain basierte Bezahlsysteme in Form von Digital Community Money oder auch Digital Currencies werden vor allem – wenn sie auf den Bedarf skalierbar sind – dort eine wichtige Rolle spielen können, wo sie eine echte Lösung für sich geänderte Bedürfnisse bieten. Solche Änderungen können sich unter anderem ergeben, wenn Maschinen von anderen Maschinen Dienstleistungen entgegen nehmen und dafür kleine Geldbeträge fällig werden oder wenn von Konsumenten zunehmend kleine Geldbeträge im eCommerce verlangt werden, sogenannte Micro- oder Nano- Payments. Neben der Möglichkeit, die Geldströme über die Bankkonten der Maschinen-Besitzer zu lenken, konkurrieren hier heute schon Varianten auf der Basis von Digital Community Moneys um die beste Lösung.

Weiterentwicklungen der Blockchain Technologie haben das Potenzial das Bezahlen in neu entstehenden Märkten wie Smart Contracts, Internet of Things, aber auch im Bereich des Micro-Payments zu verändern. Im Falle der klassischen Bezahlverfahren zwischen Konsumenten und Händlern wird ein Durchbruch der Technologie aber wesentlich weniger wahrscheinlich sein. Florian Gawlas

2.3.4 Effizienzsteigerung

Blockchain: Schier unbegrenzte Möglichkeiten

Neue Technologien werden stets von gewissen Wachstumsschmerzen begleitet. Da ist auch Blockchain keine Ausnahme. Doch das Potenzial der jungen Technologie, zahlreiche Anwendungen und Systeme in verschiedensten Branchen zu verbessern, ist enorm.

Blockchain ist ein öffentliches Kontobuch, das sämtliche Transaktionen und Bewegungen zu einem Vermögensgegenstand, z.B. der Kryptowährung Bitcoin, aufzeichnet. Die Technologie kommt neben dem Warenverkehr, wie etwa bei der Überwachung der Lieferkette, auch bei elektronischen Transaktionen und Dienstleistungen zum Einsatz. Diesbezüglich hat Mark Walport, Chief Scientific Officer der britischen Regierung, bereits letztes Jahr auf das große Potenzial der Distributed-Ledger-Technologie (DLT) im Bereich der Dienstleistungen im öffentlichen wie privatwirtschaftlichen Sektor hingewiesen. Wie bei jeder neuen Technologie erwachsen auch durch DLT neue Herausforderungen. Doch unter dem Strich könnte das Vereinigte Königreich von Blockchain als Distributed-Ledger stark profitieren.

Wenngleich das Potenzial von Blockchain unbestritten ist, bereiten die Aspekte Sicherheit, digitale Identität und Vertrauenswürdigkeit rund um die Technologie Behörden wie Unternehmen nach wie vor Sorgen. Genau in diesen Bereichen suchen und entwickeln große Marktteilnehmer wie BT, Intel oder IBM, ebenso wie kleinere Start-ups, innovative Lösungen.

Welche Anwendungen kommen in Zukunft auf uns zu?
Die meisten Innovationen rund um Blockchain finden aktuell im Bankwesen statt, insbesondere die Kapitalmärkte betreffend. Blockchain bietet Vorteile für zahlreiche Dienstleistungen zu Währungen, aber auch für sehr spezielle Bereiche vom Ölhandel bis zu Risikoregistern, da Blockchain eine Vielzahl von Transaktionen besonders schnell verarbeiten kann. Das dezentrale Netzwerk von Rechnern kann z.B. Zahlungsabwicklungen und den Handel mit Unternehmensanleihen schneller und sicherer ausführen als herkömmliche Systeme.

Für die Versicherungswirtschaft ist ein Distributed-Ledger wie etwa Blockchain sehr gut einsetzbar für komplexe Sachverhalte, an denen mehrere Parteien beteiligt sind. Ein Beispiel ist eine Versicherungslösung für eine Immobilie mit 50 Büroeinheiten, die über Air BNB befristet über Zeiträume von einer Woche bis zu einem Jahr vermietet werden. Mithilfe von Blockchain werden sämtliche noch so kleine Transaktionen zentral verwaltet und für alle beteiligten Parteien abrufbar.

Die Lieferkette im produzierenden Gewerbe ist ein weiteres Segment, in dem Blockchain komplexe und zeitkritische Funktionen vereinfachen kann. Die nahtlose Bauteilverfolgung in der Produktion eines Flugzeugs ist eine komplexe Aufgabe, die tausende verschiedene Bauteile unterschiedlicher Herkunft umfasst. Dank Blockchain können sämtliche Bewegungen dieser Vermögenswerte durch die Lieferkette gespeichert und zurück verfolgt werden. Die Hersteller haben dadurch stets einen vollständigen Überblick über ihre aktuelle Produktion. Gleichzeitig wissen sie präzise, welche Bauteile in welchem Flugzeug verbaut sind – ein besonders wichtiger Aspekt für Reparatur- und Wartungsarbeiten.

Auch im Diamanten- und Kunsthandel kommt Blockchain zum Einsatz, und das aus gutem Grund: mit Blockchain ist es möglich, die Herkunft und Eigentumsverhältnisse zu Wertgegenständen manipulations- und fälschungssicher für mehrere Parteien nachzuweisen.

Ein besonders überzeugendes Beispiel dafür, wie Blockchain einen komplexen Prozess vereinfachen kann, findet sich im Gesundheitswesen. Für die meisten modernen Krankenhäuser stellt die Verwaltung und Aufbewahrung der Patientenakten eine Herkulesaufgabe dar. Für Patientenakten gelten hohe Anforderungen an den Datenschutz, gleichzeitig muss ein Zugriff bei Bedarf schnell möglich sein. Blockchain kann diese Aufgabe revolutionieren. In einer Blockchain können Patientendaten mit höherer Datenintegrität sicher verwaltet werden. Eindeutige digitale Identitäten und konsistente Autorisierungen stellen sicher, dass jeweils nur die entsprechend befugten Benutzer Zugriff auf die relevanten Daten erhalten.

Insbesondere für schwer zugängliche Regionen und Entwicklungsländer wäre es sehr vorteilhaft, wenn Wahlen und Identitätsnachweise komplett digital erfolgen könnten. Die Kombination aus einem dezentralen Netzwerk und lokaler Verarbeitung eignet sich hervorragend zur sicheren Authentifizierung von Personen.

Das wohl großartigste Potenzial von Blockchain liegt aber in der direkten Bereitstellung von Hilfsgütern und Hilfsgeldern. Wie kann sichergestellt werden, dass Hilfsmittel die richtigen Menschen und Orte überhaupt und vor allem schnell erreichen? Laut Schätzungen von Hilfsorganisationen ‚versickern' rund 30 Prozent aller Hilfsleistungen auf dem Weg zu den dafür vorgesehenen Empfängern. Blockchain ist dezentral und für jede Person mit Internetanschluss und einem Computer oder Smartphone verfügbar. Die Verteilung von Hilfeleistungen lässt sich dadurch schnell authentifizieren. Dank größter Transparenz und der Manipulationssicherheit des Systems erreichen Hilfsgelder direkt die verifizierten Anspruchsberechtigten.

Blockchain bietet zweifelsfrei schier unbegrenzte Möglichkeiten. Noch ist es eine Vision, aber ich für meinen Teil kann es kaum erwarten, zu beobachten, wie sich diese disruptive Technologie weiter entwickelt, erwachsen wird und in welchen Segmenten sie sich fest etabliert. Matthew Key

2.3.5 Strommarkt

Mit der Blockchain die Energiewende meistern?

Dr. Axel von Perfall, Senior Manager, PricewaterhouseCoopers GmbH

Neben dem Finanzsektor ist der Energiebereich die Branche mit den meisten Aktivitäten rund um die Blockchain-Technologie. Häufig geht es bei der Anwendung der Technologie um die Möglichkeit, dezentrale Akteure direkt – also ohne zwischengeschaltete Ebenen – zusammenzubringen. Damit wird eine ganz wesentliche Herausforderung der Energiewende angegangen: die zunehmende Dezentralität ist allseits gewünscht, muss aber auch steuerbar bleiben. Hier kann die Blockchain einen wichtigen Beitrag leisten.

Durch die Verbindung von Blockchain-Technologie und Smart Contracts könnte der Strommarkt im Endkundengeschäft idealerweise komplett automatisiert werden. Zielbild ist eine App, über die sowohl Erzeuger als auch Kunden ihre Präferenzen einstellen. Über die Blockchain-Plattform findet dann – z.B. alle 15 Minuten – ein Settlement zwischen Angebot und Nachfrage statt. In der Theorie kommt dieses Modell u.a. ohne Vertriebsgesellschaften, Abrechnungsfirmen und Messstellenbetreiber aus. In der Praxis erschwert natürlich das komplexe, mehrstufige System des Energiemarkts einschließlich des regulatorischen Umfelds eine rasche Umsetzung solcher Modelle. Aber erste Schritte in diese Richtung sind deutlich erkennbar.

Blockchain in der Praxis: Energiesektor bietet diverse Anwendungsbereiche
Die nachfolgende Übersicht zeigt die uns derzeit international bekannten Aktivitäten rund um die Blockchain-Technologie im Energiebereich.

Eine der ersten Anwendungen der Blockchain im Energiebereich wurde 2016 in Brooklyn (USA) im **Projekt Transactive Grid/Brooklyn Microgrid** umgesetzt. Das Projekt wurde als Peer-to-Peer Nachbarschaftsprojekt mit den Photovoltaikanlagen von fünf Häusern realisiert. Die Startups **Conjoule** (von innogy initiiert), „**Kleine Racker**" (Kooperationsprojekt von Stadtwerke Energieverbund, Discovergy, Grünstromjeton und Sunride) und **Powerledger** (Australien) arbeiten derzeit aktiv an ähnlichen Modellen.

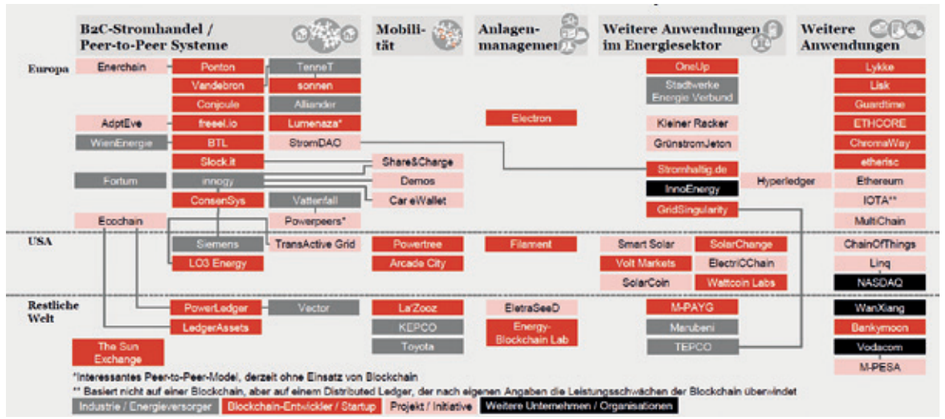


Abbildung: Unternehmen und Projekte mit Blockchain-Anwendung im Energiebereich

Eine Einsatzmöglichkeit im Bereich Elektromobilität erprobt derzeit **share & charge**, auch ein von innogy initiiertes Startup. Den Nutzern dieser Plattform soll ermöglicht werden, bei teilnehmenden Ladesäulen ohne weitere Formalitäten Ladevorgänge in Anspruch zu nehmen und abzurechnen. Damit wird ein „Roaming" bei der Nutzung fremder Ladesäulen möglich werden.

Mehrere Unternehmen arbeiten an der Nutzung der Blockchain-Technologie zur Verbesserung der Netzsteuerung – sowohl auf Verteilnetz- wie auf Übertragungsnetzebene: **TenneT** kooperiert mit **Sonnen**, um im Fall von Lastspitzen auf die Batteriespeicher der Sonnen Community zuzugreifen. Dadurch sollen teure Redispatch-Maßnahmen im Netz vermieden werden. Die Steuerung läuft über eine Blockchain-Applikation, die auf **Hyperledger** läuft.

Unter dem Namen **Enerchain** hat der Blockchain-Entwickler **Ponton** hat ein Konsortium zahlreicher Energieunternehmen zusammengebracht, um die Blockchain-Technologie für den Energiehandel voranzubringen.

Ausblick/Potenziale der Blockchain-Technologie im Energiebereich

Die Blockchain-Technologie erfährt derzeit eine enorme Aufmerksamkeit. Dies liegt zum einen daran, dass die Technologie in gewisser Weise „mystifiziert" wird: Oftmals wird sie als komplexer angenommen, als sie tatsächlich ist. Viel Interesse im Markt ensteht aus dem Wunsch heraus, die neue „Wundertechnologie" genauer zu verstehen und ihre Anwendungsmöglichkeiten abschätzen zu können. Zum anderen hat die Technologie eine bedeutsame strategische Konsequenz für die Energiewirtschaft: die zugrundeliegenden Ideen von „Peer-to-Peer" und Unabhängigkeit von zentralen Instanzen könnten eine erhebliche Bedrohung für eingespielte Geschäftsmodelle bedeuten. Die Energieversorger zwingt dies, sich noch schneller und intensiver mit den neuen digitalen, dezentralen Geschäftsmodellen zu beschäftigen.

Die Blockchain-Technologie selbst ist noch in einem „Beta-Stadium", die Projekte werden aber immer konkreter. Bislang waren es vor allem Projektideen und Simulationen, inzwischen gibt es zahlreiche Pilotprojekte mit Testkunden. Wir erwarten, dass im Laufe des Jahres 2017 immer mehr Projekte mit immer mehr „echten Kunden" und „echten Haushalten" an den Markt gehen.

Es bleiben aber auch noch zahlreiche offene Themen, die in der nächsten Zeit von der Blockchain-Community zu erarbeiten und zu klären sind: wie sehen die Erlösströme in den neuen Blockchain-Geschäftsmodellen aus? Wie profitabel sind die Geschäftsmodelle langfristig? Wie können die Schnittstellen zwischen digitaler Blockchain-Welt und Hardware (z.B. Smart Meter) zuverlässig hergestellt werden? Welche Daten und Algorithmen werden tatsächlich über die Blockchain abgedeckt, welche über andere IT-Systeme? Wird es eine Interoperabilität zwischen verschiedenen Blockchain-Systemen geben? Wie können regulatorische Hürden überwunden werden?

Sicher ist, dass die Blockchain-Technologie die Energiewirtschaft derzeit mobilisiert und die Digitalisierung der Branche insgesamt noch weiter vorantreibt.

Axel von Perfall

2.3.6 Identity

Identity as a Service ist gut, Bring Your Own Identity ist besser

Was wäre, wenn wir für jeden Onlinedienst, berufliche Anwendungen oder sogar im behördlichen Kontext nur einen einzigen Account bräuchten, der zudem noch ohne zentrale kontrollierende Instanz auskommt und gleichzeitig sehr sicher ist?

Jeder kennt das Szenario: Alleine für die Verwaltung von Accounts bei Facebook, Amazon, Google und vieler weiterer Onlinedienste werden eine E-Mail-Adresse und – so ist zumindest zu hoffen – ein separates Passwort benötigt. Auf diese Weise werden digitale Identitäten zur Massenware und die preisgegebenen Daten immer schwerer überschau- und handhabbar. Im beruflichen Alltag zeichnet sich ein ähnliches Bild ab. Es gilt eine kaum überschaubare Zahl an Anwendungen und Dateiablagen mit den richtigen Zugriffsrechten zu versehen und diese bei Bedarf auch zügig und sicher wieder zu entziehen. Beim Behördengang werden dann nochmals andere digitale IDs und Zugriffsberechtigungen benötigt.

Der Herausforderung, diesen regelrechten „Identity Spam" unter Kontrolle zu bekommen, haben sich unter dem Schlagwort **Identity** Federation bereits diverse Anbieter angenommen. Mit Diensten wie **Identity as a Service (IDaaS)** wird für den Anwender ein **Single-Sign-On (SSO)** möglich, das die Einzelverwaltung von Accounts obsolet werden lässt. Er benötigt lediglich noch eine digitale Identität, an die seine Zugriffsrechte gekoppelt werden. Die SSO-Funktionalität setzt jedoch die Integration des IDaaS mit allen relevanten Systemen voraus. Kompatibilität, Sicherheit und Verfügbarkeit sind als kritische Erfolgsfaktoren für den operativen Betrieb zu nennen. Auch wenn diese erfüllt sind, so muss der Anwender die Hoheit über seine Daten in diesem Szenario grundsätzlich abgeben. Ein Vertrauen in den IDaaS-Anbieter, der zugleich **Single Point of Failure** ist, muss zwingend vom Anwender aufgebracht werden.

Ein Ansatz, der IDaaS konsequent weiterführt und bei allen Beteiligten ein Umdenken erfordert, ist **Bring Your Own Identity (BYOI)**: Eine digitale Identität, die unter der vollständigen Kontrolle des Anwenders steht. Ohne eine zentrale kontrollierende Instanz. Mit den inhärenten Möglichkeiten, einzelne verknüpfte Informationen gezielt preiszugeben und diesen Zugriff selbstbestimmt auch wieder zu entziehen. Bring Your Own Identity ist sowohl im privaten, beruflichen wie auch im behördlichen Kontext einsetzbar.

Wie lässt sich Bring Your Own Identity realisieren?

Mit der Blockchain Technologie. Es lassen sich digitale Identitäten – IDs – mit Profilen erstellen, die in entsprechenden Attributen Informationen des Eigentümers vorhalten. Diese Informationen können von Dritten, z. B. einer autorisierten Stelle, bestätigt bzw. attestiert werden. Neben der Zuordnung von IDs zu Personen ist es auch möglich, Unternehmen, Webseiten oder Anwendungen IDs zuzuweisen. Durch entsprechende Bestätigungen und Verknüpfungen der IDs untereinander können Zugriffsberechtigungen vergeben werden. So könnte eine Anwendungs-ID einer personenbezogenen ID attestieren, dass sie diese als legitimen Nutzer betrachtet und darüber sowohl authentifizieren, als auch autorisieren. Es gibt für die Realisierung von BYOI verschiedene Lösungsansätze, wie beispielsweise Blockstack, uPort oder Sovrin. Eine flächendeckende Adaption würde maßgebliche Vorteile für Anwender und integrierende Organisationen erschließen: Sind die Hürden in punkto Kompatibilität mit den Bestandssystemen erst einmal genommen, sind kryptografische Sicherheit, hohe Verfügbarkeit aufgrund dezentraler Architektur und sogar souveräne Datenhoheit für den Anwender der Lohn.

Dr. André Kudra, CIO, esatus AG

Aktuell besteht großes Interesse, doch der unmittelbare Erfolg ist noch gehemmt

Neben der unsicheren Rechtslage in Sachen Blockchain-Technologie und den Aspekten, die die EU-Datenschutzgrundverordnung (EU-DSGVO) mit sich bringt, liegt es in der Natur der klassischen Blockchain (wie z. B. bei Bitcoin), dass prinzipiell jeder am Netzwerk teilnehmen und mitlesen kann. Dieser öffentliche Charakter ist für zahlreiche Anwendungen weniger sinnvoll und die unkontrollierbare Abhängigkeit vom gesamten Netzwerk stellt die Zukunftssicherheit auf längere Sicht in Frage. Zudem sind die derzeit verwendeten Konsensmechanismen, insbesondere **Proof-of-Work**, sehr energieintensiv. Im professionellen Kontext, also bei Unternehmen und Behörden, erscheint daher eine sog. **Public Permissioned Blockchain** eher geeignet. In dieser Blockchain – bzw. hier besser: Distributed Ledger – können alle Teilnehmer lesen, aber nur bekannte und genehmigte können schreiben, d. h. Transaktionen validieren. In einer solchen **Consortium Chain** bleiben Transparenz und Dezentralität nach wie vor erhalten, gleichzeitig entsteht aber eine gewisse Kontrollierbarkeit, die Nachhaltigkeit verspricht.

Fazit

Die digitale Identität via BYOI birgt für alle Beteiligten ein großes Potenzial. Offene Fragen sind lösbar. Eine grundlegende Bereitschaft, sich auf die neue Technologie einzulassen, ist jedoch zwingend erforderlich. Ein ggf. erheblicher Implementierungsaufwand in die bestehende Systemlandschaft darf nicht vernachlässigt werden – dies gilt allerdings für jede Art des IDaaS. Fatal wäre ein Verlust des privaten Schlüssels auf Seiten des Anwenders, der dem Verlust der digitalen Identität gleichkommt – sofern kein Wiederherstellungsmechanismus implementiert ist. Darüber hinaus lässt sich eine Blockchain, die systemimmanent keine zentrale Instanz hat, schwieriger regulieren, da das gesamte Netzwerk Änderungen adaptieren muss – hier bieten Consortium Chains einen Ausweg. Vieles spricht für Bring Your Own Identity mit der Blockchain – wer wagt den ersten Schritt?

André Kudra

2.3.7 Banking

Philippe Meyer, Managing Director, Avaloq Innovation Ltd

Uwe Krakau, Chief Market Officer Germany, Avaloq Innovation Ltd

Reality Check für Blockchain: Einsatzszenarien im Banking

Blockchain-Technologie stellt die Integrität einer Datenbank sicher, indem aufeinander folgende Datensätze kryptographisch verkettet werden. Dafür gibt es sinnvolle Anwendungsszenarien in verschiedensten Bereichen. Auch Banken haben ein wachsendes Interesse an Blockchain. Im Banking-Sektor etwa werden auf Blockchain basierende Projekte derzeit für Zahlungsvorgänge, derivative Produkte und für das Know-Your-Customer-Regulationsmanagement entwickelt. Zwar sollen die Lösungen, die diese ersten Initiativen hervorbringen, schon bald live gehen, aber noch existieren keine konsistenten Branchenprotokolle und -technologien. Auch ist Blockchain keine Zauberformel, mit der sich alle Probleme einer Bank lösen ließen. Diese Technologie wird kaum über Nacht die gesamte Finanzbranche revolutionieren. Die zukünftigen Entwicklungen brauchen ihre Zeit. Aber am Ende werden sich auf Blockchain basierende Lösungen durchsetzen. Die Auswirkungen der Blockchain-Technologie werden dabei mit den Auswirkungen des Internets und des Handys gleichgesetzt.

Großes Interesse an Bitcoin

Der bislang einzige weit verbreitete Anwendungsfall von Blockchain-Technologie ist Bitcoin. Die berühmte Kryptowährung hat eine Erfolgsgeschichte geschrieben, aus der unbestreitbar Innovationen hervorgegangen sind. Die Bitcoin-Transaktionsdatenbank wird von allen Stakeholdern geteilt. Etliche Vorteile von Blockchain-Technologie beruhen auf diesem Feature: Umständliche Abgleichsprozesse werden vermieden, Transaktionen lassen sich nach ihrer Ausführung nicht mehr verändern, und Fälschungen sind unmöglich. Bitcoin ist eines der ersten Beispiele von Blockchain-Technologie, an dem Banken Interesse gezeigt haben. Aber zugleich wird die virtuelle Währung mit einem gewissen Argwohn betrachtet, als mögliches Werkzeug für fragwürdige Geldgeschäfte. Dennoch sprechen mehr und mehr Private Banking-Kunden ihren Berater auf Bitcoin an – manche von ihnen haben größere Bitcoin-Guthaben, die sie mit ihren regulären Anlageformen integrieren möchten. Dieser Nachfragedruck wird Banken dazu bringen, Plattformen einzuführen, auf denen die Bitcoin-Anlagen ihrer Kunden direkt visualisiert sind. Eine mögliche Hürde könnte darin bestehen, dass Banken ihr Marketing für Bitcoin so ausrichten müssen, dass es skeptische Regulierungsbehörden zufriedenstellt. Auf technischer Seite gibt es dagegen keine Hindernisse, und es existiert auch schon ein funktionsfähiger Prototyp. Für Kunden bestünde der Vorteil darin, dass sie Bitcoin-Anlagen einer Bank überantworten könnten, der sie vertrauen, statt einem spezialisierten Bitcoin-Anbieter, der vielleicht noch wenig etabliert ist.

Know Your Customer: ein Paradebeispiel

Mittelfristig ist der zweite Blockchain-Anwendungsfall, der in der Branche erwartet wird, die Legitimationsprüfung. Sie ist regulatorisch vorgeschrieben und dient dazu, die Identität und das Profil eines Klienten zu verifizieren, um Geldwäsche zu verhindern: Know Your Customer (KYC). Diese KYC-Prüfung macht es für Banken zunehmend anspruchsvoller und komplexer, Neukunden zu gewinnen. Aber auch für Kunden selbst wächst dadurch die Komplexität, müssen sie doch endlos scheinende Formulare ausfüllen. Es ist sehr gut vorstellbar, dass Blockchain-Technologie hier helfen kann. Teile der KYC-Informationen könnten damit zwischen Banken übertragen und ausgetauscht werden. Start-ups aus dem Regtech-Sektor bieten solche Produkte bereits an, und auch unsere eigenen Kunden haben schon Interesse an solchen Lösungen geäußert. Dieses Interesse ist verständlich, generiert KYC doch nur Kosten, ohne wertschöpfend zu sein oder Wettbewerbsvorteile zu eröffnen. Blockchain scheint hier ein attraktives und leistungsfähiges Werkzeug, um den KYC-Verpflichtungen zu entsprechen. Zudem lässt sich Blockchain in privaten Netzwerken mit entsprechenden kryptographischen Werkzeugen nutzen, die vertrauliche Informationen schützen.

Geschäftsmodell KYC-Zertifikat

Wenn man einen verteilten KYC-Service aufbauen möchte, ist es dafür jedenfalls erforderlich, gewisse vertrauliche Informationen auszutauschen. Dennoch ist hier ein tragfähiges Geschäftsmodell denkbar. Wenn ein Kunde die Legitimationsprüfung mit Bank A durchlaufen hat und sich dann entschließt, Geschäfte mit Bank B zu tätigen, könnte er das ursprüngliche Zertifikat von Bank A nutzen, um Bank B gegenüber zu belegen, dass er den KYC-Prozess bereits abgeschlossen hat. Dies spart nicht nur dem Kunden Aufwand, sondern auch der Bank B. Diese wird Bank A gerne eine gewisse Gebühr zahlen, wenn sie dadurch die weit höheren Kosten einer neuerlichen KYC-Prüfung vermeiden kann. Zudem wird die Bank B aus dem Großteil der vertraulichen Informationen, die getauscht werden, keine Wettbewerbsvorteile ziehen können – Bank A entstehen also keine Nachteile. Ohnehin ist es im Private Banking keine Seltenheit, dass ein vermögender Kunde Beziehungen zu verschiedenen Banken unterhält. In der Schweiz beispielsweise pflegen High Net-Worth Individuals in der Regel Beziehungen zu mehreren Anbietern, da die einzelnen Kantonalbanken vergleichsweise klein sind.

Die Revolution internationaler Zahlungen

Blockchain ist auch ein Werkzeug, das grenzüberschreitende Zahlungsvorgänge vereinfacht. Ripple Labs beispielsweise hat ein Blockchain-Netzwerk für Zahlungsvorgänge aufgesetzt, das Banken weltweit verbindet. Der typische Anwendungsfall für das Open-Source-Zahlungsprotokoll Ripple ist die grenzüberschreitende Zahlung zwischen zwei KMUs. Das übliche Korrespondenzbank-System ist recht ineffizient, benötigt der Transfer doch fünf Tage, und für eine 1.000-Dollar-Transaktion können die Gebühren bis zu 50 Dollar betragen. Beim herkömmlichen System besteht auch die Gefahr, dass die zwischengeschaltete Bank zahlungsunfähig wird, sodass eine Transaktion unabgeschlossen bleibt. Die Blockchain-Lösung bietet hier mehr Effizienz. Ripple hat dazu eine interne Währung geschaffen, deren Kurse autorisierte Marktmacher festlegen. Zahlungen sind in Minuten abgeschlossen und hängen nicht mehr davon ab, dass Nachrichten ausgetauscht werden. Weil allerdings die interne Währung keine wirkliche digitale Währung ist, benötigt jede Bank gewisse Beträge, um die Transaktionen zu garantieren. Trotz dieser Einschränkung erscheint die Lösung durchaus vielversprechend. Zudem wird es die neue PSD/2 Zahlungsdiensterichtlinie Klienten gestatten, alle Konten, die sie bei verschiedenen Banken haben, durch eine einzige Nutzeroberfläche zu managen. Diese Revolution im Front-Office wird massive Auswirklungen auf die Bankenlandschaft haben. Sie könnte sogar eine vergleichbare Revolution im Back-Office nach sich ziehen. Blockchain-Technologie würde Zahlungssysteme ermöglichen, die mit Transaktionen arbeiten statt mit Nachrichten – ein Clearing-Mechanismus wäre dann überflüssig. Hat man dann noch im Hinterkopf, dass es auf der ganzen Welt Bestrebungen gibt, den Gebrauch von Bargeld massiv einzuschränken, wird die Bedeutung dieser Technologie klar.

Die Möglichkeit smarter Kontrakte

Blockchain-Technologie kann auch dazu dienen, „smarte Kontrakte“ aufzusetzen, die anhand definierter Kriterien automatisch ausführbar sind. Auch Avaloq forscht aktuell in diese Richtung, unter Einsatz von Blockchain-Technologien wie Ethereum und Hyperledger. In diesem Anwendungsszenario dient Blockchain dazu, den Lebenszyklus von Finanzprodukten zu überwachen, die komplexer als bloße Zahlungen sind – was Optionen und andere derivative Instrumente einschließt. Die Natur von Derivaten macht es für die Gegenparteien erforderlich – seien die Produkte over-the-counter oder gelistet –, stets die Marktbedingungen zu überwachen und zu monitoren, wann Barrieren erreicht sind. Denn sobald bestimmte Marktbedingungen eintreten, werden Zahlungsflüsse generiert. Mehrere hundert oder tausend solcher Produkte zu überwachen, benötigt beträchtliche Ressourcen und erfordert einige Anstrengungen für den Finanzabgleich. Es wäre darum effektiver, diesen Prozess zu automatisieren: Smarte Kontrakte auf

Blockchain-Basis könnten dazu dienen, diese Zahlungsflüsse zu terminieren. Ein weiterer Vorteil einer solchen Lösung ist, dass sie die Flexibilität von OTC mit jener Transparenz verbindet, die Regulierungsbehörden verlangen. Kurz gesagt: Sie vereint das Beste beider Welten. Auch aus diesem Grund nehmen die Vereinigten Staaten bereits eine Vorreiterrolle bei der Entwicklung von Blockchain-Technologie ein. Zahlreiche Initiativen sind in den USA in diesem Bereich angestoßen worden, wobei es den Promotern dieser Technologie hilft, dass sie einfacheren Zugang zu Kapital erhalten. Die Investments in diese Projekte haben im vergangenen Jahr bereits einen Wert von ungefähr einer Milliarde US-Dollar erreicht.

Kleineres Ökosystem, schnellere Umsetzung

Die Geschwindigkeit, mit der sich Blockchain-Technologie verbreiten kann, hängt von länderspezifischen Gegebenheiten in den Banking-Märkten ab. In kleinen oder noch nicht existierenden Ökosystemen wird ein schnellerer Fortschritt möglich sein. In dem vorgestellten Know-Your-Customer-Anwendungsfall etwa wird Blockchain keine existierenden Infrastrukturen ersetzen müssen. Hier wird der Weg zur Reife wohl einfacher sein als in größeren Use Cases. Dasselbe gilt aus geografischer Perspektive: In einem kleinerem Markt wie Australien dürfte es leichter fallen, Blockchain-Technologien einzuführen, denn unter nur vier Banken lässt sich vermutlich schneller eine Übereinkunft herstellen. Ähnliches trifft auf die Schweiz zu, denn hier ist durch das zentralisierte SIX-Zahlungssystem, an dem 130 Banken beteiligt sind, der Integrationsgrad schon recht hoch. Aber dass bereits solch ein zentralisiertes und effektives Werkzeug vorhanden ist, erschwert wiederum die Migration zu einer alternativen Lösung.

Das Beharrungsvermögen der Branche

Natürlich würde gerade der Wertpapierhandel von Blockchain-Technologie extrem profitieren. Dennoch wird die Umsetzung hier voraussichtlich langsam verlaufen – ein Zeitraum von 10 oder 15 Jahren ist wahrscheinlich. Man denke nur daran, dass Prozesse, die vor vier Jahrhunderten im Handel zwischen Amsterdam und London etabliert wurden, noch bis heute Spuren hinterlassen haben. Die Intention, die Branche innerhalb kurzer Zeit zu transformieren, wird also auf ein fest etabliertes Ökosystem mit tiefen historischen Wurzeln treffen. Auch haben viele Akteure, wie etwa Broker und Treuhänder, kein besonderes Interesse an einer Disruption, die sie überflüssig macht. Zudem geht es hier um ein System von weltweiter Dimension. Die paradoxe Situation ist diese: Je attraktiver ein Use Case aufgrund seiner Einsparungspotenziale ist, desto höher wird voraussichtlich die Zurückhaltung sein, diesen Anwendungsfall Realität werden zu lassen – gerade wegen der großen Zahl an Zwischenhändlern und Vermittlern, die alle etwas zu verlieren haben.

Eine aktuelle PwC-Studie zu Blockchain in Financial Services, die die Etablierung von Blockchain in Banken in Deutschland untersucht, scheint dies zu bestätigen. Von den befragten 150 Führungskräften halten immerhin 67 Prozent Informationssicherheit und Betrugsprävention für einen wahrscheinlichen bis sehr wahrscheinlichen Anwendungsfall für die Technologie, aber nur 35 Prozent vertreten diese Meinung im Hinblick auf Börsen- und Handelsplattformen.

Fazit: Blockchain ist die Zukunft

Im Laufe der nächsten Monate sollten die ersten Blockchain-Initiativen ihre Produktivphase erreichen. Diese potenziell miteinander wettstreitenden Initiativen unterscheiden sich in ihrer Form und Technologie voneinander – sie werden die Branche vor Integrationsprobleme stellen. Dennoch werden diese Herausforderungen nicht notwendigerweise größer sein als jene, denen wir uns schon jetzt gegenüber sehen, beispielsweise im Wertpapierbereich. Noch mag es bei den Blockchain-Lösungen einen Mangel an Standardisierung geben. Aber es ist unabweisbar: Die Technologie wird Bestand haben. Denn Blockchain gestattet es, alle Vermögenswerte wirklich zu digitalisieren. Blockchain gehört die Zukunft.

Meilensteine von Blockchain im Banking

- $93 Millionen sind in Ripple investiert worden (im Anschluss an die letzte Kapitalerhöhung des Start-ups im September 2016).
- 69 Prozent aller Banken experimentieren bereits mit Permissioned Blockchain Networks (Infosys/LTP-Studie, Februar 2017).
- Auch die Führungskräfte deutscher Banken erwarten heute zu 63 Prozent, dass Blockchain-Technologie ihr Geschäftsmodell innerhalb der nächsten zehn Jahre beeinflussen wird – so das Ergebnis einer aktuellen PwC Studie unter 150 Führungskräften im deutschen Banking (https://www.pwc.de/de/finanzdienstleistungen/assets/blockchain-in-fs.pdf).
- Eine Statista-Studie zeigt, dass 60 Prozent alle Banken erwägen, Blockchain-Technologie für internationale Transfers einzusetzen, 23 Prozent für Zahlungsabwicklungen und 20 Prozent für KYC-Legitimationsprüfungen (https://www.statista.com/statistics/648044/blockchain-usage-by-financial-institutions/)
- Eine IBM-Studie mit 200 Banken aus 16 Ländern ergab, dass 91 Prozent der Banken in Blockchain-Lösungen für Einlagen investieren: Bei 15 Prozent wird ein Blockchain-Projekt schon 2017 produktiv gehen – und damit bereits im ersten Jahr, in dem es überhaupt produktive Blockchain-Banking-Projekte gibt (IBM: „Leading the pack in blockchain banking: trailblazers set the pace“, 2016).

Uwe Krakau, Philippe Meyer

Video ist die neue Weltsprache.

Gründen Sie Ihr Medienhaus – ein Plädoyer

Wer mit Videos arbeitet, erlebt, dass seine Kunden auf dieses Medium mit einer erhöhten Kaufwahrscheinlichkeit reagieren. Eine Steigerung bis zu 1000 % ist möglich – so geschehen bei blendtec-Mixern. So ist es kein Wunder, dass Videos auf Plattformen wie Facebook ab spätestens 2019 dominieren. Dann entstehen 80 % des Traffics durch Videos.

Viele große und kleine Unternehmen positionieren sich deshalb schon jetzt in diesem Segment und werden zu Medienhäusern. Um die 40 % dieser Online-Video-„Medienunternehmen“ geben an, dass sich ihre Investitionen bereits amortisieren:

- Die Marriott-Hotel-Gruppe produziert im eigenen Content-Studio kurze Action-Comedys mit dem Titel „Two Bellmen“.
- Die dänische Jyske Bank hat ein Fernsehstudio gegründet und berichtet mit erstklassigem Expertenwissen aus der Welt der Finanzen.
- Der kleine US-Swimmingpool-Anbieter River Pools erklärt in Videos alles rund um den komplexen Poolkauf – und ist damit Marktführer in seinem Segment geworden.
- General Electric bietet ein Videoprogramm mit unterschiedlichsten Formaten auf mehreren Kanälen, das fast an die BBC erinnert. Das Unternehmen erreicht damit Millionen Kunden und User weltweit.

Was bedeutet diese Entwicklung für Unternehmen in Deutschland? Dass auch wir Geschichten in Videoform erzählen müssen, die unseren Kunden echten Nutzen und Mehrwert bieten. Das geht nur, wenn wir uns als Medienhaus verstehen und formieren.

Eine Anleitung in acht Schritten:

1. Hören Sie auf, das Thema Video weiter an Agenturen, Produktionsunternehmen oder studentische Hilfskräfte zu delegieren. Machen Sie Video zur Chefsache.
2. Gehen Sie strategisch vor. Setzen Sie ein Teamprojekt „Medienhaus“ auf, das analysiert, Experten befragt und einen kohärenten Plan entwickelt. Erst dann legen Sie los.
3. Legen Sie ein realistisches Budget für Personal, Raum, Technik und Fortbildung fest.
4. Überlegen Sie, wie Sie das Medienhaus organisatorisch integrieren: Wie steht es zu Marketing, Kommunikation, PR, HR, Vertrieb und zur Produktion? Vorsicht vor Silo-Zuordnungen.
4. Bestimmen Sie einen weiblichen oder männlichen Chief Content Officer.
5. Engagieren Sie exzellente Coaches.
6. Definieren Sie das Projekt Medienhaus als „Academy“. Trainieren Sie in Workshops und lassen Sie spielerischen Spaß zu. Machen Sie nicht alles perfekt – aber kommen Sie möglichst schnell in die Umsetzung, um beim Tun zu lernen.
7. Stellen Sie sich den Medienhaus-Prozess wie eine Treppe vor. Sie werden viele Stufen erklimmen müssen, um mit Ihrem Unternehmen in zwei Jahren auf einem anderen Niveau als Ihre Wettbewerber zu sein.
8. Gestalten Sie Ihre Kommunikation auf allen Kanälen. In den sozialen Medien, auf Ihren Homepages, in der internen Kommunikation und auf Veranstaltungen. Lernen Sie durch Interaktionen und Kommentare, wie Ihre Kunden ticken. Führen Sie einen Wachstumsdialog mit Ihnen. Erst dann können Sie den emotionalen Erlebnismarkt Ihres Unternehmens zielführend gestalten.

Uwe Walter

Uwe Walter ist Storytelling- und Change-Experte für Medien- und Industrieunternehmen. Er berät so unterschiedliche Kunden wie YouTube-Stars, Start-ups, Blogger, Verlage, Radio- und Fernsehsender sowie Filmproduktionen. Seine Expertise: Wie generiere ich Reichweite durch zukunftssicheres Erzählen.

Foto: privat

Dr. Michael Müller-Wünsch (Otto) über den Versandhandel als daten-getriebenes Echtzeitunternehmen

Networking zwischen den Vorträgen

Clarissa Käfer (Feinkost Käfer), Sebastian Wiese (Zeppelin GmbH) und Dr. Marco Maier (HYVE) im Gespräch mit Margit Dittrich (personalmanufaktur)

Das Auditorium der Allianz war mit über 300 Teilnehmern aus gut 150 Firmen restlos ausverkauft

Prof. Dr. Sami Haddadin über Roboter, die einfach und flexibel nutzbar sind

MÜNCHEN
DIGICON 2017

Zwei Tage Digitalisierung zum Anfassen, Erleben und Nachvollziehen: Die DIGICON 2017 zog am 23. und 24. November die Entscheider aus Mittelstand und Weltkonzernen im komplett ausverkauften Allianz Auditorium regelrecht in ihren Bann. Smarte Innovationen überzeugten mit hoher Praxisrelevanz. Marktreife Konzepte überraschten mit disruptivem Potenzial, wie z. B. die erste hardwareunabhängige, AR-basierte Indoor-Navigations-Lösung von der Insider Navigation GmbH.

Ein leidenschaftlich umkämpfter Münchner Digital Innovation Award, den die Firma eBlocker GmbH für ihre Lösung für anonymes Surfen und Jugendschutz gewann, hinterließ überraschende Eindrücke. Kurz: Digitalisierung mit hohem Wertschöpfungspotenzial und Begeisterungsfaktor war das klare Asset der DIGICON 2017.

Fotos: LMU München

Networking auf dem Galaabend im Cafe Reitschule

Exklusiver Galaabend mit Marktplatz der Innovationen im Cafe Reitschule

Insider Navigation auf dem Marktplatz der Innovationen

Dr. Michael Fausten (Bosch) über automatisiertes Fahren

SZENE DIGITALE WELT

Das Allianz Auditorium schien geradezu prädestiniert für ein Event wie die DIGICON – bei dem sich alles um Digitalisierung und Innovationen dreht.

Neuveröffentlichung des Buches Digital Marketplaces Unleashed

Stefan Mennerich (FC Bayern München) über die Prinzipien der Medienarbeit: Content, Rechte und Unabhängigkeit

Sandra Scherzer (Zeppelin) im Gespräch mit Joachim Schreiner (Salesforce), Dr. Michael Fausten (Bosch) und Sebastian Feld (LMU)

Stephan Schneider (Vodafone GmbH) im Gespräch mit Sven Heistermann (Google), Dr. Norbert Gaus(Siemens), Stephan Schneider (Vodafone GmbH), Andrea Martin (IBM) und Sven Rühlicke (Antenne Bayern)

Die QAware GmbH war Gastgeber für den Digitalk im Oktober 2017. Im Hauptgebäude im Süden Münchens kamen die Mitglieder des Digitalen Stadt München e. V. sowie interessierte Gäste, um sich mit dem Thema Cloud Computing auseinanderzusetzen.

Dr. Josef Adersberger (QAware) erklärte im ersten Vortrag anschaulich, welche Vor- und Nachteile dezentrale, cloud-basierte Mikroservices gegenüber herkömmlichen monolithischen Anwendungen haben.

Jörg Treiner (Chefarchitekt Allianz Deutschland) sprach darüber, wie der Migrationsprozess zur Cloud bei der Allianz vorangetrieben wird.

In einem weiteren Fallbeispiel, erzählte Leander Reimer (QAware) wie, BMW Aftersales Systeme erfolgreich migriert werden und was wichtige Voraussetzungen des Erfolgs sind.

Die Mitglieder des Digitalen Stadt München e. V. nutzten den letzten Digitalk des Jahres, um sich intensiv auszutauschen.

MÜNCHEN

Digitale Stadt München e.V.

Am 19. Oktober gastierte der Digitale Stadt München e. V. bei der QAware GmbH im Süden Münchens. Das Thema des Abends lautete Cloud (native) Computing. Dabei ging es um die Fragen: Können bestehende Systeme erhalten und gleichzeitig fit für die Zukunft gemacht werden? Wie lässt sich die Cloud nicht nur als Speicherplatz/Infrastruktur verstehen, sondern als Basis, um Anwendungen zu bauen, die bisher undenkbar waren und Prozesse in Großkonzernen revolutionieren.

Im Anschluss an die Vorträge gab es ein exzellentes italienisches Buffet und einige Erfrischungen.

Ca. 280 Gäste kamen zur OpenMunich, die am 01. Dezember 2017 im Hauptgebäude der LMU stattfand.

Open Source und New IT sind die Keywords der OpenMunich.

In der breit besetzten Podiumsdiskussion kamen AI-Experten aus verschiedensten Bereichen zu Wort.

Dr. Marco Maier von der Hyve AG stellt vor, wie man mit Open Source Technologien Innovationen kreiert.

MÜNCHEN

OpenMunich

Am 01. Dezember 2017 führte der Lehrstuhl für Mobile und Verteilte Systeme der LMU die Konferenz “OpenMunich, Conference for Open Source and New IT” durch. Mit Sponsoring und inhaltlicher Unterstützung von Red Hat, Accenture, Microsoft, Hyperledger, Bosch, Couchbase und Hyve konnten mehr als 30 Speaker für die Tageskonferenz für Vorträge und Workshop gewonnen werden.

Fotos: Digitale Stadt München, LMU München

Frauen machen Wirtschaft: Unter diesem Titel fand der Digitalk der Digitalen Stadt Düsseldorf e. V. am 9. November bei der Stadtsparkasse Düsseldorf auf der Berliner Allee statt.

Mehr als 200 Teilnehmer waren zu Gast, denn das Thema ist brandaktuell: Frauen fehlen in Spitzenpositionen.

Farblich und kulinarischer Hingucker waren die leckeren Nachspeisen.

Darf bei keinem Digitalk fehlen: Genügend Zeit zum Diskutieren und Kennenlernen.

Stephan Schneider (Vorstandsvorsitzender Digitale Stadt Düsseldorf e. V.) im Gespräch mit vl. n. r-.: Stefanie Kemp (Innogy SE), Heike Cohausz (P4 Career Consultants), Karin-Brigitte Göbel (Vorsitzende des Vorstands, Stadtsparkasse Düsseldorf), Tanja Richter (Vodafone Group).

Zu Beginn gab es zahlreiche Begrüßungen zwischen den Mitgliedern der Digitalen Stadt Düsseldorf e.V..

Geben auch als Engel eine gute Figur ab: Stephan Schneider (Vorstandsvorsitzender Digitale Stadt Düsseldorf e. V.) und Thomas Schiffer (Provinzial Rheinland)

DÜSSELDORF

Digitale Stadt Düsseldorf e.V.

Frauen machen Wirtschaft

Frauen fehlen in den Spitzenpositionen der Wirtschaft. Warum ist das so? Sind es allein soziokulturelle Gründe? Oder liegt der Fehler im System? Was machen Frauen anders, die alle Widrigkeiten überwinden und es bis an die Spitze schaffen? Dieser Thematik widmete sich die Digitale Stadt Düsseldorf e.V. beim Digitalk am 9. November. In einer hochkarätig besetzten Podiumsrunde ging es um erfolgreiche Frauenkarrieren und um den Beleg, dass Frauen in Führungspositionen ein ökonomischer Vorteil für die Gesellschaft sind.

Provinzial Rheinland

Zum traditionellen Weihnachtsdigitalk kamen rund 200 Gäste. Thema war diesmal die Nutzung der Microsoft Azure Cloud. Denn die digitale Revolution macht auch vor Versicherungsunternehmen nicht halt. Was im privaten Bereich mit iCloud und Dropbox bereits vollkommen normal ist, hält jetzt auch Einzug in die „konservative“ Versicherungs-IT. Es ist nicht mehr die Frage, ob man als Unternehmen die Cloud-Angebote großer, internationaler Anbieter annimmt, sondern nur noch die Frage des „Wann“ und „Wie“. Die Provinzial Rheinland und die Sparkassen DirektVersicherung haben sich strategisch neu ausgerichtet und stellen die strategischen Aspekte sowie die Themen IT-Technik, IT-Security und Datenschutz auf dem Digitalk vor.

Inspirierende Gespräche und ein Gläschen Wein sind ideale Begleiter um den Abend genussvoll ausklingen zu lassen.

Das Ambiente zum Digitalk bei der Provinzial Rheinland war weihnachtlich, das Thema technisch: Der Einzug der Digitalen Revolution in die Welt der Versicherungsunternehmen.

Rund 200 Leute kamen zum Digitalk bei Provinzial Rheinland.

Fotos: Digitale Stadt Düsseldorf

FACHBEIRAT

Robert Blackburn
CEO Hoffmann Group

Patric Fedlmeier
CIO Provinzial Rheinland

Norbert Gaus
Executive VP SIEMENS

Sandro Gaycken
Direktor ESMT

Michaela Harlander
Vorstand Harlander-Stiftung

Markus Heyn
GF BOSCH

Martin Hofmann
CIO Volkswagen

Manfred Klaus
Sprecher der GF Plan.Net

Andrea Martin
CTO IBM

Niko Mohr
Partner McKinsey

Frank Rosenberger
Group Director TUI

Joachim Schäfer
GF Messe Düsseldorf

Ralf Schneider
CIO Allianz Group

Stephan Schneider
Manager Vodafone

Marc Schröder
GL MG RTL Deutschland

Uwe Walter
Waltermedia

Michael Zaddach
CIO Flughafen München

IMPRESSUM

VERLAG
Vogel Business Media GmbH & Co. KG, Max-Planck-Str. 7/9, 97064 Würzburg, www.vogel.de
Geschäftsführer
Matthias Bauer, Florian Fischer, Günter Schürger

REDAKTION
Chefredaktion Claudia Linnhoff-Popien (V. i. S. d. P.)
Chef vom Dienst Marie Kiermeier
Fachbeirat Robert Blackburn, Patric Fedlmeier, Norbert Gaus, Sandro Gaycken, Michaela Harlander, Markus Heyn, Martin Hofmann, Manfred Klaus, Andrea Martin, Niko Mohr, Frank Rosenberger, Joachim Schäfer, Ralf Schneider, Stephan Schneider, Marc Schröder, Uwe Walter, Michael Zaddach
Redaktion Florentina Hofbauer, Anna-Sophie Rauschenbach
Redaktionsassistenz Kerstin Fischer, Katja Grenner
Mitarbeiter dieser Ausgabe Sebastian Feld, Thomas Gabor, Kyrill Schmid, Andreas Sedlmeier
Lektorat und Schlussredaktion KorrekturService Sand, Wolfgang Sand, Ahornallee 89, 86899 Landsberg

ANFRAGEN AN DIE REDAKTION
redaktion@digitaleweltmagazin.de

GRAFIK
Layout Ivar Våge, Alexander Auffermann
Art Director Ivar Våge, www.deed-muc.com

ANZEIGEN
Institut für Informatik, Ludwig-Maximilians-Universität München, Oettingenstr. 67, 80538 München,
anzeigen@digitaleweltmagazin.de
Ansprechpartner Tanja Zecca,
Tel. +49 89 2180-9171

HERSTELLUNG
Druck ColorDruck Solutions GmbH,
Gutenbergstraße 4, 69181 Leimen

ABO-SERVICE
eMedia Leserservice, Postfach 24 69, 49014 Osnabrück
Tel. +49 541 800 09-126, Fax +49 541 800 09-122
E-Mail: leserservice@emedia.de
DIGITALE WELT erscheint einmal pro Quartal
Einzelpreis 8,50 €; Österreich 9,50 €; Schweiz 13,90 CHF

ABONNEMENTPREISE
Vier Ausgaben inklusive Versandkosten: Inland 30,60 €, Österreich 34,20 €, Schweiz 50.– CHF; ermäßigtes Abo für Schüler, Studenten, Auszubildende: Inland 17,– €, Österreich 19,– €, Schweiz 27,80 CHF (nur gegen Nachweis)
Der Bezug der Zeitschrift DIGITALE WELT ist im Mitglieds-Beitrag des Verbandes VOICE - Bundesverband der IT-Anwender e.V., Digitale Stadt München e.V. und Hannover IT e.V. enthalten.

HERAUSGEBER
Prof. Dr. Claudia Linnhoff-Popien, Institut für Informatik, Ludwig-Maximilians-Universität München, Oettingenstr. 67, 80538 München, Tel. +49 89 2180-9153,
www.digitaleweltmagazin.de

Termine

#7 MEETUP – HANNOVER

Termin: 3. März 2018, 11:00–20:00 Uhr | Ort: Pavillon Kultur- und Kommunikationszentrum (Lister Meile 4, 30161 Hannover)
Virtual Reality (VR) hat das Potenzial, die Art wie wir unseren Alltag erleben, grundlegend zu verändern. Und das sowohl im Bereich von Freizeitaktivitäten wie Computerspielen, als auch die Art, wie wir arbeiten, lernen und mit Informationen umgehen. „HannoVR“ ist für alle, die das Potenzial der VR erkannt haben oder kennenlernen und sich mit Gleichgesinnten austauschen möchten. Jeder ist willkommen, vom Entwickler, Designer, Gamer, VR-Fan bis zum Unternehmer.

DATENGETRIEBENE DIGITALISIERUNG DURCH FORSCHUNG UND INNOVATION

Termin: 6. März 2018, 15:00–17:30 Uhr | Ort: Technische Informationsbibliothek (Welfengarten 1 B / 30167 Hannover)
In der Veranstaltungsreihe für die Wirtschaft der Technischen Informationsbibliothek in Hannover „Unterstützung der Digitalisierung durch Forschung Innovation" befasst sich das Event am 6. März 2018 mit der datengetriebenen Digitalisierung.

CMCX

Termin: 6.–7. März 2018 | Ort: Messe München
Die Content-Marketing Conference & Exposition (CMCX) – Europas größtes Content-Marketing-Event. Networking, Know-how, Branchenüberblick: Auf der CMCX, dem jährlichen Highlight der Content-Marketing-Branche, treffen sich am 6. und 7. März wieder Entscheider aus Marketing und Medien, um die neuesten Trends zu erfahren und Best Cases zu diskutieren.

SECIT BY HEISE

Termin: 6.–7. März 2018 | Ort: Niedersachsenhalle in Hannover (Theodor-Heuss-Platz 1–3 / 30175 Hannover)
secIT Hannover ist der neue Treffpunkt für Security-Anwender und -Anbieter. Besucher erfahren alles über die neuesten Trends, Methoden, Lösungsansätze sowie aktuelle Softwarelösungen und Produkte. Mitglieder der Hannover IT e. V. erhalten 25 % Rabatt auf die Eintrittskarte.

XPOMET

Termin: 21.–23. März 2018 | Ort: Kongresshalle am Zoo Leipzig (Pfaffendorfer Str. 31, 04105 Leipzig, Deutschland)
Medizinischer Fortschritt liegt mehr und mehr in der fachübergreifenden Vernetzung – das haben die Innovatoren aus dem Silicon Valley längst begriffen – der DACH-Markt scheint dabei noch hinterherzuhängen. Hier gilt es, in vielen Bereichen Brücken zu bauen, sich weiter zu öffnen und eine gemeinsame Sprache unter den Stakeholdern zu entwickeln. Für diese Art von Austausch, der unbedingt auch auf internationaler Ebene stattfinden sollte, und um den notwendigen kulturellen Wandel anzustoßen, benötigt die Healthcare-Welt eine Plattform, die die Dinge etwas anders angeht: Diese zu schaffen ist das Ziel der XPOMET Convention, die vom 21. – 23. März 2018 in der KONGRESSHALLE am Zoo Leipzig stattfindet.

36. WEBMONTAG

Termin: 16. April 2017, 18:45–22:00 Uhr | Ort: U-Turn (Bischofsholer Damm 97, 30173 Hannover)
Der Webmontag ist ein informelles, nichtkommerzielles, dezentral organisiertes Treffen, das zum Ziel hat, all diejenigen miteinander zu verbinden, die die Zukunft des Internets gestalten.

DATA FESTIVAL

Termin: 16.–18. April 2018 | Ort: Gaszählerwerkstatt / Agnes-Pockels-Bogen 6 / 80992 München
Auf dem Data Festival, das vom 16. bis 18. April 2018 erstmals in München stattfindet, dreht sich alles um Daten. Im Fokus stehen die Themen Data Science & Machine Learning, Data Engineering & Architecture, Data Visualization & Analytics, Fast Data, Infrastructure, Databases sowie Agile Development.

PERSONAL SÜD

Termin: 24.–25. April 2018 | Ort: Messe Stuttgart
Seien Sie dabei, wenn die PERSONAL Süd am 24. und 25. April 2018 zum 19. Mal in der Messe Stuttgart stattfindet. Rund 4.800 HR-Visionäre und 300 Top-Aussteller garantieren eine Leistungsshow auf höchstem Niveau. Mit rund 160 Beiträgen und interaktiven Formaten bietet das innovationsgeprägte Begleitprogramm der PERSONAL Süd Wissen aus erster Hand. Speziell aufs Networking ausgerichtete Formate garantieren spannende Fachdiskussionen und neue Impulse. Die Aussteller auf der PERSONAL Süd präsentieren Ihnen innovative Ideen und Produktlösungen aus allen HR-Bereichen – von Organisationsentwicklung und Führung über Recruiting, HR-Software und Arbeitsrecht bis zu E-Learning, Weiterbildung und Training.

PERSONAL NORD – DAS HR-EVENT IN HAMBURG

Termin: 15.–16. Mai 2018 | Ort: Messe Hamburg
Die Messe PERSONAL Nord ist die führende Veranstaltung für Personalmanagement in Norddeutschland. Am 15. und 16. Mai 2018 treffen sich rund 4.000 Personaler bereits zum siebten Mal in den Hamburger Messehallen. Über 275 Top-Aussteller präsentieren ihre Produkte, Dienstleistungen und Innovationen.

next-digital-leader.de

Der Status quo ist der Hintern.
Du bist der Tritt.

Next Digital Leader gesucht! Du willst etwas bewegen und kannst auch mal unbequem sein? Dann bist du bei uns genau richtig. Egal, ob du noch studierst oder bereits im Beruf stehst – mit deinem Drang zur Digitalisierung machst du mit uns die deutsche Wirtschaft fit für die digitale Zukunft.

Interesse? Mehr auf next-digital-leader.de!