

COMPUTERWOCHE

Ausgabe 2018 – 38-39 17. September 2018 Nur im Abonnement erhältlich

VON IDG



Innentätern auf der Spur

Wer die Verfolgung aufnimmt,
begibt sich auf sensibles Terrain.

Seite 14

VMware drängt in neue Märkte

Hausmesse VMworld
gibt die Richtung vor.

Seite 6

So digitalisiert der Daimler-Konzern

Interview mit dem Chef
von DigitalLife@Daimler.

Seite 32

Der Arbeitsplatz der Zukunft

IDG-Studie zeigt:
Die Mitarbeiter wollen
mitreden.

Seite 38

IT-Sicherheit erfordert vor allem Disziplin

In Sachen IT-Security empfiehlt es sich, Ruhe zu bewahren und seine Hausaufgaben zu machen. Es ist eine Illusion zu glauben, alle Risiken in den Griff bekommen zu können.

Wenn Sie sich einmal richtig schlecht fühlen wollen, dann besuchen sie eine der großen IT-Security-Konferenzen – von RSA beispielsweise, oder die Defcon. Sie gehen garantiert mit dem Gefühl nach Hause: Egal wie ich meine Netze absichere oder meine Mitarbeiter schule, am Ende sitze ich immer am kürzeren Hebel. Den Angreifern und Geheimdiensten wird es gelingen, in meine Festung einzudringen, mich auszuspionieren oder mich zu erpressen.

Zugegeben, in diesem Heft tragen wir nicht unbedingt zur Beruhigung bei, wenn wir zum Beispiel über Deepfakes schreiben (siehe Seite 18). Dabei manipulieren Hacker Video- und Audiodateien in einer Weise, dass man geneigt ist, US-Präsident Trump zu glauben, wenn er wieder einmal poltert: „Alles Fake!“ Spätestens wenn wir dann noch über die neuen Möglichkeiten nachdenken, die KI oder auch Quantencomputing den Angreifern bieten, wird uns endgültig schwindelig.

Die IT vollständig sicher unter Kontrolle zu haben, war schon immer eine Illusion. Aber das Risiko lässt sich senken, indem Unternehmen ihre Hausaufgaben machen – insbesondere in den naheliegenden Bereichen Patch-Management und Social Engineering Prevention. Viele Betriebe hierzulande tun das: In einer internationalen Studie von Malwarebytes, für die auch 175 Sicherheitsexperten aus Deutschland befragt wurden, heißt es: „Deutsche Unternehmen hatten bei Weitem die wenigsten Sicherheitsvorfälle aller von uns untersuchten Länder“ – zu denen die USA, Australien, Singapur und Großbritannien gehörten. 56 Prozent der hiesigen Firmen melden für die vergangenen zwölf Monate keinen Vorfall, bei allen anderen stehen Adware- und Spyware-Angriffe (21 Prozent) und Phishing-Angriffe im Vordergrund. Gerade im IT-Sicherheitsbereich zahlt sich die deutsche Gründlichkeit aus!

Herzlich,
Ihr



Heinrich Vaske, Editorial Director



Heinrich Vaske,
Editorial Director



Tipps für CISOs

Fünf Fakten, denen Chief Information Security Officers ins Auge sehen sollten:

www.cowo.de/a/3545773

▶ 14

**Innentätern
auf der Spur**

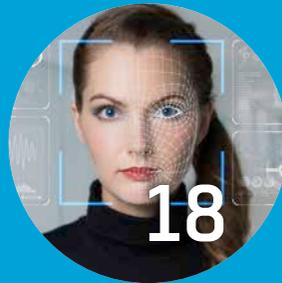
Fahrlässiges oder mutwilliges Fehlverhalten der eigenen Mitarbeiter stellt für Unternehmen das größte IT-Sicherheitsrisiko dar. Dabei bilden die Topmanager keine Ausnahme, im Gegenteil. An technischen Möglichkeiten, den Bedrohungen entgegenzutreten, herrscht kein Mangel. Dennoch treten immer wieder Schwierigkeiten auf, ist es doch alles andere als trivial, für Sicherheit zu sorgen und dabei die Datenschutz- und Persönlichkeitsrechte jedes Einzelnen zu wahren.

**Markt**

- 6 VMware blickt in die Zukunft**
Mit den Projekten Dimension, Magna und Concord stellt VMware die Weichen in Richtung Edge Computing, autonomes Rechenzentrum und Enterprise Blockchain.
- 8 Aus für Datentreuhänderschaft**
Nach eher enttäuschenden Ergebnissen nimmt Microsoft von der Idee Abstand, T-Systems als deutschen Datentreuhänder für Cloud-Geschäfte zu beauftragen.
- 12 KI – ein Mega-Markt**
McKinsey rechnet vor, wie hoch die zusätzliche Wertschöpfung durch KI für Unternehmen ausfallen kann. Wenn die Berater recht haben, sollten sich Unternehmen dringend auf den Weg machen.

**Technik**

- 24 Windows 10 Oktober 2018 Update**
Mit interessanten Neuerungen steigert Microsoft die Attraktivität von Windows 10 für End User. Auch die störenden automatischen Updates will der Softwarekonzern künftig angenehmer gestalten.
- 26 Die eine KI gibt es nicht**
In den öffentlichen Diskussionen entsteht der Eindruck, dass sich hinter künstlicher Intelligenz eine homogene Technologie verbirgt. Die gibt es aber gar nicht.
- 30 Droht Deutschland ein Blackout?**
Mit zunehmender Vernetzung und Digitalisierung sind die kritischen Infrastrukturen (Kritis) in Deutschland gefährdet.



Deepfakes

Manipulierte Video- und Audiodateien bereiten Sicherheitsexperten Sorge.



Praxis

32 Daimler auf Digitalisierungskurs

Markus Hägele leitet beim schwäbischen Autobauer den Bereich DigitalLife@Daimler. Dessen Aufgabe ist es, in allen Unternehmensbereichen den digitalen Wandel voranzutreiben. Einen Chief Digital Officer (CDO) braucht der Konzern dafür nicht.

36 Process Mining auf dem Vormarsch

Noch vor wenigen Jahren war Business-Process-Management (BPM) in aller Munde. Doch angesichts ausufernder Planungen und Modellierungen erlahmte das Interesse wieder. Heute verlassen sich Manager auf neue Techniken und Methoden der Prozessdatenanalyse.



Job & Karriere

38 Der Arbeitsplatz der Zukunft

Wie in den Unternehmen auf Dauer gearbeitet werden soll, ist eine der Kernfragen der digitalen Transformation. Deshalb ist das Thema in vielen Betrieben Chefsache. Doch die Mitarbeiter wollen mitentscheiden.

40 Home Office – ja, aber ...

Mitarbeiter glauben ebenso an die Vorzüge flexibler Arbeit wie ihre Chefs. Unterschiedliche Meinungen gibt es aber immer wieder hinsichtlich der Regeln.

44 Algorithmen für die Personalsuche

Software scheint unbestechlich, wenn es gilt, das richtige Personal auszuwählen. Doch das stimmt nicht ganz: Soziale Eigenschaften können Menschen besser einschätzen.

47 Stellenmarkt

49 Impressum

50 IT in Zahlen

VMworld 2018: Auf seiner Hausmesse greift VMware Zukunftsthemen auf

VMware hat einen Einblick in die Zukunftsprojekte „Dimension“, „Magna“ und „Concord“ gegeben. Die Dell-Tochter beschäftigt sich mit Edge Computing, dem autonomen Rechenzentrum und der Enterprise Blockchain.



Von Bernhard Haluschak,
Senior Editor Data Center
Technologies

Das Internet of Things (IoT) führt zu einer enormen Datenflut, so dass es wichtiger wird, Daten an der Entstehungsquelle verarbeiten und analysieren zu können. Das verspricht Edge Computing: Analyse-, Verarbeitungs- und Speicherfunktionen werden am Rand des Netzes lokalisiert, um Daten vor Ort zu verarbeiten oder sie nach bestimmten Regeln in die zentrale Cloud oder ein dediziertes Rechenzentrum weiterzuschicken.

Mit Project Dimension will VMware die hauseigenen Hybrid- und Multi-Cloud-Umgebungen auf die Systeme am Edge ausweiten und so das Verwalten und Automatisieren dezentraler Recheneinheiten vereinfachen. Der Softwareanbieter will sein Cloud-Angebot rund um SDDC-Infrastruktur (Software-defined Data Center) und Hardware as a Service auf Edge-Standorte ausdehnen und sich so um die Verwaltung der Infrastruktur, Fehlerbehebung, das Initiieren von Patches sowie um Wartungsarbeiten kümmern.

Cloud Foundation Stack auch für das Edge

„Es ist eine vollständige von VMware betriebene End-to-End-Umgebung“, sagte CEO Pat Gelsinger in seiner Keynote zur VMworld Ende August in Las Vegas. „Project Dimension macht den kompletten VMware Cloud Foundation Stack für Edge-, On-Premise-Systeme und die Cloud verfügbar.“

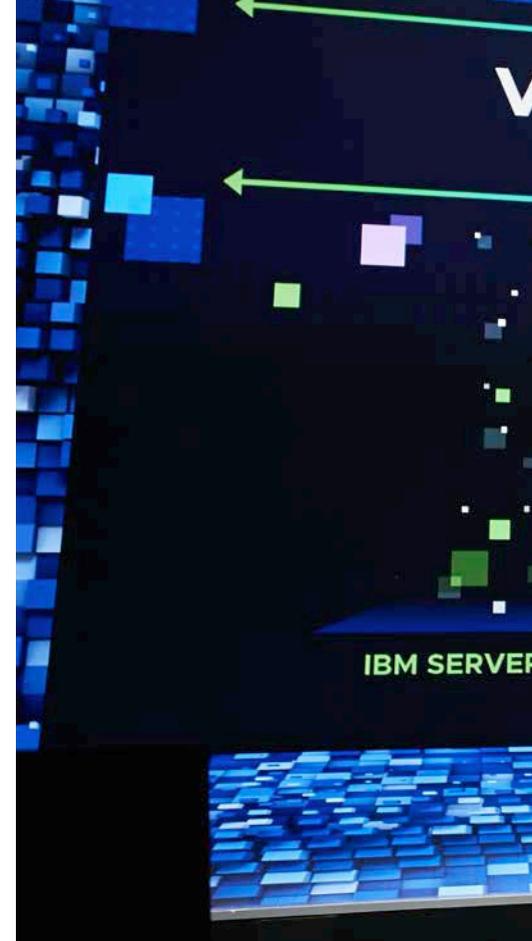
VMware arbeitet mit den Hardwarelieferanten Dell EMC und Lenovo zusammen. Sie stellen Kunden, die ein Edge-System benötigen, eine hyperkonvergente Hardware zur Verfügung. Diese ist so konzipiert, dass sie sich automa-

tisch mit der VMware Cloud verbindet und sich selbst konfiguriert, sobald der Kunde das System aktiviert hat.

Data Center sollen sich selbst optimieren

Noch in der Entwicklungsphase befindet sich Project Magna, das Teil der Initiative „Smarter Products“ ist. VMware nutzt maschinelles Lernen (ML) oder genauer: bestärkendes Lernen, um virtuellen IT-Infrastrukturen beizubringen, sich selbst zu optimieren. So sollen die Anforderungen einzelner Anwendungen im Detail erkannt und Anwendungs- sowie Infrastrukturkonfigurationen kontinuierlich verbessert werden. Ziel sei es, dass sich Rechenzentrums-umgebungen irgendwann selbst überwachen und regulieren könnten.

Laut VMware analysiert die Technologie unzählige Messpunkte auf dem System-Stack – angefangen beim Anwendungscode über die Hard- und Software-Infrastruktur bis hin zur Public Cloud und den Edge-Computern. Dabei können die gesammelten Daten der Kontrollpunkte dazu genutzt werden, die Infrastruktur in Bezug auf Leistung, Kosten oder benutzerdefinierte Richtlinien zu optimieren.



Sichere Cloud: Microsoft beendet Datentreuhand-Modell mit T-Systems

Mit Hilfe von T-Systems als Datentreuhänder versuchte Microsoft ein Cloud-Angebot zu etablieren, das besondere Sicherheit versprach – selbst vor amerikanischen Geheimdiensten. Doch die Kunden sprangen nicht darauf an.



Kunden von Microsoft Deutschland werden auch in Zukunft die erforderlichen Sicherheits-Updates erhalten, sagt Markus Nitschke, Director Microsoft Cloud Services.

Als Microsoft 2015 seine Microsoft Cloud Deutschland (MCD) ins Leben rief und dabei T-Systems zum „Datentreuhänder“ machte, ging es darum, den besonders skeptischen deutschen Kunden entgegenzukommen. Microsoft garantierte ihnen, dass auf die in der Cloud abgelegten Daten ausschließlich die Telekom-Tochter zugreifen könne. Die Daten würden Deutschland nicht verlassen. Für diesen besonderen Service sollten die Kunden allerdings einen Aufschlag zahlen.

Der Plan, den sich die Partner damals auch unter dem Eindruck der NSA-Schnüffeleien und der Snowden-Enthüllungen ausgedacht hatten, ging letztendlich nicht auf, weshalb Microsoft jetzt den Stecker gezogen hat. Für Bestandskunden steht die MCD zwar vorerst weiter zur Verfügung, nicht aber für Neukunden. Die sollen künftig Dienste aus Microsofts deutschen und europäischen Datenzentren nutzen. Derzeit sind zwei neue Großrechenzentren in Berlin und Frankfurt am Main im Bau. Dort soll der Azure Stack ab dem vierten Quartal 2019, Office 365 und Dynamics 365 dann ab Anfang respektive Mitte 2020 bereitstehen.

Nur noch aus Microsoft-eigenen RZs

In einem Blogbeitrag kündigt Markus Nitschke, Director Microsoft Cloud Services in Deutschland, an, man wolle die Cloud-Dienste künftig nur noch aus eigenen Rechenzentren in Deutschland offerieren. Das geschehe auf der Grundlage der Microsoft-Trusted-Cloud-Grundsätze sowie eines breiten Angebots an Compliance-Zertifikaten und -Testaten. Im Gespräch ist auch eine Zertifizierung nach dem Anforderungskatalog „Cloud Computing Compliance Controls Catalogue“ (C5). Ferner versichert der Konzern, die EU-Datenschutz-Grundverord-

nung (DSGVO) einzuhalten und entsprechende Regelungen in vertragliche Verpflichtungen aufzunehmen. Die Speicherung der Kundendaten erfolge in Deutschland, die Cloud-Dienste sind aber in das weltweite Microsoft-Cloud-Netz eingebunden.

Abkehr vom Treuhandmodell

Die Abkehr vom Treuhandmodell begründet Microsoft damit, dass sich in den letzten drei Jahren die Kundenanforderungen spürbar geändert hätten. Anwender hätten Vertrauen in die Cloud-Angebote der großen Provider gefasst und erwarteten jetzt vor allem umfassende Funktionen und Konnektivität zur globalen Cloud-Infrastruktur. Das habe die isolierte Microsoft Cloud Deutschland nicht ermöglicht. Seinen MCD-Kunden verspricht Microsoft aber auch künftig die erforderlichen Sicherheits-Updates. Wer migrieren wolle, könne noch in diesem Jahr erste Details zu den entsprechenden Möglichkeiten erfahren.

In der Rolle als Datentreuhänder kontrolliert und überwacht T-Systems für die Bestandskunden weiterhin jeden physischen und logischen Zugriff auf Kundendaten und beaufsichtigt auch Microsofts Zugriffe auf Server mit Kundendaten. Der Softwarekonzern verfügt über keine technischen Möglichkeiten, ohne Zustimmung des Treuhänders auf Daten zuzugreifen, und hat auch keinen physischen Zugang zu den entsprechenden Rechenzentren. Jede einzelne Datenherausgabe an Dritte muss die Telekom-Tochter freigeben. Nur wenn deutsches Recht es erforderlich macht oder der Kunde es verlangt, legt T-Systems Kundendaten offen. Auch Unternehmen in anderen EU-Ländern konnten die sichere Microsoft Cloud Deutschland in der Vergangenheit nutzen. (hv)