

Programmiersprachen:
Wird Java kostenpflichtig?

Anzeige



Support & Managed Service für
Open-Source-Umgebungen

Linux · OpenStack · Docker · Kubernetes

www.b1-systems.de

ROCKOLDING · BERLIN · KÖLN · DRESDEN

Mehr dazu im Heft!



MAGAZIN FÜR PROFESSIONELLE
INFORMATIONSTECHNIK

10
OKTOBER
2018

it-sa 2018
09.-11.10., Nürnberg:
**iX extra Security
it-sa-Guide 2018**

Marktübersicht:
**Zehn
Open-Source-
Firewalls**

VPS vs. Bare-Metal-Server:

Cloud-Server on demand

Lohnt der Umstieg?

Windows Server 2019 und Exchange Server 2019

Cloud-Infrastrukturen für das Internet of Things:

IoT-Dienste von Amazon, Google und Microsoft

Administration und Kosten im Vergleich:

Container vs. Platform as a Service

Agiles Projektmanagement:

Nichtfunktionale Anforderungen

Die nächste Spectre-Generation:

Foreshadow-Angriffe auf VMware

Security-Awareness:

Schutz vor Social Engineering

Newsletter-RFC:

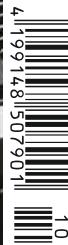
One-Click Unsubscribe

iOS und macOS verwalten:

Apple Business Manager

Neues Programmier-Tutorial:

Progressive Web Apps mit Workbox



€ 7,90

Osterreich € 8,70
Schweiz CHF 12,20
Luxemburg € 9,20

www.ix.de

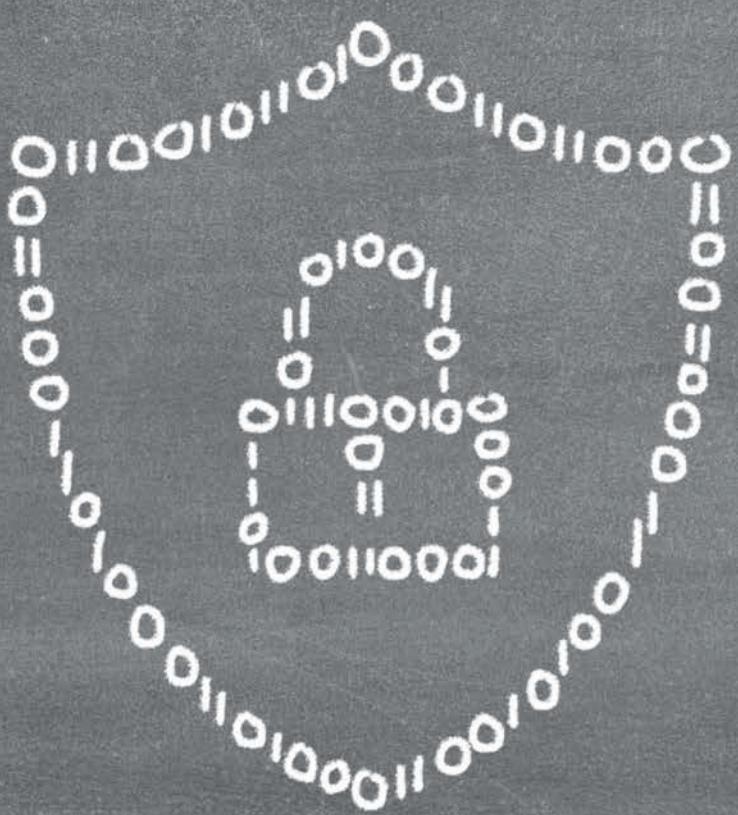


Lufthansa
Industry Solutions

Sie sind

IT-Security Spezialist (m/w)

und gehen immer
auf Nummer sicher?



- Mit der weltweiten Vernetzung von Unternehmen, Kunden und Lieferanten steigt der Bedarf an IT-Sicherheitslösungen. Als spezialisiertes Beratungsunternehmen unterstützen wir unsere Kunden dabei, ihre IT-Landschaften optimal aufzustellen.

Kommen Sie an Bord: www.lhind.de/karriere



Durch den Wandel bleibt beim Alten

Wieder hat Microsoft den Support seines angestaubten Windows 7 verlängert. Drei Jahre zusätzlich, bis 2023 sollen Unternehmen weiterhin Sicherheitsaktualisierungen erhalten – selbstverständlich gegen Bezahlung. Sofort wurden Stimmen laut, dass der Konzern auf sein nächstes Windows XP hinsteuern würde, dass Nutzer Windows 10 die kalte Schulter zeigen würden, dass die Tage Microsofts so ganz ohne Zukunftshoffnung am Horizont gezählt seien.

Auf den ersten Blick nicht ganz falsch. Die IT-Welt hat sich seit 2009, dem Erscheinungsjahr von Windows 7, stark verändert, so wie sie sich in den zehn Jahren nach Erscheinen von XP 2001 vollkommen wandelte. So begnügt sich Windows 7 zum Beispiel mit einem GByte Arbeitsspeicher und setzt keinen Multikernprozessor voraus. Heute kann selbst der gewöhnlichste Büro-Desktop mit einem Vielfachen an Rechenleistung aufwarten.

Jedoch spielt das keine Rolle – denn der zweite Wandel des letzten Jahrzehnts ist der Aufstieg der Cloud und ihrer Web-Applikationen. Das Betriebssystem bildet nicht mehr die Basis des Arbeitsalltags, der Browser hat diese Rolle für den

Großteil der Anwender übernommen. So muss ein Betriebssystem heute bloß noch zwei Aufgaben bewältigen: Chrome starten und sicher bleiben. Beide erfüllt Windows 7 noch immer zur Zufriedenheit der meisten Nutzer.

Windows 10 lockt hingegen mit solchen „Vorteilen“ wie penetranten Aktualisierungen, Verhaltensanalysen und aufdringlicher Werbung. Nichts, was sich Administratoren und Unternehmensnutzer herbeisehnen. Wenn das neue System für den Arbeitsalltag der Anwender keinen positiven Unterschied macht und Verantwortliche vor allem mehr Ärger beim Management des Systems erwarten – warum sollten sie dann wechseln?

Microsoft erhält offiziell selbstverständlich den Druck auf seine Kunden aufrecht. Das ergibt Sinn, denn so geht der Konzern langwierigen Konflikten wie beim Ende der XP-Ära aus dem Weg. Doch das Management weiß auch, dass ein Wechsel seiner Kunden zwar erfreulich, aber fürs eigene Geschäft nicht mehr von elementarer Bedeutung ist. Schon längst bildet Windows nicht mehr die Basis des Erfolgs der Redmonder.

Rechtzeitig hat man sich bei Microsoft auf die abnehmende Bedeutung des Betriebssystems eingestellt. Cloud-Dienste für Nutzer aller Couleur sind die Zukunft. Und das schlägt sich im Gewinn des Konzerns deutlich nieder – der Dominanz von Windows im Jahresabschluss weinen die Redmonder höchstens auf der Bühne eine nostalgische Träne nach.

Und was machen Unternehmen im Jahr 2023, wenn sich Windows 7 (wahrscheinlich) endgültig verabschiedet? Microsoft freut sich sicher auch dann noch über mehr Nutzer für Windows 10. Aber selbst beim Schwenk auf macOS, Chrome OS oder gar Linux kann sich der Konzern entspannt zurücklehnen – denn für seine Dienste muss der Anwender in jedem Fall bezahlen.

MORITZ FÖRSTER



MARKT + TREND

Virtualisierung

VMworld USA 2018 8

Digital Marketing

DMEXCO 18 9

High-Performance Computing

30. Hot Chips 2018 10

Personalmanagement

Zukunft Personal Europe:
Permanent Talent-Scouting 12

Programmierung

Java: Schnellere Releases,
kürzerer Support 14

COVER
THEMA

Embedded Computing

3D-Metalldruck für
die Serienproduktion 16

Systemmanagement

CNCF übernimmt Kubernetes 18

Sicherheit

Five-Eyes-Staaten fordern
Hintertüren 24

Cloud

Microsoft stellt Cloud
Deutschland ein 26

Office

Microsoft integriert Office-Apps 27

Mobile Computing

Apple präsentiert neue iPhones 29

Beruf

Mobile Erreichbarkeit belastet
die Psyche 33

Wirtschaft

Servermarkt gedeiht gut –
Dell vor HPE 34

Buchmarkt

Python 38

TITEL

Cloud-Computing

Cloud-Server als Virtual Private
Server oder Bare-Metal-System 40

COVER
THEMA

REVIEW

Microsoft

Windows Server 2019 und
Exchange Server 2019 52

COVER
THEMA

Firewall

Marktübersicht
Open-Source-Firewalls 56

COVER
THEMA

Administration

iOS und macOS mit dem
Apple Business Manager verwalten 64

COVER
THEMA

REPORT

Internet of Things

IoT-Cloud-Dienste von Microsoft,
Amazon und Google 76

COVER
THEMA

Awareness

Red Teaming:
Eindringen in der wirklichen Welt 80

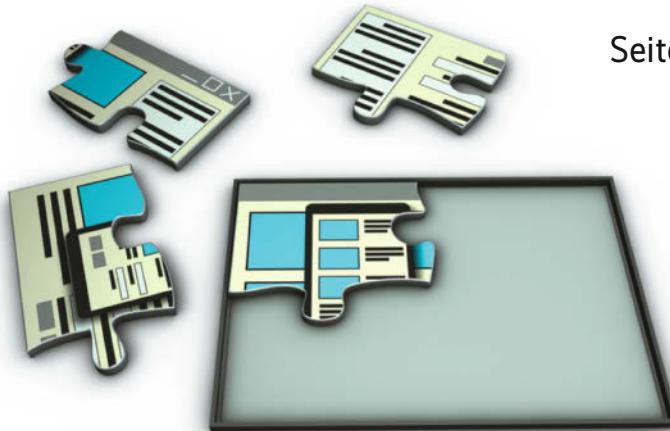
COVER
THEMA

Architekturen

Virtualisierung via CaaS und PaaS 83

Neues Tutorial: Progressive Web Apps

Progressive Web Apps sind Webanwendungen, die sich wie native Programme anfühlen. Unser neues Tutorial zeigt, wie man diese mit Googles Workbox-Library programmiert.



Seite 116

Windows Server 2019 und Exchange Server 2019



Ein erster Blick auf die Release Candidates der 2019er-Versionen von Windows Server und Exchange zeigte, dass die Änderungen vor allem für den RZ-Betrieb relevant sind. Details ab

Seite 52

Foreshadow-Angriffe auf VMware

Meltdown, Spectre und kein Ende:
Die neueste Speculative-Prediction-Lücke Foreshadow trifft vor allem Rechenzentren, die mit Virtualisierung arbeiten.

Seite 98



Cloud-Server on demand

Es müssen nicht immer die billigen und oft überbuchten virtuellen Server (VPS) sein. Bare-Metal-Server lassen sich heute fast genauso schnell in Betrieb nehmen und sind kaum teurer. Ein vergleichender Blick auf die aktuellen Angebote ab

Seite 40

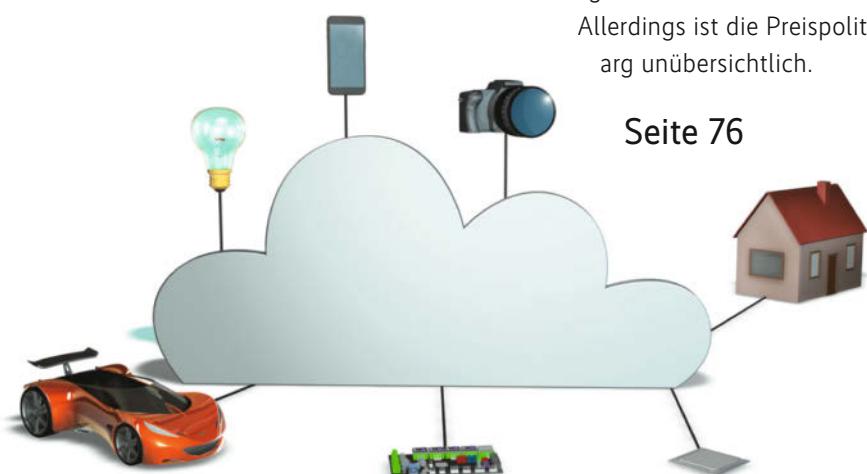


IoT-Dienste von Amazon, Google und Microsoft

Die Frage „Make or buy?“ stellt sich auch beim Entwurf von IoT-Systemen. Für die Antwort „Buy“ spricht, dass sowohl Amazon als auch Google und Microsoft fertige Module dafür anbieten.

Allerdings ist die Preispolitik arg unübersichtlich.

Seite 76



IT-Security

Vorüberlegungen zum Betrieb eines Security Operations Center

86

Projektmanagement

Nichtfunktionale Anforderungen in der agilen Welt

COVER
THEMA

90

Recht

Künstliche Intelligenz im Datenschutzfokus

92

Computergrafik

SIGGRAPH 2018: Die Zukunft digitaler Welten

96

WISSEN

Virtualisierung

Foreshadow in VMware-Umgebungen

COVER
THEMA

98

Cloud-Security

OpenStack absichern

100

Newsletterversand

Kurz erklärt: One-Click Unsubscribe

COVER
THEMA

104

PRAXIS

Webentwicklung

Progressive Web Apps mit Workbox

COVER
THEMA

116

App-Entwicklung

Firebase als Backend-Dienst für Apps

120

Machine Learning

Deep-Learning-Modelle deployen mit TensorFlow Serving

126

Desktop-Programmierung

Oberflächen mit Python und dem Framework Qt5 erstellen

130

Cloud-Monitoring

Prometheus-Tutorial, Teil 3: Skalieren und effektiv einsetzen

138

Tools & Tipps

URL-Shortener im internen Einsatz

144

MEDIEN

App-Infos

Tastaturen für jeden Zweck

146

Vor 10 Jahren

Gutes von Google

147

Rezensionen

Hacking & Security, Google Data Studio, Bildverarbeitung

148

RUBRIKEN

Editorial

3

Leserbriefe

6

Verlagsveröffentlichung

it-sa-Guide

COVER
THEMA

69

iX extra Security nach Seite

COVER
THEMA

104

Stellenmarkt

150

Inserentenverzeichnis

153

Impressum

153

Vorschau

154

Früher war alles besser!



Willkommen in der Welt der Classic Games, wo Computer- und Videospiele viel Kreativität und Spielspaß versprachen – und bis heute halten.

Wir stellen Spiele, deren Entwickler und Plattformen vor. Bei Retro Gamer finden Sie Screenshots, Fakten, Tipps und mehr zu den Hits von damals.



Testen Sie 2x Retro Gamer mit 30 % Rabatt!

Lesen Sie 2 Ausgaben für nur 18,- Euro* statt 25,80 Euro* im Handel.

Jetzt bestellen und vom Test-Angebot profitieren:
www.emedia.de/rg-mini

Telefon: (0541) 800 09 126
(Werktag von 8-20 Uhr, samstags von 10-16 Uhr),
E-Mail: rg-abo@emedia.de
eMedia Leserservice,
Postfach 24 69, 49014 Osnabrück

*Preis in Deutschland.

Leider mit Lücken

(Tools & Tipps: Synchronisation von Dateien; iX 8/2018, S. 109)

Der Artikel ist ja ganz nett, aber Wichtiges fehlt, was im Umgang mit *rsync* nicht Geübte ins Stolpern bringen könnte.

Zuerst ist zu sagen, dass aktuelle *rsync*-Implementierungen SSH als Default-Protokoll verwenden. Tut ihr *rsync* das nicht, ist es alt oder der/die Paket-maintainer/-in hat seine/ihr Arbeit nicht richtig gemacht. Die Option *-e* sollte man also hoffentlich nie verwenden müssen.

Die Aussage, dass mit einem *rsync --ignore-existing* Quelle und Ziel synchronisiert würden, ist in dieser allgemeinen Form nicht ganz korrekt. Zwar wären danach zielseitig alle Dokumente vorhanden, aber a) wären sie nicht gezwungenermaßen auf dem gleichen Stand (geänderte, bereits existierende Dokumente würden nicht transferiert) und b) würden Dokumente, die seit dem letzten Update quellseitig gelöscht worden sind, zielseitig nicht ebenfalls gelöscht. Ja, der Artikel relativiert im Nebensatz die Aussage, aber hängen bleibt erst mal „[...] würde Quelle und Ziel synchronisieren [...]“.

rsync ist eines der Tools, die ich am meisten schätze. Ich mache bei uns im Betrieb mehrmals täglich inkrementelle Snapshots wichtiger Filesysteme über *rsync*-Server inkl. automatischem Aufräumen älterer Kopien etc. Das alles, ohne irgendein spezielles Backup-Tool verwenden zu müssen.

FRANK THOMMEN, VIA E-MAIL

Der direkte Draht zu



Direktwahl zur Redaktion: 0511 5352-387

Bitte entnehmen Sie die E-Mail-Adressen dem Impressum. Diese haben die Form [Redakteurskürzel]@ix.de.

Redaktion iX | Postfach 61 04 07
30604 Hannover | Fax: 0511 5352-361
E-Mail: post@ix.de | Web: www.ix.de
 www.facebook.com/ix.magazin
 twitter.com/ixmagazin (News)
twitter.com/ix (Sonstiges)

Sämtliche in iX seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich: ftp.heise.de/pub/ix/



Bei Artikeln mit diesem Hinweis können Sie diese URL im Webbrowser aufrufen, um eine klickbare Liste aller URLs zu bekommen.

Unbewiesene Behauptung

(Tools & Tipps: Synchronisation von Dateien; iX 8/2018, S. 109)

Im Artikel „Gleichverteiler“ schreibt der Autor, dass einer der Vorteile von *rsync* sei, dass es Dateien effizienter löschen könne als *rm*. Als Beispiel wird „*rm ***“ in einem Verzeichnis mit hunderttausend Dateien aufgeführt. Wer das tut, hat IM-HO UNIX nicht verstanden, denn „**“ wird ja in eine Liste von Dateinamen expandiert, bevor das *rm*-Kommando überhaupt aufgerufen wird. Auch „*find . -type f -exec rm {} \;*“ ist ineffizient, weil für jede Datei ein „*rm*-Prozess“ gestartet wird.

Keine Magie ist „*find . -type f -print0 / xargs -0 rm*“ –, was in jedem GNU-basierten System laufen sollte und auch mit den Dateinamen klarkommt, die Leerzeichen enthalten. Warum *rsync* schneller als die Alternativen sein soll, führt der Autor allenfalls als Behauptung auf; es fehlen stichhaltige Daten und Testverfahren.

Interessant wäre die Antwort auf die Frage, um wie viel *rsync* schneller löscht als das folgende Perl-Konstrukt:

```
opendir DIR, $dir or die "open directory $dir failed: $!\n";
foreach my $entry (grep /\.+\..*/s, $dir) {
    readdir DIR; # löscht alle "\.txt" in $dir
    unlink("$dir/$entry");
}
closedir DIR;
```

ULRICH WINDL, VIA E-MAIL

BIMI DSGVO-konform?

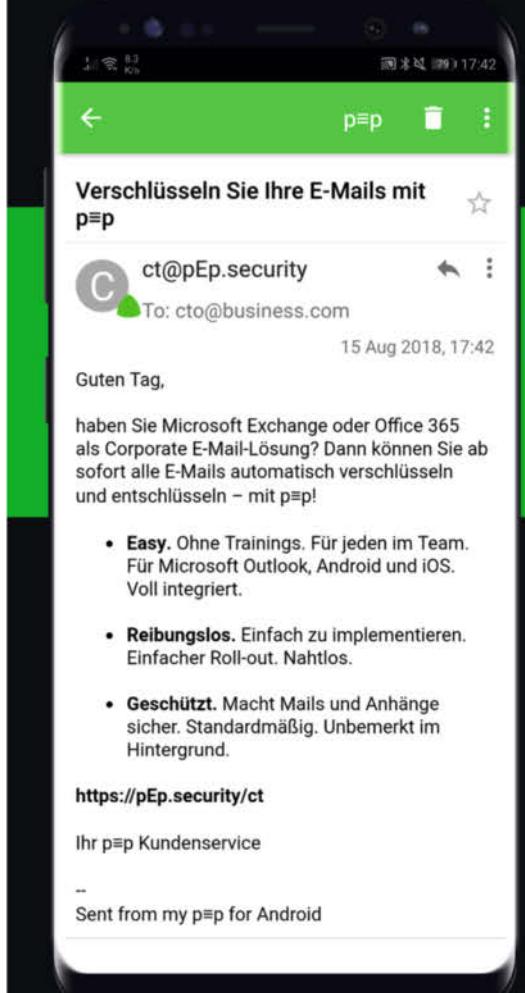
(Kurz erklärt: Brand Indicators for Message Identification; iX 9/2018, S. 117)

Verstehe ich das richtig, dass ein Logo von einem Server heruntergeladen werden soll und dieses dann im Mailclient dargestellt wird? Das hieße, dass auf Serverseite eine Menge IP-Nummern anfallen von den Clients. Und es wäre interessant, das aus Sicht der DSGVO oder ePrivacy zu bewerten. ;-)

HENNING BUSE, VIA E-MAIL

Es kommt auf die Implementierung an. Der Standardentwurf sieht einen BIMI-Location Mailheader vor, der auf das Logo verweist. Dieser Header darf explizit vom empfangenden MTA geändert werden. Ein auf Datenschutz Wert legender Mailbox-Provider könnte hier auf eine eigene Kopie des Logos verweisen. Er würde also de facto einen Proxy zwischen dem Logohost und dem Mailclient des Nutzers aufsetzen oder sogar eine data://URL nutzen. So könnte selbst im Offline-

Für Handy. Pad. Outlook.



Automatisch.
Nachvollziehbar.
Sicher.

Mit pEp.

ct@pEp.security
pEp.security/ct

privacy by default.

betrieb das Logo angezeigt werden. Das Logo müsste vom Mailanbieter nur ein einziges Mal für alle Kunden abgeholt werden. Der Versender erfährt nur wie bisher, dass eine Mail zugestellt wurde, der Mailanbieter nur, wann eine Mail von welcher IP aus abgeholt wurde.

Wie Yahoo dies implementiert hat, ist bisher nicht bekannt. In Zukunft wird man hier vermutlich die verschiedenen Ansätze der Mailbox-Provider vergleichen können. (Sven Krohlas)

Wozu Devuan?

(Linux-Distribution: Devuan GNU+Linux „ASCII“ Version 2.0; iX 8/2018, S. 60)

Ganz ehrlich: Wenn ich ein grafisches Linux möchte, dann lade ich mir eine angenehme Geschmacksrichtung von Ubuntu runter, installiere das Ganze und das Thema ist gegessen. Auf einem Desktop ist es mir gleich, was für ein Init-System da werkelt. Ich versuche ja auch nicht, OS X den Launchd abzugehören.

Auf einem Server will ich die Kontrolle und Nachvollziehbarkeit von Aktionen, die SysV-Init bietet. Da ist mir die Bootzeit wiederum ziemlich egal. Ich habe beim Upgrade meiner Deb7-Installation auf Deb8 per Apt-Pinning die Installation von Systemd unterbunden. Inzwischen laufen diese Server unter Deb9.

Wofür brauche ich gleich noch mal Devuan?

PATRICK SCHINDLER, VIA E-MAIL

Obskures WordPress

(Datenschutz-Grundverordnung: WordPress und die DSGVO; iX 9/2018, S. 52)

Der neue WordPress-Editor Gutenberg, der mit WordPress 5.0 ausgerollt werden soll und derzeit als Plug-in zur Verfügung steht, bindet ohne jegliche Hinweise in die Editor-Seite bei jedem Aufruf einen Google-Webfont ein. Das könnte noch ein großer Fallstrick für Seiten werden, bei denen sich Benutzer registrieren und anmelden können.

Das WordPress-Tool zum Exportieren und Löschen personenbezogener Daten erfasst nur hardgedecodet die Standardbenutzerprofilfelder. Die bei vielen Themes und Plug-ins extra angelegten Felder im Profil werden nicht berücksichtigt.

Weiterhin setzt das Tool die E-Mail-Adresse (!) des Benutzers praktisch im Klartext in den Dateinamen des Downloads zum Export und verrät diese so allen

Unbeteiligten in Form von Access.log, Proxy-Log, Browser-History, lokalem Dateisystem bis hin zu Cloud-Backups.

Die „Über WordPress“-Seite bindet Grafiken von externen Servern ein, ebenso der neue Hinweis im Dashboard, man möge Gutenberg testen. Beides sendet die IP und erlaubt theoretisch ein Benutzer-tracking. Irgendein Hinweis darauf: Fehlanzeige.

Ein Impressum und eine saubere Datenschutzerklärung bzgl. was WordPress wie und wo speichert und was an zentrale Server übertragen wird, fehlt auf de.wordpress.org – als verantwortlich ist nirgends irgendeine Person oder Anschrift angegeben, man versteckt sich hinter einem Textblock mit obskur E-Mail auf der Seite de.wordpress.org/about/privacy/: „Bitte nimm Kontakt zu uns auf, ... indem du eine E-Mail an dpo@wordcamp.org schreibst.“ Wenn man das in deutschen WP-Gruppen anspricht, bekommt man nur „das ist Sache der WP Foundation“ als Antwort. Alles sehr obskur.

O. ERKS, VIA E-MAIL

Herr Erks hat recht: Für die Google-Fonts im Gutenberg Editor sollte es auf jeden Fall eine Deaktivierungsmöglichkeit geben. Die eingebundenen Drittgrafiken sind wirklich unnötig, und die Benennung der Download-Dateien wurde wohl mit recht heißen Nadeln gestrickt.

Von Plug-ins hinzugefügte Profilfelder sollen in einer zukünftigen Version des Exporters berücksichtigt werden, ein Datum gibt es dazu allerdings noch nicht. (Ritchie Pettauer)

Ergänzungen und Berichtigungen

Datenschutz: Wie DSGVO-konform ist die Azure-Cloud von T-Systems? iX 9/2018, S. 82

Mittlerweile ist dieses Angebot von Microsoft und T-Systems eingestellt worden (siehe Seite 26, „Microsoft stellt Cloud Deutschland ein“).

Eine Diskussion des Artikels mit über 200 Beiträgen ist über diese URL zu finden: ix.de/ix1810006.

[Alle Links: ix.de/ix1810006](#)

Die iX-Redaktion behält sich Kürzungen und auszugsweise Wiedergabe der Leserbriefe vor. Die abgedruckten Zuschriften geben ausschließlich die Meinung des Ein-senders wieder, nicht die der Redaktion.

VMworld USA 2018

Klarer Fokus

Jens-Henrik Söldner, Torsten Volk

Vor allem große Unternehmen kamen auf der diesjährigen VMworld auf ihre Kosten, denn VMware konzentriert sich auf die Themen Multi-Cloud, DevOps und IoT.

Seit seiner Gründung vor 20 Jahren hat VMware sein Produktpotfolio stark ausgedehnt. Virtualisierung spielt nach wie vor als Basistechnik eine Rolle, im Vordergrund stehen aber zunehmend DevOps-Themen, Container und Cloud-Management. Das zeigte sich auch auf der VMworld 2018 in Las Vegas, auf der der Hersteller vom 26. bis 30. August vor 21 000 Teilnehmern seine Neuheiten vorstellte. Adressaten der Neuankündigungen waren weniger kleinere und mittlere Unternehmen, sondern in erster Linie Großkunden.

DevOps und Cloud automatisiert

Cloud, Container, Virtualisierung und DevOps wollen alle großen Anbieter unter einen Hut bringen. VMware setzt hierfür nach wie vor auf vRealize Automation als zentrale

Managementplattform, sofern es um mehr als virtuelle Maschinen geht. Allerdings gehen die Einführung und der Betrieb von vRealize Automation mit einem hohen Anpassungsaufwand einher und sind bislang nicht optimal auf DevOps-Szenarien abgestimmt. Zudem hat sich die Cloud-Landschaft seit der Einführung 2012 deutlich verändert – Multi-Cloud und Container spielen heute eine wichtige Rolle.

Richten sollen es die neuen Cloud Automation Services inklusive Cloud Assembly, Service Broker und des schon länger verfügbaren Code Stream. Mit ihnen lässt sich die Infrastruktur als Code definieren – Nutzer können einen grafischen Editor verwenden oder im YAML-Format arbeiten. Der Service Broker stellt das zentrale Selbstbedienungsportal für die SaaS-Dienste dar, mit ihm können Administratoren den Cloud-Konsum der Entwickler überprüfen und die Sicherheit

über Rollendefinitionen gewährleisten. Für Endnutzer stehen hier mehrere Clouds in einer Oberfläche bereit. Code Stream wendet sich an Entwickler und DevOps-Administratoren. Mit dem Dienst können sie eine CI/CD-Pipeline (Continuous Integration / Continuous Delivery) aufbauen, die Softwareentwicklungsprozesse beschleunigen soll.

Kunden müssen aber nicht auf SaaS-Dienste migrieren, denn seine On-Premises-Automatisierungsplattform vRealize Automation überarbeitet VMware in der kommenden Version 7.5 technisch und optisch. Unter anderem integriert die Software nun ServiceNow, umfasst NSX-T für die Netzwerkvirtualisierung und bietet Erweiterungen für Azure. Allerdings schlafst die Konkurrenz nicht: Start-ups wie Morpheus Data nutzen VMwares längere Passivität beim Cloud-Management und DevOps, um Kunden vom in die Jahre gekommenen vRealize Automation abzuziehen.

Mit den Neuerungen rund um die vSphere-Produktfamilie zeigte VMware, dass es seine Stammkunden nicht völlig vergisst. Zunächst erhält vSphere das Update 1, das wichtige und dringend benötigte Funktionen nachlieferst. Es soll bis Ende 2018 bereitstehen und den HTML5-basierten Client endlich abrunden. Künftig soll er alle Funktionen beinhalten, von denen einige noch dem alten Flash-Client vorbehalten sind. Auch ein Update von vSphere 6.5 Update 2 auf 6.7

ist vorgesehen – momentan stecken Nutzer der Version in einer Sackgasse fest. Weitere Neuerungen im Update 1 umfassen eine verbesserte Unterstützung von NVIDIAS virtualisierungsfähigen vGPUs, deren VMs sich erstmals im laufenden Betrieb migrieren lassen sollen.

Ebenfalls neu ist vSphere Platinum – bislang lizenzierten Unternehmenskunden vSphere zumeist als Standard oder Enterprise Plus. Das neue Paket kombiniert letztere Version mit VMwares Cloud-Security-Dienst AppDefense. So sollen Administratoren das Verhalten ihrer VMs mit ML-Technik beobachten und beim Abweichen von der Norm umgehend reagieren können.

Mit ARM in die IoT-Zukunft

Überraschend kündigte VMware an, dass der ESXi-Hypervisor künftig auf 64-Bit-ARM-CPUs laufen soll. Ein konkretes Veröffentlichungsdatum hat der Hersteller allerdings nicht genannt. In der Keynote konnten die Anwesenden einen kurzen Blick auf eine Entwicklungsversion ESXi 6.8.2 werfen, die auf einem ARM Cortex-A72 mit vier Kernen lief. Das Beispiel stammte laut VMware aus dem IoT-Bereich, auf den die Portierung zielt. In Gesprächen mit iX auf der Konferenz meinte der Hersteller, dass er schon seit Jahren an der ARM-Version seines Hypervisors arbeite. Die Verwaltung von ESXi-on-ARM soll wie gehabt über vCenter erfolgen.

Große Aufmerksamkeit erregte ferner die gemeinsame Ankündigung von AWS und VMware, Amazons Relational Database Service (RDS) in VMware-Infrastrukturen bereitzustellen. Diese Version wird laut AWS CEO Andy Jassy mit den Datenbankdiensten Microsoft SQL Server, Oracle, MySQL, MariaDB und PostgreSQL funktionieren.

Weitere Neuerungen sollen auf VMwares europäischer Variante der VMworld zu sehen sein, die vom 5. bis 8. November in Barcelona tagt. Die nächste VMworld USA kehrt nach mehreren Jahren in Las Vegas 2019 nach San Francisco zurück. (fo@ix.de)



Quelle: VMworld

DMEXCO: Werber üben sich in Demut

Ambivalent

Achim Born

Die DMEXCO unter neuer Leitung funktioniert. Die Messe bestätigte ihren Ruf als Branchentreff, begleitet von ein wenig Selbstkritik.

Als die DMEXCO nach zwei Veranstaltungstagen die Tore schloss, war es wie immer: Ungeachtet der Unkenrufe meldete die Messegesellschaft neben den über 1000 Ausstellern aus 40 Ländern eine im Vergleich zum Vorjahr leicht gestiegene Fachbesucherzahl von rund 41 000, darunter 45 Prozent aus dem Ausland. Die Aussteller lobten in einer Umfrage explizit die Qualität der Kontakte. Selbst wer über einen geringeren Zulauf an seinem Stand mäkelte, stimmte dem zu.

Dass es neben dem üblichen Messe-Bashing im Vorfeld eine deutliche Verunsicherung in der Branche gab, war selbstver-

schuldet. Nach der abrupten Trennung von den bisherigen Machern (siehe Kasten „Juristisches Geplänkel“) sahen sich der Veranstalter Koelnmesse und der Branchenverband BVDW zu einem Neustart mit frischem Team und neu justierter Ausrichtung gezwungen. Die Gruppe um den Chief Advisor DMEXCO Dominik Matyka, Gründer der Content- und Werbeplattform plista, machte dabei vieles richtig oder sprach zumindest die richtigen Dinge an. Das Messeomotto „Take C.A.R.E“, das für „Curiosity, Action, Responsibility, Experience“ steht, klingt für eine chronisch aufgeregte Branche wie

die digitale Werbewirtschaft etwas betulich. Es lässt allerdings hoffen, dass etwas mehr Glaubwürdigkeit und Nachhaltigkeit im Umgang mit Nutzern und Konsumenten folgt.

Bereits auf dem OnlineAd Summit am Vortag übten sich die Werber in Demut. Berater Patrick von der Gönnia klage, dass mangelnde Sensibilität im Umgang mit Kundendaten zu dem Zustand geführt habe, den die DSGVO nun beseitigen soll. Angeblich hat die Grundverordnung ein Umdenken in der Branche bewirkt.

In der Realität arrangierte man sich nach der Anlaufphase jedoch mit der Gesetzgebung und beglückt die Besucher von Websites weiterhin mit Werbung. Mehr als die DSGVO fürchten die Werber die geplante ePrivacy-Verordnung, da der Entwurf vorsieht, keine Werbebanner Dritter zuzulassen. Vor und hinter den Kulissen mühen sich die Lobbyisten, der Richtlinie die Schärfe zu nehmen.

„Mehr Verantwortung“ war auch die Leitlinie der Eröffnungsrede von Tim Höttges (siehe Abbildung). Der Telekom-Chef gab sich ungewohnt gesellschaftskritisch und warnte, dass die hohe Geschwindigkeit der Digitalisierung die Gefahr berge, dass sich viele Nutzer abgehängt fühlen. Trotz der florierenden Wirtschaft sei eine Zunahme des Populismus in westlichen Gesellschaften zu beobachten. „Was zur Hölle ist los in unserer Gesellschaft?“, fragte Höttges mit Blick auf die übeln Ereignisse in Chemnitz und Köthen. Er mahnte eindringlich, dass Unternehmen ihrer



gesellschaftlichen Verantwortung nachkommen müssen. Gleichzeitig forderte er Offenheit für neue Techniken ein.

KI muss überall rein

Ambivalente Gefühle erzeugt derzeit die allerorten gehypte künstliche Intelligenz, die in ihren unterschiedlichen Ausprägungen bestimmendes Messe-thema war. Nach Ansicht der Staatsministerin für Digitales, Dorothee Bär, wird KI oft viel zu abstrakt diskutiert. Wenn man den Menschen konkrete Anwendungen zeigen würde, seien sie viel eher bereit, sich darauf einzulassen, meinte die Politikerin in einer Diskussionsrunde. Baidu-Manager Alex Cheng führte in seinem Vortrag am Beispiel der Open-Source-Plattform Baidu Apollo vor, wie KI bei der Gesichtserkennung hilft und das Einschlafen von Lastwagenfahrern während der Fahrt verhindert.

Ob Machine Learning, Chatbots und Co. tatsächlich dazu beitragen, Konsumenten achtsamer zu behandeln, muss die Werbebranche allerdings noch nachweisen. (jd@ix.de)

Juristisches Geplänkel

Die Kölner Messegesellschaft hatte sich im November überraschend von den bisherigen Machern der DMEXCO, Christian Muche und Frank Schneider, getrennt. Deren Firma organisiert auch die Schweizer Veranstaltung D-Pulse, worin man einen

Verstoß gegen das vertraglich vereinbarte Wettbewerbsverbot sah. Vor Gericht konnte die Messegesellschaft ihre Sichtweise bislang jedoch nicht durchsetzen, weshalb eine Millionen Euro schwere Entschädigungszahlung droht.

Kurz notiert



Selfapy gewann den **Start-up-Wettbewerb „SevenVentures Pitch Day“**. Mit der Therapiekurs-Plattform soll man sein Wohlbefinden im Falle von Stress, Schlafstörungen, Depressionen, Angstzuständen und Essstörungen verbessern können.

Laut der **BVDW-Studie „Business-Relevanz Künstlicher Intelligenz“** ordneten 78 Prozent der

Befragten KI als wichtig für ihr Geschäftsmodell ein. Allerdings ist nur jedes fünfte Unternehmen in der Lage, das Potenzial auszuschöpfen.

Searchmetrics erhielt eine neue Bedienoberfläche. Die Suite des gleichnamigen Anbieters, mit deren Hilfe sich Werbecontent bei Suchmaschinen weit oben platzieren lässt, beherrscht jetzt Sunburst-Charts und hierarchisches Keyword-Tagging.

Mit der **Social Share App von Facelift** befördern Unternehmen

ihre Mitarbeiter zu Werbebotschaftern. Sie sollen bereitgestellte Werbung in ihren privaten sozialen Netzwerken teilen.

MeasureMatch hat sich bei dem mit 15 000 Euro dotierten Wettbewerb **The DMEXCO & Unilever Foundry Start-up Hatch** durchgesetzt. Über die Plattform kann man Datenexperten für Marketingprojekte anheuern.

Dass die **klassische sexistische Werbung** immer noch zieht, zeigte Pornhub: In den Toilettenräumen waren Plakate mit Hotdog nebst

Slogan „THINK LONG TERM GROWTH“ (bei den Männern) und halbgeschälter Banane nebst „GET AHEAD OF THE CURVE“ (bei den Frauen) angebracht.

Ein Sprecher des **Pornhub-Vermarkters TrafficJunkie** lobte im offiziellen Schlussbericht die Qualität und Quantität der Kontakte. Für den unvoreingenommenen Beobachter wirkte es eher so, als ob die meisten Besucher „zufällig“ vorbeihuschten und nur einen verschämten Blick wagten.

Hot Chips 2018: Neue Prozessorkonzepte

Herausgefordert

Susanne Nolte

Selten wurde auf der Hot-Chips-Konferenz das Höher-schneller-weiter so eingehend hinterfragt wie in diesem Jahr – Spectre & Co. sei dank.

Neben den CPUs der aktuellen und nächsten Generationen standen auf der dreißigsten Hot Chips Conference, die Ende August im kalifornischen Cupertino stattfand, grundsätzliche Überlegungen zur Rechenhardware im Vordergrund. Denn die CPU-Bauer ringen um Antworten auf die Fragen, die Spectre, Meltdown und Foreshadow aufwerfen.

Passend dazu widmete sich die erste Keynote-Session diesem Thema. John Hennessy, Ex-Präsident der Stanford-Universität und Chairman of the Board bei Googles Alphabet, skizzierte die durch Spectre und Co. entstandene Situation. Side-Channel-Angriffe gibt es seit den 70ern, neu sei aber, dass sich die Lecks in der Hardware befinden. Spectre und Meltdown seien erst der Anfang. Mit Foreshadow/LITF sind zudem die durch Virtualisierung errichteten Speichergrenzen überwindbar. Das sei für Anbieter

und Kunden insofern besonders schmerhaft, als sich die Lücken derzeit nur – wenn überhaupt – sehr aufwendig per Software stopfen ließen, und das kostet Performance.

Bisher sei es die Aufgabe der Hardware gewesen, Fehler der Software auszubügeln. Dagegen sind Lücken in der Hardware nicht akzeptabel, gleich, wie viel mehr an Performance dadurch herausspringt, etwa bei der Spekulation, also dem prädiktiven Ausführen erwarteter Instruktionen. Derzeit kann das Abmildern oder Schließen der Lücken sogar mehr Performance kosten, als die ursächlichen Funktionen einbringen. Zudem ist absehbar, dass Intels nächste Prozessorgeneration nicht einmal gegen Spectre v1 gefeit ist.

Paul Turner von Googles Project Zero verwarf die bisher geltende Prämisse, dass falsche Spekulationen nicht nachverfolgbar seien und keine Neben-

wirkungen haben. „SpeckHammer“, so der interne Name der ersten Entdeckungen des Zero-Projekts, strafte genau das Lügen. Deshalb müsse die Hardware künftig in der Lage sein, die Begrenzungen, die in der Software existieren, etwa zwischen Speicherbereichen, zur Kenntnis zu nehmen und einzuhalten. Zudem hat das Projekt unter anderem einen neuen „Restricted-speculation“-Typ von Programmverzweigungen vorgeschlagen, bei denen die Software der CPU Spekulationen verbietet. Intel selbst hat in seinen Microcode-Patches einen Ausführungsmodus eingeführt, der Spekulationen einschränkt.

Zu wenig Kommunikation

Jon Masters von Red Hat beklagte, dass sich Hard- und Softwareentwickler zu wenig austauschen, dass es statt besserer Anpassungen mehr und mehr Softwarelayer gibt und die Programmentwicklung immer abstrakter wird – viele, selbst gute Programmierer wüssten nicht mehr, was ein Stack oder ein Branch sei. Noch weniger wüssten, was Befehlsumsortierungen, Spekulationen oder Speicherkonsistenzmodelle seien, während die Implementierungen immer komplexer würden. Zugleich werden die Optimierungen aber durch immer aggressivere Methoden erreicht und niemand fragt, wo-

durch die Performancegewinne zustande kommen.

Die Lücken zeigen aber nun, dass Soft- und Hardwareentwickler wieder enger zusammenarbeiten müssen. Red Hat etwa hat für den Umgang mit Mikroarchitekturlücken ein „Omega“-Team ins Leben gerufen und allein bis August 2018 über 10 000 Ingenieursstunden nur in Spectre und Meltdown gesteckt und Patches entwickelt, die die einzelnen Lücken von der Software- resp. Kernel-Seite abmildern. Nichtsdestotrotz müssen die Lücken in der Hardware geschlossen werden, die Sichtweise „Sicherheit vs. Performance“ muss sich grundlegend ändern, und jeder Softwareentwickler, der etwas auf sich hält, sollte mehr über Hardware wissen, so wie man von einem Profirennfahrer erwartet, dass er viel über sein Gefährt weiß. Hierbei bietet Open Source die besten Voraussetzungen.

Mark Hill, Computerarchitekt an der Universität Wisconsin und Google Sabbatical, betonte, dass die derzeitigen Lücken nicht durch Bugs zustande kommen, sondern durch eine Mikroarchitektur, die einer über 50 Jahre alten, da aus dem Jahr 1964 stammenden Architektur 1.0 entspreche. Da es aber nicht richtig sein kann, dass darin geschützte Daten durchsickern, gilt es, eine Architektur 2.0 zu definieren und die Methoden zu ändern.

Wie seine Vорredner sprach er sich aber nicht für das Abschaffen der für die Performance so wichtigen CPU-Spekulationen aus. Stattdessen unterbreitete er eine Reihe Vorschläge, wie im ersten Schritt die Mikroarchitektur zu verbessern sei. Unter anderem sollen bestimmte Bereiche in den CPUs isoliert, Caches für bestimmte Prozesse partitioniert und deren Inhalt bei Kontextwechsel geleert werden. Dabei sind Gabelungen denkbar. Eine zeitliche könnte sein, dass die CPU zwischen einem schnellen und einem sicheren Modus wechselt könne, wobei letzterer etwa das Einrichten von Partitionen und das Ausschalten bestimmter Spekulationen beinhaltet. Eine räumliche Gabelung könnte in der Entwicklung unterschiedlicher Cores, also schneller und sicherer Cores etwa mit Security-Exten-

IBMs neuer System-Interconnect PowerAXON

IBM präsentierte auf der Hot Chips seinen BlueLink-Nachfolger PowerAXON. Der neue Interconnect des neuen Power9-Chips arbeitet mit einem Takt von 25 GHz und niedriger Latenz und verbindet die CPU mit GPUs, anderen CPUs oder OpenCAPI-fähigen FPGA-Beschleunigern. Das Designziel: Ein Chip kann als großer SMP fungieren oder mit vielen GPUs oder einem Mix aus FPGAs und GPUs kommunizieren. Beim Power9+, der für 2019 erwartet wird, sollen die CPUs darüber auch auf den Speicher zugreifen. Dazu entwickelt IBM einen dritten Prozessortyp – die beiden bisherigen Power9-Varianten arbeiten mit direktem oder gepuffertem Speicherzugriff.

Dieser Typ 3 erfordert ein neues Speichersubsystem, dessen Durchsatz von 150 auf über 350 GByte/s steigen soll. Wie bereits in der Vergangenheit implementiert IBM damit Techniken der nächsten Generation in eine Plus-Zwischenvariante, was Big Blue

gute Testmöglichkeiten auf ausgereifter Hardware verschafft. Mit Power10 kommt dann der Umstieg auf DDR5, was den Durchsatz auf über 435 GByte/s erhöhen soll – im April war noch von bis zu 435 GByte/s die Rede. Damit hätte IBM wieder das Niveau von Power8 erreicht, dessen 32 Verbindungen zwischen dem L4-Cache auf dem Speichercontroller Centaur und dem proprietären DDR3- oder DDR4-Speicher bereits 410 GByte/s lieferten.

Da IBM mit Power9 aber auch Hyperscaler und Cloud-Provider wie Google gewinnen will, blieb nur der Schwenk auf Standard-DDR4-RAM, die Integration des DDR4-Controllers auf den Prozessorchip, das Verlagern der DMI-SERDES-Schaltungen und das Aus für die proprietären Centaur-Pufferchips. Dadurch kann eine CPU nur noch 16 Speicherriegel ansprechen – was vor allem den Durchsatz senkt.

Berthold Wesseler (sun@ix.de)

sions, bestehen. Eine Trennung in der Anwendung entsteht, wenn Cloud-Provider mehr exklusive Cores anbieten.

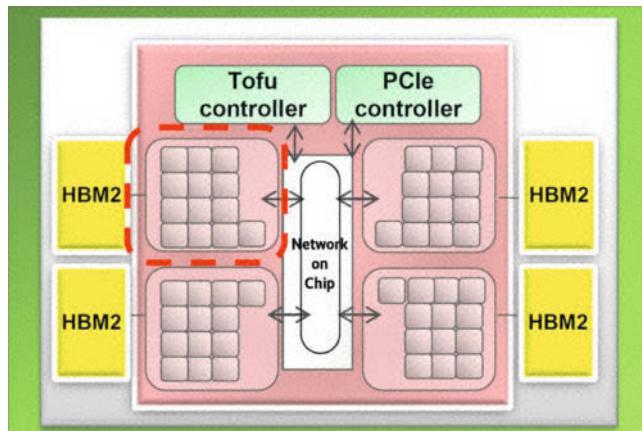
Eine Computerarchitektur 2.0, die den heutigen Anforderungen gerecht wird, könnte ein Konzept verteilter Prozessoren beinhalten, in heutigen Begriffen gedacht also aus CPUs, GPUs, DSPs (Digital Signal Processors), IPUs (Interconnect Processing Units) und TPUs (Tensor Processing Units) bestehen. Sie besäßen dedizierten Speicher und mehr ALUs (Arithmetic Logic Units) und verarbeiteten Datentypen mit geringerer Genauigkeit in einer domänenspezifischen Sprache bei einer wesentlich höheren Parallelisierung der unterschiedlichen Aufgaben. Prozessorskulationen wären dann nicht das Feature der ersten Wahl. Hill erwartet, dass viele Security-Ideen zuerst an Open-Source-Hardware wie dem RISC V ausprobiert werden.

Aufmerksamkeit zogen die Details zu Fujitsus erster ARM-CPU A64FX auf sich, die Japan

und vielleicht auch Europa ins Exascale-Zeitalter schleudern soll. Der in 7-nm-Technik gefertigte Prozessor ist der erste mit ARMv8-A SVEs (Scalable Vector Extensions), 512-Bit-Vektoreinheiten, die seine Verarbeitung von Vektorrechnungen beschleunigen. Mit zwei SVEs in jedem seiner 48 Kerne soll er eine Peak-Performance von über 2,7 TFlops erreichen.

Jeder A64FX besteht aus 8,7 Milliarden Transistoren und setzt sich aus vier Core Memory Groups (CMG) mit jeweils 13 identischen CPU-Kernen zusammen – 12 zum Rechnen und einer für I/O und Verwaltung. Jede CMG hat eine 256-GByte/s-Anbindung an 8 GByte HBM2 (High Bandwidth Memory 2). Das ergibt 32 GByte HBM2 mit 1 TByte pro Sekunde und Prozessor.

Ein NoC (Network-on-Chip) verbindet die vier CMGs miteinander und mit zwei I/O-Einheiten: Die eine versorgt die 16 PCIe-3.0-Lanes, die andere den Tofu-3-Interconnect, der die Sockel und die Rechenknoten



Die 48 Rechenkerne des A64FX unterteilen sich in vier Core Memory Groups mit je eigenem High Bandwidth Memory 2.

verbindet. Das NoC überträgt mehr als 115 GByte/s duplex. Das Torus Fusion oder Tofu 6D Mesh/Torus Network, nun in der dritten Generation Tofu D genannt, schafft 28 GBit/s pro Lane, implementiert sind 10 Ports mit je zwei Lanes.

Neues hatte Nantero über sein NRAM (Nano-RAM) zu berichten, dessen Speicherzel len aus Kohlenstoff-Nanoröhrchen oder CNTs (Carbon Nano Tubes) bestehen. Das Start-up hat nun DDR-kompatible Chips mit dem nichtflüchtigen Spei-

cher entworfen, der dieselbe Schaltgeschwindigkeit aufweist wie DRAM. Bisher hatte nur Fujitsu NRAM für den Einsatz in einem Serverprozessor lizenziert, der Ende 2018 erhältlich sein soll. Die im 28-nm-Prozess gefertigten, etwa 100 mm² großen Dice fassen 8 GBit auf zwei oder 16 GBit auf vier Lagen und lassen sich auf Speicherriegel für DDR4-Slots packen. Da die Zellen keine Refreshes benötigen, soll zudem der Durchsatz um bis zu 15 % steigen. (sun@ix.de)



Revolutionieren Sie Ihre IT-Infrastruktur!

Moderne Virtualisierung heißtt: hochskalierbare, ausfallsichere Microservice-Umgebungen. Mit unseren Büchern holen Sie sich das Wissen der IT-Experten in greifbare Nähe – zum Lernen und Nachschlagen. Damit Ihre IT-Landschaft auch in Zukunft planungssicher ist.

-Veranstaltungen

Die diesjährige **iX Cloud-Konferenz 2018** deckt in einem Technik- und in einem parallelen Strategie-Track das gesamte Spektrum aktueller Fragen rund um Cloud-Computing ab, von Automatisierung über Kubernetes bis Legacy-Software (10. Oktober 2018, Berlin, Ellington-Hotel).

Vertiefen kann man sein Cloud-Know-how durch die Teilnahme an einem der zweitägigen Workshops direkt nach der Konferenz. Angeboten werden **Kubernetes und Container für Fortgeschrittenes, Amazon Web Services vs. Microsoft Azure und System-deployment & -management mit Ansible** (11.-12. Oktober 2018, Berlin, Rocket Tower). Bei Redaktionsschluss waren nur noch wenige Plätze frei, der Stand der Dinge ist auf der Konferenz-Site nachzulesen, erreichbar über www.ix-konferenz.de.

Im letzten Jahr ausgebucht war die **heise devSec()**, eine Konferenz für sichere Software- und Webentwicklung. In den ganztägigen Workshops am Dienstag, 16. Oktober, ist kein Platz mehr frei, man kann sich aber in eine Warteliste eintragen. Am Mittwoch und Donnerstag gibt es dann in drei parallelen Tracks Vorträge zu Themen von A wie „Agil, aber sicher“ bis T wie „TCB-Minimierung, eine verlorene Kunst“ (16.-18. Oktober 2018, Heidelberg, PMA).

Frühbucherrabatte für Workshops

Bei einer Buchung bis zum 7. Oktober rund 10 Prozent der Teilnehmergebühren sparen kann man für den Workshop **Kerberos – LDAP – Active Directory: Single Sign-on in gemischten Linux- und Windows-Umgebungen**. Referent ist Mark Proehl (Puzzle ITC GmbH), Autor des ersten deutschsprachigen Kerberos-Buches, der dieses Seminar mit immer wieder aktualisierten Inhalten seit 10 Jahren abhält (19.-21. November 2018, Nürnberg).

Bis zum 9. Oktober läuft die Frühbucherfrist für **vSphere – What's new: dreitägiger Workshop zur sechsten Hypervisor**

Generation. Der Referent, Prof. Dr. Jens-Henrik Söldner, ist VMware Mentor Instructor, Gründer der Söldner Consult GmbH und Professor für IT-Sicherheit an der Hochschule Ansbach – University of Applied Sciences (20.-22. November 2018, Hannover).

Bis zum 10. Oktober gilt der Early-Bird-Rabatt für **Python für Linux-Admins: Python 3.x im Einsatz**. Den Referenten stellt die B1 Systems GmbH (22.-23. November 2018, Nürnberg).



Keynote auf der Cloud-Konferenz: Kurt Garloff, Chef-Architekt Open Telekom Cloud, zum Thema „Wie man Spectre et al. besiegt“.

Beim **Powerkurs vSphere-Administration: Mit GUI und Command Line vSphere 6.5, 6.0 und 5.x verwalten** läuft diese Frist bis zum 14. Oktober. Den Kurs hält Stefan Wacker, Senior Consultant bei der Söldner Consult GmbH (26.-30. November 2018, Hannover).

Der 22. Oktober ist der letzte „Spartag“ für den Workshop **Programme bauen mit Jenkins: Einstieg in die Continuous Integration**. Auch hier stellt den Referenten die B1 Systems GmbH (4.-5. Dezember 2018, Nürnberg).

Bei einer Buchung bis zum 24. Oktober kommt man in den Genuss reduzierter Teilnehmergebühren für den Workshop **SLES in zwei Tagen: Neue Features in SUSE Linux Enterprise Server 15**. Referent: B1 Systems GmbH (6.-7. Dezember 2018, Hannover). (js@ix.de)

www.ix-konferenz.de

Zukunft Personal Europe: Permanent Beta

Talent-Scouting

Achim Born

Auch das Personalmanagement kommt um Bots, KI und Big Data nicht herum. Solche Technik soll den perfekten Mitarbeiter ausspucken.

Bullshit-Bingo funktioniert auch bei Themen rund ums Personal. Auf der Fachmesse „Zukunft Personal Europe“ bombardierten die Redner und das Standpersonal den Besucher regelrecht mit den einschlägigen Begriffen. Fairerweise muss man ihnen zubilligen, dass das Personalwesen eine maßgebliche Rolle spielt, wenn sich ein Unternehmen in die digitale Transformation stürzt. Bei der Adaption neuer Bedingungen und Techniken, etwas Robotik und KI, befindet sich die Arbeitswelt nach Ansicht der Messemacher in einem permanenten Bestatus.

Auf der dreitägigen Veranstaltung in Köln führten gut 770 Aussteller (darunter über 100 Start-ups) und mehr als 450 Referenten den über 18 000 Besuchern vor, mit welchen Produkten und Methoden man das Personalmanagement künftig beglücken will.

Welche technischen Optionen einfließen, zeigten insbesondere die Gewinner der HR Innovation Awards. Die SSZ Beratung heimste mit ihrem Big-Data-Analyse-Tool den Preis in der Kategorie „HR Software & Hardware (Grown-up)“ ein. Das Werkzeug soll etwa Zusammenhänge zwischen Mitarbeiter- und Kundenzufriedenheit sowie Personalbedarf



John Stepper will die digitale Zusammenarbeit verbessern.

zeigen. In der Kategorie „HR Software & Hardware (Start-up)“ hat HR:Forecast gewonnen. Mittels ML- und Data-Mining-Techniken berechnet das Unternehmen den künftigen Personalbedarf.

Dass Chatbots in diesem Sektor ebenfalls an Bedeutung gewinnen, zeigte jobpal, Preisträger des Awards für Recruiting & Attraction. Das Start-up entwickelt eine Plattform, mit der Firmen Recruiting-Bots erstellen können, die Personalern bei der Vorauswahl von Talenten helfen. Eine Art Secondlife-Déjà-vu stellte sich bei der WBS Akademie ein. Der Gewinner in der Kategorie „Training & Learning (Grown-up)“ betreibt mit dem WBS Learn-Space 3D eine Virtual-Reality-Plattform zur ortsunabhängigen Schulung. Dabei sollen sich Avatare mit dem Dozenten austauschen.

Bessere Kooperation gewünscht

Neben der Digitalisierung waren die Themen Arbeitskräfte-mangel und Bindung junger Mitarbeiter allgegenwärtig. Im Ausstellungsbereich „Future of Work Village“ gab es dazu attraktive Raum- und Technik-konzepte zu sehen. Sie sollen innovative Formen der Zusammenarbeit befördern und so die anspruchsvollen Generationen Y und Z zufriedenstellen. Das methodische Rüstzeug lieferte zum Auftakt John Stepper, Erfinder des derzeit gehypten WOL (Working Out Loud). Im Prinzip geht es um einen Weg, nach dem Community-Vorbild sozialer Netze unternehmensübergreifend und hierarchiefrei Wissen zu teilen (workingoutloud.de). (jd@ix.de)

MACH, WAS WIRKLICH ZÄHLT.



#ADMIN

FOLGE DEINER BERUFUNG.

bundeswehr
karriere.de



Bundeswehr

© Copyright by Heise Medien

Java: Schnellere Releases, kürzerer Support

Komplett-sanierung

Hendrik Ebbers, Timo Brandstätter

Oracle hat angekündigt, den Java-Releasezyklus und das dazugehörige Supportmodell in diesem Jahr vollständig zu überarbeiten. Müssen Anwender künftig zahlen?

Bis Java 8 gewährte Oracle für jede Version verhältnismäßig lange Support. Updates pflegte der Anbieter sogar über die Freigabe der nachfolgenden Version hinaus. Entwickler standen dadurch nur begrenzt unter Druck, zu einer neuen Version zu wechseln. Entsprechend großzügig gestaltete sich die Planung von Updates. Das dürfte sich künftig ändern.

Die Dauer, während derer kostenloser Support für eine Java-Version respektive paral-

lief für zwei Versionen zur Verfügung stand, verschaffte Unternehmen meist genügend Zeit, zur nächsten Version zu migrieren, ohne auf kommerziellen Support zurückgreifen zu müssen. In allen längerfristigen Projekten konnten sie die restliche Zeit durch dessen Zukauf überbrücken.

Ab Java 9 erhalten die meisten Versionen nur noch ein halbes Jahr Support. Nach sechs Monaten folgt die Anschlussversion, die ihrerseits wieder nur ein halbes Jahr zur Verfü-

gung steht. Die bisher übliche Übergangszeit entfällt. Selbst wenn ein Unternehmen einen Vertrag mit Oracle abschließt, bleibt der auf die sechsmonatige Laufzeit der Version begrenzt.

Oracle verabschiedet sich vom bisherigen Modell zugunsten von „Long-Term-Support“-Versionen (LTS), für die jeweils acht Jahre kostenpflichtige Unterstützung verfügbar ist. Unternehmen dürfen sie erst nach Abschluss eines Vertrags nutzen. Viele Anwender, die bisher ohne ausgekommen sind, dürfte diese Neuerung unter Druck setzen.

Verschärfend kommen wichtige Änderungen hinzu, die den Einsatz des Oracle JDK oder des JRE in Produktion betreffen: Ab Java 11 darf man beide nur noch in Entwicklungs- und Testumgebungen kostenfrei nutzen. Zwingende Voraussetzung für den Einsatz der JRE in Produktion ist der Abschluss eines kommerziellen Supportvertrags bei Oracle. OpenJDK steht weiterhin kostenlos bereit und lässt sich grundsätzlich auch in Produktion frei nutzen.

Die Frage, warum Oracle den Releasezyklus und das Li-

Java SE Subscription

Anzahl Prozessoren	monatl. Preis
1 bis 99	25,00 \$
100 bis 249	23,75 \$
250 bis 499	22,50 \$
500 bis 999	20,00 \$
1000 bis 2999	17,50 \$
3000 bis 9 999	15,00 \$
10 000 bis 19 999	12,50 \$
Ab 20 000 Prozessoren ist ein individueller Vertrag mit Oracle erforderlich.	

Java SE Desktop Subscription

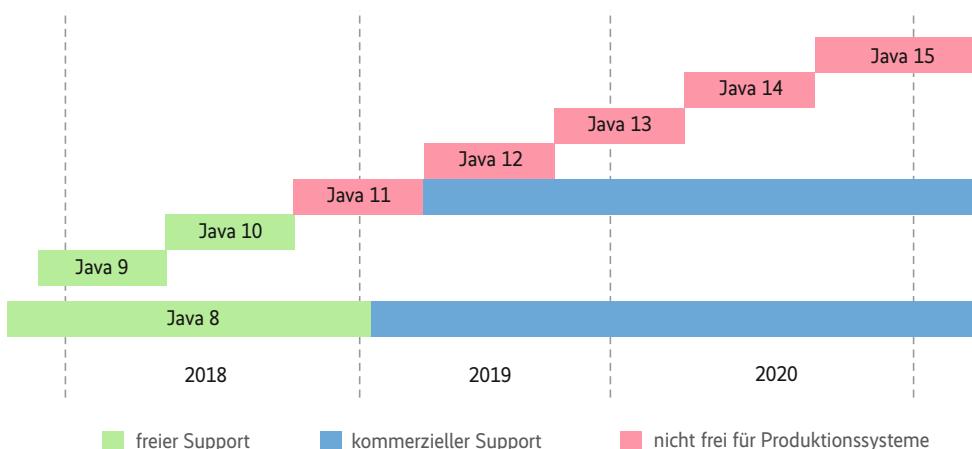
Clients	monatl. Preis pro Benutzer
1 bis 999	2,50 \$
1000 bis 2999	2,00 \$
3000 bis 9999	1,75 \$
10 000 bis 19 999	1,50 \$
20 000 bis 49 999	1,25 \$
Ab 50 000 Benutzer/Clients ist ein individueller Vertrag mit Oracle erforderlich.	

zenzmodell so stark ändert, ist berechtigt und im Kontext anderer, vergleichbarer Projekte zu betrachten: Google Chrome oder die Programmiersprache Go verwenden schon länger kurze Releasezyklen. Diese iterativen Veröffentlichungen lassen sich meist mit dem darunterliegenden agilen Prozess erklären.

Agilität schafft neue Fakten

Hier liegt für den Anwender der wichtigste Vorteil darin, dass er schneller neue Funktionen bekommt. Oracle profitiert ebenfalls: Das Unternehmen muss nicht mehr mehrere Java-Versionen parallel kostenlos unterstützen.

Mit dem neuen Releasezyklus führt Oracle auch ein neues Modell für den kommerziellen Support mit zwei Arten von Abonnements ein. Das Java-



Kürzere Release- und Supportzyklen zwingen die Anwender zum Umdenken.

>>> 2 TAGE

>>> 140 TEILNEHMER

>>> 4 BÜHNEN

>>> 22 SPEAKER

>>> 1.800 QM

// LEETCON DIE CONVENTION FÜR INFORMATIONS- UND IT-SICHERHEIT

7. - 8. November >>> Expowall Hannover

Sichere Dir jetzt Dein Ticket zum Vorteilspreis!

>>> CODE: LeetCon_2018



www.leetcon.de

SE-Subscription-Modell ist für Serverapplikationen gedacht, die Abrechnung erfolgt pro Prozessor (ix.de/ix1810014). Für Clients gilt das Java-SE-Desktop-Subscription-Modell, das pro Benutzer abgerechnet wird. Wenn Unternehmen Server- und Client-Anwendungen nutzen wollen, müssen sie beide Abonnements abschließen.

Sobald Cloud- oder Container-Anwendungen hinzukommen, lässt sich die Aussage über genutzte CPUs nicht mehr einfach beantworten. Ob Oracle das Lizenzmodell für diesen Anwendungsfall anpassen will, ist offen.

Mit Blick auf das JDK haben Unternehmen drei Optionen zur Auswahl:

- Umstieg auf eine neue Java-Version alle sechs Monate;
- kommerzieller Support von Oracle;
- die Migration erfolgt weiterhin im Tempo des eigenen Projekts beziehungsweise nach Unternehmensrichtlinien. Support entfällt vollständig oder lässt sich für die eigentlich notwendige Migration auf die neue Version durch externe Dienstleistung kompensieren.

Open-Source-Frameworks und Bibliotheken geraten nun unter Druck, wenn sie versuchen, mit Oracle mitzuhalten. Sobald sie Sprachfeatures künftiger Versionen verwenden, sind die nicht mehr kompatibel mit älteren Java-Versionen.

Es gibt Alternativen

Die bisherige Betrachtung beschränkt sich auf den Marktführer für Java Virtual Machines, doch neben Oracle bieten andere Hersteller ebenfalls Laufzeitumgebungen für Java an. Die Konkurrenten nutzen allesamt Javas Open-Source-Teil OpenJDK als Basis, der ebenfalls von Oracle bereitgestellt wird (ix.de/ix1810014). Er enthält alle notwendigen Bestandteile für eine Java-Laufzeitumgebung. Deshalb wird das OpenJDK schon seit Längerem in anderen Open-Source-Projekten wie Linux eingesetzt. Es fehlen nur wenige Oracle-spezifische Tools.

Der Releasezyklus von OpenJDK entspricht ungefähr dem von Oracle vorgegebenen. Ein entscheidender Vorteil des Development Kit: Der Support

für LTS-Versionen läuft deutlich länger als die von Oracle gewährten sechs Monate. Das AdoptOpenJDK-Projekt bietet kostenlose Unterstützung für Java 11 bis September 2022 an.

Manche suchen den Kompromiss

Derzeit erscheint die Laufzeitumgebung Azul mit dem Pro-

dukt Zulu als ein vielversprechendes Supportmodell für Java. Azul bietet ein Jahr längeren Support für die LTS-Versionen und schafft einen Kompromiss zwischen den großen LTS-Versionssprüngen und den kurzen halbjährlichen Releasewechseln (ix.de/ix1810014).

Für die eigene Hardware bietet IBM kostenlose native JDK-Versionen für AIX, Linux, z/OS und IBM i. Der Hersteller

hat angekündigt, nicht mehr jede Java-Version zu berücksichtigen, und konzentriert sich auf LTS-Versionen. In Enterprise Linux 7 verwendet Red Hat derzeit OpenJDK 8 und verspricht Support bis 2020. Wie IBM will man Java 9 und 10 überspringen.

(jd@ix.de)

 Alle Links: ix.de/ix1810014



Kein Wein ohne Schorle!

Kein Storage ohne Rausch

Ernten Sie, was wir säen: Detailverliebtes badisches Handwerk, gemischt mit leistungsstarker Hardware und einer Cuvée passender Software. Damit Ihre Server- und Storage-Lösung genau Ihren Geschmack trifft.



Wenn es passt, ist es Rausch!
Hand drauf!

RAUSCHNETZWERKTECHNIK
www.rnt.de



Rausch Netzwerktechnik GmbH · Im Stöck 4a · 76275 Ettlingen · Germany
Copyright by Rausch Netzwerktechnik · Fon +49(0)7243 5929-0 · info@rnt.de · www.rnt.de

Produktionsdatenerfassung on demand

Das Fraunhofer IOSB-INA, Institutsteil für industrielle Automation, hat einen mobilen Industrie-4.0-Analysekoffer na-



Quelle: Fraunhofer IOSB-INA

Das mobile Produktionsdatenerfassungssystem INAense sendet ohne zusätzliche Hardware.

mens INAense entwickelt, mit dem vor allem mittelständische Unternehmen ihre Maschinen und Anlagen untersuchen können, ohne in eigene Hardware oder Sensorikfachkräfte investieren zu müssen. INAense beinhaltet ein Sensorsystem, das unter anderem Vibration, Druck, Distanz, Temperatur, Luftfeuchte und Anlageneleistung misst. Eine SPS (speicherprogrammierbare Steuerung), ein interner Rechner, ein Gateway sowie ein LTE-Router verarbeiten die Daten vor und übermitteln sie per Mobilfunk an eine Datenbank. Mit KI-Verfahren lassen sich diese dann analysieren, um Ursachen für Qualitätsdefizite oder Anzeichen für eine notwendige Wartung zu erkennen. (sun@ix.de)

3D-Metalldruck für die Serienproduktion

HP hat seine neuen 3D-Dru-
cker HP Metal Jet vorgestellt,
die sich für die Fertigung gro-
ßer Serien von Metallteilen
eignen sollen. Die neuen Ge-
räte verwenden die Binderjet-
Technik, die das Metallpulver
mit einem Bindemittel festigt.
Anschließend wird das schicht-
weise hergestellte Bauteil im
Sinterprozess zu einem metalli-
schen Objekt „gebacken“. HP
Metal Jet soll 50-mal schneller
sein als andere Metalldruck-
verfahren, wozu auch die re-
dundanten Druckdüsen bei-
tragen. Bisherige Methoden
schmelzen das Pulver mit ei-
nem Laser auf.

HP sieht den Einsatz des
Metal Jet vor allem in der Fer-
tigungsindustrie für Autos und
medizinische Geräte. Volkswagen
will die neuen 3D-Drucker

nutzen, da mit ihnen nun die additive Fertigung von Serienteilen in der Automobilproduktion interessant wird. Bislang konnte Volkswagen 3D-Druck-
verfahren nur für die Sonderanfertigung einzelner Teile oder Prototypen einsetzen.

Gemeinsam mit HP und
Bauteilproduzent GKN Powder
Metallurgy entwickelt Volks-
wagen die Technik so weiter,
dass zunächst Designelemente
in kleinen Serien entstehen,
etwa Schriftzüge für die Heck-
klappe, Sonderschaltknäufe
oder Schlüssel mit individuel-
lem Schriftzug. Später will man
Stückzahlen, Bauteilgröße und
technische Anforderungen stei-
gern, bis hin zu fußballgroßen
Objekten mit einer Stückzahl
von über 100 000 Einheiten im
Jahr. (sun@ix.de)



Bei Volkswagen produziert HPs Metal Jet bereits Schaltknäufe.



Alle Meldungen: Barbara Lange

Teilautomatisiertes Fahren im Serien-Lkw

Mercedes-Benz Trucks präsentierte den Lkw Actros, der mit dem „Active Drive Assist“ ausgestattet ist. Damit kann er in allen Geschwindigkeiten selbstständig bremsen, Gas geben und lenken. Eine automatische Vollbremsung löst bei Bedarf die mittlerweile fünfte Generation des „Active Brake Assist“ aus. Er kombiniert nun Radar- und Kamerasytem. Haupt- und Weitwinkelspiegel sind beim Actros durch die serienmäßige MirrorCam ersetzt, die die Rundumsicht stark verbessern

soll. Sie besteht aus zwei außen am Fahrzeug angebrachten Kameras und zwei 15"-Displays im Fahrerhaus. Die Verantwortung bleibt aber weiterhin beim Fahrer. Deshalb dienen zwei interaktive Bildschirme als zentrale Informationsquelle, die neben Basisinformationen auch die Assistenzsysteme visualisiert und Smartphones per Apple CarPlay und Android Auto einbindet. Über das Truck Data Center ist der Lkw permanent mit der Cloud verbunden. (sun@ix.de)



Mit dem Lkw Actros will Mercedes-Benz Trucks das teilautomatisierte Fahren in die Serie bringen.

Produktentwicklung mit agilen Methoden

Agile Methoden wie Scrum und Kanban oder Lean-Ansätze eignen sich auch für die Entwicklung von Nicht-IT-Produkten. Viele Firmen haben diese Verfahren in ihren Produktentstehungsprozess (PEP) integriert, da sie etablierte Ansätze als zu starr, zu linear, zu wenig kreativ und zu langsam empfinden. Dass sie damit recht haben, zeigt die Studie „Status Quo PEP – Lean und Agil im Produktentstehungsprozess“ der Hochschule Koblenz. Demnach sind Anwender von agilen und Lean-Methoden mit ihren Er-

gebnissen in jeder Phase des Entstehungsprozesses zufriedener und erfolgreicher.

Dass sich Unternehmen trauen, einen Schritt in Richtung Lean- und agiler Methoden zu gehen, dabei aber nichts überstürzen sollten, betonen die Wissenschaftler und geben neun Empfehlungen für das richtige Vorgehen beim Produktentstehungsprozess. Befragt wurden mehr als 130 Teilnehmer, hinzu kommen 30 Experteninterviews (kostenloser Download siehe ix.de/ix1810016). (sun@ix.de)

Autonome Straßenbahn im Test

Siemens Mobility hat auf der InnoTrans 2018 eine autonom fahrende Straßenbahn vorgestellt, die auf einem sechs Kilometer langen Abschnitt des Potsdamer Tramnetzes fährt. Der Prototyp erfasst seine Umwelt mit mehreren Lidar-, Radar- und Kamerasensoren. Komplexe Algorithmen bewerten die Fahrsituationen und

prognostizieren die weitere Entwicklung. Dadurch soll das System auf Lichtsignale achten, an den Haltestellen stoppen und eigenständig auf Gefahren wie querende Fußgänger und Fahrzeuge reagieren. Für einen kommerziellen Einsatz ist das Forschungsprojekt aber nicht ausgelegt. (sun@ix.de)

TERRA CLOUD BACKUP

DIE MODERNE UND
VERLÄSSLICHE ART DER
DATENSICHERUNG



Verlässlich

Deutsches Rechenzentrum,
DS-GVO Ready und TÜV geprüft



Sicher

Ende zu Ende Verschlüsselung
Ihrer Daten



Fair

Einfach strukturierte
Services zu Fixpreisen



Zuverlässig

Über 99% Erfolgsquote
bei Sicherungen



Erfahren

Durch Millionen erfolgreicher
Datensicherungen Jahr für Jahr



Serviceorientiert

Fachkompetentes, deutsches
Backup Team



Erfahren Sie mehr zum TERRA Cloud Backup

Unseren TERRA CLOUD Vertrieb erreichen Sie unter:

Telefon: +49 5744.944 188 | E-Mail: cloud@wortmann.de

© Copyright by Heise Medien.

www.wortmann.de

WORTMANN AG

IT. MADE IN GERMANY.

NoSQL-Datenbank Redis bleibt quelloffen

Redis Labs, die US-Firma hinter der freien NoSQL-Datenbank Redis, hat Teile ihrer Software unter eine sogenannte Common-Clause-Lizenz gestellt. Ziel der neuen Lizenzpolitik ist eine Einschränkung des Wiederverkaufs von Enterprise-Add-ons für Redis wie RediSearch, RedisGraph, ReJSON, Redis-ML und Rebloom durch Dritte.

Mit dem Schritt möchte das Unternehmen aus Kalifornien nach eigenem Bekunden Cloud-Provider daran hindern, den Datenbankservice mit Enterprise-Modulen als Managed Service anzubieten und damit hohe Gewinne zu erzielen, ohne dass von diesem Geld etwas an Redis zurückfließt. Die Änderung der Lizenzpoli-



tik löste in der Open-Source-Community heftige Diskussionen aus.

Die betroffenen Redis-Zusätze (alle Eigenentwicklungen) bietet das Unternehmen ab sofort unter einer um die Common Clause erweiterten Apache-2.0-Lizenz an. Diese verbietet nicht die kommerzielle Nutzung, wohl aber den Vertrieb dieser Module im Rahmen von Drittanbieter-Dienstleistungen.

Das Kernprodukt des Unternehmens, das Datenbankmanagementsystem selbst, steht nach wie vor unter der freien BSD-Lizenz zur Verfügung und soll nach Angaben von Redis Labs auch in Zukunft reine Open-Source-Software bleiben. (akl@ix.de)

Graphdatenbankmodul für Redis

Mit RedisGraph 1.0 hat Redis Labs die erste offizielle Version einer Architektur für Graphdatenbanken vorgestellt. Sie ist in C geschrieben und nutzt die GraphBLAS-Bibliothek sowie die von Neo4j entwickelte, quelloffene Abfragesprache Cypher.

RedisGraph ist als Redis-Modul konzipiert und steht, wie andere Enterprise-Module für das NoSQL-DBMS, unter der Apache-2.0-Lizenz. Die hinzugefügte Common-Clause-Bedingung untersagt die kommerzielle Weiterverbreitung. (akl@ix.de)

SQL-Data-Warehouse SQream DB 3.0 beschleunigt Big-Data-Analysen

Mit SQream DB 3.0 hat das israelische Unternehmen SQream Technologies Ltd eine neue Version seines Data-Warehouse vorgestellt. Das RDBMS, das auf die Analyse von Big-Data-Beständen spezialisiert ist, setzt für die Verarbeitung auf



die Parallelrechenleistung der Grafikprozessoren von NVIDIA.

SQream 3.0 verspricht doppelt so schnelle Ladezeiten und bis zu 15-mal schnellere Querys für Joins über mehrere Tabellen als vorherige Versionen. (akl@ix.de)

Cloud-Speicher-Spezialist Cloudian zeigt sich beliebt bei Investoren

In einer neuen Finanzierungsrounde (Series E) hat der Objekt-Storage-Spezialist Cloudian 94 Millionen US-Dollar erhalten. Ein Drittel davon will das kalifornische Unternehmen für die technische Weiterentwicklung seiner Speicherprodukte einsetzen. Der Rest der Summe sei für den Ausbau von Services für Enterprise-Kunden

sowie für Marketing und Vertrieb gedacht. Cloudians Flaggschiff ist HyperStore, ein hoch skalierbarer Objektspeicher mit nativer S3-Schnittstelle. HyperStore lässt sich sowohl als vorkonfigurierte Appliance als auch im eigenen Rechenzentrum oder in der (Hybrid-)Cloud betreiben. (akl@ix.de)

CNCF übernimmt Kubernetes

Die Betreuung und Eigentümerschaft der Infrastruktur des Kubernetes-Projekts kommt in die Hände der Cloud Native Computing Foundation (CNCF). Die Stiftung, die sich bereits seit 2014 um die technische Weiterentwicklung des Orchestrationstools für Container kümmert, erhält dazu verteilt über drei Jahre von Google neun Millionen US-Dollar an Guthaben in Form von Google Cloud Credits.

2014 hatte Google Kubernetes aus der Taufe gehoben und das Projekt im Jahr darauf bei der CNCF als Inkubator-Projekt untergebracht. Die Regie über die Kubernetes-Infrastruktur mitsamt Repository für Container-Images verblieb jedoch bei Google Cloud. In der relativ kurzen Zeit seines Bestehens hat sich Kubernetes zum Shootingstar unter den Container-Management-Werkzeugen entwickelt. (akl@ix.de)

Red Hat veröffentlicht Ansible Tower 3.3

Linux-Spezialist Red Hat hat eine neue Version seiner webbasierten Konfigurationsmanagementsoftware für Enterprise-Kunden Ansible Tower freigegeben. Die neu gestaltete Oberfläche zeigt nun mehr Detailinformationen an und soll die Konfiguration von Scheduling-Jobs und Workflows vereinfachen und flexibler gestalten. Die in Ansible Tower 3.2 eingeführten Instance Groups, Sammlungen von Nodes, die für einen bestimmten Zweck zusammengeschaltet werden, haben die Entwickler von Red Hat leistungsfähiger gemacht. So können Administratoren die Größe



einer solchen Gruppe nun als Prozentsatz der gesamten Clusterkapazität festlegen sowie die Instanzengruppen mittels Policies verwalten.

Ansible Tower 3.3 lässt sich auf Red Hats Container-Plattform OpenShift betreiben und direkt von dort aus konfigurieren und im laufenden Betrieb durch das Hinzufügen neuer OpenShift-Pods skalieren. Verbessert und erweitert hat Red Hat zudem die Integration von Ansible Tower mit Authentifizierungs-Frameworks und -Protokollen wie SAML, LDAP und OAuth2 (Tokens und Applikationen). (akl@ix.de)

Kubernetes-SDK für Pulumi

Das Start-up Pulumi hat ein Software Development Kit für Kubernetes vorgestellt. Das SDK ermöglicht vollständigen Zugriff auf die APIs der Container-Verwaltungssoftware. Es lassen sich damit Kubernetes-Cluster provisionieren, konfigurieren und aktualisieren. Das funktioniert lokal mit Minikube, in firmeneigenen Rechenzentren sowie in Cloud-

basierten Kubernetes-Clustern. Pulumi spielt zudem mit den Managed Services von Google (GKE), Azure (AKS) und Amazon (EKS) zusammen.

Zur Erstellung von Kubernetes-Anwendungen mit Pulumi lassen sich die Skriptsprachen TypeScript und JavaScript mitsamt ihren Bibliotheken verwenden. Python und Go sollen in Kürze folgen. (akl@ix.de)

Kurz notiert

Rubrik hat die bereits im Juni angekündigte Version 4.2 von **Rubrik Alta** freigegeben. Die Managementplattform für die Enterprise Hybrid Cloud ist über Partner und Reseller verfügbar.

SAP hat Privileged Access Security, die Sicherheits-Suite von **CyberArk**, für die Verwendung mit der SAP-Geschäftsanwendungsplattform NetWeaver zertifiziert. Mit den Security-Tools lassen sich Zugriffe von privilegierten SAP-Accounts im gesamten SAP-Stack sicher verwalten.



Sicherheit & Effizienz für
Fileserver und AD



**VOM IST ZUM SOLL
... UND DORT BLEIBEN**

tenfold NEUE
VERSION
2018



**Daten und
Berechtigungen
konsolidieren
mit migRaven.one**

«Aufräumen, Umräumen,
Aussortieren ...
Eine saubere Sache!»

**Berechtigungs-
management**
der nächsten Generation

**Automatisierung
Nachvollziehbarkeit
Sicherheit**

Kleine Fritzbox für Super-Vectoring

AVM hat mit der Fritzbox 7530 ein Einsteigermodell im Programm, das an allen DSL-Anschlüssen einsetzbar ist und sich insbesondere für die bis zu 300 MBit/s schnellen Supervectoring-Zugänge (35b) eignet. Im Vergleich zur „großen“ Fritzbox 7590 sparte der Hersteller bei dem neuen Modell ein wenig an den „inneren“ Werten. Statt mit 4x4-Streams funkten die 7530 nur über 2x2-Dualband WLAN AC+N im 2,4- und 5-GHz-

Band mit Multi-User MIMO. Diese Fritzbox erreicht somit 866 MBit/s + 400 MBit/s und damit nur den halben Durchsatz des großen Modells, bietet aber gleichfalls vier GBit-LAN-Ports, verfügt immerhin über einen USB-Anschluss und beinhaltet die AVM-übliche DECT-Basisstation. Zudem besteht die Möglichkeit, als alternativen Internetzugang einen LAN-Port für den Betrieb an Kabel- oder Glasfasermodems zu nutzen. (un@ix.de)

Kurz notiert

Ethernet-Adapter mit 25 GBit/s knackte laut Dell'Oro Group im zweiten Quartal 2018 die Millionenmarke. Die schnellen Ports haben inzwischen die 10-GBit/s-Pendants als Standardausrüstung beim Kauf von Servern für große (Cloud-)Rechenzentren abgelöst.

DE-CIX erzielte im Geschäftsjahr 2017 einen Umsatz von 31,8 Mio. Euro (+9 %). Das Ergebnis vor Zinsen und Steuern (EBIT) belief sich auf 0,9 Mio. Euro. Die Frankfurter eco-Tochter unterhält inzwischen 13 Internetknoten weltweit, die von über 1500 Organisationen genutzt werden.

Dell EMC bringt mit dem Z9264F-ON einen neuen 100-GbE-Fabric-Switch der Z-Serie auf den Markt. Das System, in dem der StrataXGS-Tomahawk-II-Prozessorsatz von

Broadcom verbaut ist, bietet Platz für 64 Ports in einem Formfaktor von zwei Höhen-einheiten.

NXP schluckte das sechs Jahre alte Start-up **OmniPHY**. Mit dem Kauf pept der niederländische Halbleiterhersteller sein Angebot an schnellen Ethernet-Subsystemen für die Automotive-Branche auf.

Der österreichische Webhoster **World4You** gehört jetzt **United Internet**, genauer deren Tochter 1&1 Internet SE. World4You, der über 100 000 Kunden zählt und 250 000 Domains verwaltet, soll künftig weiterhin als eigenständiges Unternehmen auf dem österreichischen Markt aktiv bleiben.

Wie schon länger geplant gliederte die **QSC AG** zum September 2018 ihren TK-Bereich aus. Dieser bietet nun als Plusnet GmbH über die eigene Netzinfrastruktur Breitband-TK-Dienste für Unternehmen und Organisationen an.

VPN-Router mit LTE-Modem

LANCOM Systems bringt den Mobilfunk-Router 1790-4G auf den Markt. Das Gerät beherrscht LTE mit bis zu 300 MBit/s im Download (Cat 6). Zum Anschließen eines DSL-Modems steht eine GBit-Ethernet-Schnittstelle zur Verfügung. Der LANCOM-Router implementiert einige Sicherheitsmerkmale (Stateful-Inspection-Firewall, Intrusion Prevention und Dos-Schutz). Mit dabei sind außerdem fünf IPsec-VPN-Kanäle, die externen Mitarbeitern eine geschützte Anbindung ans Unternehmensnetz ermöglichen. Optional lässt sich der Router auf bis zu 25 VPN-Kanäle aufrüsten.

Virtualisierung setzt der Router mittels ARF (Advanced Routing and Forwarding) um, um für bis

zu 16 Netze einen separaten IP-Kontext mit individuellem Zuschnitt der DHCP- und DNS-Server einzurichten. Die Dual-Stack-Implementierung ermöglicht den Einsatz in IPv4-, IPv6- und gemischten Netzen. Wie bei LANCOM üblich, lässt sich das 1790-4G-Modell wahlweise über die kostenlosen Tools LANconfig und LANmonitor managen oder in die hauseigene Management-Cloud integrieren. (un@ix.de)



Glasklare Ausbauvorhaben der Telekom

In der ersten Septemberwoche feilte die Telekom einmal mehr an ihrem Image als Anbieterin schneller Internetzugänge. Der Bonner Konzern macht insbesondere beim Vectoring Tempo: Über 3,3 Mio. Anschlüsse wurden mittels dieser Technik binnen vier Wochen auf höheren Durchsatz getrimmt. Allein die Zahl der Supervectoring-Anschlüsse mit bis zu 250 MBit/s soll um 2,9 Mio. auf nun 8,9 Mio. gestiegen sein. Die Zahl der bis zu 100 MBit/s schnellen Anschlüsse erhöhte sich durch die Nachrüstung um 415 000.

Die Telekom tritt der oftmals geäußerten Kritik am weiteren Ausreizen der guten alten Kupferleitungen entgegen: Das Vectoring bremse keineswegs

den zukunftssicheren Glasfaserausbau. Man werde schließlich im ersten Schritt die Glasfaser an die Anschlussknoten in die Städte und Dörfer bringen, um überhaupt schnellere Anschlüsse feilbieten zu können. Die Ausbaupläne des Bonner Konzerns sehen außerdem vor, bis 2022 bundesweit 3000 Gewerbegebiete mit FTTH ans Glasfasernetz anzuschließen.

Zurzeit werden fast 800 km Glasfaser verlegt, wobei unter anderem das Verlegen in schmalen Schlitten (Trenching) zum Einsatz kommt. Die Telekom betreibt nach eigener Auskunft mit mehr als 455 000 km das größte Glasfasernetz in Europa. Bis Ende 2018 soll es auf über 500 000 km wachsen.

(un@ix.de)

Nahezu jeder nutzt das Internet

In Deutschland nutzen 66,5 Millionen Personen ab zehn Jahren das Internet. Das meldete das Statistische Bundesamt (Destatis). Der Anteil an der hiesigen Gesamtbewohlerung beträgt damit 90 %. 2017 lag der Wert noch drei Prozentpunkte niedriger. Rund 64 Mio. Menschen ab 10 Jahren waren in den drei Monaten vor der Befragung online, also im 1. Quartal 2018. Diese Nutzer wählten bevor-

zug Handys (87 %) für den Internetzugang. Laptops (65 %), Desktop-PCs (62 %) und Tablets (46 %) waren die weiteren präferierten Zugangsgeräte.

Immerhin 16 % greifen außerdem auf andere Endgeräte wie Media-Player, E-Book-Reader oder Smartwatches zurück. 85 % des Personenkreises, der das Internet im 1. Quartal 2018 nutzte, war auch mobil online. (un@ix.de)

Fernstudium IT-Security

Aus- und Weiterbildung zur Fachkraft für IT-Sicherheit. Vorbereitung auf das **SSCP**- und **CISSP**-Zertifikat. Ein Beruf mit Zukunft. Kostengünstiges und praxisgerechtes Studium ohne Vorkenntnisse. Beginn jederzeit.

NEU: Roboter-Techniker, Netzwerk-Techniker, Qualitätsbeauftragter /-manager TÜV, Linux-Administrator LPI, PC-Techniker

Teststudium ohne Risiko. GRATIS-Infomappe gleich anfordern!

FERNSCHULE WEBER - seit 1959
Neerstedter Str. 8 - 26197 Großenkneten - Abt. C98
Telefon 0 44 87 / 263 - Telefax 0 44 87 / 264
www.fernenschule-weber.de

EU-Parlament stimmt nun doch für Reform des Urheberrechts

Nach einem anfänglichen Nein im Juli hat das EU-Parlament jetzt mit deutlicher Mehrheit dem nur geringfügig überarbeiteten Entwurf des Rechtsausschusses zur Reform des



Urheberrechts zugestimmt. Er sieht unter anderem eine Haftung von Plattformbetreibern für Urheberrechtsverletzungen durch nutzergenerierte Inhalte vor und führt das Leistungsschutzrecht für Presseverleger europaweit ein. Außerdem dürfen zukünftig nur noch die Veranstalter Bilder und Videos von Sportereignissen verfügbar machen.

Axel Voss (CDU), Berichterstatter des EU-Parlaments für die EU-Urheberrechtsreform, freut sich nach der Abstimmung.

Rechteverwerter wie die GEMA, der Bundesverband Musikindustrie und die Verlegerverbände VDZ und BDZV sehen in dem Entwurf die Rechte der Urheber gestärkt und freuen sich auf sprudelnde Lizenzzahlungen von YouTube, Google News und Co. Kritiker von der Electronic Frontier Foundation (EFF) und Wikipedia über Bitkom und eco bis hin zum Bundesverband der Verbraucherzentralen und dem Bundesverband Deutsche Startups warnen vor Upload-Filtern, Zensur, Einschränkungen

der Meinungsfreiheit und dem Schutz veralteter Geschäftsmodelle durch das reformierte Urheberrecht.

In den folgenden Trilog-Verhandlungen müssen sich jetzt EU-Parlament, Kommission und die Mitgliedsstaaten auf eine endgültige Fassung der Reform einigen, über die dann wiederum das Parlament abstimmt. Martin Sonneborn (Die Partei) hat auf Twitter das Abstimmverhalten der deutschen Abgeordneten zusammengestellt (siehe ix.de/ix1810021).

(odi@ix.de)

Kartellrecht im Internet

Das Bundeskartellamt will noch dieses Jahr Maßnahmen gegen Facebook einleiten. Ein Bußgeld steht nicht im Raum, möglicherweise aber ein Verbot einiger Praktiken des Unternehmens. Seit März 2016 prüft die Behörde, ob Facebook seine Marktmacht missbraucht, wenn es Nutzerdaten seiner Töchter WhatsApp und Instagram auswertet.

Bundeswirtschaftsminister Altmaier hat in einer Studie untersuchen lassen, welche

Möglichkeiten das Kartellrecht bietet, um gegen unfaire Praktiken der großen Internetfirmen vorzugehen. Ergebnis: Im Großen und Ganzen reicht das europäische und deutsche Kartellrecht aus. Allerdings müsste man über die Einführung einer marktanteilsabhängigen „Daten-Sharing-Pflicht“ nachdenken, um Monopole durch die Kontrolle über Daten zu verhindern und den Zugang zu großen Datenmengen zu erleichtern. (odi@ix.de)

E-Commerce: Finanzspritze für PayDirect

PayDirect, der gemeinsame Bezahlservice der deutschen Banken und Sparkassen, soll attraktiver werden. Bis Ende 2018 sollen erhebliche Investitionen die PayPal-Konkurrenz wettbewerbsfähig machen. Bislang haben erst zwei Millionen Bankkunden PayDirect aktiviert,

obwohl theoretisch 50 Millionen Girokonten PayDirect-fähig sind – PayPal hat in Deutschland über 20 Millionen Kunden. Gut 9000 Onlineshops akzeptieren PayDirect, während Zahlungen mit PayPal bei 19 Millionen Händlern weltweit möglich sind. (odi@ix.de)

Datenschutz auf Facebook-Seiten

Im Juni hatte der Europäische Gerichtshof entschieden, dass die Betreiber von Facebook-Seiten für den Datenschutz mitverantwortlich sind. Nun hat Facebook seine Datenschutzbestimmungen angepasst: Sie erklären jetzt, dass Facebook und der Seitenbetreiber gemeinsam verantwortlich für die Verarbeitung der Nutzerdaten sind, die die Insights-Funktion zugäng-

lich macht. Seitenbetreiber müssen sicherstellen, dass sie eine Rechtsgrundlage für die Verarbeitung der Insights-Daten gemäß DSGVO haben – nach Einschätzung der Datenschutzkonferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder ist die Insights-Funktion ohne explizite Einwilligung der Nutzer der Seite rechtswidrig. (odi@ix.de)

Kurz notiert



Die neue Version 7 des Java-Script-Compilers **Babel** versteht jetzt auch TypeScript und implementiert die jüngsten Neuerungen des ECMAScript-Standards.

Große Digitalunternehmen sollen in der EU künftig mehr Steuern zahlen – in der Diskussion sind drei Prozent Umsatz-

steuer. Einige Länder wie Irland, Luxemburg und Malta, aber auch der deutsche Finanzminister sind allerdings skeptisch.

Interne **Löschtage von Facebook** sind nach einem Urteil des Oberlandesgerichts München rechtswidrig, wenn sie gegen die Meinungsfreiheit oder andere Grundrechte der Nutzer verstößen (Az. 18 W 1294/18).

EXPERTEN FÜR SICHERE ANWENDUNGEN ■ www.optimabit.com

Security Assessment

Penetrationstest

Sicherer SDLC

Code Review

ISO 27001

Mit
LIVE Hacking
Demo



OPTiMA..bit
business information technology gmbh

Besuchen Sie uns auf der

DevSec

Die Konferenz für sichere Software- und Webentwicklung

Heidelberg, Print Media Academy,
16.-18. Oktober 2018

parallel 2019

Softwarekonferenz für parallele und hochperformante Programmierung

CALL FOR PROPOSALS
bis zum 1. Oktober 2018

// THEMEN:

- Moderne Programmiermodelle und Parallelisierungsstrategien
- Erfahrungen mit Sprachen wie Ada, Clojure, Erlang, F#, Fortran, Go, Groovy, Python, Rust und Scala
- Performancemessung und -optimierung
- Ansätze, Konzepte und Werkzeuge zum Testen
- Migration bestehender Anwendungen auf parallele Architekturen
- Parallelisierung und spezielle Hardware (FPGA, GPU)
- Edge-Computing: Entwicklung verteilter IoT-Anwendungen
- Parallelprogrammierung in Big-Data-Szenarien: Deep Learning, Machine Learning und Data Analytics
- Erfahrungen hinsichtlich Echtzeit und funktionaler Sicherheit bei Embedded-Entwicklungen
- Architektur von Cloud-Anwendungen, hinsichtlich Performanz und Skalierbarkeit

Veranstalter:



Oracle gibt Solaris 11.4 frei

Wie angekündigt hat Oracle Solaris 11.4 veröffentlicht. Die neue Version fügt dem Betriebssystem einige neue Funktionen hinzu.

Neu ist beispielsweise ein verbessertes Service-Management-Framework. Damit lassen sich kritische Anwendungen und Dienste überwachen, wenn nötig leitet es einen automatischen Neustart ein. Alle Zonen des Systems – Container für Solaris – kann der Administrator nun mit einem Befehl entfernen und wieder hinzufügen. Außerdem kann er Abhängigkeiten der Zonen voneinander definieren, damit sie in der richtigen Reihenfolge starten.

Hinzu kommen einige Sicherheitsfunktionen: In einem Rechnerverbund lässt sich die Compliance aller Knoten mit einem Befehl überprüfen. Auf Wunsch führt der Verbund diese Prüfung periodisch in einem festgelegten Zeitraum durch und fasst die Ergebnisse in einem Report zusammen. Mit der neuen Immutable Zone lassen sich Zonen komplett isolieren, einzige Aktualisierungen kann der Administrator noch über das Image Packaging System (IPS)

einspielen. Erst über explizit anzulegende „vertrauenswürdige Pfade“ können Dienste wie Puppet oder Chef auf eine Immutable Zone zugreifen.

Ebenfalls in den Bereich der Sicherheit fallen die Umsetzung des Key Management Interoperability Protocol (KMIP) und eine Funktion, die Oracle Silicon Secured Memory getauft hat und die unberechtigte Speicherzugriffe erkennen soll. Hinzu kommen die üblichen Aktualisierungen der Pakete, unter anderem umfasst Solaris 11.4 X.org 1.19 sowie GNOME 3.24, Python 3.5, Puppet 5.5, Perl 5.26, MySQL 5.7 und Open Fabric Enterprise Distribution 3.18.

Trotz Oracles Ankündigung von Solaris 11.next und dem Versprechen, dass jeden Sommer eine neue Solaris-Version erscheinen soll, zweifelten viele Beobachter an der Zukunft des Betriebssystems. Gründe dafür gab es mehrere: Seit Anfang 2017 liegt Solaris 12 auf Eis. Im selben Jahr entließ Oracle viele Entwickler der Hardworbasis SPARC. Dennoch hat der Konzern 2018 sein Versprechen an die Solaris-Kunden gehalten.

Harald Weiss (fo@ix.de)

Intels fast freie UEFI-Alternative

Vorerst nur für Embedded-Systeme mit Yocto Linux hat Intel seine eigene fast freie Firmware veröffentlicht. Damit steht der Slim Bootloader (SBL) genannte Neuling in Konkurrenz zu freien Firmware-Projekten wie Coreboot, Libreboot und LinuxBoot. Ein Teil des SBL-Quellcodes steht unter der BSD-Lizenz bei GitHub zum Download bereit. Er basiert größtenteils auf TianoCore EDK2, der freien Implementierung und Werkzeugsammlung für die UEFI-Spezifikation.

Zusätzlich benötigt der Anwender das proprietäre Binärpaket FSP 2.0 (Firmware Support Package), das mittlerweile unter einer ebenfalls wenig restriktiven Lizenz steht. Es enthält allerdings umstrittene Blobs, also große binäre Objekte wie Intels Management Engine. Das Projekt Coreboot ist zum Booten von x86-Hardware ebenfalls auf FSP angewiesen. Auch der

sogenannte Memory Reference Code (MRC), mit dem das BIOS beim Start den Arbeitsspeicher anlert und initialisiert, ist proprietär.

SBL startet nach der Initialisierung des Geräts eine sogenannte Payload, standardmäßig einen mit Yocto erzeugten Linux-Kernel. Will man den SBL mit Windows verwenden, muss man die UEFI-Funktionen des EDK2 als Payload einbinden. Einige Änderungen kann man mit einem Konfigurationswerkzeug beim Bauen des SBL vornehmen, ein BIOS-Setup für Änderungen in der laufenden Firmware ist nicht vorhanden.

Kompatibel sind zunächst nur einige Apollo-Lake-Plattformen: die Entwickler-Boards UP² (UP Squared) mit Intel Celeron N3550 und die Customer Reference Boards Oxbow Hill, Juniper Hill und Leaf Hill mit Atom x7 E3980 oder Atom x5 3930. (sun@ix.de)

Linux-Kernel: Torvalds nimmt eine Auszeit

Schon öfter in der Vergangenheit hatte Linus Torvalds auf der Kernel-Mailingliste mit teils rüden Verbalattacken seinem Ärger über schlechten Code oder andere Dinge Luft gemacht. Im Zuge der Freigabe des vierten Release-Kandidaten für den Kernel 4.19 bat er öffentlich für seine oft gedankelosen Schimpftiraden um Entschuldigung. Er sei – für viele wenig überraschend – kein empathischer Typ und habe große Schwierigkeiten, die emotionale Situation der anderen Entwickler richtig einzuschätzen.

Auslöser waren die Diskussionen um den Kernel Summit, dessen ursprünglicher Termin

mit Torvalds' Urlaubsplänen kollidierte. Die daraufhin entstandenen öffentlichen und privaten Diskussionen hätten ihm quasi einen Spiegel vorgeholt. Als Folge kündigte er an, sich eine Weile aus der Kernel-Entwicklung zurückzuziehen und sich Hilfe zum besseren Umgang mit anderen zu suchen. Er zog Parallelen zu der Zeit, als er sich für das Schreiben von Git schon einmal eine Weile aus der Arbeit am Kernel ausgeklinkt hatte, betonte aber, keinen Burn-out zu haben und definitiv zurückkehren zu wollen. In der Zwischenzeit werde Greg Kroah-Hartman ihn vertreten. (avr@ix.de)



So entspannt wie hier auf der LinuxConf Europe 2014 ist Linus Torvalds im Umgang mit seinen Mitstreitern nicht immer – doch das will der Linux-Chefentwickler ändern.

Kurz notiert

Über rund 4900 Server in mehr als 60 Ländern bietet **NordVPN** Anwendern die Möglichkeit, Einschränkungen wie Geo-Blocking oder staatliche Überwachung zu umgehen – mit einer nativen App jetzt auch unter Linux.

Univention hat auf Basis von Grafana, Prometheus und dessen Node Exporter ein Dashboard für das komfortable Monitoring komplexer Umgebungen gestrickt und zum öffentlichen Betatest freigegeben.

Mit **Red Hat Enterprise Linux 7.6 Beta** kann man sich einen Einblick in die kommende RHEL-Version verschaffen: Trusted Plat-

form Module (TPM) 2.0, neue Kryptoalgorithmen, Extended Berkeley Packet Filter oder das Podman Container Toolkit.

In **OpenSSL 1.1.1** haben die Entwickler jetzt die kürzlich als IETF-Standard verabschiedete Transportverschlüsselung TLS 1.3 integriert. Weiter beherrscht die Kryptobibliothek einige neue Verfahren, etwa SHA3, EdDSA (Ed25519 und Ed448), X448 oder Multiprime RSA.

Version 8 des **Tor Browsers** hat seinen Unterbau auf Firefox 60 ESR und einige Add-ons auf die Webextension-Versionen aktualisiert. Dank geänderter Konfiguration lassen sich die Zugänge zum Tor-Netzwerk jetzt direkt im Browser einrichten.

Azure-optimierter Kernel für SLES

Für den gemeinsam entwickelten und nach eigenen Angaben ersten Enterprise-Linux-Kernel speziell für Azure versprechen Microsoft und SUSE schnelleres Booten, weniger Speicherbedarf und mehr Leistung. Erreicht habe man dies, indem der Kernel aktuelle Azure-Funktionen wie Accelerated Networking via SR-IOV (Single Root I/O Virtualization) oder den Accelerator nutzen und so die I/O-Leistung deutlich verbessern kann. In der Ankündigung spricht SUSE von bis zu

25 Prozent schnellerem Daten durchsatz und einer 23 Prozent geringeren Latenz.

Bei der Pflege des optimierten Kernels stimmen sich die beiden Partner ab. Die Entwicklung haben sie an die Releasezyklen des Azure-Teams angepasst. Im Azure Marketplace ist der neue Kernel für SLES-15-Instanzen inzwischen die Voreinstellung. Wer den bisherigen Kernel nutzen möchte, kann diesen aber über den Paketmanager Zypper problemlos aktivieren. (avr@ix.de)

CM : Sicherheit für Software, Firmware und Daten



PC- und Embedded-Anwendungen sicher geschützt mit CodeMeter

- Technisch-präventiver Schutz der Software
- Schutz von Produktions- und Technologie-Daten
- Bedarfsgerechte Wartungs- und Pay-per-Use-Modelle
- Integrierbar in zentrale ERP- und CRM-Systeme
- Neue Geschäftschancen durch Lizenzierung

Bestellen Sie Ihr CodeMeter SDK
s.wibu.com/sdk

+49 721 931720
sales@wibu.com

// heise
devSec()
16-18 Oktober
s.wibu.com/devsec

Cold-Boot-Attacke reloaded: Fast alle Laptops betroffen

Sicherheitsforscher von F-Secure haben in aktuellen Computern eine Sicherheitslücke entdeckt, die es ermöglicht, auf vertrauliches Schlüsselmaterial zuzugreifen (Details unter ix.de/ix1810024). Es handelt sich dabei um eine Neuauflage der sogenannten Cold-Boot-Attacke aus dem Jahr 2008,

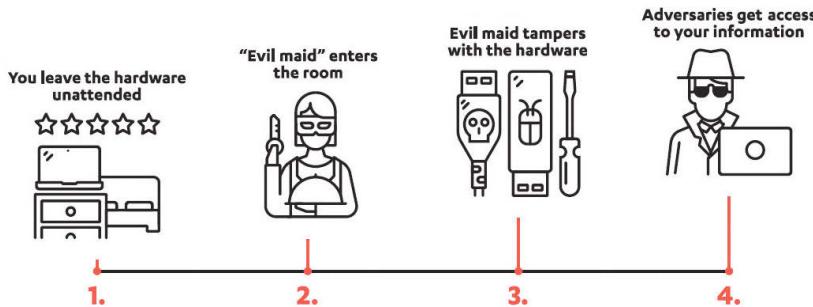
die auf einem Neustart eines nicht korrekt heruntergefahrenen Systems basierte. Dadurch konnten die Angreifer auf die im RAM noch kurzzeitig vorhandenen Daten zugreifen. Die heutigen Laptops überschreiben den Arbeitsspeicher, damit ein solcher Angriff nicht mehr funktioniert. Die For-

scher fanden nun einen Weg, den Überschreibprozess auszubauen.

Voraussetzung dafür ist wie schon bei der „klassischen“ Cold-Boot-Attacke der physische Zugriff auf das System. Da die Firmware-Einstellungen, die den Boot-Vorgang kontrollieren, nicht vor Manipulationen geschützt sind, kann man mit einem einfachen Hardwarewerkzeug den Speicherchip (Non-volatile Memory Chip) überschreiben, der diese Einstellungen enthält. Ein Angreifer kann dann den Speicher überschreiben und das Booten von externen Geräten zulassen.

Die eigentliche Cold-Boot-Attacke lässt sich anschließend mit einem speziellen Programm von einem USB-Stick aus starten. So erlangt der Angreifer Zugang zu Schlüsselmaterial und Passwörtern. Die Forscher haben ihre Resultate Intel, Microsoft und Apple mitgeteilt. Bis die Hersteller das Problem lösen können, raten sie Unternehmen, die Laptops so zu konfigurieren, dass sie automatisch herunterfahren oder in den Schlafmodus gehen. Dann muss der Anwender die BitLocker-PIN beim Hochfahren oder Wiederherstellen eingeben. F-Secure rät, Außendienstmitarbeiter und Führungskräfte über die Bedrohung zu informieren.

(ur@ix.de)



Microsoft legt Patch-Kriterien offen

Erstmals äußert sich Microsoft dazu, auf welcher Grundlage das Unternehmen über das Veröffentlichen eines Sicherheitsupdates entscheidet. Die „Microsoft Security Servicing Criteria for Windows“ (siehe ix.de/ix1810024) nennen zwei Kriterien: erstens, ob eine Schwachstelle eine Sicherheitsbarriere (Boundary) oder ein Sicherheitsfeature verletzt oder deren Absicht zuwiderläuft, und zweitens, ob der Bug schwerwiegend ist. Lassen sich beide Fragen bejahen, gibt es ein Sicherheitsupdate und gegebenenfalls eine Anleitung für Betroffene. Wenn nicht, wird die Schwachstelle in der nächsten Release berücksichtigt. Wie

gravierend eine Sicherheitslücke ist, beschreibt die „Microsoft Vulnerability Severity Classification for Windows“ (siehe ix.de/ix1810024). Zu den Update-relevanten Boundaries gehört etwa das Verhindern nicht autorisierter Zugriffe auf ein Endgerät im Netzwerk, eine Verletzung eines Sicherheitsfeatures wäre beispielsweise das Aushebeln von BitLocker oder SecureBoot. In den „Security Servicing Criteria“ erfährt man auch, für welche an Microsoft gemeldeten Schwachstellen man eine Belohnung („Bug-Bounty“) erhält – es sind alle, die ein Sicherheitsupdate rechtfertigen.

(ur@ix.de)

Sichere API-Nutzung mit KI

Im Zuge der Digitalisierung werden viele Daten, Dienste und Funktionen über APIs bereitgestellt. Befördert wird diese Entwicklung beispielsweise durch Branchenrichtlinien wie PSD2 oder FHIR/HL7, die die Zusammenarbeit von Unternehmen und den Austausch von Daten forcieren. Solche Schnittstellen sind daher interessant für Cyberkriminelle. Aus der Akquisition von Elastic Beam durch Ping Identity entstand nun das auf künstlicher Intelligenz beruhende „PingIntelligence for APIs“. Es ist Teil der

Ping Identity Platform und soll den Zugriff auf und die Nutzung von APIs in API-Infrastrukturen vor Cyberangriffen schützen. Es bietet Prüfpfade für API Traffic und blockiert automatisch erkannte Cyberattacken, die auf die Daten und Systeme hinter den Schnittstellen zielen. Eine Autodiscover-Funktion soll gewährleisten, dass keine aktive API oder zugehörige URL übersehen wird. Und schließlich erfasst PingIntelligence sämtliche API-Aufrufe für forensische oder Compliance-Reports.

(ur@ix.de)

Five-Eyes-Staaten fordern Hintertüren

Die Regierungen der sogenannten Five Eyes betreiben gemeinsam das Abhörsystem Echelon. Sie haben nun Dienstleister „ermuntert“, freiwillig Funktionen in ihre Produkte einzubauen, die für eine gesetzmäßige Überwachung nötig sind. Andernfalls drohen „technische, gesetzliche oder andere Maßnahmen“. Das geht aus der „Erklärung der Grundsätze für den Zugang zu Beweismitteln und Verschlüsselung“ hervor, die die Five-Eyes-Innenminister kürzlich veröffentlicht haben (siehe ix.de/ix1810024).

In der Erklärung heißt es weiter, dass Regierungen keine speziellen Entschlüsselungsmechanismen vorschreiben, sondern den Anbietern „angepasste Lösungen“ ermöglichen sollen. Diese können dann „auf ihre individuellen Systemarchitektu-

ren“ zugeschnitten sein. Und: „Der eingeschränkte Zugang zu den Inhalten rechtmäßig erhobener Daten ist nicht nur ein Problem der Regierungen allein, sondern eine gegenseitige

Verantwortung für alle Beteiligten.“ Klargestellt wird auch, dass ein Zugriff auf Daten stets nur im Einklang mit Recht und Gesetz erfolgen soll: „Dieser rechtmäßige Zugang

sollte immer der Aufsicht durch unabhängige Behörden und/oder der gerichtlichen Kontrolle unterliegen.“ Welche konkreten Schritte die Five-Eyes-Staaten nun einleiten, ist noch nicht bekannt. Unter der Bezeichnung Five Eyes versteht man die Zusammenarbeit jeweils mehrerer Geheimdienste der USA, Großbritanniens, Kanadas, Australiens und Neuseelands.

Tobias Haar (ur@ix.de)

Kurz notiert

In Berlin hat sich Ende August der **Bundesverband für den Schutz Kritischer Infrastrukturen e. V. (BSKI)** gegründet. Sein Ziel ist es, Sicherheitsrisiken für kritische Infrastrukturen zu reduzieren. Geplant sind For-

schungsprojekte, Publikationen, Veranstaltungen und mehr.

Das Schwachstellenmanagement-Framework **OpenVAS** (Open Vulnerability Assessment System) wird künftig **Greenbone Vulnerability Management** heißen, bleibt aber weiter Open Source und ist über greenbone.net zu erreichen.

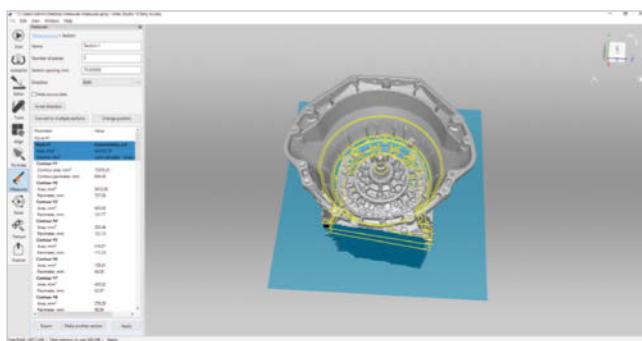
Artec Studio 13 mit schnellerem Workflow

Artec 3D hat die neue Version seines 3D-Scanning-Systems vorgestellt. Aufgrund neuer Algorithmen soll die Software sehr große 3D-Datensätze mit mehreren Hundert Polygonen schnell und präzise erfassen und verarbeiten – doppelt so schnell wie die Vorgängerversion. Unter anderem sollen drei neue Modi einen Geschwindigkeitsvorteil bringen.

Der „Röntgenmodus“ stellt die Rohdaten halbtransparent dar und entfernt das Rauschen in der Umgebung, sodass gleich nach dem Erfassen der Daten erkennbar ist, wenn etwa Bereiche eines Objekts fehlen oder die Ausrichtung des Scans

nicht optimal war. Ob der Scanner sich in der richtigen Entfernung zum Objekt befindet, zeigt „3D-Radar“ durch unterschiedliche Farbgebung an (rot, grün, blau). Diese Abstandskarte soll auch mit älteren Scannerversionen kompatibel sein. Der Modus „Max Error“ soll den Workflow beschleunigen, indem er automatisch alle Bereiche markiert, die besondere Aufmerksamkeit verlangen.

Artec Studio 13 gibt es als Professional-Version ab 400 Euro, Ultimate-Lizenzen, die auch den Einsatz von Scannern anderer Hersteller erlauben, kosten das Doppelte. (ka@ix.de)



Künstliche Intelligenz

Einer Studie des BVDW (Bundesverband Digitale Wirtschaft) zufolge rechnen deutsche Digitalunternehmen mit einem Umsatzwachstum von 22 Prozent, das auf den Einsatz von Techniken der künstlichen Intelligenz zurückzuführen ist. Befragt wurden 289 Experten aus Mitgliedsunternehmen des Verbands. Fast zwei Drittel der Befragten erwarten, dass durch diese Entwicklung Ar-

beitsplätze wegfallen, aber auch, dass im gleichen Umfang neue entstehen werden.

Den Anspruch der Bundesregierung, dass die deutsche Wirtschaft im Bereich KI eine Vorreiterrolle einnehmen wird, bezweifeln 78 Prozent der befragten BVDW-Experten. Zurückzuführen sei dies nicht zuletzt auf Regulierungsmaßnahmen unter anderem im Bereich Datenschutz. (ka@ix.de)

Neue Open-Source-Bibliothek

Auf der Big Data Conference in Kalifornien hat die Software AG Nyoka vorgestellt, eine Python-Bibliothek, mit der sich Modelle aus den Bereichen künstliche Intelligenz, Predictive Analytics und Maschinenlernen in das XML-Format PMML transformieren lassen. Die Predictive Model Markup Language ist ein von der Data Mining Group (DMG) entwickelter Industriestandard zum Austausch von Statistik- und Data-Mining-Modellen. (ka@ix.de)

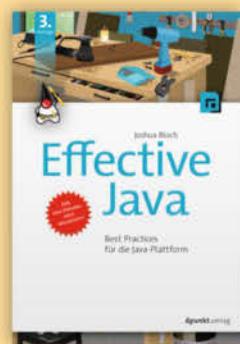
Neben den circa 500 Python-Klassen mit Tags, Konstrukturen und Parametern für PMML bietet Nyoka Klassen und Funktionen für komplexere Aufgaben, etwa das Erstellen einer PMML-Datei für ein Random-Forest-Modell auf der Basis eines Scikit-learn-Objekts. Zum Lieferumfang gehören eine HTML-Dokumentation sowie diverse Jupyter-Notebook-Tutorials. Nyoka ist kompatibel mit Python-Version 3.5 und auf GitHub erhältlich. (ka@ix.de)

J. Bloch

Effective Java

Best Practices
für die Java-Plattform

3. Auflage
2018, 410 Seiten
€ 36,90 (D)
ISBN 978-3-86490-578-0



S. Roock · H. Wolf

Scrum – verstehen und erfolgreich einsetzen

2. Auflage
2018, 264 Seiten
€ 29,90 (D)
ISBN 978-3-86490-590-2

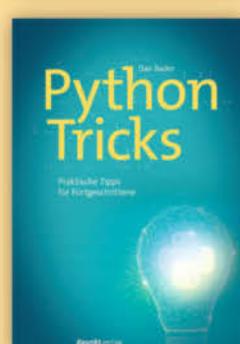


D. Bader

Python-Tricks

Praktische Tipps für Fortgeschrittene

2018, 210 Seiten
€ 29,90 (D)
ISBN 978-3-86490-568-1



H. Stauffer

Security für Data-Warehouse- und Business-Intelligence-Systeme

Konzepte, Vorgehen und Praxis

2018, 302 Seiten
€ 59,90 (D)
ISBN 978-3-86490-419-6



E. Wolff

Microservices

Grundlagen flexibler Softwarearchitekturen

2. Auflage
2018, 384 Seiten
€ 36,90 (D)
ISBN 978-3-86490-555-1



dpunkt.verlag

www.dpunkt.de



Microsoft stellt Cloud Deutschland ein

Aufgrund veränderter Kundenanforderungen stellt Microsoft die Treuhänder-Cloud mit der Deutschen Telekom ein. Das 2015 angekündigte Angebot hatte zum Ziel, Kundendaten statt in den USA in Deutschland zu speichern. Hintergrund war die Verunsicherung vieler Kunden im Zusammenhang mit der NSA-Affäre. Als Treuhänder der Cloud Deutschland fungiert die Telekom-Tochter T-Systems International, die den Zugang der Daten überwacht (zur Sicherheit der Daten siehe iX 9/2018, S. 82). Dafür zahlen die Kunden einen Aufpreis. Bestandskunden können weiterhin die Dienste nutzen und erhalten auch Sicherheitsupdates.

Microsoft baut zurzeit zwei Cloud-Zentren in Frankfurt und

Berlin auf. Azure wird im 4. Quartal 2019 verfügbar sein, Office 365 und Dynamics 365 erst im Laufe des Jahres 2020. Die Daten verbleiben auch hier in Deutschland, die Server werden aber an das internationale Netzwerk angeschlossen. Der Konzern bekennt sich zur Einhaltung der DSGVO und plant für die Cloud-Dienste eine Zertifizierung nach dem C5-Prüfungskatalog des BSI. Neukunden haben die Wahl zwischen den neuen Regionen in Deutschland und weiteren verfügbaren Regionen in Europa. Bestandskunden können die derzeit verfügbaren Cloud-Dienste nutzen oder ihre Daten migrieren. Microsoft gibt dafür noch in diesem Jahr erste Details bekannt.

(nb@ix.de)

Bare-Metal-Clouds flexibler mit OpenStack Rocky einrichten

Die 18. Release der quelloffenen Cloud-Infrastruktur-Software bietet vor allem Verbesserungen in Ironic, dem Bereitstellungsdienst für reine Hardwaresysteme, und Fast-Forward-Aktualisierungen.

Zur Unterstützung von Edge Computing, Netzwerkfunktionsvirtualisierung und maschinellem Lernen gehen Unternehmen über die Virtualisierung hinaus und stellen Container auf Bare Metal bereit. OpenStack-Bare-Metal-Clouds unter Ironic legen dafür den Grundstein. Dieses Fundament ermöglicht den Betrieb von virtuellen Maschinen und Containern auf derselben Infrastrukturplattform, so Julia Kreger, Leiterin des OpenStack-Ironic-Projektteams.

OpenStack Ironic erweitert die Bare-Metal-Infrastruktur um ausgereiftere Management-

und Automatisierungsfunktionen und ermöglicht als Nova-Treiber die Mandantenfähigkeit. Benutzer können die physische Infrastruktur genauso verwalten, wie sie es von virtuellen Maschinen gewohnt sind. Dies erreichen sie mit Conductor Groups, benutzerverwalteten BIOS-Einstellungen und einer Schnittstelle für RAM-Disk-Deployment.

Das Fast Forward Upgrade (FFU) ermöglicht es Anwendern, schneller und einfacher zu neuen OpenStack-Versionen zu kommen. TripleO-Benutzer können so von der N-Release auf die N+3-Release aktualisieren. Bisher blieben die Nutzer älterer Versionen von den Neuerungen ausgeschlossen. Die neuen Funktionen sind seit der Veröffentlichung von Rocky freigegeben.

(nb@ix.de)

Kurz notiert

Nextcloud 14 ist jetzt verfügbar. Neu in der freien Cloud-Software sind die Videoverifizierung, mit der die Passwortfreigabe über einen Videoanruf erfolgt, die Zwei-Faktor-Authentifizierung über

die Messenger Signal und Telegram sowie Anpassungen zur Einhaltung gesetzlicher Vorschriften wie der DSGVO.

Die **Deutsche Telekom** hat in Biele bei Magdeburg ein neues **Cloud-Rechenzentrum** eröffnet. Auf 11 000 Quadratmetern stehen nun 150 Petabyte Speicherplatz zur Verfügung.

CANCOM Pironet C5-zertifiziert

Der Anforderungskatalog C5 (Cloud Computing Compliance Controls Catalogue) des Bundesamts für Sicherheit in der Informationstechnik beurteilt die Informationssicherheit



von Cloud-Diensten. In 17 Anforderungsbereiche aufgeteilt, darunter Mobile Device Management, Asset Management, Verschlüsselung, Compliance und Datenschutz, gehört er laut BSI-Präsident Arne Schönbohm zum Branchenstandard für eine sichere Cloud. Behörden und andere Einrichtungen des Bundes dürfen nur solche Cloud-Dienste nutzen, die die C5-Zertifizierung erhalten haben. Dem mittelständischen Unternehmen CANCOM Pironet ist es als erstem deutschen Multi-Cloud-Provider gelungen, den C5-Standard zu erfüllen. Das Zertifikat wurde von Wirtschaftsprüfern von Ebner Stolz ausgestellt, einer der größten Prüfungs- und Beratungsgesellschaften Deutschlands.

(nb@ix.de)

Morpheus Data unterstützt jetzt auch Ansible Tower

Das Start-up Morpheus Data hat die neue Release seiner gleichnamigen Cloud-Management-Plattform vorgestellt, die insbesondere die Schnittstellen zu Drittanbieter-Managementlösungen erweitert. Konkret ergänzen neue SDN-Features die bestehende VMware-NSX-API um Funktionen für den Umgang mit Software-defined Networks, wozu die Technik im Hintergrund auf VMwares vSphere und vCloud Director zurückgreift. Mit dieser Version hat Morpheus auch php-IPAM in seine Liste der IP-Adressmanagement-Integrations von Drittanbietern aufgenommen, die Infoblox und Bluecat bereits enthält.

Schließlich soll Morpheus nun auch Ansible Tower unterstützen, womit der bestehende Support für das Automatisierungsframework Ansible nun auch Daten via API aus Red Hats Monitoringplattform bietet.

Morpheus Data integriert nach eigenen Angaben Schnittstellen zu über 75 Drittanbieterprodukten unter dem Dach seiner Cloud-Management-Plattform, was das Provisioning und das Deployment in Enterprise-Umgebungen gegenüber anderen Lösungen spürbar beschleunigen soll. Die neue Version steht den Kunden des Unternehmens ab sofort zur Verfügung.

(nb@ix.de)

ownCloud Foundation ins Leben gerufen

ownCloud und sieben weitere Institutionen und Firmen haben im August die ownCloud Foundation gegründet. Ziele der Stiftung sind, die Entwicklercommunity zu unterstützen, Arbeitsgruppen zu gründen, technische Verbesserungen umzusetzen und den Wissensaustausch zu fördern. Entwickler und Anwender erhalten verschiedene gemeinsame Ressourcen. Damit soll die Verbreitung der Plattform erhöht und ihre Wettbewerbsfähigkeit

geschaffen und nachhaltig erhalten werden.

Die Mitgliedschaft in der ownCloud Foundation ist kostenlos und für jedermann zugänglich. Die Leitung übernehmen Vertreter von Organisationen und zwei Communitymitglieder: CERN, Konica Minolta Business Solutions, AARnet, Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen (GWDG), ownCloud, GEANT und ETH Zürich.

(nb@ix.de)

Microsoft integriert Office-Apps

Einordnen

Moritz Förster

Inzwischen bietet Microsoft viele Apps für die interne Kommunikation an und tut einiges für ihre Integration.

Mit Skype for Business und Teams bietet Microsoft zwei Dienste für die Zusammenarbeit im Unternehmen an. So kündigten die Entwickler an, dass Skype for Business künftig als Onlinevariante in Teams zur Verfügung stehen soll (zu allen Links siehe ix.de/ix1810027). Außerdem sollen beide Applikationen Informationen des Nutzers austauschen können, darunter den aktuellen Status, externe und interne Chats sowie die Kontakte. Meetings lassen sich nun mit bis zu 250 Teilnehmern einrichten, die Sitzungen lassen sich optional in der Cloud aufzeichnen. Ferner arbeitet Microsoft daran, seinen Übersetzungsdiensst zu integrieren.

Zudem soll ein Teilnehmer eines Meetings in Teams immer angemeldet bleiben, selbst wenn die Netzverbindung seines Clients ausfällt. Ist er wie-

der online, kann er ohne ein erneutes Eingeben seiner Daten auf den Dienst zugreifen. Wer das Teams Conferencing Gateway einsetzt, kann nun Anwender per Telefon zuschalten. Voraussetzung ist, dass es sich um ein für Skype for Business zertifiziertes SIP-Gerät handelt. Das Videokonferenzsystem Skype Room Systems und der Großbild-all-in-one Surface Hub erhalten ebenfalls ein Update, das unter anderem eine neue Teams-Applikation einführt.

Auch für das reguläre Skype gibt es Änderungen: Optional lassen sich Chats, Anrufe und Dateien nun Ende-zu-Ende verschlüsseln. Allerdings lässt sich pro Gerät maximal eine verschlüsselte Konversation einrichten. Gleichzeitig kann die neue Skype-Version Anrufe aufzeichnen. Alle Teilnehmer eines Gesprächs erhalten dann eine Benachrichtigung und auch übertragene Dateien sichert der Dienst ab. Anschließend steht der Mitschnitt 30 Tage im zugehörigen Chat der Unterhaltung zur Verfügung, er lässt sich zudem lokal sichern.

Darüber hinaus kündigte Microsoft an, seine Cloud-Dienste OneDrive for Business und SharePoint Storage Services mit KI- und ML-Funktionen zu erweitern. So sollen Nutzer Informationen schneller finden, insbesondere wenn sie Teil von Video- oder Audioaufnahmen sind. Diese transkribieren die Dienste automatisch, damit Inhalte bei der Suche zur Verfügung stehen. Des Weiteren empfiehlt der Dateimanager dem Anwender Daten, die für ihn relevant sein könnten. Die Tipps basieren auf dem analysierten Verhalten seiner Kollegen. (fo@ix.de)

1 of 2 Next > X ⓘ

Video transcript

Quelle: Microsoft

Search

05:14 When answering customer calls, it is important to understand the customer perspective

05:22 and their pain points before jumping into a solution.

05:28 Often, if can be helpful to pause and take detailed notes.

05:33 In this situation, Alyse is asking the customer to clarify more details

05:37 on the problem that the customer is facing

05:44 The customer explains that they have had mixed results with the company's new product line

05:50 Alyse is a subject matter expert, and is able to weigh in with insights.

05:56 If she had not been an expert, she could have taken a note

Alle Links: www.ix.de/ix1810027

Auf Nummer sicher

J. Forshaw

Netzwerkprotokolle hacken

Sicherheitslücken verstehen, analysieren und schützen

2018, 366 Seiten

€ 36,90 (D)

ISBN 978-3-86490-569-8



M. Messner

Hacking mit Metasploit

Das umfassende Handbuch zu Penetration Testing und Metasploit

3. Auflage

2018, 594 Seiten

€ 46,90 (D)

ISBN 978-3-86490-523-0



K. Schmeh

Kryptografie

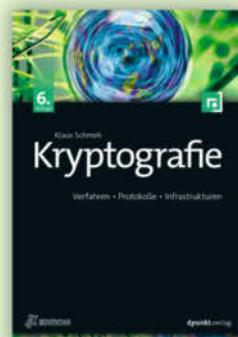
Verfahren, Protokolle, Infrastrukturen

6. Auflage

2016, 944 Seiten

€ 54,90 (D)

ISBN 978-3-86490-356-4



N. Dhanjani

IoT-Hacking

Sicherheitslücken im Internet der Dinge erkennen und schließen

2016, 302 Seiten

€ 34,90 (D)

ISBN 978-3-86490-343-4



M. Spreitenbarth

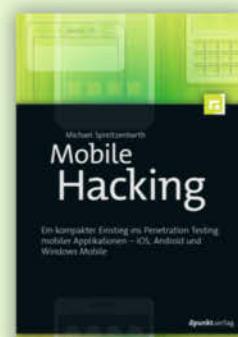
Mobile Hacking

Ein kompakter Einstieg ins Penetration Testing mobiler Applikationen – iOS, Android und Windows Mobile

2017, 236 Seiten

€ 29,90 (D)

ISBN 978-3-86490-348-9



dpunkt.verlag

www.dpunkt.de

plus+
Buch + E-Book:
www.dpunkt.plus

Helidon: Framework für Microservices

Unter dem Namen Helidon hat Oracle ein neues Java-Framework für Microservices in zwei Varianten vorgestellt. Einerseits Helidon SE, das das Java Development Kit (JDK) als Runtime einsetzt und wenige Funktionen bietet, dafür aber „leichtgewichtig“ daherkommen soll. Auf der anderen Seite steht Helidon MP (MicroProfile), das Eclipse MicroProfile implementiert und für Java-EE-Entwickler eine ähnliche Nutzererfahrung bieten soll. Helidon liegt derzeit in Version 0.9.1 vor, befindet sich also noch im Aufbau, kommt aber bereits in vielen internen Oracle-Projekten zum Einsatz.

Die Helidon-SE-Variante gliedert sich in drei Teile: Config, Security und RxServer. Damit sollen Entwicklern alle Werkzeuge zum Erstellen



eines Microservice zur Verfügung stehen. Darüber hinaus ist es möglich, das Metrics-Interface von MicroProfile in Helidon SE zu implementieren – jedoch ohne Support für Injection. Helidon MP setzt auf MicroProfile 1.1 auf und verfügt über die Komponenten JSON-P, JAX-RS/Jersey und CDI, die für die Implementierung notwendig sind.

Oracle habe erkannt, dass sich die Entwicklung in Zeiten von Cloud und Microservices verändern muss. Bisher war es zwar möglich, mit Projekten wie Eclipse Microprofile Microservices mit Java EE zu bauen, allerdings wollte Oracle eine Sammlung von Bibliotheken anbieten, die keinen Applikationsserver benötigen und in Java-SE-Applikationen Verwendung finden können. (bbo@ix.de)

Kurz notiert



Die **Versionsverwaltung GitLab 11.2** bietet eine JavaScript-Vorschau in der Web-IDE.

Facebooks **Hip Hop Virtual Machine (HHVM)** erhält in **Version 3.28** neue Ausdrücke für Type Testing und Type Assertion.

Apache HAWQ, die SQL-Abfrage-Engine für Hadoop, hat den Sprung zum Top-Level Project der Apache Software Foundation vollzogen.

Mit **TomEE 7.1** sind nun – auf dem Weg zur Kompatibilität mit Java/Jakarta EE 8 – alle Java-8-APIs im Anwendungsserver verfügbar.

OIO
Orientation in Objects

Wir suchen Dich!

* Java Senior Consultant (m/w)

* Java Consultant (m/w)

* Atlassian Consultant (m/w)

Werde Teil des bunten Teams aus Java-Experten in Mannheim - work@oio.de

[Schulung] [Beratung] [Entwicklung]

OIO · Orientation in Objects GmbH | Weinheimer Str. 69 | 68309 Mannheim | Tel. +49 621 71839-0 | Fax +49 621 71839-50 | info@oio.de | www.oio.de

Neu auf heise Developer

Java-Entwickler finden auf dem von iX betriebenen Online Channel gleich zwei Beiträge zu Microservices: ein Interview mit Michael Nygard sowie eine Erörterung der Frage, warum ein Domain-Model in die verkehrte Richtung führen kann. Darüber hinaus finden sich Artikel zu Rust als sicherer Programmiersprache, den Neuerungen von C# 7.3 sowie ein Überblick zu den Auswirkungen von Oracles neuem Java-Releasezyklus. Ein Mehrteiler zu Vue.js führt in die Umsetzung komplexer Webanwendungen mit dem JavaScript-Framework ein und ein Rechtsbeitrag zu „Common Clause“ wirft einen kriti-

schen Blick auf restriktive Lizenzierung von Open Source.

Die von *heise Developer* im vierten Quartal organisierten Konferenzen freuen sich auf Besucher. Die *heise devSec()* vom 16. bis 18. Oktober richtet sich an Security-Spezialisten, bei der Continuous Lifecycle/ContainerConf vom 13. bis 16. November dreht sich alles um CD, DevOps und Container. In Zusammenarbeit mit *The Register* organisiert *heise Developer* außerdem in London die ML-Konferenz Minds Mastering Machines (15. bis 17. Oktober) sowie erstmals die Serverless Computing (12. bis 14. November). (map@ix.de)

Jenkins wird Cloud Native

Der Continuous-Integration-Server (CI) Jenkins soll nach dem Wunsch von Kohsuke Kawaguchi, Jenkins-Erfinder und CTO von CloudBees, in einer Cloud-Native-Version erscheinen. Cloud Native Jenkins soll die Container-Orchestrierung Kubernetes als Laufzeitumgebung nutzen, damit das Projekt auf Serverless beziehungsweise Function as a Service (FaaS) als Build-Ausführung setzen kann und einige Funktionen separat als Microservices ausgerollt werden können. Diese Designprinzipien sollen dem CI-Server zu hoher Skalierbarkeit, Unveränderlichkeit und

Bedienbarkeit ohne Ausfallzeit verhelfen.

Während Cloud Native Jenkins auf die Zukunft in der Cloud setzt, soll sich auch Jenkins 2 weiterentwickeln – aber schneller. Inspiriert vom neuen Releasezyklus von Java SE soll Jenkins häufiger mit neuen Versionen aufwarten, um Nutzern früher wichtige neue Features zu liefern. Von der bisher vorherrschenden „Für immer kompatibel“-Mentalität nimmt Jenkins dadurch allerdings Abschied. Anwender sollten sich auf Breaking Changes und häufigere Migrationen einstellen. (bbo@ix.de)

Go 1.11 versteht sich auf WebAssembly

Entwickler können ihre Go-Programme neuerdings in das Binärformat WebAssembly kompilieren. Dadurch laufen sie clientseitig in den Browsern Firefox, Chrome, Safari und Edge. Derzeit erstellt der Compiler ein großes wasm-Modul, das neben dem Programmcode die Laufzeitumgebung von Go enthält, die sich unter anderem um die Garbage Collection und das Scheduling kümmert.

Dadurch haben die WebAssembly-Module eine minimale unkomprimierte Größe von 2 MByte. Damit Go-Programme JavaScript-Routinen aufrufen können, haben die Macher das derzeit als experimentell gekennzeichnete sys-

call/js-Package eingeführt. Für die erste Implementierung von WebAssembly hatte weder die Optimierung der Dateigröße noch das Zusammenspiel mit anderen Sprachen eine hohe Priorität.

Mit Veröffentlichung von Go 1.11 hält das Modulkonzept als Alternative zu Gopath Einzug in den Build-Prozess. Module sollen das Versionieren und den Umgang mit Dependencies vereinfachen. Als Modul gilt dabei eine Sammlung zusammengehöriger Go-Pakete. Die Definition erfolgt über eine *go.mod*-Datei, die eine Baumstruktur mit Go-Source-Dateien enthält. (rme@ix.de)

Abgewandelt: Apple präsentiert neue iPhones

Noch schickt Apple seine iPhone-X-Serie nicht in Rente – die Modelle Xs, Xs Max und Xr bieten einige neue Funktionen und schnellere Hardware.

Apple hat seine beiden neuen iPhone-Spitzenmodelle Xs und Xs Max vorgestellt. Während das Xs wie gehabt ein 5,8-Zoll-Display mit einer Auflösung von 2436 × 1125 Pixeln erhält, bietet das Xs Max einen 6,5-Zoll-Bildschirm mit einer Auflösung von 2688 × 1242 Pixeln. Bei beiden Ausführungen handelt es sich um ein OLED-Panell. Neu ist der im Vergleich zum iPhone X um 60 Prozent erhöhte Dynamikumfang – die Bildschirme passen die Farbtemperatur automatisch an das Umgebungslicht an und bieten darüber hinaus HDR.

Außerdem sollen beide Modelle dank einer IP68-Zertifizierung besser als bisher gegen Wasser und Staub geschützt sein. Ferner lassen sich iPhones erstmals mit zwei SIM-Karten verwenden, wobei es sich bei der ersten um eine fest integrierte eSIM handelt. Nur in China soll ein Modell mit zwei Steckplätzen für herkömmliche SIM-Karten erscheinen.

Die Designer steckten einige Arbeit in die Kameras: Auf den ersten Blick sind es dieselben wie beim iPhone X, denn auf der Vorderseite bieten die Smartphones eine 7-Megapixel- und auf der Rückseite eine 12-Megapixel-Kamera mit zwei Linsen und einer Blende von f/1.8 beziehungsweise f/2.4. Aber mit Smart HDR sollen Aufnahmen in schwierigen Lichtsituationen besser gelingen und außerdem eine bessere Tiefenschärfe bieten.

Mit an Bord ist ein neuer SoC: Apples A12 Bionic ist im 7-nm-Prozess gefertigt und soll 50 Prozent mehr Leistung als sein Vorgänger A11 bieten. Von der höheren Rechenleistung sollen insbesondere CoreML fürs maschinelle Lernen und ARKit für Augmented-Reality-Apps profitieren. Gleichzeitig soll das Xs 30 Minuten und das iPhone Xs Max 90 Minuten länger mit einer Akkuladung auskommen als das iPhone X.

Die günstigste Variante bietet 64 GByte lokalen Massenspeicher, mit ihm kostet das

Xs 1150 Euro und das Xs Max 1250 Euro. Hinzu kommen 256-GByte- und 512-GByte-Ausführungen. Der Handel soll beide Modelle ab dem 21. September führen.

Gleichzeitig stellte Apple das neue, günstige iPhone Xr vor. Es kommt mit einer geringen Auflösung von 1792 × 828 Pixeln bei einer Größe von 6,1 Zoll aus und verzichtet auf das Dualkamerasystem. Es kostet mit 64 GByte Speicherplatz 850 Euro und erscheint am 26. Oktober. (fo@ix.de)

Quelle: Apple Inc.



**Meine Daten bleiben
in Deutschland.**

gdata.de/virenschutz

Und nirgendwo sonst. Deutscher Hersteller, deutsche Datenschutzgesetze. G DATA hat sich dazu verpflichtet, keine Hintertüren für Geheimdienste offen zu lassen. Wir geben eine No-Backdoor-Garantie. Für echten Schutz vor Cyberkriminellen und Spionage. Ohne Kompromisse.

Setzen Sie jetzt auf die vielfach ausgezeichneten G DATA Businesslösungen. Mehr Infos auf www.gdata.de/business oder unter 0234 9762-170

itsa 2018
Besuchen Sie uns:
Halle 9, Stand 438

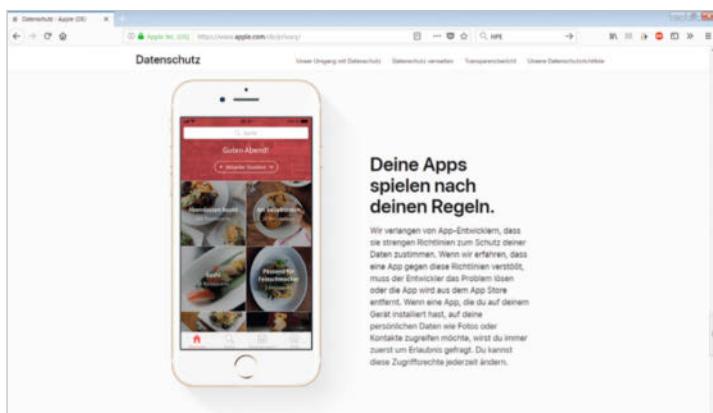
G DATA
G

TRUST IN
GERMAN
SICHERHEIT

Apple verlangt Datenschutzerklärungen

Ab 3. Oktober 2018 müssen alle Apps, die ab diesem Datum aktualisiert oder neu im App Store von Apple eingereicht werden, eine Datenschutzerklärung enthalten. Ein automatisches Sperren von Apps, die nicht aktualisiert werden, soll es jedoch nicht geben. Die Erklärung muss Angaben dazu enthalten, welche Nutzerdaten die App erfasst, wie die Datenerhebung erfolgt und wie die gesammelten Daten genutzt werden. Die

Datenschutzerklärung muss über eine Webseite und aus der App heraus „auf einfache Weise zugänglich sein“, heißt es bei Apple. Sie muss auch in die App eingebettete Analyse-Tools und SDKs von Drittanbietern und Werbeplattformen umfassen. Schließlich fordert Apple Angaben zur Datenaufbewahrung und zu den Nutzerrechten auf Wideruf einer Einwilligung sowie zur Löschung personenbezogener Daten. (ur@ix.de)



EU-US Privacy Shield im Visier

Das Europäische Parlament hat eine Resolution verabschiedet, wonach die EU-Kommission den EU-US-Privacy-Shield-Mechanismus so lange aussetzen soll, bis die USA die datenschützenden Vereinbarungen verbessert haben. Die Resolution ist für die EU-Kommission nicht bindend. Im Herbst 2018 steht ohnehin eine Evaluation

der Vereinbarungen an. Eine heftige Auseinandersetzung darüber, ob die USA ein angemessenes Datenschutzniveau gewährleisten, ist zu erwarten. Kippt die Vereinbarung, stehen Unternehmen erneut vor dem Problem, wie sie rechtskonform personenbezogene Daten an Vertragspartner in den USA übermitteln können. (ur@ix.de)

Kurz notiert

Ein Beschluss des Ministerrats Bayerns verpflichtet die Datenschutzbehörden dazu, die Ziele der **Datenschutz-Grundverordnung**, „sachgerecht und mit Augenmaß“ zu verfolgen. Amateursportvereine, Musikkapellen und andere ehrenamtlich organisierte Vereine sollen keinen Datenschutzbeauftragten bestellen müssen.

Nach einer neuen **EU-Richtlinie** werden **Betrug und Fälschungen** beim bargeldlosen Zahlungsverkehr künftig mit Mindeststrafen von drei bis fünf Jahren Haft belegt. Das betrifft Kredit- und Giro-

karten, aber auch Kryptogeld und Smartphone-Zahlungen.

Mit der Ablehnung internationaler Abkommen über die Kontrolle **autonomer Waffensysteme** durch die USA und andere Rüstungsmächte sind die Verhandlungen internationaler Abrüstungsexperten gescheitert. Gefordert wurde unter anderem, dass beim Einsatz tödlicher Waffen Menschen weiterhin die letzte Entscheidung treffen sollten.

Ein US-Gericht hat die Verwertung von **Daten aus Smart Meters** eingeschränkt. Danach darf der Stromversorger sie für eigene Zwecke speichern, aber nicht an Dritte weitergeben oder für an-

Schadenersatz bei Lizenzverstoß

Wer die Rechte eines Urhebers etwa von Fotos und Bildern verletzt, ist diesem zum Schadenersatz verpflichtet. Dieser Rechtsgrundsatz ist unstrittig. Jüngst hat das Landgericht Frankfurt am Main (Az. 2-03 O 32/17) zur Höhe eines solchen Schadenersatzes Stellung genommen, wenn Bilder unter einer Creative-Commons-Lizenz lizenziert werden. Bei der unberechtigten Fotonutzung wenden deutsche Gerichte seit Jahren die sogenannte „MFM-Tabelle“ an, um die Schadenersatzhöhe festzulegen. Hinter MFM verbirgt sich die Mittelstandsge meinschaft Foto-Marketing, ein Arbeitskreis des Bundesverbandes professioneller Bildanbieter e. V. Auf deren Webseite

ist zu lesen: „Die Mittelstands gemeinschaft Foto-Marketing (MFM) ermittelt jährlich die aktuellen Honorare für Fotonutzungen in Deutschland und gibt diese unter dem Titel Bildhonorare als Broschüre heraus.“ Die LG-Richter schließen deren Anwendbarkeit bei Creative-Commons-Lizenzen nun aus. In einem solchen Fall muss der Rechteinhaber vielmehr die Höhe des ihm entstandenen Schadens konkret nachweisen, heißt es in der Entscheidung. Denn ein Urheber soll keine hohen Lizenzgebühren für die rechtswidrige Nutzung eines Bildes verlangen können, wenn dieses ansonsten kostenlos unter einer CC-Lizenz genutzt werden darf. (ur@ix.de)

DSGVO überfordert Aufsichtsbehörden

Heute online liegen Schreiben zu Datenschutzbeschwerden vor, in denen die Landesbeauftragte für den Datenschutz Berlin auf längere Bearbeitungszeiten als vorgesehen hinweist. Die Datenschutz-Grundverordnung (DSGVO) verlangt von den Aufsichtsbehörden, dass sie innerhalb von drei Monaten ab Beschwerdeeingang das Ergebnis ihrer Untersuchung mitteilen. Zumindest muss über den Stand des Verfahrens informiert werden, wenn die Untersuchung nicht rechtzeitig abgeschlossen werden kann. Personalmangel bei einer Aufsichtsbehörde zählt nicht zu den Gründen,

die eine verspätete Mitteilung rechtfertigen.

Auch bei der Bundesbeauftragten für den Datenschutz kommt es nach Heise-Recherchen zur schleppenden Bearbeitung von Beschwerden. Sollte sich die Situation nicht verbessern, droht Deutschland ein EU-Vertragsverletzungsverfahren wegen nicht ordnungsgemäßer Umsetzung der DSGVO. Der Landesbeauftragte für Datenschutz in Baden-Württemberg Stefan Brink spricht davon, dass die Anzahl an Beschwerden nach Wirksamwerden der DSGVO weiterhin „auf hohem Niveau“ sei, insgesamt aber nachlässe. (ur@ix.de)

Gerichtsstreit um Exploits beigelegt

Mit einer Klage um Rechte und Pflichten von Exploit-Entdeckern hat die Promon AG, ein Entwickler von Sicherheitssoftware für Banken, Aufmerksamkeit erregt. Wissenschaftler aus Erlangen und München hatten mehrere Schwachstellen in dieser Sicherheitssoftware entdeckt und darüber berichtet. Daraufhin mahnte das Softwareunternehmen die Wissenschaftler ab. Die Abmahnung und den anschließenden Antrag auf einstweilige Verfügung begründete es mit Verstößen gegen das Urheberrecht. Der Rechtsstreit endete nun mit einem Vergleich.

Promon hatte moniert, willkürlich ausgewählt worden zu sein, und verwies darauf, dass es auch bei Konkurrenten vergleichbare Sicherheitsrisiken gebe. Kritisiert wurde auch, dass das Unternehmen erst durch Presseveröffentlichungen auf die Exploits aufmerksam wurde und man ihm keine

technischen Details mitgeteilt hatte. Seine Klage stützte Promon auf das Urheberrecht, da das Wettbewerbsrecht in diesem Fall gegen die Wissenschaftler nicht weiterhalf. Unter Vermittlung des Gerichts wurde in dem Vergleich ein Verfahren zur „Responsible Disclosure“ (etwa verantwortungsvolle Offenlegung) aufgenommen, das zwischen den Interessen beider Seiten vermitteln soll.

Starre Fristen sind ungeeignet

Der Vergleich sieht vor, dass die Entdecker zunächst das betroffene Unternehmen über die Sicherheitslücke informieren sollen. Dabei ist ein Termin zu nennen, bis zu dem sie die Veröffentlichung ihrer Erkenntnisse zurückhalten, damit das Unternehmen den Exploit rechtzeitig beseitigen kann. Hierzu kann das betroffene Unternehmen einen Gegenvorschlag

unterbreiten. Starre Fristen sind nach Auffassung des Gerichts ungeeignet, da Exploits unterschiedlich gravierende Schwachstellen betreffen können und ihre Beseitigung unterschiedlich lange Zeit in Anspruch nehmen kann. Für den Fall, dass das Unternehmen während der „Stillhaltezeit“ gerichtlich gegen die Exploit-Entdecker vorgeht, haben diese das Recht, Journalisten „als Moderatoren“ hinzuzuziehen.

Der Vergleich gilt nur zwischen den beiden beteiligten Parteien. Responsible Disclosure ist nicht neu und wird in vielen Fällen bereits praktiziert. Große Unternehmen haben in der Vergangenheit oftmals sogenannte „Bug Bounties“, also Prämien für die Entdeckung von Softwareschwachstellen, bezahlt. Voraussetzung hierfür war in der Regel eine Stillhaltezeit zur Beseitigung der Exploits vor deren Veröffentlichung. (ur@ix.de)

EuGH soll Vorratsdatenspeicherung erneut bewerten

Vor dem Bundesverfassungsgericht sind zahlreiche Verfassungsbeschwerden gegen die sogenannte Vorratsdatenspeicherung anhängig. Die juristischen Auseinandersetzungen dazu beschäftigen die Gerichte bereits seit vielen Jahren. Auf Wunsch der Bundesregierung soll vor dem ursprünglich noch für dieses Jahr erwarteten Urteil des Bundesverfassungsgerichts

eine Vorlage an den Europäischen Gerichtshof erfolgen. Solche Vorlagen nehmen mittlerweile Jahre in Anspruch. Konkret geht es um die Frage, ob die 2015 in Deutschland eingeführte „abgeschwächte Form“ der Vorratsdatenspeicherung auch gegen die zuvor zur alten Rechtslage ergangenen Urteile des EuGH verstößt. Die 2015 eingeführte Regelung

beschränkt das Speichern „auf bestimmte Kommunikationsmittel wie Telefondienste und Internetzugangsdienste“ und auf „nur bestimmte Datenkategorien“. Datenschützer kritisieren das Vorgehen der Bundesregierung und verweisen darauf, dass aus ihrer Sicht die EuGH-Urteile eindeutig seien. Entscheiden muss nun das Bundesverfassungsgericht. (ur@ix.de)

Google wegen Java-API-Packages verurteilt

Das US-Berufungsgericht für den Bundesgerichtsbezirk hat Google wegen der Nutzung von 37 Java-API-Packages verurteilt und Googles Verhalten als „nicht fair aus rechtlichen Gründen“ bezeichnet. Die API-Packages stammen aus der Java 2

Standard Edition, wofür Google einen eigenen Implementierungscode schrieb. Damit wollte Google Java-Entwickler motivieren, Apps für Android zu erstellen. Zuvor hatte der Bundesgerichtshof festgestellt, „dass [der] deklarierende Code

und die Struktur, Reihenfolge und Organisation („SSO“) der Java-API-Pakete Anspruch auf Urheberrechtsschutz haben“. Google hatte sich auf ein Recht auf „Fair Use“ berufen, was gerichtlich jedoch abgelehnt wurde. (ur@ix.de)

Lizenz für frei zugängliche Fotos

Der Europäische Gesetzgeber hat entschieden, dass ein Webseitenbetreiber auch dann eine Lizenz vom Urheber eines Fotos braucht, wenn es auf einer anderen Webseite frei zugänglich war (Az. C-161/17). Entscheidend ist, ob in der zwei-

ten Veröffentlichung eine (erneute) „öffentliche Wiedergabe“ zu sehen ist, was die EuGH-Richter bejahten. Wenn ein Rechteinhaber die Veröffentlichung eines Fotos im Internet genehmigt hat, bedeutet dies nicht, dass jeder beliebige

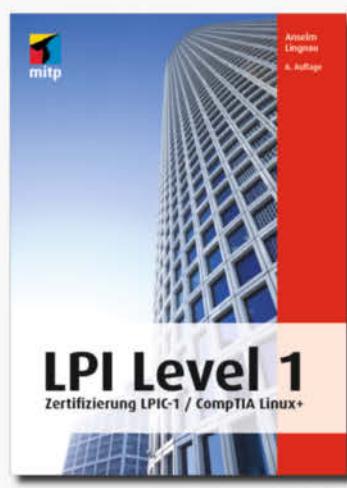
Dritte dieses Bild ebenfalls übernehmen darf. Die Richter sind der Ansicht, dass dadurch ein „neues Publikum“ erreicht wird. Für eine Zweitveröffentlichung ist eine eigenständige Lizenz vom Rechteinhaber erforderlich. (ur@ix.de)



216 Seiten | 19,99 €
ISBN 978-3-95845-555-9
www.mitp.de/555



280 Seiten | 33,00 €
ISBN 978-3-95845-595-5
www.mitp.de/595



544 Seiten | 33,00 €
ISBN 978-3-95845-297-8
www.mitp.de/297

Projektverwaltung aus der Open Source

Im Rahmen der Mitte September erschienenen Version 8.0 erhält das Programm zur Projektverwaltung OpenProject neben einer überarbeiteten Oberfläche unter anderem einen neuen Texteditor. Er beherrscht Makros, zum Beispiel zum Erstellen von Inhaltsverzeichnissen. Außerdem sollen Nutzer Dokumente und Bilder direkt aus MS Office kopieren und einfügen können.

OpenProject hält einige Menüpunkte standardmäßig vor, der Anwender kann aber auch eigene hinzufügen. Tabellen,

Statistiken und Balkendiagramme kann der Nutzer nun in vielen Seiten direkt ergänzen. Welche Informationen sie anzeigen, kann er außerdem je nach Bedarf anpassen.

Als freie Software steht OpenProject unter der GPLv3. Die OpenProject GmbH aus Berlin bietet darüber hinaus Support-Verträge für Unternehmenskunden und eine SaaS-Variante an. Für Nutzer dieser kostenpflichtigen Cloud- und Enterprise-Editionen stehen diverse zusätzliche Funktionen zur Verfügung. (fo@ix.de)

The screenshot shows the OpenProject web interface. On the left, there's a sidebar with navigation links like 'Work packages', 'Bugs', 'Gantt chart', 'Milestones', 'Tasks', and 'All open'. The main area has a title 'Demo project' and a sub-section 'All open'. It lists work packages with columns for ID, SUBJECT, TYPE, and STATUS. Some entries include 'Invite new team members...', 'Create work packages', 'Create a project plan', and 'Edit a work package'. Below this is a Gantt chart for August 2018, showing tasks like 'Great feature' and 'Terrible bug' with their start and end dates. A legend indicates task types: blue for invites, green for work packages, red for project plans, and orange for edits.

Intershop für Microsoft-Umgebungen

Intershop hat seine E-Commerce-Suite überarbeitet. Dabei setzt das Softwarehaus aus Jena wie angekündigt auf Microsoft. Unter anderem lässt sich die neue Version 7.10 der Intershop Commerce Suite nun in Microsofts ERP-Software Dynamics 365 for Finance and Operations integrieren. Das vermeidet doppelte Dateneingaben oder inkonsistente La-

gerbestände, da Informationen zu Aufträgen und Bestandsdaten zwischen der Verkaufs-umgebung und den betriebswirtschaftlichen Anwendungen synchronisiert werden. Mit der neuen Release der Intershop-Software haben Nutzer zudem die Option, den SQL Server 2017 von Microsoft statt Oracles Datenbank einzusetzen.

Achim Born (un@ix.de)

Webinare planen und auswerten

LogMeIn veröffentlichte eine neue Generation von GoTo-Webinar. Auffällig ist die neue Oberfläche des überarbeiteten Tools zum Planen und Organisieren von Webinaren. Beispielsweise erhalten Organisatoren auf einen Blick Informationen zu kommenden und vergangenen Veranstaltungen. Zudem wurde die neue Benutzeroberfläche für mobile Endgeräte optimiert, sodass sich nun von jedem beliebigen Bildschirm aus Veranstaltungen erstellen oder Teilnehmerlisten

überprüfen lassen. Hinzu kommen jetzt einige Werkzeuge zur Planungsunterstützung.

Dazu zählt das „Big Book of Webinar Stats“, das statistische Daten aus über 300 000 Webinaren umfasst. Die Nutzer erhalten Tipps für ihre Veranstaltungen, etwa zur Titelwahl oder zu Planungszeiten. Das Webinar-Tool ist auf die Kopplung an Marketingautomations- und CRM-Systeme wie AWeber, Hubspot, Unbounce und Zapier vorbereitet.

Achim Born (un@ix.de)

8-Bit-MCU-Boards mit Uno-Verbbindern

STMicroelectronics hat zwei Entwicklungsboards namens STM8 Nucleo vorgestellt. Sie erlauben den Zugriff auf sämtliche STM8-Mikrocontroller. Mit Arduino-Uno-Steckverbinder lassen sich die Boards um die quelloffenen Arduino-kompatiblen Shields erwei-

tern. Zudem können Entwickler Werkzeuge wie Cosmic IDEA Toolchain, die integrierte Entwicklungsumgebung IAR EWSTM8 sowie die kostenlose STVD IDE von ST mit den Boards nutzen (siehe ix.de/ix1810032).

Barbara Lange (sun@ix.de)

Oracles Umsatz enttäuscht die Analysten

Der US-amerikanische Softwarekonzern Oracle meldete einen wenig erbaulichen Auftritt ins Geschäftsjahr 2019. Im ersten Quartal (endete im August) verfehlte SAPs Erzrivale mit einem Umsatzwachstum von nur 1 % auf knapp 9,2 Milliarden Dollar die Erwartungen der Finanzanalysten. Die stören sich insbesondere am vergleichsweise schwachen Zuwachs der Sparte Cloud-Services und Lizenzsupport um 3 % auf 6,6 Milliarden Dollar. Der Bereich Cloud- und On-Premises-Lizenzen ging sogar um 3 % auf 867 Millionen Dollar zurück. Das chronisch schrumpfende Hardwaregeschäft kam noch auf 904 Millionen (-4 %), Dienstleistungen/allgemeine Beratung auf 813 Millionen Dollar (-5 %).

Oracles Betriebsergebnis belief sich auf 6,4 Milliarden US-Dollar (+1 %). Der Netto-gewinn stieg – auch wegen sinkender Steuerlasten – um 6 %

auf fast 2,3 Milliarden Dollar. Oracle-Chefin Safra Catz, die gemeinsam mit Mark Hurd den Konzern leitet, führte den starken Dollar als Ursache der schwachen Umsatzentwicklung an. Allerdings führt das bei Finanzakrobaten beliebte Herausrechnen der Wechselkurs-schwankungen beim Umsatzzplus zu einer Verbesserung um nur einen Prozentpunkt. Die Börsenanalysten irritiert zudem, dass Oracle anders als bisher das Cloud-Geschäft nicht mehr separat ausweist.

Ein detaillierter Vergleich mit der Konkurrenz ist folglich kaum noch möglich. Daran ändert eine alternative Rechnungslegung nichts, die sich in der Bilanzmeldung finden lässt. Hier weist das Unternehmen für die gesamte Anwendungssparte einen Umsatz von 2,76 Milliarden US-Dollar aus (+6 %). Plattform- und Infrastruktur-dienstleistungen erbrachten 4,7 Milliarden Dollar (+1%).

Achim Born (un@ix.de)

Kurz notiert



Laut Gartner werden in diesem Jahr 114 Mrd. Dollar weltweit für Sicherheitsprodukte und -services ausgegeben. 2019 sollen es 124 Mrd. Dollar (+8,7 %) sein.

Zum effizienteren Vorbereiten von Marketingkampagnen hat AB Tasty einen Marketplace entwickelt. Hier stehen fertige Widgets wie Pop-ups und Banner bereit, die sich zum Aufbau von Websites für Onlineshops an das eigene Corporate Design anpassen lassen.

Cisco entdeckt für seine WLAN-APs das Geschäft mit Kleinunternehmen. Unter dem Namen Meraki Go bringt der Konzern ein Komplett paket auf den

Markt, das sich mittels App binden weniger Minuten konfigurieren und einfach verwalten lassen soll.

Die TU Berlin nutzt seit Ende 2017 den pdfaPilot von callas software zum Konvertieren und Validieren von PDF-/A-Dateien. Die Software ist als Kommandozeilentool in eine Weboberfläche integriert. Die Implementierung liegt als Open-Source-Code auf GitHub.

SoftMaker bietet seine Programmsammlung Office 2018 künftig für Bildungseinrichtungen und Lehrkräfte kostenlos an. Schüler und Studenten zahlen je Lizenz 10 statt 70 Euro, sofern sie sie per Sammelbestellung mindestens zehn Lizzenzen beziehen.

Mobile Erreichbarkeit belastet die Psyche

Wer nach Feierabend noch dienstliche E-Mails checkt oder einen Kunden zurückruft, riskiert negative Auswirkungen auf sein Wohlbefinden am nächsten Arbeitstag. Das haben Psychologen des Leibniz-Instituts für Arbeitsforschung an der TU Dortmund in einer Tagebuchstudie mit 63 Probanden herausgefunden.

Demnach benötigt man viel Energie, um zwischen seinen

Rollen als Beschäftigter und Privatperson hin- und herzuspringen. Gleichzeitig gilt es, konzentriert zu bleiben. Viele Menschen reagieren dann sensibler auf Belastungen bei der Arbeit und erschöpfen schneller. Wer allerdings nach der beruflichen Smartphone-Nutzung gut und ausreichend lange schläft, spürt diesen Effekt am Folgetag kaum (siehe ix.de/ix1810033). (jd@ix.de)

Intrapreneurship wird vernachlässigt

Viele Unternehmen suchen nach neuen Geschäftsideen, zapfen aber die Kreativität der eigenen Belegschaft kaum an: Nur sieben Prozent der Firmen ab 20 Mitarbeitern nutzen spezielle Programme oder Projekte, in denen die Angestellten Vorschläge entwickeln können. Das hat der Branchenverband Bitkom herausgefunden.

In mittelständischen Betrieben mit 100 bis 499 Mitarbei-

tern ist dieses „Incorporate Entrepreneurship“ oder „Intrapreneurship“ etwas stärker ausgeprägt (14 Prozent), in Großunternehmen mit 500 und mehr Beschäftigten unterstützen 22 Prozent solche Projekte. Zu den beliebtesten Fördermaßnahmen gehören Geld, Räume, technische Geräte, Weiterbildung und Coaching. Befragt wurden 604 Unternehmen ab 20 Mitarbeitern. (jd@ix.de)

Kurz notiert

Laut IT-Freelancer-Portal Gulp spielt die Personalabteilung bei der **Rekrutierung von Projektmitarbeitern** nur noch eine geringe Rolle: Zwei Drittel der freien IT-Experten werden über die jeweiligen Fachabteilungen oder den Einkauf beauftragt.

Mitarbeiterbindung ist das Zukunftsthema des Personalmanagements, wie die BWA Akademie Bonn im Rahmen der

Studie „Trendreport – Digitalisierung und Arbeitsmarkt 2018“ feststellt. 92 von 100 Personalexperten haben das angegeben.

Die **Frauenquote in Informatik-Studiengängen** liegt zurzeit bei 19,4 Prozent – nur unwesentlich höher als bei der Einführung dieses Studienfachs im Wintersemester 1970/71. Die Studie des CHE Centrums für Hochschulentwicklung „Frauen in Informatik“ untersucht die Hintergründe (siehe ix.de/ix1810033).

Führungsqualitäten müssen sich ändern

Digitalisierung stellt neue Erwartungen ans Management. So dürfen dort in Zukunft nicht mehr reine Entscheider wirken, sondern eher „Entwickler und Begleiter“ sowie „Vernetzer und Ermöglicher“. Zu diesem Ergebnis kommen das Fraunhofer-Institut für Arbeitswirtschaft und Organisation und die Deutsche Gesellschaft für Personal-

führung in ihrer Studie „Führung in der digitalen Transformation“. 91 Prozent der 140 befragten Personalverantwortlichen erwarten in der Zukunft ein verändertes Rollenverständnis. Gleichzeitig glauben 38 Prozent, dass Führungsfunctionen dadurch an Attraktivität verlieren (siehe ix.de/ix1810033). (jd@ix.de)

EXPERTEN FÜR
IT-SICHERHEIT
GEH ICH GERN
INS NETZ*

NICK BECKER,
IT-SECURITY ENGINEER

* Die it-sa bietet Trends und Innovationen der IT-Security-Branche sowie Expertenvorträge.



Sichern Sie sich
jetzt Ihr
Gratis-Ticket!

it-sa 2018
Die IT-Security Messe und Kongress

**HOME OF
IT SECURITY**

Servermarkt gedeiht gut – Dell löst HPE als Marktführer ab

Das weltweite Servergeschäft erholt sich zusehends. Im vierten Quartal nacheinander legte es im Jahresvergleich zu, im zweiten Quartal 2018 sogar besonders deutlich: Laut IDC durften sich die Hersteller über ein beeindruckendes Wachstum um 43,7 % auf 22,5 Mrd. Dollar freuen. Sie mussten dazu mit 2,9 Mio. lediglich ein Fünftel mehr Serversysteme verkaufen. Günstigere Volumenmodelle erbrachten insgesamt 18,4 Mrd. Dollar (+42,7 %). Mit dem Verkauf von Servern der mittleren Leistungsklasse erzielten die Hersteller rund 2,5 Mrd. Dollar Umsatz (+63 %), im High-End-Sektor 1,7 Mrd. Dollar (30,4 %).

Laut IDC spielen die Servererneuerung in den Rechenzentren und eine steigende Nachfrage bei Cloud-Service-Providern den Herstellern in die Karten. In den Unternehmen setze sich der Trend fort, eigene Cloud-ähnliche Infrastrukturen für eine neue Anwendungsgeneration aufzubauen. Die großen Cloud-Provider, auch als Hyperscaler tituliert, investierten wiederum kräftig in den Ausbau ihrer

RZ. Davon profitieren vornehmlich sogenannte ODM-Hersteller, die Servermodelle nach Vorgaben der Kunden produzieren. Im zweiten Jahresquartal konnten die meist chinesischen oder taiwanischen Hersteller ihren Umsatz um knapp 56 % auf 5,5 Mrd. Dollar und den Marktanteil um zwei Prozentpunkte auf 24,4 % ausbauen.

Nummer eins unter den Herstellern sowohl nach Umsatz

als auch nach Absatz wurde im zweiten Quartal 2018 erstmals Dell. Der US-Konzern stieß damit Hewlett Packard Enterprise (HPE) vom Thron.

Ein Grund für das vergleichsweise niedrige Umsatzwachstum um 11,7 % auf 3,74 Mrd. Dollar besteht darin, dass HPE inzwischen die Politik „Gewinn vor Marktanteil“ verfolgt. Und tatsächlich ging die Absatzzahl im zweiten Quartal um 12,4 % zurück. IBM, die Nummer drei, profitierte von guten Geschäften mit Mainframes und Power-Servern (1,64 Mrd. Dollar, +57 %). Am schnellsten wuchs der Umsatz indes bei Lenovo (+85 %), Inspur (+112 %) und Huawei (+77 %). (un@ix.de)



Dell-Server verkauften sich im zweiten Quartal besonders gut.

Servermarkt nach Umsatz (Mrd. Dollar) ...

Hersteller	Q2/2018	Marktanteil	Änderung
Dell Inc.	4,246	18,8 %	52,9 %
HPE/New H3C Group	3,741	16,6 %	11,7 %
IBM	1,638	7,3 %	57,0 %
Lenovo	1,549	6,9 %	85,7 %
Inspur	1,088	4,8 %	112,3 %
Cisco	1,070	4,8 %	22,4 %
Huawei	0,967	4,3 %	77,1 %
Auftragsfertiger (ODM Direct)	5,488	24,4 %	55,9 %
andere	2,742	12,2 %	23,1 %
Gesamtmarkt	22,529	100,0 %	43,7 %

... und nach Absatz (in 1000 Stück)

Hersteller	Q2/2018	Marktanteil	Änderung
Dell Inc.	574,6	19,5 %	16,6 %
HPE/New H3C Group	443,7	15,1 %	-12,4 %
Lenovo	224,1	7,6 %	53,9 %
Inspur	203,2	6,9 %	69,8 %
Huawei	187,4	6,4 %	39,9 %
Super Micro	175,1	5,9 %	28,8 %
Auftragsfertiger	732,6	24,9 %	39,0 %
andere	403,0	13,7 %	5,9 %
Gesamtmarkt	2943,8	100,0 %	20,5 %

DSGVO dämpft den Werbemarkt

Der Online-Vermarkterkreis (OVK) im BVDW (Bundesverband Digitale Wirtschaft) schraubt seine Wachstumsprognose für 2018 aus dem Februar herunter. Statt mit 10 % rechnet der Verband jetzt nur noch mit 7 % Wachstum auf insgesamt 2,06 Mrd. Euro Nettoausgaben für Online- und mobile Werbung. Als eine Ursache führten die Branchenvertreter die Versunsicherung im Markt rund um die EU-Datenschutz-Grundverordnung (DSGVO) an. Seit Juni ist laut Statistik aber wieder eine gewisse Normalität eingekehrt. Mit einem Umsatz von 162,6 Mio. Euro wurde sogar ein neuer monatlicher Höchstwert für die erste Jahreshälfte erzielt. Angetrieben wird das Wachstum zurzeit von der mobilen sowie programmativen und datenorientierten Auslieferung – also vom automatischen Verkauf von Werbeplänen in Echtzeit.

Die Bedeutung der Online-Werbung respektive des Internets allgemein für die Werbewirtschaft verdeutlicht der OVK-Report anhand der Ergebnisse aus dem vergangenen Jahr. Die Nettowerbeinvestitionen in die Gattung Internet (Display- und Suchwortvermarktung) sollen demnach 2017 mit 32,3 % den größten Anteil am Nettowerbekuchen ausgemacht haben. Dies bedeutet im Vergleich zum Vorjahr eine Steigerung um 2,6 Prozentpunkte. Die lange Jahre führende Mediengattung TV folgt auf Rang 2 mit einem leicht rückläufigen Marktanteil von 29 %. Weiter abgeschlagen folgen mit einstelligen Marktanteilen die klassischen Werbeträger Zeitungen, Zeitschriften und Außenwerbung. Ohne die nur im Web mögliche Suchwortvermarktung fließt unverändert das meiste Werbegeld ins Fernsehen (37,2 %). (un@ix.de)

Alle Wirtschaftsmeldungen: Achim Bon

KI kurbelt das Wirtschaftswachstum an

Ein größeres Potenzial als seinerzeit der Dampfmaschine unterstellen die Forscher des McKinsey Global Institute (MGI) der künstlichen Intelligenz (KI). Nach ihrer Prognose kann der Einsatz das globale Bruttoinlandsprodukt (BIP) bis 2030 zusätzlich um durchschnittlich 1,2 Prozentpunkte pro Jahr steigern.

Der Wachstumseffekt läge damit deutlich höher als der, den seinerzeit Dampfmaschinen (0,3 Prozentpunkte), Industrieroboter (0,4 Prozentpunkte) oder IT und Telekommunikation (0,6 %) erzielten. Bis zum Jahr 2030 soll sich eine zusätzliche Wertschöpfung von 13 Billionen US-Dollar ergeben.

Zu diesem wesentlichen Schluss kommen die McKinsey-Forscher in ihrer umfangreichen Studie „Notes from the Frontier: Modeling Impact of AI on the World Economy“, in deren Rahmen 3000 Fir-

men aus 14 Branchen befragt wurden.

Um das jeweilige Produktivitätswachstum zu ermitteln, flossen unter anderem unterschiedliche Mikro- und Makrofaktoren wie die Adaptionsgeschwindigkeit typischer KI-Techniken durch Unternehmen, aber auch die Arbeitsmarktstruktur eines Landes in die Berechnung ein.

Mit einem zusätzlichen BIP-Wachstum von 1,3 Prozentpunkten liegt Deutschland hierbei leicht über dem Durchschnitt und gleichauf mit China. Noch besser schneiden unter anderem die USA (1,5 Prozentpunkte) und Schweden (1,7 Prozentpunkte) ab.

Die rund 60 Seiten umfassende Studie können Interessierte von der Website der Unternehmensberatung kostenlos herunterladen (zum Download-Link siehe ix.de/ix1810034). (un@ix.de)

Digitalisierung kommt kaum voran

Ungeachtet der vielen technischen Digitalisierungsinitiativen erreichen derzeit lediglich 5 % der Industrieunternehmen weltweit tatsächlich ihre Ziele. Die zu langsame Umsetzung von Digitalisierungsprojekten ist nur ein Grund dafür, heißt es in der Studie „Von der Vision zur Transformation: Digitalisierung ist Chefsache“ von Bain & Company. Als weitere Ursache führt die Managementberatung an, dass einige Topmanager die Dringlichkeit als nur mäßig einschätzen. Andere wiederum glauben, einige voneinander isolierte Leuchtturmprojekte seien bereits genug. An einer ganzheitlichen Strategie mangelt es dagegen häufig.

Erwartungsgemäß propagieren die Unternehmensberater eine konsequente digitale Strategie. Zwei bis fünf Prozent des Umsatzes in den kommenden fünf bis zehn Jahren sollten Industrieunternehmen hierfür springen lassen. Diese Investitionen zahlten sich aus. Nach ihren Recherchen wüschen digitale Vorreiter um 50 % schneller als die Konkurrenz und seien um 30 % profitabler. Die Kundenloyalität dieser Unternehmen nehme um ein Drittel zu, während sich die Prozesskosten halbierten. Trotz mehr IT-Einsatz im Zuge der Digitalisierung würden die Komplexitätskosten um durchschnittlich 20 % sinken. (un@ix.de)

Public Cloud: Infrastructure as a Service wird zur Nische

Das weltweite Geschäft mit öffentlich zugänglichen Cloud-Services soll laut Prognose von Gartner im laufenden Jahr um 21 % auf ein Volumen von 175,8 Mrd. Dollar anschwellen. Für 2019 stellt Gartner ein Plus von 17,3 % auf dann 206,2 Mrd. Dollar in Aussicht. Am schnellsten sollen dann die Geschäfte mit Infrastructure as a Service (IaaS) wachsen – um 27,6 % auf fast 40 Mrd. Dollar. Ungeachtet des hohen Wachstums stellen die Marktforscher reinen IaaS-Anbietern künftig allerdings nur ein mehr oder minder lukratives Nischenplätzchen in Aussicht: Bis 2022 dürften 90 % der Firmen IaaS-Leistungen als Bestandteil von Plattform-Services (PaaS) nutzen und dementsprechend bei einem integrierten IaaS-/PaaS-Anbieter einkaufen.

Die größte Cloud-Sparte bleibt indes der Bezug von Applicationsservices aus dem Internet (Software as a Service, SaaS), der den Anbietern im laufenden Jahr gut 72 Mrd. Dollar (+22,8 %) und 2019 gut 85,1 Mrd. Dollar (+17,8 %) in die Kassen spülen soll.

Deutlich langsamer wächst der zweitgrößte Bereich Cloud-basierter Geschäftsprozess-Services (Business Process as a Service, BPaaS), beispielsweise für Gehaltsabrechnungen oder Beschaffungsdienste.

Hier rechnen die Gartner-Analysten mit einem Zuwachs um 10,4 % auf 46,6 Mrd. Dollar beziehungsweise 7,9 % auf 50,3 Mrd. Dollar. Spätestens im Jahre 2019 würden folglich die kombinierten IaaS-/PaaS-Einnahmen das BPaaS-Volumen übertreffen.

(un@ix.de)

Cloud-Umsätze weltweit (in Mrd. US-Dollar)

Sparte	2017	2018	2019	2020	2021
Business Process Services (BPaaS)	42,2	46,6	50,3	54,1	58,1
Application Infrastructure (PaaS)	11,9	15,2	18,8	23,0	27,7
Applications (SaaS)	58,8	72,2	85,1	98,9	113,1
Management and Security	8,7	10,7	12,5	14,4	16,3
System Infrastructure (IaaS)	23,6	31,0	39,5	49,9	63,0
Gesamtmarkt	145,3	175,8	206,2	240,3	278,3

Quelle: Gartner, September 2018

Kurz notiert



Microsoft investiert weiter in **Machine Learning**. Diesmal traf es Lobe. Das Start-up entwickelt Tools zum Entwerfen von ML-Modellen mittels Drag-and-Drop, die für einen Einsatz in Standardbibliotheken wie TensorFlow oder CoreML geeignet sind.

VMWare steigerte den Umsatz im zweiten Quartal des Geschäftsjahres 2019 um 13 % auf 2,17 Mrd. Dollar. Darin enthalten waren 900 Mio. Dollar Lizenz-Einnahmen (+15 %). Als Gewinn des am 3. August beendeten Quartals wies VMWare 644 Mio. Dollar aus (+58,6 %).

HPE legt im dritten Quartal (endet im Juli) beim Umsatz um 3,5 % auf 7,764 Mrd. Dollar zu. Das Gros entfiel auf die Hybrid-IT-Sparte (Server, Speicher, Netzequipment) mit 6,243 Mrd. Dollar (+2,7 %). Der Reingewinn sprang von 165 Mio. auf 451 Mio. Dollar.

Coworking-Krösus **wework** setzt seine Einkaufstour fort und übernimmt **Team**. Das US-amerikanische Start-up, das vor rund sechs Jahren unter dem Namen EventBoard loslegte, entwickelt eine Cloud-Plattform zur Raumorganisation von Meetings.

Recht bescheiden wächst derzeit laut IDC der weltweite Absatz von **Wearables** (Uhren, Kopfhörer, Armbänder etc. mit IT- oder Tracking-Funktionen).

Er soll 2018 um 6,2 % auf 122,6 Mio. Geräte zulegen. Ab 2019 erwartet IDC jedoch wieder ein zweistelliges Wachstum.

Bechtle bringt unter dem Namen ARTICONA IT-Zubehör und Anschlusstechnik auf den Markt. Ein Büro in Taiwan pflegt den Kontakt zu den Herstellern. Die Lagerung in zwei Logistikzentren soll eine hohe Verfügbarkeit gewährleisten.

Broadcom profitiert von der starken Nachfrage nach Prozessorleistung in Datenzentren. Der Halbleiterhersteller meldet für das letzte Quartal einen Umsatz von fast 5,1 Mrd. Dollar (+13,3 %). Der Gewinn verdoppelte sich auf 1,2 Mrd. Dollar.

Zur **Nemetschek Group**, Anbieter diverser Programme für die Baubranche, gehört jetzt die **MCS Solutions** aus Belgien. MCS entwickelt Anwendungen für das Immobilien-, Facility- und Arbeitsplatzmanagement, darunter die Smart-Building-Plattform COBUNDUTM.

Hartford Steam Boiler, eine Tochter der **Munich Re**, übernimmt alle Anteile an **relayr**. Der Wert des Sensorik-Spezialisten und Herstellers einer IoT-Middleware-Plattform soll 300 Mio. Dollar betragen. HSB war bereits an dem Berliner Start-up beteiligt.

Salesforce verbuchte im zweiten Geschäftsjahresquartal 2019 (endet am 31. Juli) fast 3,3 Mrd. Dollar Umsatz (+27 %). Der Gewinn stieg von 46 Mio. auf 299 Mio. Dollar.

Smartphones verkaufen sich so gut wie Unterhaltungselektronik

Laut Bitkom dürfen die Smartphone-Anbieter 2018 mit einem Verkauf von 22,7 Mio. Geräten und mit einem Umsatz von 9,25 Mrd. Euro rechnen. Zu den guten Geschäften trägt insbesondere ein Absatzrekord von 7 Mio. Phablets bei, also Geräten ab einer Bildschirmdiagonale von 5,5 Zoll. Die kosten nach Verbandsrecherchen durchschnittlich 588 Euro, wohingegen die etwas kleineren Pendants im Mittel nur etwa 321 Euro einbringen. Laut Umsatzprognose liegt der Smartphone-Markt

nun ungefähr auf dem Niveau des hiesigen Geschäfts mit klassischer Unterhaltungselektronik. Der Bitkom prognostiziert hier einen leicht sinkenden Gesamtumsatz von 9,6 Mrd. Euro (-3,5 %) mit Geräten wie Fernsehern, Digitalkameras, Audioanlagen oder Spielkonsolen. Ein Grund für diese Entwicklung besteht nach Ansicht der Branchenvertreter darin, dass Smartphones und Tablets inzwischen für viele Verbraucher MP3-Player, Navigationsgerät oder auch das Radio ersetzen. (un@ix.de)

SAP-Dienstleistungen: Gute Geschäfte für Spezialanbieter

SAP-bezogene Dienstleistungen sind weiterhin lukrativ. Laut einer Untersuchung von PAC wuchsen die meisten Anbieter solcher Dienste (Bera-

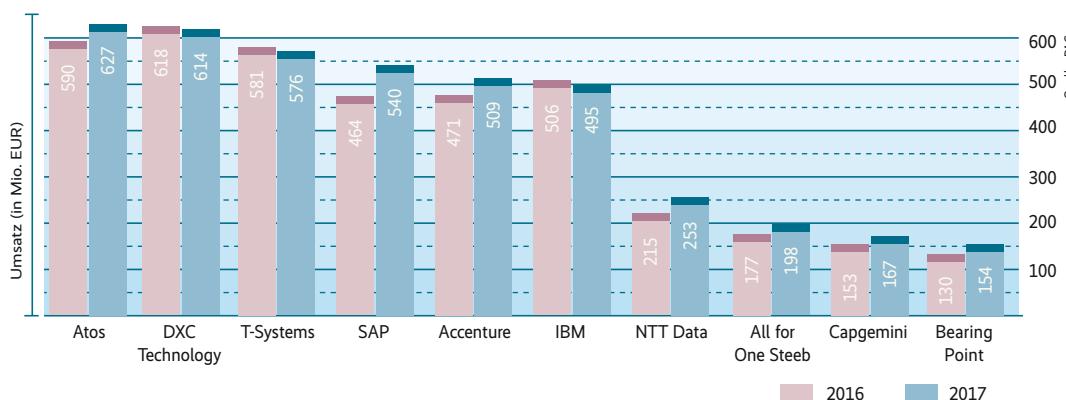
tung, Systemintegration, Anwendungsmanagement und Hosting) im vergangenen Jahr. Sie profitierten davon, dass Anwender ihre Applikationen

modernisieren und neue SAP-Produkte einführen.

Atos belegt als umsatzstärkster SAP-Dienstleister die Poleposition. Es folgen DXC

Technology (CSC mit der Servicesparte HPE), T-Systems, SAP selbst und Accenture. Besonders stark gewachsen (zum Teil durch Zukäufe) sind die Serviceumsätze von Firmen wie Wipro (Übernahme von Cellent), Deloitte, NTT Data (einschließlich itelligence), Allgeier (Akquisition von Ciber) und Cognizant.

Laut PAC sind die Umsätze sehr ungleich verteilt. Atos erwirtschaftet beispielsweise einen Großteil seiner Einnahmen mit traditionellem Outsourcing (Application Management und Hosting), während bei Accenture das Geschäft mit Consulting und Systemintegration im Vordergrund steht. Nahezu ausgewogen ist das Verhältnis bei NTT Data. (jd@ix.de)



Die zehn umsatzstärksten Anbieter von SAP-Dienstleistungen in Deutschland 2017

Orientierungshilfe in großen Datenmengen

Qlik will Big-Data-Anwendern helfen, sich in großen Datenmengen schneller zu rechtfzufinden. Das soll mit der überarbeiteten Version des Podium-Data-Katalogs geschehen. Neben umfangreichen Such- und Drill-down-Funktionen umfasst er ein Bewertungsmodell zum Einschätzen von Datensätzen. Die Benutzer sollen darüber eine bessere Orientierung selbst in sehr großen Rohdatenmengen bekommen.

Als Hilfsmittel dient eine auf der Open-Source-Software Drools basierende Regelumgebung. Eingehende Daten wer-

den nach individuellen Regeln zusammengestellt. Beispielsweise lässt sich die Funktion zum Identifizieren von personenbezogenen Informationen, Zahlungsverkehrsdaten und DSGVO-relevanten Inhalten nutzen. Zudem kann man automatisch benutzerdefinierte Skripts starten und Meldungen an zuständige Personen senden, wenn ungewöhnliche Datenmuster auftauchen. Den Katalog hat Qlik nicht selbst entwickelt, er landete durch die Übernahme von Podium Data im Juli im Portfolio des Analytics-Spezialisten. (jd@ix.de)

Am Ende steht der Werbebrief

Die Deutsche Post und Commander Act verbinden Online-marketing mit dem analogen Briefversand. Grundlage ist die Customer-Data-Plattform des Datenspezialisten Commanders Act. Händler, die dieses System einsetzen, können Zielgruppen nicht nur mit Online-werbung ansprechen, sondern nun auch individualisierte Briefsendungen zustellen.

Die Verbindung zwischen Online und Offline stellt ein Cookie her, das der geografischen Mikrozelle zugeordnet

ist, in der der Konsument wohnt. Es enthält laut Anbieter weder Namen noch personenbezogene Merkmale, sondern verknüpft Daten aus dem Web-tracking mit der Zelle. Jede der sieben Millionen Mikrozellen in Deutschland enthält Informationen von sechs bis sieben Haushalten. Der einzelne Nutzer bleibt so halbwegs anonym. Es ist beispielsweise möglich, sogenannten Warenkorabbrec-hern per Briefwerbung ein Angebot zu unterbreiten. (jd@ix.de)

Erfreuliche Noten für ERP-Software

In der jüngsten Trovarit-Studie „ERP in der Praxis“ gaben die gut 2200 Teilnehmer den ERP-Anbietern und -Systemen gute Noten. Gleichzeitig bestätigten die Autoren Erkenntnisse früherer Untersuchungen, nach denen schlanken Anwendungen, Branchenpakete und/oder Produkte kleiner Anbieter die Kunden am ehesten zufrieden stellen. Software für größere Firmen rangiert im Mittelfeld.

Weniger Funktionen und mehr Branchenbezogenheit reduzieren die Komplexität, und das Einführen, Administrieren und Aktualisieren fällt leichter. Auch kommunizieren spezialisierte Softwarehäuser besser mit ihren Kunden. Zudem sind die Releases schlankerer Pro-

grammpakete deutlich jünger. Zu den gut platzierten Systemen zählen Syslog, Orlando, ISSOSPro, Isah, ALPHAPLAN oder BMD. Meist werden sie von weniger als 25 Anwendern im Unternehmen genutzt. Angebote wie ALPHAPLAN (technischer Handel) und SI-VAS (Einzelfertiger) glänzen durch ihre Branchenausrichtung. Im Vergleich zur letzten Untersuchung (2016) schritten Infor ERP LN, FOSS, ALPHAPLAN und ams.erp in allen Belangen viel besser ab. Dagegen erhielten die zuvor als sehr gut bewerteten Systeme MegaPlus, business express und rs2 dieses Mal eine schlechtere Bewertung und landeten im Mittelfeld. (jd@ix.de)

Kurz notiert



Thinking Networks AG stellt mit **QVANTUM** ein Tool für Planungsaufgaben als Webservice bereit. Kennzahlen und Formeln kann der Nutzer von Excel-Templates aus selbst anlegen. Ge-hostet wird das Ganze vom Mutterkonzern Buhl Data Service.

Die dominierenden **Programmiersprachen zum Entwickeln von Unternehmenssoftware** sind laut einer Studie der Cloud Foundry Foundation Java (58 %), JavaScript (57 %) und C++ (46 %). C# (26 %), Python (25 %) und PHP (22 %) fallen ab.

SAP testet mit einigen Kunden einen **digitalen Assistenten für die Personalmanagement-Suite SuccessFactors**. Er nutzt Machine-Learning-Funktionen der Leonardo-Umgebung. Das Tool will man auch in Team-Plattformen wie Slack und Microsoft Teams einbinden.

Softgarden spendiert dem gleichnamigen SaaS-Angebot für Recruiting einen Empfehlungsmanager. Nach dem Prinzip „Mitarbeiter werben Mitarbeiter“ lassen sich damit Stellenangebote in Netzwerken teilen. Der Empfehler wird informiert, wenn es zum Arbeitsvertrag kommt.

Alle Meldungen: Achim Born



Shift happens.

Digitale Transformation. Mit Cloudlösungen aus Deutschland.

Fortschritt wartet nicht. Erschließen Sie das ganze Potential Ihres Unternehmens. Mit intelligenten Public-, Private- oder Hybrid-Cloudstrategien und individuellen Modellen für alle – auch die, die bisher keine Cloud wollten.

Das nächste Level für Ihre
Cloudanwendungen:

bsp.cronon.net

Wir sehen uns auf der

**CLOUD EXPO
EUROPE!**

7.-8.11.2018 | Frankfurt a. M.

Python ist eine Programmiersprache mit vielen Gesichtern. Die von Guido van Rossum entwickelte Sprache bietet Programmierern Hunderte von Bibliotheken, die insbesondere in den Bereichen künstliche Intelligenz, Mathematik und Machine Learning äußerst umfangreich ausfallen. Der Markt hält Unmengen an Büchern zum Thema bereit, allerdings beschränken sich die meisten auf das Erledigen konkreter Aufgaben. Anfänger und Quereinsteiger brauchen jedoch etwas anderes, nämlich Bücher, die die Sprache zunächst einmal als solche präsentieren.

„Python in a Nutshell“ liegt mittlerweile in der dritten Auflage vor und ist etwa 750 Seiten lang – so viel zur Nusschale. Das Werk aus dem Hause O'Reilly behandelt sowohl Python 2.7 als auch 3.5, Highlights der Version 3.6 werden angerissen. Das Autorenkollektiv unterteilt sein Buch, das sich an erfahrene Programmierer richtet, in sechs Teile. Der erste geht auf die Ausführungsumgebung ein – schon hier merkt man, dass das Buch einen Referenzanspruch stellt, da es von so gut wie allen Werkzeugen verschiedene Versionen vorstellt und vergleicht.

Der zweite Teil kümmert sich um die Feinheiten der Programmiersprache. Ein Kapitel zur Standardbibliothek sowie zwei Abschnitte zur Netzwerkprogrammierung und zur Auslieferung fertiger Anwendungen runden ihn ab. Am Buch gibt es nichts zu bemängeln – Kenntnisse in einer anderen objektorientierten Sprache sind allerdings Voraussetzung.

Michael Weigend schickt bei mitp ein fast 1000-seitiges Lehrbuch ins Rennen, das sowohl Einsteigern als auch an Umsteigern von anderen Sprachen gefallen soll. Die ersten Kapitel führen in die Syntax von Python ein und erklären Iterationen, Selektionen und Co.

Interessant wird es ab dem 14. Kapitel, wo es um konkrete Anwendungssituationen geht, etwa das Erzeugen von Grafiken mit dem Baukasten Tk. Danach finden sich Hinweise zur CGI-Programmierung, zur Interaktion mit dem Internet



MEHR KBYTES

Python

und zum Parsing von XML und JSON. Zwei Kapitel zur Nutzung des Qt-Frameworks fehlen ebenfalls nicht.

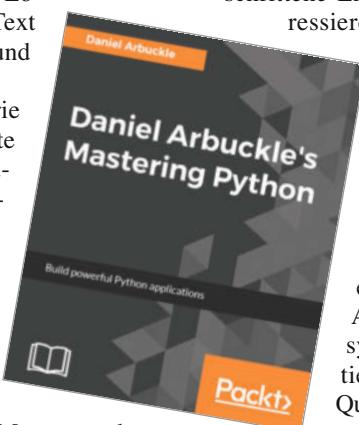
Wer mehr über das Ökosystem lernen möchte und sich wenig für syntaktische Details interessiert, dürfte das Werk von mitp sympathischer finden. Wer den trockenen Kampf mit der Programmiersprache sucht, ist bei O'Reilly besser aufgehoben, denn Bibliotheken spielen hier keine große Rolle.

Beim Hanser-Verlag versucht sich Bernd Klein an einem Beitrag für Ein- und Umsteiger. Sein als Einführung in Python 3.x konzipiertes Werk umfasst rund 470 Seiten. Am Ende finden sich zusätzlich

circa 50 Seiten Lösungen zu den im Text platzierten Fragen und Aufgaben.

Das aus einer Serie von Kursen entwickelte Buch beschreibt zunächst die Python-Umgebung, um die Unterschiede zwischen Bytecode und Maschinencode zu erklären. Danach folgen Datentypen. Interessant ist, dass der Autor Dictionary, Mengen und andere Elemente hier abhandelt, Schleifen und Verzweigungen erst danach. Klassischen Pain Points wie der Unterscheidung zwischen flachem und tiefem Kopieren widmet Klein eigene Kapitel.

Im zweiten Teil dreht sich alles um OOP. Am Schluss steht noch eine vierte



Themengruppe, die sich beispielsweise Unit-Tests und Datenpersistenz vornimmt. Reguläre Ausdrücke und Möglichkeiten, wie Python-Code mit dem zugrunde liegenden System interagiert, erhalten ebenfalls Aufmerksamkeit.

De Gruyter Oldenbourg hat ein rund 340 Seiten starkes Buch im Portfolio, das Personen mit Programmiererfahrung lesen sollen. Es konzentriert sich darauf, Python als Werkzeug für Algorithmen zu verwenden, und fällt folglich recht mathematiklastig aus.

Nach dem Kapitel zum symbolischen Rechnen mit Python schließen sich Ausführungen zur Videoverarbeitung sowie zum Scraping von Websiteinhalten an. Am Ende steht noch ein Kapitel zu Parallelisierung. Wer sich für die wissenschaftlich-mathematische Seite interessiert, könnte an diesem Buch Gefallen finden.

Der britische Packt-Verlag bietet mit „Daniel Arbuckle's Mastering Python“ ein Lehrbuch an, das sich ausschließlich an diejenigen wendet, die sich für fortgeschrittene Entwicklungsszenarien interessieren. Nach einer Einführung

in Themen, an denen Autodidakten laut Arbuckle häufig scheitern, folgen Methoden zur Auslieferung von Code. Best Practices wie das Erzeugen automatisierter Dokumentationen, das Nutzen virtueller Environments und die Arbeit mit Versionskontrollsysteinen sollen dem paketierten Code eine anständige Qualität mitgeben.

Arbuckle wechselt geschickt zwischen Theorie und Praxis. Die technischen Einführungen dienen als Einstieg in das Erstellen von Kommandozeilenwerkzeugen. Es folgen das Parallelisieren von Programmen sowie asynchrone Eingabe- und Ausgabeoperationen, wichtig für die Auslastung von

Mehrkerneprozessoren. Das Kapitel zur Metaprogrammierung setzt sich auch mit Unit-Testing auseinander. Weiter geht es mit reaktivem Programmieren, Microservices und Erweiterungsmodulen. Das mit 260 Seiten vergleichsweise kurze und codelastige Buch legt ein hohes Niveau vor. Viele der Kapitel sind als Inspiration zu verstehen, sich mit dem jeweiligen Thema in Eigenregie intensiver zu beschäftigen.

Tam Hanna (jd@ix.de)

Alex Martelli, Anna Ravenscroft, Steve Holden: **Python in a Nutshell**; 3. Auflage; O'Reilly Media 2017; 772 Seiten; 45,85 € (Paperback)

Michael Weigend: **Python 3**; Lernen und professionell anwenden; 7. Auflage; mitp 2018; 992 Seiten; 39,99 € (Hardcover)

Bernd Klein: **Einführung in Python**; Für Ein- und Umsteiger; 3. Auflage; Hanser 2017; 555 Seiten; 25 € (flexibler Einband)

Ernst Erich Doberkat: **Programmierung mit Python 3**; Ein Lern- und Arbeitsbuch; De Gruyter Oldenbourg 2018; 323 Seiten; 39,95 € (Paperback)

Daniel Arbuckle: **Daniel Arbuckle's Mastering Python**; Packt Publishing 2017; 274 Seiten; 37,99 € (Paperback)

NEU

DOMAINS | E-MAIL | HOSTING | SHOPS | SERVER

TECHNOLOGIE-BOOST!



1&1 Dedicated
Server
ab 30,- €/Monat*

Neueste Intel® Xeon® Prozessoren!



- ✓ 100% Enterprise Hardware-Komponenten für High-Performance
- ✓ Skalierbare Intel® Xeon® Silver Prozessoren speziell für Hosting-Anwendungen
- ✓ Bis zu 6-fach höhere Geschwindigkeit mit Intel® NVMe-SSD-Technologie
- ✓ ISO-zertifiziertes Rechenzentrum in Deutschland
- ✓ 24/7 kostenloser Support durch Server-Experten



DE: 02602 / 96 91
AT: 0800 / 100 668

1&1



* Preisvorteil bei 12 Monaten Mindestvertragslaufzeit: 1&1 Dedicated Server L-16 mit HDD, 3 Monate für 30,- €/Monat, danach für 50,- €/Monat.
Aufpreis für SSD-Speicher statt HDD, 10,- €/Monat. Einmalige Einrichtungsgebühr 49,- €. Preise inkl. MwSt. 1&1 Internet SE, Elgendorfer Straße 57, 56410 Montabaur.

Copyright by Heise Medien.

1und1.info

Cloud-Server als Virtual Private Server oder Bare-Metal-System

Auf Abruf

Michael Plura



Server on demand beim Hoster sind im Cloud-Zeitalter für viele schon selbstverständlich. Die billigen und oft überbuchten virtuellen Server (VPS) bekommen nun harte Konkurrenz – von Bare-Metal-Servern.

Durch die immer umfassendere Digitalisierung, das Internet der Dinge (IoT), multimediale Inhalte, soziale Netzwerke und die damit anfallenden Mengen an Daten steigt der Bedarf an IT-Rechenleistung nicht nur enorm an, sondern er fluktuiert auch extrem. Neue Konzepte wie DevOps, agile Softwareentwicklung oder Continuous Delivery zwingen professionelle IT-Infrastrukturen zudem zu immer schnelleren Anpassungen. In der glücklichen Lage, den IT-Bedarf für die nächsten Jahre in Ruhe planen und umzusetzen zu können, ist heute eigentlich niemand mehr.

Jedem IT-Verantwortlichen ist klar: Entstehen plötzlich sehr hohe Anforderungen an die Ressourcen der IT-Infrastruktur, die das eigene Rechenzentrum nicht erfüllen kann, ist es zu spät, zusätzliche Serverhardware oder mehr Bandbreite in Richtung Internet zu bestellen. Die erwartete Reaktionszeit dürfte hier nicht im Bereich von Monaten oder bestenfalls Wochen, sondern von Minuten liegen. Die einzigen Auswege im eigenen Rechenzentrum wären, entsprechende Hardware im „cold Stand-by“ vorzuhalten oder die komplette IT gleich so zu dimensionieren, dass sie jede denkbare Lastspitze abfängt. Beides ist aus ökonomischer Sicht mehr als unattraktiv.

VPS, Dedicated und Bare Metal

Auf elegante Weise schaffen mietbare Server bei einem Hoster hier Abhilfe. Die wiederum gibt es in verschiedenen Leistungsstufen:

Virtual Private Server, kurz VPS, sind virtuelle Maschinen oder sogar nur Container-Instanzen, die in Sekunden gebucht werden können. Auf dem VPS läuft in der Regel eine wählbare Linux-Distribution, auf die der Systemverwalter Zugriff als root hat. Diese vollen Zugriffsrechte bedeuten nahezu freie Konfigurierbarkeit der Software, aber auf der anderen Seite auch volle Verantwortung für die Sicherheit der Serverinstanz. Auf einem VPS-Host können wie auf jedem Hypervisor- oder Container-Host sehr viele virtuelle Serverinstanzen und damit Kunden laufen. Mehr als hundert Kunden auf einem physischen Server sind nichts Ungewöhnliches.

Bei **Bare-Metal-Servern** hingegen wird dem Kunden „pures Metall“ zur Verfügung gestellt – also ein kompletter Server ohne Software (abgesehen von der Remote-Verwaltungssoftware). Auf diesen physischen Server hat der Kunde das

alleinige Zugriffsrecht, er kann die Ressourcen des Servers komplett für sich beanspruchen und muss CPU-, Speicher- und I/O-Leistung mit niemandem teilen.

Eine Mischform stellen die **Dedicated Server** oder **Root Server** dar, die eigentlich Dedicated Resources heißen müssten. Dort reservieren die Hoster dem Kunden eine bestimmte Teilmenge der physischen Hardware, er kann beispielsweise auf einer Acht-Kern-CPU vier Kerne für sich mieten – und hat diese jederzeit exklusiv zur Verfügung. Trotzdem werden das gesamte I/O-System und auch die Speicherbandbreite von mehreren Kunden parallel genutzt. Das sind zwar wesentlich weniger als bei einem VPS-Host, trotzdem könnte ein anderer Kunde so viel Bandbreite im Speicher, auf dem I/O-System oder im Netz „verpulvern“, dass die eigene Serverinstanz darunter leidet.

Im Galopp zur Cloud

Zwar nutzt das gleichzeitige Betreiben vieler virtueller Server auf nur einer physischen Hardware diese sehr effizient, ist aber auch deren größtes Manko: Andere Anwender können – bösartig oder nicht – die Ressourcen der physischen Hardware über Gebühr ausnutzen. Sei es, dass die Prozessoren mit dem Schürfen von Kryptowährungen belastet sind oder exzessive Downloads die Netzwerkanbindung an ihre Grenze bringen, um nur zwei Beispiele zu nennen.

Hypervisoren und automatisches Cloud-Management können bedingt helfen und die Lasten durch Live-Migration neu verteilen. Dennoch bedeutet das für einen virtuellen Server oder einen VPS, dass es keine Garantie dafür gibt, eine gebuchte Leistung auch jederzeit voll abrufen zu können. In vielen AGB steht sogar, dass Nutzer angehalten sind, die Ressourcen des Systems „fair“ und nur in Maßen zu verwenden. Während unvorhersehbare Leistungsengpässe einfachen Webdien-

Mit Parallels Plesk (im Bild), aber auch mit cPanel von cPanel, Inc. lassen sich VPS und Bare-Metal-Server komplett über eine webbasierte Administrationsoberfläche administrieren (Abb. 1).

ten meist keine Problem bereiten, sind diese bei intensiv genutzten Shopsystemen aber inakzeptabel.

Viele Sicherheitsfragen

Ein weiteres Problem ist die Sicherheit. Stellvertretend sei hier auf die Panne bei DigitalOcean vor einigen Jahren hingewiesen, bei der man die Images gelöschter VPS nicht mit Nullen überschrieben hatte – der Platz wurde lediglich wie beim alten FAT-Dateisystem im Speichersubsystem freigegeben. Bei einem neu angeleg-

ten VPS konnte man per dd ein komplettes Image der eigentlich leeren virtuellen Festplatte erstellen – und fand dort Daten anderer, gelöschter VPS. Der Fehler ist natürlich behoben. Neben Konfigurationsfehlern gibt es aber auch prinzipbedingte Sicherheitsprobleme auf einem Hypervisor. Per DoS-Angriff (Denial of Service) lässt sich das Hostsystem lahmlegen und über Sicherheitslücken des Hypervisors können Gastsysteme – also beispielsweise ein VPS oder ein Dedicated Server – den Host kompromittieren. Ist das der Fall, erhält der Angreifer von dort aus Zugriff auf alle Gastsysteme und eventuell sogar weitere Teile der Cloud-Infrastruktur.

Verschärft wird die Problematik durch Sicherheitslücken wie Meltdown oder Spectre in den Prozessoren insbesondere von Intel, aber teilweise auch AMD oder sogar ARM, PowerPC und SPARC. Bei Meltdown/Spectre kann ein normaler Anwender Unzulänglichkeiten der spekulativen Ausführung von Maschinencode in allen modernen CPUs nutzen, um über Tricks auf Informationen des Kernelspeichers und somit auf die Prozesse des Hosts oder anderer Benutzer zuzugreifen.



- Virtual Private Server (VPS) sind sehr preiswerte, aber leistungs- und sicherheitstechnisch eingeschränkte Serverinstanzen mit Root-Zugriff in die virtuellen Maschinen.
- Bei einem Bare-Metal-Server erhält der Kunde vollen und exklusiven Zugriff auf die physische Hardware eines Servers.
- Dank sinkender Preise wird der Wechsel von VPS auf Bare-Metal-Server zunehmend attraktiver.

Das impliziert natürlich, dass der Angreifer Code auf dem System ausführen kann – was auf Servern im eigenen RZ nur von außen über Exploits machbar ist, auf einem VPS oder Dedicated Server aber gerade das Betriebsprinzip darstellt. Für alle relevanten Betriebssysteme gibt es Patches, die diese Fehler verhindern sollen. Um auch gegen noch unveröffentlichte weitere Meltdown-/Spectre-Varianten gewappnet zu sein, hilft nur eines: Die Hardware ohne Dritte zu betreiben, also einen Bare-Metal-Server zu verwenden. Nur der bietet den vollen und definitiven Zugriff auf alle Hardwareressourcen und somit die maximale Sicherheit.

Das Beste beider Welten

Einen Bare-Metal-Server zu mieten, war bis vor Kurzem noch ein langwieriges, umständliches und vor allem teures Unterfangen. In den letzten Jahren sind die Bare-Metal-Servers mit Monatsmieten ab etwa 40 Euro nicht nur bezahlbar geworden. Inzwischen ist die Bereitstellung durch aus der Cloud bekannte Techniken vereinfacht und beschleunigt worden. Vorgefertigte Systeme lassen sich automatisch – vergleichbar einer virtuellen Maschine – aus der Ferne per Remote-Management konfigurieren und adminis-

trieren. Die physischen Server, die die Hoster in ihren Rechenzentren bereitstellen, haben vom schnellen Deployment der Cloud-Server gelernt. Bare-Metal-Servers sind heute in wenigen Minuten einsatzbereit und die Abrechnung erfolgt teilweise sogar nach Betriebsstunden.

Für den Systemverwalter verschwimmt die Grenze zwischen VPS, Dedicated Server und Bare-Metal-Server fast komplett, denn auch letztere lassen sich über API-Aufrufe oder OpenStack orchestrieren. Aber auch ohne diese Automatismen ist der Weg zum Bare-Metal-Server mit dem zu einem VPS fast identisch: Buchung und Verwaltung der Systeme erfolgen über das Web-Frontend des Hosters, oft cPanel oder Plesk. Während der die VPS in der Regel mit einem Betriebssystem-Image versieht, kann das bei Bare-Metal-Servers auch ein Rescue-System oder ein Fernwartungszugang sein, über den die Kunden das gewünschte Betriebssystem aus der Ferne installieren. Im Endeffekt hat der Administrator in wenigen Minuten einen funktionierenden SSH-Zugang zum System und kann mit dem Installieren von Software beginnen.

Mit der Maus einrichten

Wie man einen VPS einrichtet, dürfte bekannt sein: Im Webshop des Providers

wählt der Kunde seine VPS-Konfiguration oder legt sie mittlerweile oft mit Schieberegeln für die variablen Komponenten fest. Nach Angabe der Kundendaten und eventueller Bezahlung erhält der Systemverwalter eine E-Mail mit der IPv4-Adresse und dem Root-Passwort – von da an wird der VPS wie eine virtuelle Maschine per SSH administriert (und als Erstes natürlich das Root-Passwort geändert). Manche Anbieter erlauben es, einen SSH-Schlüssel anzugeben, was die unsichere E-Mail mit dem Passwort vermeidet.

Bei einem Bare-Metal-Server sieht es im Grunde genauso aus. Bei 1&1 beispielsweise unterscheiden sich die ersten Schritte bis zur SSH-Sitzung zum VPS nicht von denen zu einem Bare-Metal-Server. Hetzner hingegen hat leicht unterschiedliche Frontends für VPS (Cloud) und Bare-Metal-Server (Robot), zwischen denen man aber wechseln kann.

Exemplarisch hier eine Übersicht: Das Management der VPS erfolgt in in der grafischen „Cloud Console“ in Form von „Projekten“, zu denen mehrere VPS-Instanzen gehören können. Hier werden neben Backups und Snapshots auch „Floating IPs“ verwaltet. Das sind feste IP-Adressen, die man wahlweise einem der VPS zuordnen kann – bei Wartungsarbeiten wird also kurzzeitig einfach auf einen anderen VPS umgeschaltet. SSH-Schlüssel, API-Tokens für die automatische Steuerung und weitere Zugänge zum Delegieren von Aufgaben finden sich hier ebenfalls. Für jeden VPS gibt es eine Reihe weiterer Funktionen, beispielsweise lässt sich ein ISO-Image des aktuellen OpenBSD 6.3 einbinden und über das vorinstallierte System installieren – ein sicheres Zeichen übrigens, dass Hetzner hier virtuelle Maschinen und keine auf Linux beschränkten Container einsetzt.

Das „Robot“-WebGUI für Bare-Metal-Server wirkt nüchterner und erlaubt den Zugriff auf mehr und speziellere Funktionen. So lassen sich fertig installierte Bare-Metal-Servers auf andere Kunden übertragen, virtuelle Switches und Firewalls regeln die Verbindungen (VLAN) zwischen Servern im Rechenzentrum und selbst WoL (Wake on LAN) lässt sich einrichten. Betriebssysteminstallation und Wartungsarbeiten auf einem Bare-Metal-

The screenshot shows the DigitalOcean 'Create Droplets' page. On the left, there's a sidebar with 'PROJECTS' (digitalocean, + New Project), 'MANAGE' (Droplets, Spaces, Images, Networking, Monitoring, API), and 'ACCOUNT' (Profile, Billing, Security, Referrals). The main area has a search bar 'Search by Droplet name or IP (Ctrl+B)' and a 'Create' button. Under 'Choose an image', 'Distributions' is selected, showing options for Ubuntu (selected), FreeBSD, Fedora, Debian, and CentOS. A dropdown menu for 'This distribution requires' shows '11.2 x64 zfs' as selected. Under 'Choose a size', 'Standard Droplets' are listed with options like 11.1 x64, 10.4 x64 ZFS, 10.4 x64, 10.3 x64, and 10.3 x64. A dropdown menu for 'Choose a size' shows '11.2 x64 zfs' as selected. To the right, 'CPU Optimized Droplets' are described as Compute optimized virtual machines with dedicated hyper-threads from best in class Intel CPUs for CPU intensive applications like CI/CD, video encoding, machine learning, ad serving, batch processing and active front-end web servers. Below this, two tables show price details for different memory and vCPU configurations.

MEMORY	VCPU	SSD DISK	TRANSFER	PRICE
1 GB	1 vCPU	25 GB	1 TB	\$5/mo \$0.007/hr
2 GB	1 vCPU	50 GB	2 TB	\$10/mo \$0.015/hr
3 GB	1 vCPU	80 GB	3 TB	\$15/mo \$0.023/hr

MEMORY	DEDICATED VCPU	SSD DISK	TRANSFER	PRICE
4 GB	2 vCPUs	25 GB	4 TB	\$40/mo \$0.060/hr
8 GB	4 vCPUs	50 GB	5 TB	\$80/mo \$0.119/hr
16 GB	8 vCPUs	100 GB	6 TB	\$160/mo \$0.238/hr

DigitalOcean als Vorreiter preiswerter VPS bietet ein vorbildlich einfaches WebGUI zum Ausrollen und Managen der virtuellen Server (Abb. 2).



WHERE THE CLOUD LIVES

Am deutschen Cloud Hub von Interxion in Frankfurt haben Sie direkten Zugang zu den großen HyperScale Clouds ebenso wie zu vielen lokalen Cloud-Anbietern. Von unseren Colocation-Rechenzentren aus bauen Sie sicher, performant und kosteneffizient Ihre hybride- oder Multi-Cloud-Umgebung auf.

www.interxion.de



interxion™

VPS-Anbieter

	1&1 Internet SE	1blu AG	DigitalOcean	gridscale GmbH	Hetzner Online GmbH	Host Europe GmbH	
Firmensitz	Montabaur, D	Berlin, D	New York, USA	Köln/Wuppertal, D	Gunzenhausen, D	Köln, D	
Produktreihe	Virtual Server Cloud	vServer	Droplet	CloudServer	Cloud Server	Virtual Server	
Ausstattung							
vCPUs	1-4	1-12	1-32	1-32	1-8	2-10	
RAM (GByte)	1-8	2-32	1-192	1-192	2-32	2-32	
Storage (GByte)	50-160	60-600	25-3840	10-4096	20-240	100-800	
SSD	✓	✓	✓	✓	NVMe SSD	✓	
alternativ HDD	-	-	-	-	-	-	
Netzanbindung							
Inklusivvolumen	unbegrenzt	inklusive	1-12 TByte	2 TByte	20 TByte	Traffic Flatrate	
IPv4-Adressen	1	1	1	1, weitere je 2,59 €/Monat	1	1	
IPv6-Adressen	/64	k. A.	optional	✓	✓	✓	
Besonderheiten							
API, Scripting	✓	k. A.	✓	✓	API, CLI-Tools, Go-Bibliothek	✓	
Backups/Snapshots	✓	✓	✓, +20 % Aufpreis	✓, Snapshots	✓ / ✓	✓	
Extras	Plesk	SSL-Zertifikate, Let's Encrypt per Klick, .de-Domain inklusive	Load Balancer, Floating IP (failover), DNS-Management, Team Accounts	API, Autoscaling Database- und Application-Stack, Marketplace für Apps	API, Webmin, Plesk/cPanel, Floating IPs	Plesk	
SLA, Uptime	99,90 %	99,00 %	99,99 %	100,00 %	99,90 % (Netzwerk)	99,95 %	
Betriebssysteme							
Linux	Arch Linux ¹ , CentOS 6/7, CoreOS ¹ , Debian 8/9, openSUSE ¹ , Ubuntu 16.04/18.04 LTS	Ubuntu 16.04 LTS	CentOS 6.9/7.1, Debian 8.10/9.5, Fedora 27/28, Ubuntu 14.04.5/16.04.4/18.04 LTS	CentOS 7, Debian 8/9, Fedora 25, Ubuntu 16.04/18.04 LTS	CentOS 7, Debian 9, Ubuntu 16.04/18.04 LTS; aus ISO: Alpine, Arch Linux, CoreOS, Devuan, Fedora, NixOS, openSUSE, PhotonOS, RancherOS	CentOS 7, Debian 8, Ubuntu 16.04 LTS	
Free-/Net-/OpenBSD	-	-	FreeBSD 10.3/10.4/11.1/11.2 (x64 ufs, x64 ZFS)	FreeBSD 11.1/pfSense/OPNsense über ISO-Image	aus ISO: FreeBSD 10/11, OpenBSD 6.2/6.3, pfSense/OPNsense (Firewall)	-	
Windows	Server 2012/2016	-	-	Server 2012 R2 / 2016 Standard	aus ISO: Server 2012 R2 / 2016, virtio-Treiber-CD	Server 2012 R2 Datacenter	
sonstige	-	eigene ISO-Images	CoreOS, RangerOS, Fedora Atomic	eigenes ISO-Image, iPXE-Boot	aus ISO: VyOS (Router-OS)	-	
RZ-Standorte							
Deutschland	✓	Frankfurt am Main	Frankfurt am Main	Frankfurt am Main	Nürnberg, Falkenstein	Köln	
Europa	-	-	Amsterdam, London	-	Helsinki	Straßburg	
USA/Kanada	✓	-	New York, San Francisco, Toronto (Kanada)	-	-	-	
Asien/Pazifik	-	-	Singapur	-	-	-	
Preise							
Einrichtung (kurze Laufzeit)	9,99 €	9,90 €	-	-	-	-	
Minimalkonfiguration: Name	Virtual Server Cloud M	vServer 2R	Droplet	CloudServer	CX11	Virtual Server Starter	
dafür pro Stunde	-	-	0,007 US-\$	0,0275 €	0,005 €	-	
dafür pro Monat	9,99 €	3,90 €	5,00 US-\$	19,83 €	2,96 €	9,99 €	
Abrechnung pro	Monat	Monat/Quartal	Stunde	Minute	Monat	Monat	

alle Daten Herstellerangaben; ¹ nur bei Reinstalltion; ² siehe Text

Cloud Anbieter Vergleich								
	IP-Projects GmbH & Co. KG	Linevast, Droptop GmbH	Linode, LLC	OVH GmbH	Server4You	Strato AG	Vultr Holdings Corp.	Webtropia
Waldbrunn, D	Schwielowsee/ Geltow, D	Galloway Township, NJ, USA	Saarbrücken, D	Hürth, D	Berlin, D	Matawan, NJ, USA	Düsseldorf, D	
Linux V-Server	Linux vServer	Linode	VPS SSD	vServer	V-Server Linux	Vultr Cloud Compute VC2	vServer 6.0	
1-8	2-8	1-32	1-2	2-16	1-16	1-24	1-8	
2-16	4-32	1-300	2-8	4-18	2-32	0,5-1	2-16	
50-400	50-200	25-3840	20-80	100-400	50-1000	20-800	75-500	
HDD mit SSD-Cache	✓	✓	✓	✓	HP 3PAR StoreDev	✓	✓	
RAM-Größe zusätzlich als SSD-Swap verfügbar	✓, größer bei gleichem Preis	-	-	✓, doppelter Platz zum gleichen Preis	immer SSD-HDD-Kombination	✓, Storage Instance	-	
5 TByte	Traffic Flat	1-20 TByte	unbegrenzt	Flatrate	Flatrate	1-15 TByte	Flatrate	
bis 5 kostenfrei	1, weitere je 1,50 €	1, mehr auf Anfrage	1, 16 weitere je 2,40 €	1, drei weitere zu- buchbar	1, eine weitere zubuchbar	- (1, 2 weitere je 2 US-\$/Monat) ²	1, 31 weitere für je 1 €	
✓	/64	✓	1	k. A.	optional	optional	/128	
-	✓	API, Lish, CLI, StackScripts	✓	-	-	✓	-	
✓	k. A.	✓, ab 2,50 US-\$/Monat	Snapshots	✓	✓	✓, +20 % Aufpreis	✓	
Plesk, I-MSCP	API, DDoS-Protection	NodeBalancer	API, DDoS-Protection, Netzwerk-Firewall	Plesk, Domain inklusive	Plesk	Compute/Storage/ Dedicated Instance, Auto-Backup, DDoS-Protect	Plesk	
99,90 %	99,90 %	99,90 %	99,95 %	99,00 %	99,00 %	100,00 %	99,00 %	
Asterisk 1.4.22, CentOS 5/6/7, Debian 6/7/8/9, Fedora 18-23/ Core11, Gentoo, openSUSE 11/12/13/42, Oracle Linux 6/7, Scientific Linux 6/7, Ubuntu 12.04-17.04, weitere auf Anfrage	CentOS 6/7, Debian 8/9, Fedora 23, Ubuntu 16.04	Arch Linux, CentOS 7, Debian 8/9, Fedora 27/28, Gentoo, openSUSE 15.0/43.2, Slackware 14.2, Ubuntu 16.04/18.04 LTS	Arch Linux, CentOS 6/7, Debian 7/8/9, Fedora 26, Ubuntu 16.04 LTS Server	CentOS 7, Debian 8, Ubuntu 16.04 LTS	CentOS 6/7, Debian 8/9, Ubuntu 16.04/ 18.04 LTS	CentOS 6/7, Debian 8/9, Fedora 27/28, Ubuntu 14.04/ 16.04 LTS	CentOS 6/7, Debian 7/8, openSUSE 13.2, Ubuntu 14.04/ 16.04 LTS	
✓	-	-	-	-	-	FreeBSD 10.4, 11.2, OpenBSD 6.3	-	
✓, ohne Lizenz im HVM-Modus	-	-	Server 2012 R2 / 2016 Standard Edition für VPS Cloud	-	nur in der teureren „V-Server Windows“-Reihe	Server 2012 R2 / 2016	Server 2008 R2 / 2012	
-	-	-	-	-	-	CoreOS, Installation aus ISO und über iPXE	-	
Frankfurt am Main	Frankfurt am Main	Frankfurt am Main	✓	-	Karlsruhe, Berlin	Frankfurt am Main	Düsseldorf	
-	-	London	Breslau, London, Straßburg	Straßburg	-	Amsterdam, London, Paris	-	
-	-	Newark, Fremont, Atlanta, Dallas	Beauharnois (CAN)	St. Louis	-	Atlanta, Chicago, Dallas, Los Angeles, Miami, New York, Seattle, Silicon Valley	-	
-	-	Singapur, Tokio	VPS SSD „APAC“ ab 2,40 € in Sydney, Singapur	-	-	Singapur, Sydney, Tokio	-	
-	-	-	-	-	-	-	-	
V-Server S	Linux vServer Basic	Nanode 1GB	VPS SSD 1	vServer SSD S8	V-Server Linux V10	VC2	vServer S 6.0	
-	-	0,0075 US-\$	-	-	-	0,004 US-\$	-	
3,90 €	6,99 €	5 US-\$	3,56 €	5,00 €	5,00 €	2,50 US-\$	3,99 €	
Quartal	Monat	Stunde	Monat	Monat	Monat/Quartal	Stunde	Monat	

Server erfolgen bei Hetzner über das WebGUI oder ein Rescue-System (Debian oder FreeBSD). Per *installimage* wählt man im Menü das neue System aus und legt eventuelle Parameter fest. Beim anschließenden Reboot generiert das neue System frische SSH-Schlüssel, man muss diese für eine erneute SSH-Sitzung ersetzen. Von Anbieter zu Anbieter unterscheiden sich die Verwaltungsoberflächen und -möglichkeiten stark, stellen erfahrenere Systemverwalter jedoch vor keine großen Probleme. Oft lässt sich ein Bare-Metal-Server kostenlos testen – bei Hetzner beispielsweise 14 Tage.

Neues bei den VPS?

Bis DigitalOcean ab 2011 den Markt mit seinen 5-US-Dollar-VPS aufrollte, waren virtuelle Server im Netz kaum für unter 20 Euro zu haben. Der New Yorker Hoster zwang auch andere Anbieter dazu, Kampfpreise anzubieten. Die neue Marktlage war mit ein Grund für die VPS-Übersicht der *iX* vor zweieinhalb Jahren [1]. Ein aktueller Blick auf den Markt zeigt, dass sich nach 30 Monaten enttäuschend wenig getan hat.

Ein weiterer dramatischer Preisverfall ist nicht zu sehen, auch wenn **Vultr** inzwischen die Untergrenze für einen funktionsfähigen VPS auf 2,50 US-Dollar pro Monat gesenkt hat. Das ging mit einer Reduzierung des RAMs einher, doch für viele Einsatzgebiete reichen eine

vCPU, 512 MByte RAM und 20 GByte SSD-Speicher aus. Eine als root administrierbare Serverinstanz in einem professionellen Rechenzentrum für umgerechnet rund 26 Euro pro Jahr ist demnach die unterste Einstiegsgrenze. Bei **Vultr** heißen die VPS nun **Vultr Cloud Compute (VC2)**. Neu ist der angesprochene Minimal-VPS für 0,4 US-Cent pro Stunde oder maximal 2,50 US-Dollar im Monat – kleiner Haken: Dies ist der einzige VPS in der Übersichtstabelle, für den es in der Minimalkonfiguration nur IPv6, aber kein IPv4 gibt. Sehr praktisch ist die Möglichkeit, beim Anlegen eines VPS bereits ein Startup-Script zum Installieren und Konfigurieren von Software zu übergeben.

Beim Primus der letzten Übersicht, **DigitalOcean**, gibt es inzwischen mehr virtuelle Hardware fürs Geld. Der Einstiegs-VPS, liebevoll **Droplet** genannt, hat nun 1 GByte statt 512 MByte RAM und mit 25 GByte etwas mehr SSD-Speicher. Der Preis ist bei 5 US-Dollar pro Monat geblieben, wobei der Anbieter wie üblich die Laufzeit stundenweise abrechnet. Kräftiger sind die großen VPS geworden, dort gibt es nun 32 statt 25 vCPUs, 192 statt 64 GByte RAM und statt 700 GByte satte 3,84 TByte SSD-Speicher. Die Sicherheit wurde verbessert: DigitalOcean benennt das Prüfverfahren nicht, aber sobald ein Login etwas anders wirkt als üblich, muss zusätzlich eine per E-Mail „on-the-fly“ zugesandte Zahlenkombination angegeben werden.

Alle Ressourcen (Droplets, Spaces, Load Balancers, Domänen und Floating IPs) lassen sich nun in „Projects“ für unterschiedliche Aufgaben, Kunden oder eben Projekte zusammenfassen.

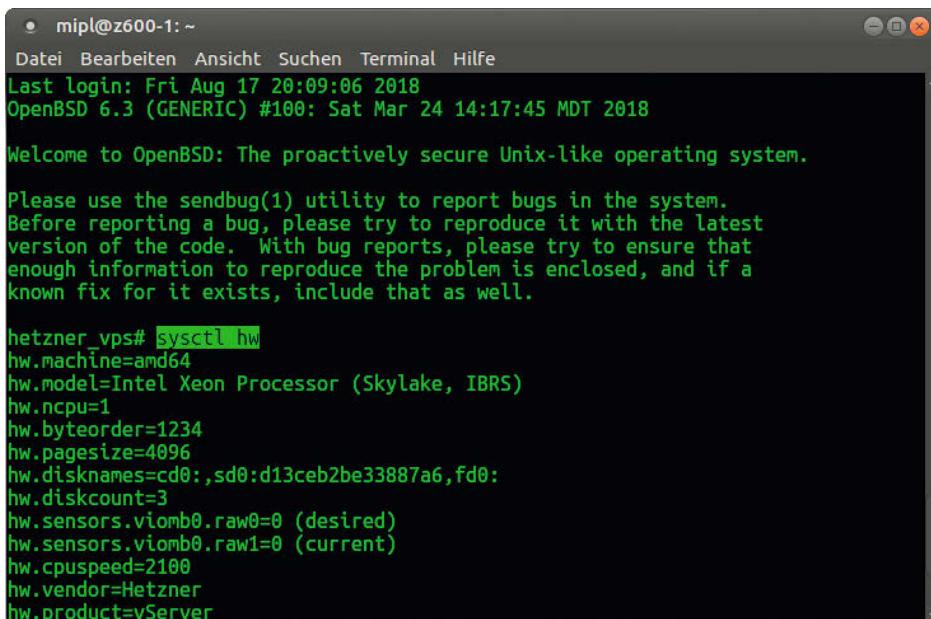
Linode ist mittlerweile auch bei einem Minimal-VPS namens **Nanode 1GB** für 5 US-Dollar angekommen. Das angenstaubt wirkende WebGUI ist dennoch übersichtlich und erlaubt durch die vielen sicht- und bearbeitbaren Optionen eine rasche Administration. Linode erprobt eine neue Version des WebGUI, die auch für DevOps, die nur über ein Smartphone verfügen, geeignet, aber leider zu bunt und umständlich zu bedienen ist.

Bei **1blu** ist mit dem **vServer R2** ein VPS zum Kampfpreis hinzugekommen: 3,90 Euro sind monatlich fällig für 1 vCPU, 1 GByte RAM und 60 GByte SSD-Speicher. Nicht nur der Server, sondern auch der Unternehmensstandort liegt in Deutschland.

Bei **OVH** ist der Preis für den kleinsten **VPS SSD** kurz nach der letzten *iX*-Übersicht um 17 Prozent gestiegen und liegt nun bei 3,56 Euro pro Monat – statt bei damals 2,99. Noch billiger sind die neuen VPS im asia-pazifischen Raum, die als „APAC“-Varianten ab 2,40 Euro erhältlich sind.

Hetzner, ein deutsches Unternehmen mit deutschen und finnischen Rechenzentren, hat den Preis für sein Einstiegs-VPS **Cloud Server** auf 2,96 Euro pro Monat gesenkt. Einzig das US-amerikanische Vultr ist etwas günstiger, bietet aber nur 512 MByte RAM, Hetzner dagegen satte 2 GByte. Außerdem laufen Hetzners VPS auf Skylake-Prozessoren und schnellen NVMe-SSDs. Die Geschwindigkeit macht sich auch in der Bereitstellung bemerkbar, die teilweise weniger als 10 Sekunden dauert. Die Auswahl an Betriebssystemen ist bei den Hetzner-VPS sehr groß, denn es lassen sich ISO-Images für einen Neustart einbinden, was bei den meisten anderen Hostern nicht geht. Hetzner bietet eine Liste an, über die sich beispielsweise ein systemd-freies Devuan GNU+Linux, ein OpenBSD, eine pfSense- oder OPNsense-Firewall oder sogar ein VyOS-Router/Firewall-System (siehe Artikel „Freie Filter“ ab S. 56) installieren. Im Wiki beschreibt ein Artikel, wie man mit einigen Tricks auch eigene Images nutzen kann (siehe [ix.de/ix1810040](#)).

Bei **Host Europe** – mittlerweile vom US-amerikanischen GoDaddy geschluckt – wurde der Einstiegs-VPS **Virtual Server** bei doppelter CPU-Leistung ein Drittel günstiger: 2 vCPUs mit 2 GByte RAM und 100 GByte SSD-Speicher kos-



```

mip1@z600-1: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
Last login: Fri Aug 17 20:09:06 2018
OpenBSD 6.3 (GENERIC) #100: Sat Mar 24 14:17:45 MDT 2018

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code. With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

hetzner_vps# sysctl hw
hw.machine=amd64
hw.model=Intel Xeon Processor (Skylake, IBRS)
hw.ncpu=1
hw.byteorder=1234
hw.pagesize=4096
hw.disknames=cd0:,sd0:d13ceb2be33887a6,fd0:
hw.diskcount=3
hw.sensors.viomb0.raw0=0 (desired)
hw.sensors.viomb0.raw1=0 (current)
hw.cpuspeed=2100
hw.vendor=Hetzner
hw.product=vServer

```

VPS des unteren Preissegments sind oft eher unflexible Linux-Container. Hetzners 2,96-Euro-VPS ist eine virtuelle Maschine, in der sich auch andere Betriebssysteme installieren lassen (Abb. 3).

ten nun 9,99 Euro. Wenig berauschend sind die zur Verfügung stehenden angestaubten Betriebssystem-Images: Bei Ubuntu reichte es in zweieinhalb Jahren gerade zum Update von 14.04 auf 16.04. Debian 9, Ubuntu 18.04 LTS oder Windows Server 2016 stellt Host Europe gar nicht bereit.

Server4You, eine Marke von Host Europe und damit GoDaddy EMEA, hat lediglich die Preise gesenkt. Einen **vServer** gibt es ab 5 Euro pro Monat.

Webtropia, eine Marke der myLoc managed IT AG, hat die Anzahl der vCPUs halbiert, den maximalen Arbeitsspeicher von 24 auf 16 GByte reduziert und den SSD-Speicherplatz beim Einstiegs-VPS um ein Drittel geschrumpft – dafür kostet der **vServer S 6.0** mit 3,99 Euro pro Monat auch nur noch die Hälfte. Einzelne vCPUs (+5 Euro), 1 GByte RAM (+2,50 Euro) oder Speicherplatz (+2,50 Euro für 50 GByte HDD oder 25 GByte SSD) lassen sich individuell zubuchen.

Strato hat den Einstiegspreis um gut 40 Prozent gesenkt, dafür aber die in seinem **V-Server Linux** enthaltenen vCPUs und den Arbeitsspeicher halbiert – im Endeffekt also eine Verteuerung. Der „SSD/HDD“-Speicher heißt so, weil er auf einer HP-3PAR-Speicherplattform liegt: Regelmäßig benutzte Daten liegen auf SSDs, wenig benutzte Datenbereiche lagert das System auf billigere Festplatten aus. Strato hat openSUSE aus dem Portfolio der Linux-Betriebssysteme gestrichen. Die Berliner gehören zu den wenigen Hostern, die VPS-Kunden mit einer 12-monatigen Mindestvertragslaufzeit gleich ein ganzes Jahr an sich binden.

Auch **1&1** hat beim **Virtual Server Cloud** die vCPUs und den SSD-Speicher etwas gestutzt, im Vollausbau ist mit 8 GByte RAM etwas mehr Arbeitsspeicher verfügbar. Über geschönte Preise versucht 1&1 nach wie vor, Kunden vermeintlich billige VPS zu verkaufen, die später deutlich teurer werden. Die echten, weil langfristigen Preise mit einmonatiger Vertragslaufzeit beginnen nun bei satten 9,99 Euro pro Monat für einen eher sparsam ausgestatteten VPS mit 1 vCPU, 1 GByte RAM und 50 GByte SSD – Host Europe verlangt denselben Preis, bei allerdings doppelter Ausstattung. Spannend: Auf einem VPS mit 1 GByte RAM lässt sich auch Windows Server 2016 für 10 Euro monatlich buchen – Windows läuft so nur ohne GUI, da die Oberfläche mindestens 2 GByte RAM voraussetzt. **IP-Projects** hat seine **Linux V-Server** von HDD auf

The screenshot shows a detailed configuration page for a server. At the top, there's a summary table with columns for 'Summen' (EUR) and 'Artikel'. The table includes rows for 'Gesamtsumme Konfiguration' (0,00 €), 'Gesamtsumme pro Monat (vor Steuern)' (249,94 €), and 'Endgültige Gesamtsumme pro Monat' (249,94 €). A note says 'Anteilige Anfangsgebühr' (not applicable). Below the table, there are several sections: 'Systemkonfiguration' (including 'Standort: Frankfurt 2', 'Server: Single Intel Xeon E3-1270 v3 (4 Cores, 3,50 GHz)', 'RAM: 8 GB RAM' (143,79 €), 'Betriebssystem: FreeBSD 11.x (64 bit)', 'Plattencontroller: Non-RAID', and 'Erste Festplatte: 1,00 TB SATA' (25,09 €)); 'Netzoptionen' (including 'Öffentliche Bandbreite: 500 GB Bandwidth Allotment', 'Uplink-Port-Geschwindigkeiten: 100 Mbps Public & Private Network Uplinks' (Öffentlicher Netzwerkport: 100 Mbps Public Uplink, Privater Netzwerkport: 100 Mbps Private Uplink)); 'Service-Add-ons' (including 'Überwachung: Host Ping' and 'Antwort: Automated Notification'); 'Erweiterte Systemkonfiguration' (including 'Bereitstellungsscripts' with a URL input field, 'SSH Keys' with a 'Hinzufügen' button, and 'Host- und Domänennamen' with a table for 'Server 1' showing 'Hostname: test' and 'Domäne: plura.de'); and a 'Fragen?' (Questions?) section with a note about accepting terms and conditions. The bottom right corner notes that 'Die Gesamtsummen variieren abhängig von den aktuellen Wechselkursen.'

Statt nur Ware von der Stange zu bieten, erlauben es einige Anbieter – wie hier IBM –, Bare-Metal-Server individuell zu konfigurieren (Abb. 4).

SSD umgestellt, bietet etwas mehr virtuelle Hardware und dazu um 20 Prozent gesenkte Preise. Statt 5 TByte Datentransfer pro Monat gibt es nun eine „fair use“-Flatrate, bis zu fünf IPv4-Adressen sind buchbar. Als interessantes Detail verrät IP-Projects, dass man „maximal 120 vServer pro Hostsystem“ konfiguriert. Erfreulich groß ist die Auswahl an Betriebssystemen, die von der Telefon-distribution Asterisk über Gentoo und openSUSE bis hin zu Oracle und Scientific Linux geht. Begrüßenswert ist, dass IP-Projects im Gegensatz zu anderen Anbietern ganz fair die (höheren) Preise für die einmonatige Vertragslaufzeit nennt. Kunden können den Vertrag aber auf sechs-, zwölf- oder 24-monatige Vorauszahlung umstellen, was IP-Projects mit 3, 5 oder 10 Prozent Rabatt belohnt.

Auch **Linevast** hat seine VPS aufgestockt, die sich preiswert als Linux-Container, etwas teurer als virtuelle KVM-Maschinen buchen lassen. Bis auf den Mainstream nahm der deutsche Hoster alle exotischen Linux-Versionen aus dem Programm und erhöhte den Einstiegspreis

für seinen **Linux vServer Basic** auf 6,99 beziehungsweise 7,99 Euro pro Monat – für 2 vCPUs (zuvor 1) und 4 GByte RAM (zuvor 0,5).

Die Jungs von **gridscale**, die jeden sofort duzen und eine ungewöhnliche, kachelartige und per Drag-and-Drop zu bedienende Weboberfläche verwenden, haben weiter an einer durchdachten Benutzerführung gearbeitet. Die Preise für ihren **CloudServer** sind nach wie vor hoch, dafür lässt sich beim Storage aber aufpreispflichtig zwischen unterschiedlichen SSD-Geschwindigkeiten wählen, wobei sich nicht erschließt, was und wie das skaliert wird. Eigene ISO-Images können als Grundlage für VPS dienen, die auch über eine API automatisch managbar sind. Die Abrechnung erfolgt stundenweise.

Bare-Metal-Server als Alternative

Dass Bare-Metal-Server ein lohnendes Geschäft sein müssen, zeigt der Einstieg

von Vultr und vor allem Amazon in diesen Bereich. **Vultr** bietet ab sofort einen Xeon E3-1270v6 mit 32 GByte RAM und zwei 240 GByte SSDs unter dem Namen **Bare Metal Simplified** für 120 US-Dollar pro Monat an. In diesem Preis ist laut Werbung ein 60%iger Rabatt enthalten, woraus sich ein stolzer Normalpreis von 300 US-Dollar ergibt. Im Vergleich zu den übrigen auch deutschen Angeboten ist das zu teuer. **Amazon** bietet ohne besondere Bewerbung seit rund einem Jahr seine **I3.Bare-Metal-Instanzen** an, die sich in Amazons VMware Cloud einbinden lassen. I3.Metal-Instanzen enthalten Intels Xeon-Prozessoren mit 2,3 GHz (36 Kerne plus HT), 512 GByte RAM und 15,2 TByte NVMe-Speicher, angebunden per 25 GbE.

Groß ist auch **IBM** im Geschäft, wobei das bei dem maximal ausgebauten **BI.S2.H880** wörtlich zu nehmen ist: Vier Intel E7-8890v4 mit je 24 Kernen (plus HT), satten 8 TByte RAM und 27 Laufwerken mit über 30 TByte Speicherplatz und einer redundant ausgelegten 10 GbE-Anbindung kosten 30 000 Euro Miete – pro Monat! IBMs Einstiegsklasse beginnt bei 250 Euro und einem E3-1279v3 mit 8 GByte RAM.

Günstigste Bare-Metal-Server für unter 40 Euro im Monat bekommt man beispielsweise bei **Server4You (Green Line)** und deren Muttergesellschaft **Host Europe (Dedicated Server S)**. Auch **Hetzners** Angebote starten mit dem **EX41-SSD** hier, allerdings mit doppelt so viel RAM (32 GByte). Eine Spezialität von Hetzner ist dazu die als Insider-Tipp geltende „Serverbörse“. Die Preise mancher der dort angebotenen Server sinken in regelmäßigen Abständen. Üblicherweise sind einfache Server ab etwas über 20 Euro pro Monat zu erhaschen. Die dort angegebenen CPU-B zeigen den Score des PassMark-Benchmarks an – was zu beachten ist, denn bei einem Wert von unter 1400 CPU-B reduziert sich die Netzwerkanbindung vom üblichen 1 GBit/s auf 100 MBit/s.

Hardware und leere 19"-Racks

Einfache Bare-Metal-Server sind bei eigentlich allen Anbietern für unter 100 Euro Monatsmiete zu bekommen. Wo die VPS jedoch preismäßig enden,

geht es bei den physischen Servern erst richtig los. Für leistungsfähige Hardware müssen Kunden gerne auch ein paar Hundert Euro pro Monat bezahlen. Im Vergleich zur entsprechenden Hardware mag das teuer wirken, jedoch muss man hier den Standort im Rechenzentrum samt Infrastruktur dazurechnen.

Bei Bare-Metal-Servern gibt es bei einigen Anbietern zusätzlich Optionen, die man von VPS nicht kennt. Zunächst kann man, da es sich um Hardware handelt, diese auch aufrüsten. Weitere SSDs/NVMes/Festplatten samt RAID-Controller, mehr RAM oder zusätzliche Netzwerkkarten sind gegen Aufpreis möglich. Auch ein lokales physisches Netz (LAN) mit eigenem Switch ist machbar, sofern alle Server in einem Rack untergebracht sind. Dort lässt sich unter Umständen auch freier 19"-Platz reservieren.

Einzig das Besichtigen des Servers wird aus Sicherheitsgründen nicht erlaubt. Hierfür kann man bei einigen Anbietern in gesonderten Teilen des Rechenzentrums eine „Colocation“ mieten. Das geht von einem einzelnen Einschub in einem Rack über ein komplettes, abschließbares Rack für eigene Serverhardware bis hin zu besonders gesicher-

Anbieter von Bare-Metal-Servern (Teil 1)

	1&1 Internet SE	1blu AG	Hetzner Online GmbH	Hetzner Online GmbH	Host Europe GmbH	IBM Corp.	IBM Corp.
Firmensitz	Montabaur, D	Berlin, D	Gunzenhausen, D	Gunzenhausen, D	Köln, D	Armonk, NY, USA	Armonk, NY, USA
Produkt	Bare Metal Server S SSD	DedicatedServer XP	EX41-SSD	SX292	Dedicated Server S	Intel Xeon E3-1270 v3	BI.S2.H8800
Anzahl Produkte min./max.	3 min.	3 min.	18 + Serverbörse min.	18 + Serverbörse max.	6 min.	85 min.	85 max.
Ausstattung							
CPU (Kerne)	Intel E3-1230-v6 (4)	Intel E3-1230v2 (4)	Intel Core i7-6700 (4)	Intel E5-1650v3 (8)	Intel E5v4 (8)	Intel E3-1279v3 (4)	Intel E7-8890v4 (4 x 24)
RAM (GByte)	16	16	32	256	16	8	8192
SSD	480 GByte	–	2 x 500 GByte	–	2 x 500 GByte	gegen Aufpreis	3 x 800 GByte + 8 x 1,2 TByte + 18 x 1,2 TByte
alternativ HDD	1 TByte (10 € günstiger)	2 x 2 TByte	✓, 2 x 4 TByte	15 x 10 TByte	2 x 2 TByte (10 € günstiger)	1 TByte	–
Netzanbindung							
Anbindung (Gbit/s)	0,4	1	1	1	1	0,5	10 (redundant)
Inklusivvolumen (TByte)	unbegrenzt	unbegrenzt	30	100	unbegrenzt	0,5	unbegrenzt
IPv4-Adressen	1	2	1	1	1	1	1
zusätzliche Adressen	✓	k. A.	bis /27 (30 IPs) für 32,00 €	bis /27 (30 IPs) für 32,00 €	k. A.	Aufpreis 4 IPs: 3,86 €, 8 IPs: 7,72 €	k. A.
IPv6-Subnetz	/64	k. A.	/64	/64	k. A.	/64 optional (Aufpreis 4,83 €)	k. A.
Administration							
Bereitstellung	k. A.	k. A.	k. A.	k. A.	<60 Minuten	30 Minuten	2–4 Stunden
Verwaltung	Plesk	KVM over IP	VNC, Plesk, cPanel	VNC, Plesk, cPanel	k. A.	Plesk, cPanel	KVM over IP
API, Scripting	k. A.	k. A.	✓	✓	k. A.	✓, SoftLayer API ²	✓, SoftLayer API ²

alle Daten Herstellerangaben; ¹ nur bei Reinstalltion; ² siehe ix.de/ix1810040

ten Räumen. Viele Möglichkeiten und Informationen dazu bietet beispielsweise die KAMP Netzwerkdienste GmbH (www.kamp.de).

Benchmarks wenig sinnvoll

Es ist schwierig, die tatsächlich verfügbare Leistung eines VPS zu beurteilen. So genannte „Noisy Neighbors“ können die Ressourcen des Hosts kurzfristig auslasten und so die Ergebnisse verfälschen. Man müsste Benchmarks also über einen langen Zeitraum sehr häufig fahren, um die maximale, die durchschnittliche sowie die minimale Leistung einigermaßen akkurat ermitteln zu können. Dabei wiederum produziert man genau das, was alle anderen VPS-Nutzer auf dem Host haben: einen „Noisy Neighbor“.

Das automatische Ressourcenmanagement des Hosters verteilt VPS darüber hinaus im Laufe der Zeit, sodass für alle Kunden (das können mehr als hundert sein) auf einem Host eine ausgewogene Leistung bereitsteht. Ein VPS „wandert“ also unter Umständen im Laufe der Zeit auf andere Hardware – per Live-Migration.

The screenshot shows the Hetzner Online GmbH Robot interface. On the left, there's a sidebar with navigation links like Administration, Einstellungen, 2-Faktor-Auth, Rechnungen, Hauptfunktionen (DNS-Einträge, Storage Boxes, Server, Traffic-Statistik, Verlauf), and Service (Bestellung, Serverbörse, Newsletter, Störungsmeldungen). The main area is titled "Server" and shows a table for "EX41-SSD (30 TB #90)". The table includes columns for IP, Reset, Rescue, Linux, VNC, Windows, cPanel, Plesk, WOL, Backup, Monitoring, Addons, Adminzugang, Telefonpasswort, Übertragung, Support, Kündigung, Verlauf, and Firewall. Below the table, there's a note with instructions for Reverse-DNS entries and traffic limits. Further down, there are sections for IP-Adressen and Subnetze, each with traffic limit reporting settings. At the bottom, there are buttons for Zeige Trafficstatistik, Traffic Flatrate, and Zusätzliche Ips / Netze bestellen.

Die Verwaltung eines Bare-Metal-Servers ist umfangreicher als die eines VPS, wodurch er sich flexibler einsetzen lässt (Abb. 5).

	InterNetX GmbH	Leaseweb Deutschland GmbH	Leaseweb Deutschland GmbH	OVH GmbH	Packet	Packet	Server4You	Vultr Holdings Corp.
Regensburg, D	Frankfurt am Main, D	Frankfurt am Main, D	Saarbrücken, D	New York, USA	New York, USA	Hürth, D	Matawan, NJ, USA	
BM 1	Intel Quad-Core Xeon E3-1230	Dell R930	HOST-32L	t1.small.x86	m2.large.x86	Green Line	Bare Metal Simplified	
4 min.	k. A.	k. A.	35	9 min.	9 min.	3 max.	1, weitere geplant einzig	
Intel E5 (4)	Intel E3-1230 (4)	4x Intel E7-4850v3 (4 x 14)	Intel Xeon D-1520 (4)	Intel Atom C2550 (4)	2x Intel 5120 (2 x 14)	AMD Opteron mit 2,4 GHz (8)	Intel E3-1270v6 (8)	
64	8	384	32	8	384	16	32	
2 x 280 GByte NVMe	–	8 x 960 GByte	2 x 480 GByte (Aufpreis 13,10 €)	80 GByte	2 x 120 GByte NVMe	2 x 250 GByte	2 x 240 GByte	
2 x 1 TByte (zusätzlich)	4 x 1 TByte	–	✓, 2 x 2 TByte	–	3,8 TByte (zusätzlich)	2 x 2 TByte (10 € günstiger)	–	
2 x 1 (LACP)	1	1	0,25 (Burst: 1)	2,5	2 x 10	0,1	10	
1 TByte /29	10 TByte k. A.	unbegrenzt	unbegrenzt	k. A.	k. A.	unbegrenzt („fair use“)	5	
k. A.	1	1	1	1	1	1	1	
5,00 € pro zusätzlicher IP, max. 16	5,00 € pro zusätzlicher IP, max. 16	2,40 € pro zusätzlicher IP	k. A.	k. A.	bis zu 3 IPs zusätzlich je 2,00 € pro Monat	k. A.	k. A.	
/64	k. A.	k. A.	/64	k. A.	k. A.	k. A.	optional	
ca. 10 Tage	k. A.	k. A.	120 Sekunden	k. A.	k. A.	k. A.	„in Minuten“	
Plesk, LiveConfig	k. A.	Plesk, cPanel	ISPConfig 3, Plesk, cPanel, DirectAdmin	k. A.	k. A.	Plesk, cPanel	Web-Frontend, cPanel, Plesk	
k. A.	k. A.	k. A.	✓	k. A.	k. A.	k. A.	✓	

Anbieter von Bare-Metal-Servern (Teil 2)

Anbieter	1&1 Internet SE	1blu AG	Hetzner Online GmbH	Hetzner Online GmbH	Host Europe GmbH	IBM Corp.	IBM Corp.	
Betriebssysteme								
Linux	Arch Linux ¹ , CentOS 6/7, Debian 8/9, openSUSE ¹ , Ubuntu 16.04/18.04 LTS	Ubuntu 16.04 LTS	Arch Linux, CentOS 6.10/7.5, Debian 9.5, Fedora 28, openSUSE 42.3, Ubuntu 16.04.5/18.04.1 LTS	Arch Linux, CentOS 6.10/7.5, Debian 9.5, Fedora 28, openSUSE 42.3, Ubuntu 16.04.5/18.04.1 LTS	CentOS 7, Debian 9, Ubuntu 16.04/18.04 LTS	CentOS 6/7, Cloud-Linux 6, Debian 8/9, RHEL 6/7, Ubuntu 14.04/16.04 LTS	RHEL 7.4 für SAP HANA, SLES 12 SP2 für SAP HANA	
Free-/Net-/OpenBSD	–	–	–	FreeBSD 10.1 (Rescue System)	–	FreeBSD 10/11	–	
Windows	Server 2012/2016	–	Server 2016 Standard/Datacenter Edition	Server 2016 Standard/Datacenter Edition	–	Server 2012 R2 / 2016 Standard/Datacenter Edition	–	
sonstige, Virtualisierung	CoreOS ¹	–	ISO-Image	ISO-Image	–	Brocade (Virtual Router), Citrix Xen 7, VMware ESXi 6.0/6.5	–	
RZ-Standorte								
Deutschland	✓	Frankfurt am Main	✓	✓	k. A.	Frankfurt am Main	Frankfurt am Main	
Europa	✓ (im Produkt als Neuanlage)	–	Helsinki	–	–	Amsterdam, London, Mailand, Paris	Amsterdam, London, Mailand, Paris, Oslo	
USA/Kanada	✓	–	–	–	–	Dallas, Houston, Seattle, San Jose, Washington, D.C., Montreal/Toronto	Dallas, Washington, D.C., Montreal/Toronto	
Asien/Pazifik	–	–	–	–	–	Hongkong, Seoul, Tokio, Melbourne/Sydney	Hongkong, Seoul, Tokio, Chennai, Singapur, Melbourne/Sydney	
sonstige	–	–	–	–	–	Queretaro (MX)	Queretaro (MX), Sao Paulo (BR)	
Preise und Laufzeit								
Einrichtung	–	89,00 €	0,00 € (HDD), 94,01 € (SSD)	320,11 €	99,99 €	–	–	
Mindestvertragslaufzeit	–	1 Monat	–	–	–	1 Monat	1 Monat	
stündlich	0,069 €	k. A.	k. A.	k. A.	–	– (0,588 €) ³	–	
monatlich	49,99 €	69,00 €	40,46 €	320,11 €	39,99 €	249,84 €	29 832,40 €	
Anmerkungen	Software-RAID1, Preise laufzeit-abhängig	6 Monate: 0,00 € Einrichtung, erste 6 Monate 39,00 €	„Serverbörsen“ ab 23,00 €			Nettopreis	Nettopreis	

alle Daten Herstellerangaben; ¹ nur bei Reinstalltion; ² siehe ix.de/ix1810040; ³ ein besser ausgestattetes Modell

tion übrigens ohne eine Unterbrechung des Betriebs.

Betreibt man mehrere VPS bei verschiedenen Anbietern, fällt gerade bei wenig genutzten VPS auf, dass diese manchmal erst nach zwei/drei Sekunden auf eine Anfrage reagieren, dann aber wesentlich schneller ansprechbar sind. Dass die Leistung wirklich komplett über einen längeren Zeitraum einbricht, ist eher unwahrscheinlich.

Sag mir, wie alt du bist

Viel störender kann es sein, dass ein VPS aus unerfindlichen Gründen neu gestartet wurde, die *uptime* verrät dies manchmal. Das bedeutet für das Einrichten eines jeden VPS aber, dass er „reboot-fähig“ sein

sollte, nach einem Neustart also alle benötigten Dienste automatisch startet und kein händisches Eingreifen verlangt.

Wer die Leistung seiner VPS testet, bemerkt dennoch ein paar Unterschiede. Hochpreisige VPS tendieren dazu, schneller zu sein als ihre Kampfpreis-Pendants. Das verwundert wenig, schließlich muss sich ein Angebot für den Hoster finanziell irgendwie rechnen.

Dennoch muss man sich ehrlich die Frage stellen: Ist die Geschwindigkeit eines VPS in einem Rechenzentrum mit professioneller Infrastruktur bei einem Preis von unter 36 Euro pro Jahr (Vultr, Hetzner) überhaupt relevant? Wer wirklich mehr Leistung braucht, ist sicherlich auch bereit, dafür zu bezahlen, und bucht einfach ein paar vCPUs und RAM dazu. Muss ein Server verlässlich und jederzeit

eine definierte Leistung erbringen können, eignen sich VPS prinzipiell sowieso nicht: Hier empfiehlt sich der Schritt zum Bare-Metal-Server.

Letztlich beeinflusst die Anbindung des Hosters an die großen Internet-Backbones die „gefühlte“ Geschwindigkeit. Die Auswirkungen zeigen sich meistens erst bei sehr hohen Lasten und hängen von der eigenen Anbindung ans Internet oder der Zielgruppe ab. Die meisten Hoster sind gut vernetzt und geben an, an welche Backbones sie direkt angeschlossen sind: Das können die der Deutschen Telekom, von Level 3, Global Crossing, cogen, DE-CIX, interoute und anderen Backbone-Betreibern sein. Vorbildlich aufgelistet findet man solche Informationen beispielsweise bei Hetzner im Unternehmensprofil unter „Data Centers“. Ei-

	InterNetX GmbH	Leaseweb Deutschland GmbH	Leaseweb Deutschland GmbH	OVH GmbH	Packet	Packet	Server4You	Vultr Holdings Corp.
	CentOS, Debian, RHEL, Ubuntu, weitere a. A.	CentOS 6/7, Debian 8/9, Ubuntu 14.04/16.04 LTS	CentOS 5/6/7, Debian 8/9, Ubuntu 12.04/14.04/16.04 LTS	Arch Linux, CentOS 6/7, CloudLinux 7, Debian 8/9, Fedora 26/27, Gentoo, openSUSE, Ubuntu Server 14.04 LTS/16.04 LTS/17.10	CentOS 7, Debian 8/9, NixOS 18.03, openSUSE 42.3, Scientific Linux 6, Ubuntu 14.04/16.04/18.04 LTS und 17.10	CentOS 7, Debian 8/9, NixOS 18.03, Scientific Linux, Ubuntu 14.04/16.04/18.04 LTS und 17.10	CentOS, Debian, Ubuntu	CentOS 6/7, Debian 8/9, Fedora 27/28, Ubuntu 14.04/16.04/18.04 LTS
k. A.	FreeBSD 10/11	FreeBSD 10/11	FreeBSD 10/11	FreeBSD 10/11	FreeBSD 10.3/10.4/11.0/11.1	FreeBSD 10.3/10.4/11.0/11.1	FreeBSD	FreeBSD 10.4/11.2, OpenBSD 6.3
Server 2016	Server 2012 R2 Standard/Data-center Edition	Server 2012 R2 Standard/Data-center Edition	Server 2012 R2 / 2016 Standard/Datacenter Edition	Server 2012 R2 / 2016	–	–	Webserver 2008 R2	Server 2012 R2 / 2016
ISO-Image	VMware ESXi 5.5/6.0	VMware ESXi 5.5	nur bei höherwertigen Produkten: Citrix Xen 7, CoreOS, Proxmox VE 4/5, SmartOS, SolusVM, VMware ESXi 6.0/6.5	CoreOS, Custom iPXE, RancherOS	CoreOS, Custom iPXE, RancherOS	–	CoreOS, ISO-Image, CentOS/Debian/Ubuntu auch 32-Bit	
München	Frankfurt am Main	Frankfurt am Main	Limburg	–	–	–	Frankfurt am Main	
–	Amsterdam, London	Amsterdam, London	Gravelinnes, London, Roubaix, Straßburg, Warschau	Amsterdam	Amsterdam (zum Testzeitpunkt nicht verfügbar)	Straßburg	Amsterdam	
–	Chicago, Dallas, New York, Phoenix, San Francisco, Washington, D.C.	Chicago, Dallas, New York, Phoenix, San Francisco, Washington, D.C.	Beauharnois (CAN)	New York, Sunnyvale	New York, Sunnyvale	St. Louis	Chicago, Los Angeles, Miami, New York, Silicon Valley	
–	Hongkong, Singapur, Sydney	Hongkong, Singapur, Sydney	Singapur, Sydney	Tokio	Tokio	–	Singapur	
–	–	–	–	–	–	–	–	
99,90 €	–	–	–	k. A.	k. A.	19,00 €	–	
36 Monate	1 Monat	1 Monat	1 Monat	k. A.	k. A.	1 Monat	–	
k. A.	k. A.	k. A.	–	0,07 US-\$	2 US-\$	k. A.	0,179 US-\$	
199,90 €	47,59 €	2 269,11 €	72,00 €	–	–	34,99 €	120 US-\$	
Managed Services: 99,00 €/Jahr, keine Einrichtungskosten			internes privates Netzwerk (vRack)	Preise nur per Stunde	Preise nur per Stunde		Abrechnung stundenweise, Deckelung bei 120 US-\$/Monat	

nen ersten Anhaltspunkt für die Anbindung vom eigenen Standort her können *traceroute* (Linux) oder *tracert* (Windows) auf die IP des VPS oder Bare-Metal-Servers liefern.

Fazit

Die Preise für VPS sind weiter gefallen, allerdings nicht auf breiter Front – OVH wurde beim Einstiegs-VPS sogar teurer. Es gibt jedoch etwas mehr Leistung (vCPUs, RAM) und vor allem mehr SSD-Speicher. Galten SSDs bei einem VPS vor zweieinhalb Jahren noch als technischer Leckerbissen, sind sie nun dank des massiven Preisverfalls und der Vorteile beim Betrieb im Rechenzentrum Standard. Klassische Festplatten kann

man allenfalls als billige Datengräber hinzubuchen.

Auffallend ist, dass die Hoster mit den IPv4-Adressen knausern. Gab es vor zwei-einhalb Jahren zusätzliche IPv4-Adressen teilweise noch kostenlos (bei Host Europe gab es pro gebuchter vCPU eine IPv4-Adresse), erhält man nun oft nur noch einen IPv4-Zugang. Vultr beschränkt sein 2,50-Dollar-Kampfangebot sogar kategorisch auf den IPv6-Adressraum.

Bare-Metal-Server sind nichts Neues, sind aber in der Cloud angekommen. Mit wenigen Klicks ausgerollt sind sie zwar nicht wie in der Werbung versprochen in Minuten, aber für physische Hardware erstaunlich schnell in einer oder wenigen Stunden betriebsbereit. Durch den deutlichen Preisverfall und die immer neuen Sicherheitslöcher auf insbesondere Intel-

CPUs ist ein Wechsel von einem großen VPS auf einen kleinen Bare-Metal-Server auf jeden Fall eine attraktive Option.
(avr@ix.de)

Michael Plura

arbeitet in Schweden als freier Autor mit den Schwerpunkten IT-Sicherheit, Virtualisierung und freie Betriebssysteme.

Literatur

- [1] Michael Plura; Cloud-Computing/I; Server im Spiel; Marktübersicht: Virtual Private Server für KMU; iX 2/2016, S. 26

Windows Server 2019 und Exchange Server 2019

Serverpflege

Nils Kaczenski



Im Herbst bringt Microsoft die 2019er-Versionen von Windows Server und Exchange auf den Markt. Neues gibt es vor allem für große Rechenzentren.

Demnächst wird Microsoft neue Hauptversionen seiner beiden Premiumprodukte für das Rechenzentrum veröffentlichen. Windows Server 2019 und Exchange Server 2019 will das Unternehmen auf seiner Hauskonferenz „Ignite“ Ende September in Orlando, Florida, vorstellen. Wie bei den Vorgängerversionen dürfte damit auch der Launch beider Produkte stattfinden und die allgemeine Verfügbarkeit für Kunden und Händler im Oktober folgen. Auch die Client-Produkte Windows 10 und Office sollen dann erneuert vorliegen. Mit seiner

Management-Suite System Center hingegen will sich Microsoft bis zum kommenden Frühjahr Zeit lassen.

Technisch beruhen das Client-Windows und dessen großer Server-Bruder auf derselben Codebasis. Während Microsoft bei Windows 10 aber seit dessen Erscheinen im Sommer 2015 auf regelmäßige Updates setzt (derzeit zweimal jährlich), gibt es das vollwertige Serverprodukt traditionell im Abstand von etwa drei Jahren. Da dieser lange Zyklus im Zeitalter der Container-Technik nicht mehr ausreicht, hat man in Redmond vor einem Jahr auch

für den Server eine halbjährliche Update-Frequenz ersonnen. Diese „Semi-annual Releases“ gelten allerdings nicht als Vollversionen, sondern zielen ausdrücklich auf reduzierte „Nano“-Server, die nur ausgewählte Dienste ausführen können. Das eignet sich als Container-Grundlage, aber nicht für herkömmliche Allzweckserver.

Ausgefeilteres Servermanagement

Auf Windows Server 2019 konnten Kunden vorab in drei Preview-Versionen einen Blick werfen. Von der Oberfläche her unterscheiden sich diese nicht von ihrem Vorgänger Server 2016 – technisch allerdings ebenfalls kaum. Die wesentliche Arbeit hat Microsoft in Funktionen fürs Rechenzentrum gesteckt; wie schon in den vergangenen Jahren gibt es für die Brot-und-Butter-Funktionen von Windows Server praktisch nichts Neues zu vermelden. Auch weiterhin stehen drei Installationsvarianten zur Verfügung: die fokussierten Fassungen Nano und Core sowie die komplette Installation mit dem Kennzeichen „Desktop Experience“. Nur letztere enthält das vertraute GUI. Die Entscheidung fällt beim Installieren; ein Wechsel etwa von Core zum GUI ist nicht möglich.

Während sich ein Nano-Server nur automatisiert mit festgelegten Funktionen einrichten und auch nur remote verwalten lässt, hat die nächsthöhere Variante Core nun „Features on demand“ an Bord, mit denen sich Funktionsmodule nachrüsten lassen. Damit führt Microsoft den modularen Aufbau des Betriebssystems weiter und will den Einsatz der Core-Installation nicht zuletzt wegen deren kleinerer Angriffsfläche attraktiver machen. Ein wichtiger Schritt besteht darin, dass sich Core-Server nun auch endlich für Exchange eignen, dazu weiter unten mehr.

Den Betrieb seiner Server will Microsoft mit zwei Neuerungen erleichtern. System Insights nennt der Hersteller eine neue Infrastruktur für Monitoring und Analyse, die Voraussagen zu Stabilität und Leistung des Systems treffen soll. Eine Cloud-Integration ist dafür ebenso wenig erforderlich wie beim neuen Administrations-Framework Windows Admin Center, zuvor unter dem Projektnamen „Honolulu“ bekannt. Als Webapplikation soll das neue Werkzeug die zuvor versprengten Tools wie den Servermanager und diverse MMC-Konsolen überwinden und eine zentrale Instanz zur Administration bereitstellen. Der Weg dahin ist al-

Einträgliche Abkehr vom R2-Modell

Mit der neuen Windows-Version verabschiedet sich Microsoft stillschweigend vom Release-Modell der letzten 15 Jahre. Bisher gab es immer abwechselnd eine neue Hauptversion (mit Jahreszahl) und eine Zwischenversion mit angehängtem „R2“. So konnte der Hersteller kaschieren, dass es von Version zu Version manchmal nur wenig Neues gab.

Auf Windows Server 2016 folgt aber kein R2, sondern gleich die neue Major-Version 2019. Das ist nicht nur Kosmetik, sondern kostet die Kunden viel Geld. Bisher galten die Clientlizenzen (Client Access License, CAL) nämlich sowohl für die Hauptversion als auch für den R2-Nachfolger. Kunden mussten also nur bei jeder zweiten Release die Clients neu

lizenzierten. Das ändert sich nun: Server 2019 erfordert neue CALs, auch wenn bereits flächendeckend 2016-CALs vorhanden sind.

Das grundlegende Serverlizenzmödell soll unverändert bleiben, die CPU-Kerne der Hardware bilden wieder die Grundlage für die Anzahl der Lizenzen. Ebenso sind virtuelle Windows Server über die Hauptlizenz der Hosthardware mitlizenziert (unbegrenzte VM-Anzahl nur in der Datacenter Edition).

Parallel zur angekündigten Preiserhöhung wird die Neulizenenzierung Kunden also teuer zu stehen kommen. Die Verbreitung des neuen Servers dürfte Microsoft damit nicht beschleunigen.

lerdings auch nach der ersten Release noch weit, denn derzeit kann das Admin-Center nur eine kleine Auswahl lokaler Konfigurationen und Funktionen steuern. Komplexe Applikationen wie das Active Directory sind noch nicht eingebunden. Immerhin steht das Center über APIs auch Drittherstellern für Erweiterungsmodulen offen, wenige erste Partner haben schon grundlegende Plug-ins im Angebot.

Windows für Speichersysteme

Eine gewisse Ernsthaftigkeit darf man Microsofts Ambitionen bescheinigen, seinen Server zum Storage-Backend auszubauen. Den RAID-Ersatz Storage Spaces hatte der Hersteller in Windows Server 2016 als Storage Spaces Direct (S2D) mit Replikation und Tiering zur Basis von Hyperconverged-Systemen ausgebaut. Hier legen Virtualisierungshosts ihre Daten auf lokalen Plattensystemen ab, die mit Redundanz- und Replikationslogiken eine hohe Zuverlässigkeit und Performance innerhalb ihres Verbunds gewährleisten.

Die neue Server-Release verbessert diese Funktion im Detail und bewirkt mit S2D Performance History eine bessere Kontrolle der Systemleistung. Ein neuer halbmanueller Modus zur Datenverteilung soll in bestimmten Setups besseren

Schutz vor Datenverlusten bei Teilausfällen bieten. Interessant für kleinere Unternehmen ist, dass die Storage-Funktionen Replica und S2D künftig teilweise auch mit der Standardlizenz verfügbar sind und nicht mehr die teure Datacenter Edition erfordern.

Eine etwas überraschende Neuerung bietet Server 2019 im Bereich „klassischer“ Dateiserver. Während deren Grundfunktionen seit Windows 2000 nahezu unverändert geblieben waren, bringt der neue Server nach vielen Jahren diesmal ein neues Managementwerkzeug mit: Der Storage Migration Service soll es Administratoren erleichtern, von älteren Windows-Dateiservern auf die neue Version umzusteigen. Eine solche Migration erfordert oft langwierige Planungen und sorgfältig aufeinander abgestimmte Schritte, die der neue Dienst großteils automatisieren und vereinfachen soll. Dazu analysiert er die Quell- und Zielsysteme und schlägt Konfigurationsschritte und Migrationsjobs vor.

In großen Umgebungen bleiben indes einige Wünsche offen: So ist eine Anpassung von Berechtigungsstrukturen derzeit ebenso wenig vorgesehen wie eine Neudefinition der Ordnerhierarchien. Immerhin gibt es eine Roadmap zur weiteren Entwicklung des Dienstes, die vermutlich mit Updates ins System kommt (siehe ix.de/ix1810052).

IX-TRACT

- Microsoft wird voraussichtlich noch im Herbst 2018 seinen Server 2019 und Exchange 2019 auf den Markt bringen.
- Für Endanwender sind kaum Neuerungen spürbar, etwas mehr tut sich für Administratoren und die Betreiber von Rechenzentren.
- Neue Erscheinungsintervalle ohne R2-Zwischenausgaben werden zu einer deutlichen Verteuerung der Lizenzkosten beitragen.



AHA-EFFEKT GESUCHT?

Schulungen für Linux-Admins, die durchblicken wollen.

Schulung von Profis, das ist wörtlich zu nehmen. Vielen Dank, konnte sehr viel mitnehmen und freue mich auf die nächste Schulung.

Werbeaussage „obere 10% des Wissens“ eingehalten.

Sehr lehrreicher Kurs mit kompetenten, offenen und sympathischen Mitarbeitern. Exzellente Verpflegung und Organisation!

Jetzt anmelden:

www.heinlein-akademie.de

heinlein
akademie

System Insights > CPU capacity forecasting – Übersicht

Aufrufen Settings Disable

Übersicht

Status	Prognose	Last run	Schedule
Ok	Die CPU-Auslastung wird voraussichtlich innerhalb der verfügbaren Kapazität bleiben.	4.9.2018, 13:35:00	Alle 5 Minuten

Prognose

CPU ↑

Verlauf Prognose

150 %
100 %
50 %
0 %

3.8.2018 10.8.2018 17.8.2018 24.8.2018 31.8.2018 7.9.2018 14.9.2018

Stabile Virtualisierungsgrundlage

Auf dem Gebiet der Virtualisierung scheint die Zeit der großen Entwicklungen vorbei. Hyper-V hat sich als robuste Grundlage für virtuelle Serverumgebungen in Unternehmen jeder Größe und in Rechenzentren etabliert. Der Ehrgeiz, Platzhirsch VMware von den Futterstellen zu vertreiben, scheint aber verflogen zu sein: Microsoft setzt offenkundig eher darauf, die Infrastruktur der erfolgreichen Azure-Cloud zu versorgen, die auf Hyper-V beruht und zu der VMware kein echtes Pendant hat. Cloud-Umgebungen setzen seit einiger Zeit verstärkt auf Container-Virtualisierung, die Hyper-V seit der letzten Release im Server 2016 nativ beherrscht.

Neben einer verbesserten Docker-Integration bietet Server 2019 Container-Betreibern zwei wesentliche Neuerungen. Das Windows Subsystem for Linux (WSL) soll es ermöglichen, Container mit

Windows-Basis auf demselben Wirt zu betreiben wie solche mit Linux-Unterbau. Letztere benötigen dann keine Linux-VM mehr als Grundlage, sondern nutzen direkt die WSL-Komponente in Windows, die sich an Ubuntu orientiert. Damit will Microsoft Windows als einheitliche Basis für heterogene Container-Applikationen ins Spiel bringen. Auch hier ist technisch noch viel zu tun, wenn auch Beobachter den Redmontern beachtliche Zwischenfolge bescheinigen.

Der zweite Entwicklungsstrang bezieht sich auf die Container-Orchestrierung mit Kubernetes. Die Software, die auf Google zurückgeht, ist derzeit der De-facto-Standard für komplexe Webapplikationen, die aus einer Vielzahl von Containern bestehen. Erst seit diesem Sommer bietet Microsoft – den Anforderungen des Marktes gehorrend – Kubernetes-Dienste in seiner Azure-Cloud offiziell an. Von diesen Anstrengungen können Kunden nun auch in ihren eigenen Infrastrukturen profitieren. Der Hintergedanke: Unternehmen sollen auf

In Gestalt von System Insights bietet Server 2019 ein Monitoring mit Prognosefunktion (Abb. 1).

ihren Systemen eine Anwendungswelt vorfinden, die sie mit möglichst geringem Aufwand in Microsofts Cloud erweitern und schließlich übertragen können.

Sicherheit im Detail

Die neuen Sicherheitsfunktionen im Server 2019 konzentrieren sich ebenfalls auf virtuelle Infrastrukturen. Software-defined Networks (SDN) lassen sich in der neuen Release auf niedriger Ebene verschlüsseln. Davon profitieren Anwendungen, die intern noch keine Mechanismen wie TLS beherrschen. Gleichzeitig verbessert dieser Ansatz die Trennung unterschiedlicher Mandanten, die ihre virtuellen Netzwerke im VM-Rechenzentrum eines Providers laufen lassen.

Dasselbe Szenario gehen Shielded VMs an. Die in Windows Server 2016 eingeführte Technik gibt Kunden die Garantie, dass ihre VMs durch vollständige Verschlüsselung von den RZ-Administratoren ihres Providers nicht zu manipulieren sind. Das erfordert beim Provider eine aufwendige Infrastruktur, ermöglicht diesem aber, auch vertrauliche Kunden-Workloads in sein RZ zu holen. Der Server 2019 bringt hier etwas mehr Flexibilität, unter anderem durch einen Offlinemodus für verschlüsselte VMs. Dieser lässt eine vorhandene Shielded VM auch dann starten, wenn die separate Sicherheitsinfrastruktur vorübergehend nicht antwortet.

Verbesserungen der Windows-Cluster-technik sollen die Betriebssicherheit im RZ erhöhen. Das neue logische Konstrukt Cluster Sets fasst mehrere separate Windows-Cluster zu einer Verwaltungseinheit zusammen. Dadurch lässt sich die technische Obergrenze von 64 Servern überwinden, die einen Failover-Cluster bilden. Diese Grenze technisch zu erweitern, hätte größere Risiken für die Stabilität bedeutet, sodass der neue Ansatz einige Beschränkungen im täglichen Betrieb auf andere Weise aufhebt.

Logische Umstellungen im RZ werden dadurch einfacher, dass Windows-Cluster künftig die Domäne wechseln können. Bisher war es immer sehr umständlich, Clustersysteme von einem Active Directory in ein anderes zu überführen, etwa



Exchange 2019 lässt sich erstmals auch in der Core-Variante des Serverbetriebssystems installieren. Das erhöht die Sicherheit und reduziert die Zahl der System-Updates (Abb. 2).

In einer Core-Installation lässt sich Exchange 2019 lokal verwalten – aber ohne GUI, nur über die PowerShell (Abb. 3).

bei Konsolidierungen oder Eigentümerwechseln des Unternehmens. Weitere Detailverbesserungen im Clustering betreffen den File Share Witness als Entscheidungsinstanz bei Teil-ausfällen im RZ sowie den vollständigen Verzicht auf das veraltete Authentifizierungsprotokoll NTLM in Clustersystemen.

Gemeinsam mit dem neuen Server-Windows wird ein neuer Exchange Server erscheinen. Schon seit Windows 2000 gab es stets einen Zusammenhang zwischen dem Server-OS und dem Messaging-System, doch so direkt waren die Versionen selten aufeinander bezogen. Dennoch ist Windows Server 2019 keine Voraussetzung, das neue Exchange zu betreiben, bildet aber die bevorzugte Plattform. Die Exchange-Preview ließ sich auch unter Server 2016 installieren, das wird wohl auch für das fertige Produkt gelten.

Exchange ein bisschen neu

Das Installieren des Systems bildet gleich die größte Neuerung von Exchange Server 2019: Erstmals lässt sich die Software auf einem Core-Server einrichten, einer reduzierten Variante des Serverbetriebssystems, die nicht nur auf eine grafische Oberfläche, sondern auch auf zahlreiche Komponenten und Bibliotheken verzichtet. Das hatte in der Vergangenheit dazu geführt, dass komplexe Applikationen wie Exchange nicht darauf liefen.

Parallel dazu hat Microsoft die Grenzen der Skalierbarkeit ausgeweitet. Ein Exchange Server darf künftig bis zu 48 CPU-Cores und 256 GByte Arbeitsspeicher nutzen. Das interessiert nur sehr große Rechenzentren, denn die bisherigen Limits ließen sich durch horizontales Skalieren auf mehrere Server meist gut handhaben. Das Verteilen auf eine Exchange-Serverfarm bleibt auch künftig relevant, um die Verfügbarkeit bei einzelnen Serverausfällen hoch zu halten.

Funktional ist für die neue Exchange-Version hingegen wenig Neues in Sicht.

Name	Alias	ServerName	ProhibitSendQuota
Sirup, Aaron	aaron.sirup	ex19	Unlimited
Kahn, Ada	ada.kahn	ex19	Unlimited
Lass, Ada	ada.lass	ex19	Unlimited
Tion, Addi	addi.tion	ex19	Unlimited
ADFS Service	adfs-service	ex19	Unlimited
Lette, Adi	adi.lette	ex19	Unlimited
ter Native, Al	al.ternative	ex19	Unlimited
Herum, Albert	albert.herum	ex19	Unlimited
Platz, Alexander	alexander.platz	ex19	Unlimited
Bert, Ali	ali.bert	ex19	Unlimited
Mente, Ali	ali.mente	ex19	Unlimited
Mater, Alma	alma.mater	ex19	Unlimited
Nach, Alma	alma.nach	ex19	Unlimited
Gehzauch, Anders	anders.gehzauch	ex19	Unlimited
Theke, Andi	andi.theke	ex19	Unlimited
Völcker-Dieserwelt, Andi	andi.völcker-die...	ex19	Unlimited
Kreuz, Andreas	andreas.kreuz	ex19	Unlimited
Kette, Anka	anka.kette	ex19	Unlimited

Microsoft hat die interne Suchmaschine durch die von Bing ersetzt und stellt bessere Ergebnisse in Aussicht. Die Indizes speichert Exchange nun direkt in seiner Datenbank, sodass sie auch nach einem Failover auf dem Zielsystem zur Verfügung stehen. Das erhöht allerdings die Anforderungen an Speicherplatz und -durchsatz.

Überraschenderweise kann Exchange 2019 nativ mit SSD-Storage umgehen. Bisher hatte der Hersteller betont, dass die Datenbank derart zugriffsoptimiert sei, dass „billiger“ und langsamer HDD-Speicher völlig ausreiche. Die neue Argumentation: Mittlerweile seien Magnetfestplatten so groß geworden, dass die Gesamtleistung zurückgehe. Hier sollen SSDs als reiner Cache mit dynamischem Tierung als „Nachbrenner“ agieren. Exchange steuert das alles selbst – die Server brauchen weder teure RAID-Adapter noch eine dedizierte Tierung Logik.

Anwender sollen neue Komfortfeatures erhalten, die schon von Office 365 bekannt sind. Diese finden sich vor allem im Umgang mit Kalendern und Terminen. Die gemeinsame Nutzung von Kalendern wird einfacher, parallel erhalten Admins die Möglichkeit, Einträge und Berechtigungen zentral zu steuern. Das soll mit allen Outlook-Varianten funktionieren, also außer per Windows-PC auch unter iOS und Android sowie beim Webzugriff.

Nicht mehr an Bord ist die Serverrolle „Unified Messaging“, die bislang die Brücke schlug zu Skype for Business (vormals Lync). Wer solche Funktionen

braucht, muss sich nun bei Drittanbietern umsehen.

Fazit

Wer bislang die Hoffnung hegte, dass Microsoft trotz seines Cloud-Fokus auch die Kunden mit lokalen Infrastrukturen mit Innovationen versorgt, könnte von den neuen Serverversionen ernüchtert sein. Sowohl Windows Server 2019 als auch Exchange Server 2019 sind mit dem Etikett „Produktpflege“ am besten beschrieben; Neuerungen für eine breite Kundenbasis gibt es nur in homöopathischen Dosen. Besonders Exchange zeigt deutlich, dass die eigentliche Premium-Plattform aus Office 365 in der Cloud besteht, die laufend neue Funktionen erhält. Lokale Exchange Server schließen mit der neuen Version nur teilweise auf und dürfen wohl nur auf stiefmütterliche Weise weiterentwickelt werden.

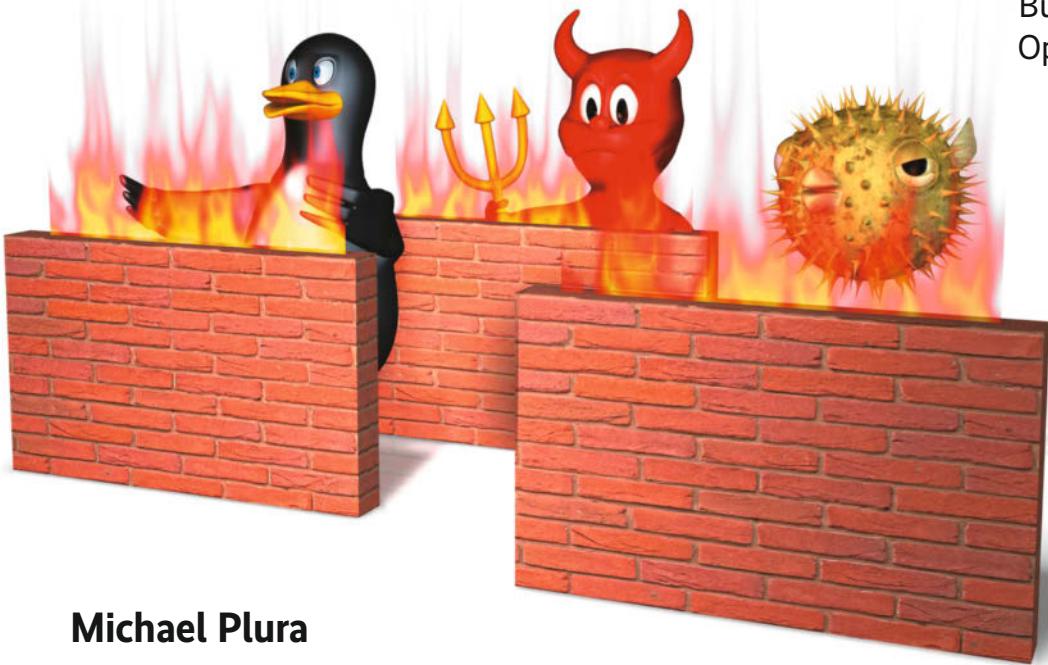
Für Rechenzentren bringen beide Produkte immerhin interessante Updates im Detail. Ob das reicht, um im großen Stil auf die neuen Versionen umzusteigen, wird mancher IT-Verantwortliche aber skeptisch beurteilen. (un@ix.de)

Nils Kaczenski

leitet das Consulting bei der Michael Wessel Informationstechnologie in Hannover. In der IT-Community ist er als Sprecher und Blogbetreiber bekannt.

Marktübersicht: Open-Source-Firewalls

Freie Filter



Michael Plura

Eine Firewall schützt Einzelsysteme und Rechnernetze vor unerwünschten Zugriffen. Diverse BSD- und Linux-basierte Ansätze stehen zur Wahl.

Für einen erklecklichen Geldbetrag versprechen Hersteller wie Check Point, Cisco, Juniper oder WatchGuard den ultimativen Schutz. Bugs, Hintertüren für Techniker und Geheimdienste sowie hohe Kosten lassen manchen Systemverwalter nach Alternativen suchen. Je nach Einsatzszenario muss es dabei nicht unbedingt um einen kompletten Ersatz einer großen kommerziellen Firewall-Appliance gehen. Teilbereiche des Netzes oder Außenstellen könnten mit einer einfachen Open-Source-Firewall bereits ausreichend und preiswert geschützt sein.

Und es gibt einen weiteren Aspekt: Eine gute Firewall besteht – wie auch das BSI im IT-Grundschutz unter M 2.73 empfiehlt (siehe ix.de/ix1810056) – aus drei Stufen: erster Paketfilter (zum WAN), Applikation Level Gateway, zweiter Paketfilter (zum LAN). Anhand verschiedener einfacher Kriterien entscheiden Paketfilter, ob sie Pakete weiter-

reichen, zurückweisen oder still verwerfen. Die Kriterien umfassen unter anderem Quell- und Zieladresse, Quell- und Zielport oder den Protokolltyp. Zusätzlich kann die Stateful Inspection Pakete einer bestehenden Verbindung erkennen und ohne weitere Prüfung zulassen. Über eine Deep Packet Inspection auf dem Application Level Gateway (ALG) und mit Proxies lassen sich Pakete inhaltlich prüfen und etwa auf Schadsoftware untersuchen. Während die Rechenleistung für einen Paketfilter noch überschaubar bleibt, fordert ein ALG schon deutlich mehr Ressourcen.

Aus Sicherheitssicht ist sogar eine physische Trennung der drei Komponenten zu empfehlen, wobei die beiden Paketfilter idealerweise von unterschiedlichen Herstellern stammen sollten. So kann ein Angreifer nicht gleich beide Filter in einem Rutsch überwinden. Die deutsche genua GmbH verfolgt dieses Prinzip in ihren genugate-Sicherheits-Ap-

pliances und verbaut dort in einem 19"-Gehäuse gleich zwei Computersysteme mit OpenBSD und dessen *pf*-Paketfilter. Als drittes System (der Paketfilter am WAN) empfiehlt genua korrekterweise, das Produkt eines anderen Herstellers (notfalls den Router des ISP) einzusetzen.

Bunt gemischt: Open-Source-Firewalls

Die hier vorgestellten Firewalls sind allesamt Open-Source-Software und damit kostenlos. Sie stehen größtenteils unter freien Lizenzen wie der GPL oder einer BSD-Lizenz, teilweise aber erweitert oder um Closed-Source-Komponenten ergänzt. Beim Support ist der Systemverwalter zunächst auf sich selbst gestellt, Hilfestellung bekommt er in teilweise durchwachsener Qualität über Community-Foren. Zeitnahe Hilfe gibt es in eventuell vorhandenen Mailinglisten oder IRC-Chats. In der Regel antworten dort auch Mitglieder des Entwicklerteams,

wobei das bei einigen Projekten eine einzige Person sein kann. Viele Projekte verweisen zusätzlich auf kommerziellen und damit kostenpflichtigen Support, der für viele Unternehmen zwingende Voraussetzung für einen Einsatz ist.

Als Hardware setzen die Systeme in der Regel einen x86-kompatiblen PC mit 64-Bit-CPU und mindestens zwei Netzwerkkarten voraus. Die Leistung der Firewall skaliert dabei natürlich mit den Fähigkeiten der Hardware, sodass eine CPU mit AES-NI und Intel PRO/1000-Server- oder vergleichbare NICs mehr als empfehlenswert sind. Je nach gewünschten Zusatzfunktionen wie Proxyserver, Filter oder VPN steigt der für einen reinen Paketfilter eher geringe RAM-Bedarf deutlich. Nicht unberücksichtigt lassen sollte man die von Intel in fast allen modernen CPUs verbauten Hintertüren: Active Management Technology / Management Engine (AMT/ME) und das heimlich laufende Minix-System sollen der Fernwartung dienen, lassen sich theoretisch aber missbrauchen. Über eine virtuelle serielle Schnittstelle, die über Ethernet oder sogar WLAN funktioniert, können Angreifer das System kontrollieren und Dateien übertragen. Das Perfide dabei: Serial over LAN

(SoL) arbeitet unterhalb der Zugriffs- und Kontrollmöglichkeiten einer Firewall – diese ist also bei aktivem AMT/ME blind und machtlos. Eine kleine ARM64-Firewall-Appliance könnte dafür besondere Sicherheitsansprüche eine Lösung sein – auch wenn die Performance derartiger Embedded-Systeme noch unterirdisch ist.

Die Übersicht teilt sich in drei Gruppen: Firewall-Appliances auf Basis von Linux, auf Basis von FreeBSD und Regelsatz-Compiler. Während die Appliances mehr oder weniger umfangreich und dank Weboberfläche bedienerfreundlich sind, beschränken sich Regelsatz-Compiler oder das an Ciscos IOS angelehnte VyOS auf eine Kommandozeile. Deren Vorteil ist der geringe Ressourcenbedarf und die Option, Vorgänge oder ganze Installationen durch Skripte zu automatisieren. Mehr als historischer Exkurs betrachtet der Kasten „Firewall-Veteranen“ einige veraltete Vertreter.

Sowohl WebGUI als auch CLI haben Vor- und Nachteile. GUIs sind grundsätzlich einfacher zu bedienen, da die wählbaren Optionen oft in einer Auswahlliste vorgegeben sind. Ein „Port öffnen“ und dabei zwischen „SSH (22)“ und „HTTP (80)“ auszuwählen versteht auch ein frisch gebackener DevOp. Muss man zum Öffnen des SSH-Ports stattdessen wie bei OpenBSDs *pf*

```
pass in log on em0 proto tcp to port 22
```

oder Linux' *iptables*

```
iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

eintragen, ist das zwar mehr oder weniger gut lesbar, aber ohne Hintergrundwissen um das jeweilige Regelwerk nicht gerade aus dem Ärmel zu schütteln. Dafür lassen sich beide CLI-Beispiele schnell um *from <IP/Net>* oder *-s <IP/Net>* erweitern, um den Zugriff nur bestimmten IP-Adressen oder (Sub-)Net-

Dienste	Status	PID	Speicher
Cron-Server	LAUFT	2901	744 kB
DHCP-Server	LAUFT	2771	10060 kB
DNS-Provider	LAUFT	1799	12632 kB
Einschussdetektierung (BLUE)	iptables		
Einschussdetektierung (GREEN)	ANGEHALTEN		
Einschussdetektierung (ORANGE)	ANGEHALTEN		
Einschussdetektierung (RED)	ANGEHALTEN		
GeoIP Block	LAUFT	1699	4916 kB
Zugriff auf BLAU	LAUFT	8288	1780 kB
Kernel-Protokollierungs-Server	ANGEHALTEN		
NTP-Server	LAUFT	1764	560 kB
OpenVPN	ANGEHALTEN		
Protokollierungs-Server	LAUFT	15353	928 kB
Secure Shell Server	LAUFT		
VPN	ANGEHALTEN		
Web-Proxy	LAUFT	2850	4540 kB
Web-Server	ANGEHALTEN		

IPFire tritt in die Fußstapfen des Klassikers IPCop, ist einfach zu bedienen und erfüllt mittlere Ansprüche (Abb. 1).

zen zu erlauben – bietet ein GUI dafür keine Option, bleibt diese wichtige Möglichkeit unerreichbar.

IPFire

Ursprünglich war IPFire eine IPCop-Distribution, etwas erweitert um Samba, VoIP (Asterisk), QoS sowie einen Printserver (LPR-ng). Diese Dienste, die auf einer professionellen Firewall nichts zu suchen haben, steckten die Zielgruppe ab: Heimanwender und kleinere Unternehmen. Mit Version 2 wurde das gesamte System überarbeitet und von Grund auf neu entwickelt. IPFire basiert seitdem auf „Linux From Scratch“, lässt sich modular erweitern und ist bis auf die Schnittstelle zum WebGUI eine einigenständige Entwicklung.

Eine Installation sollte über das aktuelle ISO-Image erfolgen – die angebotenen Flash-Images sind fertige Systeme, die nicht mehr installiert werden. Eine Installation löscht die gesamte erste Festplatte und formatiert diese mit Ext4 (mit oder ohne Journal), XFS oder dem überholten ReiserFS. Nach einem Neustart wird IPFire lokalisiert, die Domain festgelegt und Passwörter für „root“ und „admin“ (WebGUI) vergeben. Die Netzkonfiguration erinnert an IPCop: Zunächst definiert man die Netze: rot (WAN), grün (LAN), orange (DMZ) und blau (WLAN); die ersten beiden sind Pflicht, DMZ und WLAN optional. Vorteilhaft ist es, die MAC-Adressen parat zu haben, um sie zuordnen zu können. Intern vergibt IPFire feste IP-Adressen, extern sind auch DHCP oder PPP-Einwahl möglich. Während der Installation lässt sich ein DHCP-Server für das LAN-Interface einrichten.

Das WebGUI ist aus dem LAN über HTTPS und den ungewöhnlichen Port 444 erreichbar. Wie bei den meisten OSS-FWs wird von aktuellen Browsern ein fehlerhaftes, weil selbst ausgestelltes Zertifikat moniert. IPFire bietet einen optionalen SSH-Zugang auf Port 222, der sich auf Wunsch automatisch nach 15 oder 30 Minuten beenden lässt. Hier lässt sich Software – alternativ zum WebGUI – über die Paketverwaltung *pakfire* installieren. Die Liste der Add-ons ist recht lang: CUPS, Epson- und HP-Treiber, Samba, QEMU oder ein Torrent-Client für den privaten

X-TRACT

- Open-Source-Firewalls bieten einen ähnlichen, im Vergleich zu kommerziellen Lösungen meist aber etwas eingeschränkten Funktionsumfang an.
- Das breite Spektrum der Produkte deckt von Regelsatz-Compilern über Linux- und FreeBSD-basierte Firewalls mit WebGUI bis hin zum Router-Betriebssystem VyOS jedes Bedienkonzept ab.
- Kostenloser Support gibt es in unterschiedlicher Qualität über Foren, Mailinglisten und Chat.
- Einige Hersteller bieten einen Upgrade-Pfad zu kommerziellen Produkten samt professioneller Unterstützung.

Bereich, aber auch Nagios/Icinga, Squid, FreeRADIUS, Asterisk und Bacula.

Eine Besonderheit ist IPFires Update-Accelerator. Er setzt auf Squid auf und kümmert sich um das Caching von Updates für Windows, Linux, Virenscanner oder frei definierbare Quellen. Einen erneuten Abruf eines anderen Clients im LAN bedient IPFire dann direkt und entlastet langsame Internetverbindungen. Ebenfalls praktisch ist die Backup-Funktion. Sowohl die Konfiguration als auch optional die Logdateien lassen sich speichern. Auf Wunsch erzeugt IPFire daraus ein ISO-Image, das auf CDR gebrannt für eine Neuinstallation samt Konfiguration und Logs dienen kann. Auch die Einstellungen einiger Add-ons lassen sich sichern. Für Support oder den Kauf von mit IPFire vorinstallierten Appliances verweist die Projektseite auf die in Datteln (Ruhrgebiet) ansässige Lightning Wire Labs GmbH.

Zum Testzeitpunkt war IPFire 2.19 Core120 aktuell, es gab aber schon Images der Version 2.21 Core122. Ein Problem bereitete dabei das Upgrade des Kernels von 3.14 auf 4.14, da dort immer ein */dev/hwrng* (Hardwarezufallsgenerator) existiert, auch wenn der physisch gar nicht vorhanden ist. Gerade ältere Plattformen,

sparsame Prozessoren für den Embedded-Bereich oder VMs generieren dann nicht genug Entropie, was dazu führt, dass der Linux-Kernel beim Starten unter Umständen für Minuten hängt. Das Problem dürfte mit Erscheinen dieser iX gelöst sein.

Endian Firewall Community

Die hier getestete Endian Firewall Community ist die frei unter der GPL vertriebene und abgespeckte Variante der Endian UTM, die der Hersteller Endian Spa aus Südtirol auch als Hardware-Appliance anbietet. Im Prinzip ist die Software ein stark weiterentwickelter Fork von IPCop. Die Installation ist einfach und schnell und erkennt das WAN-Interface in einer VirtualBox-Testumgebung mit vier NICs selbstständig – andere Distributionen liegen hier falsch und sind manuell anzupassen. Über den Network Configuration Wizard richtet man noch im Textmodus einfache alle Schnittstellen und DHCP ein.

Vor der weiteren Arbeit am WebGUI muss der Admin persönliche Informationen und eine valide E-Mail-Adresse angeben, um Updates zu erhalten – das fordert keine andere Firewall im Test. Über die

Geo-IP wurde der in Schweden lebende Autor als in „Thailandia“ ansässig erkannt, richtig wäre „Svezia“. Deutsche Nutzer müssen „Germania“ wählen. Die Registrierung funktionierte im Test nicht, lässt sich bei der Installation aber überspringen und später über „System → Update“ nachholen.

Während das WebGUI liebevoll gestaltet ist, ist es um die Community recht ruhig geworden. Dort wurde schon seit Längerem bemängelt, dass die Entwicklung nur schleppend und vom Hersteller oft ohne Einbeziehung der Nutzer stattfindet. Die kommerzielle Endian UTM bietet wesentlich mehr Funktionen als die Open-Source-Variante.

Untangle

Untangle, vor 2007 als Metavize bekannt, hat das hauseigene Firewall-Produkt mittlerweile zur Next Generation Firewall in der Version 14.0.0 ausgebaut, die sich dank diverser Erweiterungsmöglichkeiten zur Unified Threat Management Firewall (UTM) aufrüsten lässt. Das Grundsystem basiert auf Debian GNU/Linux 9.4 „Stretch“ und lässt sich frei herunterladen. Zur Verfügung stehen ein CD- (ISO) und ein USB-Image (IMG) für 32-/64-Bit-Prozessoren, ein 64-Bit-Image für VMs (OVA) sowie Firmware für Linksys WRT1900ACS und Tarris Omnia. Im AWS-Marketplace steht ein 64-Bit-Amazon-Machine-Image (AMI) bereit.

Das Aufspielen übernimmt ein Debian-Installer im Text- und für eine Firewall-Appliance überraschenderweise auch im Grafikmodus. Nach dem Neustart findet sich der Administrator auf einem grafischen Desktop wieder, der – wieder überraschend – das WebGUI der Untangle Firewall in einem Chromium-Browser darstellt. Über „Konfiguration → Netzwerk → Erweitert → Access Rules“ lässt sich der SSH-Zugang zur Shell freischalten – einer komfortablen zsh. Ein ps fax zeigt dort eine eindrucksvolle Liste an Prozessen, angefangen vom systemd-Framework, Apache2, Xorg und Teilen des Xfce-Desktops bis hin zur besagten Instanz des Chromium-Browsers. Die laufende grafische Oberfläche erklärt, warum Untangle bereits im Leerlauf über 700 MByte Arbeitsspeicher belegt.

Im WebGUI gibt es ein eindrucksvolles Dashboard, das unter anderem auf einer Weltkarte alle kontaktierten IP-Adressen lokalisiert. Die Ernüchterung folgt, sobald der Systemverwalter auf spezielle Funktionen zugreifen will. Das Basisystem ist zwar frei, aber nur mit beschränktem

The screenshot shows the Endian Firewall Community dashboard. On the left, there's a sidebar with links like System, Status, Network, Services, Firewall, Proxy, VPN, and Logs and Reports. The main area has several sections:
 - **Dashboard**: Shows the Appliance Version (3.2.5), Uptime (2h 56m), and a 'Community Account' button. It also shows Signature updates (No recent signature updates found) and Hardware information (CPU 1, Memory, Swap, Main disk, Data disk, Configuration disk, Log disk).
 - **Network Interfaces**: A table showing six interfaces (eth3, br2, eth2, br1, eth1, br0) with their type (ethermet), link status (Up), and traffic rates (In and Out in KB/s).
 - **Incoming traffic in KB/s (max 6 interfaces)** and **Outgoing traffic in KB/s (max 6 interfaces)**: Two line graphs showing traffic over time for the same six interfaces.
 - **Uplinks**: A table showing uplinks with columns for Name, IP Address, Status, Uptime, Active, and Managed.

Mit der Endian Firewall Community gibt es eine Art Lite-Version der professionellen Produktrreihe des Herstellers Endian Spa (Abb. 2).

Firewall-Veteranen

mOnOwall (mit zwei Nullen im Namen) ist ein typisches Open-Source-Projekt: Ihr Entwickler Manuel Kasper mochte 2003 seine FreeBSD-Firewall und den Paketfilter *pf* nicht mehr über die Befehlszeile konfigurieren, sondern wünschte sich ein hübsches, einfaches, freies und leicht zu bedienendes WebGUI. Im Laufe der Zeit entwickelte sich mOnOwall von einem FreeBSD-Router zu einer Firewall-Appliance mit immer mehr Diensten. Im Februar 2015 stellte Manuel Kasper die Weiterentwicklung ein. mOnOwall gilt jedoch als Meilenstein in der Entwicklung von Open-Source-Firewalls, weil es die Basis für zwei der beliebtesten aktuellen Vertreter ist: pfSense und OPNsense. Sogar das FreeNAS-Projekt ging aus mOnOwall hervor.

Noch älter ist die unter der GNU/GPL stehende Router- und Firewall-Distribution IPCop. Sie könnte als der Prototyp vieler moderner Linux-Firewalls gelten und war ursprünglich eine Erweiterung der Smooth-

wall GPL. Die Weiterentwicklung ist vor Jahren eingeschlafen, die Entwickler löschen im Forum Anfragen zu virtuellen IPCop-Installationen, weil sie diese ebenso wie die ARM-Plattform (Netzwerk via USB) als nicht angemessen erachten. Auch mehr als ein Interface pro Klasse (LAN, WAN, DMZ, WLAN) oder IPv6 gelten als „Long Term Goals“.

Eine der ältesten noch gepflegten Open-Source-Firewalls ist Smoothwall Express, auf deren Grundlage viele weitere Linux-Firewalls entstanden. Die erste Version der damals noch Smoothwall GPL genannten Firewall erblickte im August 2000 das Licht der Welt und konnte einen unbenutzten PC in eine für damalige Verhältnisse ansehnliche Firewall verwandeln. Updates gibt es nur noch selten und auch moderne Features wie IPv6 fehlen, sodass Smoothwall Express sich wie mOnOwall und IPCop für einen produktiven Einsatz im professionellen Umfeld nicht eignet.

Funktionsumfang. Erweitert wird Untangle über Apps, von denen einige frei, andere nur gegen eine monatliche Gebühr erhältlich sind. Manche kostenpflichtigen Apps sind ebenfalls als freie Lite-Apps mit weniger Leistung verfügbar. Ein Adblocker beispielsweise ist kostenlos, einen Spamfilter gibt es gegen Bezahlung oder als freie Lite-Version, Bandbreitenmanager, WAN-Balancer und -Failover sind nur gegen Geld zu bekommen und kosten je fünf US-Dollar pro Monat. Ein vollwertiger Spam- oder Virus-Blocker schlagen mit je 10 US-Dollar und das Bandbreitenumagement schon mit 25 US-Dollar pro Monat zu Buche; die Preise für US-basierten Support beginnen bei 216 US-Dollar jährlich. Für den nicht kommerziellen, privaten Einsatz gibt es die Untangle Firewall HomePro, die alle Apps bis auf Branding, Virus-Blocker und Live-Support enthält. Die Anzahl der Geräte ist nicht begrenzt, Untangle versucht aber, auf nicht öffentlich dokumentierte Weise eine kommerzielle Nutzung zu erkennen, und schränkt die Leistung dann ein. 2016 übernahm mit Providence Strategic Growth eine Investmentsgesellschaft Untangle und setzte mit Scott Devens einen neuen Geschäftsführer ein.

Zeroshell

Wie der Name impliziert, ist Zeroshell eine angeblich komplett über ein Webinterface zu administrierende Firewall-Lösung – quasi das Gegenteil der weiter unten besprochenen Shorewall. Jedoch ist die Installation der aktuellen Version 3.9.0 textbasiert und etwas unübersichtlich. Die Basiskonfiguration erfolgt über das Textmode-Interface oder ein Web-GUI, das zunächst fix auf 192.168.0.75 liegt. Standardmäßig öffnet Zeroshell auf diesem Management-Interface die Ports 53 (DNS), 80 (HTTP), 443 (HTTPS) und 749 (Kerberos). Über das Shell-Interface lässt sich die IP-Adresse ändern, an-

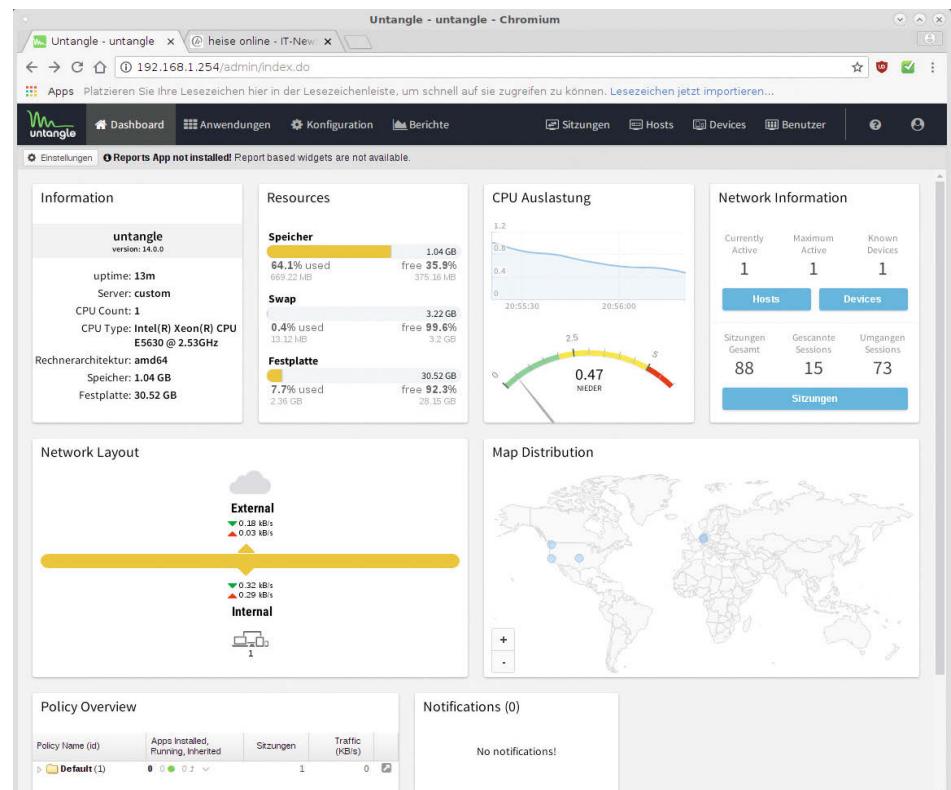
schließend muss man auch die Gateway-Adresse von Hand im Text- oder Web-GUI eingeben, um Updates oder Erweiterungen (Packages) zu bekommen. Unter der ID 49f00 bietet Zeroshell einen 64-Bit-Kernel 4.14.29 an, der mehr Speicher und Performance verspricht. Per Default installiert das System einen 32-Bit-Kernel.

Das WebGUI ist sehr umfangreich, dabei aber logisch aufgebaut sowie schlüssig und funktionell gehalten. Es erinnert an die WebGUIs klassischer Firewalls. Für einen funktionierenden Router mit Firewall legt man zunächst ein neues Profil an, richtet die beteiligten Netzwerkschnittstellen ein, trägt diese in eine NAT-Liste ein, definiert ein Gateway und konfiguriert

DHCP und eventuell DNS. Erfahrene Administratoren dürften die vielen Einstellungsmöglichkeiten erfreuen, wer das erste Mal eine Firewall einrichtet, kann hier leicht scheitern. Eine ausführliche Hilfe zur Installation war auf der Webseite des Projektes nicht zu finden. Dafür haben die Entwickler Zeroshell jedoch auf einige ARM-Plattformen wie Raspberry Pi 2/3 und Orange Pi portiert.

pfSense

In der aktuellen Version 2.4.3 gibt es die Community Edition der wohl bekanntesten Open-Source-Firewall pfSense für 64-Bit-x86-Systeme und Netgate ADI.



Zwar bietet die freie Variante der Untangle UTM Firewall optische Leckerbissen, für den professionellen Einsatz muss man sie jedoch mit kostenpflichtigen Apps ausrüsten (Abb. 3).

Fertige Cloud-Instanzen gibt es für AWS und Azure, aber auch für Hypervisoren.

Bereits bei der Installation dürften BSD-feste Admins den FreeBSD-Installer wiedererkennen, da pfSense auf FreeBSD 11.1-RELEASE-p10 basiert. Nach der Installation, die auch „experimentell“ auf ein ZFS-Dateisystem erfolgen kann, konfiguriert man die Schnittstellen. Im Gegensatz zu den meisten Linux-Firewalls zeigt pfSense die NICs hier mit MAC-Adresse an, was die Zuordnung erleichtert. Eine automatische Zuordnung ist möglich, indem der Installer der Reihe nach die Schnittstellen vorgibt (WAN, LAN, OPTx) und der Systemverwalter die entsprechenden Netzwerkkabel einsteckt. Die Voreinstellungen nach der Installation entsprechen einer typischen Konfiguration mit einem WAN-Interface (IPv4- und IPv6-DHCP), einem LAN-Interface (192.168.1.1 und WAN-delegated IPv6) samt NAT, einem DHCP-Server für IPv4/IPv6 und DNS-Resolver. Eine technisch derart komplette Vorkonfiguration sucht man bei anderen Firewalls vergebens.

Am WebGUI meldet sich der Systemverwalter via HTTPS und „admin/pfSense“ an. Beim ersten Mal hilft ein Assistent bei der grundlegenden Konfigu-

Listing: Einfaches Regelwerk per UFW

```
ufw default deny incoming
ufw default allow outgoing
ufw allow 80/tcp
ufw allow ssh
ufw enable
ufw status verbose
```

ration. Ein wenig nervig sind die permanenten Hinweise auf Netgates Produkte und Support und dass pfSense nicht kommerziell vertrieben werden darf – hier merkt man, dass nach der Übernahme von pfSense durch Rubicon Communications LCC die Vermarktung von Netgate-Produkten leider zu einem wichtigen pfSense-Feature wurde. Ein Grund übrigens für den unten vorgestellten Fork OPNsense.

pfSense verwendet den Paketfilter *pf*, der ursprünglich von OpenBSD 4.6 (erschienen 2009) stammt. Bei OpenBSD wurde *pf* seitdem stark weiterentwickelt und bildet mit weiteren Tools eine solide und vor allem auf Sicherheit ausgelegte Grundlage für Netzwerk-Appliances. Bei FreeBSD stand im Gegensatz dazu die Performance im Vordergrund, weswegen die Entwickler vor allem den bei Version 4.6 fehlenden SMP-Support einbauten. Nennenswerte weitere Verbesserungen gibt es nicht. Die Syntax beider Varianten unterscheidet sich, sodass Regelsätze nicht eins zu eins übertragbar sind.

Auch wenn pfSense bereits alle wichtigen Funktionen einer Firewall-Appliance mitbringt, ist die leichte Erweiterbarkeit durch Packages eine Stärke und umfangreicher als bei den Linux-Firewalls. Von acme, einer automatischen Verwaltung von „Let’s Encrypt“-Zertifikaten, über Snort (IDS), FreeSwitch (VoIP), Squid (Web-Proxy) oder Darkstat (Netzwerkmonitor) sind allerlei praktische Tools enthalten – alle kostenlos installierbar und viele sogar mit kostenpflichtigem Support durch Netgate.

OPNsense

OPNsense ist die freiere Variante von pfSense, steht unter der 2-Clause BSD License und darf daher auch kommerziell weiterverbreitet werden. Da es ein Fork von pfSense ist, waren sich beide Firewalls ursprünglich sehr ähnlich. OPNsense setzt ebenfalls auf FreeBSD, nutzt jedoch auch die Address Space Layout Randomization (ASLR) von Hardened-BSD. Während pfSense nur OpenSSL verwendet, lässt sich bei OPNsense alternativ LibreSSL einsetzen. Viele weitere Änderungen unter Einbeziehung der aktiven Community haben aus OPNsense ein mittlerweile eigenständiges Produkt gemacht – die Entwickler sprechen von weniger als 10 % verbliebenem Code aus dem Fork von 2014.

Die Gründe dafür lagen wie üblich in einem Zwist unter den Entwicklern. Die Veränderung der Schwerpunkte und Ziele durch die Kommerzialisierung von pfSense fand bei den freien Entwicklern wenig Freunde. Diese wollten OPNsense zusammen mit der Community weiterentwickeln; wie bei OpenBSD sollte die Sicherheit insgesamt im Fokus stehen. Dass Netgate bei der Übernahme von pfSense die nötigen Entwicklungswerzeuge auf GitHub löschte, erboste die freien Entwickler besonders. Die Spaltung hat immerhin zu einem Wettbewerb beider Systeme geführt, der die Entwicklung auch bei pfSense spürbar beschleunigt hat. Der ehemalige pfSense-Hauptsponsor, die niederländische Deciso B. V., unterstützt nun OPNsense. Selbst m0n0wall-Entwickler Manuel Kasper empfiehlt auf seiner Webseite OPNsense und nicht pfSense.

OPNsense gibt es als DVD-Image (auch für VMs), als USB-Installer entweder mit VGA-Modus oder serieller Konsole sowie als vorinstalliertes 4-GByte-Image namens „Nano“ für USB-Sticks, SD- oder CF-Karten. Letzteres schreibt

The screenshot shows the Zeroshell Net Services web interface. At the top, it displays system information: Release 2.8.0, 113.40 Kbit/s (Connections: 29 Load: 0%), Intel(R) Xeon(R) CPU E5630 @ 2.53GHz, 2526 MHz, 1023886 kB (9% used), Uptime: 0 days, 0:14. Below this is a navigation bar with tabs: SETUP, Packages, Profiles, Network, Time, Web, SSH, Scripts/Cron. Under the Network tab, there are sub-tabs: Show ALL, GATEWAY, INAT, DOHS, New VPN, New BRIDGE, New BOND, New PPPoE, New 3G Modem. The main content area lists four network interfaces:

- ETH00**: 1000Mb/s Full Duplex, Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 02). Status: UP. IP: 192.168.1.254, Subnet: 255.255.255.0. MAC: 0800000000F1. Buttons: Create VLAN, Edit VLAN, Rem. VLAN, Dyn IP, Add IP, Edit IP, Remove IP.
- ETH01**: 1000Mb/s Full Duplex, Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 02). Status: UP. IP: 192.168.1.254, Subnet: 255.255.255.0. MAC: 0800000000F2. Buttons: Create VLAN, Edit VLAN, Rem. VLAN, Dyn IP, Add IP, Edit IP, Remove IP.
- ETH02**: 1000Mb/s Full Duplex, Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 02). Status: UP. IP: 10.0.0.188, Subnet: 255.255.255.0. MAC: 0800000000F3. Buttons: Create VLAN, Edit VLAN, Rem. VLAN, Dyn IP, Add IP, Edit IP, Remove IP.
- ETH03**: 1000Mb/s Full Duplex, Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 02). Status: UP. IP: 10.0.0.188, Subnet: 255.255.255.0. MAC: 0800000000F4. Buttons: Create VLAN, Edit VLAN, Rem. VLAN, Dyn IP, Add IP, Edit IP, Remove IP.

At the bottom of the interface, a log window shows two entries:

```
Jul 12 23:16:09 SUCCESS: DHCP subnet 192.168.1.0/255.255.255.0 successfully saved.
Jul 12 23:17:07 SUCCESS: DHCP subnet 192.168.1.0/255.255.255.0 successfully saved.
```

Auch wenn Zeroshell altbacken wirkt, stecken im Paket viele Funktionen – IPv6 muss man allerdings von Hand konfigurieren (Abb. 4).

(Log-)Daten in eine RAM-Disk, um „Wearout“ zu vermeiden, und basiert auf NanoBSD, nicht wie die anderen Versionen auf FreeBSD. OPNsense bootet als vollständiges Live-System, alle Änderungen sind daher (außer bei Nano) nach einem Neustart verloren. Für die Installation auf Festplatte lässt man OPNsense bis zum Login-Prompt starten und meldet sich dort mit „installer/opnsense“ an. Nach dem Neustart konfiguriert man als „root“ die angeschlossenen Netze über das von pfSense her bekannte Textmenü („Assign Interfaces“ und „Set Interface IP Address“). Ein beim ersten Start des Web-GUI laufender Assistent fragt die zum grundlegenden Betrieb nötigen Informationen ab, dann ist OPNsense einsatzbereit. Auch OPNsense lässt sich erweitern, wobei sich die Ergänzungen von denen aus dem pfSense-Fundus unterscheiden.

Regelsatz-Compiler und CLI-Ansätze

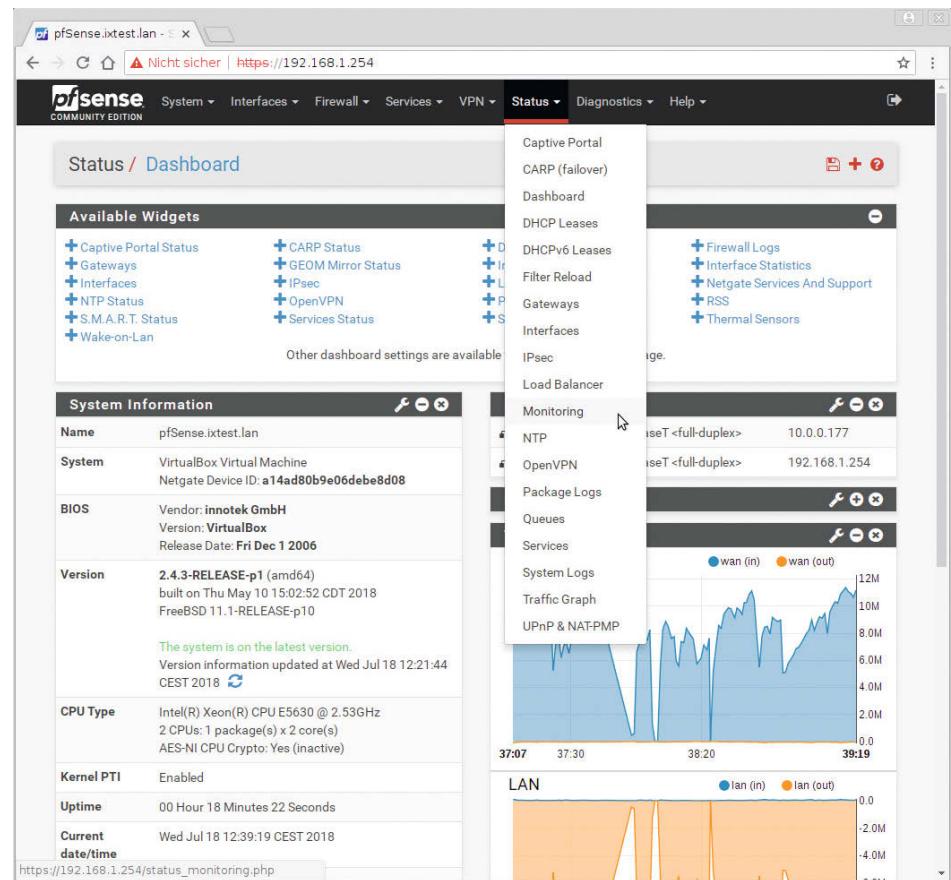
Bei allen bisher betrachteten Firewalls erfolgen Konfiguration und Verwaltung nach der Installation über ein WebGUI. Das erlaubt eine einfache Handhabung, wird jedoch bei Backups, Neuinstallatioen oder beim Ausrollen vieler Instanzen problematisch. Hier können Produkte punkten, die sich leicht skripten lassen. Drei Ansätze zeigen, wie unterschiedlich das aussehen kann.

Linux-Firewalls arbeiten seit Kernel 2.4 mit Netfilter, das mit mehr oder weniger verständlichen *iptables*-Befehlen konfiguriert wird – so auch die oben aufgeführten Linux-Firewalls. Wer *iptables* beherrscht, kann selbst eine Router-/Firewall-Appliance oder auch nur eine Firewall für ein exponiertes Einzelsystem wie einen Webserver zusammenstricken.

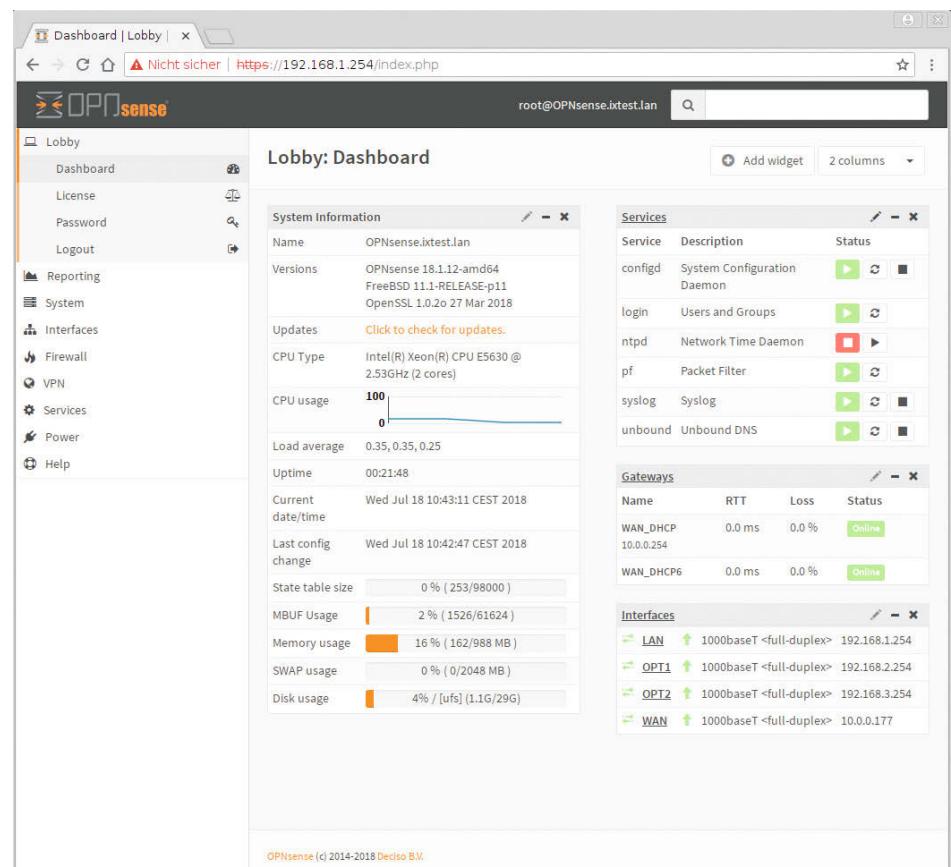
UFW

Vereinfachen lässt sich das durch UFW (Uncomplicated Firewall), ein Paket von Python-Skripten, das es für wohl jede Linux-Distribution gibt. Über *ufw*-Befehle definiert man einfach Regelwerke, die das System in */etc/ufw/** und */var/lib/ufw/user.rules* ablegt.

Das Listing auf Seite 60 zeigt einen typischen Regelsatz: Eingehende Verbindungen werden geblockt, ausgehend ist alles erlaubt. TCP-Verbindungen zu Port 80 (HTTP) und SSH (Port 22) – hier in den beiden unterschiedlichen Schreibweisen – sind erlaubt. Standardwerte finden sich in */etc/default/ufw*, in der ein Eintrag



Das auf FreeBSD und dem Paketfilter pf basierende pfSense CE legt die Messlatte für Open-Source-Firewalls recht hoch und ist auch für professionelle HW-Appliances erhältlich (Abb. 5).



Wenn Freiheit im Sinne von Open Source ein wichtiges Kriterium ist, bietet OPNsense als ehemalige Abspaltung von pfSense die Alternative zur kommerziellen Vorlage (Abb. 6).

IPv6=yes Regeln parallel auch für IPv6 erstellt. Die Manualpages erklären weitere Funktionen. Wer auch UFW unbedingt mit der Maus bedienen will, kann mit *gufw* ein GTK-Frontend für UFW installieren (siehe ix.de/ix1810056).

Shorewall

Die Shoreline Firewall, kurz Shorewall, ist ein Regelsatz-Compiler für Netfilter-Firewalls. Sie funktioniert nach dem „Compile and execute“-Prinzip. Die Konfiguration erfolgt in mehreren Dateien unter */etc/shorewall/**. Der Aufruf */sbin/shorewall start* startet den Shorewall-Compiler, der wiederum das Skript */var/lib/shorewall/.start* anlegt. Gelingt dies fehlerfrei, wird das Skript gestartet, das sich selbst nach */var/lib/shorewall/firewall* kopiert. Anschließende */sbin/shorewall start/stop/clear/reload*-Befehle führen immer das letztgenannte Skript aus.

Die Software besteht aus mehreren Paketen: Neben dem immer benötigten *shorewall-core* enthält *shorewall* den Compiler und alle IPv4-Funktionen, es muss auf mindestens einem System laufen. *shorewall6* fügt die IPv6-Pendants hinzu. Die **-lite*-Versionen der letzten beiden Pakete enthalten nur das Runtime ohne den Compiler, lassen sich also auf verteilten Firewalls einsetzen. So kann man Konfigurationen zentral kompilieren und auf „Satelliten“-Firewalls ausrollen. Schließlich beeinflusst *shorewall-init*, ob Shorewall vor oder nach dem Start des Netzwerks aktiv wird.

Nach einem *apt-get install shorewall* unter Ubuntu, Debian oder Devuan kopiert der Systemverwalter die Beispieldateien für eine minimale Shorewall-Konfiguration (*interfaces*, *policy*, *rules* und *zones*) aus */usr/share/doc/shorewall/examples/Universal/* (oder *.../onetwo/three-interfaces*) nach */etc/shorewall/*. Die **.gz*-Dateien enthalten kommentiert alle Optionen. Ein */sbin/shorewall start* kompiliert den minimalen Regelsatz und füttert *iptables* damit, das damit nur noch Ping und SSH von außen zulässt. Fügt man in */etc/shorewall/rules* die Zeile

```
Web(ACCEPT) net $FW
```

oder die beiden Zeilen

```
ACCEPT net $FW tcp 80
ACCEPT net $FW tcp 443
```

an und kompiliert den Regelsatz per */sbin/shorewall restart* neu, sind in beiden Fällen zusätzlich die HTTP-/HTTPS-Ports 80 und 443 offen. *Web*(...) kennzeichnet ein Makro und damit vordefinierte Regelbau-

Open-Source-Firewalls

Kategorie	klassisch, veraltet			Linux
Hersteller/ Entwickler	Manuel Kasper	IPCop-Projekt	Neal P. Murphy	IPFire-Projekt
Produkt	m0n0wall	IPCop	Smoothwall Express	IPFire
Version	1.8.1	2.1.9	3.1	2.19 Core Update 120
Lizenz	BSD	GPL	GPL	GPL
Installationsmedien	ISO, Flash, Flash/serial	tgz	ISO	ISO, Flash, Flash/serial, Xen
Plattformen	i386	i486	i586, amd64	i586, amd64, arm
Basisystem	FreeBSD 8.4	Linux 2.6	Linux 3.4	Linux from Scratch
ohne systemd	ja	ja	ja	ja
serielle Konsole	ja	ja	ja	ja
SSH-Konsole	nein	ja	ja	ja
WebGUI	ja	ja	ja	ja
lokales GUI	nein	nein	nein	nein
IPv4/IPv6	ja/ja	ja/nein	ja/ja	ja/via CLI
erweiterbar	nein	ja	nein	ja
Anmerkungen	2015 eingestellt	letzte Version in 02.2015	v3.1 SP4 in 04.2018	-

URLs zu den Produkten siehe ix.de/ix1810056

steine für Shorewall. */sbin/shorewall show macros* listet alle verfügbaren Makros.

Auf den ersten Blick wirkt Shorewall kompliziert, ist jedoch nach kurzer Einarbeitung über die Onlinedoku oder die Manpages ein ausgesprochen effizientes und mächtiges Werkzeug zum Erstellen von *iptables*-Regelsätzen. Ohne Webserver samt hübschen Frameworks bleibt der Ressourcenbedarf im Vergleich zu anderen OSS-Firewalls minimal. Damit eignet sich Shorewall nicht nur als Router-/Firewall-Distribution, sondern vor allem als Firewall-Konfigurator für Server und eingebettete Systeme. Shorewall aus den Paketquellen lief im Test problemlos sowohl mit Debian „Stretch“ (systemd) als auch mit Devuan „ASCII“ (SysV-Init). Jedoch sollte man der Verlockung widerstehen, Shorewall direkt über die Paketverwaltung zu installieren, da die Versionen in den Linux-Distributionen oft veraltet sind – für eine Firewall eher unpraktisch. Der Download der aktuellen Stable Release 5.2.0.4 ist ein wenig kompliziert, da die Download-Verzeichnisse unübersichtlich sind und mehrere Mirrors (unter anderem der in Deutschland) nicht antworten. SourceForge bietet nur eine veraltete Version an.

VyOS

Als reinrassige Router-/Firewall-Distribution erfolgt die Konfiguration von VyOS ausschließlich interaktiv über eine Shell im Textmodus. Das System basiert auf

Debian GNU/Linux und ist 32- und 64-bittig für die x86-Plattform verfügbar. Es gibt ein LiveCD/Install-ISO für den produktiven Einsatz und eine Entwicklerversion als Rolling Release.

Entstanden ist VyOS aus der freien Open-Router-Firmware Vyatta, die 2012 von Brocade Communication Systems übernommen wurde. Das Unternehmen machte aus dem Open-Source- ein Closed-Source-Projekt, für das es fortan Geld verlangte. 2017 kaufte AT&T die Vyatta-Software samt Entwicklungsteam von Brocade, um beides im eigenen Unternehmen zu nutzen – Support für frühere Kunden gibt es nicht mehr. Die Vyatta-Community sah sich bereits 2013 genötigt, einen Fork von Vyatta Core 6.6R1 anzulegen, der seitdem als VyOS unter der GPL frei verfügbar ist.

Die Installation erfolgt in sogenannte Images (squashfs-Dateisysteme), die zusammen mit den getrennt gespeicherten, veränderlichen Daten (Konfiguration et cetera) das System bilden. Das erinnert an traditionelle Hardware-Router, die einzelne Softwareversionen ebenfalls getrennt voneinander und damit quasi redundant vorhalten, während sie die Konfiguration zentral speichern. Die Live-CD bietet ein voll funktionsfähiges VyOS-System, an dem man sich per „vyos/vyos“ anmeldet – auf deutschen Tastaturen also „vz0s/vz0s“. Ein *install image* startet den geführten Transfer auf Festplatte, den ein *reboot* abschließt.

Die VyOS-Shell erinnert an eine Mischung aus Bash und Cisco IOS, vervoll-

			FreeBSD	Regelsatz-Compiler	Router-SW
Endian Spa	Untangle	Fulvio Ricciardi	Rubicon Communications LCC / Netgate	OPNsense-Projekt	Jamie Strandboge et al.
Endian UTM Community	Untangle NG Firewall	Zeroshell Linux Router	pfSense CE	OPNsense	UFW
3.2.5	14.0.0	3.9.0	2.4.3	18.4.7	0.35
Endian	Untangle	GPLv2	ehemals BSD, seit 2016 Apache 2.0	2-clause-BSD	GPLv3
ISO	ISO, IMG, OVA, AWS	ISO, IMG	ISO, IMG	ISO, IMG, IMG/serial	Paket, tgz
amd64	amd64	i686/amd64, arm	amd64, Netgate ADI	i386, amd64	universell
Linux 4.1	Debian GNU/Linux 9	Linux	FreeBSD	FreeBSD	Linux
ja	nein	ja	ja	ja	Host OS
ja	ja	ja	ja	ja	Host OS
ja	ja	ja	ja	ja	Host OS
ja	ja	ja	ja	ja	Host OS
nein	nein	nein	nein	nein	optional
ja/nein	ja/ja	ja/via CLI	ja/ja	ja/ja	ja/ja
ja	ja, Apps	nein	ja	ja	nein
IPv6 kommt 2018	-	-	i386 nur ältere Versionen	-	-

ständigt Befehle per Tabulator und kennt zwei Betriebszustände: Im Operational Mode (Prompt: \$) wird das System verwaltet oder der gesamte Router neu gestartet, außerdem werden Dienste und neue Versionen installiert. Das Kommando *configure* wechselt in den Configuration Mode (Prompt: #), in dem man die Konfiguration inklusive Rollback-Funktion bearbeitet – zurück geht es per *exit*. Nach der Installation konfigurieren beispielsweise die folgenden Schritte eine Schnittstelle sowie den SSH-Zugang (per Passwort):

```
$ show configuration
$ configure
# set interfaces ethernet eth0 z
      address 192.168.1.1/24
# set service ssh port 22
# commit
# save
```

Per *commit* werden die Änderungen wirksam, jedoch erst *save* speichert diese auf Festplatte. Über SSH von der eigenen Workstation hilft dem Systemverwalter die deutsche Tastaturbelegung und er kann Befehle per Copy-and-Paste einfügen. Ein *show configuration commands* zeigt eine Liste aller Befehle, die für die aktuelle Konfiguration nötig sind – praktisch für ein Backup oder als Grundlage für weitere VyOS-Instanzen. Alle Befehle funktionieren auch in VyOS-Skripten, sofern deren erste zwei Zeilen den VyOS-Header enthalten und allen Befehlen für den Operation Mode ein *run* vorangestellt ist:

```
#!/bin/vbash
source /opt/vyatta/etc/functions/script-7
      template
run ...
```

Wer VyOS einsetzt, sollte unbedingt das Entwickler-Blog verfolgen, das bereits die Funktionen der kommenden Version 1.2.0 vorstellt (siehe ix.de/ix1810056).

Was für wen?

Sicherlich lässt sich nicht jede professionelle, kommerzielle Firewall einfach durch eine beliebige Open-Source-Firewall ersetzen. Die grundlegende Technik, also Netfilter oder *pf*, setzen die kommerziellen Appliances jedoch oft ebenfalls ein. Open-Source-Firewalls eignen sich daher als Ergänzung zu professionellem Equipment zum Errichten einer weiteren Sicherheitshürde. Kleine und mittlere Unternehmen können mit einer freien Firewall Kosten sparen, sofern das Wissen zum korrekten Einrichten vorhanden ist.

Mit UFW lässt sich im Handumdrehen jedes Linux-System mit dem im Kernel vorhandenen Netfilter absichern – es gibt keinen Grund, dies nicht zu tun. Der Regelsatz-Compiler Shorewall professionalisiert diesen Ansatz und lässt deutlich feiner abgestimmte Regelsätze zu. VyOS ist, hat man einmal die Bedienung verinnerlicht, eine ideale Plattform, um auch größere Installationen mit Routern/Firewalls einzurichten und zu pflegen.

Linux-Firewalls mit ihren grafischen WebGUIs unterscheiden sich vor allem im Funktionsumfang. Auch die Art der Bedienung kann – je nach Vorlieben des Systemverwalters – entscheidend sein.

IPFire ist eine gute Basis, zielt aber mehr auf den Heim- und SOHO-Bereich. Zeroshell und vor allem Endian NG Firewall gehen einen Schritt weiter und bieten mehr Funktionen. Untangle und ClearOS sind für eine Firewall-Appliance zu groß, als Ersatz für einen Windows SBS, der auch die Aufgabe von Router und Firewall übernehmen muss, vielleicht trotzdem eine gute Wahl.

OPNsense und pfSense sind robuste Firewall-Ansätze, wobei pfSense das ausgereiftere Produkt mit einem Upgrade-Pfad zu kommerziellen Appliances ist – aber genau das nutzt der Hersteller für nervendes Marketing. OPNsense als echtes Open-Source-Projekt scheint den Fokus kompromissloser auf Sicherheit zu setzen – für eine Firewall sicherlich eine gute Eigenschaft. Beide Projekte nutzen als FreeBSD-Systeme aber einen veralteten Paketfilter *pf* von OpenBSD 4.6 (2009). Ist Sicherheit das wichtigste Argument, ist OpenBSD und der seit neun Jahren weiterentwickelte *pf* die bessere Wahl – allerdings muss man das Regelwerk dann von Hand zusammenstricken oder einen externen Dienstleister damit beauftragen.

(avr@ix.de)

Michael Plura

arbeitet in Schweden als freier Autor mit den Schwerpunkten IT-Sicherheit, Virtualisierung und freie Betriebssysteme.



Apples Bereitstellungsprogramme für Hard- und Software existieren seit vielen Jahren unter den Namen Device Enrollment Program (DEP) und Volume Purchase Program (VPP). Nun hat der Konzern beide überarbeitet und im Apple Business Manager (ABM) zusammengeführt. Ziel ist, dass der Administrator mit den Programmen und seinem MDM-System (Mobile Device Management) iOS- und macOS-Geräte effizient, zuverlässig und ohne Fehler konfigurieren und verwalten kann.

Das MDM dient dazu, mobile Endgeräte, etwa ein iPhone, aus der Ferne mit Befehlen zu steuern. So lassen sich Ge-

iOS und macOS mit dem Apple Business Manager verwalten

Fäden in der Hand

Mark Zimmermann

Im neuen Apple Business Manager finden sich die alten Bereitstellungsprogramme DEP und VPP wieder. Mit ihnen können Administratoren ihre iOS- und macOS-Systeme einfach verwalten.

Apples Bereitstellungsprogramme für Hard- und Software existieren seit vielen Jahren unter den Namen Device Enrollment Program (DEP) und Volume Purchase Program (VPP). Nun hat der Konzern beide überarbeitet und im Apple Business Manager (ABM) zusammengeführt. Ziel ist, dass der Administrator mit den Programmen und seinem MDM-System (Mobile Device Management) iOS- und macOS-Geräte effizient, zuverlässig und ohne Fehler konfigurieren und verwalten kann.

Zusammenspiel mit dem MDM

Ein MDM-Server kommuniziert mit dem Apple Push Notification service (APNs) und überträgt so die Befehle, Einstellungen und Apps auf die Geräte. Der APNs (zum Testen: api.development.push.apple.com:443, produktiv: api.push.apple.com:443) unterhält eine ständige Verbindung zu den Clients. Damit ein MDM-System per APNs Nachrichten senden darf, muss

es ein gültiges Push-Zertifikat (<https://identity.apple.com/pushcert/>) beantragen und erhalten.

Jede Interaktion beginnt mit einer POST-Anforderung von einem MDM-Server, die eine JSON-Payload und ein Geräte-Token enthält. Der APNs leitet die Benachrichtigungs-Payload an das Gerät oder die App weiter. Ob es sich um den korrekten Client handelt, erkennt das MDM-System anhand des enthaltenen Geräte-Tokens der APNs-Anfrage.

Empfängt ein Gerät den Hinweis, dass neue Befehle vorliegen, kommuniziert es mit dem MDM-System und empfängt die Anweisungen, Konfigurationsprofile oder Apps. Dies erhöht die Vertraulichkeit, da die APNs-Server so nie den Inhalt der Befehle kennen und zum Beispiel Kennwortrichtlinien oder VPN-Einstellungen nicht einsehen können.

Hier stellen sich zwei Fragen: Woher weiß ein Endgerät, an welchem MDM-System es sich melden soll? Woher weiß ein MDM-System, welche Geräte zu ihm gehören?

Als ersten Schritt muss sich das Gerät bekannt machen. MDM-Hersteller bieten von Haus aus Zugangswege durch den Anwender selbst, in dem Fall nutzt er ein Self-Service-Tool. Der Administrator kann alternativ zentral und manuell mit dem kostenlosen Apple Configurator 2 (AC-2) Hardware und MDM-System verbinden.

Komfortabler ist Apples Device Enrollment Program (DEP). So lassen sich die Geräte mit einem MDM automatisiert registrieren und konfigurieren. MDM-

IX-TRACT

- Der ABM bündelt Apples Bereitstellungsprogramme Device Enrollment Program (DEP) und Volume Purchase Program (VPP).
- Im Zusammenspiel mit einem MDM-System lassen sich iOS- und macOS-Systeme einfach verwalten.
- Administratoren, Gerätemanager und Inhaltsmanager können in derselben Oberfläche auf unterschiedliche Funktionen zugreifen, Apple könnte den ABM aber noch besser integrieren.

OPNsense optimierte Server-Systeme

Höchste Sicherheit für Ihr Netzwerk

Ob kompakte Low Energy Systeme, optional mit LTE Modem, oder unsere performanten 1HE- und 2HE-Server – bei Thomas-Krenn finden Sie optimierte Hardware für Ihre OPNsense Firewall. Und wie Sie OPNsense mit Plugins erweitern und optimieren können, lesen Sie in unserem kostenlosen E-Book.



Jetzt OPNsense optimierte
Server-Systeme konfigurieren.

Mehr erfahren:

+49 (0) 8551.9150-300
thomas-krenn.com/opn-sense

THOMAS
KRENN[®]

Systeme können aber auch Apps auf einem Client installieren, wobei sie ihm mitteilen, dass er Software aus dem App Store herunterladen soll. Da man ein MDM-System für beliebig viele Endgeräte nutzen kann, sollte man Volumenlizenzen erwerben und zuweisen können. Genau das bietet das Volume Purchase Program (VPP).

DEP und VPP als Teil des ABM

DEP und VPP gehen nun im ABM auf. Der Konzern hat bei der Gelegenheit allerdings einige Aktualisierungen vorgenommen. Die Weboberfläche des ABM ähnelt dem School Manager für den Bildungsbereich. Beim Anmelden am DEP oder VPP weist Apple Administratoren darauf hin, dass der ABM zur Verfügung steht. Umsteigen müssen sie zwar noch nicht, nach dem Wechsel gibt es allerdings keinen Weg zurück.

Die Migration übernimmt alle bisherigen Einstellungen des DEP und ebenso alle Käufe des VPP. Sie dauert etwa fünf Minuten. Im Rahmen der Migration muss der Administrator die Domäne seiner Firma angeben. Mit ihr erstellt man später verwaltete Apple-IDs, mit denen man den ABM bedienen kann. Die Domäne lässt sich nachträglich bearbeiten und um weitere Domänen ergänzen. Apple validiert (noch) nicht, ob die Domäne dem Unternehmen wirklich gehört.

Existieren mehrere VPP-Konten, also mehrere Einkäufer in einem Unternehmen, muss man alle gleichzeitig migrieren. Der Administrator lädt hierzu die anderen Nutzer per E-Mail zum ABM ein. Alle zuvor erworbenen Lizenzen und registrierten Geräte finden sich nach der Migration im ABM wieder. Letzterer gliedert sich in Standorte, die ein eigenes Token (Zugriffskontrolle) verwenden, das auf dem migrierten Token aus dem VPP-Portal basiert. Hat ein Unternehmen noch keinen Zugang zu den Bereitstellungsprogrammen, muss es sich unter business.apple.com registrieren.

Den Programmverantwortlichen nennt Apple mit Einführung des ABM Administrator. Er ist berechtigt, das Unternehmen beim DEP und VPP zu registrieren, und benötigt hierfür mindestens die folgenden Informationen:

- Art, rechtsgültigen Namen und Postanschrift des Unternehmens;
- Name und E-Mail-Adresse des zu berechtigenden Ansprechpartners;
- Nummer des Data Universal Numbering System (DUNS);
- zeichnungsbevollmächtigte Person des Unternehmens als Bestätigungskontakt. Die eingangs verwendete E-Mail-Adresse legt Apple als verwaltete Apple-ID an. Daraus darf für sie noch keine Apple-ID existieren. Die Adresse lässt sich anschließend nicht mehr ändern – verlässt ein Mitarbeiter die Organisation, kann man im Extremfall nicht mehr auf die Programme zugreifen. Daher sollte man entweder direkt

weitere Administratoren benennen oder keine personenbezogenen E-Mail-Adressen verwenden. Allerdings lassen sich beim ABM nur bis zu vier zusätzliche Konten für Administratoren einrichten.

Nach der Registrierung startet ein interner Prüfprozess bei Apple. Der Konzern kontaktiert telefonisch den hinterlegten Zeichnungsbevollmächtigten als Bestätigungskontakt, damit Letzterer die Korrektheit der Registrierung durch den Administrator bestätigt.

Alles an seinem Platz

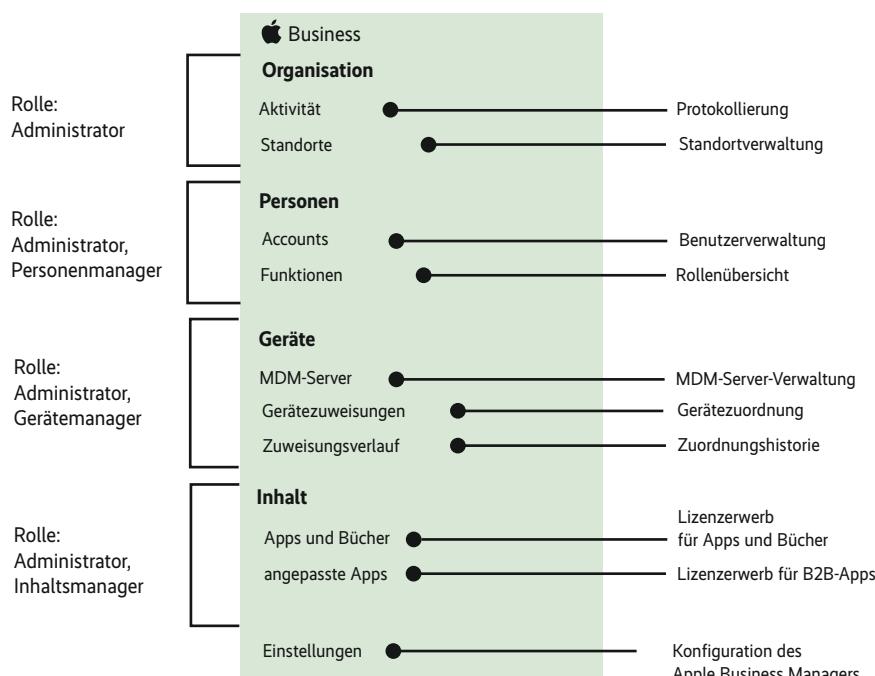
Die neue ABM-Konsole begrüßt den Administrator mit einer aufgeräumten Oberfläche. Im linken Bereich befindet sich die Hauptnavigation (siehe Abbildung 1). Die hier angezeigten Einträge hängen von der Rolle des jeweiligen Anwenders der ABM-Konsole ab.

Administratoren müssen als Erstes die Standortinformationen des Unternehmens überprüfen und ergänzen. Dazu lassen sich bestehende Standorte aufrufen und weitere Standorte oder Büros einer Organisation nachfragen und entfernen. Dabei muss man darauf achten, dass Inhaltsmanager und Administratoren zuerst die verwalteten Apple-IDs, App- und Bücherlizenzen des zu löschen Standortes auf einen anderen Standort übertragen.

Innerhalb des ABM können mehrere Personen mit unterschiedlichen Berechtigungen arbeiten. Hierzu können Personenmanager oder der Administrator verwaltete Apple-IDs anlegen. Eine Schnittstelle für einen unternehmenseigenen Verzeichnisdienst, zum Beispiel ein Active Directory, existiert nicht.

Verwaltete Apple-IDs führte der Konzern erstmals im School Manager ein. Eine verwaltete Apple-ID des ABM gehört einer Organisation und kann Mitarbeitern bestimmte Berechtigungen verschaffen. Der Nutzen der Apple-IDs in der Geschäftswelt ist derzeit jedoch eingeschränkt, da einige Dienste und Funktionen für sie deaktiviert sind. Hierunter fallen das Einkaufen im App Store, iTunes und iBooks Store, der Einsatz des iCloud-Schlüsselbunds, mit HomeKit verbundene Geräte, iCloud-Mail, die Funktionen Finde mein iPhone, Finde meinen Mac und Finde meine Freunde sowie die iCloud-Familienfreigabe.

Jede verwaltete Apple-ID ist mit den Informationen Status (neu, aktiv, deaktiviert), Vorname, zweiter Vorname und Nachname, Funktion (Rolle) und Standort sowie bestehende (dienstliche) E-Mail-



Im Hauptmenü kann der Nutzer auf die für seine Rolle freigegebenen Bereiche zugreifen (Abb. 1).

Einer verwalteten Apple-ID kann der Administrator einzelne oder mehrere Rollen und einen Standort zuordnen (Abb. 2).

Adresse assoziiert. Einer verwalteten Apple-ID lassen sich mehrere Funktionen zuordnen (siehe Abbildung 2):

- Administrator: erlaubt einem Anwender alle Funktionen aller Rollen auszuführen;
- Personenmanager: gestattet das Bearbeiten der Benutzerverwaltung und das Zuordnen von Rollen;
- Gerätanager: kann Geräte im ABM verwalten und sie so beispielsweise aktivieren oder entfernen;
- Inhaltsmanager: darf Apps und Bücher kaufen.

Hinzu kommt die Rolle „Mitarbeiter“. Damit dürfen Nutzer verwaltete Geräte verwenden, sich bei icloud.com anmelden und verwaltete Apps und Bücher öffnen. Das widerspricht Apples Aussage, wonach sich verwaltete Apple-IDs im Unternehmen ausschließlich für die Arbeit mit dem ABM einsetzen lassen.

Erstes Anmelden und Kennwörter

Alle verwalteten Apple-IDs erhalten beim Anlegen automatisiert ein temporäres Kennwort. Die Anwender müssen es beim ersten Anmelden ändern und eine Telefonnummer für den zweiten Faktor hinterlegen. Über sie bezieht der Nutzer seinen sechsstelligen Bestätigungscode beim Anmelden am ABM. Letzteren fordert das System alle 30 Tage ein. Wechselt der Anwender seine Handynummer, lässt sie sich über den ABM zurücksetzen.

Administratoren und Gerätanager können mit dem ABM Geräte direkt ei-

nem MDM-System zuordnen, um sie bereits zu konfigurieren, bevor der Nutzer sie auspackt. Der Bereitstellungsprozess basiert auf dem Einhalten einer Vertrauenskette von der Geräteproduktion über die autorisierten Händler bis hin zum endgültigen Einsatz. Private Endgeräte lassen sich nicht in den ABM überführen – mit einer Ausnahme: Mit dem AC-2 können Administratoren Geräte im ABM aufnehmen, die nicht von DEP-Händlern stammen. In diesem Fall gilt jedoch eine Übergangszeit von 30 Tagen, beginnend mit der ersten Aktivierung, während der der Nutzer die DEP-Zuordnung widerrufen kann.

Der ABM muss eine Verbindung zum MDM-System herstellen, damit man es mit Apple-Geräten verknüpfen kann. Hierzu muss man mindestens eine Apple-Kundennummer oder DEP-Händler-ID im ABM eintragen. Um das MDM-System einzurichten, hinterlegt der Administrator oder Gerätanager den öffentlichen Schlüssel des MDM-Systems und

lädt das ABM-Server-Token (.p7m-Datei) herunter, um es im MDM-System vorzuhalten (siehe Abbildung 3). Das Server-Token läuft nach einem Jahr ab.

Alle eingerichteten MDM-Server führt der ABM als Liste auf. Hier lässt sich ein Server umbenennen, ein neues Token generieren oder ein neuer öffentlicher Schlüssel aus dem MDM einspielen. Ferner können Administratoren hier festlegen, welcher Server standardmäßig für eine Gerätekasse zum Einsatz kommt. Den ABM kann man mit mehreren MDM-Systemen, ein MDM-System aber immer nur mit einem ABM verbinden.

Per ABM an ein MDM-System angebundene Geräte bieten dem Administrator zusätzliche Konfigurationsoptionen. Zum Beispiel kann er definieren, dass der Anwender die MDM-Anbindung nicht entfernen kann. Interessanter ist aber die Option, die Geräte in den Supervised Mode (siehe Kasten „Geführter Zugriff“) zu versetzen und den Einrichtungsassistenten eines jeden Gerätes zu konfigurieren. Administratoren können hier einzelne Schritte ausblenden.

Geführter Zugriff

Das Enrollment-Profil erlaubt es, den „geführten Zugriff“ (Supervised Mode) auf einem iOS-Gerät zu aktivieren. Er ist für eine tiefere Verwaltung durch ein MDM-System gedacht. Apple führt Konfigurationen immer öfter ausschließlich für diesen Modus ein und immer mehr Konfigurationen verlangen ihn. Entsprechend sollten Administratoren unternehmenseigene Geräte in den „geführten Zugriff“ versetzen.

Apps und Bücher für viele Nutzer einkaufen

Die Funktionen des VPP hat Apple ebenfalls im ABM gebündelt. Mit ihnen können Administratoren und Inhaltsmanager Apps, B2B-Apps und Bücher in großen Stückzahlen für ihre Standorte lizenziieren und an Geräte oder Mitarbeiter verteilen. Die Anbindung des VPP an ein

In einer einfachen Webmaske muss der Administrator oder Gerätemanager das MDM-System mit dem ABM verknüpfen (Abb. 3).

MDM-System ist einfach: Der Administrator muss hierzu in den Einstellungen ein VPP-Token herunter- und es in das MDM-System hochladen. Damit ist die Anbindung abgeschlossen und das MDM-System kann auf die erworbenen Lizenzen zugreifen. Auch dieses Token ist 365 Tage gültig.

Beim Erwerb von Lizenzen im ABM gibt es mehrere Optionen, sie später an die Anwender oder Geräte zu verteilen. Mit „verwaltet“ sind dies:

- Zuweisen an eine (verwaltete) Apple-ID (VPP User Assignment): Hier ordnet das MDM-System eine App einer (verwalteten) Apple-ID zu. So kann ein Anwender die Lizenz mehrfach verwenden, indem er die Apple-ID auf mehreren Geräten nutzt. Für die Familienfreigabe ist dies jedoch nicht gedacht.
- Zuweisen an ein iOS-Gerät (VPP Device Assignment): Hier verknüpft das MDM-System oder der AC-2 die App direkt mit einem Gerät. Eine Apple-ID benötigt man nicht. Das Gerät selbst listet das Programm nicht in der Kaufhistorie auf, das Installieren und Aktualisieren obliegt dem MDM-Server. Manche Apps sind hiermit technisch nicht kompatibel.

Zum Zuweisen kostenpflichtiger Apps und Bücher ohne ein MDM-System existiert eine weitere Variante im ABM: das Verteilen von Einlösecodes (VPP User Redemption). Hier generiert man eine Liste gültiger Installationscodes, die jeder

Nutzer für seine Apple-ID im App Store als Gutscheincode einlösen kann. Die Liste ist im ABM abrufbar.

Neben den technischen gibt es lizenzrechtliche Unterschiede. Ausschließlich bei einer MDM-gestützten Verteilung bleiben die Eigentumsrechte der App beim jeweiligen Unternehmen. Die Einlösecodes übertragen auch die Eigentumsrechte auf die Anwender, die Weitergabe lässt sich nicht widerrufen.

Lizenzen lassen sich unter anderem mit dem Guthaben des VPP erwerben. Die Bestellung lässt sich per Online Store (siehe ix.de/ix1810064), Telefon sowie Apple Store oder bei einem autorisierten Händler in Auftrag geben. Ein Kauf per Kreditkarte ist komplizierter einzurichten. Apple sieht dies im ABM nicht vor, das alte VPP-Portal (vpp.itunes.apple.com)

hilft hier jedoch weiter. Danach steht die Kreditkarte im ABM bereit.

Der ABM protokolliert alle Aktionen. Wenn er eine erfolgreich abgeschlossen hat, trägt er sie in die Datei *UPDATE* ein. Andernfalls versucht der ABM, mit Hinweisen zum Fehler im Protokoll zu helfen.

Fazit

Insgesamt finden sich im ABM die meisten wichtigen Funktionen des DEP und VPP wieder. So können Administratoren einfach und schnell ihre iOS- und macOS-Geräte verwalten. Praktisch ist, dass sie in derselben Oberfläche Apps erstehen und verteilen können. Allerdings könnte der Konzern den ABM an vielen Stellen noch besser integrieren – noch immer referenzieren zum Beispiel viele Stellen das VPP und für Kreditkarten muss der Administrator wie gehabt auf die alte Oberfläche zurückgreifen.

(fo@ix.de)

Mark Zimmermann

ist als Experte im Bereich Mobile Computing tätig. Sein Fachgebiet umfasst die Konzeption und Architektur sicherer mobiler Anwendungen.

Alle Links: ix.de/ix1810064





it-sa – Die IT-Security Messe und Kongress

9. bis 11. Oktober 2018 im Messezentrum Nürnberg

Europas größte Fachmesse für IT-Sicherheit

Mit rund 700 Ausstellern aus 24 Ländern bietet die it-sa das weltweit größte Angebot an IT-Sicherheitsprodukten und -lösungen, darunter physische IT-Sicherheit, Dienstleistungen, Forschung und Beratung.

Vom 9. bis 11. Oktober bieten die führende europäische Fachmesse und das begleitende Kongressprogramm Congress@it-sa umfassende Informationen zum Schutz von IT-Infrastrukturen.

Das erwartet Sie auf der it-sa 2018:

- Israel, die Niederlande und die Tschechische Republik beteiligen sich mit Gemeinschaftsständen.
- Die Sonderfläche Startups@it-sa und die IAM Area rücken junge Unternehmen und das Thema Identity und Access Management in den Fokus.
- Ein umfangreiches Vortragsprogramm mit fünf offenen Foren vermittelt mit rund 350 Beiträgen Know-how. Neu ist das internationale Forum I10.
- it-sa insights bieten produktneutrale Experteneinschätzungen zu Trends, Rechtsfragen und Spezialthemen.
- Beim Live-Hacking zeigen Experten, wie Cyberkriminelle vorgehen.
- Die weltweit bekannte IT-Sicherheitsexpertin Paula Januszkiewicz hält die Special Keynote. Am 11. Oktober spricht sie zum Thema "Attacks of the Industry: A View into the Future of Cybersecurity".
- Congress@it-sa bietet zusätzliche Informationen zum aktuellen Stand in der IT-Sicherheit, beispielsweise zur EU-Datenschutz-Grundverordnung oder dem Schutz für Mittelständler.
- Bereits am Vortag der Messe treten 18 Start-ups an, um den Pitch für den UP18@it-sa Award für sich zu entscheiden.

Ein Besuch der it-sa lohnt sich: 2017 waren 98 Prozent der Besucher mit den Informations- und Kontaktmöglichkeiten auf den Messeständen zufrieden.

**Sichern Sie sich jetzt Ihr kostenfreies Ticket mit dem Gutschein „iX4itsa18“ unter:
www.it-sa.de/gutschein**



© NürnbergMesse



© CQURE



© NürnbergMesse



Die **aikux.com GmbH** ist ein IT-Spezialdienstleister aus Berlin, der sich seit vielen Jahren ausschließlich mit den Themen Konzeption, Migration und Restrukturierung von Unternehmensdaten und Zugriffsrechten beschäftigt.

Mit der Erfahrung aus hunderten Projekten in Unternehmen, Behörden und internationalen Organisationen und dem Wissen um die speziellen Anforderungen verschiedenster Branchen können wir Ihnen praxisbewährte Lösungen und eine individuelle Umsetzung bieten. Dabei ist klar: Kein Projekt ist wie das andere – weshalb die Erfüllung der speziellen Anforderungen Ihres Unternehmens durch individuelle Beratung im Vordergrund steht.

Das Leistungsspektrum von **aikux.com** erstreckt sich von der Beratung und Konzepterstellung bis zur Umsetzung der einzelnen Lösungen in Ihrem Unternehmen. Unser Ziel sind langfristige Lösungen für zufriedene Kunden, die auch nach Jahren keine Rezertifizierung Ihrer Daten- und Rechtestruktur scheuen brauchen.

Sie finden uns als Mitaussteller von tenfold in Halle 9 / 9-524

Halle 9, Stand 9-524
www.aikux.com



Die österreichische **Antares-Netlogix Netzwerkberatung** ist seit über zehn Jahren zuverlässiger Partner für Managed Security Services. Zu den Kunden zählen Unternehmen und Organisationen mit höchsten Sicherheitsanforderungen, bspw. aus Finanzsektor, Behörden oder KRITIS.

Die Managed Security Services umfassen:

- globaler Firewall-Betrieb
- Mail/Web Security
- Vulnerability Management
- Verschlüsselung
- APT Protection
- PKI Security
- Access- und Identity-Management

Sämtliche Module werden über das in Amstetten ansässige **Security Operations Center (SOC) mit 24x7-Bereitschaft** betreut. Für Projekte steht ein erfahrenes Security-Consulting-/DevOps-Team zur Verfügung.

Mitaussteller ist **iQSol** mit Appliances für grundlegende Sicherheitsfunktionen im Unternehmen: Monitoring, Alerting sowie geordneter Shutdown und automatischer Wiederanlauf der Systeme. Auch die schwedische **Advenica**, Spezialistin für die Absicherung kritischer Infrastrukturen, ist vor Ort.

Halle 10.1, Stand 208
www.netlogix.at



Halle 10.0, Stand 422
[www.axa.de/
cyber-versicherung](http://www.axa.de/cyber-versicherung)

Der AXA Konzern zählt mit Beitragseinnahmen von 10,9 Mrd. Euro (2017) und 9.087 Mitarbeitern zu den führenden Versicherungs- und Finanzdienstleistungsgruppen in Deutschland. Die AXA Deutschland ist Teil der AXA Gruppe, einem der weltweit führenden Versicherungsunternehmen und Vermögensmanager mit 165.000 Mitarbeitern und Vermittlern sowie mehr als 100 Millionen Kunden in 64 Ländern.

Cyber-Versicherung für Unternehmen

AXA bietet Unternehmen jeder Größe und Betriebsart ein passgenaues Konzept, um sich bedarfsgerecht gegen Risiken der digitalen Welt abzusichern. Dabei geht die Deckung weit über Schäden durch Cyberattacken hinaus. IT-Ausfälle gehen oft mit kostenintensiven Betriebsunterbrechungen einher. Ursachen können hierbei der Ausfall der Telekommunikation, aber auch die externer Dienstleister, beispielsweise bei Cloud-Anbietern, sein. Auch Szenarien wie Fehlbedienung oder Manipulation der Systeme durch Mitarbeiter sind gedeckt.

IT-Haftpflichtversicherung

Für IT-Unternehmen ist die IT-Haftpflichtversicherung unverzichtbar. Die AXA bietet hier eine umfassende, professionelle Lösung, die Personen- und Sachschäden wie auch umfassend Vermögensschäden abdeckt.



Halle 10.0, Stand 215
www.baramundi.de

baramundi software AG

Wir ermöglichen Unternehmen und Organisationen das effiziente, sichere und plattformübergreifende Management von Arbeitsplatzumgebungen. Mehr als 2.500 Kunden aller Branchen und Größen profitieren weltweit von unserer langjährigen Erfahrung und ausgezeichneten Produkten. Diese sind in der baramundi Management Suite (bMS) nach einem ganzheitlichen, zukunftsorientierten Unified-Endpoint-Management-Ansatz zusammengefasst: Client-Management, Mobile-Device-Management und Endpoint-Security erfolgen über eine gemeinsame Oberfläche, in einer einzigen Datenbank und nach einheitlichen Standards.

Durch Automatisierung von Routinearbeiten und eine umfassende Übersicht über den Zustand aller Endpoints optimiert die bMS Prozesse des IT-Managements und sorgt dafür, dass immer und überall die benötigten Rechte und Anwendungen verfügbar sind.

Besuchen Sie uns an unserem **Stand 215 in Halle 10.0** bei der it-sa 2018!



Halle 10.1, Stand 110
<http://pages.checkpoint.com/itsa2018>

Step up to the 5th Generation of Cyber Security

Schützen Sie sich vor den Cyberbedrohungen der 5. Generation!

Vom 9. bis 11. Oktober öffnet Europas führende Fachmesse für IT-Sicherheit it-sa die Tore und **Check Point** begrüßt Sie in **Halle 10.1 / Stand 110**. Als führender Anbieter von Cybersicherheits-Lösungen für öffentliche Verwaltungen und Unternehmen weltweit, schützen wir Kunden vor Cyberattacken mit einer branchenführenden Erkennungsrate von Malware, Ransomware und anderen Arten von Attacken.

Check Point bietet eine umfassende Sicherheitsarchitektur, um Unternehmen zu schützen. Egal, ob Netzwerk, Cloud oder Mobilgerät – Check Point deckt alle Bereiche ab und kann diese über seine leicht verständliche Sicherheitsmanagementplattform verwalten. Über 100.000 Organisationen vertrauen seit 25 Jahren auf den Schutz von Check Point. Überzeugen auch Sie sich von unseren Lösungen & Produkten.

Zusammen mit den Mitausstellern Algosec, Arrow ECS, Bechtle, TAP.DE, Safe-T und Westcon bieten wir den Besuchern der it-sa ein Komplett-Paket an Fachwissen, Lösungen und Support. Besuchen Sie uns in **Halle 10.1 am Stand 110**.

Wir freuen uns, Sie am Stand von Check Point begrüßen zu dürfen!



Alles in die Cloud? Aber sicher!

Die direkt gruppe stellt auf der it-sa 2018 ihre Sicherheitslösungen zu Compliance, DSGVO und Identity & Access Management vor. Unsere Experten präsentieren unsere Compliance Factory, unser Cloud Baseline und Compliance as a Service. Ole Westphal berichtet über „Alles in die Cloud? Aber sicher!“

IAM mit der direkt gruppe & econet

Die econet GmbH konzentriert sich auf Software Made in Germany für alle Organisationen, die ihre Benutzer- und Berechtigungsverwaltung sicher und effizient gestalten wollen.

In Ihrem Portfolio befinden sich hochspezialisierte Lösungen im Bereich Identity & Access Management (IAM) für Windows sowie für Data Access Governance (DAG). Das econet IAM-Kompaktsystem vereinfacht die Versorgung von Mitarbeitern mit Kern-IT-Diensten grundlegend.

Treffen Sie uns in Halle 10.0 auf der IAM-Area (10.0.- 420) und beim Cyber-Sicherheitsrat e.V. (Stand 10.0.- 405).
Mehr Infos auf: cloud.direkt-gruppe.de

Halle 10.0, Stand 405 und 420
[https://cloud.direkt-gruppe.de](http://cloud.direkt-gruppe.de)



ENDPOINT PROTECTOR

Next Generation DLP made in Europe

Die Endpoint Protector GmbH vertreibt als Ländergesellschaft von CoSoSys deren Lösungen in der D-A-CH-Region und den Niederlanden. CoSoSys ist auf Data Loss Prevention und Mobile Device Management spezialisiert und wurde 2017 als einziges europäisches Unternehmen in den Gartner MQ für Enterprise DLP aufgenommen. Das Flaggschiffprodukt Endpoint Protector unterstützt Firmen jeder Größe beim Schutz vor Datenverlust und Datendiebstahl durch Innenräuber. Zu der DLP-Lösung gehören die Module

- Schnittstellenschutz (Device Control),
- Container-Verschlüsselung für USB-Sticks (EasyLock),
- Kontrolle von Dateiinhalten beim Transfer (Content Aware Protection),
- Suche nach unstrukturierten sensiblen Daten auf Arbeitsplatzrechnern (eDiscovery).

Halle 10.0, Stand 109
www.endpointprotector.de

Die gesamte Funktionalität steht für Windows, macOS und Linux zur Verfügung. Die DLP-Lösung lässt sich durch MDM für die Einbindung mobiler iOS- und Android-Geräte ergänzen.



ENJOY SAFER TECHNOLOGY™

Halle 9, Stand 9-326
www.eset.de

ESET ist ein europäisches Unternehmen mit Hauptsitz in Bratislava (Slowakei). Seit 1987 entwickelt ESET preisgekrönte Sicherheits-Software, die bereits über 110 Millionen Benutzern hilft, sichere Technologien zu genießen. Als ganzheitlicher Lösungsanbieter gehört ESET mit seiner jahrzehntelangen Erfahrung, einem globalen Netzwerk an Forschungs- und Entwicklungszentren sowie Niederlassungen in mehr als 200 Ländern und Regionen zu den Top-Unternehmen der Security-Branche.

Mitte August hat ESET die neue Generation seiner B2B Produkte veröffentlicht.

IT-Sicherheit ist kein Zustand, sondern ein Prozess! Und so stecken auch in dem neuen ESET Portfolio an Produkten und Services vier Jahre kontinuierlicher Entwicklung und Optimierung, um den stetig wachsenden An- und Herausforderungen von Unternehmen gerecht zu werden.

Live Präsentationen am Stand!



TRUST IN GERMAN SICHERHEIT

Halle 9, Stand 438
www.gdata.de/business

Ganzheitliche IT-Security aus Deutschland. Für den Mittelstand.

Keine Chance für Cyberkriminelle: Die G DATA Software AG ist der Erfinder des AntiVirus. Das 1985 in Bochum gegründete Unternehmen hat vor mehr als 30 Jahren das erste Programm gegen Computerviren entwickelt. Heute gehört G DATA zu den weltweit führenden Anbietern von IT-Security-Lösungen, die in mehr als 90 Ländern erhältlich sind.

Meine Daten bleiben in Deutschland

Als deutsches Unternehmen unterliegt G DATA den strengen deutschen Datenschutzgesetzen und arbeitet nicht mit Geheimdiensten zusammen. G DATA gibt eine No-Backdoor-Garantie und verspricht, dass alle Kundendaten ausschließlich in Deutschland gespeichert und verarbeitet werden.

Sicherheitslösungen für Unternehmen und Endkunden

Um den vielfältigen Cyberbedrohungen Herr zu werden, braucht es heute ganzheitliche Sicherheitskonzepte. Die G DATA Businesslösungen schützen nach dem „Layered Security“-Konzept schichtweise vor Online-Angriffen und Schadprogrammen.

Weitere Informationen zum Unternehmen und zu G DATA Businesslösungen finden Sie unter www.gdata.de/business oder auf unserem **it-sa Messestand: Halle 9/438**.



Heise Medien steht für hochwertigen und unabhängigen Journalismus. Heise verlegt mit **c't** und **iX** zwei erfolgreiche Computertitel, das zukunftsweisende Technologiemagazin **Technology Review** sowie das mehrfach ausgezeichnete Online-Magazin **Telepolis**.

Heise Medien schärft sein Profil im Bereich IT-Sicherheit mit dem neuen **Veranstaltungformat secIT**. Termin 2019: secIT 13.–14. März 2019 im HCC, Hannover.

35 Jahre c't – ein Meilenstein in der Geschichte der IT.

Die zusätzliche c't Geburtstagsausgabe 27/2018 erscheint am 23. Oktober.

Aktionen rund um das Jubiläum und zur secIT am Heise Stand Halle 10.0 - 620



IoT Inspector – Firmware-Schwachstellen aufdecken

Die Firmware-Security-Analyse-Plattform IoT Inspector wurde entwickelt, um den Sicherheitsstatus von IoT-Firmware effizient auf Sicherheitsrisiken zu testen und Sicherheitslücken in „intelligenten“ Geräten aufzuspüren. Dabei überzeugt die einfache Handhabung dieses Tools: In nur drei Schritten – Firmware hochladen, IoT Inspector analysieren lassen, Report ansehen – werden Schwachstellen in der Firmware aufgedeckt, bevor sie von Cyberkriminellen ausgenutzt werden können. Plugins erkennen Schwachstellen und nutzen dabei zusätzlich auch Datenquellen wie die IoT-Suchmaschine Censys sowie die National Vulnerability Database von NIST. Eine große Bandbreite an vernetzten Geräten wie IP Kameras, Router oder Drucker wird abgedeckt. Unternehmen ist es so möglich, die Firmware von IoT-Devices vor und nach Inbetriebnahme auf Schwachstellen zu überprüfen – selbstständig und schnell.

Halle 10.1, Stand 108
www.iot-inspector.com

it.sec

security for your information

www.it-sec.de

The Cyber Security People

- Penetrationstests & Sicherheitsuntersuchungen
- Cybercrime – Prävention, Reaktion und Aufarbeitung
- Schutz Kritischer Infrastrukturen

it.sec GmbH & Co. KG

Seit 1996 unterstützen unsere Informatiker und Juristen Unternehmen sowie staatliche und nichtstaatliche Institutionen in mehr als 30 Ländern in Fragen zu Informationssicherheit, Datenschutz & IT-Compliance. Wir adressieren multi-regulatorische Anforderungen auch im internationalen Kontext, hacken uns im Auftrag in Online-Systeme und -Shops, Firmen, Banken oder industrielle Anlagen, helfen bei der Aufklärung von IT-bezogenen Sicherheitsvorfällen („Cybercrime“) und bieten High-End Services für eDiscovery und eSearch Anforderungen.

ITsure

Halle 9, Stand 426
www.it-sure.de

Ihr Partner in Fragen rund um IT & IT Security

Wir bieten Ihnen ein ganzheitliches Portfolio aus Konzepten, Strategien, Hardware, Software, Security und Services. Unser Angebot reicht von Beratung, über den Aufbau komplexer Infrastrukturen, bis zum Outsourcing und Managed Services.

Unsere Security Solutions

• Konzepte & Workshops

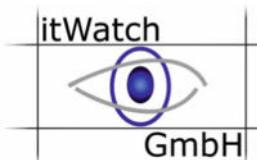
Der Beginn liegt in der Betrachtung Ihres Ist-Zustandes. Unsere Workshops sind die Basis, Ihnen ein maßgeschneidertes Sicherheitskonzept zu bieten.

• Lösungen

Wir übersetzen Ihre Anforderungen in konkrete Lösungen. So individuell Ihr Unternehmen ist, so individuell ist auch Ihr Sicherheitskonzept.

• Professional & Managed Services

Sie erhalten Professional Services zur Implementierung, Einführung und Dokumentation Ihrer Security Lösung. Mit unseren Managed Services übernehmen wir deren Betrieb: Regelwerke, Sicherheitsrichtlinien, Patches ... - erfahrene Security Consultants sorgen für größtmögliche Sicherheit.

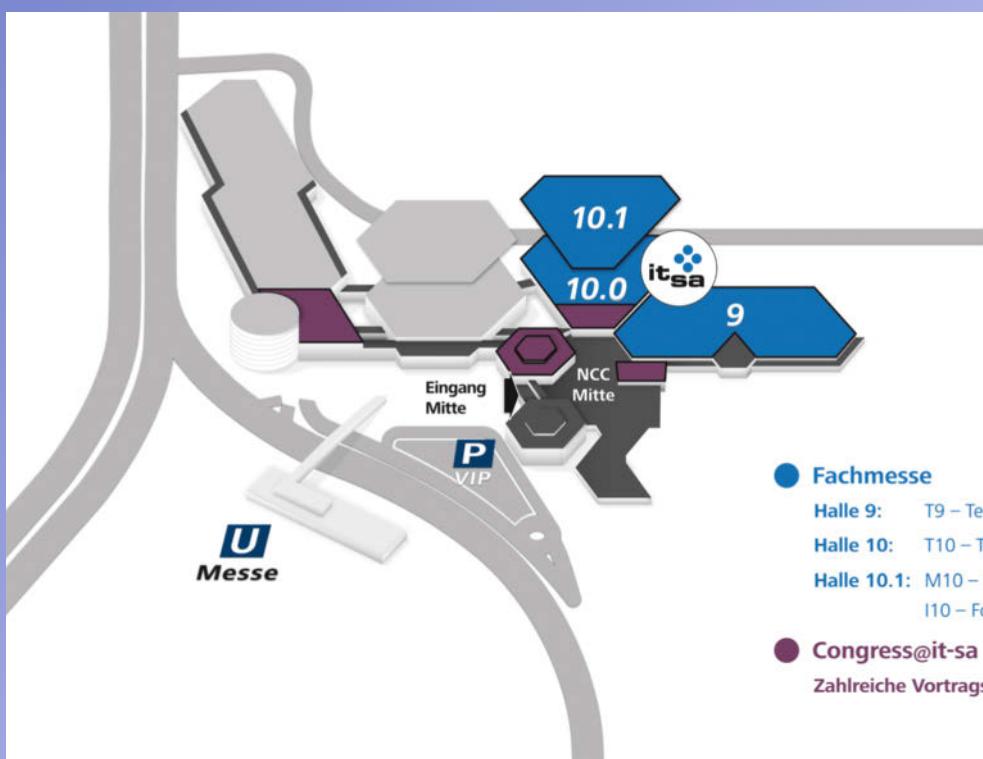


Halle 9, Stand 203
www.itWatch.de

itWatch Produkte schützen vor modernsten Angriffsformen (APT), versteckten Angriffsvektoren und Datendiebstahl. Mit dem Produkt **itWash** unterstützt itWatch internationale Organisationen bei der „Cyberdatenwäsche“. Die patentierten **itWatch** Sicherheitslösungen mit großen Installationen, weit über 100.000 Lizenz, bieten durch ihre weltweiten Alleinstellungsmerkmale viele Vorteile – im Bereich IT-Sicherheit, GRC und natürlich beweisbarem Datenschutz. Hohe Anforderungen von Nachrichtendienst, Militär und Polizei werden ebenso erfüllt, wie solche von Standard-Büro Arbeitsplätzen. Seit 1997 schützt die **itWatch Enterprise Security Suite** ihre Kunden millionenfach auf den Gebieten Device-, Port-, Application-, Media-, Print-, Content-Control, Security Awareness, sichere Tastatur, Risiko Audit, Endpoint Security, DLP, sicheres Löschen, sichere Schleusensysteme, Risiko Identifikation, Inventarisierung & Minimierung, sicheres LogOn sowie Verschlüsselung.

Der **IoT** und **Industrie 4.0 Markt** wird mit Infrastrukturlösungen auf embedded Systemen und durchgehenden Security Lifecycle Lösungen bedient.

Alle itWatch-Produkte werden in Deutschland entwickelt, getestet und weltweit über Partner vertrieben.



Fachmesse

Halle 9: T9 – Technik Forum | M9 – Management Forum

Halle 10: T10 – Technik Forum | IAM Area

Halle 10.1: M10 – Management Forum | Startups@it-sa

I10 – Forum International

Congress@it-sa

Zahlreiche Vortragsreihen bereits ab 8. Oktober



Halle 9, Stand 9-632
www.keyidentity.com

Sicherheit durch MFA: Die KeyIdentity GmbH aus Weiterstadt zeigt auf der it-sa 2018 ihre hochskalierbaren, einfach einzusetzenden Multi-Faktor-Authentifizierungslösungen zur Absicherung digitaler Transaktionen und Identitäten. Highlight des Messeauftritts ist die neue Lösung zu Identity Access Management:

- Höchste Sicherheit „made in Germany“
- Neue, nichttechnokratische Lösung
- Einfache Dokumentation und Verwaltung von Zugriffsrechten
- Schafft eine übersichtliche Struktur
- Einzigartige Usability

Besuchen Sie auch unseren Expertenvortrag:

„Wenn das IAM funktioniert – Ein IAM, das dich und das Business versteht“
von Dr. Amir Alsbih, CEO KeyIdentity GmbH
am 10. Oktober um 10.30 Uhr im Management-Forum in Halle 9



www.kobil.com

Über KOBIL Systems:

KOBIL Lösungen sind heute ein Standard für digitale Identität und hochsichere Datentechnologie. 1986 gegründet, ist die 120-Personen starke KOBIL Gruppe, mit Hauptsitz in Worms, ein Pionier in den Bereichen Application Shielding, Benutzeroauthentifizierung, Transaktionsauthentifizierung und digitale Signaturen, Smart Card, Einmalpasswort, Authentifikation und Kryptographie. Kern der KOBIL Philosophie ist es, durchgängiges Identitäts- und Mobile Security Management auf allen Plattformen und allen Kommunikationskanälen zu ermöglichen. Knapp die Hälfte der KOBIL Mitarbeiter sind in der Entwicklung tätig, darunter führende Spezialisten für Kryptographie und PKI. KOBIL wirkt bei der Entwicklung neuer Verschlüsselungsstandards entscheidend mit. Die Commerzbank, DATEV, der Deutsche Bundestag, die Migros Bank, Société Générale, UBS, ZDF und viele andere setzen und vertrauen auf KOBIL.



Halle 10.0, Stand 120
www.ncp-e.com

Brücken zwischen IT und OT zu bauen, betrifft alle Unternehmen.

Diese müssen so gebaut sein, dass sie den Anforderungen nach IT-übergreifender Kommunikationssicherheit gerecht werden. Neue Anwendungsszenarien müssen auf einfache Weise genutzt werden und gleichzeitig die bestehende klassische IT integrieren. Damit dieses Kunststück gelingt, brauchen IT-Chefs schon heute zentrale Managementsysteme wie das NCP Secure Enterprise Management.

Alle Details dazu auf der it-sa.

Stand 120, Halle 10



Halle 9, Stand 546
www.nttsecurity.com

Securing your Digital Transformation

NTT Security ist das auf Sicherheit spezialisierte Unternehmen und „Security Center of Excellence“ der NTT Group, einem der größten IKT-Unternehmen weltweit. Mit „Embedded Security“ bietet NTT Security zuverlässige Lösungen für Anforderungen in der digitalen Transformation und sichert eine effiziente Ressourcennutzung, indem Kunden der richtige Mix an ganzheitlichen Managed Security Services, Security Consulting Services und Security-Technologie zur Verfügung gestellt wird – unter optimaler Kombination von lokalen und globalen Ressourcen.

Zahlen und Fakten

- 1.500 Sicherheitsexperten weltweit, über 250 in der DACH-Region
- Betrieb von zehn globalen SOCs (Security Operations Center) und sieben Forschungs- und Entwicklungszentren
- Über 10.000 Kunden
- Fast 170.000 verwaltete, gesicherte und überwachte Endgeräte
- Analyse von jährlich 6,1 Billionen Log-Einträgen
- 150 Millionen abgewehrte Attacken pro Jahr



Halle 9, Stand 216
www.nuvias.com

Ob Authentifizierung, Antivirus oder Encryption – bei Nuvias erhalten Sie erprobte IT-Sicherheitslösungen führender Hersteller an einem Stand. Das Besondere am Nuvias Konzept: Nuvias agiert EMEA-weit und vertreibt die Lösungen seiner Partner über lokale Standorte in über 20 Ländern. Dabei legt der VAD besonderen Wert auf ein gleichbleibendes hohes Serviceangebot.

Am it-sa Stand können sich Besucher von den Qualitäten des Distributors überzeugen und auch gleich mit den Experten ins Gespräch kommen. Das Stand-in-Stand Konzept ermöglicht ein persönliches Treffen mit internationalen Herstellern wie Kaspersky Lab, WatchGuard, HID Global, FireEye, Malwarebytes, Symantec und OneSpan (ehemals Vasco).

In der interaktiven Cyberattack-Simulation können Sie den Ernstfall proben und sich live einem Angriff aussetzen.

Sie benötigen noch ein Ticket für die it-sa?
Bei uns erhalten Sie Ihr Ticket kostenlos: <http://bit.ly/it-sa2018>



Sicherer Umgang mit mobilen Datenträgern

Schadsoftware gelangt häufig über mobile Datenträger oder mobile Geräte (Android, iOS, ...) in die Netze der kritischen Infrastrukturen. Aber auch Unternehmen und Behörden benötigen einen umfassenden Perimeterschutz zur Abwehr der Bedrohung. Nach dem Stand der Technik kombiniert unsere Datenschleuse PROVAIA mehrere Sicherheitssysteme und macht Malware zuverlässig unschädlich. Einfach Stick einstecken und prüfen. Auch USB-Krypto-Sticks, TrueCrypt-Container, BitLocker und passwortgeschützte Archive (ZIP, ARJ, ...) werden unterstützt.

Freuen Sie sich auf:

- Einfache Bedienung
- Größtmögliche Sicherheit

Halle 10.1, Stand 312
www.pre-sense.de

PRESENSE Technologies GmbH · Sachsenstraße 5 · D-20097 Hamburg · Telefon +49-40-2442407-0



Rohde & Schwarz Cybersecurity schützt Unternehmen und öffentliche Institutionen weltweit vor Cyberangriffen. Mit den neuen Generationen seiner innovativen Sicherheitslösungen R&S Web Application Firewall und R&S Trusted Gate schließt das Unternehmen Sicherheitslücken bei der Nutzung von Web Applikationen und Cloud-Diensten. Mit R&S Web Application Firewall lassen sich bspw. False-Positives erheblich reduzieren, ohne dass Mitarbeiter komplexe Einstellungen treffen müssen.

R&S Trusted Gate setzt auf eine neue Art der Absicherung von Daten in der Cloud mittels „datenzentrischer Sicherheit“. Die Sicherheit wird dabei direkt in die Dateien integriert, anstatt sie an ein äußeres Tor zu übertragen. Die neuen Konzepte erzeugen eine höhere Sicherheit – und sie sind besonders anwenderfreundlich. Das gilt auch für den völlig neu entwickelten R&S Trusted Communicator, eine Kommunikations- und Kollaborationsplattform, die einen hochsicheren Messenger samt verschlüsselter Telefonanrufe in einem bietet.

Rohde & Schwarz Cybersecurity auf der it-sa 2018: Halle 10.0 / Stand 112

Halle 10.0, Stand 112
www.rohde-schwarz.com/cybersecurity



SANS ist weltweit der größte und damit führende Anbieter von Cyber Security Trainings. Gegründet in 1989 operiert SANS in über 30 Ländern und hat über 200.000 Teilnehmer erfolgreich ausgebildet. Über 25 Jahre haben wir mit über 500 weltweit führenden Unternehmen, Organisationen und Regierungen zusammengearbeitet. Technologie mag sich in dieser Zeit gewandelt haben, aber die SANS Mission im Kern bleibt bestehen: Menschen, deren Güter und deren IT Infrastruktur durch unsere Trainingsmaßnahmen vor Cyberattacken zu schützen.

Das SANS Curriculum deckt alle Bereiche der IT Sicherheit ab: Cyber Defense, Digitale Forensik, Incident Response, Management, Penetration Testing, sichere Software Entwicklung, Industrial Control Systems, Security Awareness und Audit.

Die über 60 SANS Kurse sind praxisorientiert, werden von erfahrenen, zertifizierten SANS Trainern mit jahrelanger Praxiserfahrung geführt. Neben unseren mehr als 200 Liveveranstaltungen jährlich bieten wir über 30 weltweit anerkannte GIAC Zertifizierungen an und nahezu alle Kurse sind auch als Online Veranstaltungen verfügbar.

Unser Versprechen: Alle Teilnehmer können ihr erworbene Wissen aus den Kursen sofort in der täglichen Arbeit einsetzen.

Halle 9, Stand 9-253
www.sans.org/emea



SEC Consult ist einer der führenden Berater im Bereich Cyber- und Applikationssicherheit. Das Unternehmen ist mit Niederlassungen in Europa, Asien und Nordamerika vertreten und auf den Aufbau von Informationssicherheits-Management, Zertifizierungsbegleitung ISO 27001, Cyber-Defence, DDoS-Tests, externe und interne Sicherheitstests (Pentests) und sichere Software(-Entwicklung) spezialisiert - Ziel ist die nachhaltige Verbesserung des Sicherheitsniveaus.

Darüber hinaus ist SEC Consult Mitglied im Open Web Application Security Project (OWASP). Mit einem der größten White-Hat-Hackerteams und dem Vulnerability Lab als internes Security-Labor stellt SEC Consult die notwendige Umgebung bereit, um aktuelle Bedrohungen zu analysieren und entsprechende Lösungen entwickeln zu können. Zu den Kunden von SEC Consult zählen führende Unternehmen, Behörden und Organisationen aus verschiedenen Sektoren der Privatwirtschaft sowie der kritischen Infrastruktur.

Halle 10.1, Stand 108
www.sec-consult.com



MEHR LEISTUNG DURCH IT-SICHERHEIT

In Staat, Gesellschaft und Wirtschaft kommt es zunehmend darauf an, sich zuverlässig gegen Bedrohungen aus dem Cyberraum zu schützen. Ein ganzheitlicher IT-Sicherheitsansatz bedeutet dabei nicht, Performance einzubüßen – im Gegenteil: Neben dem Schutz gegen konkrete Gefahren wie Hacking-Angriffe können moderne IT-Sicherheitslösungen – richtig eingesetzt – auch die Leistung von Prozessen, Netzwerken und Infrastrukturen erhöhen. Somit trägt IT-Sicherheit entscheidend dazu bei, das zentrale Effizienzversprechen der Digitalisierung einzulösen.

secunet entwickelt für E-Government, Behörden, militärische Organisationen, kritische Infrastrukturen, Industrie 4.0 und die Automotive-Branche Konzepte und Lösungen, die anspruchsvolle IT-Sicherheit und Effizienz verbinden. Besuchen Sie uns und die Mitaussteller finally safe und Mellanox Technologies auf der **it-sa 2018 an Stand 10.0-307**.

Halle 10.0, Stand 307
www.secunet.com



IT-Technologie made im Ruhrgebiet

Das Unternehmen **TAROX** zählt zu den führenden IT-Anbietern ganzheitlicher Lösungen und umfassender Produktfamilien für den Mittelstand im deutschsprachigen Raum. TAROX beschäftigt derzeit 170 Mitarbeiter. Die Teams der unterschiedlichen Business-Units versorgen flächendeckend Partner im Systemhaus und im Fachhandel für ihre Auftraggeber- und Anwender-Kunden in B-to-B-Branchen und Behörden. Das Know-how aus den fünf Kompetenzfeldern Machines, Distribution, Consulting, Data und Services bündelt sich zum Geschäftsmodell „Smart Business“.

Wir beraten Sie zu einer Vielzahl an Themenbereichen wie: Informationssicherheit, Datenschutz, DSGVO, ISO 27001, Compliance, ISMS, Risikomanagement, VDS 10010, VDS 3473. Dies alles in Kooperation mit unseren Security Allianz Partnern.

Halle 9, Stand 9-512
www.tarox.de

Treffen Sie uns in der **Halle 9, Stand 9-512** – Wir freuen uns auf Sie!



tenfold ist **Berechtigungsmanagement der nächsten Generation**. Mit unseren revolutionär einfachen Methoden und Werkzeugen gehören unübersichtliche und gefährliche Berechtigungsstrukturen der Vergangenheit an. Mit tenfold erstellen Sie automatisch Benutzerkonten, visualisieren Berechtigungen und binden Datenverantwortliche aus den Fachbereichen in jedem wichtigen Schritt im Workflow ein. tenfold bietet übrigens erstklassige Auswertungsmöglichkeiten für Ihre Audits.

tenfold ist in 3 Editionen erhältlich!

- Essentials: Active Directory® & Fileserver spielend einfach verwalten.
Optimal für Microsoft® Umgebungen.
- Essentials Plus: Berechtigungsmanagement für Microsoft SharePoint® & Exchange®.
- Enterprise: Anwendungsberechtigungen über Drittsysteme hinweg bequem managen, z.B. SAP®, ERP-, CRM-Systeme, Ticketing-Systeme etc.

Jetzt NEU: tenfold 2018 – Mit unserer **bahnbrechenden Plugin-Technologie** bieten wir Vorsprung durch technologische Innovation!

Halle 9, Stand 524
www.tenfold-security.com



Mehr Wert.
Mehr Vertrauen.

TÜV SÜD – Mehr Wert. Mehr Vertrauen.

Digitale Sicherheit bedarf heute Leistungen, die neue Standards für morgen definieren. TÜV SÜD unterstützt Sie als kompetenter Wegbegleiter mit Sealed Cloud Lösungen und Services zu Cyber Security, Cyber Risk Management und Datenschutz.

Mit Hauptsitz in München, ca. 24.000 Mitarbeitern und 1.000 Standorten weltweit hat sich TÜV SÜD seit 1866 als eines der führenden technischen Dienstleistungsunternehmen international etabliert – mit Prüfungen und Produkttests, mit Inspektionen, Auditierungen und System-zertifizierungen, mit Trainings und Schulungen. Mit unserem umfassenden Portfolio unterstützen wir Unternehmen dabei, Geschäftsprozesse zu optimieren, Risiken zu managen und in globale Märkte zu expandieren.

TÜV SÜD: Mit Sicherheit digital. Besuchen Sie uns auf der it-sa in **Halle 9, Stand 9-458**.

Halle 9, Stand 9-458
www.tuev-sued.de



Halle 9, Stand 510
www.vds.de

Auch zu spät?

Jetzt DSGVO mit nur 32 Seiten umsetzen.

Prämierte, kompakte Leitfäden für Datenschutz + Informationssicherheit. Speziell für KMU.

Mit den zertifizierungsfähigen Managementsystemen von VdS Schadenverhütung GmbH, einem in Europa führenden Anbieter für Unternehmenssicherheit, nutzen Sie Synergien und reduzieren so Ihren Aufwand – bei optimaler Absicherung.

- **VdS 10000, Informationssicherheit** (bereits unter den Top 3 der in Deutschland implementierten ISMS, ausgezeichnet mit dem „Branchenoscars“ Security Innovation Award, BSI-/ISO-vereinbar)
- **VdS 10010, Datenschutz** („Best of“-Preis der Initiative Mittelstand für besonders wirkungsvolle IT-Lösungen)

Beide kostenlos am **Stand 9-510** und auf vds.de/cyber

Heidelberg, Print Media Academy.
 16.-18. Oktober 2018

// heise
devSec()

Die Konferenz für sichere Software- und Webentwicklung

KEYNOTES BY: ■ *Paula Januszkiewicz*, Gründerin der Sicherheitsfirma CQURE Inc.
 ■ *Mikko Hypponen*, internationaler Sicherheitsexperte (F-Secure)

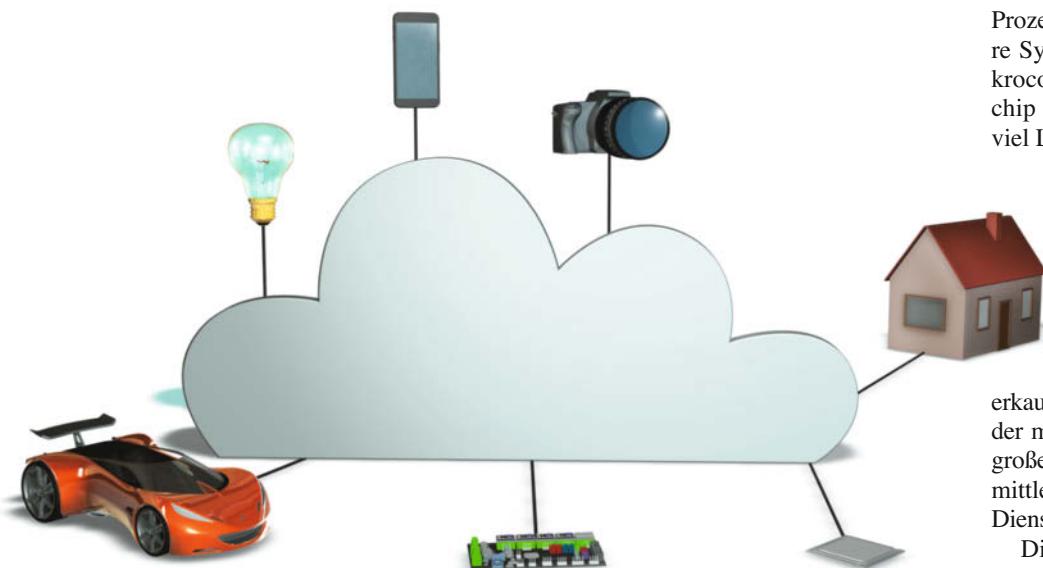
JETZT ANMELDEN!

Weitere Infos zum Programm, Tickets & Co. unter: www.heise-devsec.de

IoT-Cloud-Dienste von Microsoft, Amazon und Google

Stützräder in der Wolke

Tam Hanna



Komplett von Hand entworfene IoT-Systeme mögen besonders effizient sein, hinsichtlich der Kosten liegen jedoch vorgefertigte Module vorn. Dafür bieten Amazon, Google und Microsoft in ihren Cloud-Diensten IoT-Funktionen, die dieser Artikel vergleicht.

Allen IoT-Diensten gemein ist, dass sie sich von manuell realisierten Architekturen deutlich unterscheiden. Stattdessen setzen die Cloud-Anbieter darauf, die Geräte mit einer Einlaufstelle zu verbinden, die die Informationen sammelt und danach an hauseigene Services weiterleitet, etwa Maschine Learning oder Event-Busse. Klassische zentrale Server spielen in dieser schönen neuen Welt nur eine untergeordnete Rolle – wer die IoT-Daten mit einem lokalen Programm verarbeiten will, hat wenig Freude.

Alljährlich befragt die IoT Working Group der Eclipse Foundation Entwickler zu diversen Eckdaten ihrer IoT-Projekte, unter anderem zur Nutzung von Cloud-

Diensten ([a], siehe ix.de/ix1810076). Google musste zwischen 2017 und 2018 Haare lassen – sein Marktanteil sank von 20,4 % auf 18,8 %. AWS ist mit 51,8 % der King of the Hill, während Azures Anteil auf 31,21 % anstieg. Allerdings sind diese Erkenntnisse mit Vorsicht zu genießen: Die Antworten stammten 2018 von 500 Teilnehmern, 2017 waren es noch 200 mehr.

Linux dominiert die Prozessrechner

IoT-Systemverbünde bestehen aus einer Gruppe von Endgeräten (Nodes), die meist recht leistungsschwach sind. Am

bequemsten ist sicher die Nutzung fertiger Prozessrechner wie Raspberry Pi und Co. – hier lässt sich das Hantieren mit aufwendig integrierbaren SoCs vereinfachen. Weder Android Things noch Windows 10 für IoT konnten in diesem Bereich bisher viel erreichen – ist ein Prozessrechner am Start, so setzt man auf Linux.

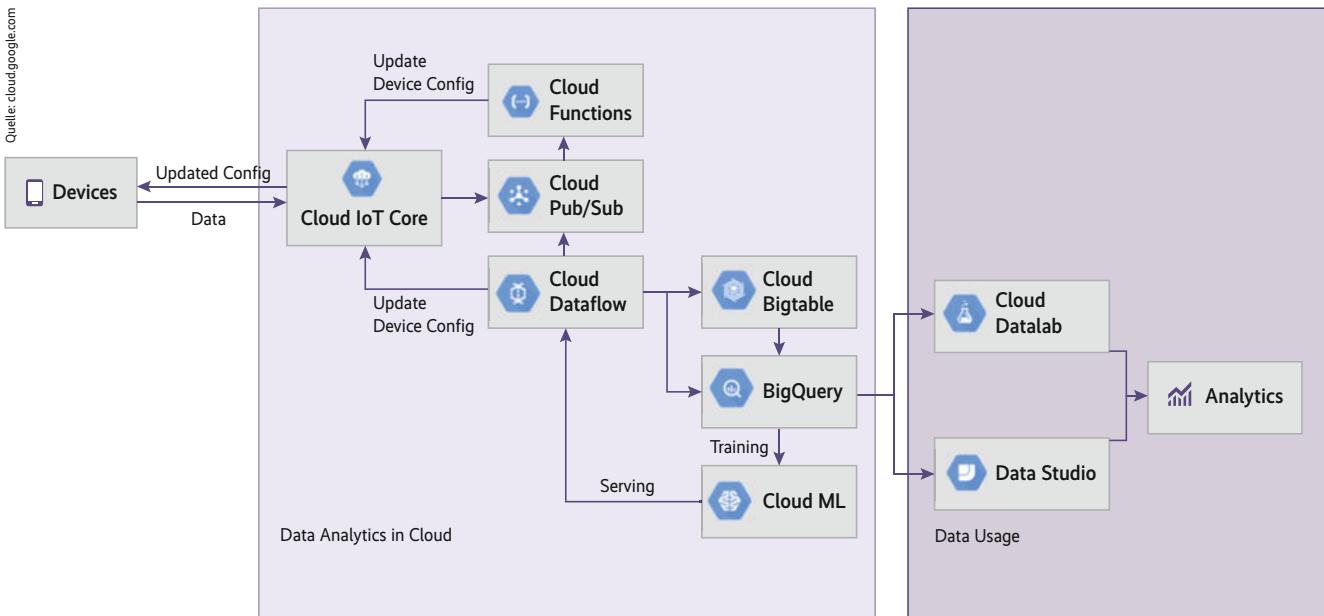
Leider sind Einplatinencomputer kein Universalheilmittel. Sie verbrauchen viel Strom, Stand-by-Modi fehlen und die Echtzeitfähigkeiten lassen zu wünschen übrig. Deshalb kann es sich auch für Kleinserien lohnen, eigene Boards zu bauen. Das sind dann meist aber keine Prozessrechner-Derivate, sondern kleinere Systeme, etwa auf Basis diverser Mikrocontroller – ST, Renesas, TI, Microchip und Konsorten bieten heutzutage viel Leistung fürs Geld.

Aufgrund fehlenden Speicherschutzes und wenig RAM spielt Linux in diesem Bereich nur eine untergeordnete Rolle. Stattdessen setzt man auf dedizierte Echtzeitbetriebssysteme, von denen iX einige vorgestellt hat [b]. Ihnen gemeinsam ist eine geringere Latenz, erkauft durch kleineren Funktionsumfang der mitgelieferten Bibliotheken. Fast alle großen Betriebssystemanbieter offerieren mittlerweile Erweiterungen, die Cloud-Dienste einbinden.

Die im nächsten Abschnitt besprochenen Integrationsserver arbeiten mit standardisierten Protokollen. Deshalb kann man Systeme auf WLAN-Modulen wie dem ATWINC1500 aufbauen. Entwickler löten diese als ESP32-artiges „Dickschichtmodul“ vorliegende WiFi-to-SPI-Brücke auf die Platine; der vorhandene Mikrocontroller nimmt per SPI (Serial Peripheral Interface) Kontakt zum Kommunikationsprozessor auf dem Modul auf. Das Modul agiert dann als Abstraktionsschicht, die sich um Protokollauswertung und Ähnliches kümmert. Microchip zeigt online einige Beispiele [c].

Echtzeitbetriebssystem von Amazon

Cloud-Anbieter schauen den Mikrocontroller-Experimenten ihrer Kunden im Allgemeinen desinteressiert zu – solange man das Protokoll implementiert, ist alles gut. Amazon tanzt hier allerdings aus der Reihe. Durch die Übernahme von FreeRTOS sicherte es sich ein Alleinstellungsmerkmal. Der Klassiker für Echtzeitbetriebssysteme schlechthin ist direkt mit AWS verbunden. Die einzige wichtige Frage ist, ob man eigene Geräte lieber di-



Bei Integrationsservern laufen die Daten der IoT-Geräte ein (Abb. 1).

rekt mit den AWS-Servern kommunizieren lässt oder mit einer der später besprochenen Edge-Varianten indirekt anbindet.

Microsoft geht mit Azure Sphere einen interessanten Sonderweg, der im Moment allerdings noch kaum im Markt angekommen ist. Für einen Prozesserrechner kombiniert es einen unter Linux laufenden ARM-Prozessor mit einem Echtzeitkern, um so sowohl Echtzeitanforderungen als auch komplexe Aufgaben lösen zu können. Hauseigene ARM-CPUs – noch gibt es nur den MT3620AN aus dem Hause MediaTek – treten in Kombination mit einem adaptierten Linux-Kernel auf.

Das für Ende 2018 angekündigte Development Kit erlaubt erste Einblicke in die Hardwarekonfiguration des Prozesserrechners à la Microsoft. Gerüchteweise hat der Haupt-A7-Prozessor 4 MByte RAM und einen Takt von 500 MHz, den beiden für Echtzeitaufgaben vorgesehenen Cortex-M4F-Cores steht rund 1 MByte RAM zur Verfügung.

Für Geräteentwickler ist die Diskussion über die Betriebssysteme der IoT-

Geräte immens wichtig. Am Server arbeitende Kollegen betrachten sie jedoch als akademisch, weil die Kommunikation mit dem Rechnerverbund über eine Art Integrationsserver erfolgt (siehe Abbildung 1). Er sammelt von den Devices eingehende Ereignisse ein, entpackt die Ereignisinformationen aus dem MQTT-Container und übersetzt sie in das Event-System des jeweiligen Cloud-Anbieters. Bei Microsoft hört dieser Server auf den Namen Azure IoT Hub, bei Amazon auf AWS IoT Core. Googles Dienst nennt sich Cloud IoT Core und verhält sich ähnlich wie die beiden anderen.

Drei Protokolle stehen zur Wahl

Für die Kommunikation auf unterer Ebene setzen alle Systeme auf TCP/IP – ohne Netzwerk-Stack ist es nicht möglich, Informationen direkt in Richtung der Cloud zu schicken. Auf der Applikationsschicht haben sich die Protokolle im

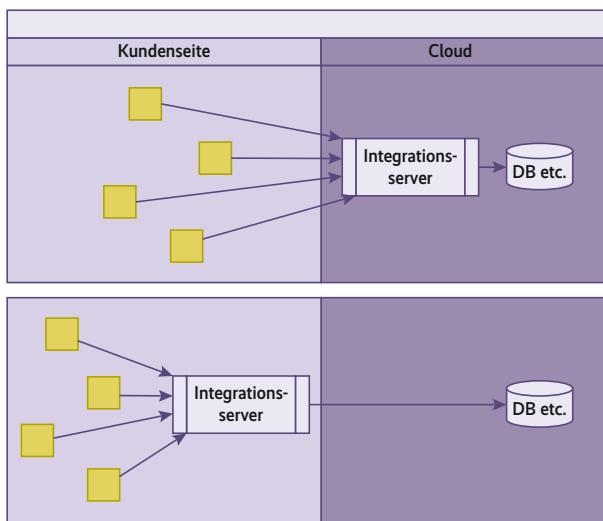
Großen und Ganzen standardisiert. Die Integrationsserver richten sich in Sachen Protokollunterstützung am Markt aus: Alle bieten MQTT (Message Queuing Telemetry Transport) und HTTP. Das an HTML erinnernde AMQP (Advanced Message Queuing Protocol) unterstützt zurzeit nur Microsoft direkt, das es ebenso wie MQTT auch über WebSockets anbindet [d]. Amazons MQTT-Umsetzung enthält ebenfalls WebSocket-Tunneling. Das erleichtert den Einsatz, wenn nur HTTP(S)-Verbindungen möglich sind. Wer zugunsten der Rechenleistung auf Verschlüsselung verzichten möchte, hat derweil wenig Auswahl: Microsofts Azure IoT Hub akzeptiert nur mit SSL gesicherte Verbindungen, AWS verhält sich ähnlich.

Cloud IoT Core geht einen anderen Weg: Google bietet keinen MQTT-WebSocket-Tunnel zum Umgehen von Firewalls an. Stattdessen erlaubt es unverschlüsselte HTTP-Verbindungen – witzigerweise muss aber MQTT mit TLS abgesichert werden. Alle Anbieter implementieren MQTT 3.1.1, 5.0 ist nirgends im Angebot. Bei Amazon unterliegt es einigen Einschränkungen, die Rechenzeit sparen sollen, etwa weniger QoS-Level [e]. Ein netter Ersatz für deren Fehlen sind die Kanäle \$aws/events/presence/connected/clientId und \$aws/events/presence/disconnected/clientId, über die das Backend das Auftauchen und Verschwinden von Clients avisiert.

Der auffälligste Unterschied zwischen den IoT-Umsetzungen ist die für die Preisberechnung betrachtete Größe der ausgetauschten Nachrichten. Bei Micro-

TRACT

- Anbieter wie Amazon, Google und Microsoft verbinden IoT-Geräte mit Cloud-Diensten. Außerdem stellen sie Technik bereit, die einfachere Aufgaben „on Premises“ ausführt, um die Abhängigkeit von der Internetverbindung zu reduzieren.
- Damit lassen sich Kosten bei der IoT-Hardware sparen: Sie kann auf preiswertere und stromsparende Spezialnetze statt auf TCP/IP setzen.
- Die Preismodelle der IoT-Cloud-Dienste sind so unübersichtlich, dass es kaum möglich ist, die Kosten zu vergleichen.



Bei Cloud-Edge-Systemen (oben) liegt der Integrationsserver in der Cloud, während er beim Device Computing beim Endanwender steht (Abb. 2).

stehende Gedanke ist einfach: Statt alle Arbeit in der Cloud zu erledigen, lässt man lokale Hard- und Software Aufgaben ausführen.

Neben verringerter Latenz ermöglicht Device Edge Computing den Einsatz einfacherer Hardware für die IoT-Geräte. Statt TCP/IP und stromfressender Protokolle kann man energieeffiziente Vernetzungsverfahren einsetzen, was zu geringeren Kosten führt.

Google geht hier insofern einen eigenen Weg, als es bisher kein dediziertes Gateway-Betriebssystem anbietet. Der Entwickler hat die Qual der Wahl – dass Android Things ob der Verfügbarkeit diverser Bibliotheken zur Kommunikation mit dem hauseigenen Cloud IoT Core eine günstige Position einnimmt, liegt nahe.

Manche Cloud-Aufgaben selbst erledigen

Amazon preschte mit Greengrass vor, während Microsoft seine Edge-Runtime erst später auslieferte. Durch den späten Einstieg ist dessen Architektur solider: Die Edge-Module liegen bei Microsoft als Docker-Container vor, die nur wenige Beziehungen zum zugrunde liegenden Betriebssystem unterhalten. Greengrass geht die Sache weniger allgemein an und unterstützt nur vier Hostsysteme: ARMv7l mit Raspbian, x86_64 mit Amazon Linux oder Ubuntu (14.04 bis 16.04) und ARMv8 ebenfalls mit Ubuntu.

Greengrass wie Edge erlauben das lokale Ausführen diverser Payloads, die normalerweise in der Cloud laufen. Die gelieferten Container und Programme enthalten Zusatzsoftware mit abgespeckten Versionen der Cloud-Features. Neben den Funktionen und Device Shadows können die Geräte auch kleinere Machine-Learning-Aufgaben ausführen. Dabei kommen die schwachbrüstigen CPUs von Raspberry Pi und Co. jedoch nicht weit.

Microsoft verlangt nichts für sein Azure Edge, Kosten entstehen nur beim Nutzen von Diensten wie Machine Learning oder den weiter oben besprochenen Rechenfunktionen. Amazon erhebt für Greengrass pro Gerät rund 2 US-Dollar pro Jahr, abgerechnet wird monatlich.

soft sind es 0,5 KByte (für das kostenlose Angebot) und 4 KByte, bei Amazon durchgehend 5 KByte. Google wiederum berechnet mindestens 1024 Byte. Bei den eigentlichen Cloud-Diensten nehmen sich die Angebote nur wenig. Der primäre Unterschied zwischen AWS und Azure ist der Name, die Services sind im Großen und Ganzen identisch. Das gilt auch für die Data Centers – öffnet ein Anbieter in einer neuen Region ein Rechenzentrum, folgt ihm die Konkurrenz auf den Fuß.

Amazon EC2 gilt als flexibler, während Microsoft dank der exzellenten Integration zwischen Azure und Visual Studio Entwicklungszeit spart. Beim Übertragen von Notifications liegt Google vorne; Amazon und Microsoft bieten allerdings komfortable Schnittstellen für die Nutzung von Google Cloud Messaging (GCM), das sich mittlerweile als De-facto-Standard in Sachen Notifications etabliert hat und insbesondere im Mobilbereich jedermann bekannt ist.

Alle drei Firmen bieten Visualisierungsprodukte, die für den Verkauf von IoT-Systemen hilfreiche Grafiken generieren. Zum Verarbeiten der eingehenden Nachrichten stehen diverse virtuelle Maschinen zur Verfügung – Amazon zeichnet sich hierbei durch eine Vielzahl vorgefertigter Images aus.

Wer lieber ohne VM auskommt, kann bei allen Anbietern auf „Cloud Functions“ setzen. Bei Microsoft sind das „Azure Functions“, Amazon nennt sie „Lambda Functions“ und bei Google heißt der Ser-

vice „Cloud Functions“. Die dahinterstehende Idee ist indes identisch – Entwickler dürfen Applikationscode hochladen, den die Plattform beim Eintreffen eines Trigger-Ereignisses ausführt.

Weniger Latenz durch lokale Hardware

Der wichtigste Unterschied zwischen den drei Diensten ist die Anzahl der unterstützten Programmiersprachen, die die Tabelle kurz zusammenfasst. Microsofts scheinbare Überlegenheit muss man allerdings mit Vorsicht betrachten, da nicht alle Versionen der Runtime jede Sprache gleichermaßen anbinden – weitere Daten hierzu finden sich unter [f].

Alle drei Unternehmen bieten ihren Kunden Analyse- und Machine-Learning-Dienste an. Deren vollständige Besprechung würde den Rahmen dieses Artikels sprengen. Wer sich mit einer der Plattformen auskennt, sollte auf keinen Fall zu einem anderen Anbieter wechseln – der Aufwand des Neulernens amortisiert sich in der Regel nicht.

Zugriffe vom Endgerät zur Cloud unterliegen Latzenzen – selbst bei sehr schnellem Internetzugang ist ein lokal angebundenes System besser erreichbar. Die bisher besprochene Anbindung an die Cloud heißt im Englischen „Cloud Edge“; die Verlagerung der Einlaufstelle in das lokale Netz ermöglicht das alternative Device Edge oder Edge Computing (siehe Abbildung 2). Der dahinter-

Programmiersprachen für IoT-Dienste

Amazon Lambda Functions	Google Cloud Functions	Microsoft Azure Functions
Node.js (v8.10, v6.10, v4.3), Java 8, Python (3.6, 2.7), .NET Core (1.01, 2.0), Go 1.x	„JavaScript“	C#, JavaScript, F#, Java, Python, PHP, TypeScript, Batch (.cmd, .bat), Bash, PowerShell

Neue IoT-Geräte automatisiert anbinden

Alle drei Anbieter kümmern sich bis zu einem gewissen Grad um das Provisio-

nieren von IoT-Devices. Als Beispiel dafür sei der in Abbildung 3 gezeigte Prozess bei Microsoft angenommen.

Ein Secure Element – es handelt sich hier übrigens nicht unbedingt um die vom PC bekannten Chips [g] – hält dafür eine für jedes Gerät einzigartige ID vor. Beim Verbindungsaufbau kontaktiert das Gerät eine Schnittstelle, die für die Provisionierungsvorgänge verantwortlich ist.

Nach einer Identitätsprüfung (Schritt 3) nimmt der Provisionierungsdienst Kontakt zu einem IoT-Hub auf, der das neue Gerät anlegt. Er liefert daraufhin einen Verbindungsstring an das Endgerät, der es fortan gegenüber dem IoT-Hub ausweist (Schritt 6). Die Auslieferung der Konfigurationseinstellungen erfolgt über Device Twins, um die es weiter unten geht.

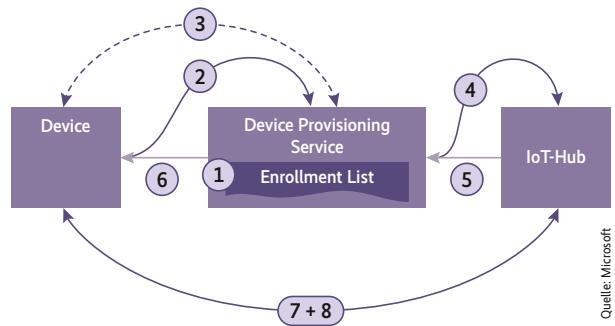
Amazon verfolgt ein ähnliches Konzept, in dem der Entwickler im ersten Schritt Templates festlegt. Auch hier erfolgt anschließend eine Provisionierung anhand eines Secure Element. Cloud-Provider kooperieren normalerweise mit Herstellern solcher Sicherheitschips. Google arbeitet beispielsweise mit den von Microchip angebotenen Secure Elements, was durch fertige Provisionierungsskripte Zeit spart.

Verlagerung von Zuständigkeiten zum Kunden mag Internetausfälle bis zu einem gewissen Grad kompensieren. Allerdings bleiben solche Aufgaben, die nur der Server erledigen kann. Um sie bei fehlender Verbindung zum Endgerät so effizient wie möglich auszuführen, bieten sich Caches an. Das sind zwischen Integrationsserver und Endgerät geschaltete Speicher, die bei fehlender Internetverbindung Informationen bereitstellen oder zwischenspeichern.

Amazon nennt diese Dienste Device Shadows, Microsoft spricht von Device Twins. In beiden Fällen handelt es sich um Caches, die zwischen Gerät und Server stehen und dem Server einen Key-Value-Speicher zur Verfügung stellen. Dieser nimmt vom Gerät angelieferte Messwerte entgegen und speichert bei Verbindungsabbrüchen Änderungsbefehle zwischen – besteht die Netzverbindung wieder, muss das Gerät die Deltas auswerten. Google trennt diese Funktionen, da es Device State (vom Gerät zur Cloud) und Device Configuration (in die Gegenrichtung) als separate Dienste betrachtet.

Als Austauschformat für diese Caches dient prinzipiell JSON. Allerdings erweist sich dessen insbesondere bei Microsoft immens komplizierte Struktur als Ärgernis. Die Daten umfassen schon mal einige Kilobyte und sind Dutzende Ebenen tief

Der Provisioning-Prozess von Cloud-Anbietern setzt ein Secure Element voraus und verläuft in mehreren Schritten (Abb. 3).



Quelle: Microsoft

verschachtelt. Client und Server können sich bei Änderungen informieren lassen oder regelmäßig pollen, um die Inhalte der Dokumente abzugleichen.

Kostenschätzung mutwillig schwer gemacht

Ein alter Kalauer in der Welt der Cloud-Dienste behauptet, das Mieten einer Ressource über ein Jahr entspreche dem Kaufpreis. Cloud-Provider bekommen ihr Geld eben nicht für preiswerte Offeren, sondern für das übernommene Risiko und die bereitgestellten Skalierungsreserven. Azure und Co. erschweren das Schätzen von Kosten absichtlich, da Preisvergleiche nicht in ihrem Interesse liegen.

Als Erstes sei ein Blick auf die Integrationsserver geworfen, die es in einer Vielzahl von Varianten gibt. Microsoft hält pro übertragener Nachricht die Hand auf und unterscheidet zudem verschiedene Editionen seiner Server. Google berechnet stattdessen das übertragene Datenvolumen und setzt als Mindestgröße pro Transaktion ein Kilobyte an. Da es komprimierte Payloads vor der Berechnung auspackt, kann es mitunter zu deutlichen Preiserhöhungen kommen.

Amazon nutzt ein wesentlich komplexeres Preisberechnungsmodell [h], das die von Microsoft und Google verwendeten Verfahren kombiniert. Dass die Preise je nach geografischem Ort der Ressourcen um 75 % und mehr differieren,

erschwert die Schätzung zusätzlich. Einen aktuellen Vergleich der Kosten verschiedener Einsatzszenarien hat Ian Skerret erstellt [i]. Dort kommt Amazon am besten weg, gefolgt von Google und Microsoft. Dieser Vergleich berücksichtigt jedoch nur die Kosten für IoT-Messages und betrachtet weder Speicher noch Rechenzeit.

Schließlich sei angemerkt, dass die Qualität der Dokumentation ein wichtiger Entscheidungsfaktor ist. Der mit Windows Mobile aufgewachsene Autor empfindet Microsoft als am bequemsten, sieht Amazon auf dem zweiten Platz und Google weit abgeschlagen. Andere Entwickler mögen zu einer abweichenden Platzierung kommen.

Fazit

Die Auswahl der bestgeeigneten IoT-Plattform ist eine schwierige Aufgabe, bei der eine Vielzahl verschiedener Parameter zu beachten ist. Betriebskosten sind dabei nicht das einzige Kriterium, ist das Ziel doch die Reduktion der Gesamtkosten. Trotz der auf den ersten Blick unterschiedlichen Angebote von Microsoft, Google und Amazon gilt, dass nur einige Wege nach Rom führen. Es gilt das Prinzip der konvergenten Evolution, etwa bei Trägerraketen mit der Ähnlichkeit zwischen Sojus und Saturn.

Finden sich im Gesamtökosystem bereits Komponenten von einem der drei Anbieter, ist es im Allgemeinen empfehlenswert, auch den Rest aus dieser Quelle zu beziehen – das Weiterreichen von per Azure IoT eingesammelten Daten beispielsweise an Google arbeitet in Arbeit aus.

(odi@ix.de)

Tam Hanna

ist Gründer der Tamoggemon Holding k.s. Er befasst sich seit Jahrzehnten mit interdisziplinären Lösungen im Handcomputerbereich.





Red Teaming: Eindringen in der wirklichen Welt

Mit Hand und Fuß

Sascha Herzog

Der fünfte Artikel der Serie zu „Red Team Assessments“ beschreibt das Thema physisches Eindringen in Gebäude und gesicherte Bereiche. Von den Analysten verlangt das, ihre gewohnte Komfortzone am Schreibtisch zu verlassen und sich die Hände schmutzig zu machen.

Der erste Artikel dieser Serie [1] skizzierte bereits einen Fall, bei dem es uns nachts gelang, über schlecht gesicherte Tiefgaragen Zugang zu wichtigen Gebäudeteilen einer kritischen Infrastruktur zu erlangen. In solchen Fällen verwendet man häufig auch Werkzeuge wie Lockpicking-Sets und geklonte RFID-Karten, um verschlossene Türen zu öffnen (Links zu den Werkzeugen und alle weiteren Links des Artikels sind unter ix.de/ix1810080 zu finden).

In dem Fall, der heute beschrieben werden soll, bevorzugten wir Social Engineering als Werkzeug der Wahl, um uns physischen Zugang zu einem gut gesicherten Bereich in einem der Gebäude unseres Kunden zu verschaffen. Bei dem Kunden handelt es sich um ein internationales Unternehmen aus einem speziellen Bereich der industriellen Fertigung.

Die gesamte Aktion erforderte ein hohes Maß an Planung und Vorbereitung – weshalb wir uns wie immer zu Beginn

möglichst viele taktisch relevante Informationen beschafften, um daraus die effektivsten Angriffspfade zu konstruieren. Eine Idee war, sich als Servicetechniker auszugeben, der die Wartung einer zentralen Maschine vornehmen muss. Diese stand im gut gesicherten Reinraum zur maschinellen Fertigung spezieller Komponenten und würde einem Angreifer nach erfolgreicher Kompromittierung ermöglichen, die gesamte Produktion nachhaltig und lange Zeit unbemerkt zu stören oder vollständig lahmzulegen.

Im schlimmsten Fall droht der Ruin

So etwas ist beispielsweise durch die Veränderung von Bohrlöchern im Millimeterbereich oder durch die Zerstörung extrem teurer Spezialmaschinen möglich. Deren Austausch kann viele Monate dauern, ohne dass währenddessen weiter produziert werden kann. Im schlimmsten Fall bedeutet das für ein Unternehmen den finanziellen Ruin oder eine anhaltende Rufschädigung.

Nur zwei Personen im Unternehmen hatten Zugang zu dem gut gesicherten Bereich, in dem die Maschine stand. Um in diesen Raum zu gelangen, musste man zuvor mehrere zugangsgeschützte Bereiche und eine Schleuse passieren, ganz abgesehen von den Überwachungskameras und dem Alarmsystem. Der beste Weg dorthinein war also ein autorisierter Zugang per Einladung durch das Unternehmen selbst.

Durch unsere Informationsbeschaffung zu Beginn kannten wir den Maschinenhersteller und die Techniker, die für Servicewartungen zuständig waren. In einem ersten Schritt klonten wir die Webseite des Maschinenherstellers, besorgten uns ein gültiges Serverzertifikat und richteten einen Mailserver für die neue Domain ein. Daraufhin meldeten wir uns telefonisch beim Fertigungsleiter, den wir über LinkedIn ausfindig machen konnten, unter dem Vorwand, dass wir aufgrund eines Fehlers in der Software der Maschine gerade überall manuell Patches einspielen müssten, da es sonst zu Fehlern in der Produktion kommen könnte.

Angekündigter Servicebesuch

Der Fertigungsleiter kaufte uns die Geschichte am Telefon ab, verwies uns aber an seinen Teamleiter, der ihn während seines Urlaubs, den er eine Woche später

 Termin Wartung

Sehr geehrte Damen und Herren,

vor kurzem wurde ein Fehler in der Steuerungssoftware der [REDACTED]-Serie gefunden. Laut unserer Kundendatenbank verfügt Ihr Betrieb über mindestens eine [REDACTED]. Der Fehler führt bei einzelnen Maschinen zu Fehlproduktion (ca. 1/500) und/oder Produktionsstillständen sowie Verringerung der Produktionsraten. Der Software-Fehler scheint datumsabhängig ausgelöst zu werden.

Da in letzter Zeit vermehrtes Auftreten dieses Fehlers und mehrtägige Produktionsausfälle gemeldet wurden, sendet [REDACTED] aktuell Service-Techniker zu allen Kunden aus. Unser Terminplan sieht Anfang Juni für den Raum [REDACTED] vor. Gemäß Absprache mit Ihrem Betrieb würde ein Service-Techniker am [REDACTED]

gegen
10:30
die Wartung vornehmen.

Die Länge des Wartungsfensters beträgt ca. 30 Minuten. Die Aktualisierung kann im laufenden Betrieb durchgeführt werden, sodass die Produktion nicht unterbrochen werden muss.

Wir entschuldigen uns für die Unannehmlichkeiten. Sollten bei ihrer [REDACTED] Fehler auftreten, teilen Sie uns dies bitte umgehend unter [not-service@\[REDACTED\].de](mailto:not-service@[REDACTED].de) mit.

Freundliche Grüße / Best regards,

[REDACTED] | Service | Germany
T +49 (0) 17 [REDACTED] | F +49 ([REDACTED])
[service@\[REDACTED\].de](mailto:service@[REDACTED].de) | [REDACTED]
Sitz (Seat): [REDACTED]

Dank der ähnlichen Domain und des echten Hersteller- und Maschinennamens ließ sich eine plausible, echt wirkende E-Mail konstruieren (Abb. 1).

antreten wollte, vertreten sollte. Er bat uns, diesem eine E-Mail zu schicken und einen Termin vorzuschlagen. Da wir ja eine sehr ähnliche Domain wie der echte Servicetechniker besaßen, konnten wir eine authentisch aussehende E-Mail an den Vertreter des Fertigungsleiters senden (Abbildung 1).

Der Ortstermin wurde uns kurze Zeit darauf bestätigt und wir konnten einen

Analysten schicken, der, als Servicetechniker verkleidet, versuchen würde, an die Maschine zu kommen. Dafür brauchte er natürlich echt aussehende Visitenkarten und einen Mitarbeiterausweis. Beides erstellten wir kurzerhand mit unserem Visitenkartendrucker (Abbildung 2).

So vorbereitet, erschien unser Mitarbeiter pünktlich um 10:30 Uhr am Haupteingang des Unternehmens, meldete sich

bei der Empfangsdame und übergab ihr gleich seine Visitenkarte. Die Empfangsdame bat die Vertretung des Fertigungsleiters telefonisch, ihn abzuholen.

Der Fertigungstechniker führte unseren Analysten bereitwillig durch sämtliche Türen. Auf dem Weg zu dem Raum, wo die Maschine stand, warf unser Mitarbeiter nebenbei noch einen USB-Stick mit einem Trojaner unauffällig in ein offenes

SMARTE
FLEDERMAUS-LEUCHTE

ODER
AUTONOME DROHNE?

Neugierig geworden?

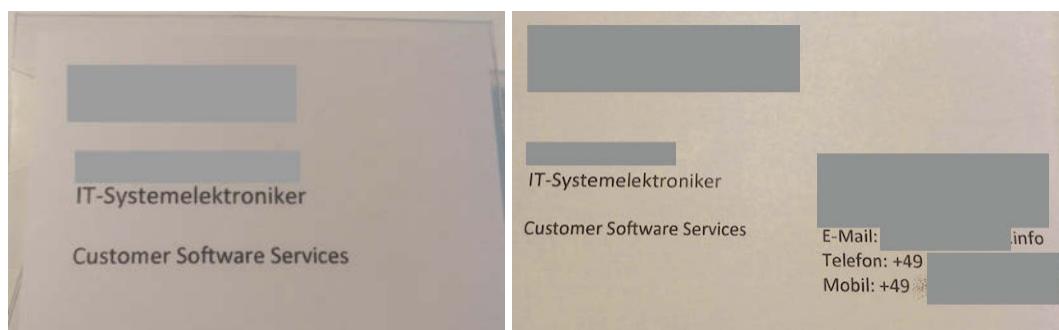
Testen Sie jetzt 3 Ausgaben Technology Review und sparen Sie über 9 Euro.

Lesen, was wirklich zählt in Digitalisierung, Energie, Mobilität, Biotech.



Bestellen Sie jetzt unter
trvorteil.de/3xtesten





Visitenkarte und Mitarbeiterausweis unterstreichen die Glaubwürdigkeit des Auftretens als Service-mitarbeiter (Abb. 2).

Büro. Die Vertretung des Fertigungsleiters wollte beobachten, was unser Mann mache, und fragte nach, was denn jetzt genau das Problem sei und wie es behoben werden würde.

Angebliches Diagnoseprogramm eingeschmuggelt

Unser Analyst entgegnete, dass er erst mal ein Diagnoseprogramm starten werde, um mögliche Fehler zu lokalisieren, und dann den Patch einspielen wolle. Wie genau der Patch funktioniere, wisse er auch nicht, allerdings wisse er, dass dieser Patch selten verwendete Steuerungsroutinen korrigieren werde. Das sei es, was man ihm mitgeteilt habe. Das System lief in einer UNIX-Umgebung, weshalb wir das angebliche Diagnoseprogramm im Vorfeld erstellen und auf einen USB-Stick bringen konnten.

Unser Programm war harmlos und gab nur ein paar gefälschte Codezeilen auf dem `stdout` der Konsole aus und beendete sich danach. In der Realität hätten Angreifer hierüber allerdings spezielle

Konfigurationsparameter der Maschine verändern oder Malware auf das System spielen können. Wie unser gefälschtes Diagnoseprogramm aussah, zeigt Abbildung 3.

Nach Beendigung des Programms machte unser Analyst noch einen Schnappschuss von dem Bildschirm samt Maschine, um einen Beweis für die Kompromittierung zu haben. Zu dem anwesenden Fertigungstechniker sagte er, das brauche er, um die „Response Codes“ zu dokumentieren, die er in seinen Bericht schreiben müsse. Der Techniker kaufte ihm alles ab und begleitete ihn anschließend noch bis zum Ausgang. Alles in allem dauerte der Vororteinsatz nur 25 Minuten. Somit hatten wir den Beweis angetreten, dass und auf welche Weise es möglich ist, das Herzstück der Fertigung und damit das Herzstück des Unternehmens vollständig zu kompromittieren und das Ziel dieser Red-Team-Kampagne zu erreichen.

Wir erfuhren später, dass der USB-Stick mit dem Trojaner zwar von einer Mitarbeiterin gefunden, allerdings nicht in ihren PC eingesteckt, sondern vorbild-

lich bei der Unternehmensleitung abgegeben wurde.

Festgelegte Prozesse etablieren

Ein paar Wochen nach diesem Einsatz führten wir eine Awareness-Kampagne bei dem Kunden durch und schulten die Mitarbeiter, wie sie mit solchen und ähnlichen Angriffen umgehen sollten. Zudem unterstützten wir den Kunden in der Entwicklung von Richtlinienkatalogen und Prozessen, um so etwas zukünftig zu vermeiden. Alleine das Anfordern von Ausweisen am Empfang kann hier schon einiges bewirken und hätte einen realen Eindringling wahrscheinlich abgewehrt.

Auch die Rücksprache mit bekannten Ansprechpartnern im echten Serviceunternehmen hätte dabei helfen können, das falsche Unternehmen zu enttarnen. Positiv zu bemerken war, dass das Unternehmen in Sachen Zugangsschutz und physischer Überwachung bereits sehr gut ausgerüstet war. Und ebenso waren einzelne Mitarbeiter, wie die Dame aus dem Büro, schon ausreichend geschult, um auf manche Arten des Social Engineering nicht hereinzufallen.

Im nächsten Artikel unserer „Red Teaming“-Serie befassen wir uns intensiv mit der Technik hinter Backdoor-Trojanern, dem Umgehen von Sicherheitstechnologien, schwer zu entdeckenden „Command & Control“-Kanälen und dem Ausbreiten in internen Netzwerken, dem „lateral Movement“. (ur@ix.de)

```
top:~$ ./update.sh
Updater v.1.1.3 ----
radio signal to activate wireless maintenance module.....
maintenance module activated!
g for unpatched machines.....
found! Commencing update.....
ng file /lib/modules/3.19.0-16-generic/kernel/drivers/firewire/nosy.ko.
ng file /sys/devices/LNXSYSYMT:00/LNXSYBUS:00/PNP0A08:00/device:22/device
ce:29/power/runtime_enabled.
ng file /sys/devices/LNXSYSYMT:00/LNXSYBUS:00/PNP0A08:00/device:3a/device
ce:3c/device:44/power/runtime_usage.
ng file /sys/devices/platform/PNP0C14:02/power/runtime_active_time.
ng file /etc/apparmor.d/abstractions/likewise.
ng file /etc/vmware-installer/components/vmware-ovftool.
ng file /lib/modules/3.19.0-18-generic/kernel/drivers/net/ethernet/qlogi
```

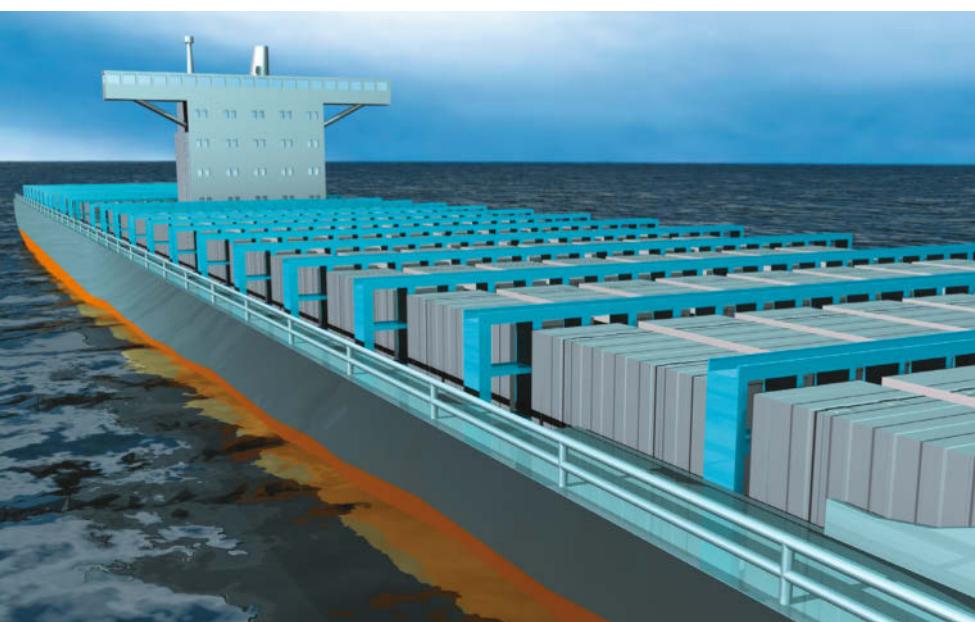
Das in diesem Fall harmlose Diagnoseprogramm hätte auch schlimme Auswirkungen nach sich ziehen können, etwas das Manipulieren von Konfigurationsparametern (Abb. 3).

Sascha Herzog

ist technischer Geschäftsführer und Penetrationstester bei der NSIDE ATTACK LOGIC GmbH in München.

- [1] Sascha Herzog; Awareness; Mit allen Mitteln; Sicherheitstests: Angriffe auf Technik und Mensch; iX 2/2018, S. 78





Virtualisierung via CaaS und PaaS

Richtig gestapelt

Christoph Huber, Daniel Takai

Container as a Service und Platform as a Service versprechen in Sachen Virtualisierung von Webanwendungen große Vorteile gegenüber konventionellen Architekturen. Aber was verbirgt sich dahinter, und wann nimmt man was?

Traditionell wird Software per Paketmanager auf dem Betriebssystem installiert, auf dem sich dann die verschiedenen Bibliotheken und Software-pakete vermischen. Schon lange sind die daraus resultierenden Probleme bekannt. Exotische Fehlerbilder ziehen langwierige Analysen nach sich, die viele Stunden später vielleicht eine minimale Differenz in der Version einer verwendeten Bibliothek oder einen zusätzlichen Slash in einem Konfigurationseintrag aufspüren.

Solche Effekte treten besonders häufig auf, wenn das Betriebssystem und ein Administrator die Bibliotheken auf einem sogenannten Snowflake Server manuell pflegen (siehe Kasten „Müll besser vermeiden“). Ganz schnell wird die Sache bei steigender Anzahl der beteiligten Personen immer chaotischer. Konfigurations- und Automatisierungssoftware wie Ansible oder Puppet versprechen zwar

Abhilfe, da sie es ermöglichen, einheitliche Konfigurationen zu verwalten und auszuspielen [1]. Allerdings verlangen solche Werkzeuge fundiertes Wissen und Erfahrung. Sie einzusetzen ist aufwendig und das Entwicklungsteam hat dafür selten Zeit.

Dies endet oft in einer unbefriedigenden Situation: Die Kosten für das Konfigurationsmanagement bleiben trotz guter Werkzeuge hoch, und es entstehen wieder inkonsistente Systemzustände, da nur ein Teil der Konfigurationen aktiv gewartet wird. Das frische Aufsetzen einer Umgebung ist hier gar nicht oder nur mit großem Aufwand möglich. Wer nicht in diese Falle tappen will, sollte um Snowflake Server also einen Bogen machen.

CaaS- und PaaS-Angebote (Container as a Service, Platform as a Service) erfüllen das Versprechen der sogenannten Immutable Infrastructure und verhindern

Snowflake Server effektiv (siehe Kasten „In Stein gemeißelt“). Aber was macht diese Virtualisierungen aus, und wie unterscheiden sie sich von anderen? Abbildung 1 zeigt die verschiedenen Schichten, die nun genauer unter die Lupe genommen werden sollen.

Prozesse und Daten sauber trennen

Bei Infrastructure as a Service (IaaS) stellt der Anbieter eine Laufzeitumgebung für virtuelle Maschinen bereit. Der Anwender muss sich also nicht mehr um Hardware und Netzwerk kümmern, aber immer noch um das Betriebssystem und alle darauf aufbauenden Schichten. Auf die Maschinen greift er über einen Hypervisor zu. Der isoliert vor allem die virtuellen Maschinen, damit sich deren Prozesse und Daten nicht in die Quere kommen.

Für die Entwicklung ist eine IaaS-Umgebung genauso wenig hilfreich wie das eigene Blech im Keller: Der Aufwand für das Konfigurieren des Betriebssystems und aller darüberliegenden Ebenen bleibt gleich. Es entfallen lediglich die Kosten für Hardware, Mieten, Strom und Ersatzteillager. Vergleicht man die Preise der IaaS-Anbieter, so stellt man jedoch bisweilen fest, dass man mehr Geld investieren muss als beim Eigenbetrieb. Dazu weiter unten mehr.

CaaS stellt auf Basis eines Image und seiner Konfiguration automatisch Container bereit, verteilt, verwaltet und überwacht sie. Prominentester Vertreter dieser Technik ist Kubernetes [2]. Die Container werden anders als bei IaaS auf einem Betriebssystem virtualisiert. In Abbildung 1 muss man also Betriebssystem und Virtualisierungsschicht vertauschen, um das korrekte CaaS-Schichtenmodell zu erhalten. Wie bei IaaS müssen auch hier die Anwendungen voneinander und vom Betriebssystem getrennt werden. Diese Abgrenzung gilt auch für das Dateisystem,

Müll vermeiden

Ein manuell gepflegter Server sammelt mit der Zeit sogenannten Crust an. Dieser Müll besteht aus Konfigurationen und Software-paketen, die beispielsweise für Bugfixes oder Patches individuell eingespielt wurden. Das erschwert die Administration und benötigt viel Dokumentation. Ein Server, der nicht automatisch per Configuration Service verwaltet wird, heißt Snowflake Server (siehe ix.de/ix1810083).

In Stein gemeißelt

In einer Immutable Infrastructure darf niemand die Konfiguration einer Maschine modifizieren. Sie lässt sich nur ändern, wenn eine neue Maschine hinzukommt. Im laufenden Betrieb dürfen Administratoren keine lokalen Konfigurationen vornehmen. Das bedingt unter anderem auch, dass der Service selbst seinen Zustand externalisieren muss, damit Neuprovisionierungen gelingen können. Beispielsweise sollte er seine Konfigura-

tion in eine Datenbank schreiben und nicht in das lokale Filesystem. Erst danach lassen sich Dienste vollständig automatisch wiederherstellen. Da Webanwendungen häufig neu justiert werden, benötigen sie oft auch neue Maschinen. Somit erreicht die Methode eine hohe funktionale Qualität der Betriebsabläufe. Sie sorgt zudem für Integrität in der Konfiguration und verhindert das Entstehen von Snowflake Servern.

sodass die Container zwischen verschiedenen Systemen austauschbar sind.

Der größte Unterschied zu einem traditionellen Deployment ist, dass die Laufzeitumgebung als fertiges Image angelegt wird und nicht erst beim Deployment entsteht. Die Instanziierung des Containers entkoppelt die Anwendung von der darunterliegenden Infrastruktur und macht sie portabel. So lässt sich das-selbe (immutable) Image für Funktions- tests, Akzeptanztests und in der Produktion nutzen. Zudem ergibt sich so eine klare Aufgabentrennung: Das Betriebs- team kümmert sich nur noch um die Umgebung und soll und darf nicht mehr in die Anwendung hineinschauen.

Hat ein Image den Funktionstest bestanden, kann ein Continuous-Integration/-Deployment-Service es nach nochmali- ger Prüfung automatisch auf die gewünschte Umgebung schieben. Dieses einfache Vorgehen begünstigt eine rasche Evolution der Software bei minimalem Overhead, denn idealerweise reicht nun ein Commit des Entwicklers zum Aktualisieren der Produktionsumgebung. Mög- lich ist das zwar auch in einer IaaS-Um- gebung, allerdings benötigt man mehr Spezialwerkzeuge in der Produktionskette, verursacht also höhere Kosten. PaaS ver-

einfacht das Ganze noch weiter, denn hier muss man sich nicht mehr um die Konzeption und Entwicklung der Continuous- Deployment-Umgebung kümmern.

Verfügbare Ressourcen richtig nutzen

CaaS bietet zudem die Möglichkeit der automatischen Skalierung einzelner Container, und zwar sowohl horizontal als auch vertikal. Das kann in Kombination mit der fachlichen Dekomposition der Services eine effiziente und genaue Nutzung der verfügbaren Ressourcen erge- ben. Hierzu gehören Dienste für Routing und Load Balancing. Stürzt ein Container ab, stellt ihn die Umgebung automatisch wieder her.

PaaS und CaaS bieten ähnliche Funk- tionen und sind schwer zu unterscheiden. Tatsächlich funktionieren PaaS-Angebote wie Google App Engine auf einer CaaS- Technik wie Kubernetes. PaaS ist also ein Ansatz, der Quelltext annimmt und da- raus eine fertige Laufzeitumgebung baut, installiert und betreibt. Er beinhaltet sämtliche CaaS-Funktionen, erweitert um mindestens das Erstellen der Container auf Basis reinen Quellcodes.

Dieses Prinzip homogenisiert die Laufzeitumgebung und erleichtert es, Systembetrieb und Entwicklung klar zu trennen: Ersterer stellt sicher, dass die Plattform und die darauf laufenden Anwendungen funktionieren, der Entwickler muss sich „nur“ um den Quellcode kümmern. Will das Betriebsteam beispielsweise eine Komponente oder eine Laufzeitumgebung aktualisieren, erledigt es das global auf der Plattform, das Aktualisieren der Applikationen geschieht automatisch, ohne dass bekannt sein muss, welche Programme wo und wie arbeiten.

Anwendungen, die auf derselben Plat- form laufen, lassen sich isolieren, sodass mehrere Entwicklungsteams die Umge- bung unabhängig voneinander verwenden können. Programme einer Organisation dürfen nicht auf die einer anderen zugrei- fen, es sei denn, sie nutzen eine öffent- liche Schnittstelle.

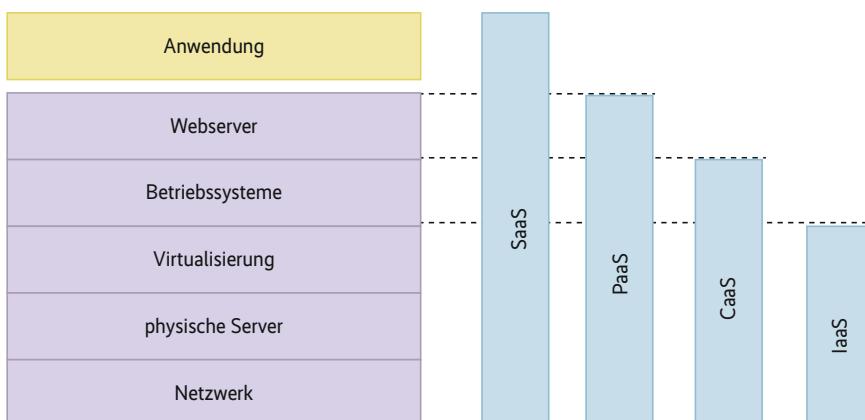
Weiterhin kann eine PaaS-Umgebung Datendienste bereitstellen, etwa Daten- bank- und Cache-Services. Sie beinhaltet oft eine einfache Konvention, die besagt, wie Applikationen automatisch notwendi- ge Konfigurationen zur Verwendung eines Service erhalten (beispielsweise Verbin- dungsdaten). Oft lassen sich solche Dien- ste auf einem Markt- platz mit verschie- denen Attributen bereitstellen. Typische weitere Dienste sind Logging und per- sistentes Messaging für die asynchrone Kommunikation.

PaaS ist in der Lage, die klassischen Leiden von Webapplikationen gut zu be- handeln, wenn sie allein in der Cloud lie- gen (siehe Kasten „Cloud-native Syste- me“). Es ist möglich, sie automatisch mit dem eingehenden Traffic zu skalieren. Datendienste hingegen lassen sich un- gleich schwieriger anpassen, je nachdem wie die Anforderungen an die Datenkon- sistenz aussehen. Da eine Webanwen- dung ihren Zustand in einer Datenbank speichern muss, stößt auch hier die Skalierbarkeit an Grenzen. Die Entscheidung für eine Architektur will daher gut über- legt sein, Kapazitätstests für die Dienste sind zu empfehlen.

CaaS und PaaS können mehr

CaaS und PaaS bieten also eine Reihe von Vorteilen:

- Das Trennen von Entwicklung und Sys- tembetrieb schafft klare Verantwortlich- keiten.
- Fehler lassen sich leichter analysieren, weil keine Snowflake Server im Spiel sind.



Schichtenmodell der Virtualisierung: In einer PaaS-Umgebung müssen sich die Entwickler anders als bei der CaaS-Variante nicht mehr selbst um die Laufzeitumgebung kümmern (Abb. 1).

- Teams arbeiten effizienter, weil Mittelsmänner entfallen.
- Entwickler können die Anwendungen mit Werkzeugen der Hersteller besser handhaben.
- Bei Fehlern ist das Rollback einer Version leichter zu bewerkstelligen.
- CaaS und PaaS sind Türöffner für Testverfahren (Canary Deployments, A/B-Tests, Blue-Green Deployments) [3].
- Das Vorgehen begünstigt Microservice-Architekturen, da das Zusammenstellen von Diensten hier einfacher ist. Denn ohne PaaS ist viel Handarbeit gefordert.
- Dienste lassen sich abhängig von den Anforderungen an die Datenintegrität automatisch skalieren.
- Die Sicherheit erhöht sich, da die Plattform garantiert, dass alle Applikationen die neuesten Sicherheitsupdates verwenden. Bei einer PaaS-Installation geht das sogar bis hin zu den Laufzeitbibliotheken.

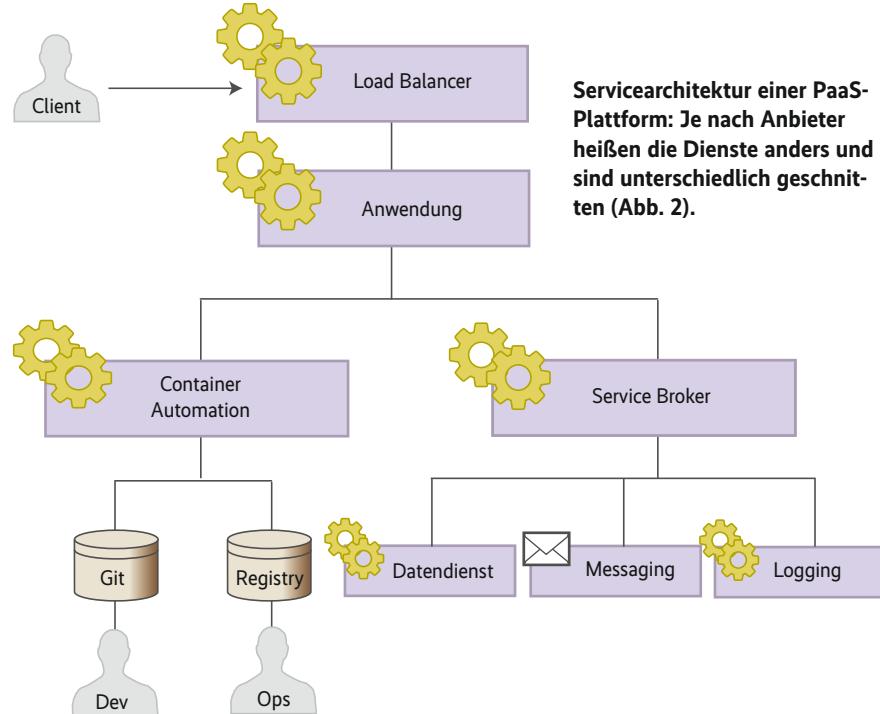
Da man sich irgendwann für eine Variante entscheiden muss, stellt sich die Frage nach den wesentlichen Kriterien. Eine Barebone-Lösung auf Basis von IaaS ist heute aufgrund der wirtschaftlichen und technischen Nachteile nicht mehr vertretbar. Wenn keine guten Argumente für den Eigenbetrieb von Hardware vorliegen (Business Continuity, Compliance et cetera), empfiehlt sich der Einsatz einer externen Plattform. Die lässt sich mit einem motivierten und kompetenten Betriebsteam sogar selbst betreiben.

Als Faustregel kann gelten: Komplexe Architekturen mit vielen beteiligten Teams, geografisch verteilten Microservices, speziellen Datendiensten und aufwendigen Konfigurationen sind mit CaaS besser bedient, weil hier die Kontrollmöglichkeiten vielfältiger sind. Und die Teams können ihre Produktionsworkflows an die hauseigene Kultur anpassen. In diesem Fall ist ein dediziertes Dev-Ops-Team für die Konfiguration der CaaS-Plattform zu empfehlen.

Wer nur ein einfaches System mit wenigen Services und einer überschaubaren Anzahl von Teams umsetzen will, für den bietet PaaS die bessere Alternative, weil sich die Entwicklung hier vereinfachen und automatisieren lässt. Zudem existieren vorgefertigte Plattformdienste.

Kosten im Blick behalten

Es ist möglich, Services auf CaaS und PaaS zu mischen. Ein wichtiger Punkt sind die Kosten. Es empfiehlt sich, eine Gesamtkostenbetrachtung anzustellen und nicht nur die reinen Preise der Container



Servicearchitektur einer PaaS-Plattform: Je nach Anbieter heißen die Dienste anders und sind unterschiedlich geschnitten (Abb. 2).

pro Stunde mit den Hardwarekosten im eigenen Rechenzentrum zu vergleichen. Der Cloud-Anbieter dürfte in der Regel teurer sein; die Ausgaben für die reine Infrastruktur würden also steigen. Ob das System deswegen insgesamt kostspieliger ist, bleibt zu klären.

Denn der Rechnung sollte man die erhöhte Effizienz im Deployment und das Setup neuer Entwicklungsprojekte zuschlagen. Die Personalkosten für Entwickler bleiben hoch, und schon Einsparungen von wenigen Tagen Arbeitszeit können die CaaS-/PaaS-Rechnung ganz anders aussehen lassen.

Es kommt hinzu, dass beim Einsatz von Microservice-Architekturen, bei denen Anwendungen individuell nach Last skaliert werden können, die Ressourceneffizienz sehr hoch sein kann. Gegebenenfalls sinkt also der Bedarf an Maschinen gegenüber der selbst betriebenen Variante.

Wer heute eine neue Architektur entwirft, kommt um Container nicht herum.

Ob nun CaaS oder PaaS für das vorliegende Szenario die bessere Wahl darstellt, ergibt sich aus dem Einzelfall. Dabei kann die Entscheidung pro Service und nicht notwendigerweise pro System ausfallen. Dennoch gibt es auch hier einige Indikatoren, die dem Architekten helfen, die richtige Wahl zu treffen. (jd@ix.de)

Christoph Huber

arbeitet bei der Silberrücken AG in Bern als Servicearchitekt. Seine Arbeitsschwerpunkte sind verteilte Systeme, Cloud- und Geschäftsarchitekturen.

Daniel Takai

arbeitet bei demselben Unternehmen als Unternehmensarchitekt, Autor und Facilitator. Seine Schwerpunkte sind sozio-technische Systeme sowie Cloud- und Geschäftsarchitekturen.

Literatur

- [1] Victor Volle: Automatisierungs-Tools; Werkzeugkiste; Chef, Puppet und Ansible; Developer-Sonderheft Continuous Integration 2016, S. 70
- [2] Erkan Yanar; Clusterverwaltung; Ressourcen fischen; Services mit Kubernetes bereitstellen; iX 2/2017, S. 38
- [3] Daniel Takai, Architektur für Websysteme; Serviceorientierte Architektur, Microservices, Domänengetriebener Entwurf; Hanser Verlag 2017





Vorüberlegungen zum Betrieb eines Security Operations Center

Vorgeschaltete Sicherheit

Tim Cappelmann

IT-Sicherheit kommt ohne vorgelagerte automatisierte Erkennungsprozesse kaum mehr aus. Durchgesetzt haben sich sogenannte Security Operations Center, die man selbst betreiben oder ganz oder teilweise Dienstleistern überlassen kann.

Der Betrieb eines Security Operations Center (SOC) ist eine effektive Möglichkeit, auf die heute zu beobachtenden Cyberangriffe zeitgemäß zu reagieren (siehe Kasten „Was ist ein Security Operations Center?“). Kein IT-System ist frei von ausnutzbaren Fehlern (Exploits). Angriffe aus Schadcode nutzen zudem im Jahr 2018 gern mehrere Angriffsvektoren gleichzeitig. So ist eine sin-

guläre Perimeterabwehrtechnologie nicht mehr in der Lage, die Angriffe verlässlich zu detektieren.

IT-Nutzer reagieren zunehmend, indem sie klassische IT-Security-Disziplinen wie Schadcodescanner, Firewalls, Intrusion Detection (siehe Glossar) et cetera vernetzen. Die Hersteller der Branche implementieren dazu APIs und bilden Ökosysteme für die Interaktion miteinander.

Doch auch bei einer Verbindung dieser „Best-of-Breed“-Technologien wird ein Angriff mittels signaturbasierter Erkennung nicht mehr zum Erfolg führen. Ein Schadcode „überlebt“ im statistischen Mittelwert oft nur Minuten oder Sekunden, bevor er wieder permutiert und für signaturbasierte Scanner bis zum nächsten Update nicht mehr zu erkennen ist.

Die Anatomie der Attacken erfordert es, nicht mehr ausschließlich nach „bekanntem Code“ zu suchen, sondern vielmehr „bekannte Methoden“ im Datenstrom auszumachen. Maschinenbasiertes Lernen, SIEM-Technologien (Security Information and Event Management) und die Erfassung aller Verbindungsdaten an exponierten Punkten im Netzwerk sind die Grundvoraussetzung für eine vollständige Darstellung der aktuellen Lage. Nach den Konzernen passen längst auch Mittelstandsumunternehmen die IT-Security an die neuen Gegebenheiten an.

Keine Chance ohne Sicherheitsexperten

Bereits in der Planung der technologischen Ausrichtung stellt sich die bekannte Frage nach möglichen „Plug-and-Play“-Ansätzen, doch diese bleiben letztlich ein Feigenblatt. Hersteller bewerben Umbrella-Lösungen und SIEM-Systeme gern als wartungsarm – doch die Realität sieht leider anders aus. Denn neben der Systempflege durch Spezialisten benötigt jede Erkennungstechnik auch die Sicherheitsanalysten, die der Arbeitsmarkt heute kaum noch bereithält. Ein Security-Analyst wird aufwendig ausgebildet und kennt seinen Marktwert. Die Hochschullandschaft hat zwar mit entsprechenden Vertiefungsrichtungen der Studiengänge reagiert, der Bedarf an Security-Spezialisten wächst allerdings schneller, als diese ausgebildet werden können.

Die Leitungsebene einer IT-Organisation steht damit vor einer gewichtigen Entscheidung, die noch weit vor der Lösung technischer Toolprobleme zu klären ist: „Make IT oder buy IT?“ Diese Bewertung gehört daher ganz nach oben in jede Entscheidungsvorlage zur Implementierung eines eigenen Security Operations Center. Doch sind die Spielarten tatsächlich so digital? Es lohnt sich immer, zunächst alle zu treffenden Entscheidungen für ein mögliches SOC aufzulisten:

- Wer ist verantwortlich für das SOC?
- Lässt sich die SOC-Mission eindeutig beschreiben?
- Welche Stakeholder gibt es, wie sind die Anforderungen zu priorisieren?

- Welche Möglichkeiten für Incident Response stehen prinzipiell zur Verfügung?

Diese Fragestellungen lassen sich weiter auffächern. Mit einer ausreichenden Detailtiefe kommt hier ein nicht zu unterschätzender Change-Prozess an die Oberfläche, der mindestens eine eindeutige Legitimation durch hohe Führungsebenen der Organisation erfordert (Abbildung 1). Ein klarer Auftrag und Kompetenzregelungen sind die absoluten Mindestanforderungen, bevor ein SOC geplant, budgetiert und in der Organisation verortet werden kann. Ein „SOC-Projekt“ auf der Ebene eines IT-Teams erscheint daher unrealistisch – nicht zuletzt weil strategische Fragestellungen zu klären sind. Doch zurück zu den skizzierten Fragen.

Wer ist verantwortlich für das SOC?

Eine reflexartige Zuschreibung von Zuständigkeiten ist oft zu beobachten. Es geht im SOC doch um Cyber-Security-Themen, also ist dies offenbar ein klarer Fall für die Firewall-Admins. Weit gefehlt! Dieser Schluss ist nicht zwingend, oft genug birgt diese Aufgabenbündelung zusätzliche Herausforderungen. Bei der Beschreibung der SOC-Mission wird dies später verdeutlicht.

Ein SOC sollte idealerweise in einer Stabsstelle der Organisation angesiedelt werden – hier bietet sich beispielsweise das Informationssicherheits- oder das Risikomanagement an. Innerhalb bestehender Governance-Funktionsstellen wird sich eine Heimat für das SOC finden. Ob die eingesetzten Analysten dann disziplinarisch in der IT-Linie arbeiten (der Stabsstelle untergeordnet) oder selbst vollständig als Stab agieren, ist zweitrangig.

Die taktische und strategische Ausrichtung sollte man nicht den Firewall-Admins

Was ist ein Security Operations Center?

Das Security Operations Center (SOC) bezeichnet eine Organisationseinheit, die sich ausschließlich um die Cybersicherheit der IT-Systeme kümmert. Ein SOC setzt sich aus Know-how, Technik und den geeigneten Organisationen zusammen. Meist werden Security-Analysten in einem speziellen Leitstand zusammengezogen, von dem aus sie mit IT-

Sensorik die Security permanent überwachen und steuern. Ein SOC greift bei Sicherheitsverletzungen ein und lenkt die Gegenmaßnahmen. Dabei besitzen die Spezialisten Methodenkenntnisse der Angreifer und verfolgen stets die aktuellen Trends und Sicherheitslücken auf der Suche nach aktuellen „Indicators of Compromise“ (IoC).

überlassen. Zum einen kontrolliert das SOC auch die Regelqualität der Firewalls – dabei steht im Raum, wie einzelne Funktionen voneinander zu trennen sind –, zum anderen werden Daten aus allen IT-Bereichen und gegebenenfalls auch aus dem Business erhoben. Hier scheitert das Firewall-Team voraussichtlich an Hierarchiegrenzen. Welcher Firewall-Admin hat schon Zugriff auf die Virenscanner der Server, auf die Datenbanklogs des ERP-Systems oder gar auf die Cloud-Instanzen? Der Fokus liegt dabei auf mehr Dingen als auf dem reinen Perimeter. Auch ein Verständnis für Gesamtzusammenhänge der kompletten IT-Architektur darf nicht zwangsläufig dem Firewall-Team zugeschrieben werden. Viele Systemspezialisten richten ihre Aufmerksamkeit zu schnell auf die Technologie.

Eindeutiger Zweck eines SOC

An erster Stelle steht die Beschreibung der Mission. Dabei lohnt es sich, über die Details nachzudenken – ein simples Statement „Cyber Security Incidents entdecken“ reicht bei Weitem nicht aus. Die konkrete Beschreibung ist nicht zuletzt deswegen wichtig, weil daraus alle Anforderungen an Technik, Personal und Kompetenzen kausal abgeleitet werden

müssen. Das Topmanagement muss einen konkreten Auftrag an das SOC unterschreiben, denn bei der Interaktion mit den vielen beteiligten Organisationseinheiten sind Widerstände absehbar.

Aus der Mission sind Prozessbeschreibungen abzuleiten. Dabei ist Transparenz zu wahren. Alle Vorfälle müssen in gleicher Weise und in vorgegebenen Rechercheschritten bearbeitet werden. Die Prozeduren sollten auch einer Revision standhalten. Ein SOC sollte Cyber Security Incidents verfolgen und nach Bedarf ein Computer Emergency Response Team (CERT) aktivieren. Die Behandlung der Vorfälle durch Field Services und CERT muss nicht mehr zwingend durch das SOC geschehen. Hier bietet sich bereits eine Übertragung der Zuständigkeiten an.

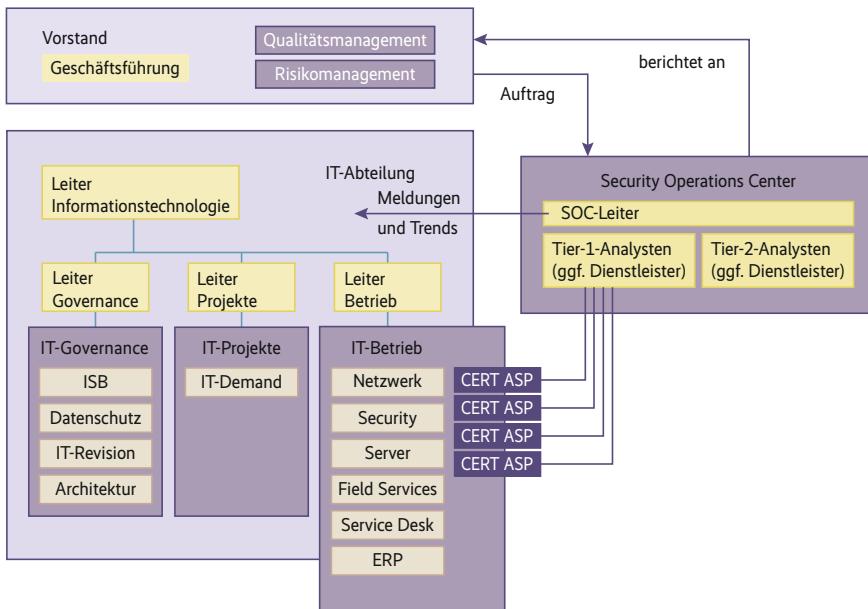
Weiterhin liefert ein SOC Kennzahlen für alle Stakeholder aus dem Bereich Governance, beispielsweise für den Risikomanagementbeauftragten, den Datenschützer, den Informationssicherheitsmanager. Ein SOC hinterfragt permanent die verarbeitete Datenqualität der eigenen Sensorik und justiert diese nach. Alles in allem lässt sich – abgesehen von Katastrophenzenarien – ein SOC als beratende und auch anweisende Organisation beschreiben, weniger als eine Gruppierung der konfigurierenden Systemspezialisten für Perimetersicherheit.

Stakeholder, Anforderungen, Prioritäten

Viele Argumentationen zielen auf das eigene SOC. Compliance-getriebene Organisationsformen werden schnell Kennzahlen und Risikoberichte einfordern. Es besteht die Gefahr, bei den Aufgaben das Augenmerk zu stark auf Reporting-Anforderungen zu richten. Wenn Systemspezialisten ein SOC organisieren, droht hingegen eine Technikschlacht. Administratoren beschaffen in einem solchen Projekt Lieblingssysteme, um eine Waffengleichheit mit den Angreifern herzustellen.



- Die Zeit des reinen Perimeterschutzes und der singulären Sicherheitssysteme ist endgültig vorbei – wer sein Unternehmen vor Cyberangriffen schützen will, kommt um eine vorgelagerte Angriffs- und Datenanalyse nicht herum. Etabliert haben sich sogenannte Security Operations Center.
- Nicht für jedes Unternehmen ist es sinnvoll, ein SOC in Eigenregie zu betreiben. Je nach Größe, Personalsituation, Know-how und weiteren Faktoren lohnt es sich, das „Vorfiltern“ und Interpretieren Security-relevanter Daten auszulagern – auch teilweise.
- Beendet ist ein solches Projekt wie auch die IT-Sicherheit im Allgemeinen nie: Stets gilt es, neue Erkenntnisse und Trends, aber auch Erfahrungen und Gelerntes in den Regelbetrieb einfließen zu lassen.



So sieht die ideale Organisation eines SOC im Unternehmen aus: Die oberste Leitungsebene beauftragt und legitimiert das SOC, das wiederum über die benannten Ansprechpartner (ASP) die relevanten Fachteams steuert. Die CERT-Mitarbeiter müssen dem SOC nicht disziplinarisch unterstehen, es reicht hier die fachliche Steuerung durch das SOC (Abb. 1).

Der Betriebsrat wittert hingegen Leistungskontrolle und bringt Ideen zur Beschränkung allzu umfangreicher Analysen ein. IT-Teams befürchten potenziellen Machtverlust und geben die benötigten Daten „ihrer Systeme“ nicht freiwillig preis. Die mit einem SOC erzeugte Transparenz wird auch nicht von jedem Systembetreuer unterstützt werden. Doch Security-Know-how-Silos sind im Kontext der heutigen Anatomie einer Attacke nicht mehr sinnvoll.

Die Frage nach den beteiligten Interessengruppen ist frühzeitig zu beantworten,

eine klare Priorisierung des SOC-Auftrages sollte neben der Unterschrift einer hohen Leitungsebene helfen. Ohne einen unumstößlichen Auftrag wird ein Querschnittsprojekt wie die Etablierung eines SOC in der Organisation nahezu zwangsläufig scheitern.

Bei der Planung eines SOC muss man sich fragen, welche eigenen Möglichkeiten man hat, auf Security-Vorfälle zu reagieren. Auch wenn ein SOC nicht zwangsläufig die Incident Response übernehmen muss, so sind doch bereits Leitplanken für die benötigten Aufwendungen

des SOC erkennbar. Wieso sollte ein SOC 24×7 arbeiten, wenn die gegebenenfalls benötigten Fachteams für ein Reagieren gar keine Rufbereitschaft bereitstellen? Wenn keine Regelungen zum Umgang mit verdächtigen Netzeilnehmern existieren, wieso sind dann Field Services oder gar Forensiker auszubilden?

Die Anforderungen aus dem Business werden ganz individuell formuliert. Ein produzierendes Unternehmen in der Liniensfertigung wird kompromittierte Systeme nicht abschalten, sondern allenfalls isolieren. Die Entscheidung trifft die Produktion, nicht die IT. Ein Finanzdienstleister wird bei bestätigten Incidents anders reagieren als ein Krankenhausbetreiber. Die denkbaren Varianten der letztlich möglichen Reaktionen geben Hinweise auf ein maßvoll ausgestaltetes SOC.

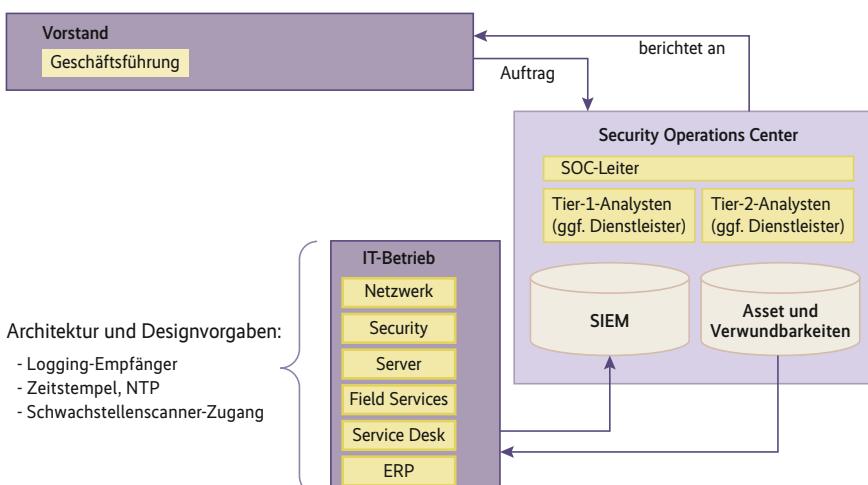
Strategien zum Aufbau

Bei der Implementierung eines SOC wird es vermutlich immer einfacher sein, ein neues Feld zu bestellen, als bestehende Ablauforganisationen nachhaltig zu verändern. Ein SOC benötigt ein klares und unumstößliches Mandat und erhält damit zwangsläufig auch Macht. Ein vormals gleichberechtigtes IT-Team nun mit dem Teilzeitauftrag zum SOC zu erheben, kann deshalb eigentlich nur scheitern. Eine neue Organisationseinheit mit einer Steuerung aus einer Stabsstelle heraus erscheint nach diesen Überlegungen der schnellste und zugleich krisensicherste Weg zum Ziel zu sein.

Die neue Organisation kann auch skalieren – nicht gleich zu Beginn müssen alle Analysten ausgebildet und am Arbeitsmarkt akquiriert sein. Solange IT-Security nicht das Kerngeschäft des Unternehmens ist, kann man den Einsatz von Spezialisten besser per Service Level Agreement sicherstellen. Eine Aufteilung in Tier-1-(Erstanalyse, Nachweis von False Positives) und Tier-2-Analysten (tiefgehende Forensik) kann hier durchaus helfen.

Es gibt einige Argumente für die Fremdvergabe der Tier-1-Analyse an Dienstleister. Mit dem eigenen Know-how weniger Experten im Hause kann die Dienstleisterqualität weiterhin bewertet werden. Dagegen sind Tier-2-Analysten selten am Wochenende oder nachts im Einsatz, dies kann den eigenen Experten zugemutet werden. Das Outtasking für die First Triage erzielt hingegen sofort Skaleneffekte und Spezialisierungsvorteile – und dies nicht erst im Dreischichtbetrieb.

Tier-2-Analysten müssen in ihren Untersuchungen weiterhin potenziell mit in-



Jedes beteiligte IT-System muss zwei Designrichtlinien erfüllen: Zum einen muss es Logs an das SIEM im Verantwortungsbereich des SOC senden, zum anderen werden alle Netzeilnehmer aktiv auf Verwundbarkeiten gescannt. Komplexe technische Verflechtungen mit den jeweils eingesetzten IT-Technologien muss es nicht geben (Abb. 2).

Glossar

voltierten Anwendern in den Dialog treten. Dies ist mit Dienstleistern ohne Stallgeruch schwer zu organisieren. Eigene Kollegen können benötigte Informationen über zu untersuchende Vorgänge auf dem kurzen Dienstweg effizienter zusammentragen, als dies für externe Spezialisten jemals möglich wäre.

Aus einem weiteren Grund eignet sich die Rolle des Tier-2-Analysten weniger gut für eine Besetzung von außen: Hier ist auch das Verständnis des Business vom Analysten gefordert. Nichtsdestotrotz können Abrufkontingente für einen direkten Zugriff auf Tier-2-Analysten oder IT-Forensiker das eigene SOC schnell handlungsfähig machen.

Letzte Vorbereitungen vor dem Start

Wenn die Aufstellung des Teams steht, ob nun mit Hilfe eines Dienstleisters oder ohne, ist organisationsweit eine simple Architekturvorgabe zu machen. Jeder Netzeilnehmer hat dann ab sofort – die Systemzeit zu synchronisieren, – Eventlogs an ein zentrales SIEM zu senden, – zyklisch Schwachstellenscans aus dem SOC über sich ergehen zu lassen. Die Umsetzung dieser wenigen Vorgaben hat Projektcharakter, ist aus der Praxis heraus jedoch nicht sonderlich kompliziert (Abbildung 2). Vorbehalte sind zu bearbeiten, die Umsetzung muss überwacht werden. Im SOC hingegen entsteht nun die eigene und sehr spannende interne Tool-Landschaft, die mindestens aus ei-

nem SIEM und einem Asset-Management-Werkzeug besteht. Ein internes Ticketsystem, ein Betriebslogbuch und viele begleitende Tools sind als verbindliche Werkzeuge im SOC festzuschreiben.

Schriftliche Prozesse und Handlungsanweisungen innerhalb des SOC sorgen für Transparenz, Formulare für Handlungsempfehlungen und Advisories an die IT-Fachteams helfen in der Gleichbehandlung aller Vorfälle. Gesonderte Geheimhaltungsvereinbarungen mit den Mitarbeitern des SOC-Teams sollten bedacht werden. Kennzahlen sind an den Hauptprozessen zu erheben, um Trends zu erkennen und eine langfristige Steuerung der Qualität des Security Operations Center zu gewährleisten. Jede untersuchte Fehlmeldung triggert einen Lernprozess zur Verbesserung der eigenen Effizienz.

Das SOC arbeitet produktiv – und nun?

Nach einer durchlaufenen Lernkurve wird das SOC in einen Regelbetrieb überführt. Doch auch dann ist die Arbeit nicht abgeschlossen. Die SOC-Leitung muss fortwährend darauf achten, dass die Mission geschützt wird. Die Wahrung der Transparenz und der vorhersehbaren Leistung

hilft, Vorbehalte aus zunächst nicht beteiligten Fachteams abzubauen. Eine gewisse Verschwiegenheit und professionelle Kommunikation aller Stakeholder bleibt grade in der Betriebsphase wichtig. Daher ein simpler Ratschlag zum Schluss: Halten Sie sich mit detaillierten PowerPoint-Präsentationen über das eigene SOC lieber zurück. (ur@ix.de)

Dipl.-Ing. Tim Cappelmann, MBA,

ist Leiter Managed Services bei der AirITSystems GmbH.

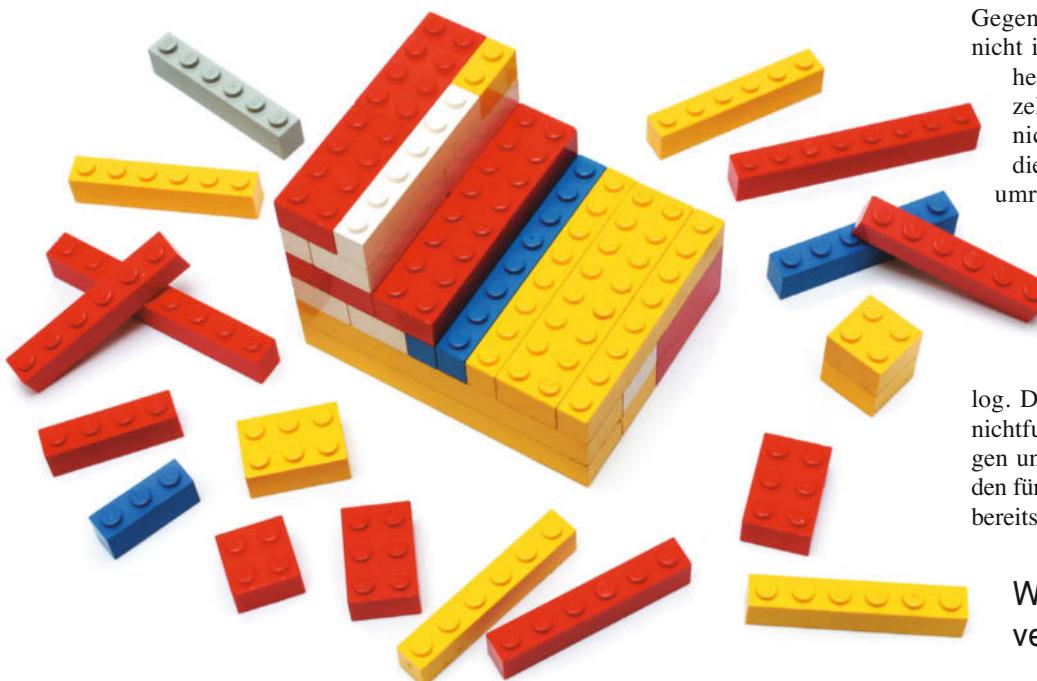


Es gibt 10 Arten von Menschen. iX-Leser und die anderen.

Jetzt Mini-Abo testen: 3 digitale Ausgaben + iX-Kaffeebecher nur 14,10 €
www.iX.de/test

Nichtfunktionale Anforderungen in der agilen Welt

Raus aus der Nische



Juliane Merkel, Maik Wienströer

Produktmanager steuern Projekte über die funktionalen Anforderungen. In vielen agilen Vorgehensmodellen endet hier ihre Verantwortung. Wartbarkeit, Skalierbarkeit und Bedienerfreundlichkeit kommen dabei oft zu kurz.

Wenn es um sogenannte nicht-funktionale Anforderungen geht, denken viele Entwickler vermutlich an DIN-Kriterien wie Zuverlässigkeit, Benutzbarkeit, Änderbarkeit oder an andere abstrakte Begriffe wie Korrektheit und Skalierbarkeit. Diese Schlagworte benötigen jedoch dringend einen Transfer in die Praxis. Skalierbarkeit gerät zum Beispiel schnell zu einem Nebenschauplatz, wenn der Kunde eine fest definierte Umgebung hat und deren

Erweiterung ausschließt (etwa bei Maschinенsoftware).

Aussagen wie „Verschlüsselung von Datenströmen“ oder „angemessene Reaktionszeiten für Klickereignisse“ liefern bereits Hinweise für Anforderungen, sind jedoch zu unkonkret. Präzise wäre „Verschlüsselung aller Datenströme mit dem SHA-256-Algorithmus“ oder „Reaktionszeiten für Klickereignisse müssen unter einer Sekunde liegen“. Diese Beispiele zeigen eine wesentliche Eigenschaft nicht-

funktionaler Anforderungen: Sie bilden den Rahmen des Projekts. Der Produktmanager muss nun dafür sorgen, dass die Entwickler die klar formulierten Wünsche in die Software einbauen.

Es liegt nahe, sie im Product Backlog zu erfassen, das schon die funktionalen Anforderungen enthält. Aus den dort gesammelten Einträgen lassen sich Entwicklungsaufträge mit einer Komplexitätsabschätzung ableiten, auf der die spätere Umsetzung beruht. Nichtfunktionale Anforderungen verlangen nach permanenter Beachtung und lassen sich, im Gegensatz zur funktionalen Variante, nicht in einem Rutsch fertigstellen. Daher ist ihre Abbildung in Form einzelner Einträge im Product Backlog nicht sinnvoll. Da sie in der Regel die Grundannahmen für das Produkt umreißen, sind sie vertragsrelevant.

Sie klar und kontinuierlich zu beschreiben und zu verwalten, ist daher unumgänglich. Es empfiehlt sich das Anlegen einer zentralen Dokumentation außerhalb des Backlog. Dort kann der Produktmanager die nichtfunktionalen Anforderungen eintragen und sie dem Team sowie dem Kunden für Kommentare und Rückmeldungen bereitstellen.

Wünsche miteinander verbinden

Wie lassen sich nun die nichtfunktionalen mit den funktionalen Anforderungen, die etwa als User Stories erfasst sind, verbinden? Da erstere sehr unterschiedlich geartet sein können, gibt es mehrere Möglichkeiten. Beispielhaft könnte eine Anforderung wie folgt lauten: „Nach dem Login soll der Kunde mit maximal zwei Klicks die letzte Version der Vertriebsstatistik aufrufen können.“ Hier ist die Nähe zur Vertriebsstatistik und damit eine enge Verbindung zur funktionalen Anforderung (Vertriebsstatistik erstellen) erkennbar. In diesem Fall bietet es sich an, die notwendigen Voraussetzungen als Akzeptanzkriterien in die funktionale Anforderung zu integrieren. Die dauerhafte Umsetzung könnte ein automatisierter Test begleiten, der wiederum in der Definition of Done verankert wird (DoD, Liste von Kriterien, die eine Anforderung erfüllen muss, um als erledigt zu gelten).

Aus Sicht des Produktmanagements ist die Anforderung einfach zu verwalten, da zu keinem Zeitpunkt Prioritäten für die verschiedenen Anforderungsarten ver-

Verknüpfen nichtfunktionaler Anforderungen

Benutzbarkeit	Dokumentation	Status	letzte Änderung
Nach dem Login soll der Kunde mit maximal zwei Klicks das letzte Update seines wichtigsten Berichts aufrufen können.	- funktional umgesetzt in Sprint KW3 im Rahmen der Login User Story - laufend getestet in jeder App-Release via GUI-Test-Login	erfüllt ab Version 1.0	15.04.2018
Die Software soll dem firmenweiten Styleguide genügen.	Logo-Position, Typografieregeln und Farbmanagement definiert im Rahmen der Design-Story „Basis-Design“	Spezifikation abgeschlossen, Umsetzung geplant ab Version 1.1	17.04.2018
Die Software soll native User Experience für iOS und Android bereitstellen.	Mockups für iOS werden derzeit begutachtet in Team Apple „Ticket-ID“.	Spezifikation läuft	10.04.2018
Die Software soll Berichte für alle gängigen mobilen Endgeräte im responsive Design anzeigen.	- Definition von Geräteklassen nach Displaygröße - verwendet in Design-Story Berichtslayout - verwendet in DOD GUI-Tests	erfüllt ab Version 1.0	16.04.2018

geben werden müssen, sondern das Ganze ein Paket bildet.

Wenn eine nichtfunktionale Anforderung produkt- und/oder projektübergreifenden Kriterien genügen muss, sieht die Sache etwas anders aus. Beispiel: „Die Software soll dem firmenweiten Styleguide genügen“. Eine Verfolgung des vorherigen Plans würde bedeuten, die Konformität mit dem Styleguide im Kontext jeder funktionalen Anforderung zu interpretieren und zu dokumentieren, was enorm aufwendig und redundant wäre. Erschwerend käme hinzu, dass das Aktualisieren des Styleguides aufgrund der Neubetrachtung aller Anforderungen kaum möglich wäre.

Die naheliegende Alternative besteht darin, eine eigene User Story für die nichtfunktionale Anforderung zu erzeugen, die Vorrang genießt. Die agile Literatur rät von diesem Vorgehen jedoch ab, da aus dieser Anforderung kein direkter Vorteil in Form einer Funktionserweiterung für den Kunden erwächst. Zu beachten ist, dass nichtfunktionale Anforderungen nicht selten eine Art Hygiene-funktion ausüben und das System oft erst durch ihre Integration eine gute „User Experience“ aufweist. Der Produktmanager muss daher den Kunden für diese Anforderungen sensibilisieren und um seine Akzeptanz werben.

In der Praxis wäre der nächste Schritt, den vorliegenden Styleguide zu analysieren, um daraus den Aufbau der Software grafisch abzuleiten. Er bildet die Grundlage für alle weiteren Funktionswünsche. Die Erfassung als User Story ist anders als die Integration in alle funktionalen Anforderungen deutlich effizienter und daher zu bevorzugen. Nachgelagerte Aufgaben wie Dokumentation und Nachverfolgung gestalten sich ebenfalls deutlich einfacher.

Ob eine nichtfunktionale Anforderung als Bestandteil der Definition of Done oder als eigene User Story erfasst wer-

den soll, lässt sich nicht pauschal beantworten. Vielmehr ergibt sich eine qualifizierte Beurteilung oft erst im Alltag. Häufig stellen sich dabei vermeintlich kleine Anforderungen bei genauerer Betrachtung als komplexe und umfangreiche Strukturen heraus.

Nachvollziehbar durch Versionierung

Bei der Dokumentation ist es wichtig, dass man die Anforderungen nicht direkt ändert, sondern immer eine neue Version anlegt. Durch die Versionierung lässt sich der Werdegang nachvollziehen. Eventuelle Einflüsse und zugrunde liegende Annahmen kann man dann auch später noch verstehen.

Die meisten Anforderungen verschwinden in den Tiefen des Backlogs, sobald sie erfüllt sind. Solche wie der genannte Styleguide werden zwar initial interpretiert, müssen jedoch fortlaufend überwacht und bei jeder Erweiterung geprüft werden. Um eine kontinuierliche Begleitung der Anforderungen zu ermöglichen, müssen die Verantwortlichen sie zunächst mit den zugehörigen Dokumenten in eine Tabelle schreiben. Ergänzend empfiehlt es sich, die in Akzeptanzkriterien oder anderweitig erfassten Anforderungen ebenfalls aufzunehmen und mit dem entsprechenden Eintrag im Backlog zu verknüpfen. Dadurch erhält der Produktmanager eine Übersicht über den jeweiligen Erfüllungsgrad und kann bei Rückfragen des Kunden oder nachträglichen Änderungswünschen schnell reagieren.

Die Tabelle zeigt eine minimalistische Form des Verknüpfens nichtfunktionaler Anforderungen und ihrer Umsetzung im Rahmen einer zentralen Dokumentation. Das Beispiel enthält alle Anforderungen zum Benutzen der entstehenden Software. Mit der eigentlichen Anforderung

sind Quelldokumente, etwa ein Styleguide, aber auch Verweise zur Spezifikation und Umsetzung zusammengeführt. Eine chronologische Sammlung bietet dabei die Möglichkeit, den Ursprung und die Entwicklung jeder einzelnen Anforderung nachzuvollziehen. Hier werden überwiegend Links genutzt. Das Beispiel zeigt, dass einige Anforderungen im späteren Prozess neu interpretiert und dadurch im regulären Lebenszyklus begleitet werden müssen.

Auf den ersten Blick scheint dieses Vorgehen aufwendig. Bei genauerer Betrachtung entsteht jedoch die Basis für eine nachhaltige Produktentwicklung, was auch eine bessere Akzeptanz bei den Kunden bewirkt.

Die Kunst des agilen Projektleiters oder Produktmanagers besteht darin, schon während der Anforderungsaufnahme die wesentlichen Eigenschaften einer Software sowie eventuelle spätere Begehrlichkeiten zu erkennen und zu berücksichtigen. Auch das Team steht in der Verantwortung und muss sich vom ausschließlichen Fokus auf die technischen Funktionen lösen. Wer eine nachhaltige Produktentwicklung etablieren möchte, muss die nichtfunktionalen Anforderungen aus ihrem Nischendasein befreien. (jd@ix.de)

Juliane Merkel

ist Product Owner bei ip.labs (FUJIFILM Group) in Bonn. Sie arbeitet seit fünf Jahren als Produktmanager in der agilen Softwareentwicklung.

Maik Wienströer

ist freiberuflich mit seinem Unternehmen IT meets People im Bereich der sozialen Verbindung von IT und Business zur Steigerung der unternehmerischen Effizienz tätig (www.it-meets-people.de).



Künstliche Intelligenz im Datenschutzfokus

Datenautomat



Tobias Haar

Künstliche Intelligenz braucht viele Daten für ihre Analysen. Das kollidiert häufig mit dem Datenschutz, insbesondere der Datenschutz-Grundverordnung. Es kommt aber immer auf die Ausgestaltung im Einzelfall an.

Mit der Datenschutz-Grundverordnung (DSGVO) hat der EU-Gesetzgeber auf die Veränderungen beim Umgang mit personenbezogenen Daten seit 1995 reagiert und die damals verabschiedete Datenschutz-Richtlinie ersetzt. Dort, wo ihnen die DSGVO einen Spielraum gelassen hat, haben die nationalen Gesetzgeber nachgezogen und ihre jeweiligen Datenschutzgesetze angepasst. Nur wenige Monate nach Inkrafttreten beschäftigt das neue Datenschutzregime immer noch Scharen von Juristen, IT-Fachleuten, Geschäftsführern und schließlich die Aufsichtsbehörden. Vieles ist weiterhin unklar und wird erst im Laufe der Zeit, womöglich erst nach Jahren, abschließend geklärt werden. Im Zweifel müssen auch hier die Gerichte und nicht zuletzt der Europäische Gerichtshof entscheiden.

Eines dieser zunehmend kontrovers diskutierten Themen ist das Zusammenspiel zwischen dem, was man landläufig unter künstlicher Intelligenz versteht, und dem Datenschutzrecht. „Müssen sich Unternehmen in ihre Algorithmen schauen lassen?“ oder „Künstliche Intelligenz – Die Risiken für den Datenschutz“ lauten nur zwei Überschriften von Onlineartikeln zu diesem Thema. Wie immer kommt es zum einen darauf an, ob verarbeitete Daten tatsächlich einen Personenbezug haben, und zum anderen, wer sie wie und für welchen Zweck erhebt und verarbeitet.

Für das Datenschutzrecht spielt es keine Rolle, ob neue Technologien und Geschäftsmodelle unter der Bezeichnung „künstliche Intelligenz“ oder anderen Schlagwörtern diskutiert werden. Diesen Begriffen kommt juristisch keine Bedeu-

tung zu, da sie (noch) nicht gesetzlich definiert sind. Es gilt der juristische Grundsatz, dass es nicht darauf ankommt, was auf der Verpackung einer Technologie draufsteht, sondern was im Detail in ihr enthalten ist.

Wenn allerdings künstliche Intelligenz oder ihr Teilbereich Deep Learning auf Big-Data-Analysen beruhen, ist der Datenschutz nicht weit. Es geht stets um große Mengen an Daten, die zu bestimmten Erkenntnisse führen sollen – sei es für von Menschen gesteuerte Anwendungen oder um „intelligente Maschinen“ in die Lage zu versetzen, eigenständig Entscheidungen in bestimmten Bereichen zu treffen. Selbst auf den ersten Blick reine Maschinendaten können einen Personenbezug haben, wenn man von ihnen womöglich auf die die Maschinen bedienenden Menschen oder die hinter einer Produktion stehenden Kunden schließen kann.

Gibt es noch Daten ohne Personenbezug?

Datenschutzrechtler fassen personenbezogene Daten sehr weit. Aus diesem Grund sind dynamische IP-Adressen mit zugehörigem Zeitstempel als personenbezogene Daten einzustufen. Erst recht gilt das für IPv6-Adressen. Da meist ein rein objektiver Datenbegriff verwendet wird, sprechen manche bereits davon, dass es angesichts der heutigen technischen Möglichkeiten gar keine nicht personenbezogenen Daten mehr geben kann, denn jedes Datum könnte mit anderen Daten kombiniert auf eine Person schließen lassen. Der objektive Datenbegriff bedeutet, dass ein Personenbezug auch dann vorliegt – und damit das Datenschutzrecht greift –, wenn irgendjemand aus einem Datum auf eine Person schließen kann. Ob der jeweilige Datenverarbeiter das kann, spielt danach keine Rolle.

Datenschutzrechtliche Probleme im Bereich künstlicher Intelligenz ergeben sich beispielsweise aus Artikel 22 DSGVO. Dieser räumt den Betroffenen, um deren personenbezogene Daten es geht, das Recht ein, „nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden“, die ihnen gegenüber „rechtschaffene Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“. KI-Anwendungen, die diese Wirkungen haben, sind mit Personendaten nur zulässig, wenn sie Gegenstand eines Vertrages oder einer Einwilligung sind, die den da-

tenschutzrechtlichen Vorgaben an Transparenz und Aufklärung genügen.

Hintergrund dafür ist, dass ein Mensch nicht bloßes Objekt maschinel-ler Entscheidungen sein darf. Dies folgt zudem aus Artikel 1 des Grundgesetzes, der die Menschenwürde verfassungs-rechtlich schützt. Zudem dürfen selbst bei vorliegender Einwilligung biometri- sche oder andere „besondere Kategorien personenbezogener Daten“ nicht für rein automatisierte Entscheidungen verwen-det werden.

Teils mit, teils ohne Mensch

Heutige KI-Anwendungen sind zudem oft noch nicht so weit, „ausschließlich“ automatisierte Entscheidungen zu treffen. Wird beispielsweise beim Einsatz von Kreditkarten oder im Onlinebanking von Dienstleistern KI eingesetzt, um betrügerisches Verhalten aufzudecken, entschei-den letztlich oft noch Menschen unter Abwägung weiterer Faktoren. Dass es aber auch schon vollautomatisierte Ent-scheidungsverfahren gibt, ist klar. On-linebanken ermitteln mitunter automa-

tisch den Zinssatz für ein Darlehen an-hand des konkreten Profils desjenigen, der es benötigt.

Christopher Millard, Professor für Da-tenschutz- und Informationsrecht an der Queen Mary University in London, for-dert eine vorherige Risikofolgenabschät-zung [1], wenn auf Algorithmen basieren-de Systeme zur Analyse menschlichen Verhaltens eingesetzt werden. Dies wäre beispielsweise beim Scoring zur Boni-tätsprüfung erforderlich, für das zusätz-liche datenschutzrechtliche Vorschriften exis-tieren. Erst recht gilt dies für Anwen-dungsfälle wie „Predictive Policing“ zur Berech-nung der Wahrscheinlichkeit zu-künftiger Straftaten. In diesem Bereich dürfte neben der DSGVO auch das jewei-lige Polizei-, Ordnungs- und Strafrecht relevant sein. Das Beispiel der Risikobe-wertung bei Kreditkarteneinsätzen zeigt aber, dass KI-basierte „Predictive Fraud Prevention“ (Betugsvermeidung durch Vorhersage) auch im privaten Sektor zunehmend eine Rolle spielt.

Ein Problem stellt sich allerdings bei der Risikofolgenabschätzung im KI-Be-reich: KI-Systeme sollen selbstlernend sein und aus den jeweils neuen Erkennt-

nissen „eigene“ Entscheidungen oder Entscheidungsvorschläge ableiten. Das ist bei der Risikofolgenabschätzung nach der DSGVO deswegen zu berücksichti-gen, weil sich durch KI die Folgen der Datenverarbeitung für die Betroffenen mit der Zeit ändern können. Dann aller-dings fordert das Gesetz eine erneute Ri-sikofolgenabschätzung, um den geänder-ten Rahmenbedingungen Rechnung zu tragen. Wie kurz die Intervalle zwischen zwei Abschätzungen aufgrund geänderter Risikolage sein sollen, bedarf wiederum einer Entscheidung im Einzelfall.

Das Aufklärungs- und Transparenz-gebot im Datenschutzrecht findet aber dort seine Grenze, wo Betriebs- und Ge-schäftsgeheimnisse eines Unternehmens betroffen sind. Dass auch der Gesetzgeber Unternehmensgeheimnisse umfassend schützen will, zeigt sich in der 2016 in Kraft getretenen „EU-Geheimnisschutz-Richtlinie“, die derzeit von den EU-Mit-gliedsstaaten umgesetzt wird.

Der Bundesgerichtshof hat im Jahr 2014 noch unter der alten Rechtslage entschieden, dass die Schufa ihre soge-nannte Scoreformel für die Bonitätsein-schätzungen nicht offenlegen muss (Az.

SECURITY DIALOGUE

THREAT HUNTING & INCIDENT RESPONSE Effektive Abwehr von IT-Sicherheitsbedrohungen

14. Oktober, InterContinental Frankfurt

JETZT
ANMELDEN

In diesem Roundtable diskutieren wir mit Ihnen über aktuelle Fragestellungen zum Thema „IT-Sicherheitsbedrohungen“. Folgende Themen ergänzen den gemeinsamen Dialog:

Eindämmung von Cyber-Gefahren

Threat-Hunting-Services

Untersuchung eines Vorfalls durch das SpiderLabs DFIR-Team

Partner



Organisiert von



VI ZR 156/13). Im Rahmen des datenschutzrechtlichen Auskunftsrechts muss das Daten verarbeitende Unternehmen nicht angeben, welche „allgemeinen Rechengrößen, wie etwa die herangezogenen statistischen Werte, die Gewichtung einzelner Berechnungselemente bei der Ermittlung des Wahrscheinlichkeitswerts und die Bildung etwaiger Vergleichsgruppen als Grundlage der Scorekarten“ es verwendet. Es besteht kein Anspruch auf Mitteilung der „abstrakten Methode der Scorewertberechnung“, heißt es im Leitsatz der Entscheidung.

Für den Einsatz „geheimer“ KI-Methoden dürfte nichts anderes gelten, denn die DSGVO ist auch verfassungsrechtlich auszulegen und die Verfassung schützt Unternehmen und ihre Betriebs- und Geschäftsgeheimnisse, was bei der Abwägung zu berücksichtigen ist.

Transparenzgebot versus Geschäftsgeheimnis

Problematisch ist es auch, wenn Unternehmen sich künstliche Intelligenz von Dritten einkaufen, beispielsweise Watson von IBM. Manche sprechen hier von einer „Blackbox-KI“, da die Verfahren und Algorithmen nicht nur dem Betroffenen, sondern dann auch dem Verwender im Detail unbekannt sind. Dennoch muss der KI-Verwender aussagekräftige Informationen über die eingesetzte Logik offenlegen, und das in klarer und verständlicher Sprache. Die Transparenzvorschriften in den Artikeln 13 ff. DSGVO betreffen unter Strich nicht einseitig den Datenverwender, sondern gehen davon aus, dass im Einzelfall ein angemessener Ausgleich zwischen den widerstreitenden Interessen des Verbrauchers und seinem Recht auf „faire und transparente Verarbeitung“ und denen des Verantwortlichen gefunden werden muss.

Der Anspruch endet zudem dort, wo er mit einem „unverhältnismäßigen Aufwand“ verbunden wäre und wenn durch eine Datenauskunft die „Rechte und Freiheiten anderer Personen“ beeinträchtigt werden. Wie so oft in der Juristerei kommt es also auf den konkreten Einzelfall an. Allerdings sollten sich KI-Anwender frühzeitig Gedanken darüber machen, welche Informationen sie den Betroffenen zur Verfügung stellen müssen, und sich eine gute Argumentation zurechtlegen, wenn sie Details der dahinterliegenden KI nicht offenbaren wollen.

Auch andere Datenschutzgrundsätze sind auf den ersten Blick „KI-inkompatibel“. Der Grundsatz der Datensparsamkeit

und Datenminimierung läuft Big-Data-Ansätzen zuwider, bei denen mehr Daten immer besser sind. Zudem fordert die DSGVO in Artikel 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in Systemen, also Privacy by Default durch geeignete technische und organisatorische Maßnahmen.

Kritisch zu sehen ist in diesem Zusammenhang auch das in die DSGVO aufgenommene Diskriminierungsverbot und das Gebot zur Zweckbindung von Daten. Daten dürfen gemäß Artikel 6 DSGVO nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Soll eine Zweckänderung erfolgen, muss der Betroffene darin einwilligen, es sei denn, eine Rechtsvorschrift erlaubt diese Zweckänderung. Letztlich soll der Betroffene bei einer Zweckänderung so behandelt werden wie bei der erstmaligen Datenerhebung – er soll transparent aufgeklärt in die Datenverarbeitung einwilligen können.

Für diese Hürden sind derzeit einige Ansätze in der Diskussion, wie man den KI-Einsatz datenschutzkonform ausgestalten kann. Apple beispielsweise hat den Crowdsourcing-Ansatz ins Spiel gebracht. Entwickler und andere Verwender von mittels KI verarbeiteten Daten sollen nur Datensätze bezogen auf bestimmte Kohorten erhalten, daraus aber keine Rückschlüsse auf Einzelpersonen ziehen können. Auf einer Apple-Supportseite heißt es hierzu: „Die von Apple erfassten Crowdsourcing-Daten werden in einer Form gesammelt, die keinerlei Rückschlüsse auf deine Person zulässt.“ Apple verwendet danach die Informationen von vielen Geräten für seine Ortungsdienste, den Aufbau einer Datenbank für den Straßenverkehr, aber auch für Marketingzwecke et cetera.

Mehr Anonymität – weniger Aussagekraft

Letztlich geht dieser Ansatz in die Richtung der „Differential Privacy“. Wikipedia schreibt: „Differential Privacy (engl. für „differentielle Privatsphäre“) hat das Ziel, die Genauigkeit von Antworten zu Anfragen an Datenbanken zu maximieren, unter Minimierung der Wahrscheinlichkeit, die zur Beantwortung verwendeten Datensätze identifizieren zu können. [...] Mechanismen, die Differential Privacy erfüllen, verhindern, dass Angreifer unterscheiden können, ob eine bestimmte Person in einer Datenbank enthalten ist oder nicht.“

Die zugrunde liegenden Mechanismen umfassen etwa das Hinzufügen von Dantummays, einem „Rauschen“, um die

genaue Herkunft von Daten – und damit deren Personenbezug – zu verschleieren. Dass hierdurch letztlich aber auch die Qualität der Datenbank beeinträchtigt und die Aussagekraft der darauf basierenden KI-Ergebnisse geschwächt wird, liegt auf der Hand.

Mit der „k-Anonymität“ hat Harvard-Professor Latanya Sweeney 2002 ein Modell entwickelt, das einer Datenbank mit personenbezogenen Daten den Personenbezug nehmen und so das Datenschutzrecht ausschließen soll. Allerdings gilt dieses Modell nicht als sicher, da bei Vorliegen von Zusatzinformationen zu einzelnen Personen oftmals ein Rückschluss auf die in der Datenbank zu dieser Person gespeicherten Informationen möglich ist. Nach dem Datenschutzrecht reicht dies also nicht aus, um ein Datum zu anonymisieren. Bei ausreichend großen Datenmengen und entsprechend komplexer Generalisierung der einzelnen Informationen könnte dies aber im Einzelfall genügen.

Fazit

Der Einsatz künstlicher Intelligenz wirft zahlreiche juristische Fragen auf. Neben Haftungs- und Ethikaspekten ist hier das Datenschutzrecht zu nennen. Und die Gemengelage zwischen KI und dem Datenschutz wird weiter am Brisanz gewinnen. Es gibt Forderungen nach einer gesetzlichen Begrenzung der Verwendung von Erkenntnissen aus KI-Anwendungen.

Soll etwa bei vorliegender Einwilligung eine Verhaltensanalyse oder Krankheitserkennung für Versicherungen erlaubt sein? Darf es Predictive Policing geben, um Straftaten zu vermuten, bevor sie begangen wurden? Die meisten KI-Anwendungen werden aber voraussichtlich zulässig bleiben. Wie der Datenschutz eingehalten werden kann, muss jedoch im Zweifel anhand des Einzelfalls beurteilt werden – am besten in der Zusammenarbeit zwischen Fachleuten aus den Bereichen IT und Recht. Auch eine Anfrage bei den zuständigen Aufsichtsbehörden kommt in Betracht. (ur@ix.de)

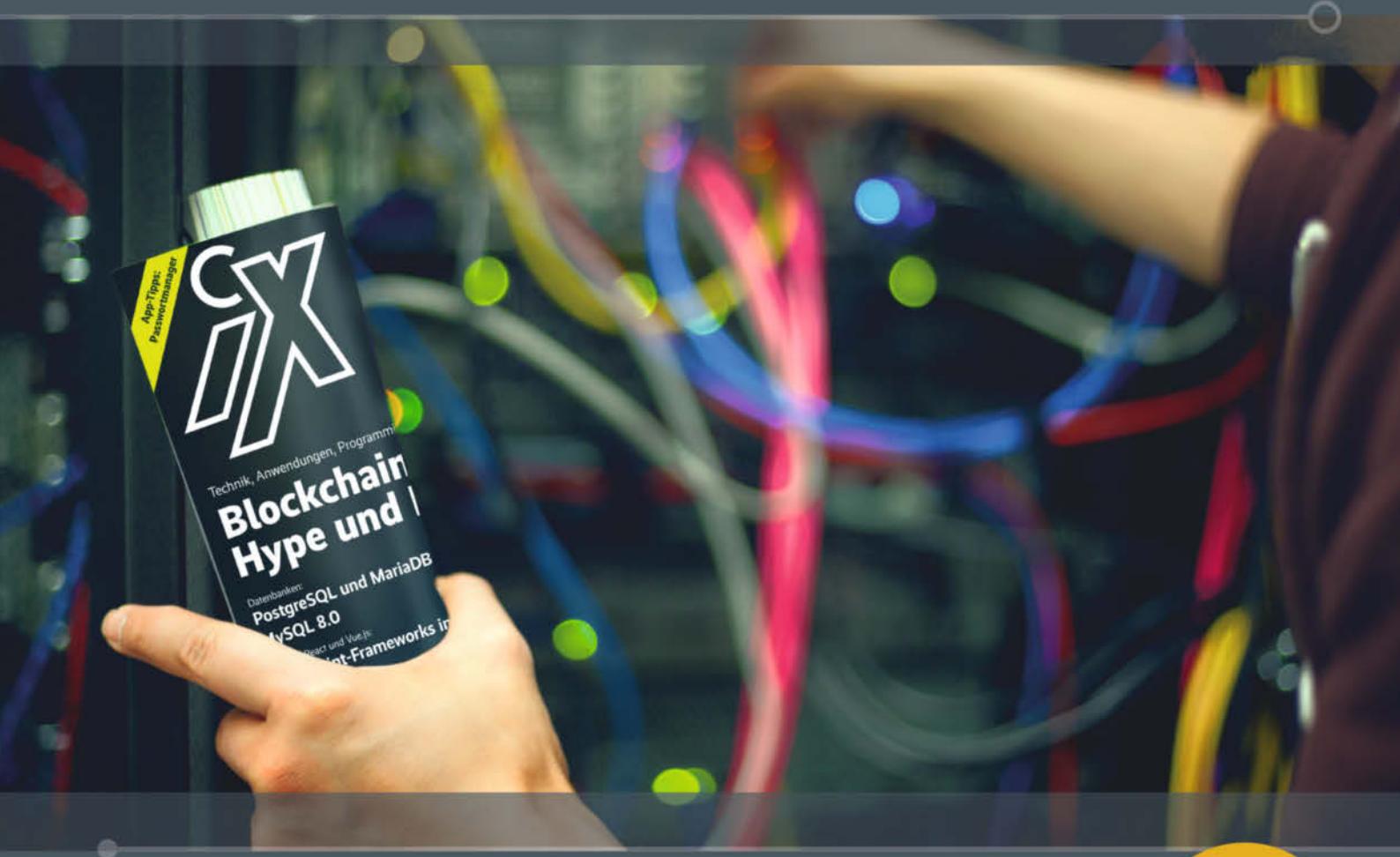
Tobias Haar, LL.M. (Rechtsinformatik), MBA,

ist Rechtsanwalt bei Vogel & Partner in Karlsruhe.

[1] Tobias Haar; DSGVO II; Folgenreich; Risikofolgenabschätzung nach der Datenschutz-Grundverordnung; iX 9/2018, S. 46



Es gibt **10** Arten von Menschen. iX-Leser und die anderen.



Jetzt Mini-Abo testen:
3 Hefte + iX-Kaffebecher
nur 14,70 €

www.iX.de/test



3 x als
Heft



www.iX.de/test



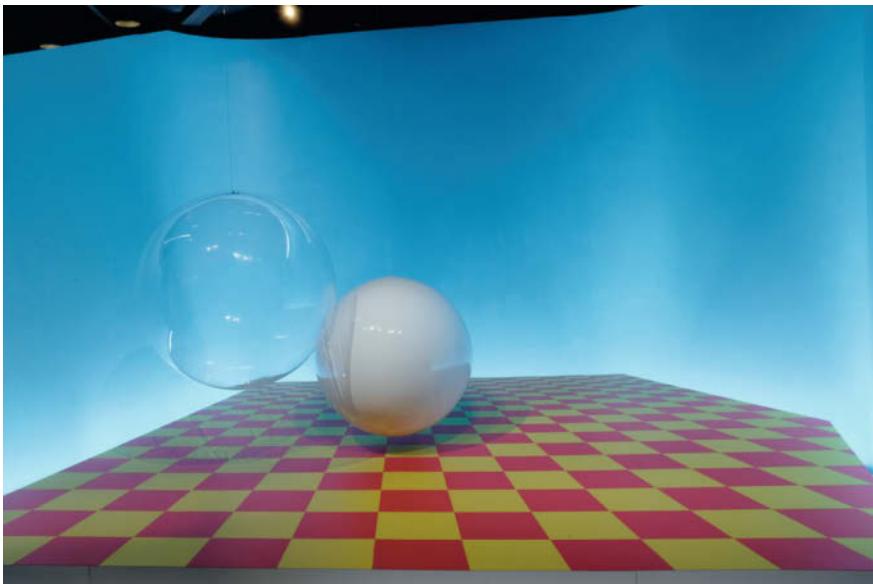
49 (0)541 800 09 120



leserservice@heise.de



MAGAZIN FÜR PROFESSIONELLE
INFORMATIONSTECHNIK



SIGGRAPH 2018: Die Zukunft digitaler Welten

Relative Realität

Paul Grimm

Lag in den letzten Jahren der Schwerpunkt der Computergrafik oft auf der Optimierung einzelner Techniken, so stehen jetzt künstliche Intelligenz und die virtuelle und erweiterte Realität im Fokus.

Eine Frage wie „Is it real what I see?“ wird nicht nur auf Konferenzen wie der diesjährigen SIGGRAPH gestellt. In Zeiten der Fake News dürfen sich das jeder immer öfter fragen. Schon die heutigen Möglichkeiten zum Erzeugen und Verändern realistisch wirkender Fotos und Videos mit künstlichen Inhalten sind überzeugend.

Viele der Entwicklungen, die Wissenschaftler dieses Jahr auf der SIGGRAPH in Vancouver vorgestellt haben, sind heute leicht verfügbar und weit verbreitet. Umso mehr werden alle Nutzer in den nächsten Jahren die Verlässlichkeit von Medieninhalten hinterfragen müssen. In dem für die Konferenz neuen Format „The Future is waiting“ hat man rückblickend betrachtet, was vor fünf oder zehn Jahren für heute erwartet wurde – unter anderem Fake News – und welche Schlüsse man daraus für die Entwicklungen der nächsten Jahre ziehen kann. Bei-

spielsweise steht zu erwarten, dass das Volumen ergänzender Daten für Fotos und Videos deutlich steigen wird.

Neuronale Netze in allen Bereichen

Der Einsatz von Methoden der künstlichen Intelligenz (KI) und insbesondere der neuronaler Netze hat endgültig den Bereich der Grafik und Interaktion erreicht. Ob Bildanalyse, Simulation oder Geometrieverarbeitung, Techniken des Deep Learning auf der Basis von Convolutional Neural Networks (CNN) stellen heute ein übliches Arbeitsmittel dar, das sich in fast allen Anwendungsbereichen als nützlich erweist.

Die Herausforderungen liegen insbesondere im Bereich der Trainingsdatenerstellung sowie in der Übertragbarkeit auf andere Themengebiete. Die Khronos

Group, bekannt durch die von ihr definierten Standards wie OpenGL, Vulkan oder OpenXR, hat für den Austausch trainierter neuronaler Netze das Format NNEF (Neural Network Exchange Format) spezifiziert und kürzlich die Version 1.0 vorgestellt (siehe *iX* 9/2018, S. 26).

Computer Graphics Reinvented

Seit etwa zehn Jahren versuchen Grafikspezialisten, die Darstellung von Bildern (Rendering) zu verbessern, um das Ergebnis realitätsnäher zu gestalten. Dabei simulieren sie die Ausbreitung aller Lichtstrahlen (Raytracing). In der Realität können alle Objekte mit allen anderen Objekten in Bezug auf die Verdeckung und Lichtausbreitung interagieren, etwa indem ein Gegenstand einen anderen verdeckt oder einen Schatten auf einen anderen wirft. Denkbar ist auch, dass ein Objekt von indirektem, also von einer Oberfläche reflektiertem Licht beleuchtet wird. Solche Situationen treten beispielsweise auf, wenn man unter einem Baum steht oder sich tagsüber in einem Raum ohne direkten Sichtkontakt zur Sonne befindet. Raytracing erlaubt das Nachbilden all dieser Effekte und Einflüsse.

Im Bereich der Echtzeitgrafik war es dagegen üblich, nur die direkte Interaktion von Lichtquellen mit einzelnen Objekten zu betrachten. Mit Shader-Techniken lassen sich zudem einzelne Effekte wie Schattenwurf oder Reflexionen umsetzen, wie sie etwa auf Wasseroberflächen erscheinen. Raytracing kann den Entwicklungsaufwand neuer Software deutlich verringern und gleichzeitig die visuelle Qualität verbessern. Eines der ersten mit rekursivem Raytracing berechneten Bilder hat Turner Whitted 1980 erzeugt. Es zeigt eine Szene mit einer spiegelnden und einer transparenten Kugel. In Anlehnung daran hat NVIDIA diese Szene auf der SIGGRAPH in einer begehbarer Installation nachgebaut (siehe Aufmacher).

Den Durchbruch haben die kontinuierliche Verbesserung der Shader-Hardware und die wachsende Leistungsfähigkeit neuronaler Netze zur Rauschreduzierung gebracht. NVIDIA hat dafür vier Einheiten in seine neue Raytracing-GPU integriert: den Tensor-Core zur Berechnung der neuronalen Netze, den RT-Core für das Raytracing sowie den Shader und den Compute-Bereich, der einer Weiterentwicklung bisheriger Grafikkarten entspricht (Näheres zur Spezifikation der Quadro RTX siehe *iX* 9/2018, S. 20).

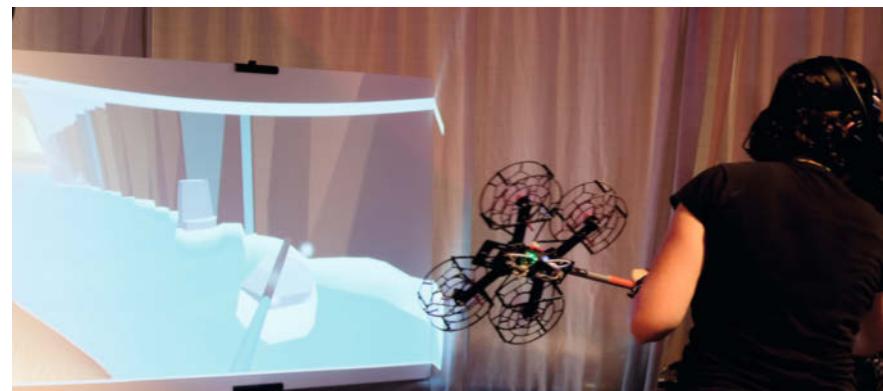
Eins der vielen Highlights der SIGGRAPH sind die Emerging Technologies, die zukunftsweisende Arbeiten zum Anfassen vorstellen. Unter anderem konnten die Besucher neue Displays testen, die auch räumliche Darstellungen aus unterschiedlichen Perspektiven ermöglichen, und Brillen ausprobieren, die ein größeres Sichtfeld zeigen. Innovative Eingabegeräte für VR-Anwendungen sollen zusätzlich zu den optischen Reizen weitere Sinne des Menschen ansprechen.

Normale VR-Controller sind leicht und vermitteln nur sehr eingeschränkt die haptischen Eigenschaften der Objekte, mit denen ein Mensch in der virtuellen Welt interagiert. Ob er beispielsweise einen kleinen Tischtennisschläger, einen großen Tennisschläger oder eine lange Schaufel in einer VR-Anwendung schwingt – alles fühlt sich im virtuellen Raum gleich an. In der Realität hingegen könnte man den Unterschied zwischen diesen Dingen allein durch das Erfühlen erkennen, da sie unterschiedliche Schwerpunkte und Massen aufweisen.

Eingabegeräte mit haptischem Feedback

Das Projekt „Transcalibur: Weight moving VR Controller“ der Universität Tokio nutzt daher Gewichte, deren Position über einen Motor verändert wird, um den Abstand des Schwerpunkts zur Hand sowie die Rotationsträgheit dynamisch zu steuern. Dadurch fühlen sich virtuelle Welten deutlich authentischer an. Die Verlagerung von Gewichten sowie eine Modifikation der Form des Eingabegeräts ändern die Haptik von Objekten spürbar.

„LevioPole“ nutzt Ventilatoren, um zusätzliche Kräfte auf die Eingabegeräte zu erzeugen. In einer der auf der SIGGRAPH angebotenen Demonstrationen konnten Interessierte durch einen virtuellen Kanal paddeln. Die unterschiedlichen



LevioPole gibt Objekten in der virtuellen Realität zusätzliches Gewicht, indem Ventilatoren Kräfte ausüben. So spürt der Anwender beispielsweise den Wasserwiderstand (Abb. 1).

Widerstände beziehungsweise Kräfte, die in der realen Welt beim Bewegen des Paddels durch die Luft respektive durch das Wasser auftreten, macht LevioPole auch in der virtuellen Realität erlebbar. Die VR-Anwendung steuert die Ventilatoren, die jeweils zu viert auf beiden Seiten einer Stange angeordnet sind, so, dass sie beim Paddeln zusätzliche Kräfte ausüben, die zum visuellen Eindruck passen, den der Benutzer hat. Damit sich Effekte, die nur auf eine Seite wirken sollen – etwa beim Paddeln in einem virtuellen Kajak –, oder gleichmäßig verteilte Kraft wie beim Anheben einer Hantel simulieren lassen, kann man die Ventilatoren auch getrennt voneinander steuern. Konferenzbesucher konnten so ihre Kräfte beim Paddeln in der virtuellen Welt oder beim Gewichtheben erproben.

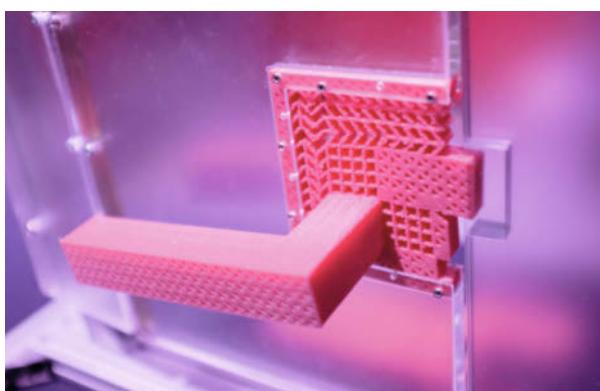
Reale Hilfe aus weiter Ferne leisten

Die Frage, wie jemand, der sich räumlich weit entfernt befindet, jemanden vor Ort unterstützen und ihm zur Hand gehen kann, geht das Projekt „Fusion“ an. Die lokal anwesende Person setzt sich den Helfer einfach auf die Schulter – das

heißt, sie schnallt sich Roboterarme und einen VR-Rechner auf den Rücken.

Eine Stereokamera nimmt die lokale Umgebung auf und zeigt sie in einer VR-Anwendung der körperlich nicht anwesenden Person, die so aus der Ferne die Roboterarme über handelsübliche VR-Controller steuern kann. Auf diese Weise haben zwei Personen eine identische Sicht auf die reale Umgebung und können zusammen agieren und Aufgaben lösen. Insbesondere für Schulungen bietet sich das System an, da für die Beteiligten kein Perspektivwechsel mehr nötig ist. Zur Unterstützung körperlich eingeschränkter Menschen eignet sich das System ebenfalls.

Mit „Metamaterial Devices“ hat das HPI aus Potsdam Materialien mit mechanischen Eigenschaften vorgestellt, die sich durch intelligente Einsatzmöglichkeiten und eine einfache Herstellung auszeichnen. Hierbei hat man nicht nur die äußere Form der Materialien betrachtet, sondern auch die innere Mikrostruktur. Der Aufbau aus einzelnen Zellen verleiht Objekten mechanische Eigenschaften. Als Beispiel zeigten die Forscher in Vancouver ein Türschloss, das in einem Stück als 3D-Druck hergestellt wurde, sodass die Montage einzelner Teile nicht mehr notwendig ist. Aufgrund der Zellstruktur führt dabei die Drehung der Klinke zu einem Zurückziehen der sogenannten Falle. Im Rahmen dieses Projekts war auch eine Webanwendung zu sehen, die die Konstruktion solcher Geräte aus Metamaterialien vereinfacht. (ka@ix.de)



Die Mikrostruktur des Materials verleiht der als 3D-Druck hergestellten Türklinke die Fähigkeit, die Falle wie gewünscht zurückzuziehen (Abb. 2).

Prof. Dr. Paul Grimm

ist Professor für Computergraphik an der Hochschule Fulda. Seine Interessen liegen im Vereinfachen der Erstellung virtueller und augmentierter Realitäten.



Foreshadow in VMware-Umgebungen

Überschattet

Jörg Rieher

Dass sich mit der Angriffsmethode Foreshadow ausgerechnet die Sicherheitstechnik SGX aushebeln lässt, ist vor allem bitter für Intel. Dass aber vor der NG-Variante VMs und Hypervisoren nicht mehr sicher sind, trifft vor allem die mit Virtualisierung arbeitenden Rechenzentren.



Als Anfang 2018 zwei Teams internationaler Sicherheitsforscher unabhängig voneinander die Schwachstelle Foreshadow entdeckten, die sich ähnlich wie Spectre und Meltdown der spekulativen Ausführung heutiger Intel-CPUs kombiniert mit einer Seitenkanalanalyse bedient, beschränkte sich die Reichweite auf Intels SGX-Technik. Durch die inzwischen unter CVE-2018-3615 gelistete Lücke erlangten die Teams Zugang zu in einer SGX-Enklave geschützten Daten und Kryptoschlüsseln im Klartext, indem sie sie in den Datenzwischenspeicher der CPU-Kerne L1d, kurz L1-Cache, kopieren und auslesen konnten. Die Links zur Dokumentation und zu allen weiteren Beschreibungen sind unter ix.de/ix1810098 zusammengefasst.

Intels Überprüfung brachte jedoch ans Licht, dass abgewandelte Techniken aka Foreshadow-NG nicht nur die von den Forschern erbeuteten Daten aus dem L1-Cache extrahieren können, sondern jede Information, die sich im L1-Cache des entsprechenden CPU-Kerns befindet. Mit dieser unter CVE-2018-3620 gelisteten Methode gelang es, auch den Speicher des Kernels auszulesen und den Speicher, den die im SMM (System Management Mode) ausgeführte Firmware verwendet.

Teilen sich virtuelle Maschinen mit anderen VMs oder mit dem Hypervisor einen physischen CPU-Kern, etwa weil Intels Hyperthreading ihn in zwei logische zerlegt, lassen sich deren Speicherbereich die Informationen mit der Variante CVE-2018-3646 entreißen. Intel selbst

fasst alle drei unter L1TF (L1 Terminal Fault) zusammen.

Insbesondere für Betreiber und Kunden von Cloud-Infrastrukturen mit Virtualisierung ist die letztgenannte Variante von erheblicher Bedeutung. Foreshadow Typ 1 und 2 lassen sich mit Microcode-Updates, kombiniert mit Betriebssystem-Updates, Service Packs oder Kernel-Patches, abmildern. Auch dürften diese Updates inzwischen weit verbreitet sein. Bei Variante 3 ist es leider nicht so einfach. Zudem kann es erhebliche Konsequenzen für die Performance der Systeme haben.

Appliances betroffen

Im Folgenden sollen die Auswirkungen aller drei Varianten auf VMwares vSphere-Umgebungen beleuchtet werden. Die erste stellt keine Gefahr dar, da ESXi SGX weder benutzt noch für die Gäste virtualisiert. Anders bei Variante 2: VMware listet auf seiner Website alle virtuellen Appliances auf, für die bisher noch keine Patches vorhanden sind. Dazu zählen vCenter Server Appliance (vCSA) 6.0, 6.5 und 6.7.

Produkte, die nicht betroffen seien, listet VMware in seiner Knowledge Base auf. Die Begründung: Es gebe keinen Weg zum Ausführen von beliebigem Code ohne Administratorrechte, solange man sich an die empfohlene Konfiguration halte. Im selben Dokument heißt es, dass VMwares Hypervisoren ebenfalls nicht betroffen seien von CVE-2018-3620 alias Foreshadow Typ 2.

Die dritte Variante betrifft vSphere-Umgebungen allerdings erheblich. Sie erfordert Änderungen am Hypervisor-System. Die CVE-2018-3646 skizziert zwei Angriffsvektoren. VMware beschreibt diese als „Sequential-context Attack Vector“ und „Concurrent-context Attack Vector“. In beiden teilen sich zwei VMs respektive VM und Hypervisor einen Prozessorkern und damit seinen L1-Cache, in der Regel, weil ein eingeschaltetes Hyperthreading ihn als zwei logische Kerne durchreicht und der Hypervisor sein eigenes Scheduling der vCPUs darüberlegt.

Bei Ersterem kann ein Individuum oder System, das eine VM kontrolliert, an L1-Cache-Daten eines vorherigen Thread des Hypervisors oder einer anderen VM kommen, so sie auf dem gleichen Prozessorkern läuft. Dazu muss noch nicht einmal Hyperthreading aktiviert sein. Die Gefahr, dass jemand auf diese Weise an Daten kommt, kann man mit einem von Intel entwickelten Patch reduzieren, der ein „L1 Cache Flush“ betreibt. Er leert nach wie auch immer optimierten Regeln periodisch den L1-Cache und reduziert damit die Wahrscheinlichkeit eines erfolgreichen Angriffs. Den Patch stellte Intel von März bis Mai 2018 als CPU-Microcode-Update bereit.

Beim „Concurrent-context Attack Vector“ führen die Nutzer der beiden logischen CPUs dank Hyperthreading ihre Prozesse quasiparallel aus. Einen Zugriff des einen Thread auf die Daten des anderen will Intel deshalb mit dem „Core Scheduling“ unterbinden. Diese Technik erlaubt die quasiparallele Ausführung der beiden logischen CPUs nur unter bestimmten Umständen. Dadurch sind die Betriebssystemhersteller gezwungen, solche vertrauenswürdigen Rechenzeitnutzer – VMs oder Hypervisor – zu definieren, damit sie Zugriff auf denselben physischen Kern bekommen.

VMware stellt sie unter dem Namen „ESXi Side-Channel-Aware Scheduler“ oder kurz „SCA-Scheduler“ bereit. Die zum Redaktionsschluss vorliegende erste Version vollbringt aber wahrlich keine Wunder. Sie gewährleistet lediglich, dass immer nur ein logischer Prozessor eines Hyperthreading-aktivierten Kerns benutzt werden kann, gleich ob von einer VM oder vom Hypervisor selbst. Vertrauenswürdige CPU-Nutzer sind noch nicht implementiert. Das wirft die Frage auf, warum man Hyperthreading nicht gleich abschaltet. VMware rät davon ab, weil es ja sein könne, dass man es dank zukünftiger Verbesserungen wieder aktivieren müsse. Die Leistungseinbußen erörtert VMware in seiner Knowledge Base.

VMware liefert den Patch über den Update-Manager aus, aktiviert aber nur den Patch mit dem L1 Cache Flush, sofern das entsprechende Microcode-Update vorhanden ist. Die Leistungsverluste beziffert VMware mit maximal 3 %. Den SCA-Scheduler installiert VMware zwar, schaltet ihn aber nicht scharf. Der Grund dürfte in den erheblichen Leistungseinbußen liegen, die eintreten können. Im ungünstigen Fall, bei einem voll ausgelasteten Host mit wenig oder gar keinen CPU-Reserven, kann die Systemperformance nach der Aktivierung des SCA-Scheduler laut VMware um 32 % zurückgehen (siehe Tabelle „Performanceverluste durch den SCA-Scheduler“).

Mit weniger Leistung

In vSphere-Umgebungen mit großzügiger CPU-Reserve sollte man auch mit aktiviertem SCA-Scheduler über die Runden kommen. VMware rechnet vor, dass bei einem Linux-OLTP-Datenbanksystem und einem Hypervisor-Host, dessen CPU-Gesamtlast bei etwa 62 % liege, der Leistungsverlust nach Aktivieren des SCA-Scheduler nur etwa 1 % betrage. Aber Obacht: War die identische Maschine vor der Aktivierung zu 90 % ausgelastet, liege der Leistungsverlust danach bei 32 %.

Auch wer im eigenen Rechenzentrum über ausreichend Reserven verfügt, sollte sich die Lastentwicklung über einen längeren Zeitraum vor Augen führen. Es genügt, wenn in einer großzügig ausgelegten Umgebung mit Hunderten ESXi-Hosts zu einem Zeitpunkt bestimmte Tasks hundert- oder tausendfach gleichzeitig laufen, seien es nun zahlreiche Datenbanktransaktionen, Backup-Aufträge oder Windows-Updates. In solchen Momenten könnte selbst eine zuvor wie geschmiert laufende Infrastruktur plötzlich haken.

In voll ausgelasteten Umgebungen kann es nach der Aktivierung des SCA-Scheduler zu erheblichen Leistungseinbußen kommen.

Mögliche Performanceverluste durch den SCA-Scheduler laut VMware-Labor

Anwendungs-Workload/Gast-OS	Performanceeinbußen nach Aktivieren des SCA-Scheduler
Datenbank OLTP/Windows	32 %
Datenbank OLTP/Linux (mit vSAN)	32 %
gemischte Workloads/Linux	25 %
Java/Linux	22 %
VDI/Windows	30 %

Man sollte also seine Umgebung und insbesondere die CPU-Last ausführlich analysieren, bevor man den SCA-Scheduler einschaltet. Dies kann man in den erweiterten Systemeinstellungen, indem man die Variable *VMkernel.Boot.hyperthreadingMitigation* auf *true* setzt und anschließend einen Reboot durchführt.

VMware hat zudem ein Werkzeug entwickelt, mit dessen Hilfe man eine solche Evaluierung automatisieren kann (siehe ix.de/ix1810098). Schaltet man den Scheduler nicht scharf, gibt vSphere für die betreffenden Hosts eine Warnmeldung aus, die sich auf Wunsch deaktivieren lässt, indem man die Variable *UserVars.SuppressHyperthreadWarning* auf *1* setzt. Obgleich Intel darauf hinweist, dass es sich bei L1TF um eine hochentwickelte Angriffs-methode handele und bis heute keine Be-richte über tatsächliche Angriffe bekannt seien, sollte man dies dennoch ernst nehmen und seine Umgebung nach den jewei-ligen Möglichkeiten absichern, vor allem, wenn Externe Zugriff darauf haben.

In der VMware Cloud on AWS ist laut VMware der sequenzielle Angriffsvektor bereits „mitigated“, also abgeschwächt, die Anpassung für den gleichzeitigen Angriffsvektor gelang kurz vor Redak-tions-schluss. Für die Horizon Cloud werden entsprechende Updates derzeit priorisiert entwickelt. VMware Workspace One SaaS sei auf Grundlagen der derzeitigen Bewer-tungen von Foreshadow nicht betroffen.

Die Workstation und den Player hat VMware ab Version 14.1.3, die Mac-Hypervisor Fusion und Fusion Pro ab 10.1.3 mit Updates zum verbesserten Schutz gegen den sequenziellen Angriffsvektor ausgestattet. In Hinblick auf den gleichzeitigen Angriffsvektor empfiehlt der Hersteller, Hyperthreading komplett zu deaktivieren. An einem PC geht man dafür ins BIOS- oder EFI-Setup, für den Mac hat VMware ein Werkzeug bereitgestellt (siehe ix.de/ix1810098).

Fazit

Zwar kann man seine virtuellen Umgebungen mit Intel-CPUs gegen Fore-shadow-Angriffe schützen, doch muss man sich vor allem bei solchen mit einer sehr hohen CPU-Gesamtauslastung auf Leistungseinbußen einstellen. Gleichzei-tig bleibt zu hoffen, dass es VMware gelingt, den SCA-Scheduler performanter zu gestalten.

(sun@ix.de)

Jörg Riether

ist spezialisiert auf die Bereiche IT-Sicherheit, Hochverfügbarkeit und Virtualisie- rung. Er arbeitet als Leiter der IT bei der Vitos Haina gemeinnützige GmbH.

[Alle Links: ix.de/ix1810098](#)



Im heise shop: Der Raspberry Pi 3 B+



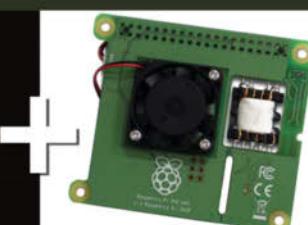
Mehr Power für Ihre Projekte!

- Ca. 10 % mehr Leistung (1,4 GHz)
- WLAN: 2,4 oder 5 GHz
- Bluetooth 4.2
- Vollständig PoE- und HAT-Kompatibel
- Verbesserter Heatspread

Perfekt dazu:

PoE HAT-Modul

- speziell für Raspberry Pi 3 B+
- Strom per Ethernet-Kabel
- optimal für IoT- und Embed-ded-Projekte



Jetzt Raspberry Pi und viel Zubehör portofrei im **heise shop** bestellen!

heise shop

shop.heise.de/raspi-plus

OpenStack absichern

Die Herausforderung meistern

**Marius Feldmann,
Markus Hentsch,
Kai Martius,
Josephine Seifert**



Die Cloud-Infrastruktur OpenStack bietet etliche Angriffsflächen. Gegen einige Schwachstellen helfen feingranulare Zugriffsregelungen und der Einsatz von Kryptografie.

OpenStack gilt als äußerst komplexe Softwaresammlung. Bei dem Gedanken an die Absicherung kommt einem der bekannte Satz von Bruce Schneier in den Sinn: „Komplexität ist der größte Feind der Sicherheit.“ Typischerweise werden in OpenStack-Infrastrukturen zwar punktuelle Sicherheitsvorkehrungen wie das Ausführen von Prozessen ohne Systemverwaltungsrechte getroffen. Aber ein umfassendes Sicherheitskonzept im Sinne von kontrollierten Kommunikationsregeln und kryptografisch gesicherten Verbindungen zwischen den Diensten ist keine verbindliche Vorgabe. Der offizielle Security Guide entspricht eher einer fragmentierten Sammlung von Empfehlungen ohne darunterliegendes Gesamtkonzept. Provider, die eine OpenStack-Infrastruktur einrichten und betreiben, können zwar eine Vielzahl von Linux-Bordmitteln nutzen, sind dabei aber auf sich allein gestellt, aus einem Bedrohungsmödell auch geeignete Maßnahmen abzuleiten.

Dabei sind die Bedrohungen in einer geteilt genutzten und von Dritten betriebenen Infrastruktur vielfältig. In einer naiv durchgeführten Installation von OpenStack ist für Angriffe noch nicht

einmal ein Hardwarezugang in die Kerninfrastruktur nötig: Sämtliche Nutzerdaten können sowohl im Netzwerk als auch auf den Storage-Servern im Klartext abgefangen werden.

Eine Vielzahl von Angriffsvektoren ist über den komplexen Software-Stack zu erwarten: Bricht ein „bösaftiger“ Nutzer aus einer virtuellen Maschine aus oder findet ein Angriff über die Schnittstellen der Cloud zum Internet statt, können Dienste manipuliert und Nutzerdaten von Dritten abgefangen werden.

Abbildung 1 zeigt eine schematische Darstellung eines OpenStack-Diensts wie Nova oder Cinder. Diese Dienste offerieren nach außen in Richtung Nutzer wie auch in Richtung anderer OpenStack-Dienste REST-APIs, über die Funktionen zum Cloud-Ressourcenmanagement angeboten werden. Hinter der API-Komponente befinden sich mehrere Dienstkomponenten, durch deren Zusammenwirken bestimmte Funktionen des Dienstes umgesetzt werden. Im Falle von Nova existieren beispielsweise die Dienstkomponenten nova-scheduler und nova-compute. Sie greifen für ihre Kommunikation und für die Datenablage auf weitere Systeme in der Infrastruktur zu: Neben Memcached und einer Message

Queue handelt es sich dabei vor allem um eine relationale Datenbank.

Gefahrenquelle REST-APIs

Die größte Angriffsfläche auf OpenStack-Infrastrukturen bieten die REST-API-Dienste der verschiedenen OpenStack-Komponenten wie nova-api für die Verwaltung virtueller Maschinen und cinder-api für virtuellen Blockspeicher. Härtungsmaßnahmen sollten in einem ersten Schritt diese REST-APIs adressieren. Der Einsatz von HTTPS ist hier selbstverständlich. Weiterhin sollten die API-Komponenten in einem eigenen Ausführungskontext isoliert werden. Hierfür bieten sich Linux Namespaces oder Mechanismen wie SELinux und AppArmor an. Im Falle eines erfolgreichen Angriffs verhindert dies, dass der Host dieser nach außen exponierten Komponenten compromittiert wird. Weiterhin gehört die Vorlagerung eines HTTPS-Proxys mit zusätzlichen Features wie einem Rate Limiting für die Absicherung gegen Denial-of-Service-Angriffe in den Werkzeugkasten für die Infrastrukturhärtung. Von außen erreichbare API-Bestandteile sind idealerweise von denen separiert, die

nur von innerhalb der Infrastruktur angesteuert werden.

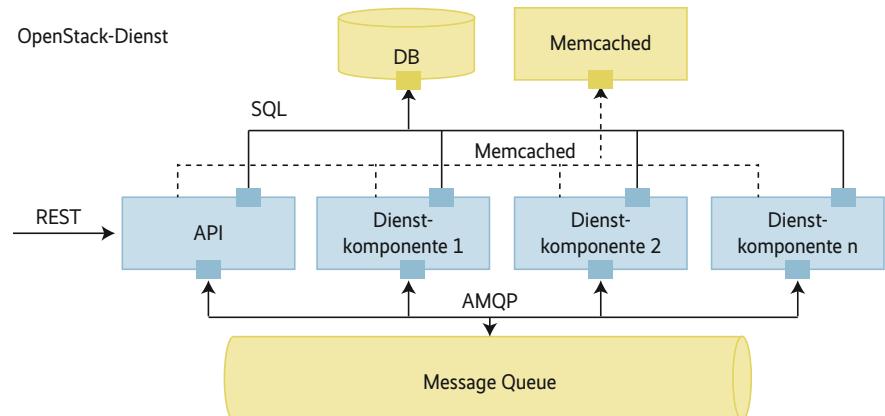
Neben diesen Absicherungsmaßnahmen zur Verschlüsselung und Authentifizierung der Kommunikationspartner sollte auch eine feingranulare Zugriffskontrolle auf die REST-APIs konfiguriert werden. Hierfür bietet OpenStack einen Policy-basierten Mechanismus. Die pro Dienst bereitgestellte Konfigurationsdatei *policy.yml* schränkt Zugriffe auf die REST-APIs rollenbasiert ein.

Standardregeln befinden sich in einer vordefinierten Policy-Datei im Konfigurationsverzeichnis einer Komponente oder aber im Programmcode der Komponente, wie für Nova ab API-Version 2.1. Letzteres ist in der Umstellung auf die Policy-Unterbibliothek der OpenStack-Oslo-Bibliotheksammlung begründet, die alle Standarddefinitionen von Policies im Programmiercode selbst verankert, ohne eine derartige YAML-Datei beizulegen. Auf diese Eigenheit geht die aktuelle Fassung des Security Guides nicht ein. Die YAML-Datei zur Definition von angepassten Policies ist auch für diese Komponenten weiterhin zu nutzen, aber die Standardkonfiguration und damit die Liste möglicher Regelnamen muss für betroffene Komponenten zunächst manuell erzeugt werden. Das erledigt der folgende Befehl, wobei bei *namespace* die entsprechende Komponente anzugeben ist:

```
oslopolicy-sample-generator --namespace nova --output-file default-policy.yml
```

Auf Basis der generierten Datei kann anschließend eine individuelle Einschränkung der verfügbaren Funktionen der API erfolgen. So ist es möglich, einer Gruppe von Nutzern durch die Zuweisung einer bestimmten Rolle das Erstellen von Objekten (beispielsweise von Volumes oder virtuellen Maschinen) zu verbieten. Listing 1 zeigt einen Teil einer Policy-Datei der Komponente Cinder.

Im oberen Teil befinden sich Deklarationen, die die zusätzliche Definition eigener Nutzerkriterien für Regeln wider-



Anatomie der Infrastruktur wichtiger OpenStack-Dienste (Abb. 1)

Listing 1: Ausschnitt aus einer Policy-Datei der Cinder-Komponente

```
{
  "admin_or_member": "is_admin:True or project_id:%(project_id)s",
  "volume:create": "",
  "volume:delete": "role:admin",
  "volume:get": "rule:admin_or_member",
  "volume:get_all": "rule:admin_or_member",
  "volume:extend": "rule:admin_or_member",
  ...
}
```

Listing 2: Die Konfigurationsdatei in Cinder anpassen

```
[database]
connection = mysql+pymysql://cinder:password@galera.cloudandheat.com/cinder?charset=utf8 &ssl_ca=/etc/ca-cert.pem&ssl_cert=/etc/cinder-cert.pem&ssl_key=/etc/cinder-key.pem
```

spiegeln. Im hier dargestellten Fall wurde das Kriterium *admin_or_member* so definiert, dass ein zugelassener Nutzer entweder ein Administrator sein oder sich im gleichen Projekt befinden muss. Die Rolle *admin* ist hierbei vordefiniert, *admin_or_member* wurde als benutzerdefiniertes Kriterium festgelegt. Nach der Deklaration solcher benutzerdefinierter Kriterien sind die eigentlichen Regeln festgelegt. Hierbei verwendet OpenStack bestimmte Bezeichner, um die einschränkenden Aktionen zu identifizieren (Beispiel *volume:create*). Die Menge der definierten Bezeichner ist komponentenspezifisch und daher nur für die jeweilige Komponente wirksam.

Das Auflisten einzelner oder aller Volumes sowie das Erweitern eines Volumes über das deklarierte Kriterium *admin_or_member* ist ausschließlich einem Administrator oder Projektteilnehmer vorbe-

halten. Das leere Kriterium für das Erstellen von Volumes *volume:create* führt zur Freigabe der Aktion für beliebige Nutzer und legt keine Beschränkungen fest. Für das Löschen von Volumes ist hier eine Rollenprüfung auf die *admin*-Rolle festgelegt. Die definierten Policy-Regeln überschreiben die Standardregeln der jeweiligen Komponente. Bis auf *volume:get* enthält die Cinder-Standardvorgabe für alle obigen Policies keine Beschränkungen.

Die Datenbank schützen

Eine besonders sensible Infrastruktorkomponente stellt die erforderliche relationale Datenbasis dar. Diese sollte aus Hochverfügbarkeitsgründen selbstverständlich redundant ausgelegt und synchron repliziert werden. Es empfiehlt sich, die Interaktion der OpenStack-Dienste mit der Datenbank abzusichern.

Die SQL-Kommunikation mit dem Datenbankserver in einer OpenStack-Infrastruktur ist standardmäßig unverschlüsselt. Zunächst ist auch hier TLS-Verschlüsselung für die SQL-Kommunikation zu aktivieren, um zusätzlich zur Passwortauthentifizierung einen abgesicherten und verschlüsselten Kanal bereitzustellen. Dafür muss die Konfiguration des SQL-Servers erweitert und ein Serverzertifikat darauf eingerichtet werden. Darüber hinaus sollte jede Dienstkompo-



- OpenStack verwaltet Cloud-Computing-Plattformen. Es besteht aus vielen Einzelkomponenten, die größtenteils in Python geschrieben sind.
- Aufgrund seiner komplexen Infrastruktur ist OpenStack vielfältigen Angriffen ausgesetzt. Die größte Gefahr lauert bei den REST-APIs der Komponenten. Doch auch die zentrale Datenbank muss geschützt werden.
- Mit verschlüsselten Volumes und signierten Images lassen sich die Cloud-Ressourcen schützen. Der Schlüsseldienst Barbican hilft hierbei.

nente, die die Datenbank nutzt, einen eigenen Datenbanknutzer zur Authentisierung verwenden.

Als maximal restriktive Variante kann für jeden Datenbanknutzer die Zugriffsberechtigung so gesetzt werden, dass ein Clientzertifikat mit bestimmten Attributen gefordert wird. Hierfür muss auf Clientseite ein Zertifikat bereitgestellt und die Komponentenkonfiguration entsprechend angepasst werden. Dafür findet sich in der Konfigurationsdatei einer jeden OpenStack-Komponente die Spezifizierung des SQL-Servers. Dort können sowohl Zieladresse als auch Verbindungsoptionen gesetzt werden. Es gilt sicherzustellen, dass die Zieladresse mit dem Common-Name-Attribut des Serverzertifikats übereinstimmt. Hierfür bietet sich die Nutzung eindeutiger Rechnernamen (Fully Qualified Domain Name, FQDN) im Zusammenhang mit Namensauflösung an. Die Anpassung der Konfigurationsdatei in Cinder zeigt Listing 2.

Weiterhin ist es möglich, die Quellen, von denen aus sich ein Datenbankclient verbinden kann, anhand von IP-Adressbereichen oder FQDNs zu beschränken. Dazu muss in dem GRANT-Befehl die Hostangabe nach dem Nutzernamen näher spezifiziert werden. Um beispielsweise nur Clients aus dem Subnetz 10.1.2.0/24 zu erlauben, wäre die Anpassung wie folgt:

```
GRANT ALL ON cinder.* TO 'cinder'@'10.1.2.%' IDENTIFIED BY 'password' REQUIRE ...
```

Zertifikatsbasierte Clientauthentifizierung gegenüber den REST-APIs ist leider derzeit mit OpenStack nicht möglich. Hierfür

müsste der OpenStack-Client um eine entsprechende Funktion erweitert werden.

Message Queue und Cloud-Ressourcen absichern

Die AMQP Message Queue, für die meist RabbitMQ eingesetzt wird, bildet eine weitere Achillesferse der OpenStack-Infrastruktur, die es zu schützen gilt. Gehen über sie übermittelte Nachrichten verloren, werden repliziert oder abgehört, kann dies große Auswirkungen auf die Sicherheit der Infrastruktur haben. Analog zur HTTPS-Kommunikation mit den REST-APIs sollte die AMQP-Kommunikation verschlüsselt erfolgen. RabbitMQ kann hierfür ebenfalls TLS nutzen, um Vertraulichkeit und Integrität zwischen Message Broker und Clients zu gewährleisten. Zusätzlich kann wechselseitige Authentizität durch den Einsatz von Server- und Clientzertifikaten erreicht werden. Authentizität der über den Message Broker kommunizierenden Instanzen (beispielsweise nova-api und nova-scheduler) lässt sich damit hingegen nicht sicherstellen.

Neben der Infrastruktur spielt in OpenStack-Umgebungen der Schutz von Cloud-Ressourcen eine zentrale Rolle. Der Fokus von OpenStack liegt hierbei auf der Verschlüsselung von Volumes und der Signatur von Images. Für die Verwaltung der Schlüssel und Zertifikate muss der OpenStack-Schlüsseldienst namens Barbican [1] in der Cloud-Infrastruktur betrieben werden.

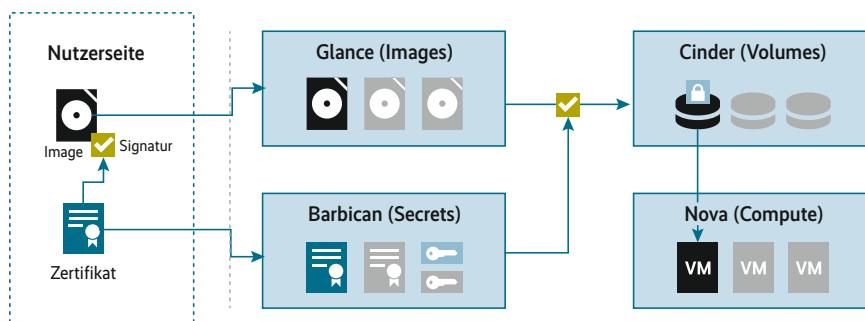
Ein einfaches Beispiel der Abläufe zeigt Abbildung 2. Auf Nutzerseite wird

ein Image signiert und gemeinsam mit der erzeugten Signatur an die OpenStack-Infrastruktur übermittelt. Weiterhin wird das Zertifikat in Barbican abgelegt. Anschließend kann in der Infrastruktur nach einer Überprüfung der Image-Signatur aus dem Image ein Volume generiert werden, das verschlüsselt vorgehalten wird. Von diesem verschlüsselten Volume kann abschließend eine virtuelle Maschine booten. Barbican stellt den Schlüssel für die Volume-Verschlüsselung während des Volume-Erzeugungsprozesses bereit. Typischerweise liegen die Schlüssel beim Cloud-Provider in Barbican.

Ein weiterer Weg zur Absicherung von Cloud-Ressourcen ist die Verschlüsselung des Ephemeral Storage, die bei der Verwendung des Logical Volume Managers unterstützt wird. Obwohl verschlüsselter Ephemeral Storage bereits in der Icehouse-Release (4/2014) enthalten war, war er über mehrere Releases aufgrund eines Bugs nicht verwendbar. In der Queens-Release (2/2018) ist das Feature allerdings einsatzbereit. Um es zu aktivieren, sind die in Listing 3 gezeigten Konfigurationen für Nova (*nova.conf*) erforderlich.

Wichtig ist, dass eine gewählte *key_size* von 512 zur Verwendung von AES-256 bei der Storage-Verschlüsselung führt, da sich die Schlüssellänge des AES-Anteils durch das eingesetzte XTS-Verfahren halbiert. Der maximal mögliche Wert für *key_size* ist jedoch unter anderem durch den eingesetzten Key Manager limitiert, der die Schlüssel generiert und bereitstellt. Dies ist im Regelfall OpenStack Barbican, der in der aktuellen Queens-Release noch auf die Generierung von maximal 256 Bit langen Schlüsseln (und damit AES-128 bei XTS) beschränkt ist. Und dies nur, wenn das Simple-Crypto-Plug-in als Backend zur Verwaltung des Schlüsselmaterials verwendet wird (Standardvorgabe). Diese Beschränkung wird voraussichtlich in der nächsten OpenStack-Release auf 512 Bit für XTS-Schlüssel angehoben. Der Einsatz anderer Backend-Plug-ins für Barbican, wie etwa HSMs über PKCS#11- oder KMIP-Schnittstellen, ist hiervon nicht betroffen.

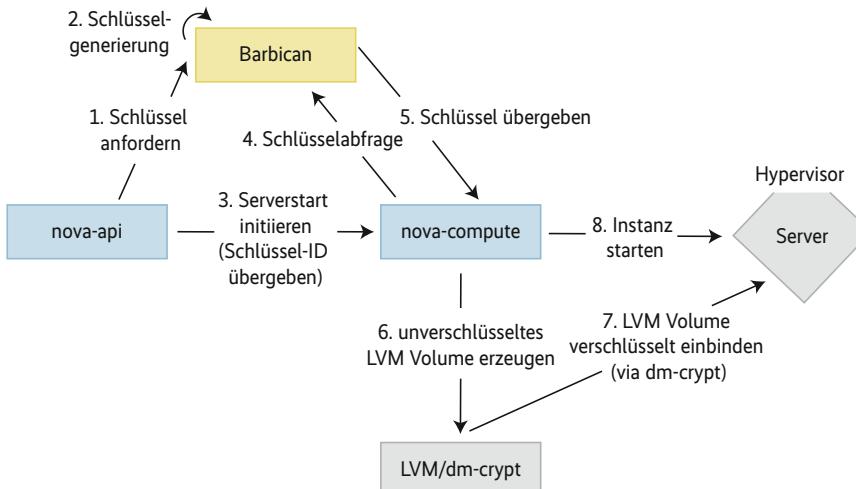
Abbildung 3 zeigt den Ablauf. Nach dem Erhalt einer Anfrage zur Erzeugung einer VM fordert die nova-api-Komponente bei Barbican einen Schlüssel an (1, 2). Nach der Selektion eines Hypervisors im Cluster durch den Scheduler wird die von Barbican erhaltene Schlüssel-ID an die auf dem Hypervisor laufende novacompute-Instanz übergeben (3), die unter Verwendung dieser ID den Schlüssel von Barbican abfragen kann (4, 5). Die nova-



Barbican verwaltet kryptografische Informationen und prüft Images, bevor Cinder daraus Volumes erstellt (Abb. 2).

Listing 3: Konfigurationen für Nova (*nova.conf*)

```
[ephemeral_storage_encryption]
cipher = aes-xts-plain64
enabled = True
key_size = 512
[key_manager]
api_class = castellan.key_manager.barbican_key_manager.BarbicanKeyManager
[barbican]
auth_endpoint = http://keystone_address:5000/v3
```



Für Ephemeral Storage erzeugt Barbican Schlüssel. nova-compute fragt sie ab und verschlüsselt den Speicher mithilfe von dm-crypt (Abb. 3).

compute-Instanz erzeugt daraufhin ein Logical Volume Manager (LVM) Volume (6) und verschlüsselt es unter Verwendung von dm-crypt (7). Die Instanz kann schließlich gestartet werden (8).

Die Absicherung der Cloud-Ressourcen für OpenStack steckt noch in den Kinderschuhen. Rund um Volumes und Images hat OpenStack zwar ausgewählte Sicherheitsmechanismen integriert. Dennoch bleiben einige Lücken offen, die die Sicherheitsstrategie weit entfernt von einem Defence-in-Depth-Ansatz positionieren. So fehlen eine kryptografische Absicherung von Netzwerken einzelner Mandanten oder der Verzicht auf den Schlüsseldienst auf Cloud-Provider-Seite durch Einsatz eines Bring-your-own-Key-Mechanismus (BYOK), durch den keinerlei Schlüsselmaterial beim Cloud-Provider gespeichert werden muss.

Fazit

Was in den präsentierten ausgewählten Mechanismen zur Absicherung einer OpenStack-Infrastruktur und von Cloud-Ressourcen deutlich wird, ist der hohe manuelle Aufwand, der sich bei einer ausgedehnten Absicherung abzeichnet. Hier setzt einer der wichtigsten Garanten für eine sichere Infrastruktur an: Zur Vermeidung manueller Schritte, der Einführung klarer Betriebsstandards wie auch einer möglichen Überprüfbarkeit des Infrastrukturstatus ist eine Automatisierungs- und Monitoringinfrastruktur essenziell. Bei der Automatisierungssoftware ist es selbstverständlich Voraussetzung, dass sie nicht nur den regulären Lebenszyklus einer OpenStack-Infrastruktur verwalten, sondern auch kryptografisches Material sicher in der Infrastruktur verteilen und aktualisieren kann. Generell ist es eine oft vernachlässigte Selbstverständlichkeit, dass der Einsatz kryptografischer

Mechanismen immer auch eine sichere Erzeugung von Schlüsseln sowie ein durchdachtes und automatisiertes Schlüsselmanagement voraussetzt.

Der mit einem ganzheitlichen Lebenszyklusmanagement wie auch einem fundierten Schlüsselmanagement verbundene Aufwand ist hoch. Inwiefern er sich lohnt, hängt davon ab, welcher Betriebsstandard für die jeweilige OpenStack-Infrastruktur erforderlich ist. Aus Sicherheitsperspektive lohnt er sich in jedem Fall. (nb@ix.de)

Dr. Marius Feldmann

ist COO der Cloud&Heat Technologies GmbH und beschäftigt sich seit über fünf Jahren mit OpenStack.

Markus Hentsch

ist Head of Cloud Innovation bei der Cloud&Heat Technologies GmbH und übernimmt dort die technische Leitung des SecuStack-Projekts.

Dr. Kai Martius

ist CTO bei secunet und hat dort Erfahrungen in der Entwicklung hochsicherer Verschlüsselungsprodukte gewonnen.

Josephine Seifert

ist Innovation Assistant bei der Cloud&Heat Technologies GmbH und beschäftigt sich im SecuStack-Projekt mit Upstream-Beiträgen zu OpenStack.

Literatur

- [1] Martin Gerhard Loschwitz; Streng geheim; Geheimnisse in OpenStack mit Barbican verwalten; *iX* 4/2018, S. 132

Mit allen Wassern gewaschen:

iX DEVELOPER Java 2017
Zusatrmaterial auf DVD
Buchbeschreibung
Technik
Anwendungen
Arbeit mit Java
Programmierung
Paket Spieldaten
Beispiele

iX DEVELOPER Java
Auch als Download erhältlich.
12,90 € >

iX kompakt - Container und Virtualisierung
Zusatrmaterial auf DVD
Docker
Kubernetes
Mesos und Container
Migrieren in die Cloud
Beispiele

iX kompakt
CONTAINER UND VIRTUALISIERUNG
Auch als Download erhältlich.
12,90 € >

iX kompakt - Container und Virtualisierung
Hinweise für Administratoren und Anwender
Docker, Kubernetes, Mesos und Co.
Containerisierung
Virtualisierung
Cloud Migration
Beispiele

iX kompakt 2018
Auch als Download erhältlich.
12,90 € >

Weitere Sonderhefte zu vielen spannenden Themen finden Sie hier:
shop.heise.de/specials2018

Kurz erklärt: One-Click Unsubscribe

Weggeklickt

Sven Krohlas



Wohl jeder hat schon unangenehme Überraschungen nach dem Klick auf einen „Abmelden“-Link in einer Werbemail erlebt. Die Aufforderung zum längst vergessenen Login oder zur Verifikation von Daten wie der beim Dienst hinterlegten Postanschrift ist für manche Nutzer eine Hürde für die Abmeldung – erst recht, wenn sie sich gar nicht an einen Registrierungsvorgang erinnern können. Umso erfreulicher, wenn ohne weitere Umstände eine Meldung wie „Sie wurden erfolgreich abgemeldet“ erscheint. Dies ist jedoch nicht selbstverständlich. Auch der optionale, oft nicht direkt vom Mailprogramm angezeigte Header „List-Unsubscribe“ führt meist zu keinem anderen Workflow.

Eine mögliche Ursache für diese Situation könnte eine ungenaue Formulierung im 20 Jahre alten RFC 2369 sein, der die Mail-Header-Zeile „List-Unsubscribe“ beschreibt (Quellen siehe ix.de/ix1810104). Das im Header angegebene Kommando soll den Nutzer „directly“ abmelden. Doch das wird in der Praxis immer wieder anders interpretiert. Die Interessen vieler Versender scheinen auf den ersten Blick im Widerspruch zu denjenigen der Adressaten zu stehen. Mit dem bloßen Ausstoß an E-Mails steigen jedoch weder die Bekanntheit der versendenden Marke noch die Einnahmen der Versanddienstleister dauerhaft: Uninteressierte Nutzer verschieben E-Mails oft in den Spamordner, anstatt sie zu löschen – insbesondere wenn unklar ist, wie man sich vom Newsletter abmelden

Das Entfernen von Adressen aus den Verteilern von E-Mail-Newslettern ist ein Standardprozess bei den Versendern. Dennoch haben die Empfänger oft Schwierigkeiten, sich von Massenmailings abzumelden. Ein neues Verfahren soll die Lage verbessern.

kann. Das wirkt sich auf die Inhaltsfiltrierung aus und die Reputation des Versenders nimmt bei den großen Mailboxprovidern ab.

Im schlimmsten Fall könnten die Werbemails nicht nur bei einzelnen Nutzern, sondern bei Mailprovidern wie Web.de oder T-Online systemweit als Spam wegsortiert oder sogar abgewiesen werden. Ein derartiges Blacklisting wäre ein enormer Schaden für die versendende Marke sowie den Versanddienstleister.

Nur E-Mails mit für die Empfänger interessanten Inhalten steigern die Reputation dank hoher Öffnungs- und Klickraten. Daher sollten nicht nur Kampagnen auf die Interessen der Adressaten zugeschnitten sein, sondern auch Nutzer, die kein Interesse mehr an einem Newsletter haben, sollten sich möglichst leicht abmelden können. Eine andere Herausforderung gibt es auf technischer Seite. Leider rufen manche Sicherheitsprodukte URLs automatisiert zur Analyse auf. Dies hat mit Inkrafttreten der DSGVO zu kuriösen automatischen Bestätigungen der Zustimmungsmails zur Datenerhebung und -verarbeitung geführt.

All die genannten Schwierigkeiten geht nun der RFC 8058 mit der Beschreibung einer „One-Click“-Vorgehensweise an. So müssen bei RFC-8058-konformen E-Mails die Abmelde-URLs per POST- anstatt mit dem bisher üblichen GET-Request aufgerufen werden. Dies sollten die Versender im Regelfall mit einer minimalen Codeänderung umsetzen können.

Ist der Abmeldelink nutzerspezifisch und nicht vorhersehbar gestaltet, beispielsweise mit einer eindeutigen, zufälligen ID statt der Mailadresse des Abonenten, können ihn Angreifer auch nicht zum Leeren des Verteilers missbrauchen. Dies sollte unabhängig von RFC 8058 als Best Practice bekannt sein. Verzichten müssen die Versender jedoch auf in den Abmeldeprozess integrierte Umfragen, beispielsweise zum Grund der Abmeldung. Diese sind in der aktuellen Version des Standards nicht vorgesehen.

RFC 8085 lässt sich ziemlich einfach umsetzen. Ein Newsletter signalisiert mit einer neuen Zeile im E-Mail-Header die Möglichkeit der Abmeldung: *List-Unsubscribe-Post*: *List-Unsubscribe=One-Click*. Mailclients, die diesen Standard implementieren, können nun die unter „List-Unsubscribe“ angegebene URL mit einem POST-Request aufrufen. Signaliert der Response-Code keinen Fehler, war die Abmeldung erfolgreich. Damit Spammer auf diesem Weg keine Adressbestätigung erhalten, sollten Versanddienstleister diese Funktion nur Kunden mit einer ausreichenden Reputation zur Verfügung stellen. Mailboxprovider und Mailclients können die Abmeldefunktion mit einem Button in das Nutzerinterface integrieren oder beim Verschieben in den Spamordner nachfragen, ob es sich wirklich um Spam handelt oder ob eine ordnungsgemäße Abmeldung infrage kommt.

Weite Verbreitung in Aussicht

Die meisten großen Mailboxprovider haben bereits Unterstützung für One-Click Unsubscribe gemäß RFC 8058 signalisiert. So empfiehlt Google (Gmail) die Nutzung auf seinen Postmaster-Seiten. Die Certified Senders Alliance (CSA) des eco-Verbands verpflichtet ihre Mitglieder ab dem 1. Juli 2019 zur Umsetzung. Die CSA hat viele internationale Mailbox-provider wie AOL, Microsoft (Outlook), Yahoo oder Yandex als Partner. Da es sich um eine Initiative des eco e. V. handelt, hat der Standard auch im deutschsprachigen Raum Aussichten auf eine hohe Verbreitung. (un@ix.de)

Sven Krohlas

ist E-Mail-Spezialist und IT Security
Consultant bei BFK edv-consulting GmbH
in Karlsruhe.

IT-Sicherheit im Fokus

Trends und Produkte zur it-sa

Endpoint Security: essenziell für die Netzwerksicherheit

Bis zum Ende

Seite III

Stand der Malware-Industrie

Hase und Igel

Seite VI

Zugriffssteuerung via
Cloud Access Security Broker

Einlasskontrolle

Seite X

Vorschau: Hosting

Cloud- Geschäftsmodelle

Seite XI

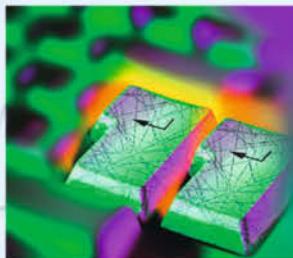


iX extra zum Nachschlagen:
www.ix.de/extra



Softwareentwicklung

JETZT
anmelden
und Ticket
sichern!



Parallele Programmierung

5. bis 7. November
2018 in Hannover



Jenkins

4. bis 5. Dezember
2018 in Nürnberg



C++11/C++14/C++17

11. bis 13. Dezember
2018 in Nürnberg



Weitere Infos unter:
www.heise-events.de/workshops
www.ix-konferenz.de



Bis zum Ende

Endpoint Security: essenziell für die Netzwerksicherheit

Viele aktuelle Sicherheitsvorfälle zeigen, dass nach wie vor die Endgeräte im Netzwerk Angreifern Tür und Tor öffnen. Neue Methoden bei ihrem Schutz sind dringend notwendig: Endpoint Detection and Response soll Endpoint Protection Platforms ergänzen und mit maschinellem Lernen anreichern.

Für Administratoren und IT-Verantwortliche können Anwender mit vielen Geräten, die sich im Firmennetzwerk tummeln, zum echten Albtraum werden – denn es wird immer schwerer, diese Endpunkte so zu überwachen und so zu sichern, dass sie nicht zum Einfallstor für alle mögliche Schadsoftware und Bedrohungen werden. Die vielen Ransomware-Vorfälle in letzter Zeit sprechen hier eine deutliche Sprache. So beklagen auch Analysten und Sicherheitsfachleute immer wieder die mangelhafte Sicherheit der Endgeräte in vielen Unternehmen. Zudem sind sie sich darüber einig, dass herkömmliche Sicherheitsansätze wie Antivirenprogramme für deren Schutz nicht mehr ausreichen.

Zu wenig Sicherheitspersonal

IT-Fachabteilungen in den meisten Unternehmen gehen zunächst davon aus, dass die Endpunkte ihres Netzwerks grundsätzlich sicher sind und entsprechend den Unternehmensrichtlinien installiert wurden. Deshalb erscheint es ihnen nicht notwendig, sie noch einmal besonders zu überwachen und zu schützen.

Zudem gibt es in den Unternehmen weitere Vorschriften und Richtlinien, wie die Nutzer mit ihren Endgeräten umzugehen haben – etwa dass sie ihre Systeme und Software patchen und auf dem aktuellen Stand halten. Aufgrund der Arbeitslast und der dünnen Personaldecke müssen sich viele IT-Ab-

teilungen darauf verlassen, dass das wie gewünscht funktioniert.

Die Wirklichkeit mit vielen mobilen Geräten, die mit und ohne BYOD-Strategie (Bring your own Device) ins eigene Netz gelangen, beweist leider, dass diese Annahmen eher illusorisch sind: Das Problem beginnt häufig schon damit, festzustellen, wie viele Endpunkte (und entsprechende Geräte) im Firmennetzwerk vorhanden sind. Das setzt sich unter anderem fort mit Fragen nach deren Konfiguration oder installierter Software. Vom Sicherheitsbewusstsein vieler Endanwender, die im Zweifelsfall die „bremsenden, umständlichen“ Sicherheitsvorkehrungen lieber abschalten, ganz zu schweigen.

Endpoint Security soll es richten. Diese Techniken sollen Endpunkte jeder Art im Netzwerk absichern, ob individuelle Workstations und PCs, Smartphones, Tablets oder andere Devices. Auch die weitverbreiteten IoT-Geräte fallen in diese Kategorie, zumal deren Sicherheitszustand oftmals unzureichend ist. Auf den ersten Blick mag das wie eine weitere Marketingidee klingen, um Antivirussoftware und Firewalls für den PC besser zu positionieren und zu verkaufen.

Profi-IT: Zentral verwaltete Geräte

Doch ein wichtiger Punkt, in dem sich dieser Ansatz von „normalen“ Sicherheitslösungen im KMU- und SOHO-Bereich unterscheidet, ist die Tatsache,

dass die verschiedenen Programme und Tools der Endpoint Security auf den Endgeräten von der Unternehmens-IT zentral gesteuert werden. Damit existieren also zwei Ebenen für diese Sicherheitsmaßnahmen: Softwareagenten sind im Hintergrund auf den Endgeräten aktiv und es gibt ein Managementsystem, das diese Agenten überwacht und verwaltet: Es kann sich dabei um ein Dashboard im Browser handeln, das vom IT-Fachpersonal überwacht wird. Dieses greift ein, wenn Probleme auftauchen.

Abwehr teilweise automatisiert

Es kann aber auch eine Software sein, die automatisiert die verschiedenen kritischen Punkte und Sicherheitsbedrohungen auf den Endgeräten beseitigen kann. Vielfach finden sich heute auch Kombinationen dieser beiden Ansätze, die beispielsweise den IT-Fachleuten Routinetasks der Arbeit abnehmen können.

Solche sogenannten Endpoint Protection Platforms (EPPs) sind in der einen oder anderen Ausprägung wohl in fast jeder Netzwerkinfrastruktur eines Unternehmens zu finden. Sie kontrollieren bekannte Bedrohungen wie herkömmliche Malware und Viren. Sie können aber durch Heuristik auch mit unbekannten Bedrohungen umgehen, wenn etwa eine neue Variante bereits bekannter Malware auf die Endpunkte zielt.

Allerdings haben sich die Angriffsszenarien und die dafür

verwendeten Techniken im Laufe der letzten Jahre rasant weiterentwickelt, sodass es spezieller Tools und Techniken bedarf, um neue Angriffe zu bekämpfen. Ein Beispiel dafür sind sogenannte Bypass-Techniken, die installierte Sicherheitssysteme umgehen können. Dazu untersuchen die Angreifer zunächst die bestehende Infrastruktur und natürlich auch die vorhandenen Systeme für die Endpunktsicherheit.

Künstliche Intelligenz gilt als Königsweg

Die bislang existierenden Sicherheitsprodukte sind allzu häufig noch auf die Sichtbarkeit jedes einzelnen Endpunktes ausgerichtet. Das bedeutet, sie können trotz EPP nicht alle Endpunkte in Echtzeit über eine zentrale Schnittstelle darstellen und überwachen. Zudem sind sie in der Regel nicht in der Lage, auf neue Methoden wie datenlose Angriffe, Speicherinjektionen oder Malware-freie Bedrohungen adäquat zu reagieren. Es sind also neue, „intelligenten“ Systeme gefragt, die mit ihren Techniken diese Lücken schließen.

Wenn es ein Schlagwort gibt, das nicht nur von Marketing- und Vertriebsexperten, sondern auch von vielen IT-Spezialisten häufig als Lösung für viele Probleme gepriesen wird, dann ist es die sogenannte künstliche Intelligenz. Das gilt auch im Umfeld der IT-Security, und mittlerweile gibt es kaum einen Anbieter von Sicherheitssoftware, dessen Programme nicht auf die eine oder andere Art mit dieser Intelligenz aufwarten können. Die Vorteile dieses Ansatzes sind in der Tat bestechend, vor allen Dingen dann, wenn die Firmen realistisch an die Sache herangehen und – wie etwa in Forscherkreisen und an Universitäten durchaus üblich – sich mehr auf die Vorteile des maschinellen Lernens (ML) konzentrieren, anstatt der Illusion von denkenden Maschinen nachzujagen.

Vor dem Einsatz solcher Techniken mussten Menschen

Anbieter von Endpoint Protection

Hersteller	Produkt	Webadresse
Bitdefender	GravityZone for Endpoints	www.bitdefender.de
Carbon Black	Cb Predictive Security Cloud	www.carbonblack/de
Checkpoint Software	Endpoint Complete Protection	www.checkpoint.com
Cisco	Cisco AMP für Endpoints	www.cisco.com/c/de_de
Comodo	Comodo Endpoint Protection	www.comodo.com
Cylance	CylancePROTECT	www.cylance.com/de-de
ESET	ESET Endpoint Security	www.eset.com/de
Ivanti	Ivanti Endpoint Security for Endpoint Manager	www.ivanti.de
Kaspersky Lab	Kaspersky Endpoint Security for Business	www.kaspersky.de
McAfee	McAfee Endpoint Security	www.macafee.com/de-de
Microsoft	Microsoft System Center Endpoint Protection (SCEP)	www.microsoft.de
Sophos	Sophos Endpoint Protection (Intercept X)	www.sophos.com/de-de
Symantec	Symantec Endpoint Protection 14	www.symantec.com/de/de
Trend Micro	Smart Protection Suite (XGen Security)	www.trendmicro.com/de_de

Durch den Einsatz von ML-Methoden bei Endpunkten werden diese in die Lage versetzt, Angriffe selbst abzuwehren. Diese Techniken sind sicher nicht perfekt, tragen aber zu deutlich mehr Sicherheit bei. Zwar können AI und ML helfen, Cyberattacken zu vermeiden, einen Königsweg, der aktuelle fortgeschrittene Bedrohung aufhalten kann, gibt es jedoch nicht.

Mehr Sicherheit durch EDR?

Die geschilderten Hintergründe machen es deutlich: Es reicht auf keinen Fall mehr aus, Angriffe, Schadsoftware und entsprechende Aktionen nur zu entdecken und zu melden, in der Hoffnung, dass die IT-Mannschaft dann irgendwann die Zeit findet, Gegenmaßnahmen einzuleiten. Auch wenn es immer noch genügend Angriffe beispielsweise mit altbekannten Viren oder einfache Versuche des Abscannens der Endpunkte

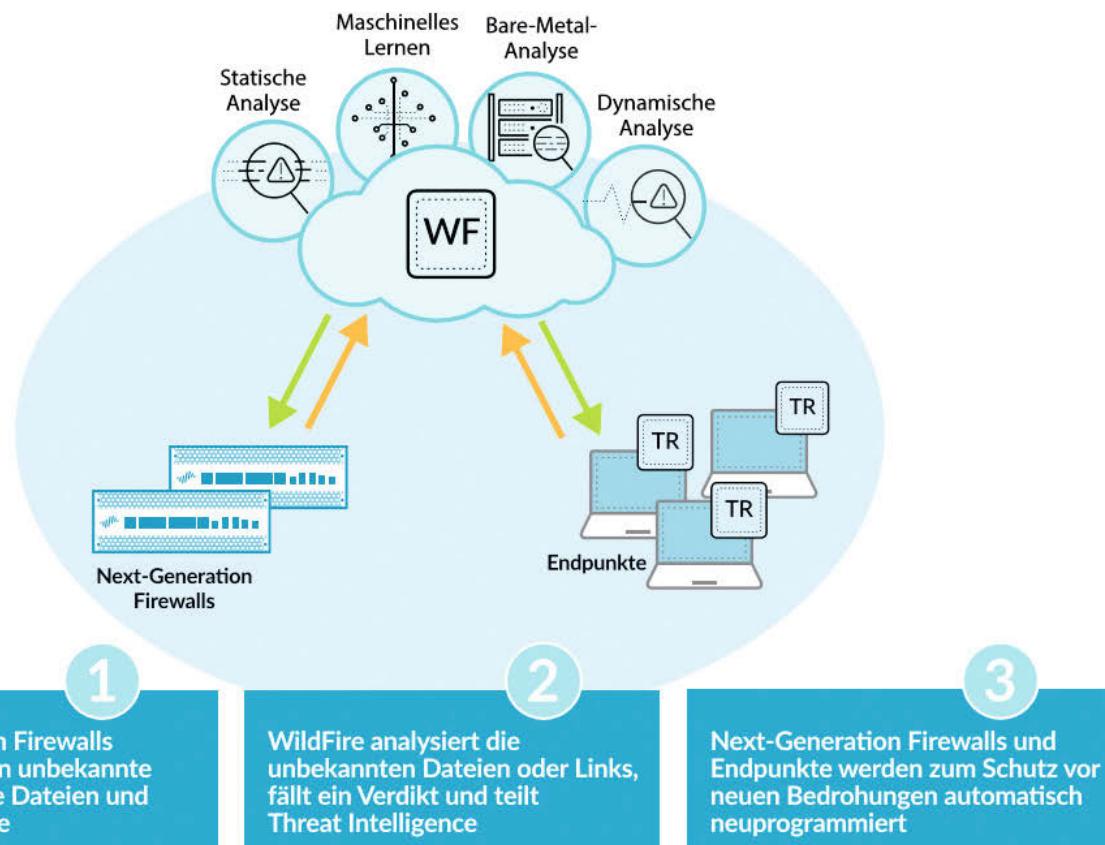
definieren, was beispielsweise schädliche Daten sind, wie solche Daten zu analysieren und welche Datensätze entsprechend zu untersuchen sind. Das ist auch bei modernen Ansätzen mit maschinellem Lernen zunächst immer noch der Fall. Allerdings besteht der große Vorteil darin, dass nicht mehr wie früher Menschen jede Anpassung laufend manuell durchfüh-

ren müssen. Mit maschinellem Lernen können die Systeme das nach einer entsprechenden Lern- und Trainingsphase selbstständig und sehr viel schneller als Menschen erledigen.

Auch können die Systeme sehr viel größere Datensätze in überschaubaren Zeiträumen durchsuchen, schneller als dies Menschen je möglich wäre. Sie können die relevanten Daten

herausfiltern und dabei Verhaltensweisen und Angriffsmethoden analysieren. Gerade das Erkennen von Verhaltensweisen steht besonders im Fokus: Da es nur eine begrenzte Anzahl sinnvoller und Erfolg versprechender Möglichkeiten gibt, ein System zu infizieren, können KI-Lösungen solche Verhaltensweisen erkennen und Abwehrmethoden einleiten.

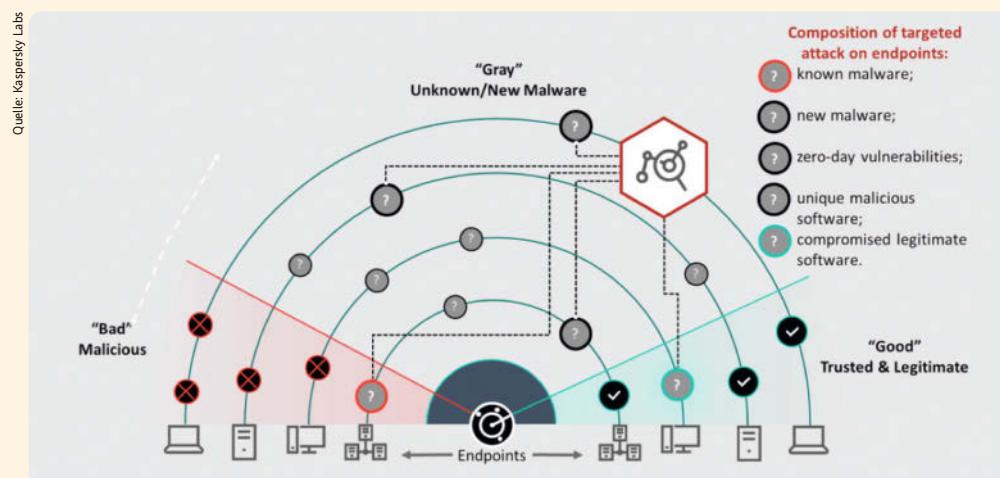
Quelle: Palo Alto Networks



Ganz gleich, ob sich die Produkte als „Next Generation“ oder nur einfach als EDR-Ansätze verstehen — fast alle modernen Schutzsysteme für die Endpunkte greifen auf die eine oder andere Art auf ML (Machine Learning) oder andere Methoden künstlicher Intelligenz zurück (Abb. 1).

geben wird – die Gefahren durch sich ständig ändernde Angriffsvektoren erfordern eine Abwehrtechnik, die ebenso wandelbar ist.

Hier kommt EDR (siehe Abbildung 1) ins Spiel: Diese Abkürzung steht für Endpoint Detection and Response, die Analysten von Gartner bezeichnen sie auch als Endpoint Threat Detection and Response. Eine ganze Reihe unterschiedlicher Techniken fällt unter diesen Begriff. Dazu zählen neben den verhaltensbasierten Analysen die Anwendungskontrolle, das maschinelle Lernen sowie anpassbare Sandboxes und die Sicherheitslückenprävention. EDR



Das wichtigste Ziel von EDR ist das Erkennen neuer, unbekannter und zuvor nicht erkannter Bedrohungen. Insbesondere analysieren solche Produkte Ereignisse und Prozesse, die sich in einer Grauzone befinden (Abb. 2).

Vertrauenswürdige IT-Sicherheit made in Germany

Wir sind immer da aktiv, wo viel auf dem Spiel steht. Wo sensible Daten und Identitäten elementare Werte von Behörden und Unternehmen sind. Wo Kunden in Sicherheitsfragen vor komplexen Herausforderungen stehen.

Unsere Spezialisten schützen Staat, Gesellschaft und Wirtschaft zuverlässig vor Cyberbedrohungen. Wir haben die IT-Sicherheitslösungen für digitale und vernetzte Infrastrukturen – und das bis zu höchsten Anforderungen an die Vertraulichkeit.

www.secunet.com



secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland

hat hauptsächlich ein Ziel: die proaktive Erkennung neuer und unbekannter Bedrohungen sowie von Infektionen, die zuvor nicht erkannt wurden.

Dabei werden Ereignisse und auch Prozesse analysiert, die sich vom System aus gesehen in einer Grauzone befinden (Abbildung 2). Das ist ein Bereich, in dem alle Objekte (und auch Prozesse) zu finden sind, die noch nicht als „vertrauenswürdig“ oder „definitiv schädlich“ einge-

stuft wurden. Die EDR-Komponenten besitzen grundsätzlich mehr Kapazitäten, um auf diese Art und Weise auch unbekannte Bedrohungen schneller und weiters genauer zu identifizieren und eine entsprechende Reaktion anzustoßen.

Fazit

Wenn es darum geht, Endpunkte zuverlässig zu schützen, müssen EPP und EDR Hand in Hand ar-

beiten: Die EPP-Lösungen helfen mittels Erkennung und automatischer Blockierung weitverbreiteter bekannter Bedrohungen dabei, die große Zahl kleinerer Angriffe zu bekämpfen. Wenn es aber um zielgerichtete Angriffe, die sogenannten Advanced Persistent Threats (APT), geht, dann können EDR-Techniken diese weiters zuverlässiger und effizienter analysieren.

Nach dem Erkennen und Analysieren können sie die Ein-

schätzungen direkt an die Plattform für den Endpunktsschutz weiterleiten. Die beiden kombinierten Techniken EPP und EDR bieten auf diese Weise einen integrierten Ansatz für möglichst umfassende Sicherheit und einen weitgehenden Schutz an den Endpunkten auch vor fortgeschrittenen und komplexen Bedrohungen. (ur@ix.de)

*Frank-Michael Schlede
ist freier Journalist für IT in Pfaffenhofen.*

Hase und Igel

Stand der Malware-Industrie

Cyberkriminelle gehen mit der Zeit und erarbeiten sich Zugang zu neuen Geschäftsfeldern. Zukunftsmärkte wie das Internet der Dinge und Kryptowährungen sind, neben den bisherigen einträglichen Geschäftsfeldern, lohnende Ziele. Doch auch die Malware-Entwicklung für die „klassischen Betriebssysteme“ gibt Anlass zur Sorge.

Analysen des aktuellen Sicherheitsreports des AV-TEST-Instituts geben keine Entwarnung. Laut den Messungen steigen die Malware-Zahlen für Betriebssysteme wie Windows, Android und macOS beständig an – einige dramatisch. So gab es seit Oktober 2017 eine Verdoppelung der monatlichen Malware-Neuentwicklungen. Lagen die Messwerte erfasster neuer Malware für alle Betriebssysteme im Oktober 2016 noch bei 7 629 305 Samples, verdreifachte sich dieser Wert bis zum Monat des

Folgejahres auf fast 17 445 659. Im Durchschnitt entwickeln Cyberkriminelle 3,9 neue Schadprogramme pro Sekunde (Abbildung 1).

Ideales Umfeld für digitale Erpressung

Das zurückliegende Jahr bot für Cyberkriminelle beste Bedingungen zur Verbreitung von Malware. Die erfolgreichsten Massenangriffe erfolgten dabei durch das Ausnutzen unpatchter Sicherheitslücken in Standardsoftware: Mit Cloud-

bleed etwa offenbarte sich Angriftern eine massive Sicherheitslücke in der auf Millionen Websites eingesetzten Serversoftware von Cloudflare. Und das Bekanntwerden der vorher lange heimlich durch die NSA genutzten Sicherheitslücke Eternal Blue bot die Möglichkeit, umfangreiche Ransomware-Kampagnen mit Schädlingen wie WannaCry, NotPetya und Bad Rabbit zu starten – die nach wie vor anhalten, wenn auch mit sinkendem Wirkungsgrad.

Besonders drastisch fielen die Folgen der Ransomware-Angriffe durch die Malware NotPetya aus. Allein das global agierende Logistikunternehmen Maersk meldete eine Schadenssumme von mehreren Hundert Millionen Dollar. Durch den Angriff der Ransomware im letzten Jahr erlitt es einen nahezu Totalausfall aller IT-Systeme. Auch andere Großunternehmen gehörten zu den Opfern, darunter der Pharmareise Merck, der durch den NotPetya-Angriff eine Schadenssumme von über 300 Millionen beklagte, und das Logistikunternehmen FedEx. Gemeinsam hatten alle Betroffenen, dass sie die vorwiegend in der Ukraine eingesetzte Steuersoftware MeDoc auf ihren Systemen hatten.

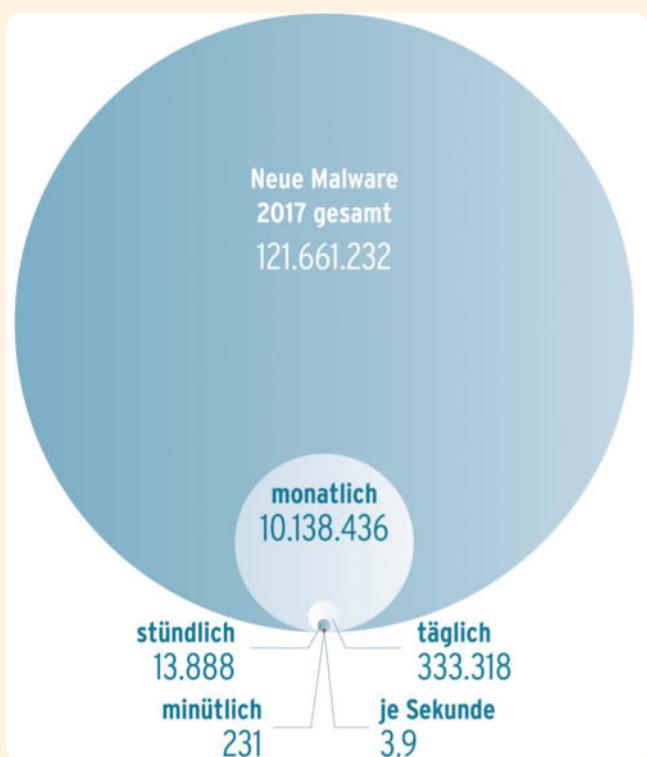
Bei den NotPetya-Angriffen nutzten die Täter genau dieselben Windows-Lücken, die schon vorher für staatliche Angriffe herhalten mussten – allerdings kamen diese aus einer ganz anderen Ecke. Bereits im August 2016 veröffentlichte die Hackergruppe „Shadow Brokers“ Teile

des Programmcodes einer Cyberwaffe, die sie bei einem Hack der NSA-Abteilung „Equation Group“ erbeutet hatte. Diese 256 MByte große Datei ließ 2016 zumindest erahnen, welches Potenzial in dem staatlich entwickelten Schadcode steckt. Brisant wurde die Situation jedoch erst im April 2017, als die Shadow Brokers den kompletten Code der Cyberwaffe im Internet veröffentlichten – die Geburtsstunde der Ransomware WannaCry.

Updates sind Pflicht

Dass das möglichst zeitnahe Aufspielen von Patches ein Muss ist, zeigt sich deutlich am Beispiel der WannaCry-Angriffe. Wie lange die NSA die nun frei zugänglichen Exploits namens Eternal Blue im Server Message Block (SMB) nahezu aller Windows-Systeme (CVE-2017-0144) bereits nutzte, ist umstritten. Schätzungen gehen von über fünf Jahren aus. Fakt ist, dass Microsoft die Lücken des Netzwerkprotokolls als „MS17-010 – Kritisch“ am 14. März 2017 patchte. Mitte Mai starteten die ersten groß angelegten Cyberattacken von WannaCry. Und wie sich herausstellte, war auf mindestens 230 000 Computern in 150 Ländern für zwei Monate nicht das entscheidende Sicherheitsupdate von Microsoft installiert worden. Zu den Betroffenen zählten vor allem Krankenhäuser in Großbritannien, aber auch große Unternehmen wie FedEx, Renault, Nissan, die Deutsche Bahn sowie der chinesische Ölkonzern PetroChina.

Im ersten Quartal dieses Jahres präsentierte sich die Entwicklung neuer Ransomware dagegen rückläufig. Deren Anteil im Verhältnis zur Malware-Gesamterfassung sank von 1,78 auf 1,38 Prozent. Ein Wert, der allerdings noch keine validen Aussagen über die Entwicklung der Schädlingsgattung im gesamten Jahr 2018 erlaubt. Zu vermuten ist jedoch, dass Cyberkriminelle durch die mit Ransomware gemachten Erfahrungen ein neues und lukrativeres, auf Kryptowähr-



Keine Entwarnung bei der Malware-Entwicklung: Die Anzahl an neuen Schädlingen ist alarmierend hoch (Abb. 1).

rungen basierendes Erwerbsmodell gefunden haben.

Die Anonymität vieler Kryptowährungen garantiert Cyberkriminellen optimale Geschäftsgrundlagen. Denn Bitcoin & Co. erlauben das direkte Abkassieren von Opfern ohne das Zwischenschalten von „Handlern“. Damit minimiert sich das Risiko bei gleichzeitiger Einsparung von „Personalkosten“. Daraum setzen auch kriminelle Vorwerker auf die Blockchain. 2017 entwickelte die Malware-Industrie zunehmend Schadcode zum Schürfen digitaler Währungen unter Missbrauch fremder Ressourcen.

Anstatt die Cyberwährung von ihren Opfern über Ransomware zu erpressen, gingen die Kriminellen zunehmend dazu über, die Rechenleistung infizierter Hardware zum Coin-Mining zu missbrauchen. Lag die Zahl der Neuentwicklungen von Mining-Malware Mitte 2017 noch bei durchschnittlich 3500 Samples pro Monat, verdoppelte sich deren Rate ab September und steigt seither quasi unbremst auf bis zu 470 000 neue Samples pro Monat.

Hochentwickeltes Krypto-Mining

Der Blick auf die Verteilung der Mining-Malware nach Betriebssystemen zeigt deutlich, dass sich die Kriminellen 2017 noch in der Entwicklung des Geschäftsmodells befanden. Zu diesem Zeitpunkt zielten über die Hälfte aller Coin-Miner auf Windows-Systeme (55,44 Prozent). Die andere Hälfte (44,13 Prozent) versuchte, die Rechenleistung infizierter Hardware über Browser und andere Internetverbindungssoftware abzusaugen.

Das änderte sich 2018 drastisch, denn die Anzahl an Coin-Minern für Windows-Systeme stieg überproportional um knapp 30 Prozent auf 84,69 Prozent an. Damit legen sich Cyberkriminelle, wie auch bei anderer Malware, auf die für sie bewährten Windows-Systeme als Hauptangriffsziel fest (Abbildung 2). Ob es sich lediglich um

einen Trend handelt, bleibt abzuwarten.

Möglicherweise ist die höhere zu erbeutende Rechenleistung gegenüber Plattformen wie Android oder unterschiedlichen IoT-Geräten ein Argument, auf Windows zu setzen. Allerdings riskieren Angreifer hier aufgrund der hohen Verbreitung von Antivirensoftware auch, dass ihre Mining-Malware leicht entdeckt wird.

Wiedergeburt der Banking-Trojaner

Angriffe durch Banking-beziehungsweise Passwort-Trojaner nahmen im Laufe des letzten Jahres stark zu und gipfelten Anfang 2018 in einer verschafften Rate neuer Samples gegenüber dem Vorjahr. Professioneller Schadcode, etwa Zeus, Neverquest und Gozi, bahnte sich seinen Weg auf fremde Systeme über infizierte E-Mail-Anhänge und gekaperte oder durch Kriminelle selbst erstellte Websites. Auf infizierten Systemen schalten sich die Schadprogramme in die Kommunikation ein, sobald infizierte Rechner Kontakt zu Bankenservern aufnehmen, und greifen meist durch manipulierte und umgeleitete Login-Websites und Formulare Einwahl- sowie Finanzdaten der Opfer ab. Zur Abwehr der ständig aktualisierten Malware-Versionen bedarf es ebenfalls ständig aktualisierter Scan-Engines mit neuestem Datenstand.

Die Angriffsintensität auf Googles Mobilplattform nimmt ebenfalls weiter zu: 2017 zielten 6,53 Prozent aller Schadprogramme auf Android-Geräte – im Vergleich zum Vorjahr eine Zunahme von 0,88 Prozentpunkten. Was marginal klingt, hat in Wirklichkeit eine durchschlagende Wirkung, denn bisher kommt auf den wenigsten Mobilgeräten unter Android eine Sicherheits-App, geschweige denn ein wirkungsvoller Virenschutz zum Einsatz. Gleichzeitig läuft auf mehr als jedem dritten weltweit genutzten Android-Gerät eine veraltete Version des Betriebssystems (Version 1.1 bis

5.1.1), für die keine Sicherheits-updates mehr zur Verfügung steht. Mit der aktuellen, uningeschränkt mit Sicherheits-updates versorgten Android-Version 8 alias „Oreo“ sind gerade einmal 5,2 Prozent aller Android-Geräte ausgestattet.

Wer von Android-Malware spricht, meint damit im Wesentlichen Trojaner. Mit über 90 Prozent aller Android-Schadprogramme sind sie das Allround-Werkzeug der Cyberkriminellen. Sie eignen sich sowohl zum Ausspähen von Daten als auch zum Nachladen weiteren Schadcodes. Das können beispielsweise höher spezialisierte Trojaner wie Ransomware sein. Und tatsächlich erfassten die AV-TEST-Systeme gegen Ende 2017 ein spürbares Beben von über 2,5 Prozent des Malware-Gesamtanteils im Bereich dieser Schädlingsgattung. Danach flachte die Welle der registrierten Erpresser-Schadcodes wieder auf kaum mess-

bare Werte ab. Dies könnte bedeuten, dass sich Ransomware auf Mobilgeräten für Kriminelle nicht auszahlt.

Ein Grund dafür ist sicherlich, dass sich die meisten Ransomware-Attacken bisher noch durch das Zurücksetzen der Geräte in den Werkszustand entschärfen lassen. Zudem dürfte die Zahlungsbereitschaft der Opfer deutlich geringer sein als bei infizierten PCs. Der Schutz von Android-Geräten, selbst solchen, die auf aktuellem Patch-Level sind, lässt sich durch den Einsatz guter Sicherheits-Apps deutlich ausbauen. In Anbetracht des genutzten Funktionsumfangs gibt es wenig Argumente, die für die Vernachlässigung der Sicherheit dieser Geräte sprechen.

Auch Apple braucht Schutz

Apple-Nutzer sind nur von einem verschwindend geringen

Anzeige



**ENDPOINT
PROTECTOR**

DLP auch für den Mac

Schnittstellenschutz und Container-Verschlüsselung für USB, die inhaltsbasierte Kontrolle von Datei-Transfers sowie die Suche nach sensiblen Daten auf Arbeitsplatzrechnern gehören zu den Aufgaben von Unternehmen bei der Durchsetzung von Sicherheits-Richtlinien und Regelungen wie der DSGVO.

Die Aufgabe, sensible Informationen vor Datenverlust durch Mitarbeiter zu schützen, besteht unabhängig vom Betriebssystem und betrifft gleichermaßen Mac-, Linux- und Windows-Rechner. Von einem Mac können ebenso gut Daten per E-Mail, über browserbasierte Anwendungen oder USB-Sticks die Firma verlassen wie von Linux-Rechnern oder Windows-PCs.

Die DLP-Lösung Endpoint Protector stellt die gesamte Funktionalität für Data Loss Prevention auch für den Mac zur Verfügung. Sie berücksichtigt bei der Inhaltskontrolle im Modul Content Aware Protection Austrittspunkte wie Mail, Safari und andere Browser unter Mac, AirDrop, iBooks Author, iTunes oder Thunderbold-Schnittstellen. Mit dem Modul eDiscovery werden auch auf dem Mac unstrukturierte sensible Daten aufgespürt. Das Modul Device Control überwacht den Datentransfer auf externe Datenträger wie USB-Sticks und andere Geräte. Mit der Container-Verschlüsselung EasyLock sind Daten auf USB-Sticks geschützt. Endpoint Protector stellt lückenlosen Schutz in heterogenen Umgebungen sicher.

www.endpointprotector.de

Anteil neu programmiert Malware betroffen, allerdings steigt die Malware-Quote für das Apple-Universum kontinuierlich an. Im letzten Jahr stellte das AV-TEST-Institut eine Zunahme der Malware für macOS um 370 Prozent gegenüber dem Vorjahr fest. Diese Entwicklung hält an und erreicht einen aktuellen Gesamtwert von insgesamt 78 929 Samples.

2017 handelte es sich bei vier von zehn Schadprogrammen für macOS um Trojaner (40,93 Prozent). Ansonsten spielten schädliche Skripte mit 12,66 Prozent eine herausragende Rolle. Viren, Würmer und andere, etwa auf Windows-Systemen relevante Malware-Gattungen sind auf Mac-Rechnern gar nicht oder bestens im geringen Maße vorhanden. Auch Ransomware-

Angriffe finden auf Mac-Systemen quasi nicht statt.

Die Dominanz von Trojanern bei macOS-Systemen setzte sich im 1. Quartal 2018 dramatisch fort, die Anzahl verdoppelte sich und erreichte über 86 Prozent der Gesamtsumme der für Apple geschriebenen Malware. Auch wenn die Verbreitung von Mac-Malware wie OSX.MaMi, Crossrider und X-agent im Vergleich zu Windows und Android gering erscheint, ist die Plattform aufgrund der geringen Verbreitung von Sicherheitssoftware interessant für Kriminelle.

IoT: Massen ungeschützter Geräte

Sollten selbst vorsichtige Schätzungen von Marktforschungs-

unternehmen zutreffen, werden bis 2020 weltweit über 830 Millionen Wearables und 20,8 Milliarden vernetzte Geräte im Einsatz sein. Solche Zahlen begeistern nicht nur Unternehmen, sondern auch Cyberkriminelle. Und so entsteht eine brisante Mischung: Auf der einen Seite stehen Produkthersteller ohne Fachwissen im Bereich IT-Sicherheit, die schnell ihre Produkte auf den boomenden Markt werfen wollen. Auf der anderen Seite lauert die Cyber-Mafia mit einem großen Arsenal bereits funktionierender und erprobter Schadprogramme für die Masse an Geräten und Onlineservices, die ihnen jede Menge Schwachstellen zur Verbreitung von Schadcode bieten.

Unter der erfassten Malware befindet sich Schadcode zur Ausnutzung der Rechenleistung internetauglicher Geräte für sogenannte DDoS-Angriffe (Distributed Denial of Service) nach dem Vorbild von Mirai. So etwa der Schädling Gafgyt alias Bashlite, der mit 21,52 Prozent Platz eins der Top Ten belegt. Dieser Linux-Trojaner ist in der Lage, jedes ungepatchte Unix-basierte Betriebssystem zu infizieren. Verläuft die Infektion erfolgreich, verbreitet sich Gafgyt wie ein Internetwurm im ange schlossenen Netzwerk. Der Schädling zwingt vor allem IP-Kameras und digitale Videorekorder in sein Botnetz, das dann unter anderem für DDoS-Attacken eingesetzt wird.

Die über die IoT-Malware Mirai durchgeführten Angriffe verknüpften zeitweise über 500 000 infizierte IP-Kameras und digitale Videorekorder zu einem der bisher größten Botnetze der Welt. Über DoS-Attacken wurden dabei weite Teile des Internets lahmgelagert. Später wurde das per Mirai erzeugte Botnetz für DDoS-Erpressungen gegen große Provider und Diensteanbieter genutzt. Nach wie vor kommt der erfolgreiche Schadcode in modifizierten Fassungen zum Einsatz. Für Kriminelle bleibt der Schadcode weiterhin attraktiv, da für viele IP-Kameras sowie andere gefährdete IoT-Geräte weder Secu-

rity- noch Firmware-Updates zur Verfügung stehen, teilweise nicht einmal eine entsprechende Update-Funktion.

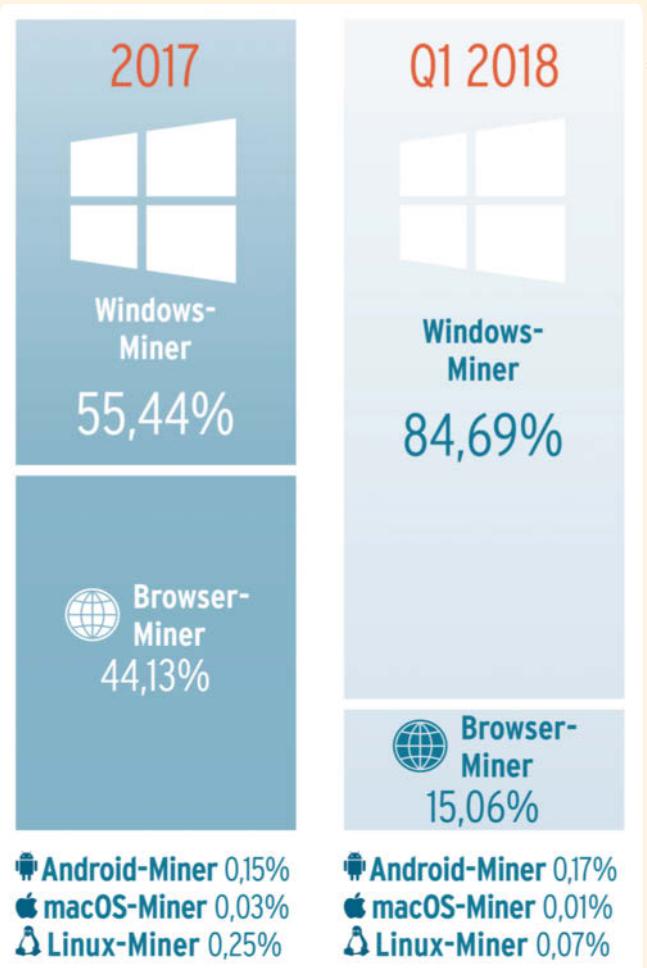
Neben dem Aufbau großer Botnetze rückt mit Millionen ungeschützter IoT-Geräte ein weiterer krimineller Geschäftsplan der Cyberkriminellen in den Vordergrund. Denn was liegt näher, als die weitestgehend ungeschützte und immer weiter steigende Rechenleistung von IoT-Produkten zum Schürfen von Kryptowährungen einzusetzen. Für IoT- und Smart-Home-Infrastrukturen können Angreifer Schadprogramme auf Linux-Basis zum Einsatz bringen, um die Geräte-CPUs für sich arbeiten zu lassen. Während Coin-Miner anfangs noch die volle CPU-Leistung für das Schürfen von Bitcoin & Co. nutzten und Geräte bis zum Ausfall an ihre Leistungsgrenzen führten, reguliert die neue Generation die genutzte Leistung und verhindert so den Ausfall des infizierten Wirtssystems. Zudem führt diese Strategie dazu, dass die infizierten Geräte weniger leicht zu erkennen sind und damit für einen längeren Zeitraum zur Verfügung stehen.

Seit Anfang 2018 entwickeln Kriminelle über 300 neue Varianten der lukrativen Schädlingsgattung pro Monat. Derzeit ist davon auszugehen, dass diese Entwicklung in absehbarer Zeit auf hohem Niveau stagnieren wird, denn Cyberkriminelle können auf eine wachsende Zahl meist ungeschützter IoT-Geräte zugreifen. Dementsprechend besteht für sie kein Entwicklungsdruck. Allerdings wird die qualitative Entwicklung der Coin-Miner weitergehen, und es werden zunehmend Samples mit ausgefeiltem CPU-Management zu sehen sein. Nutzer von IoT-Geräten sollten beim Kauf neben dem Funktionsumfang auch klar die Sicherheit der Geräte im Fokus haben.

(ur@ix.de)

Olaf Putsche

ist CCO des AV-TEST-Instituts in Magdeburg und Mitglied in Beiräten von Behörden und Wirtschaftsverbänden zum Thema IT-Sicherheit.



Cyberkriminelle setzen nach einer Erprobungsphase verstärkt auf Windows-Plattformen für ihre illegalen Schürfaktionen – vermutlich aufgrund der höheren zu erbeutenden Rechenleistung als bei Android oder zahlreichen IoT-Geräten (Abb. 2).

Mannheim, Congress Center Rosengarten, 13.-16. November 2018

Die Konferenz für
Continuous Delivery und DevOps

Die Konferenz zu
Docker, Kubernetes und Co.

Jetzt anmelden!

// CONTINUOUS CONTINUOUS

Auswahl aus dem Programm:

- Continuous Delivery – Mehr als eine Pipeline
- Warum funktioniert Continuous Delivery nicht?
- Jenkins X – Continuously Driving the Cloud
- Qualitätsziele kontinuierlich im Auge behalten
- Infrastructure as Code: Tests und Monitoring
- Observability for Spring Boot Applications
- Terraform-Deployments mit InSpec überprüfen

Workshops:

- Continuous Deployment im Embedded-Umfeld
- DevOps-Discovery-Workshop mit Lego und Schokolade

// VENI, VIDI, CONTAINER!

Auswahl aus dem Programm:

- Developer Experience mit Kubernetes steigern
- On-Premises-Containerisierung mit Microsoft TFS und Docker EE
- Kubernetes-Sicherheit 101
- Serverless und Functions as a Service mit Docker und OpenFaaS
- Istio Service Mesh
- Integrationstests mit Testcontainern

Workshops:

- Container-Orchestrierung mit Kubernetes
- Docker: Schnelleres Container-Deployment

Platin-Sponsor:



Gold-Sponsoren:



Silber-Sponsoren:



Bronze-Sponsor:



Veranstalter:



Einlasskontrolle

Zugriffssteuerung via Cloud Access Security Broker

Cloud Access Security Broker schaffen eine zentrale Stelle für die Steuerung des Zugriffs auf Cloud-Dienste von allen Benutzern, ob innerhalb oder außerhalb des Unternehmens und auf jedem Gerät.

Sogenannte CASBs (Cloud Access Security Broker) haben in den letzten Jahren deutlich an Popularität gewonnen. Es handelt sich um Cloud-Dienste, die zusätzliche Sicherheitsfunktionen für den Zugriff auf andere Cloud-Dienste bereitstellen, indem sie diesen faktisch vorgeschaltet werden. Sie sollen Herausforderungen meistern, die sich durch Sicherheitsgeräte und -software wie Enterprise Network Firewalls, Web Application Firewalls und andere Formen von Web-Access-Gateways nicht lösen lassen.

Schatten-IT bereitet Probleme

Unternehmen wollen durch Einsatz von Cloud-Diensten von deren Vorteilen der Bereitstellung (keine lokale Installation), der Flexibilität (Elastizität in der Nutzung) und des Preises (Abrechnung nach Nutzung und idealerweise geringere Kosten) profitieren. Doch eines der Kernprobleme dabei ist neben

den oftmals unzureichenden Sicherheitsfunktionen der Cloud-Services die sogenannte Schatten-IT, also IT-Funktionen, die Mitarbeiter und Partner an der verantwortlichen IT-Organisation vorbei nutzen. Verantwortliche in Fachabteilungen können Cloud-Dienste bestellen, ohne dafür ein Risiko-Assessment oder den Einfluss auf die Compliance berücksichtigen zu müssen, und mobile Endgeräte ermöglichen den Zugriff auf diese Dienste, ohne jemals den Perimeter der Organisation zu berühren.

Auf der anderen Seite sind Cloud-Dienste und ihre Verwaltung bisher noch nicht gut in die normalen IT-Prozesse, die Sicherheitsverfahren und die Access-Governance-Prozesse integriert. Dabei stellt sich die berechtigte Frage, ob es dafür einer gesonderten Lösung bedarf. Die Praxis zeigt, dass die meisten Cloud-Dienste im Bereich Sicherheit ebenso wie beim Identity- und Access-Management bestenfalls in Teilberei-

chen über Standards verwaltet und gesteuert werden können und oft wesentliche Sicherheits- und Governance-Funktionen vermissen lassen.

Ebenso ist es in weiten Bereichen bis heute nicht gelungen, das Management von Sicherheit und Governance in ausreichender Form in Cloud-Diensten zu integrieren. Ergänzende und alternative Lösungen, die für sich genommen nicht ausreichen, sind in der Tabelle „Abgrenzung CASB von anderen Sicherheitsdiensten“ im Vergleich mit CASBs aufgeführt. Dazu gehören das Rights Management, also das Verschlüsseln unstrukturierter Daten mit den Metadaten definierten Zugriffsberechtigungen, Data Leakage Prevention, Web Access Gateways und Access Governance.

Eine zusätzliche Sicherheitsschicht

Hier kommen CASBs ins Spiel, indem sie eine zusätzliche, auf

Cloud-Services ausgerichtete Schicht für den Schutz und die Kontrolle dieser Dienste schaffen. Zu den grundlegenden Funktionen gehört die Möglichkeit zu erkennen, welche Cloud-Dienste genutzt werden, von wem sie genutzt werden und für welche Daten. Dies gilt insbesondere für den Datenverkehr, der das Unternehmen verlässt, respektive für bekannte Anwendungen durch Analyse des dort eingehenden Datenverkehrs aus der jeweiligen Organisation, also beim Mandanten für diese Organisation.

Darüber hinaus gehören weitere Funktionen zum Funktionsumfang typischer CASBs. Im Mittelpunkt steht die Zugriffssteuerung, also die Steuerung darüber, wer welche Funktionen von Cloud-Diensten in welcher Weise nutzen darf. Sobald der Dienst bekannt ist, kann der Datenverkehr durch den CASB geleitet werden, der damit dann als Gateway fungiert. Damit können dann auch Zugriffskontrollen bei dem CASB umgesetzt werden.

CASBs integrieren zunehmend Funktionen auch aus anderen Bereichen, um einen umfassenderen Schutz beispielsweise in enger Verzahnung mit DLP-Funktionen (Data Leakage Prevention) bieten zu können. Weitere Features umfassen ergänzende Sicherheitsdienste wie das Verschlüsseln und Blockieren bestimmter Daten, Compliance-Reporting

Abgrenzung CASB von anderen Sicherheitsdiensten

	Erkennung	Steuerung	Schutz
Rights Management	können manchmal bestimmte Arten von Daten erkennen und klassifizieren	individuelle Zugriffe auf unstrukturierte Daten	gegen unberechtigte Zugriffe auf Dateien, auch wenn diese weitergeleitet werden oder unbefugt in fremde Hände gelangen
Data Leakage Prevention	bestimmter Arten von Daten, die gespeichert oder übertragen werden	warnen, berichten, Daten isolieren, entfernen, Übertragung verhindern	gegen unzulässige Speicherung und Übertragung bestimmter Arten von Daten
Secure Web Gateway	Zugriffe auf URLs	Welche URLs dürfen genutzt werden? Filterung von Malware	Einige unterstützen die Verschlüsselung und Pseudonymisierung von Daten.
Access Governance	von Benutzern, Rollen und Berechtigungen	über Berechtigungen gegen Richtlinien und SoD-Regeln (Segregation of Duties, Funktionstrennung)	Durchsetzung der Änderung von Berechtigungen, die gegen Richtlinien und Regeln verstossen
Cloud Access Security Broker	Wer greift auf welchen Cloud-Dienst zu?	granulare Steuerung, wer welche Transaktionen von welchem Gerät aus durchführen darf	gegen unberechtigten Zugriff auf bestimmte Dienste, Transaktionen und Daten

und den generellen Schutz vor bekannten Angriffsmustern.

Im Laufe der Entwicklung hat sich der Markt für CASBs signifikant verändert. Eine Reihe von Start-up-Unternehmen, die meist mit stark spezialisierten Lösungen für Einzelfunktionen wie das Erkennen der genutzten Cloud-Dienste gestartet waren, wurden zwischenzeitlich von großen Cloud- und Security-Anbietern übernommen. Damit vergrößert sich auch der Funktionsumfang, insbesondere bezüglich des Schutzes vor Cyberangriffen und bei der Integration in DLP-Funktionen. CASBs werden damit immer mehr zu einem Bestandteil umfassender Sicherheitslösungen für Unternehmen.

Fazit

Mit der wachsenden Nutzung von Cloud-Diensten durch Organisationen ist es faktisch unvermeidlich, sich auch mit

CASBs zu beschäftigen. Sie sind in gewisser Hinsicht nur eine Notlösung, weil die Sicherheit von Cloud-Diensten nicht alleine über Standards und vorhandene

Enterprise-Lösungen für IT-Sicherheit zu erreichen ist. Aber schon mangels Alternativen sind sie daher auch unverzichtbar, um den Schritt in die Cloud sicherer

zu gestalten, als es ohne CASBs möglich ist. (ur@ix.de)

Martin Kuppinger
ist Gründer und Analyst von
KuppingerCole.

In iX extra 11/2018 Hosting: Cloud-Geschäftsmodelle

Wurden flexible Abrechnungsmodelle von Cloud-Providern wie Amazon und Google von deutschen Hosting-Providern zunächst als Bedrohung empfunden, so haben viele von ihnen inzwischen vergleichbare

Services in Form von VPS oder Cloud-Speicher im Portfolio. Darüber hinaus entwickeln sich Kooperationen und mehrstufige Hosting-Modelle, bei denen Softwareprovider ihrerseits Infrastrukturen und Plattformen

wie AWS oder Azure nutzen. So können innovative Provider schnell neue Dienste wie Communications as a Service oder Container as a Service zur Verfügung stellen, ohne dafür eine eigene Infrastruktur aufzubauen.

Die weiteren iX extras:

Ausgabe	Thema	Erscheinungstermin
02/2019	Embedded Computing: Neuheiten zur embedded world	24.01.2019
03/2019	Hosting: Hosted E-Commerce	21.02.2019
05/2019	Cloud-Computing: Cloud-Sicherheit	25.04.2019
10/2019	Security: Trends und Produkte zur it-sa	26.09.2019

Heidelberg, Print Media Academy,
16.-18. Oktober 2018

// heise
devSec()

Die Konferenz für sichere Software- und Webentwicklung

Sichere Software beginnt vor der ersten Zeile Code

AUSZUG AUS DEM PROGRAMM:

- „Scaling Security“ in Organisationen: Trampelpfade auf dem Weg zu höherer Softwaresicherheit – *Roland Brethauer*
- Kryptografie in der Praxis – *Severin Wischmann*
- Sicherheit & IoT – Stand der Gefährdung im Jahr 2018 *Stefan Strobel*
- Agile Penetrationstests und Continuous Delivery: Sichere Software von Anfang an – *Christoph Haas*

KEYNOTES:

- *Paula Januszkiwicz*, Gründerin der Sicherheitsfirma CQURE Inc.
- *Mikko Hypponen*, internationaler Sicherheitsexperte (F-Secure)

JETZT ANMELDEN!

- Daten speichern, löschen, Auskunft erteilen – Erste Erfahrungen mit der DSGVO – *Jörg Heidrich*
- Sicherheitsaspekte von Containern und Kubernetes *Thomas Fricke*
- Threat Modeling als Kompass durch moderne Softwarearchitekturen – *Bastian Braun*

WORKSHOPS:

- Kryptografie sicher nutzen – *Eric Bodden*
- Java Web Security – *Dominik Schadow*
- Passwort123! – Der richtige Umgang mit Credentials *Christoph Iserlohn, Jochen Christ*

Gold-Sponsoren



OPTiMA..bit
business information technology gmbh

Silber-Sponsoren

WIBU SYSTEMS

Sonatype

heidelpay
your all-in-one payment partner

inovex

RIGS IT

SYNOPSIS®

Bronze-Sponsor

INNOQ

Veranstalter

heise Security

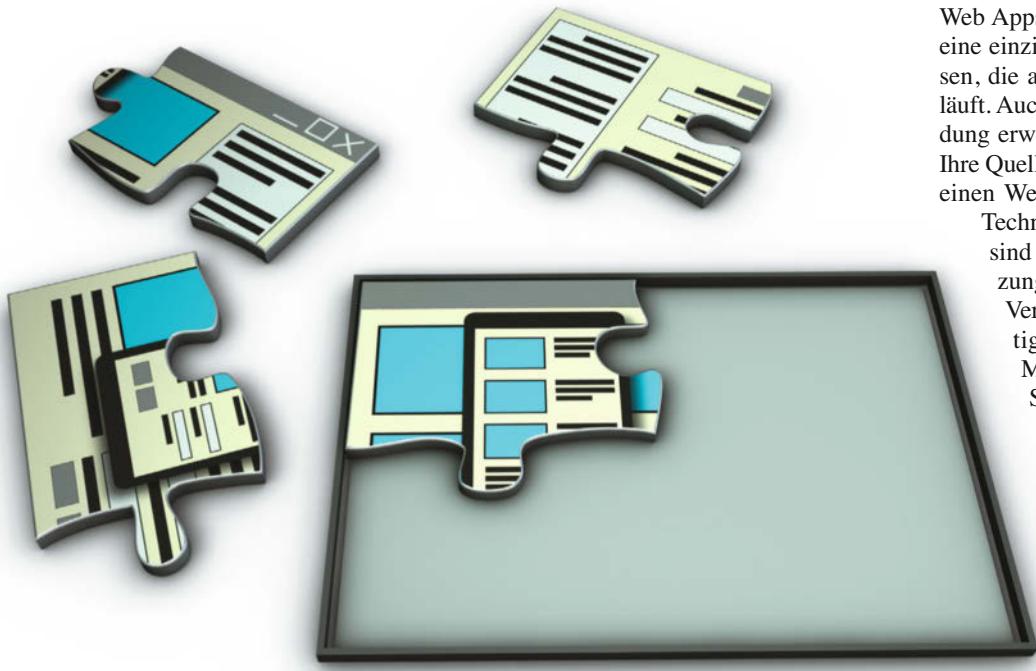
heise Developer

dpunkt.verlag

Tutorial: Progressive Web Apps mit Workbox, Teil 1

Fortschrittlich

Christian Liebel



Progressive Web Apps sind Webanwendungen, die sich wie lokal installierte Apps anfühlen. Ein wesentliches Element ist der Service Worker, der dafür sorgt, dass PWA auch ohne Netzwerkverbindung funktionieren.

Progressive Web Apps (PWA) sind das App-Modell der Zukunft: Schon seit einigen Jahren treibt Google ein Konzept voran, das Webanwendungen in auf dem Gerät installierte Apps verwandeln möchte. Dazu gehören native Features wie ein eigenes Symbol auf dem

Home-Bildschirm oder in der Programmliste des Systems, Push-Benachrichtigungen oder Offlinefähigkeit.

Das Anwendungsmodell funktioniert plattformübergreifend, vom iPhone über das Android-Tablet bis hin zum Windows-Desktop. Ausführungsumgebung sind die

Webbrowser, die seit dem Aufkommen von HTML 5 eine wahre Flut an modernen Webschnittstellen mit nativer Power erlebt haben: Mittlerweile ist es möglich, aus dem Webbrowser heraus auf Mikrofon und Kamera des Anwenders zuzugreifen oder hardwarebeschleunigte 2D- und 3D-Visualisierungen umzusetzen und darauf aufbauend Virtual-Reality-Anwendungen zu implementieren.

Für Entwickler haben Progressive Web Apps den Vorteil, dass sie nur noch eine einzige Anwendung schreiben müssen, die auf unterschiedlichen Systemen läuft. Auch die Bereitstellung der Anwendung erweist sich als besonders einfach: Ihre Quelldateien werden schlichtweg auf einen Webserver hochgeladen. Zentrale

Techniken bei Progressive Web Apps sind der Service Worker zur Umsetzung von Offlinefähigkeit und das Verschicken von Push-Benachrichtigungen sowie das Web App Manifest, das die Gestaltung des Symbols auf dem Home-Bildschirm und in der Programmliste konfiguriert.

Alle vier großen Browserhersteller sind mit ihren Webbrowsern an Bord: Google Chrome (ab Version 40), Mozilla Firefox (ab Version 44), Microsoft Edge (ab Version 17) und Apple Safari (ab Version 11.3).

Das Ausmaß der Unterstützung variiert jedoch je nach Browser, es stehen also nicht auf jedem Browser sämtliche PWA-Features zur Verfügung.

Das Konzept der Progressive Web Apps kommt zunehmend in der realen Welt an. So setzen bmw.com und lotto.de die oben genannten Techniken ein, um ihr Webangebot zu einem gewissen Grad auch offline verfügbar zu machen. Um Apps im engeren Sinne handelt es sich bei beiden Angeboten allerdings nicht. Vorzeigbare Progressive Web Apps, die diesen Namen verdienen, sind beispielsweise Twitter Lite (mobile.twitter.com), der offizielle mobile Client für das soziale Netzwerk, oder die Progressive Web App der Financial Times (app.ft.com).

In dieser und den kommenden drei Ausgaben der *iX* zeigen mein Kollege Steffen Jahr und ich, wie Sie Progressive Web Apps mit Googles Werkzeug Workbox entwickeln können. Im ersten Teil des Tutorials geht es um die Eigenschaften, die Progressive Web Apps auszeichnen, die Frameworkunabhängigkeit des Anwendungsmodells und Workbox als eine Lösung zur Entwicklung von PWA.

iX-TRACT

- Progressive Web Apps sind Webanwendungen, die sich wie lokal installierte Apps verhalten.
- PWA integrieren sich dazu in den Home-Bildschirm, den Programmstarter und den App Switcher und können Systembenachrichtigungen verschicken.
- Dank Service Worker funktionieren sie auch ohne Netzverbindung.

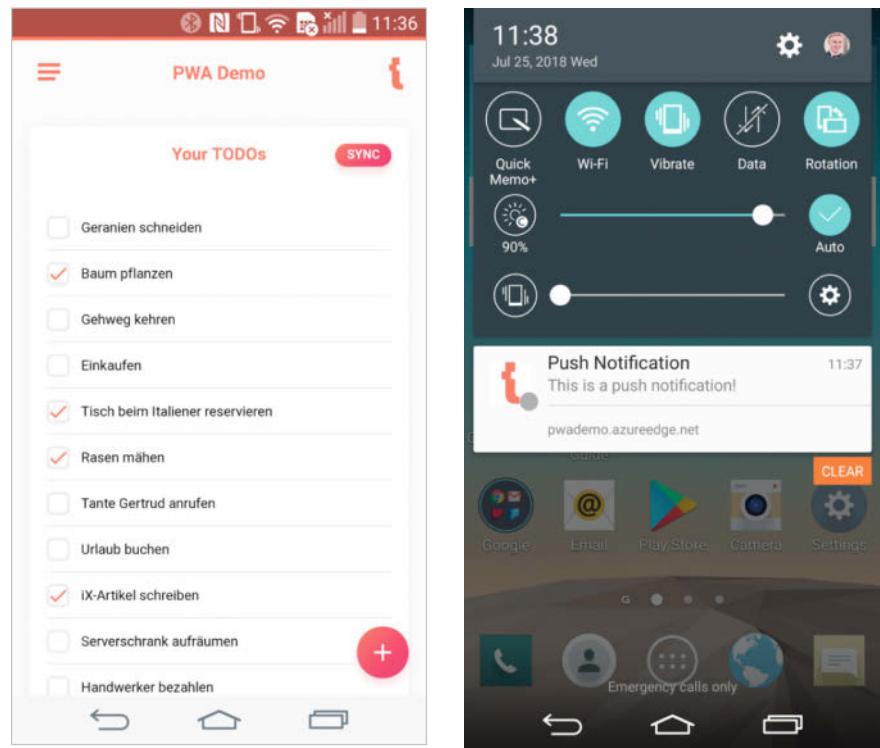
Der zweite Teil beschäftigt sich mit der Installation von PWA auf dem Home-Bildschirm und der Umsetzung von Push-Ereignissen auf nativer und Anwendungsebene. Themen von Teil 3 sind der technische Kern der PWA, der Service Worker, und Caching-Strategien, um Anwenderdaten und die Quelldateien der Anwendung offline zu halten. Schließlich stellen wir im vierten Teil einige moderne Webschnittstellen vor und geben eine Einschätzung, wann sich Investitionen in dieses Anwendungsmodell für Softwareentwickler lohnen.

Die DNA von Progressive Web Apps

Progressive Web Apps bezeichnen keine in sich geschlossene Technologie, sondern eher eine Sammlung von Eigenschaften, die eine solche Webanwendung umsetzen sollte. Die zehn Eigenschaften sind:

Progressiv: Nicht alle Webbrowser und -versionen, die Anwender weltweit verwenden, unterstützen sämtliche PWA-Schnittstellen. Eine Progressive Web App soll auf diesen Systemen allerdings dennoch laufen – zumindest im Rahmen des Möglichen. Dieses Prinzip nennt man Progressive Enhancement: Auf Systemen, die eine Unterstützung für die PWA-Schnittstellen mitbringen, erhält der Anwender eine bessere Benutzererfahrung. Auf keinen Fall darf die Anwendung wegen einer fehlenden Schnittstelle abbrechen.

Responsiv: Die Anwendung soll ein responsives Webdesign umsetzen. Dabei passt sich die Gestaltung der Anwendung



Progressive Web Apps sind von nativen Apps nicht zu unterscheiden (Abb. 1).

den zur Verfügung stehenden Bildschirmabmessungen an: Während auf Smartphones mit Fingereingabe Menüs eingecklappt und nur die wichtigsten Inhalte dargestellt werden, sind auf Desktop-Geräten zusätzliche Inhalte sichtbar und Steuerelemente lassen sich dichter beieinander platzieren, da die Maus eine präzisere Eingabe ermöglicht. Das stellt sicher, dass Anwender sowohl auf Smartphones als auch an einem Desktop-Arbeitsplatz

Die Beispiel-App versendet auch native Push-Benachrichtigungen (Abb. 2).

mit einem 27-Zoll-Bildschirm eine sinnvolle Benutzererfahrung haben.

App-like: Progressive Web Apps sollen Anwendungsrahmen (App-Shells) mit einer Navigationsstruktur, Übergangseffekten und Interaktionen wie Touch-Gesten implementieren, wie sie der Anwender von nativen Anwendungen kennt. Im Idealfall merkt der Anwender gar nicht, dass er gerade eigentlich mit einer Website interagiert.

2x Make testen und 6 € sparen!

Ihre Vorteile:

- ✓ Neu: Jetzt auch im Browser lesen!
- ✓ Zugriff auf Online-Artikel-Archiv*

Für nur 15,60 Euro statt 21,80 Euro.

* Für die Laufzeit des Angebotes.

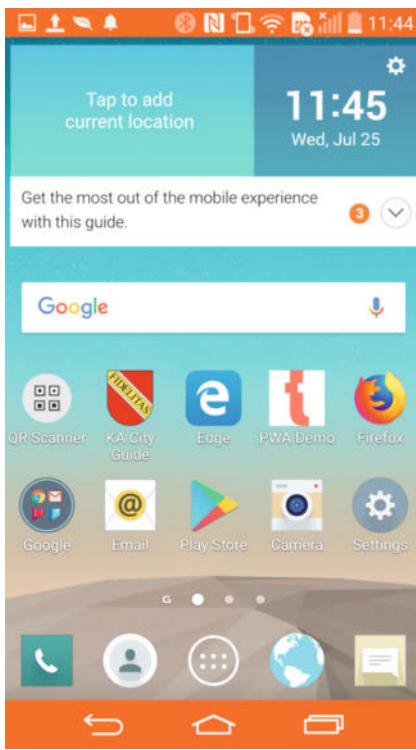
- ✓ Zusätzlich digital über iOS oder Android lesen
- ✓ Action-Buch für Maker GRATIS

Jetzt bestellen:

make-magazin.de/minibook

GRATIS!





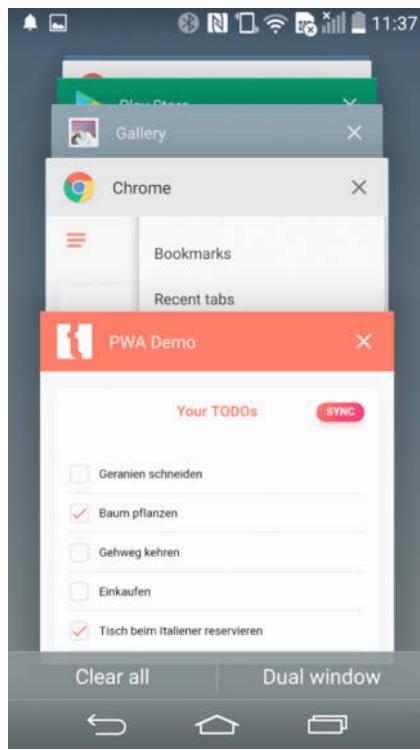
Die Beispiel-PWA lässt sich auf dem Android-Homescreen installieren (obere Zeile, zweites Icon von rechts) (Abb. 3).

Offlinefähigkeit: PWA sollen nicht von der Internetverbindung abhängen. Selbst wenn der Anwender komplett offline ist, müssen sie im Rahmen des Möglichen funktionieren – hier kommt der Service Worker ins Spiel. Die Eigenschaft der Offlinefähigkeit deckt zwei Aspekte ab: einerseits die Anwendungsquelldateien, sodass die App-Shell offline läuft, andererseits die Anwenderdaten. Kann ein Anwender Änderungen nicht abschicken, kann die App diese lokal zwischenspeichern und bei Bestehen einer Internetverbindung hochladen.

Aktuell: Wenn der Service Worker die Webanwendung lokal zwischenspeichert, müssen auf dem Webserver bereitgestellte Änderungen im Zwischenspeicher nachgeführt werden. Dazu gibt es einen Updateprozess, der sicherstellt, dass dabei keine Inkonsistenzen auftreten und die Anwendung immer schön frisch bleibt.

Zwang zur Verschlüsselung

Sicher: Da die PWA-Schnittstellen, allen voran der Service Worker, sehr mächtig sind, ist zum Einsatz dieser Schnittstellen eine Verbindung über das Hypertext Transfer Protocol Secure (HTTPS) erforderlich. Für die Transport Layer Security (TLS) muss ein entsprechendes Zertifikat



Der App Switcher unterscheidet nicht zwischen Progressive Web Apps und nativen Apps (Abb. 4).

auf dem Webserver installiert werden. Ausnahmen bestehen zu Entwicklungszwecken auf dem lokalen Rechner (localhost).

Auffindbar: Da Progressive Web Apps „nur Webseiten“ mit Zusatzfeatures sind, müssen sie von anderen Webseiten unterschieden werden können. Dafür sorgt das Web App Manifest mit verschiedenen Metadaten zur Webanwendung. Diese Datei können zum Beispiel Suchmaschinenbetreiber auswerten, um eine dedizierte Suche nach Progressive Web Apps anzubieten.

Re-engageable: PWA sollen in der Lage sein, ihre Anwender zum Wiederverwenden der App anzuregen. Dazu können sie – ganz wie native Anwendungen – Push-Benachrichtigungen an die Benachrichtigungszentrale des Systems senden. Das Prinzip kennt man von sozialen Netzwerken („Peter hat Ihr Bild kommentiert“) oder Free-to-play-Spielen („Sonderangebot: 300 gelbe Diamanten für nur 1,59 Euro“). Diese Funk-

tion ist unter Apple Safari derzeit nicht verfügbar.

Installierbar: Progressive Web Apps können ein Symbol auf dem Home-Bildschirm oder in der Programmliste des Anwenders erhalten (siehe Abbildung 3). Von dort ausgeführt, starten sie in einem eigenen Fenster mit nativer Fensterdecoration beziehungsweise auf Mobilgeräten im Vollbildmodus ohne Menü- und Statuszeilen des Webbrowsers. Darüber hinaus erscheinen sie im App Switcher (siehe Abbildung 4) und in der Taskleiste oder im Dock. Die Ausführungsumgebung bleibt aber weiterhin der Browser. Diese Funktion ist unter Microsoft Edge und Apple Safari auf dem Desktop derzeit nicht verfügbar.

Verlinkbar: Die letzte Eigenschaft ergibt sich schon aus der Struktur des Web: Auf Progressive Web Apps kann mithilfe eines Uniform Resource Locator (URL) verwiesen werden. Je nachdem, wie die Anwendung implementiert ist, besteht sogar die Möglichkeit, auf einzelne Sichten innerhalb der Progressive Web App zu navigieren. Die URL lässt sich als Lesezeichen im Browser anheften oder mit einem Kollegen teilen.

In diesem Tutorial demonstrieren wir die PWA-Schnittstellen mit einer Beispielanwendung, die To-do-Listen verwaltet. Die Eingaben des Anwenders werden im Zwischenspeicher persistiert, sodass sich auch bei schwacher oder fehlender Internetverbindung Änderungen an den To-do-Datensätzen vornehmen lassen. Die Beispielanwendung setzt alle genannten Eigenschaften von Progressive Web Apps um.

Es geht ganz ohne Framework

Die Eigenschaften von PWA lassen sich auf unterschiedlichste Weise umsetzen. Da grundsätzlich jede Website zur Progressive Web App werden kann, ist nicht einmal der Einsatz eines Frameworks erforderlich. Die App-Shell könnte beispielsweise auch mit jQuery implementiert werden.

Gut geeignet zur Entwicklung von Progressive Web Apps ist allerdings das Architekturmodell der Single-Page Applications (SPA). Diese lassen sich unter anderem mit Angular, React oder Vue.js implementieren. SPA-Frameworks bringen oft Architekturelemente zur Strukturierung von Webanwendungen mit, sodass sich selbst größere Anwendungen problemlos ins Web bringen lassen. Die in diesem Tutorial vorgestellte Beispielan-

Tutorialinhalt

Teil 1: Eigenschaften von PWA

Teil 2: Systemintegration

Teil 3: Service Worker und Caching-Strategien

Teil 4: Moderne Webschnittstellen für PWA

Listing 1: Workbox-Konfigurationsdatei

```
module.exports = {
  "globDirectory": ".",
  "globPatterns": [
    "**/*.html"
  ],
  "swDest": "sw.js"
};
```

wendung haben wir mit Angular entwickelt, werden allerdings auf Implementierungsdetails jenseits der PWA-Aspekte nicht näher eingehen. Ein dreiteiliges Angular-Tutorial finden Sie in *iX* ab Ausgabe 5/2017.

Workbox erleichtert die Entwicklung von PWA

Das Herzstück von Progressive Web Apps ist der Service Worker. Die Implementierung des Service Workers ist eine völlig eigene Disziplin, da es sich hierbei um Infrastrukturcode handelt: Der Service Worker stellt einen zentralen Adapter dar, der entscheidet, ob eine Anfrage der Webanwendung über das Netz oder aus dem lokalen Cache des Browsers bedient wird. Somit wird die Implementierung unterschiedlicher Caching-Strategien möglich (Network-only, Cache-only, Cache-first-then-Network, Network falling back to Cache ...).

Das Angular-Framework bringt zwar schon ein Zusatzmodul für Progressive Web Apps mit, das einen passenden Service Worker für die Webanwendung generieren kann. Es erlaubt dabei aber nur einen sehr begrenzten Eingriff in den generierten Code. Die größten Freiheiten hat der Anwender, wenn er den Service Worker vollständig selbst implementiert. Da dies bei Anpassungen der Anwendung aber zur lästigen Aufgabe werden kann, gibt es auch einen Mittelweg: Workbox 3.0. Dieses Toolkit von Google kann ebenfalls Service Worker generieren, allerdings kann der Entwickler hier eigenen Code in den Service Worker einfügen und Workbox nur einen Teil des Skriptes generieren lassen.

Das Workbox-Kommandozeilentool namens Workbox CLI lässt sich wie üblich über *npm* installieren; außerdem benötigt man zum Testen das Tool *lite-server*:

```
npm i -g workbox-cli lite-server
```

Zum Start legt man in einem neuen Verzeichnis eine leere Datei namens *index.html* an und führt in diesem Verzeichnis den Befehl

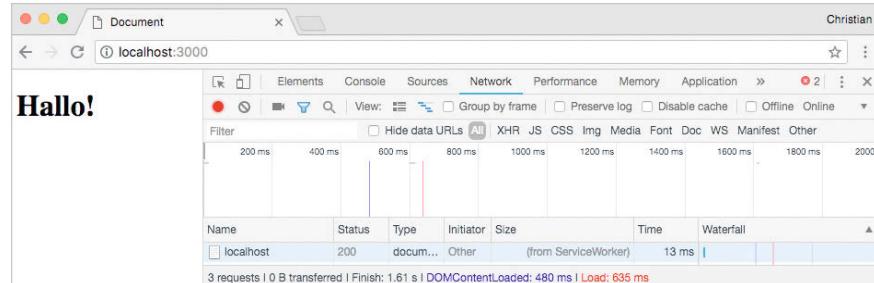
```
workbox wizard
```

Listing 2: Durch Workbox generierter Service Worker

```
importScripts("https://storage.googleapis.com/workbox-cdn/releases/3.4.1/workbox-sw.js");
self.__precacheManifest = [
  {
    "url": "index.html",
    "revision": "d41d8cd98f00b204e9800998ecf8427e"
  }
].concat(self.__precacheManifest || []);
workbox.precaching.suppressWarnings();
workbox.precaching.precacheAndRoute(self.__precacheManifest, {});
```

Listing 3: Service Worker auf der Website registrieren

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <title>Document</title>
</head>
<body>
<h1>Hallo!</h1>
<script>
  if ('serviceWorker' in navigator) {
    navigator.serviceWorker.register('/sw.js');
  }
</script>
</body>
</html>
```



Dass die Website gerade vom Service Worker ausgeliefert wird, ist in den Entwickler-tools am Eintrag „from ServiceWorker“ in der Spalte „Size“ zu sehen (Abb. 5).

aus. Auf der Kommandozeile stellt die Workbox-CLI nun verschiedene Fragen, etwa nach dem Root-Verzeichnis der Anwendung („.“) und danach, welche Dateitypen offline zwischengespeichert werden sollen (HTML). Auch bei den anderen Fragen kann man den Vorschlag übernehmen. Resultat ist die Konfigurationsdatei *workbox-config.js* (Listing 1).

Der Befehl *workbox generateSW* generiert nun den Service Worker (Listing 2). Um ihn zu verwenden, muss der Service Worker in der Datei *index.html* registriert werden. Listing 3 zeigt ein einfaches Beispiel.

Entwicklungsserver integriert

Der Befehl *lite-server* startet den Entwicklungsserver und öffnet die URL *localhost:3000* im Standardbrowser. Sollte dieser Browser die PWA-Schnittstellen nicht beherrschen, muss man die Adresse mit einem passenden Browser ansteuern. Wenn nun der *lite-server* mit *Ctrl + C* ab-

gebrochen wird, steht kein Server mehr zur Verfügung, der *index.html* ausliefern könnte – die Anwendung ist praktisch offline. Wenn man im Webbrowser jedoch die dargestellte Seite neu lädt, zeigt der Browser immer noch die Meldung „Hallo!“ an: Das ist der Service Worker in Aktion (Abbildung 5).

Zugegeben, dies ist nur ein sehr einfaches Beispiel, doch zeigt es schon deutlich eine der Kernfunktionen des PWA-Rückgrats, des Service Workers. Im nächsten Teil geht es um das Hinzufügen der Progressive Web App zum Home-Bildschirm und das Versenden von Push-Benachrichtigungen inklusive des dafür notwendigen Web-Push-Protokolls – dann am Beispiel der To-do-Demoanwendung. (odi@ix.de)

Christian Liebel

ist Consultant bei Thinktecture in Karlsruhe, wo er Cross-Platform-Apps auf Basis von Webtechnologien umsetzt. Für seine Communitybeiträge wurde er als Microsoft MVP in der Kategorie Developer Technologies ausgezeichnet.



Firebase als Backend-Dienst für Apps



Angefeuert

Thomas Künne

Google baut Firebase Stück für Stück zur zentralen Plattform für mobile Anwendungen aus. Entwickler können so das Backend der Cloud überlassen und sich auf die App konzentrieren.

X-TRACT

- Sowohl Anbieter als auch Nutzer erwarten von modernen Apps Backend-Dienste. Rein lokale Programme gibt es bei Mobilgeräten nur noch selten.
- Google bietet mit Firebase viele Funktionen für das Backend mobiler Apps an. Sie lassen sich mit Android wie mit iOS nutzen.
- Mit Firebase Functions lassen sich einfache Berechnungen in die Cloud auslagern. Die App übergibt ausschließlich die Werte und holt sich das Ergebnis ab.

Neben der besseren Integration in die jeweilige Plattform war lange Zeit die Unabhängigkeit vom Internet ein Hauptargument für native Apps gegenüber mobilen Webseiten. Hier hat das Web jedoch aufgeholt und auch native Apps greifen zunehmend und regelmäßig aufs Backend zu.

Gründe hierfür gibt es viele: Der Benutzer muss sich authentifizieren und der Server ihn autorisieren. Der Anbieter möchte das Anwenderverhalten messen, um Daten für Werbeaktionen, Kaufanreize und personalisierte Angebote zu erhalten. Stürzt die Anwendung ab, soll der Entwickler den Fehler schnell analysieren und beheben. Um den Nutzer, solange es geht, in der App zu halten, ist oft eine Integration sozialer Medien wie Facebook und Twitter sinnvoll. Außerdem wollen viele Anwender ihre Daten über mehrere Geräte synchronisieren.

Letztlich muss der Entwickler eine ganze Reihe von Webservices orchester, deren Programmierschnittstellen kennen und sie in der eigenen App richtig nutzen. Gibt es für eine Art Dienst mehrere Anbieter, sollte er idealerweise alle unterstützen – schließlich weiß er nicht, welchen der Nutzer lieber verwendet. Dies alles für nur ein mobiles Betriebssystem zu gewährleisten, ist schon keine leichte Aufgabe. Kommt eine zweite Plattform hinzu, muss der Entwickler zusätzlich unterschiedliche Programmiersprachen und Architekturen bei der Implementierung berücksichtigen.

Backend as a Service

Seit einigen Jahren erfreuen sich deshalb solche Cloud-Angebote wachsender Beliebtheit, die speziell auf die Bedürfnisse mobiler Apps zugeschnitten sind. Man bezeichnet sie als Mobile Backend as a Service (MBaaS) oder Backend as a Service (BaaS). Neben den bereits angesprochenen Funktionen gehören eine Geschäftslogik im Backend, Cloud-Speicher und -Datenbanken, standortbasierte Dienste, Nachrichten, Chats und Push-Benachrichtigungen zum Standardrepertoire.

Gerade letztere verdeutlichen den Mehrwert von BaaS-Diensten: Android wie iOS kennen Cloud-basierte Benachrichtigungen. In beiden Fällen sendet der Server bloß kleine Infohäppchen an ein oder mehrere Geräte. Die technische Umsetzung ist tief in das jeweilige Ökosystem eingebettet – insbesondere die Gerätidentifikation variiert stark.

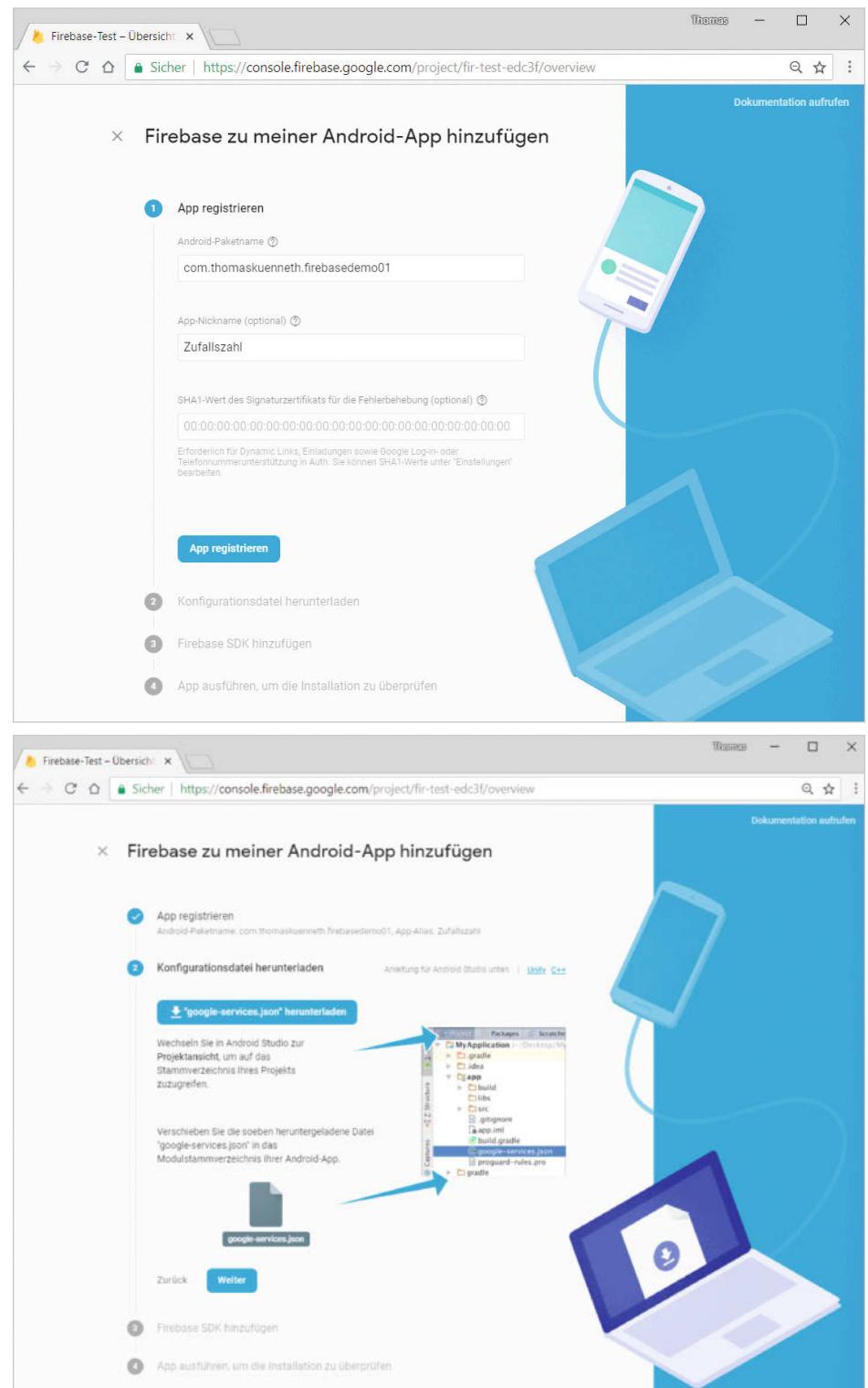
Eine gemeinsame API, beispielsweise auf Basis eines RESTful Webservice, in

Verbindung mit einer plattformübergreifenden Nutzer- und Geräteverwaltung würde die Integration durch den Entwickler deutlich vereinfachen. BaaS-Dienste fungieren als Brücke zwischen Apps und unterschiedlichen Cloud-Backends, indem sie vereinheitlichte Programmierschnittstellen und Entwicklungswerkzeuge zur Verfügung stellen. Hierzu gehören vorgefertigte Bibliotheken und Pakete, die man mit minimalem Aufwand in den Build-Prozess der jeweiligen Plattform integrieren kann. Dies ist auch ein wichtiges Abgrenzungsmerkmal gegenüber vielen Angeboten aus den Bereichen Software as a Service (SaaS), Infrastructure as a Service (IaaS) oder Platform as a Service (PaaS). Schließlich sind Dateiablage und -weitergabe, Geschäftslogik (Lambdas, Functions) und Datenbanken Funktionen, die jeder Cloud-Dienstleister in seinem Portfolio hat.

Firebase ist Googles BaaS-Angebot an alle Android-, iOS- und Webentwickler. Der Konzern übernahm die 2011 gegründete Firma Firebase, Inc. im Oktober 2014 und hat die gleichnamige Plattform seitdem kontinuierlich ausgebaut und erweitert. Neben den Schlüsselfunktionen Datenbank und Dateiablage, Nutzerauthentifizierung, Hosting, Cloud Messaging (Googles offizielle Alternative zum 2012 für veraltet erklärten, nativen Cloud to Device Messaging), Absturz- und Verhaltensanalyse stehen dem Entwickler zahlreiche weitere Dienste zur Verfügung. Beispielsweise läutete die Google I/O 2018 die Betaphase der Machine-Learning-Komponente ML Kit ein. Und den URL-Kürzungsdienst goo.gl ersetzt künftig Firebase Dynamic Links.

Firebase in der eigenen App

Für den Einsatz von Firebase ist ein Google-Konto erforderlich. Eine zentrale Webkonsole erlaubt das Anlegen, Verwalten und Überwachen von Projekten. Letztere enthalten Apps für eine oder mehrere Plattformen. Beim Hinzufügen einer Android-App trägt man deren Paketnamen (`package="..."` in der Manifestdatei), optional einen alternativen Anwendungsnamen (Nickname) und für die Fehlerbehebung den SHA1-Schlüssel des Signaturzertifikats in das Webformular ein. Das Registrieren der App erzeugt die zentrale Konfigurationsdatei `google-services.json`. Sie muss man herunterladen und dem Android-Studio-Projekt hinzufügen. Bei Apps, die aus einem Modul bestehen, landet die Datei üblicherweise



Assistiert: Das Hinzufügen einer Android-App geht schnell von der Hand (Abb. 1).

im Verzeichnis *app*. Während des kompletten Prozesses greift dem Nutzer ein Assistent unter die Arme (siehe Abbildung 1).

Damit eine App mit dem Firebase-Backend kommunizieren kann, benötigt sie das Firebase-SDK. Dieses verankert man Android-üblich in zwei *build.gradle*-Dateien. Als Erstes erweitert man die Datei im Projektwurzelverzeichnis im Block *dependencies { ... }* um eine Zeile:

```
classpath 'com.google.gms:google-services:4.0.1'
```

Die modulspezifische `build.gradle` erhält im Block `dependencies {...}` die Zeile:

```
implementation 'com.google.firebaseio:firebase-core:16.0.3'
```

Außerdem muss man am Ende der Datei ein

apply plugin: `z`

'com.google.gms.google-services'

einfügen.

Google rät, zum Überprüfen der Änderungen und nach dem Synchronisieren

Firebase mit iOS nutzen

Google-Dienste nutzen CocoaPods, um Abhängigkeiten zu installieren und zu verwalten. Das Werkzeug muss der Entwickler vor dem Einsatz von Firebase in Apps für Apples iPhones oder iPads auf seinem Rechner einrichten. Der Assistent zum Hinzufügen einer iOS-Applikation ähnelt dem für Android: Als Erstes trägt man die Bundle-ID sowie optional die App-Store-ID und einen alternativen App-Namen ein. Nach dem Registrieren der App in Firebase muss man die Datei *Google-Service-Info.plist* herunterladen, in den Xcode-Projektstamm verschieben sowie in allen Ziehen hinzufügen.

Die folgenden Terminal-Befehle führt man im Basisverzeichnis des Xcode-Projekts aus. *pod init* erzeugt eine Datei namens *Podfile*. Ihr

fügt man unterhalb der Zeile `# Pods for Zufallszahl` ein `pod 'Firebase/Core'` hinzu. Anschließend erzeugt der Befehl `pod install` eine *.xcworkspace*-Datei. Sie bildet die Basis für die weitere Entwicklung der App und wird mit Xcode geöffnet. Als Letztes muss man der Klasse *AppDelegate* in der Funktion *application* die Zeile `FirebaseApp.configure()` spendieren. Im Bereich mit den Imports ist zusätzlich die Zeile `import Firebase` nötig.

Startet man nun die App, zeigt der Projektassistent in der Firebase-Konsole eine erfolgreiche Kommunikation mit dem Hinweis „Sehr gut, Sie haben Firebase erfolgreich zu Ihrer Anwendung hinzugefügt“ an. Die Firebase-Dienste erfordern wie unter Android weitere Bibliotheken.

wenn sich neue Nutzer in der App registrieren.

Technisch handelt es sich bei Cloud Functions um JavaScript- oder TypeScript-Code, den das System mit minimalem Aufwand hochlädt und den der Server in einer sicheren, betreuten Node.js-Umgebung ausführt. Um Functions implementieren zu können, muss man die Firebase CLI installieren. Sofern auf dem Entwicklungsrechner schon eine Node-Umgebung vorhanden ist, reicht hierfür ein

```
npm install -g firebase-tools
```

Anschließend startet der Befehl `firebase init` einen Assistenten, der im aktuellen Verzeichnis ein neues lokales Projekt anlegt und es auf Wunsch mit einem Projekt in der Firebase-Konsole verknüpft. Damit das funktioniert, muss man sich mit `firebase login` bei Firebase angemeldet haben. Funktionen legt man im Unterverzeichnis `functions` an und lädt sie mit dem Befehl `firebase deploy` hoch.

Zufallszahlen mit Firebase Functions

Listing 1 zeigt eine Firebase Function. Sie reagiert auf das Eintreffen einer HTTPS-Anfrage. Der Funktion `zufallszahl` über gibt das Programm ein JSON-Objekt, das die obere Grenze der zu ermittelnden Zufallszahl enthält. Sie liefert eine JSON-Datenstruktur, die neben diesem Wert die Zufallszahl beinhaltet.

Nach dem Hochladen der Function mit `firebase deploy` kann man sie zum Beispiel mit dem Kommandozeilentool `curl` testen:

```
curl -X POST -H "Content-Type:application/json" https://us-central1-fir-test-edc3f.firebaseio.cloudfunctions.net/zufallszahl -d '{"data": {"max": 42}}'
```

Die URL ist unter anderem vom Firebase-Projektnamen abhängig und steht in der Firebase-Konsole. Letztere gewährt zudem Einblick in die Logdateien. Functions können mit `console.log()` auf INFO- und mit `console.error()` auf ERROR-Ebene protokollieren.

Um Functions unter Android zu nutzen, trägt man in der modulspezifischen `build.gradle` die Zeile

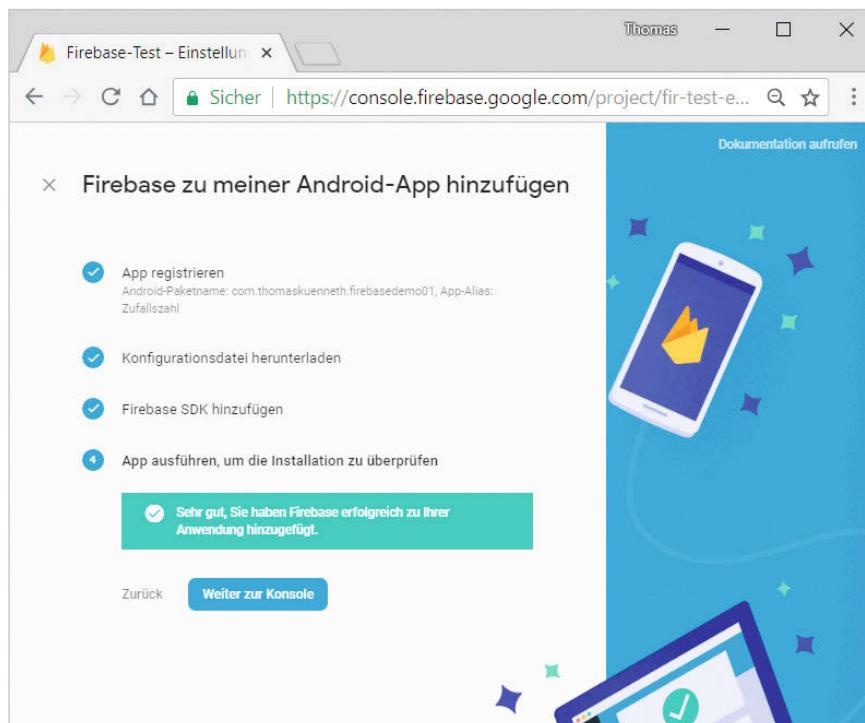
```
implementation 'com.google.firebaseio:firebase-functions:16.1.0'
```

ein. Außerdem muss man in der Manifestdatei die Berechtigung `android.permission.INTERNET` anfordern. Hierbei handelt es sich um eine normale Berechtigung, in der *Activity* ist deshalb keine programmatische Anforderung nötig.

des Projekts die App auszuführen. Einen erfolgreichen Verbindungsversuch zeigt Abbildung 2. So lernt eine App aber noch keine neuen Funktionen – sie kann lediglich rein prinzipiell mit dem Firebase-Backend kommunizieren. Wie man die von Firebase zur Verfügung gestellten Dienste nutzt, zeigt die App „Zufallszahl“ am Beispiel von Firebase Functions. Den Quelltext stellt der iX-Listing-Server bereit.

Mit Firebase Functions ermittelt das Programm eine Zufallszahl und zeigt sie

auf dem Gerät an. Über Functions setzt Google die Idee um, Logik in der Cloud auszuführen. Als Entwickler muss man sich keine Gedanken über Serverkonfiguration, SSL-Zertifikate, Lastverteilung, Ausfallsicherheit oder Skalierung machen. Es geht nicht darum, komplexe Geschäftsvorfälle umzusetzen, sondern einfache Aktionen auszuführen – und zwar beim Eintreten spezifischer Ereignisse, zum Beispiel nach Änderungen in der Firebase Realtime Database, beim Empfang von HTTPS-Anfragen oder



Überprüft: Ein Start der App zeigt, ob man Firebase erfolgreich hinzugefügt hat (Abb. 2).

Listing 1: Firebase Function in der index.js

```
const functions = require('firebase-functions');

exports.zufallszahl = functions.https.onRequest((req, res) => {
    console.log(req.body);
    var max = req.body.data.max;
    var result = randomInt(max);
    res.setContentType("application/json");
    res.status(200);
    var s = JSON.stringify({
        data: {
            max: max,
            result: result
        }
    });
    console.log("Output: " + s);
    res.send(s);
});

function randomInt(max) {
    return Math.floor(Math.random() * Math.floor(max));
}
```

Listing 2: Auszug aus MainActivity.java

```
mFunctions
    .getHttpsCallable("zufallszahl")
    .call(data)
    .addOnFailureListener(new OnFailureListener() {

        @Override
        public void onFailure(@NonNull Exception e) {
            Log.e(TAG, "onFailure()", e);
        }
    })
    .addOnCompleteListener(new OnCompleteListener<HttpsCallableResult>() {

        @Override
        public void onComplete(@NonNull Task<HttpsCallableResult> task) {
            Log.d(TAG, "onComplete()");
        }
    })
    .addOnSuccessListener(new OnSuccessListener<HttpsCallableResult>() {

        @Override
        public void onSuccess(HttpsCallableResult httpsCallableResult) {
            handleResult((Map<String, Integer>) httpsCallableResult.getData());
        }
    });
});
```

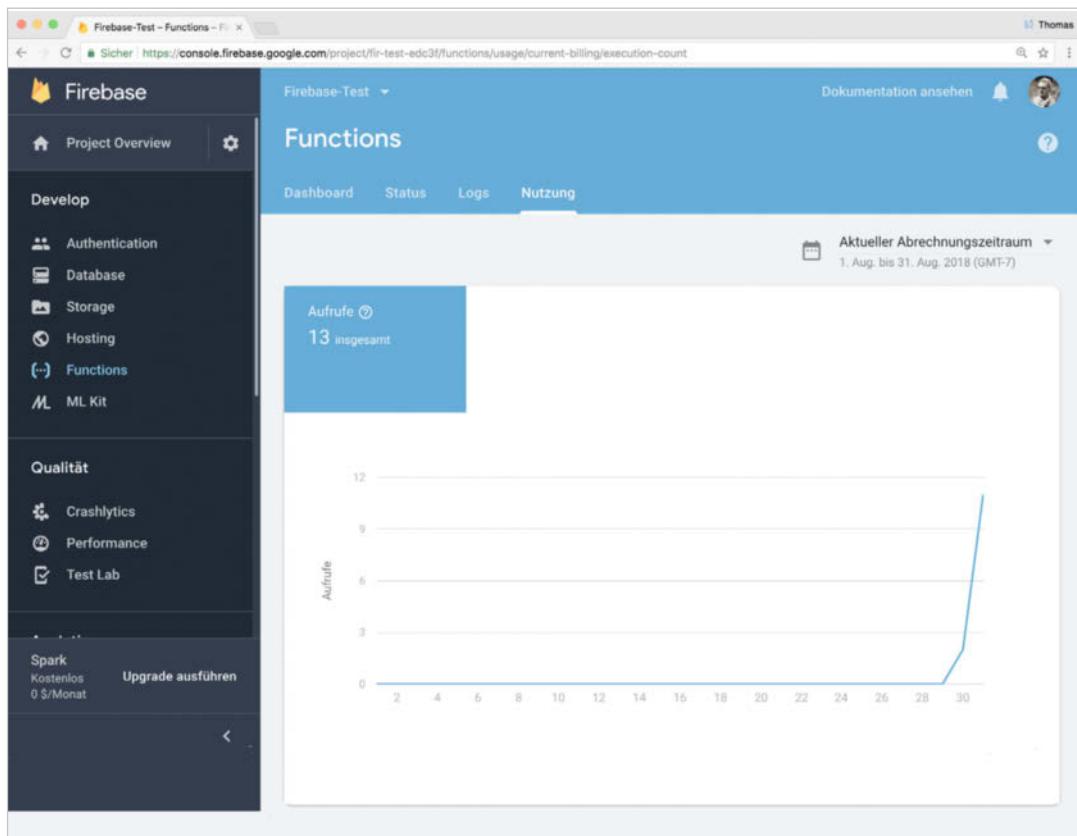
Der Zugriff auf Functions erfolgt über ein Objekt des Typs `com.google.firebaseio.functions.FirebaseFunctions`, das man durch den Aufruf von `FirebaseFunctions.getInstance()` erhält. Es bietet sich an, die Referenz in einer privaten Instanzvariablen zu speichern und sie in `onCreate()` zu initialisieren. Den eigentlichen Funktionsaufruf zeigt Listing 2.

Als Erstes erzeugt `getHttpsCallable()` ein Objekt des Typs `HttpsCallableReference` und ruft dessen Methode `call()` auf. Ihr übergibt das Programm eine Map, deren einziges Element die obere Grenze der Zufallszahl darstellt. `call()` liefert ein `Task<HttpsCallableResult>`-Objekt. Auf diesem schließlich registriert man Listener, die die App im Erfolgs-

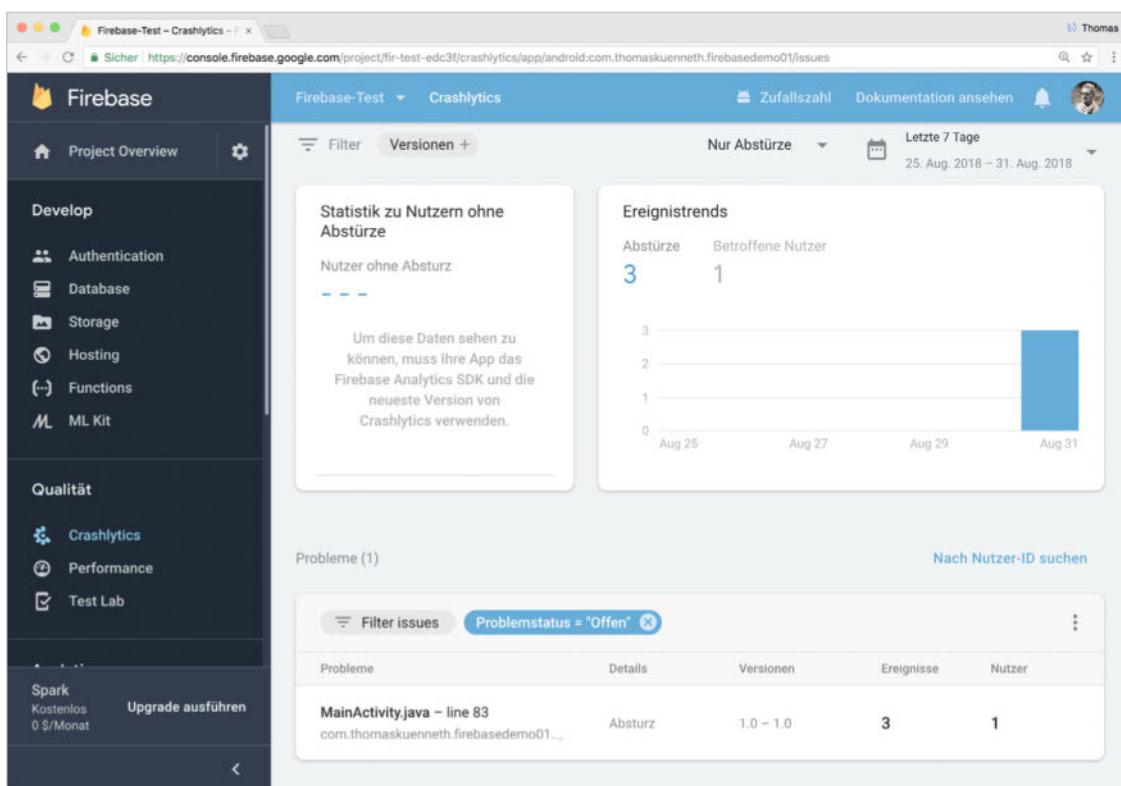
oder Fehlerfall aufruft. Abbildung 3 zeigt, wie die Firebase-Konsole den Einsatz von Functions wiedergibt.

Fehler aufspüren

Firebase Crashlytics ist ein leichtgewichtiger Echtzeit-Crashreporter für An-



Im Blick:
Die Functions
in der Firebase-
Konsole (Abb. 3).



droid- und iOS-Apps. Tritt ein Problem auf, überträgt das Programm die Daten an das Firebase-Backend, das sie aggregiert. Ziel ist es, Entwicklern beim Erkennen, Priorisieren und Beheben von Absturzursachen zu helfen. Häufig gestellte Fragen sind: Tritt der Absturz bei vielen Nutzern auf oder lässt er sich auf wenige, spezifische Anwender eingrenzen? Beschränken sich die Abstürze auf bestimmte Gerätetypen und Betriebssysteme oder treten sie bei allen Android-Versionen und Tablets wie Smartphones auf?

Um Crashlytics in eine App zu integrieren, muss man die projektweite *build.gradle* wie in Listing 3 erweitern. Der modulspezifischen *build.gradle*

Datei im Verzeichnis *app* fügt man zu dem ein

```
apply plugin: 'io.fabric'
...
dependencies {
    ...
    implementation 'com.crashlytics.sdk.android:crashlytics:2.9.5'
}
```

hinzzu.

Nachdem Android Studio das Projekt synchronisiert und neu gebaut hat, steht Crashlytics automatisch zur Verfügung. Die Beispiel-App „Zufallszahl“ enthält eine Schaltfläche, die eine *NullPointerException* provoziert (Abbildung 4). Zu Testzwecken lassen sich Abstürze auch mit *Crashlytics.getInstance().crash()*; simulieren.

da man sich auf die App selbst konzentrieren kann.

Etablierte Cloud-Anbieter entdecken zunehmend mobile Geräte für sich und locken mit einfacher Integration. Warum also eine zusätzliche Plattform? Wer beispielsweise seine Unternehmensanwendung mit Xamarin Forms entwickelt und hierfür ein Backend braucht, ist wahrscheinlich mit Microsofts Azure gut bedient. Wie bei Amazon gilt hier aber: „Wir können auch Mobile.“ Echte MBaaS-Dienste konzentrieren sich auf Smartphones und Tablets. Insofern ist ein ausgefeiltes, leicht zu nutzendes Client-SDK für die etablierten mobilen Plattformen Pflicht. Dies ist bei Firebase der Fall, denn die Integration ist sowohl unter Android als auch unter iOS in wenigen Minuten erledigt.

Bei aller Begeisterung über die vielen Services, die Skalierungs- und Monetarisierungsoptionen erbt Firebase dennoch viele Nachteile anderer Cloud-Dienste. Neben dem Vertrauen in die Langlebigkeit des Produkts gehört dazu die bewusste Entscheidung, seine Firmen- und Kundendaten einem Dritten zu überlassen.
(fo@ix.de)

Fazit

Apps ohne Netzwerkfunktion finden sich nur noch selten, praktisch alle benötigen ein Backend für das Speichern, Verteilen und Abfragen von Daten, für das Trigger-basierte Ausführen von Geschäftslogik und das Erheben von Kennzahlen sowie das Messen und Bewerten des Nutzerverhaltens. Bei geringen Anwendernzahlen mag man das noch on Premises betreiben können. Steigen die Anforderungen, wird der Betrieb aufwendig – von den Kosten einmal ganz abgesehen. Insofern sind Cloud-Angebote attraktiv,

Thomas Künne

arbeitet als Principal Consultant für die MATHEMA Software GmbH. Neben zahlreichen Artikeln hat er drei Bücher über Android, Java und Eclipse veröffentlicht.

iX Cloud-Konferenz 2018

Cloud Services effektiv und sicher nutzen

10. Oktober 2018 • Berlin

Unsere Sprecher sind z.B.:



Kurt Garloff,
T-Systems:
Wie man Spectre et al
besiegt



Andreas Neeb,
Red Hat GmbH:
Istio & Kubernetes



Oliver Annau & Malte Brodersen,
Zoi TechCon GmbH:
HashiCorp Terraform



WEITERE TOP-THEMEN:

- Edge Computing
- Serverless Infrastructure
- DSGVO und Cloud

- Kubernetes
- DevOps-Performance
- Microservices

**Jetzt
Ticket
sichern!**

Workshops am 11. und 12. Oktober:

- Kubernetes und Container für Fortgeschrittene
- Amazon Web Services (AWS) und Microsoft Azure im direkten Vergleich
- Systemdeployment & -management mit Ansible

weitere Informationen & Anmeldung unter www.heise-events.de/cloudkonf

Partner



Organisiert von

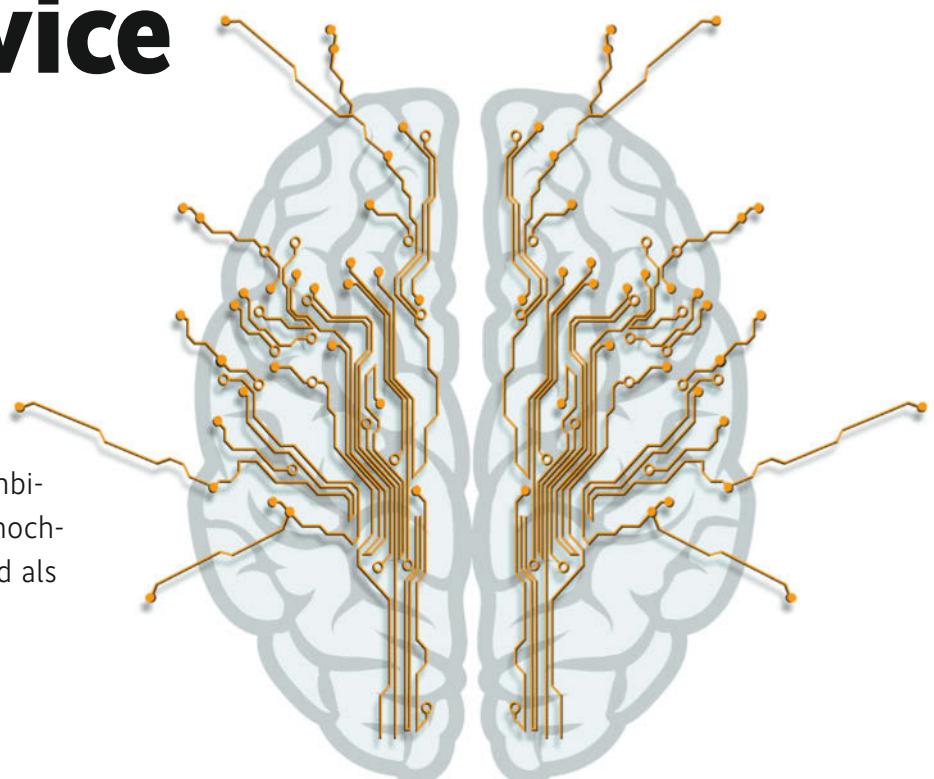


Deep-Learning-Modelle deployen mit TensorFlow Serving

Machine Learning as a Service

Mark Keinhörster

TensorFlow Serving stellt Machine-Learning-Modelle schnell, flexibel und vor allem performant in Produktionsumgebungen bereit. In Kombination mit Keras lassen sich so hochskalierbare Modelle erstellen und als Services in Anwendungen integrieren.



Dank moderner Frameworks wie TensorFlow und Keras haben Deep-Learning-Methoden mittlerweile den Weg aus der Forschung in die Industrie gefunden. Ob in der Verarbeitung natürlicher Sprache oder bei der Objekterkennung – neuronale Netze sind kaum mehr wegzudenken.

Eines der meistgenutzten Frameworks für Deep Learning ist Keras, eine High-Level-API für neuronale Netze, die TensorFlow als Backend für verteilte Berechnungen nutzen kann. Durch die einfache API und den modularen Aufbau lassen sich in Keras schnell funktionale Proto-

typen für eine Vielzahl von Netzarchitekturen definieren und trainieren. Doch Machine-Learning-Modelle werden heute nicht mehr nur für einmalige Analysezwecke genutzt – in Anwendungen ersetzen sie oft statische Regelwerke oder Algorithmen. Daher stellt sich die Frage, wie sich trainierte Modelle in Anwendungen integrieren lassen.

Während es im Big-Data-Bereich bereits Frameworks wie Apache Airflow oder Luigi von Spotify gibt, die eine robuste Verarbeitung in großen Batches ermöglichen, muss man bei der Integration neuronaler Netze in Anwendungen an-

ders vorgehen. Hier werden Modelle nicht periodisch aus Batch-Jobs angewendet, sondern live als Aufruf in der Applikation. Um diese Art der Integration zu erleichtern, hat Google TensorFlow Serving entwickelt. Mit dem integrierten ModelServer lassen sich TensorFlow-Modelle mit wenig Aufwand bereitstellen und nutzen.

TensorFlow Serving besteht im Wesentlichen aus dem ModelServer als Hauptkomponente und der TensorFlow Serving API für Python. Das zentrale Konzept für das Deployment nativer TensorFlow-Modelle ist das Servable, das die vom Server geladenen Modellinstanzen abstrahiert. Die weiteren Komponenten von TensorFlow Serving sind lediglich erforderlich, wenn der ModelServer erweitert werden soll, da er von Haus aus TensorFlow-Modelle nur aus dem lokalen Dateisystem laden kann. Für solche Erweiterungen muss man TensorFlow Serving jedoch neu kompilieren.

TensorFlow Serving kann zur Laufzeit verschiedene Versionen eines Modells als

TRACT

- TensorFlow Serving stellt mit TensorFlow oder Keras erstellte Machine-Learning-Modelle übers Netz bereit.
- Clients greifen auf die Modelle via gRPC und eine Python-API zu.
- Das Werkzeug erleichtert das Überführen von ML-Prototypen in den Produktionsbetrieb und die Integration von ML in Anwendungen.

Servable laden und auch löschen, sodass sowohl sukzessive Rollouts neuer Modelle als auch Deployments ohne Downtime gewährleistet sind. Abbildung 1 zeigt das Zusammenspiel zwischen Modellen im Dateisystem, Servables, der Ladestrategie und der Client-API.

Ein Wetterfrosch für Jena

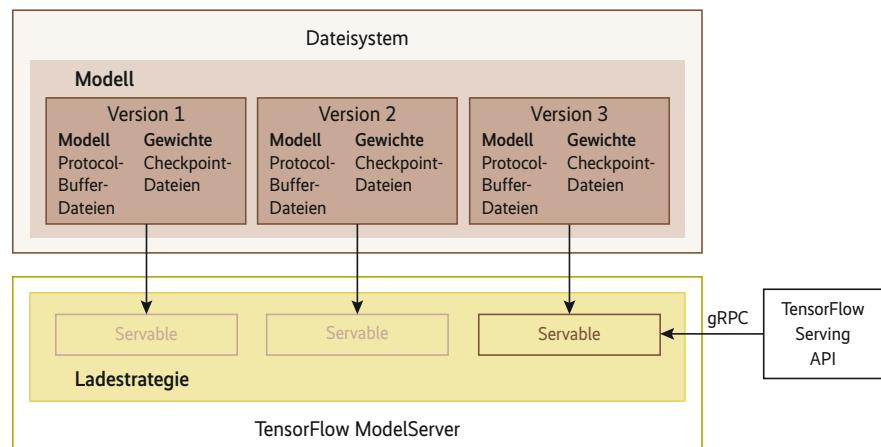
Ein Modell zur Wettervorhersage für die Stadt Jena soll das Konzept und die Funktionsweise des ModelServers veranschaulichen. Der Wetterfrosch wird als Service mit TensorFlow Serving bereitgestellt. Er soll anhand der Daten der letzten fünf Tage die Temperatur in Jena für den nächsten Tag vorhersagen. Die für das Training verwendeten Wetterdaten stehen frei im Netz zur Verfügung (siehe ix.de/ix1810126). Das Modell wird in Keras mit TensorFlow als Backend implementiert.

Der Trainingsdatensatz ist eine Zeitreihe über den Zeitraum von 2009 bis 2016 mit 14 Merkmalen, vom Luftdruck über die Temperatur bis hin zu Windgeschwindigkeit und -richtung, mit einer Granularität von zehn Minuten. Ein Auszug ist in der Tabelle „Die Trainingsdaten ...“ aufgelistet. Da Wetterdaten sich langsamer als im Zehn-Minuten-Takt ändern, haben wir die Granularität zum Training des neuronalen Netzes auf stündliche Werte reduziert. Damit schrumpft die Menge an Eingaben, was die Verarbeitung beschleunigt.

Bei Zeitreihendaten bietet sich ein rekurrentes neuronales Netz zur Wettervorhersage an. Rekurrente Netze machen während des Trainings jede Berechnung zum Zeitpunkt t abhängig vom vorherigen Ergebnis (t-1), wodurch sich periodische Merkmale wie beispielsweise Jahreszeiten effektiver lernen lassen. Das trainierte neuronale Netz steht im von Keras unterstützten HDF5-Format (Hierarchical Data Format) zum Download auf GitHub bereit (ix.de/ix1810126). Die Funktion `load_model()` lädt es in Keras (siehe Listing 1).

Die Funktion `plot_model()` im Listing speichert eine Grafik der Netzarchitektur. Das ist gerade bei extern erstellten Modellen sehr nützlich, um die Dimensionalität (das Shape) des Eingabevektors zu verifizieren. Durch den Parameter `show_shapes=True` werden die Shapes der Input- und Outputvektoren mit ausgegeben. Die Layernamen sind weniger wichtig und lassen sich mit `show_layer_names=False` unterdrücken.

Die Schichten des Modells mit ihren In- und Outputs sind in Abbildung 2 dar-



Die Ladestrategie bestimmt, welche Modellversionen der ModelServer den Clients als Servables anbietet (Abb. 1).

Die Trainingsdaten der Wetterstation

Datum	Luftdruck (mbar)	Temperatur (°C)	...	Windstärke (m/s)	Windrichtung (Grad)
01.01.2009 00:10:00	996,52	-8,02	...	1,03	152,30
...
31.12.2016 23:50:00	999,81	-4,23	...	1,49	225,80

gestellt. Keras-Modelle arbeiten bei der Prediction in Batches und können mehrere Vorhersagen gleichzeitig verarbeiten. Aus diesem Grund ist der eigentliche Input um eine Dimension höher als der Datensatz (120 Stunden mit jeweils 14 Messwerten). Einen Batch kann man sich wie eine Liste mit Datensätzen vorstellen, für die das Modell eine Vorhersage treffen soll. Da die Zahl der Datensätze in einem Batch variabel ist, kann sie das Modell nicht festlegen; daher ist sie mit `None` spezifiziert. Für die Vorhersage eines einzelnen Temperaturwerts ergibt sich ein Inputvektor mit dem Shape (1,120,14), bei zwei Vorhersagen in einer Anfrage hat der Batch das Shape (2,120,14).

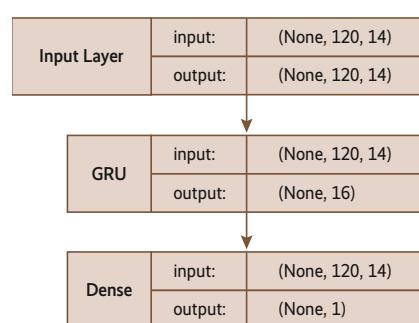
Als rekurrente Schicht kommt ein GRU-Layer (Gated Recurrent Unit) zum Einsatz. Während bei einfachen rekur-

renten Netzen der Output aus dem Zeitpunkt t-1 ungefiltert in die Berechnung zur Zeit t mit einfließt, wendet der GRU-Layer Filter auf die Daten an, die bestimmen, welche Informationen aus t-1 nach t übertragen werden. Forschungen haben gezeigt, dass diese Art Layer sich deutlich besser für das Trainieren längerer zeitlicher Abfolgen eignet. Keras abstrahiert diese Komplexität, sodass sich der Anwender nicht mit den Details herumschlagen muss. Der Dense-Layer aggregiert die Outputs aus der GRU-Schicht in einen einzelnen Wert: die vorhergesagte Temperatur. Den gesamten Code, inklusive Training der Modelle, finden Sie im GitHub-Repository (siehe ix.de/ix1810126).

Export des TensorFlow-Graphen

Das Modell wurde mit Keras erstellt. Damit es TensorFlow Serving übers Netz bereitstellen kann, muss es in dessen Exportformat vorliegen. Ab diesem Punkt muss man Keras als Abstraktionsschicht verlassen und direkt mit TensorFlow-Bordmitteln arbeiten.

Vor dem Export des Graphen mitsamt seinen Gewichten ist eine passende Modellsignatur zu definieren, die die Eingang- und Ausgaben des Modells beschreibt. Sie wird als Teil des Modells exportiert und später vom ModelServer verwendet.



Das neuronale Netz des Wetterfroschs besteht aus drei Schichten (Abb. 2).

Listing 1: Laden und Plotten eines bereits trainierten Modells in Keras

```
from keras.models import load_model
from keras.utils import plot_model

model = load_model("...")

plot_model(model,
            to_file="...",
            show_shapes=True,
            show_layer_names=False)
```

Listing 2: Erstellen der Modellsignatur

```
from tensorflow.python.saved_model import signature_constants
import tensorflow as tf

info_input = tf.saved_model.utils.build_tensor_info(model.input)
info_output = tf.saved_model.utils.build_tensor_info(model.output)

prediction_signature = (
    tf.saved_model.signature_def_utils.build_signature_def(
        inputs={'input': info_input},
        outputs={'prediction': info_output},
        method_name=signature_constants.PREDICT_METHOD_NAME))
```

Listing 2 zeigt, wie die Signatur für den Wetterfrosch zusammengebaut wird.

Die Funktion `build_tensor_info()` konvertiert die Ein- und Ausgaben in einen `TensorInfo` Protocol Buffer. TensorFlow Serving nutzt gRPC zur Kommunikation mit dem Client und gRPC selbst wiederum nutzt Protocol Buffer zur Serialisierung. Die Ausgabe von `tensor_info_input()` zeigt, dass das Input-Shape des Buffers mit dem der Modellinputs übereinstimmt:

```
name: "gru_3_input:0"
dtype: DT_FLOAT
tensor_shape {
  dim { size: -1 }
  dim { size: 120 }
  dim { size: 14 }
}
```

Während Keras für variable Batchgrößen `None` nutzt, verwendet TensorFlow dafür aufgrund der Implementierung mit Numpy-Arrays `-1`. Beide Werte haben in diesem Fall jedoch die gleiche Bedeutung, es lassen sich beliebig viele Vorhersagen in einen Aufruf verpacken.

Die Funktion `build_signature_def()` erstellt die Signatur. Sie bekommt `inputs`, `outputs` und einen `method_name` übergeben. `method_name` legt fest, welche API der ModelServer intern nutzt. Das Deployment nutzt die Predict API, da sie flexibel mit In- und Outputs umgehen kann.

Mit der Signatur kann der Wetterfrosch exportiert werden (Listing 3). Beim Spei-

ichern ist es wichtig, auf die Modellversion zu achten. Im Listing ist der Basispfad `/models/weather` und das Modell landet im Unterordner `/models/weather/1`. Mit dem Pfad wird ein `SavedModelBuilder` instanziert.

Das Speichern erledigt die Funktion `add_meta_graph_and_variables()` des Builders, die mit einer Session, einer Liste von Tags sowie der Modellsignatur aufgerufen wird. `save()` speichert anschließend den Graphen als Protocol Buffer und die Gewichte als sogenannte Checkpoint-Dateien.

Da Keras das TensorFlow-Backend nutzt, kann man auf die TensorFlow-Session mit `keras.backend.get_session()` zugreifen. Die Session kapselt den Zustand des Modells und führt die internen Berechnungen während des Trainings und bei Vorhersagen aus. Wenn man den Graphen, der das Modell repräsentiert, mit einem Python-Skript vergleicht, ist die Session wie der Python-Interpreter, nur dass sie statt Code die Operationen im Graphen ausführt.

Deployment als Servable

Für TensorFlow Serving muss man den Graphen als Serving-Graph speichern. Dazu wird in der Tag-Liste das Tag `SERVING` angegeben. Mithilfe von Tags lassen sich unterschiedliche Metagraphen

auf einen Berechnungsgraphen abbilden. Beispielsweise sind Serving-Graphen ausgedünnt und speziell auf Inferenzen zugeschnitten. Sie enthalten im Gegensatz zu Training-Graphen weder die Loss-Funktion noch den Optimierer oder Dropout-Schichten.

Um ein einzelnes Modell als Servable bereitzustellen, wird der ModelServer wie folgt gestartet:

```
tensorflow_model_server --port=9000 \
--model_name=weather \
--model_base_path=...
```

Die Parameter sind fast selbsterklärend: `port` gibt an, auf welchem Port der Server lauscht. `model_name` bestimmt, unter welchem Namen das Modell für den Client erreichbar ist, und `model_base_path` gibt den Speicherort des Modells an, in dem TensorFlow Serving nach auslieferbaren Versionen sucht.

Leider lassen sich nicht alle Konfigurationen über die Kommandozeile vornehmen, beispielsweise der Umgang mit verschiedenen Versionen eines Modells. Erstellt man etwa ein weiteres vortrainiertes Modell des Wetterfroschs mit weiteren GRU-Schichten und exportiert es wie oben beschrieben als Version 2 für TensorFlow Serving, zeigt ein erneuter Blick auf die Konsole: Der Server hat die neue Version erfolgreich erkannt, geladen und im Anschluss daran die ältere verworfen. Dieses Verhalten entspricht der Standardladestrategie, die dafür sorgt, dass der Server nur das neueste Modell bereitstellt.

Detailliertere Einstellungen erfordern eine Konfigurationsdatei für TensorFlow Serving. Auch sie legt Basispfad und Name des Modells fest. Dazu kommt die Ladestrategie (`model_version_policy`). Die Konfiguration in Listing 4 stellt die drei neuesten Versionen gleichzeitig bereit und verwirft alle älteren Servables. Neben der Strategie `latest` gibt es noch `all`, die alle gefundenen Modellversionen bereitstellt, und `specific`, die eine festgelegte Version lädt. Weitere Parameter erläutert die Dokumentation. In der `model_config_list` lassen sich mehrere Modelle mit `config` definieren.

Die Konfiguration übergibt man dem Server beim Start:

```
tensorflow_model_server --port=9000 \
--model_config_file=models.conf
```

Alle Befehle für die Installation und Bereitstellung des ModelServers als Docker-Container finden Sie ausführlich dokumentiert im Git-Repository (siehe ix.de/ix1810126).

Über eine API können Clients mit dem ModelServer sprechen. Ein gRPC-Chan-

Listing 3: Den Wetterfrosch V1 exportieren

```
from tensorflow.python.saved_model import signature_constants
from tensorflow.python.saved_model import tag_constants
from tensorflow.python.saved_model import builder
import tensorflow as tf

model_version = "1"
export_path = "./models/weather/1"
tf_builder = builder.SavedModelBuilder(export_path)
with tf.keras.backend.get_session() as sess:
    tf_builder.add_meta_graph_and_variables(
        sess=sess,
        tags=[tag_constants.SERVING],
        signature_def_map={
            signature_constants.DEFAULT_SERVING_SIGNATURE_DEF_KEY: prediction_signature
        })
tf_builder.save()
```

Listing 4: Konfigurationsdatei für TensorFlow Serving

```
model_config_list: [
  config: {
    name: "weather",
    base_path: "./models/weather",
    model_version_policy: {
      latest: {
        num_versions: 3
      }
    }
  }
]
```

Listing 5: PredictionServiceStub für den Wetterfrosch

```
import grpc
from tensorflow_serving.apis import prediction_service_pb2

host = "localhost"
port = "9000"
channel = grpc.insecure_channel("localhost:9000")
stub = prediction_service_pb2.PredictionServiceStub(channel)
```

Listing 6: Metadaten über die Client-API abfragen

```
from tensorflow_serving.apis import get_model_metadata_pb2

status = get_model_metadata_pb2.GetModelMetadataRequest()
status.model_spec.name = 'weather'
status.metadata_field.append("signature_def")
response = stub.GetModelMetadata(status)
```

nel stellt Stubs bereit, über die Clients mit dem ModelServer kommunizieren können. Listing 5 zeigt das Erstellen eines Stubs für den Wetterfrosch. Da dieser die Predict API nutzt, wird ein *PredictServiceStub* angelegt, über den Clients Requests absetzen können.

Intelligenz aus dem Netz

Leider bietet TensorFlow Serving in der aktuellen Version noch keine Möglichkeit, den ModelServer mit gängigen Monitoringlösungen zu überwachen oder ein Modell-Deployment zu verifizieren. Um dennoch einen Produktionsbetrieb zu gewährleisten, kann man *GetModelMetadataRequest()* nutzen.

Listing 6 zeigt, wie ein Client Metainformationen zum Wetterfrosch abfragen kann. Dazu wird der Request *status* erstellt und mit dem Modellnamen sowie dem anzufragenden Metadatentyp gefüllt. In der aktuellen Version unterstützt die API lediglich das Abfragen der Modellsignatur, daher muss zwingend "signature_def" als Datentyp verwendet werden. Mit *status.model_spec.version.value* lässt sich noch eine Version spezifizieren,

Ergebnisse der beiden Modellversionen

Wetterfrosch	Vorhersage
Version 1	15,27 °C
Version 2	13,62 °C

ansonsten erhält man die Metadaten des neuesten Modells. Konnte der Server das angefragte Modell in der gewünschten Version nicht laden, liefert der Stub den Status *NOT_FOUND* zurück.

Der Wetterfrosch in Aktion

Ein *PredictRequest* berechnet eine Vorhersage auf dem ModelServer. Wie gehabt gibt man dabei Modellname und optional die Version mit an. Zudem erhält der Request die Inputdaten. Um dies zu veranschaulichen, soll das Modell die Temperatur für den 10.05.2018 um 00:00 Uhr vorhersagen. Listing 7 zeigt grob, wie die Daten für die Inferenz vorverarbeitet werden.

Der Code lädt den Zeitraum vom 04.05.2018 bis zum 09.05.2018 aus der CSV-Struktur mit den Wetterdaten der Stadt Jena, reduziert die Daten auf Stundenwerte und selektiert die gewünschten Daten. Um den Datensatz in das Shape (1, 120, 14) des Eingabeformats des Modells zu bringen, erweitert Numpy ihn um eine weitere Dimension von (120, 14) auf (1, 120, 14).

Listing 8 erzeugt zunächst einen *PredictRequest*. Die Funktion *make_tensor_proto()* wandelt die Daten in das passende Format für TensorFlow. *stub.predict(request)* startet die Berechnung auf dem ModelServer.

Das Ergebnis kommt als *PredictResponse* zurück. Ändert man die Version im Request auf 2, lässt sich das zweite

Listing 7: Modellieren der Inputs

```
import numpy

schritt = 6 # = 1 Datenpunkt pro Stunde
rueckblick = 120 # = 5 Tage = 5*24 Stunden
ausblick = 24 # = 1 Tag in die Zukunft vorhersagen

# Lade den gesamten Datensatz vom
# 04.05.2018 bis zum 10.05.2018
# als Numpy-Array
10_min_data = lade_daten(...)

# Reduziere auf volle Stunden
stundlich = reduziere_auf_stunden(10_min_data)

# Selektiere die Inputdaten
# vom 04.05.2018 bis zum 09.05.2018
input_daten = stundlich[:rueckblick]
input_datensatz = numpy.expand_dims(a=input_daten, axis=0)
```

Listing 8: Vorhersage durch den Wetterfrosch

```
from tensorflow_serving.apis import predict_pb2
from tf.contrib.util import make_tensor_proto

request = predict_pb2.PredictRequest()
request.model_spec.name = 'weather'
request.model_spec.version.value = 1
input_proto = make_tensor_proto(input_vektor)
request.inputs['input'].CopyFrom(input_proto)
result = stub.Predict(request)
```

Servable für die Inferenz heranziehen. Die Tabelle „Ergebnisse“ gibt einen kurzen Überblick über die Ergebnisse. Die tatsächlich gemessene Temperatur lag bei 14,06 Grad Celsius.

Fazit

Googles TensorFlow Serving ist ein flexibles und skalierbares Werkzeug zur Bereitstellung von TensorFlow-Modellen über Netz, das auch Keras-Modelle einfach dynamisch laden kann. Damit kommen Data Scientists und Entwickler dem Rapid Prototyping, Deployment und anschließenden Betrieb von Deep-Learning-Modellen als Service einen großen Schritt näher.

(odi@ix.de)

Mark Keinhörster

ist Data Architect bei der codecentric AG. Er ist im Big-Data-Zoo zu Hause und beschäftigt sich außerdem mit Docker, Microservices und Cloud-Technologien.

Literatur

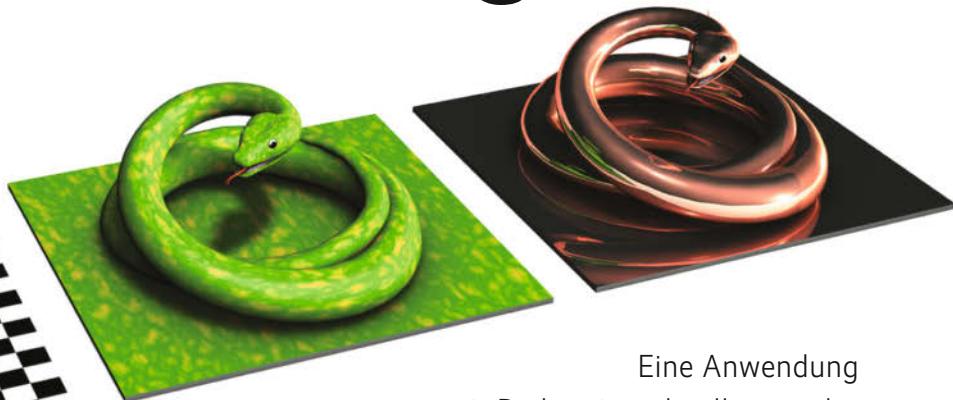
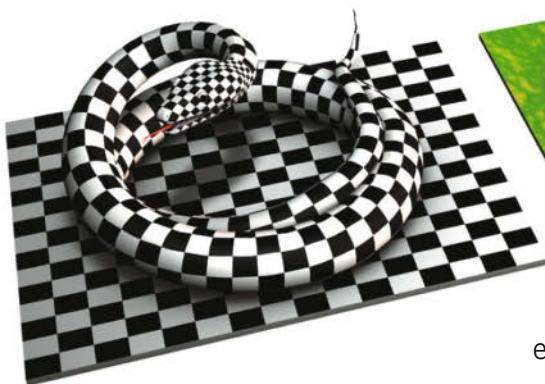
- [1] Géron A.; Hands-On Machine Learning with Scikit-Learn and TensorFlow; O'Reilly 2017
- [2] Chollet F.; Deep Learning with Python; Manning 2017



Oberflächen mit Python und dem Framework Qt5 erstellen

Mit Außenwirkung

Gerhard Völk



Eine Anwendung mit Python ist schnell gemacht. Sollen andere damit arbeiten, braucht man dafür eine Bedienoberfläche, die auf unterschiedlichen Plattformen läuft. Hier bietet sich das Framework Qt an.

Bereits 1991 haben Haavard Nord und Eirik Chambe-Eng in ihrer Firma Trolltech das Framework Qt entwickelt, später hat Nokia es gekauft. Heute gehört es der Qt Group. Eigentlich ist Qt ein plattformübergreifendes C++-Framework, aber da sich solche Bibliotheken relativ gut in Python einbinden lassen, gingen die Leute der britischen Firma Riverbank Computing Limited ans Werk und erstellten mit PyQt eine Integration für Python.

In diesem Artikel geht es um Qt5 mit Python 3. Es gibt ältere Versionen, die sich in einigen Details von der aktuellen Release unterscheiden. Für PyQt existieren unterschiedliche Lizenzmodelle – von der kostenlosen GNU General Public License (GPL) bis hin zu einer kommerziellen Lizenz. Mehr dazu findet sich auf dem Webserver der Firma Riverbank (URL unter ix.de/ix1810130). Der Eigentümer des Frameworks Qt hat ebenfalls den Markt für Python erkannt und eine eigene Integration unter der Bezeichnung PySide in Arbeit.

Von C++ nach Python

Mehr denn je ist es im mobilen Zeitalter erforderlich, dass man aus einer Codebasis performante Anwendungen für unterschiedliche Hardware erzeugen kann. Das plattformübergreifende C++-Framework leistet genau das – Embedded-Ap-

plicationen eingeschlossen. Qt enthält die üblichen, von Desktop-Anwendungen bekannten Oberflächenelemente. Darüber hinaus gibt es unzählige weitere Module, angefangen vom Datenbankzugriff über Netzwerkkommunikation bis hin zu Web- oder 3D-Oberflächen (siehe Tabelle). Dieser Artikel konzentriert sich auf gängige Desktop-Oberflächen, da diese die Basis für komplexere Benutzerschnittstellen bilden.

PyQt lässt sich wie gewohnt mit Pip

```
pip install pyqt5
```

oder Anaconda installieren:

```
conda install pyqt5
```

Auf einigen Linux-Plattformen, etwa Raspberry Pi, gibt es eigene Pakete für die Installation:

```
sudo apt-get install python3-pyqt5
```

Normalerweise verwendet ein Python-Programmierer die Namenskonvention, die die Entwickler der Programmiersprache in PEP8 vorgeschlagen haben. Da Qt aus der C++-Welt stammt und PyQt die Namen aller Objekte eins zu eins übernommen hat, kommt man bei der Namenskonvention um etwas „Mischmasch“ zwischen beiden Welten nicht herum.

Funktional und objektorientiert

Listing 1 zeigt das Grundgerüst einer Qt-Desktop-Anwendung in Python. Sie besteht lediglich aus ein paar Funktionsaufrufen, deren zentrales Objekt von der Klasse *QApplication* abgeleitet und im Modul PyQt5.QtWidgets zu finden ist. Es repräsentiert die gesamte Anwendung.

iX-TRACT

- PyQt ist eine Python-Implementierung des in C++ geschriebenen Qt-Frameworks.
- Mit der Bibliothek lassen sich Oberflächen für Python-Programme erstellen, die die GUI-Spezifika unterschiedlicher Plattformen berücksichtigen.
- Seit der letzten Qt-Version kann der Programmierer Oberflächen alternativ mit Qt Quick deklarativ beschreiben, was speziell im IoT-Umfeld vorteilhaft sein kann.

Beim Erzeugen bekommt das neue *QApplication*-Objekt als Parameter eine Liste der Argumente (*sys.argv*), mit denen der Anwender das Python-Programm gestartet hat und die vor allem das Erscheinungsbild der Anwendung beeinflussen. *QApplication* enthält die Hauptschleife, die sich um die Abarbeitung der Ereignisse kümmert, die es in einer Oberfläche geben kann – etwa ein Mausklick-Event in einem Fenster –, und sucht den möglichen Empfänger. Die Basisklasse für alle Oberflächenelemente in Qt ist *QWidget*.

Alle Methoden, die wie *setGeometry* mit „set“ beginnen, ändern die Eigenschaften eines Objekts, wie hier in Zeile 7 den Titel in der oberen Fensterleiste. Diese Namenskonvention hält Qt in allen Modulen durch. Um im Gegenzug den Wert eines Attributs zu ermitteln, gibt es allerdings keine Methode „*getWindowTitle*“, sie heißt einfach nur *window.setWindowTitle()*.

Da die Methode *exec_* der Klasse *QApplication* verhindert, dass das Fenster nur kurz aufflackert, bleibt es so lange sichtbar, bis der Anwender die Applikation beendet oder ein Fehler zum Abbruch führt. Den Rückgabewert, der anzeigen, ob ein Fehler aufgetreten ist oder das Programm normal beendet wurde, sollte das Programm an die Methode *sys.exit* weitergeben, die ihn ihrerseits an das Betriebssystem weiterreicht. Hat ein Skript das Programm gestartet, kann dieses auf Fehler reagieren. In der C++-Bibliothek von Qt heißt diese gerade beschriebene Methode nur *exec* – ohne den Unterstrich am Schluss. Der kam hinzu, weil dieser Name in Python bereits vergeben war.

Bei größeren Anwendungen empfiehlt Qt natürlich eine objektorientierte Vorgehensweise (Listing 2). Für ein eigenes Fenster mit Bedienungselementen leitet man dafür eine eigene Klasse von *QWidget* ab (Zeile 6 bis 9). Beim Initialisieren eines neuen Fensters ist es sinnvoll, über *super().__init__()* zunächst das Elternobjekt der Klasse *QWidget* zu initialisieren. Darauf folgt die Hauptaufgabe der Methode *__init__* – das Erzeugen aller im Fenster zu sehenden Oberflächenelemente. Die Methode *QPushButton* liefert einen Befehlsknopf zurück, der ebenfalls von der Klasse *QWidget* abgeleitet ist, wie in diesem Fall der Push-Button, der zum Schließen des Fensters dient.

Alle Objekte der Klasse *QWidget* haben grundsätzlich ein Parent-Element. Sollte man vergessen, es anzugeben (in diesem Fall *self* für den *QPushButton*),

Häufig genutzte Qt-Module

Modul	Funktion
QtCore	Basisklassen, in denen verschiedenste Module Verwendung finden, zum Beispiel Datentypen oder Konstanten
QtGui	Klassen zur Integration von Fensteroberflächen, Ereignisverarbeitung, 2D-Grafik, Bilder, Zeichensätze
QtWidgets	Klassen für Oberflächenelemente einer Desktop-Anwendung
QtMultimedia	Klassen für Multimediainhalt, etwa den Zugriff auf Kameras
QtBluetooth	Bluetooth-API
QtNetwork	Netzwerkkommunikation mit TCP/IP und UDP
QtPositioning	Positionsbestimmung mit GPS, WLAN etc.
QtWebSockets	WebSocket-API
QtWebKit	Webbrowser auf Basis von WebKit2
QtXml	XML-API mit SAX und DOM
QtSvg	Darstellen von SVG-Dateien
QtSql	Zugriff auf Datenbanken
QtTest	Testen

würde es nirgends erscheinen. Die einzige Ausnahme davon sind eigenständige Fenster wie *FirstWindow*.

Ereignisse lösen Signale aus

Wenn es um die Verarbeitung von Ereignissen geht, findet man in der Qt-Dokumentation die Begriffe Signale und Slots. Das Framework erzeugt ein bestimmtes Signal, in diesem Fall *button.clicked*, wenn dieses Ereignis eintritt (Zeile 14). Unter einem Slot versteht Qt eine Methode beziehungsweise irgendetwas, das es aufrufen kann, in Python Callable genannt. Verbindet der Entwickler ein Signal mit einem Slot, ruft Qt die zugehörige

Methode auf, sobald das Ereignis (Signal) eintritt. Der Entwickler definiert dies einmal, um den Rest kümmert sich Qt. Wichtig ist allerdings, dass nach dem *connect* die Methode *self.close* ohne Klammern steht, da hier der Verweis auf die Methode und nicht ihr Aufruf benötigt wird.

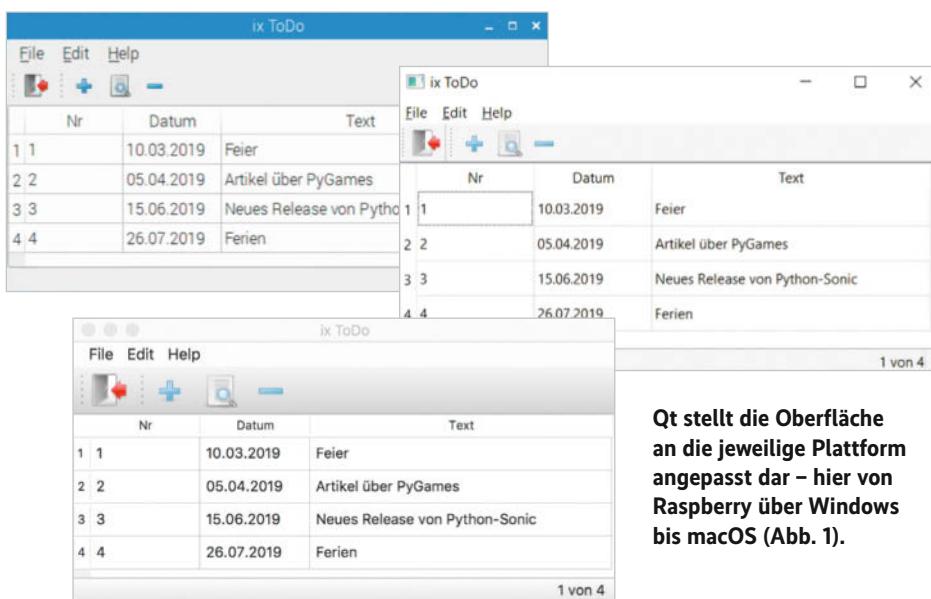
Neben der Verarbeitung von Events mit *connect* kennt das Framework vorgefinierte Methoden, die es aufruft, wenn ein bestimmtes Ereignis eintritt. Soll das

Listing 1: *first.py*

```
1 from PyQt5.QtWidgets import *
2 import sys
3
4 app = QApplication(sys.argv)
5 window = QWidget()
6 window.setGeometry(0,0,500,500)
7 window.setWindowTitle('First')
8
9 window.windowTitle()
10
11 window.show()
12
13 sys.exit(app.exec_())
```

Listing 2: *first_obj.py*

```
1 from PyQt5.QtWidgets import *
2 from PyQt5.QtGui import *
3
4 import sys
5
6 class FirstWindow(QWidget):
7
8     def __init__(self):
9         super().__init__()
10
11         button = QPushButton('Close', self)
12         button.move(50, 50)
13         button.setToolTip("Fenster schließen")
14         button.clicked.connect(self.close)
15
16         self.setGeometry(400,400,200,200)
17         self.setWindowTitle('FirstWindow')
18         self.setWindowIcon(QIcon("testicon.png"))
19
20         self.show()
21
22     def closeEvent(self, event):
23         reply = QMessageBox.question(self, 'Nachricht', "Soll die Anwendung geschlossen werden?", QMessageBox.Yes | QMessageBox.No, QMessageBox.No)
24
25         # Variante 1
26         if reply == QMessageBox.Yes:
27             event.accept()
28         else:
29             event.ignore()
30
31
32 if __name__ == "__main__":
33     app = QApplication(sys.argv)
34     mainWindow = FirstWindow()
35     app.quit()
36     sys.exit(app.exec_())
```



Qt stellt die Oberfläche an die jeweilige Plattform angepasst dar – hier von Raspberry über Windows bis macOS (Abb. 1).

eigene Programm an dieser Stelle etwas tun, kann der Entwickler die vorhandene Methode überschreiben. So erlaubt es die vordefinierte Methode `closeEvent` der Klasse `QWidget` in den Zeilen 22 bis 25, dass der Anwender vor dem Schließen des Fensters bestätigt, dass er das wirklich will.

Der eigentliche Programmstart ist hinter der für Python klassischen Abfrage nach `"__main__"` untergebracht. Die Zeilen 33 bis 37 führt Python bekanntlich nur aus, wenn Listing 2 als Programm läuft und nicht als Modul Verwendung findet. Schließt der Anwender bei einer mit Qt erstellten Applikation alle Fenster, beendet sich das Objekt `app` selbst. Soll dies nicht passieren, kann man das über die Methode `setQuitOnLastWindowClosed(False)` jederzeit ändern. Für das Beenden der Anwendung genügt dann der Aufruf `app.quit()`.

In der Praxis besteht an dieser Stelle die Schwierigkeit darin, in irgendeinem Modul, in dem sich das Programm gerade befindet, an das aktuelle Anwendungsobjekt zu kommen. Dies geht in Qt entweder über die Klasse `QApplication`, die mit der Methode `QApplication.instance()` das aktuelle Objekt zurückliefert, oder über den globalen Verweis `qApp`, der auf das aktuelle Anwendungsobjekt zeigt.

Layout-Manager für Dialoge

Eine größere Anwendung besteht meistens aus einem Hauptfenster und einigen Dialogen, die der Anwender über Menüpunkte öffnen kann. Ein Beispiel wäre der Eigenschaftsdialog, über den man

Einstellungen des Programms festlegen kann (Abbildung 2).

Qt leitet ein Dialogfenster normalerweise von der Klasse `QDialog` ab, die wiederum selbst von `QWidget` abstammt. `QDialog` bringt zusätzliche Eigenschaften mit, etwa die Definition eines Befehlsknopfs als Default-Button oder dass ein Dialog modal aufgerufen werden kann, sodass er die ganze Anwendung sperrt, bis der Anwender ihn wieder schließt.

Grundsätzlich gibt es in Qt zwei Möglichkeiten, Widgets in einem Fenster zu positionieren: mit genauen Größenangaben und Koordinaten für jedes Element oder über einen Layout-Manager, der sich um Größe und Position der einzelnen Elemente kümmert und die Widgets entweder in einer Zeile (`QHBoxLayout`), übereinander (`QVBoxLayout`), tabellarisch (`QFormLayout`) oder wie in einem Formular – Texte und Eingabeelemente jeweils untereinander – (`QGridLayout`) gruppiert.

In Listing 3 ordnet ein Layout-Manager der Klasse `QVBoxLayout` in einem einfachen Eigenschaftsfenster die Inhalte in Zeilen übereinander an. Für welche Elemente der Layout-Manager zuständig ist,

erfährt er über seine Methode `addWidget` (Zeile 12 und 13), die Methode `setLayout` teilt ihm in Zeile 43 zudem mit, um den Inhalt welches Fensters (hier `self`) er sich kümmern soll. Das Arbeiten mit Layout-Managern ist nicht auf Fenster begrenzt, da jedes Objekt, das von der Klasse `QWidget` abgeleitet ist, die Methode `setLayout` hat.

Im Beispielprogramm bietet sich für die Eingabe des Namens der Datenbankdatei sowie der Sprache der Layout-Manager `QFormLayout` an (Zeile 15), da links in einer Spalte die Beschreibungen und rechts daneben die Steuerelemente für die Eingabe stehen.

Wie jedes Steuerelement können Layout-Manager-Objekte Elemente anderer Layout-Manager sein. Dadurch kann sich beispielsweise ein Layout-Manager um einen bestimmten Bereich kümmern und ein anderer um den gesamten Dialog (Zeile 35).

Wie die Layout-Manager die Elemente genau anordnen, hängt von der Plattform ab, auf der das Programm läuft. Ein Betriebssystem (Windows) möchte die Beschreibungstexte für Eingabefelder linksbündig, ein anderes (macOS) will sie rechtsbündig zur Eingabe hin angeordnet haben. Darum kümmert sich Qt. Hat der Entwickler eigene Vorstellungen, kann er sie mit den Eigenschaften des Layout-Managers durchsetzen (Zeile 16). Der Layout-Manager reagiert automatisch, wenn sich die Größe eines Fensters ändert. Als Entwickler kann man über die Methode `setFieldGrowthPolicy` (Zeile 17) eine Richtlinie für diesen Fall vorgeben.

Auch die Standard-Befehlsknöpfe „Ok“ und „Cancel“ im unteren Bereich eines Dialogs lassen sich am einfachsten über einen Layout-Manager realisieren:

```
hBoxLayout.addStretch(1)
hBoxLayout.addWidget(okButton)
hBoxLayout.addWidget(cancelButton)
```

Die Methode `addStretch` fügt zunächst einen leeren Platz ein, konkret ein Objekt vom Typ `QSpacerItem`. Dadurch rutschen die Buttons auf die rechte Seite, wie man es von Dialogen gewohnt ist. Da die An-



Layout-Manager übernehmen das Positionieren der Oberflächenelemente. Für die plattformspezifische Erscheinungsform der Buttons ist `QDialog ButtonBox` zuständig (Abb. 2).

Listing 3: dialog.py

```

1 from PyQt5.QtWidgets import *
2 from PyQt5.QtGui import *
3 from PyQt5.QtCore import Qt
4
5 class Property_Dialog(QDialog):
6     def __init__(self):
7         super().__init__()
8         self.setGeometry(100, 100, 250, 180)
9         self.setWindowTitle('Eigenschaften')
10
11    verticalLayout = QVBoxLayout()
12    self.saveWindowSize = QCheckBox('Fenstergröße am Programmende speichern')
13    verticalLayout.addWidget(self.saveWindowSize)
14
15    formLayout = QFormLayout()
16    formLayout.setFormAlignment(Qt.AlignLeft | Qt.AlignTop)
17    formLayout.setFieldGrowthPolicy(QFormLayout.ExpandingFieldsGrow)
18    self.dbfileLabel = QLabel('DB-Datei')
19    formLayout.setWidget(0, QFormLayout.LabelRole, self.dbfileLabel)
20
21    horizontalLayout = QHBoxLayout()
22    self.dbfile = QLineEdit()
23    horizontalLayout.addWidget(self.dbfile)
24    self.dbfileButton = QPushButton('?')
25    horizontalLayout.addWidget(self.dbfileButton)
26
27    self.dbfileButton.clicked.connect(self.showFileDialog)
28
29    formLayout.setLayout(0, QFormLayout.FieldRole, horizontalLayout)
30    self.languageLabel = QLabel('Sprache')
31    formLayout.setWidget(1, QFormLayout.LabelRole, self.languageLabel)
32    self.language = QComboBox()
33    self.language.addItem('Deutsch', 'Englisch', 'Spanisch')
34    formLayout.setWidget(1, QFormLayout.FieldRole, self.language)
35    verticalLayout.addLayout(formLayout)
36
37    self.buttonBox = QDialogButtonBox()
38    self.buttonBox.setOrientation(Qt.Horizontal)
39    self.buttonBox.setStandardButtons(QDialogButtonBox.Cancel | QDialogButtonBox.Ok)
40    self.buttonBox.setObjectName("buttonBox")
41    verticalLayout.addWidget(self.buttonBox)
42
43    self.setLayout(verticalLayout)
44    self.buttonBox.accepted.connect(self.accept)
45    self.buttonBox.rejected.connect(self.reject)
46
47    def showFileDialog(self):
48        #Klassenmethode
49        file_name = QFileDialog.getOpenFileName(self, 'DB-Datei', '/', 'DB-Datei (*.db);;Alles (*.*)')
50
51        fileDialog = QFileDialog(self, 'DB-Datei', '/', 'DB-Datei (*.db);;Alles (*.*)')
52        fileDialog.setFileMode(QFileDialog.ExistingFile)
53        fileDialog.setViewMode(QFileDialog.Detail)
54        fileDialog.exec_()
55        file_name = fileDialog.selectedFiles()
56
57        if file_name[0]:
58            self.dbfile.setText(file_name[0])
59
60    if __name__ == "__main__":
61        import sys
62        app = QApplication(sys.argv)
63
64        dialog = Property_Dialog()
65
66        dialog.saveWindowSize.setChecked(True)
67        dialog.language.setCurrentText('Deutsch')
68        dialog.dbfile.setText('')
69
70        if dialog.exec_(): # Modal
71            print ('Fenster speichern: {} {}'.format(dialog.saveWindowSize.isChecked()))
72        else:
73            print ('Kein Speichern')
74

```

und es passend konfigurieren (Zeile 51 und 52). Durch die Methode *setFileMode* mit dem Parameter *ExistingFile* kann der Anwender nur vorhandene Dateien auswählen, aber keine neuen Dateinamen eingeben. Informationen über die gewählte Datei erhält man über den *Detail-Modus* (Zeile 53). Der Dialog erscheint, sobald das Programm dessen Methode *exec* aufruft, die ausgewählten Dateien liefert die Methode *selectedFiles* zurück (Zeile 54, 55). Darüber hinaus gibt es Klassen für weitere Standarddialoge wie *QColorDialog* zum Auswählen einer Farbe, *QFontDialog*, um einen Zeichensatz festzulegen, sowie

QInputDialog für die Eingabe eines einzelen Wertes.

Für das Hauptfenster gibt es in Qt die Klasse *QMainWindow*, die das Management des grundsätzlichen Layouts und des Menüs mitbringt. Das Starten einer Anwendung mit der Klasse *QMainWindow* geht ähnlich wie mit einem anderen Fenster. Zuerst leitet man eine eigene Klasse von der Klasse *QMainWindow* ab:

```

class MainWindow(QMainWindow):
    def __init__(self, parent=None):
        super(MainWindow, self).__init__(parent)

```

Von dieser erzeugt ein Programm ein eigenes Applikationsobjekt:

ordnung dieser Buttons nicht bei allen Plattformen gleich ist, gibt es in Qt dafür eine eigene Klasse *QDialogButtonBox*, die das übernimmt (Zeile 37 bis 39). Der Entwickler legt mit der Methode *setStandardButtons* fest, welche Buttons vorhanden sind – um das restliche Verhalten und das Layout kümmert sich dann das Objekt der Klasse *QDialogButtonBox* (Zeile 44 und 45).

Weiterarbeiten oder sperren

Wenn ein Programmteil einen Dialog aufruft, ist die wesentliche Entscheidung, ob der Anwender mit der restlichen Applikation weiterarbeiten können soll (*modeless*) oder ob sie gesperrt ist (*modal*). Im Fall von *modal* erzeugt die Anwendung als Erstes den Dialog (Zeile 65), anschließend belegt sie die Attribute, die der Anwender ändern kann, mit den aktuellen Werten (Zeile 67 bis 69) und schließlich ruft die Methode *exec_* den Dialog auf und führt die gewünschten Änderungen aus.

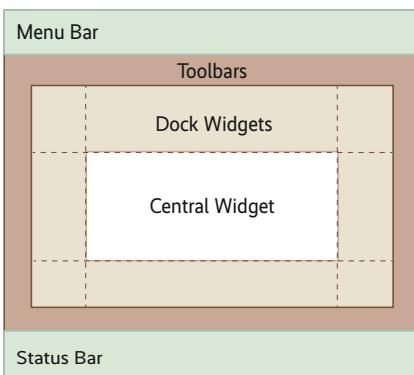
Bei nicht modalen Dialogen, in denen der Anwender etwas einstellt und sich sofort etwas ändert, gilt eine andere Vorgehensweise. Zuerst erzeugt man einen Dialog mit den Knöpfen „Anwenden“, „Ok“ und „Schließen“. Beim Start erhält der Dialog einen Verweis auf die Datenstrukturen der Anwendung, die die zu ändernden Eigenschaften enthält. Die Methode *dialog.show* ruft den Dialog nicht modal auf. Beim Drücken auf „Anwenden“ oder „Ok“ führt der Dialog die Änderung aus.

Die meisten Plattformen bieten für häufig wiederkehrende Aufgaben, beispielsweise die Auswahl einer Datei, eigene, bereits fertige Dialoge. An den Dialog für die Dateiauswahl kommt man über die Klasse *QFileDialog*, am einfachsten mit der Klassenmethode *QFileDialog.getOpenFileName* (siehe dazu die im Listing auskommentierten Zeilen 48 und 49).

Das Hauptfenster und seine Kinder

In der Variablen *file_name* kommt ein Python-Tupel zurück, dessen erstes Element die ausgewählte Datei bezeichnet. Falls der Anwender nichts ausgewählt hat, ist das Ergebnis eine leere Zeichenkette.

Reicht diese einfache Variante nicht aus, kann ein Programm ein eigenes Objekt der Klasse *QFileDialog* erstellen



Das Central Widget, in dem die eigentliche Oberfläche läuft, kann ein beliebiges Qt-Widget sein (Abb. 3).

```
if __name__ == '__main__':
    app = QApplication(sys.argv)
    main_window = MainWindow()
    main_window.show()
    sys.exit(app.exec_())
```

Die eigentliche Oberfläche der Anwendung läuft im zentralen Bereich, dem Central Widget, das mit der Methode `setCentralWidget` gesetzt wird und das in Qt jedes beliebige Widget sein kann. Für ein Zeichenprogramm etwa käme ein Objekt der Klasse `QGraphicsView`, bei einer Datenbanktabelle `QTableWidget` in Frage.

Komplexere Anwendungen definieren häufig ein eigenes Element, das von `QWidget` abgeleitet ist.

Ein Fenster von der Klasse `QMainWindow` hat automatisch eine horizontale Menüleiste vom Typ `QMenuBar`. Auf den meisten Plattformen ist sie oben im Fenster zu sehen, bei macOS steht sie separat am oberen Bildschirmrand. Wer sich bei seiner Anwendung nicht an diese Vorgabe halten will, kann die Platzierung mit der Methode `setNativeMenuBar` an die anderen Plattformen anpassen:

```
menuBar.setNativeMenuBar(False)
```

Die einzelnen Menüpunkte der Hauptmenüleiste sind wiederum eigene Menüs der Klasse `QMenu`:

```
fileMenu = menuBar.addMenu('&File')
```

Die Methode `addMenu` erzeugt ein neues Objekt `fileMenu` mit der Beschriftung `File` und fügt es der Menüleiste hinzu. Das `&` vor `File` bewirkt bei Betriebssystemen wie Windows, dass der Anwender den Menüpunkt mit der Tastenkombination Alt + F aufrufen kann. Einzelnen Menüpunkt können die Klassen `QAction`, `QSeparator` und `QMenu` repräsentieren.

Die Methode `setShortcut` weist der Aktion eine auf die Plattform passende Tastenkombination zu. Qt hat diese im Attribut `Quit` der Klasse `QKeySequence` hinterlegt:

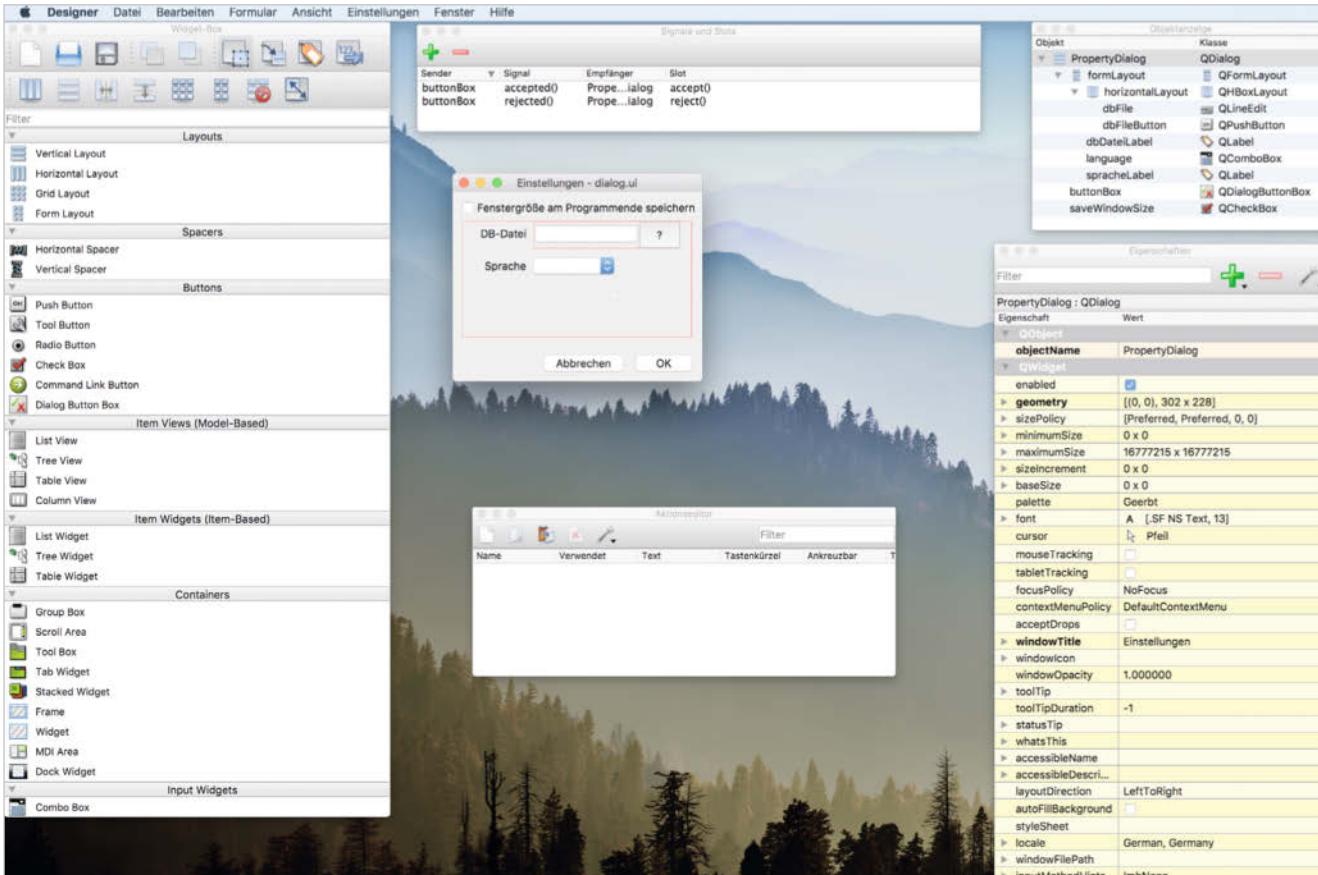
```
quitAction.setShortcut(QKeySequence.Quit)
```

Falls `QKeySequence` keine Tastenkombination für eine bestimmte Aktion hat, beispielsweise das Editieren eines Eintrags, kann man eine eigene definieren:

```
editAction.setShortcut(QKeySequence(Qt.CTRL + Qt.Key_P))
```

Ein weiterer Vorteil der Klasse `QKeySequence` besteht darin, dass sie die Tasten plattformspezifisch anpasst. Die Kombination Ctrl + E gibt es so nicht auf macOS. Qt setzt sie automatisch auf das übliche Cmd + E um.

Da nicht jede Anwendung eine Toolbar unterhalb der Menüleiste hat, ist diese in Qt nicht wie beim Menü automatisch in `QMainWindow` vorhanden. Erst die Methode `addToolBar` erzeugt eine neue Toolbar (Klasse `QToolBar`). Das Panel kann Buttons mit Text und Icon sowie weitere Widgets enthalten. Obwohl es sich standardmäßig unterhalb der Menüzeile befindet



Der Qt Designer bietet dem Programmierer einen Editor, in dem er eine Oberfläche visuell erstellen kann (Abb. 4).

det, ist es je nach Wunsch frei verschiebbar, bei Bedarf auch vom Anwender.

Neben der Hauptarbeitsfläche haben die meisten Anwendungen zusätzliche Bereiche, die ständig sichtbar und für bestimmte Aufgaben zuständig sind. Diese Fenster kann der Anwender dort andocken, wo er am besten damit arbeiten kann. Sie sind in Qt von der Klasse *QDockWidget* abgeleitet.

Ein Dock-Window kann der Anwender bewegen (*movable*), schließen (*closable*) oder sogar abdocken und als eigenständiges Fenster verwenden (*floatable*). Die Methode *addDockWidget* fügt dem Hauptfenster das Dock-Window hinzu. Der erste Parameter teilt Qt mit, wo das Fenster beim Programmstart erscheinen soll:

```
mainwindow.addDockWidget(7  
    (Qt.LeftDockWidgetArea, logDockWidget)
```

Visuell entwickeln mit Qt Designer

Dialoge oder komplexe Oberflächen für umfangreiche Anwendungen direkt im Quellcode zu erstellen, wie es die bisherigen Beispiele gezeigt haben, ist ziem-

lich zeitaufwendig. Deshalb gibt das Framework dem Programmierer das Werkzeug Qt Designer an die Hand, das ihm einige Aufgaben abnimmt.

Mit Qt Designer erstellt man die Oberfläche visuell mit einem Editor und speichert jedes neue Fenster in einer Datei mit der Endung *.ui*. Da Python damit nicht viel anfangen kann, setzt der Qt-Befehl *pyuic5* diese Datei in ein Python-Modul um, das dem neuen Dialog entspricht:

```
pyuic5 dialog.ui -o ui_dialog.py
```

Der erste Parameter bezeichnet die Designdatei und der zweite den Namen des Python-Moduls, das die neue Klasse für das Fenster enthält. Jedes Mal, wenn der Entwickler etwas ändert, muss er diesen Befehl erneut ausführen, der dann wiederum das Python-Modul überschreibt. Deshalb sollte man es unbedingt vermeiden, im generierten Python-Code etwas zu ändern oder zu ergänzen. Stattdessen leitet man eine eigene Klasse von der generierten ab und bringt dort die Änderungen unter.

Zwar enthält die generierte Klasse *Ui_PropertyDialog* aus dem Modul *ui_dialog* alle Steuerelemente – aber viel

mehr nicht. Daher muss der Programmierer die eigene Klasse zusätzlich von der Qt-Klasse ableiten, zu der sie gehören soll, beispielsweise der Klasse *QDialog* oder bei Hauptfenstern *QMainWindow*. Hier kommt Pythons Mehrfachvererbung zum Einsatz:

```
import ui_dialog  
class Property_Dialog(QDialog,  
ui_dialog.Ui_PropertyDialog):
```

Die Initialisierungsmethode initialisiert erst die Basisklasse und ruft danach die Methode *setupUI* aus der generierten Klasse auf, die alle Steuerelemente erzeugt:

```
def __init__(self, parent=None):  
    super(Property_Dialog, self). __init__(parent)  
    self.setupUi(self)
```

Der Quelltext der generierten Klasse ist lesbares Python, das man sich einmal ansehen sollte.

Einfache Aktionen wie das Schließen eines Fensters kann man mit dem Qt-Designer direkt definieren. Das Schreiben von Programmzeilen wie mit anderen Designtools ist damit aber nicht möglich. Daher gehört es zu den Aufgaben der ei-

iX-Workshop

Python

Python – Interaktion mit Linux

Dieser Workshop bietet einen praxisorientierten Einstieg in das administrative Arbeiten mit der Programmiersprache Python im Linux-Umfeld. Dabei wird Bezug auf aktuelle Technologien genommen.

Basierend auf der aktuellen Implementierung Python 3.x wird neben der Sprache Python unter anderem das Benutzen und Erstellen von REST-Schnittstellen demonstriert.

Voraussetzungen:

Als Teilnehmer des Workshops sollten Sie ein grundlegendes Verständnis für die Systemadministration unter Linux und Programmierkenntnisse der Sprache Python mitbringen. Grundelegende Kenntnisse von KVM und Docker sind nicht zwingend erforderlich.

Termin: 22. bis 23. November 2018 in Nürnberg

Frühbucherticket: 1.480,50 Euro (bis 10.10.2018)

Standardticket: 1.645,00 Euro

alle Preise inkl. MwSt.



Weitere Infos unter:
www.heise-events.de/python
www.ix-konferenz.de

Ihr Referent wird
gestellt von:



Eine Veranstaltung von:



Organisiert von:



Listing 4: qtquick.qml

```

1 import QtQuick 2.5
2 import QtQuick.Controls 1.4
3
4 ApplicationWindow {
5
6     width: 300
7     height: 200
8     title: "Qt Quick"
9
10    Button {
11        anchors.centerIn: parent
12        text: 'Schließen'
13        onClicked: Qt.quit()
14    }
15 }

```

Listing 5: qtquick.py

```

1 from PyQt5.QtWidgets import QApplication
2 from PyQt5.QtQml import *
3
4 app = QApplication([])
5
6 engine = QQmlApplicationEngine()
7 engine.load('qtquick.qml')
8
9 win = engine.rootObjects()[0]
10 win.show()
11
12 app.exec_()

```

genen Klasse, eine Verbindung zum restlichen Programm herzustellen.

Nachdem die Methode *setupUI* gelau-
fen ist, sind alle darin enthaltenen Objekte
bekannt und können genauso wie selbst
definierte angesprochen werden. Deshalb
unterscheidet sich die Zuweisung der Er-
eignisse nicht.

Für das erstellte Design bietet der Qt-
Designer dem Programmierer eine Voran-
sicht, bei der er zwischen verschiedenen
Plattformen wählen kann. Das vermittelt
dem Programmierer ein erstes Gefühl da-
für, wie sein eigener Dialog auf den un-
terschiedlichen Betriebssystemen ausse-
hen könnte:

```
self.dbFileButton.clicked.connect _  
    (self.showFileDialog)
```

Texte für jeden verständlich

Oberflächen enthalten Texte, die für jede Sprache zu übersetzen sind, in der es die Anwendung geben soll. Qt bietet dafür den Befehl *pylupdate5*, der aus dem Programmtext alle betreffenden Zeichenketten herausfiltert, seien es Menüpunkte, Beschriftungen von Befehlsknöpfen, Tooltips oder Statusanzeigen. Welche Quelldateien er untersuchen soll, findet der Befehl in einer Steuerdatei mit der Endung *.pro*.

Für das einfache Beispiel in *trans.py* enthält diese Datei die Beschreibung der Quelle in der Variablen *SOURCES* und die gewünschten Übersetzungsdateien in der Variablen *TRANSLATIONS*:

```
SOURCES = trans.py  
TRANSLATIONS = trans_de.ts
```

Für jede Sprache wird eine eigene Datei benötigt. *pylupdate5* erzeugt die Dateien mit der Endung *.ts* oder ergänzt sie, falls bereits Einträge vorhanden sind:

```
pylupdate5 -verbose trans.pro
```

Eine ts-Datei ist eine XML-Datei, die die Zeichenketten und gegebenenfalls deren

grammierung mit HTML kennt. Der Entwickler beschreibt die Elemente in einer Datei, und Qts QML-Engine erzeugt daraus die gewünschten ausführbaren Objekte. Die Bibliothek Qt Quick enthält die Elemente zur Erstellung einer Oberfläche mit Qt QML.

Die Beispiel-QML-Datei *qtquick.qml* (Listing 4) zeigt eine einfache Anwendung, die aus einem Befehlsknopf besteht, der das erzeugte Fenster wieder schließt. Eine QML-Datei beginnt mit dem Import der darin verwendeten Objekte, hier der Oberflächenelemente von Qt Quick. Danach folgt das erste Objekt, im Beispiel vom Typ *ApplicationWindow*, mit den Attributen, die es besitzt. Die Syntax erinnert stark an JSON-Objekte in JavaScript oder Dictionaries in Python. Ein Objekt kann wieder andere Objekte enthalten, im Beispiel einen Befehlsknopf.

Im nächsten Schritt gilt es, diese Datei in Python zum Laufen zu bringen (Listing 5). Als Erstes braucht man ein Applicationsobjekt – einfachheitshalber ohne Parameter, deshalb die leere Liste. Dann kommt die QML-Engine hinzu, die die QML-Datei mit der Beschreibung lädt und die eigentliche Arbeit übernimmt. Das erste Objekt, das die QML-Engine aus der Datei geladen hat, ist das *ApplicationWindow*, das Python wie jedes andere Fenster in Qt mit der Methode *show* anzeigt.

Fazit

Qt Quick bietet hilfreiche Unterstützung bei der Erstellung von Oberflächen. Da diese Bibliothek noch neu ist, gibt es wenige Beispiele für ihren Einsatz. Ihre Vorteile zeigen sich bei Oberflächen, die sich vom gängigen Desktop-Design unterscheiden, etwa für Geräte im IoT-Bereich. Die klassischen Qt Widgets kommen aus der Desktop-Entwicklung und sind damit groß geworden.

Das Framework Qt ist eine bewährte Herangehensweise, Oberflächen auf unterschiedliche Plattformen zu bringen. Darüber hinaus bietet es viele Module – beispielsweise für Datenbankzugriffe oder das Erstellen von Grafiken, die auf unterschiedlichen Betriebssystemen laufen.

(ka@ix.de)

Gerhard Völkl

ist Fachjournalist für Python, Datenbankprogrammierung und Computergrafik.

Alle Links: ix.de/ix1810130



SEMINARE FÜR MEHR SOFTWARE QUALITÄT

AGILE METHODEN

Requirements Engineering für die agile Softwareentwicklung	27.11.2018 - 28.11.2018	München
--	----------------------------	---------

ARCHITEKTUR

ISAQB Certified Professional for Software Architecture - Foundation Level (CPSA-FL)	05.11.2018 - 08.05.2018	Frankfurt, Hamburg
	12.11.2018 - 15.11.2018	Berlin, Köln
	26.11.2018 - 29.11.2018	Frankfurt, Hamburg
	03.12.2018 - 06.12.2018	München
	10.12.2018 - 13.12.2018	Berlin, Köln

EMBEDDED SYSTEME

Funktionale Sicherheit	09.10.2018 - 10.10.2018	München
------------------------	----------------------------	---------

PROJEKTMANAGEMENT

Aufwandsschätzung in Softwareprojekten	17.10.2018 - 18.10.2018	Berlin, Hamburg
	14.11.2018 - 15.11.2018	Frankfurt, Köln
	21.11.2018 - 22.11.2018	München

RISIKOMANAGEMENT

Risikomanagement in Softwareprojekten	16.10.2018	Berlin, Hamburg
	13.11.2018	Frankfurt, Köln

REQUIREMENTS

IREB Certified Professional for Requirements Engineering Foundation Level (CPRE-FL)	23.10.2018 - 25.10.2018	Berlin, Köln
	13.11.2018 - 15.11.2018	München



Professionelles Requirements Engineering und Management	18.12.2018 - 20.12.2018	München
---	----------------------------	---------

PROGRAMMIERUNG & CODE

Testgetriebene Softwareentwicklung	16.10.2018 - 18.10.2018	Frankfurt, Köln
	23.10.2018 - 25.10.2018	Berlin, Hamburg
	06.11.2018 - 08.11.2018	München

TESTEN

ISTQB Certified Tester - Foundation Level (CTFL)	06.11.2018 - 08.11.2018	Berlin, Köln
	18.12.2018 - 20.12.2018	München
ISTQB Certified Tester - Foundation Level (CTFL), (English)	04.12.2018 - 06.12.2018	München



ISTQB Certified Tester - Advanced Level: Test Manager (CTAL-TM)	26.11.2018 - 30.11.2018	München
	03.12.2018 - 07.12.2018	Berlin, Köln
	10.12.2018 - 14.12.2018	Frankfurt, Hamburg
ISTQB Certified Tester - Advanced Level: Technical Test Analyst (CTAL-TTA)	13.11.2018 - 15.11.2018	München



ISTQB Certified Tester - Advanced Level: Test Analyst (CTAL-TA)	22.10.2018 - 25.10.2018	Frankfurt, Köln
	05.11.2018 - 08.11.2018	Berlin, Hamburg
	10.12.2018 - 13.12.2018	München

Testgrundlagen für Softwareentwickler	09.10.2018 - 11.10.2018	München
	20.11.2018 - 22.11.2018	Frankfurt, Köln
	04.12.2018 - 06.12.2018	Berlin, Hamburg

Prometheus-Tutorial, Teil 3: Skalieren und effektiv einsetzen

Besser überwachen



Martin Loschwitz

Welche nützlichen Prometheus-Erweiterungen stehen zur Verfügung und wie müssen Admins vorgehen, wenn das Monitoring in die Breite wachsen soll?

iX-TRACT

- Telegraf ist eine sinnvolle Alternative zum Prometheus Node Exporter und verfügt über einen deutlich größeren Funktionsumfang.
- Spezielle Exporter für einzelne Applikationen liefern mehr und vor allem bessere Metrikdaten als die generischen.
- Im Gespann mit Prometheus erledigt InfluxDB die Langzeitspeicherung von Daten zuverlässig und gut.

Während sich der erste Tutorialteil vorrangig mit Prometheus selbst in Abgrenzung zu etablierten Monitoringverfahren beschäftigte, war der zweite Teil sehr praktisch und erklärte die Installation eines basalen Prometheus-Clusters. Ist der Admin erst einmal so weit gekommen, steht ihm ein verlässliches Monitoring-Tool zur Verfügung – doch perfekt ist die Situation vermutlich noch nicht.

Spätestens, wenn Prometheus unter der Last der in ihm abgelegten Metrikdaten zu stöhnen beginnt, ist guter Rat teuer: Wie skaliert man Prometheus sinnvoll, welche Fallstricke gilt es zu beachten und welche Lösungsmöglichkeiten stehen zur Verfügung? Dieser dritte und letzte Teil des Tutorials ist ein Potpourri verschiedener Tipps und Hinweise, die großteils aus der direkten betrieblichen Erfahrung des Autors stammen – und das Potenzial haben, manchem Admin buchstäblich den Hintern zu retten.

Node Exporter? Schön und gut, aber ...

Der erste Rat direkt aus dem Alltag bezieht sich auf den Node Exporter, der als Komponente quasi zu Prometheus gehört – auch wenn er separat vom eigentlichen Monitoring-Tool entwickelt wird. Zur Erinnerung: Prometheus ist nach dem Prinzip konstruiert, dass das MAT-Paket (Monitoring, Alerting und Trending) Metrikdaten direkt auf den Zielsystemen einsammelt. Auf Letzteren laufen dazu die Agenten, die im Prometheus-Sprech „Exporter“ heißen: Sie sammeln die Metrikdaten lokal ein und stellen sie über eine API nach dem REST-Prinzip zum Download bereit. Die laufende Prometheus-Instanz verfügt im Gegenzug über ein jederzeit aktuelles Verzeichnis aller Exporter auf den Zielsystemen und fragt diese reihum ab. Am Ende hat Prometheus die Metrikdaten aller Zielsysteme.

Der bekannteste Vertreter im Prometheus-Universum ist zweifellos der Prometheus Node Exporter (Abbildung 1). Er sammelt elementare Metriken wie die RAM-Nutzung, die anliegende CPU-Last oder den Füllstand der Festplatten des Systems. Weil er modular aufgebaut ist, ermöglicht er aber auch das Erfassen ausgefällerer Metrikdaten, etwa über das DRBD-Plug-in. Das Funktionsschema ist stets dasselbe: Per Konfigurationsdatei legt der Admin fest, welche Plug-ins der Node Exporter grundsätzlich aufzeichnen soll. Es empfiehlt sich hier freilich, nur



Der Prometheus Node Exporter zeichnet verschiedene Systemparameter auf, die sich anschließend per Grafana darstellen lassen (Abb. 1).

die Daten zu sammeln, die auf dem System tatsächlich anfallen. Es ist etwa völlig sinnlos, DRBD-Metriken auf Systemen zu erfassen, die gar kein DRBD haben. Davon abgesehen funktioniert das Prinzip aber super. Weil Prometheus beim Einsammeln von Metrikdaten – dem „Scraping“ – stets alle Daten eines Exporters holt, fällt auf der Prometheus-Seite auch kein zusätzlicher Aufwand an.

Wer auf der Suche nach basalen Leistungsdaten seines Systems ist, wird mit den Metrikdaten, die der Node Exporter einsammelt, vermutlich glücklich – es sei denn, dass auf den Systemen Parameter zu prüfen sind, die der Node Exporter ob eines fehlenden Plug-ins schlicht nicht erheben kann. Der Admin steht dann im sprichwörtlichen Regen, denn ohne Weiteres lässt sich der Node Exporter nicht erweitern. Das ginge nur über ein separates Plug-in. Es ist zwar nicht unmöglich, ein solches zu schreiben – aber aufwendig ist der Vorgang definitiv.

Unterstützung vom TICK-Stack

Gut, dass es eine Alternative gibt. Die kommt aus eher unerwarteter Richtung – von den Entwicklern des TICK-Stacks. TICK steht für „Telegraf, InfluxDB, Chronograf, Kapacitor“ und bezieht sich damit auf ein direktes Prometheus-Konkurrenzprodukt (Abbildung 2). Denn InfluxDB ist schließlich selbst eine waschechte Zeitreihendatenbank und die erwähnten Werkzeuge entsprechen ungefähr den Prometheus-Komponenten: InfluxDB ist das Äquivalent zu Prometheus, Telegraf das Gegenstück zum bereits er-

wähnten Node Exporter und Chronograf wie Kapacitor spiegeln im Tandem die Alertmanager-Funktionen wider.

Weil Prometheus und InfluxDB aber beide im Open-Source-Umfeld unterwegs sind, haben die Entwickler der Lösungen schon vor Jahren beschlossen, dass Freundschaft cool ist, und ihre Werkzeuge einfach kompatibel gemacht. Aus Sicht des Systemadministrators ist das ein Geschenk des Himmels, denn er kann die Komponenten der beiden Stacks beinahe beliebig miteinander kombinieren. Insbesondere kann er die Aufgabe, Metrikdaten von den Zielsystemen einzusammeln, vom Node Exporter auf Telegraf übertragen – und so sein Setup um eine Reihe nützlicher Funktionen erweitern.

Doppelbekämpfung hilft nicht

Klar, die Grundfunktionen und die Liste der Metriken, die Telegraf erfasst, unterscheiden sich zunächst gar nicht groß von dem, was der Prometheus Node Exporter liefert. Viele Admins lassen auf den Zielsystemen beide Dienste gleichzeitig laufen, was allerdings nur bedingt sinnvoll ist. Denn letztlich sammelt man so die meisten Metrikdaten doppelt ein, und zwar einmal über den Node Exporter und

einmal über Telegraf. Wer beide Dienste auf den Zielsystemen laufen lassen möchte, sollte sie so konfigurieren, dass sie nur die Metrikdaten erheben, die das jeweils andere Programm mangels der nötigen Funktionen nicht liefern kann. Für die Grundmetrikdaten sollte man sich entweder für den Node Exporter oder für Telegraf entscheiden.

Wobei Administratoren in den meisten Fällen vermutlich Telegraf den Vortritt lassen. Denn über dessen Funktionsumfang lässt sich nicht meckern: Die gängigen Metrikdaten wie CPU-Last und RAM-Nutzung liest der Dienst natürlich aus, hinzu gesellen sich jedoch diverse zusätzliche Plug-ins. Postfix lässt sich mit Telegraf ebenso überwachen wie OpenLDAP, nginx, MySQL (oder MariaDB) oder Redis. Und falls partout mal kein Plug-in in Telegraf für eine bestimmte Software verfügbar ist, erleichtert der Dienst Admins händische Nachrüstungen deutlich: Telegraf genügt ein Shell-Script mit entsprechender Ausgabe, das regelmäßig aufzurufen ist. Die so generierten Metrikdaten wandelt es dann ins Prometheus-Format und lässt Prometheus sie auslesen. Damit das funktioniert, aktiviert der Admin in Telegraf einfach das Prometheus-Output-Plug-in – wie das geht, verrät die Dokumentation (siehe ix.de/ix1810138).

Tutorialinhalt

- Teil 1: Monitoring per Zeitreihendatenbank
- Teil 2: Installation und Konfiguration von Prometheus
- Teil 3: Prometheus mit Begleitkomponenten anreichern**

Andere Labels, andere Dashboards

Aus Systemverwaltersicht ist es sinnvoll, die Frage „Telegraf oder Node Exporter?“ am Anfang zu beantworten – denn so erspart man sich später zusätzliche Arbeit.

Erfolgt die Umstellung im laufenden Betrieb, ist ein bisschen Aufräumen im Nachgang nötig – was insbesondere daran liegt, dass der Node Exporter und Telegraf unterschiedliche Namen (Labels) für die einzelnen Metriken nutzen.

Anders formuliert: Die vom Node Exporter gesammelten Metriken heißen anders als die in Telegraf. Das ist dann relevant, wenn man auf Basis der Werte einzelner Metrikdaten die Alarmierung in Prometheus konfiguriert hat. Das Anzeigen grafischer Dashboards in Grafana ist ebenfalls betroffen. Sowohl die Alarne als auch Grafana-Dashboards setzen letztlich auf Prometheus-Abfragen, bei denen sie die Metrikdaten für bestimmte Labels auslesen. Ändern sich die Labels, sind die entsprechenden Prometheus-Querys zu ändern.

Immerhin: Im Dashboard-Shop von Grafana finden sich diverse Dashboards, die auf die Kombination Prometheus und Telegraf ausgelegt sind (siehe ix.de/ix1810138). Wer sich allerdings ein spezifisches lokales Setup gebaut hat, wird in den meisten Fällen nicht umhinkommen, dieses nach einem Umstieg auf

Telegraf anzupassen. Das Mehr an Funktionen, das Telegraf bietet, lohnt den Aufwand aber definitiv (Abbildung 3).

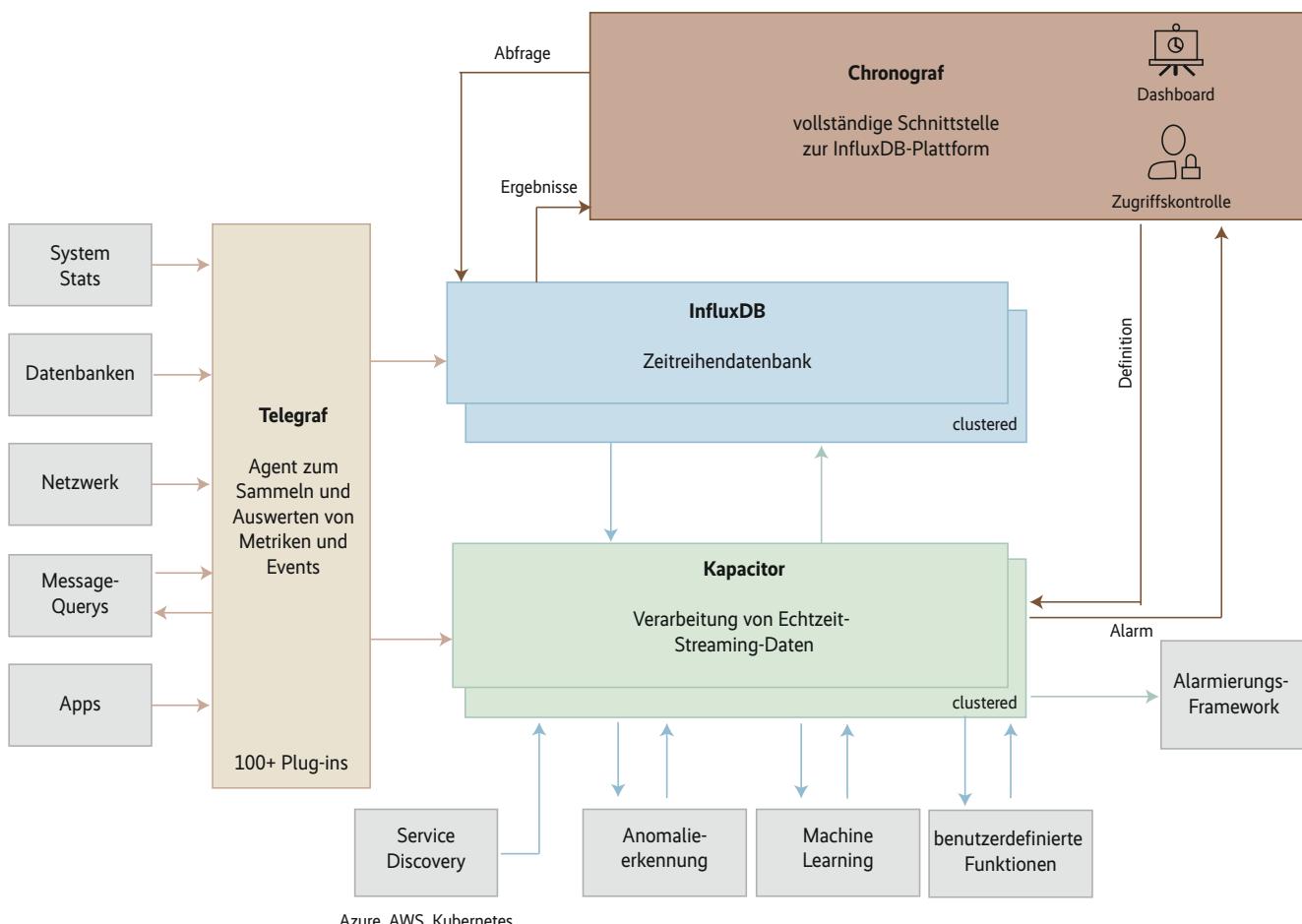
Noch mehr Metriken

Selbst wenn die vorangegangenen Absätze den Eindruck vermitteln, so handelt es sich bei Telegraf nicht um die eierlegende Wollmilchsau im Kontext der Metrikbeschaffung bei Zeitreihendatenbanken. Zwar ist der Funktionsumfang von Telegraf in der Tat deutlich größer als der des Node Exporters von Prometheus. Jedoch sind verschiedene Einsatzzwecke so speziell, dass weder der Node Exporter noch Telegraf sie abdecken. Hinzu kommt, dass Telegraf zwar für viele Dienste rudimentäre Metrikdaten sammeln kann, oft genug jedoch gibt es für die jeweiligen Programme eigene Prometheus-Exporter, die umfangreicher sind und besser funktionieren.

Steht für den eigenen Dienst ein solcher Exporter zur Verfügung, ist es sicherlich sinnvoll, diesen auch zu verwenden. Daraus ergeben sich aber mehrere ganz

praktische Konsequenzen. Zunächst gilt: Jeden Exporter muss der Admin in seine Automation integrieren. Soll etwa der offizielle MongoDB-Exporter auf allen MongoDB-Servern zum Einsatz kommen, sorgt er dafür, dass die Komponente per Ansible, Chef, Puppet, Salt oder wie auch immer automatisch ihren Weg auf die betroffenen Systeme findet. Denn wenn insgesamt 250 Systeme mit entsprechenden Funktionen zu überwachen sind, ist das händische Ausrollen des jeweiligen Exporters eine Fleißarbeit, für die im Alltag der modernen IT die Zeit und die Notwendigkeit schlicht nicht mehr vorhanden sind. Ein noch besseres Beispiel ist hier der offizielle IPMI-Exporter, der auf den Systemen Werte wie Stromverbrauch und die Geschwindigkeiten der einzelnen Lüfter aufzeichnet – der sollte wirklich auf jedem System der Plattform vorhanden sein, falls IPMI zur Verfügung steht (und nicht etwa Dell dRAC, IBM RSA oder HP iLO).

Auch das Thema Iptables spielt eine wichtige Rolle. Denn für jeden Exporter auf den Zielsystemen ist im Zweifelsfall ein lokaler Port zu öffnen, damit Prome-



Eigentlich ist der TICK-Stack ein Konkurrenzprodukt zu Prometheus; im Gespann ergänzen sich die beiden Ansätze allerdings hervorragend (Abb. 2).

theus später auf die API zugreifen kann. Gerade im Corporate-Kontext ist das aus Compliance-Gründen oft ein großer Aufwand und bedingt viel Dokumentation und Diskussion. Setzt man, wie in Teil 2 des Tutorials beschrieben, Consul ein, fällt es leicht, nach dem Installieren des zusätzlichen Exporters Prometheus mit diesem bekannt zu machen. Denn es genügt, auf den betroffenen Systemen einen Serviceeintrag in Consul zu ergänzen. Der Weisheit letzter Schluss ist der Ansatz allerdings nicht, denn gerade das Iptables-Thema birgt viel Problempotenzial.

Leichter mit Telegraf

An dieser Stelle eilt Telegraf dem Admin allerdings nochmals zu Hilfe – und bietet eine elegante Lösung, auf den einzelnen Knoten zusätzliche Exporter auszurollen. Telegraf übernimmt bei Bedarf nämlich die Vermittlung zwischen Exportern auf dem System und dem zentralen Prometheus-Server. Und das geht so: Per Prometheus-Import-Plug-in fragt Telegraf bei den lokalen Exportern die dort vorhandenen Metrikdaten ab und speichert sie zwischen. Das bedeutet einerseits, dass der jeweilige Exporter nur einen Port auf 127.0.0.1 öffnen muss, sodass Iptables außen vor bleibt. Und andererseits erspart sich der Admin die Bastelei in Consul, muss im Gegenzug aber die Telegraf-Konfiguration auf dem Host so anpassen, dass sie die lokalen Exporter abfragt. Aus Compliance- und Sicherheitssicht ist dieser Ansatz aber in den meisten Fällen trotzdem der sinnvollere, weil er aus der Host-Firewall keinen Schweizer Käse macht – was Sicherheitsbeauftragte ruhiger schlafen und arbeiten lässt.

Das Ende des Exporter-Themas ist ein wichtiger Hinweis: Viele und gerade moderne Anwendungen, die „Cloud-ready“ sein sollen, sind schon auf den Prometheus-Zug aufgesprungen und bieten eine Schnittstelle, über die Prometheus direkt Metriken abfragen kann. Ein Exporter ist dann unnötig. Ein gutes Beispiel ist der verteilte Objektspeicher Ceph: Der hat für Prometheus eine Metrikschnittstelle, die die ohnehin aufgezeichneten Performance daten für Ceph exponiert. In Prometheus kann der Admin auf diese Weise Metrikdaten bis hin zu einzelnen Festplatten seines Ceph-Clusters darstellen. Nicht immer muss es also ein Exporter sein. Wer Prometheus installiert, sollte auf der Übersicht im Prometheus-Wiki nachschauen, ob die genutzte Software nicht ohnehin passende Metrikdaten bereitstellt (siehe [ix.de/ix1810138](#)).



Auch für per Telegraf gesammelte Daten existieren fertige Dashboards in Grafana, die die Daten optisch aufbereitet darstellen (Abb. 3).

Hat der Admin sein Setup auf Basis der bisherigen Tipps und Hinweise mit den nötigen Exportern nur so zugepfostert, werden diese ihm schon bald zu einem echten Graus. Das ist spätestens dann der Fall, wenn Prometheus unter der Last der abgelegten historischen Metrikdaten zu ächzen beginnt und immer langsamer wird.

Das leidige Thema Skalierbarkeit

Eben dieser Umstand ist einer der größten Treppenwitze in der Karriere des Autors dieses Artikels: Ursprünglich war die Wahl auf Prometheus gefallen, weil sich damit im Gegensatz zu klassischen Monitoringsystemen wie Nagios auch der Trending-Teil perfekt umsetzen ließ. Im Laufe des PoC-Projektes kam allerdings sukzessive heraus, dass Prometheus für die langfristige Speicherung großer Mengen an Metrikdaten völlig ungeeignet ist – irgendwann reagiert es nur noch langsam und behäbig. In den letzten Prometheus-Versionen haben die Entwickler diesen Effekt abgemildert. Dennoch ist aber weiterhin unbedingt davon abzuraten, Prometheus mit historischen Metrikdaten von Hunderten oder gar Tausenden Hosts zu füttern, die bis in die graue Vorzeit zurückreichen.

Und damit ist dieser Artikel beim Thema Skalierbarkeit angekommen, also bei der Frage, wie ein Prometheus-Setup aus-

sehen muss, damit es auch bei vielen zu überwachenden Systemen und langem Vorhalten der Metrikdaten noch funktioniert, statt zu implodieren. Eine sinnvolle Antwort lässt sich nur dann geben, wenn man sich zunächst die beiden wichtigsten Faktoren anschaut, die bei Prometheus im Hinblick auf Skalierbarkeit von Bedeutung sind: Einerseits geht es um die schon erwähnte Fähigkeit, mit alten Metrikdaten effizient umzugehen. Und andererseits spielt natürlich die Frage eine Rolle, wie viele Zielsysteme eine einzelne Prometheus-Instanz realistisch abarbeiten kann, bis das Tool an die Grenzen seiner Leistungsfähigkeit kommt. Hat man etwa 1000 Systeme und möchte 250 Metrikwerte pro Server alle 15 Sekunden auslesen, sieht Prometheus sich pro Minute immerhin einer Million Messwerten gegenüber, die es erst mal zu verarbeiten gilt.

Die gute Nachricht: Für beide Probleme gibt es funktionale Lösungen. Die weniger gute Nachricht lautet: Beide lassen sich nicht mit demselben Ansatz erschlagen – der Admin braucht also derer zwei, die unabhängig voneinander sind. Beide Teile beschreibt dieser Artikel in den folgenden Absätzen.

Skalieren in die Breite

Zunächst geht es um die Frage, wo die Performancegrenzen einer einzelnen Prometheus-Instanz liegen und wie sich Setups abdecken lassen, deren Knoten-

zahl höher ist. Grundsätzlich gilt: Prometheus kommt ab Werk ohne einen klassischen Cluster-Mechanismus und hat auch keinen integrierten, verteilten Speicher. Die Daten liegen bei Prometheus immer lokal. Mehrere Instanzen lassen sich also nicht so, wie man das etwa von Galera für MySQL kennt, zu einem Cluster zusammenschalten. Am nächsten kommt diesem Prinzip die Federation-Funktion, die Prometheus seit einigen Releases hat. Mancher Admin soll schon auf die Idee gekommen sein, eine zentrale Prometheus-Instanz zu bauen, die selbst gar keine Metrikdaten bei Zielsystemen einsammelt, sondern per Federation-Funktion die gesamten Inhalte anderer Instanzen abfragt. Hiervon raten die Entwickler allerdings offiziell ab und bezeichnen den Vorgang gar als „Missbrauch“ der Federation-Funktion – zumal die Lösung auch nur auf dem Papier zufriedenstellend funktioniert. In der Praxis ergeben sich in dieser Konstellation schnell Probleme epischen Ausmaßes.

Die fehlende Clusterfähigkeit von Prometheus war bereits mehrmals Gegenstand heftiger Diskussionen im Kreise der Entwickler. Diverse Firmen haben in der Vergangenheit an Lösungen gearbeitet,

die mittlerweile aber allesamt wieder in der Versenkung verschwunden sind. Langer Rede kurzer Sinn: Klassisches Clustering mit Prometheus funktioniert nicht, der Admin braucht eine andere Taktik.

Glücklicherweise erleichtert Prometheus und die Werkzeuge aus seinem Ökosystem das einigermaßen – und die Lösung für das Problem ist im zweiten Teil des Tutorials schon Thema gewesen. Denn letztlich muss sich der Admin nur des klassischen Sharding bedienen, so wie man es von Mailservern kennt. Heißt konkret: Verschiedene Prometheus-Instanzen kümmern sich um Teile des gesamten Setups. Möchte man diese hochverfügbar machen, kann man auch mehrere Prometheus-Instanzen dieselben Teile der Installation abfragen lassen, sodass die jeweiligen Daten mehrmals unabhängig vorhanden sind.

Knifflige Konfiguration

Wer Sharding nutzen möchte, sollte sich über das Setup zuvor ein paar Gedanken machen – denn es gestaltet sich zumindest etwas komplexer als das Setup mit nur einer Prometheus-Instanz. Beim Ein-

satz von Consul muss man etwa sicherstellen, dass die Prometheus-Instanzen tatsächlich nur ihre Zielsysteme abfragen und nicht das gesamte Setup. Verglichen mit der Komplexität, die der Admin sich bei verteilten Storage-Lösungen im Cluster-Modus ans Bein bindet, ist die Lösung auf Basis von Sharding bei Prometheus allerdings überschaubar und führt zum gewünschten Resultat.

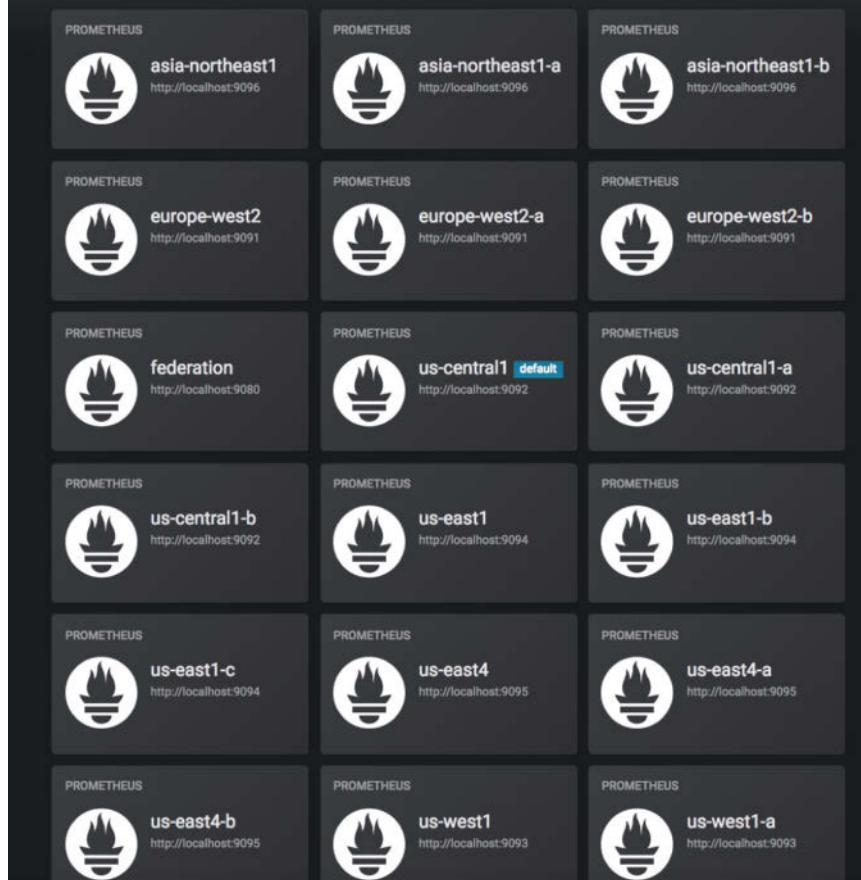
Übrigens: Die modulare Architektur von Prometheus und der Begleitkomponenten führt dazu, dass der Vorteil des „Single Point of Administration“ durch den Einsatz mehrerer Prometheus-Instanzen nicht verloren geht. Grafana lässt sich im Hintergrund an mehrere Prometheus-Instanzen anbinden, und ein Alertmanager in einer Installation kann problemlos die Alarne verschiedener Instanzen von Prometheus verarbeiten. Hinzu kommt, dass der Alertmanager sogar einen echten Clustermodus hat, also im HA-Betrieb funktioniert. Wer daher die Administration der Umgebung nicht auf verschiedene Punkte aufteilen möchte, muss das auch nicht tun – und kann das Überwachen der Graphen sowie das Alerting zentral bündeln.

Daten sinnvoll dauerhaft speichern

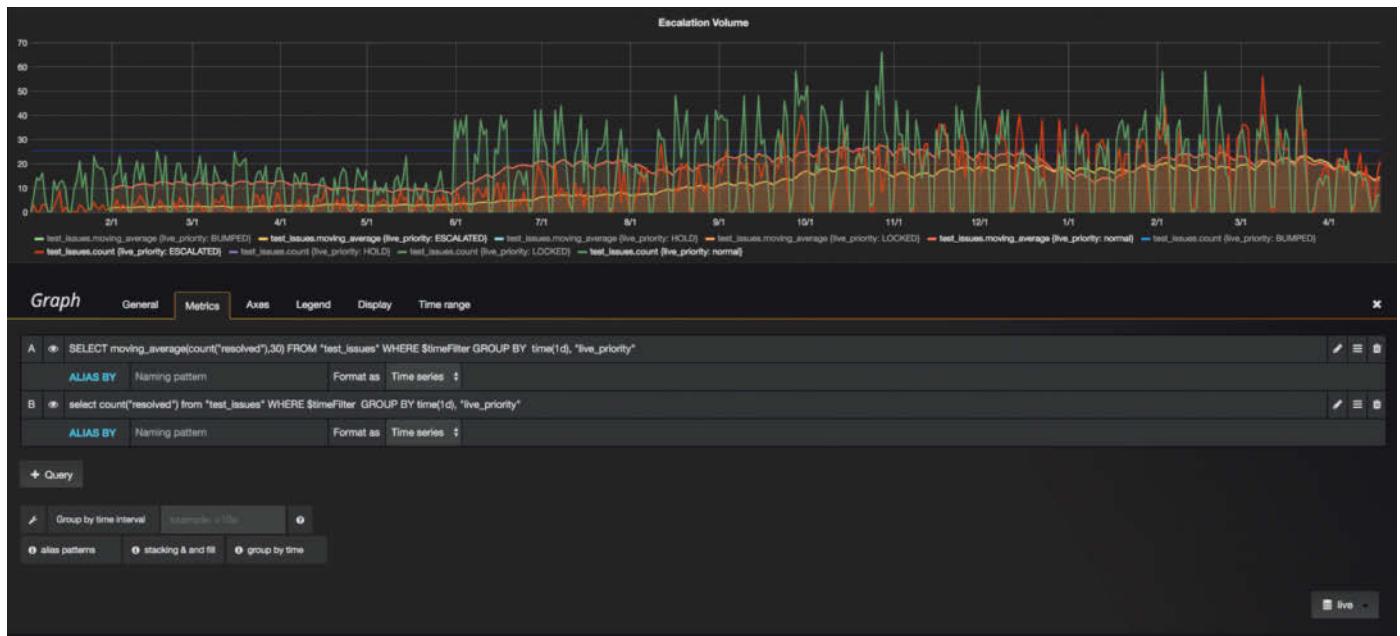
Wie begegnet man der eigentlich größeren Herausforderung, nämlich der im Hinblick auf Performance effizienten Langzeitspeicherung von Trending-Daten? So viel sei vorab verraten: nicht mit Prometheus. Auch hier gereicht dem Admin die Tatsache ein weiteres Mal zum Vorteil, dass Prometheus freie Software ist und sich über seine Schnittstellen mit verschiedenen anderen Anwendungen schnell und leicht kombinieren lässt. Frei nach dem Motto: Wenn Prometheus sich nicht sinnvoll für Long-Term Trending nutzen lässt, kommt halt eine andere Lösung zum Zug, die Prometheus sinnvoll ergänzt.

Das funktioniert so: Im Backend installiert man zusätzlich zum schon existierenden Prometheus eine weitere Zeitreihendatenbank, die sich besser für das Long-Term Trending eignet. InfluxDB sowie Graphite sind dabei die naheliegenden Alternativen und bieten beide bessere Leistung, wenn es darum geht, die Trending-Daten langfristig zu speichern. Im folgenden Beispiel geht der Text von InfluxDB aus.

Wobei das an dieser Stelle gar keinen großen Unterschied bedeutet: Prometheus hat nämlich eine Plug-in-Schnittstelle, über die es Treiber für externen Speicher nachladen kann – und Plug-ins existieren



In Grafana lassen sich diverse Prometheus-Instanzen problemlos als verschiedene Datenquellen nutzen (Grafik: PerimeterX) (Abb. 4).



Zwar benötigt man für InfluxDB und Trending in Grafana eine weitere, eigene Datenquelle und eigene Einstellungen – doch dann klappt es auch mit der Langzeitdarstellung von Daten (Abb. 5).

sowohl für InfluxDB als auch für Graphite. Konkret bedeutet das: Prometheus kann anhand der Konfiguration des Admins spezifische Metrikdaten von sich aus und direkt in InfluxDB ablegen – oder in Graphite, OpenTSDB, Gnocchi und diversen anderen Datenbanken – und so deren Fähigkeiten zum langfristigen Speichern von Metrikdaten nutzen (siehe ix.de/ix1810138).

Die Guten ins Töpfchen ...

Selbst wenn InfluxDB oder Graphite deutlich besser darin sind, Metrikdaten auch langfristig zu speichern: Der Admin sollte sich unbedingt die Frage stellen, welche Metrikdaten er überhaupt dauerhaft aufheben muss. Nicht selten führt die Kombination aus Prometheus und InfluxDB dazu, dass kurzerhand sämtliche Prometheus-Daten ihren Weg nach InfluxDB finden – völlig sinnlos: Nur in den aller seltesten Fällen dürfte es den Admin interessieren, welche Antwortzeiten die eigenen Load Balancer an einem Samstagmittag vor drei Jahren hatten. Eher wird er wissen wollen, wie sich die Nutzung virtueller CPUs und virtuellen RAMs in den vergangenen Jahren entwickelt hat. Und selbst dafür braucht er nicht alle Werte der jeweiligen Metrik im 15-Sekunden-Abstand über die letzten fünf Jahre; stattdessen genügen gut gemittelte größere Intervalle. Oder anders formuliert: Bevor der Admin Daten aus Prometheus in InfluxDB oder Graphite schreiben lässt, sollte er das sogenannte „Downsampling“ vollziehen, also die Menge der zu schreibenden Daten auf sinnvolle Werte runterrechnen.

Ist dieser Schritt vollzogen, ist der Rest simpel: Man konfiguriert den Connector für InfluxDB in Prometheus und stellt sicher, dass der Datentransfer wie gewünscht funktioniert. Dann richtet man Prometheus so ein, dass die Daten, die ihren Weg zu InfluxDB erfolgreich gefunden haben, aus Prometheus selbst gelöscht werden. Der größte Teil der Konfiguration ist damit im Grunde schon fertig.

Was allerdings noch fehlt, ist die optimale Aufbereitung der InfluxDB-Daten. Für die zeichnet wie üblich Grafana verantwortlich. Einmal mehr zeigt sich an dieser Stelle, dass die Grafana-Architektur flexibel und mächtig zur selben Zeit ist. Denn InfluxDB lässt sich einfach als zusätzliche Datenquelle in Grafana einrichten und rangiert auf derselben Ebene wie Prometheus – auch wenn sich die bestehenden Dashboards nicht unmittelbar recyceln lassen. Der Admin sollte hier etwas Zeit einplanen, um passende Dashboards für den eigenen Bedarf zu entwerfen. Lediglich an den Alertmanager lässt sich InfluxDB nicht ohne Weiteres anschließen – aber das wäre auch völlig unnütz, denn für die Alarmierung ist ja ausschließlich Prometheus verantwortlich (siehe Abbildung 4 und 5).

Und Schluss

Durch das Einrichten eines effizienten und mächtigen Long-Term Trending auf Basis von InfluxDB fügt der Admin seinem Setup die letzte noch fehlende Komponente hinzu – und ist mit seinem MAT grundsätzlich fertig. Im Rahmen der drei Tutorialteile hat Prometheus sich als ein

potentes und vielseitiges Werkzeug für Monitoring, Alerting und Trending herausgestellt, das den Vergleich mit den etablierten Vertretern wie Nagios nicht scheuen muss. Die Kombination aus Prometheus, Grafana, dem Node Exporter, dem Alertmanager und Drittanbieterkomponenten wie Telegraf bringt zusätzliche Funktionen.

Für viele der ausführenden Admins dürfte die größte Herausforderung bei der Nutzung von Prometheus das sprichwörtliche Umparken im Kopf sein. Denn es gibt genau eine Funktion, die klassische Monitoringsysteme wie Nagios beherrschen, Prometheus aber nicht: das typische „Event-Monitoring“, also etwa das Triggern einer Aktion, weil eine spezifische Zeile in einem Log auf einem System auftaucht.

Spricht man die Prometheus-Entwickler auf diesen vermeintlichen Mangel an, ist die Antwort simpel: Wer Logdateien analysieren möchte, sollte das nicht über eine Krückenkonstruktion in seinem Monitoring tun, sondern durch zentrales Logging mit entsprechender automatischer Logfile-Analyse. Betreiber großer Plattformen dürften in aller Regel ohnehin zentrales Logging nutzen. Wie so oft in der Cloud gilt also das Prinzip, dass man das richtige Werkzeug für eine Aufgabe braucht.

(avr@ix.de)

Martin Loschwitz

ist Public Cloud Architect bei T-Systems und beschäftigt sich vorrangig mit OpenStack, Ceph und Kubernetes.

URL-Shortener im internen Einsatz

Machs kurz



Es begann mit der Suche nach der URL des Incident-Service. Im Intranet brachte sie wie so oft nur Präsentationen und Projektberichte auf den Bildschirm. Nach einigem Telefonieren war sie gefunden: http://z990006.unserefirma.corp/SAPGui/xjj_hhr/servlet/addticket.jsp. Eine intuitiv merkbare und verbal transportierbare URL sieht anders aus.

Diese Situation ist symptomatisch und in vielen Firmen präsent. Während bei öffentlichen Webservices der Dienstleister offenkundig ist und sich die URL dem Benutzer erschließt wie bei dhl.de/sendungsverfolgung, sind URLs in Firmennetzen weit davon entfernt. Dass sich in den heterogenen IT-Landschaften von Firma und Subunternehmen ein einheitliches URL-Schema nur schwer umsetzen lässt, ist dem Benutzer jedoch egal. Er will und muss nicht wissen, ob der Ticketservice von einem SAP oder Remedy gehostet wird. Er will wie bei DHL den gewünschten Dienst mit einer gut merkbaren URL aufrufen können.

Die Technik, von einer kurzen URL auf verschiedene Zielseiten zu verzweigen, ist im Internet verbreitet. Prominente Beispiele sind bit.ly oder goo.gl. Solche URL-Shortener sind in verschiedenen quelloffenen Paketen verfügbar. Dahinter steckt eine relativ triviale Webanwendung, bestehend aus einer Datenbanktabelle mit den zwei Spalten *shortcut* und *targetURL*. Den Aufruf *http://shortener/aShortcut* beantwortet sie mit einem *301* oder *302 HTTP-REDIRECT* auf die zu *aShortcut* gehörende *targetURL*. Der Browser leitet den Benutzer damit automatisch auf diese *targetURL*.

Kai Altstaedt

URL-Shortener sind im öffentlichen Internet eine Selbstverständlichkeit. Auch im Intranet können sie die Effizienz und die Produktivität steigern.

Das eigene Projekt verwendete das Open-Source-Paket YOURLS. Es läuft auf einem einfachen LAMP-Stack und lässt sich durch Plug-ins erweitern. Einige davon sind bereits auf den Einsatz im Intranet abgestimmt, etwa das LDAP-Plug-in. Für die Anbindung an ein Single Sign-on sind ebenfalls nur wenige Anpassungen nötig. Das Einrichten von YOURLS ist in wenigen Stunden erledigt.

Design und Funktion der Startseite lassen sich anpassen, sodass ein Mitarbeiter von hier aus direkt einen Shortcut anlegen kann. Im Projekt sind von dort vier Seiten mit Shortcut-Listen erreichbar: Die erste zeigt alle erstellten Shortcuts alphabetisch („Gelbe Seiten“), die zweite nach Erstellungsdatum, die dritte die Top Ten nach Benutzungszahlen sortiert und die vierte die des Benutzers mit der Option, Shortcuts zu löschen.

Der Charme von URL-Shortenern steigt mit dem Benutzerkomfort. Um den zu erhöhen, kann man sich die Vervollständigungsfunktion der Browser und des DNS zunutze machen. Installiert man etwa den URL-Shortener unter dem FQDN *intra.unserefirma.corp*, löst der Browser die Zeile *intra/incident* wiederum zu einem *http://intra.unserefirma.corp/incident* auf und bekommt dort den HTTP-Redirect auf *http://z990006.unserefirma.corp/SAPGui/xjj_hhr/servlet/addticket.jsp*. Dazu müssen aber die Rechner der Benutzer den Host in der richtigen Domain suchen. Leider funktioniert deshalb die Abkürzung nicht auf Smartphones, wo sie noch wichtiger wäre.

Auf diese Weise aufgesetzt und mit einem kurzen und knackigen DNS Short Name wie *intra*, *link*, *nach* oder *goto* erreichbar, wurde die Funktion sehr schnell

genutzt: Sei es der Verweis auf einen Durchlaufzettel der Unternehmensbibliothek oder der Link auf dem neuesten Plakat der Kommunikationsabteilung. Auch werden in firmeninternen Chatsystemen wie Yammer oder Mattermost-Kanälen mittlerweile die Kurzformen der URL einfach eingetippt statt umständlich aus anderen Browsetabs herauskopiert. Auch die URLs von Validierungs- und Testsystemen sind leichter weiterzugeben: Während das Produktionssystem über *intra/zeit* erreichbar ist, kann man das Validierungssystem mit *intra/zeit_val* ansprechen.

Nur über Freigabeprozesse?

Heftig diskutiert wurde die Frage, ob man einen Freigabeprozess braucht, um einerseits den Missbrauch zu verhindern und andererseits besonders schützenswerte Shortcuts wie *intra/CEO* oder *intra/kommunikation* zu sichern. Die Erfahrung zeigt aber, dass die Hemmschwelle für den Missbrauch in Firmennetzwerken relativ hoch ist.

Im Projekt kann jeder Mitarbeiter beliebige Shortcuts anlegen, die User-ID des Erstellers ist aber für andere Benutzer einsehbar, die ihn direkt kontaktieren können. Konflikte lassen sich einvernehmlich oder hierarchiegetrieben lösen: Wenn der CEO den Shortcut *CEO* haben will, kriegt er ihn, und das Projekt „Creative Engineering Operations“ muss sich einen anderen suchen. Insgesamt gab es nach zwei Jahren Projektaufzeit im Großkonzern und über 2000 angelegten Shortcuts nur drei Konflikte.

Zudem legten die Benutzer die Links in ihrer Sprache an. Während die IT-Abteilung für den Incident-Service den Shortcut *remedy* nahm, erstellten die Anwender Shortcuts wie *problem* und *ticket*. Inzwischen kann man in der alphabetischen Liste zu den Anfangsbuchstaben springen. Am Ende ist sie dadurch nicht nur eine Art Gelbe Seiten, sondern auch ein Thesaurus für die Services geworden.

Auch die nach Erstellungsdatum sortierte Liste ist ausgesprochen beliebt. Darüber hinaus bietet ein so offenes System Raum für die eigene Kreativität. So hat ein Mitarbeiter die Seite der Werksfeuerwehr unter *intra/112* verlinkt, und URL-Kundige haben Shortcuts mit dem Telefon-URL-Schema angelegt, die bei Eingabe einen Telefonanruf starten. (sun@ix.de)

Kai Altstaedt

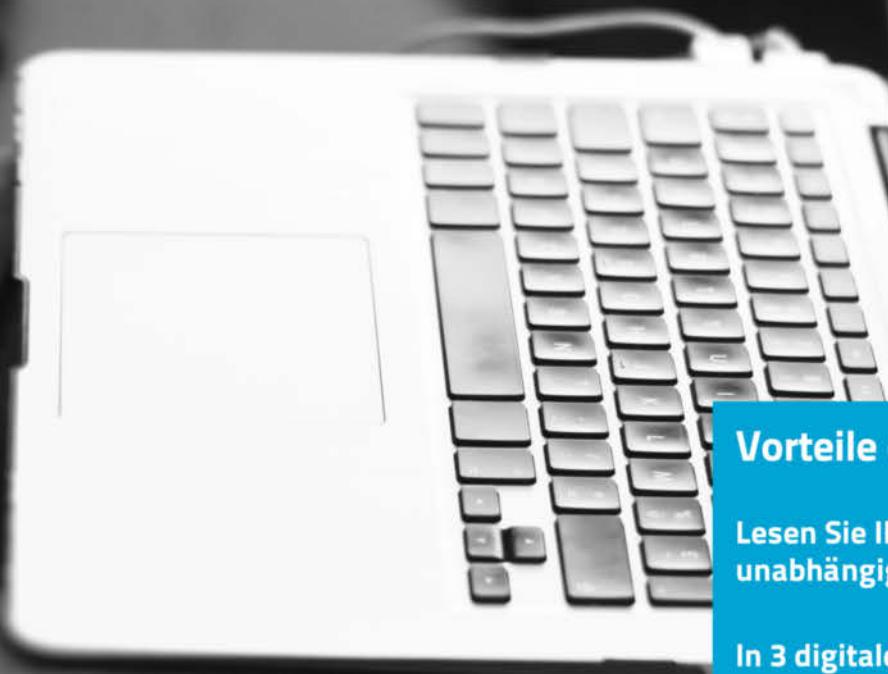
ist Diplom-Informatiker und nebenberuflich freier Autor und Entwickler.



Das c't-Digital-Abo

Genau mein Ding.

Immer und überall top informiert



Vorteile des c't-Digital-Abo

Lesen Sie Ihre Magazine Zeit und Raum unabhängig.

In 3 digitalen Formaten verfügbar:

-  Klassisch als PDF-Download
heise.de/onlineshop
-  Mobil als c't-Magazin-App
iOS, Android oder Kindle Fire
-  Lesefreundlich als Browser-Magazin
heise.de/select

Geräteübergreifende Synchronisierung

Testen Sie jetzt 6 digitale Ausgaben und freuen Sie sich auf eine **Smartwatch** als Dankeschön.

9 €
Rabatt

Zum Angebot:
ct.de/digital-erleben

Tastaturen für jeden Zweck

Schreibhilfen

Kai König

Ob man lieber mit dem rechten oder dem linken Daumen schreibt, lieber Linien malt oder mit dem Finger tippt – für fast jede Vorliebe gibt es die richtige Tastatur.

Entscheidungskriterien bei der Anschaffung eines neuen Handys oder Tablets sind heute meist die Größe des Bildschirms, der verfügbare Speicher oder die Anzahl der CPU-Kerne. Daneben spielen der Hersteller und das Betriebssystem des Mobilgeräts eine Rolle. Da die meisten Geräte dieser Kategorie einen Touchscreen haben, macht sich kaum jemand Gedanken über die integrierte Tastatur.

Vor einigen Jahren war das noch anders. Vor dem ersten iPhone gab es Handys und die sogenannten PDAs. Erstere hatten in der Regel eine für Telefone typische Tastatur mit zehn bis 15 Tasten, PDAs kamen entweder mit Touchscreen und Stift oder einer kleinen eingebauten Hardwaretastatur. Auch das BlackBerry-Ökosystem soll hier nicht unerwähnt bleiben. Dessen PDAs hatten fast alle eine ins Gerät integrierte Tastatur.

Heute basieren die meisten erhältlichen Geräte auf Android oder iOS und haben eine virtuelle Bildschirmtastatur. Natürlich kann man Mobilgeräte relativ problemlos mit externen Tastaturen verbinden, sei es mithilfe von USB-Kabeln, proprietären Steckverbindungen oder über Bluetooth. Um sie soll es im Folgenden jedoch nicht gehen, sondern um Tastatur-Apps für iOS und Android.

Von der Hardware zum Virtuellen

Die ersten Versionen von Android-Geräten besaßen noch eine Hardwaretastatur. Mit Version 1.5 bekam Android Unterstützung für virtuelle Tastaturen. Es dauerte allerdings bis zum Jahr 2012 und der Veröffentlichung von Android 4.1, bevor die Hersteller Tastaturen von Drittanbie-

tern zugelassen haben. iOS-Geräte besaßen niemals eine Hardwaretastatur, und Apple erlaubt virtuelle Tastatur-Apps von Drittanbietern seit der Version 8 von iOS.

Warum aber soll man die vom Betriebssystem mitgelieferten Tastaturen überhaupt durch Apps von Drittanbietern ersetzen? Wie groß können die Unterschiede zwischen Tastaturen schon sein? Eine Tastatur soll den Schreibprozess unterstützen, muss daher schnell reagieren und darf nicht dem Fingeranschlag hinterherhinken. Die Tastatur soll akkurate Trefferzonen haben, aber gleichzeitig so fehler-tolerant sein, dass man selbst auf kleinen Bildschirmen problemlos schreiben kann.

Für Nutzer mehrerer Sprachen müssen landesspezifische Varianten einfach zugänglich sein. Gleches gilt für Emoji-Tastaturen oder solche, die mit Stickern oder anderen grafischen Elementen wie animierten GIFs belegt sind. Vielleicht möchte man auch für bestimmte Anwendungsfelder spezialisierte Tastaturen nutzen können, ähnlich den aus Ziffern gebildeten Tastaturen in Telefon-Apps. All das und einiges mehr bieten spezifische Apps.

Malen statt anschlagen

Gleichzeitig muss man sich vergegenwärtigen, dass Tastaturen von Drittanbietern potenzielle Sicherheitslücken mit sich bringen können. Die Texteingabefunktion befindet sich an zentralen Stellen eines Systems und könnte abhängig von gewünschten Features Daten an den Drittanbieter übertragen. Nicht immer ist es einfach zu verstehen, welche Daten die App weiterreicht und wo sie die Daten verarbeitet und gegebenenfalls speichert.

Eine der besten Tastaturen sowohl für Android als auch für iOS ist Googles kos-



tenloses „Gboard“. Die App war früher als „Google Keyboard“ bekannt und wurde 2016 plattformübergreifend in das Gboard-Branding überführt. Gboard hat eine Vielzahl nützlicher Features, die man in den Standardtastaturen nicht findet.

Diese beginnen mit der Option, Text mithilfe einer zeichnerischen Geste einzugeben. Anstatt jede Taste einzeln anschlagen zu müssen, malt man mit dem Finger eine durchgehende Linie zu allen gewünschten Zeichen. Selbst wenn man während dieses Prozesses nicht jedes Zeichen trifft, interpretiert Gboard die Eingabe anhand seines Lexikons in Kombination mit KI-basierten Vorschlägen nahezu immer korrekt. Mit etwas Übung ist diese Art der Eingabe deutlich schneller und bequemer als das übliche Schreiben auf einer virtuellen Tastatur.

Die Space-Taste kann mehr als nur ein Leerzeichen erzeugen, sie dient gleichzeitig als Mini-Trackpad. Bewegt man den Finger auf der Taste nach links und rechts, steuert diese Bewegung die Cursorposition. In der Regel ist das ein schnellerer und einfacherer Weg, den Cursor zu positionieren, als mit Fingern und Bildschirmlupe die richtige Position im Text zu finden.

Gboard integriert Googles Suchfunktionen und bietet eine Vielzahl von Emojis und Stickern als Teil des Pakets. Darüber hinaus kann man die App thematisch anpassen. Außerdem versteht sie mehrere Sprachen und kennt unterschiedliche Tastaturlayouts. Auf iOS lassen sich mehrere Sprachen gleichzeitig deutlich komfortabler mit Gboard als mit der iOS-Tastatur verwalten. Das Umschalten erfolgt über einen simplen Tastendruck. Gboard verfügt über eine Rechtschreibung für mehrere Sprachen und macht geeignete Korrekturvorschläge auch in gemischtsprachigen Texten.

Auf Android-Modellen ist die App heute in einigen Fällen bereits installiert und als Default-Tastatur eingerichtet. Meist handelt es sich dabei um Nexus- und Pixel-Geräte sowie Handys von OEMs mit eher unverändertem Android – zum Beispiel OnePlus oder Nokia.

Die Installation erfordert ansonsten einen Prozess aus mehreren Schritten. Nach dem Herunterladen der App muss der Anwender sie einmalig ausführen, dann leitet sie ihn in der Regel zu den zugehörigen Einstellungen im mobilen Betriebssystem. iOS warnt als Teil dieses Prozesses deutlich davor, dass man Gboard an dieser Stelle Vollzugriff geben muss. Das liegt allerdings nicht an Gboard, das System fordert dieses Privileg für jede iOS-Tastatur von Drittanbietern.

Auf iOS unterliegen Tastaturen, die nicht von Apple kommen, generell einigen grundlegenden Einschränkungen. Beispielsweise erzwingt iOS die Nutzung der eingebauten Tastatur für die Passworteingabe im App Store oder in der iCloud. Auch kann man von Nicht-Apple-Tastaturen aus die Spracheingabe mit Siri nicht nutzen. Gboard auf iOS bietet allerdings einen einfachen Zugriff auf Googles eigene Spracheingabe.

Wer die Funktionen von Gboard schätzt, dem könnte auch SwiftKey gefallen. Bis 2016 war die App ein unabhängiges Produkt, dann hat Microsoft sie übernommen. Die App funktioniert einwandfrei, und Features wie das Malen von Wörtern, Korrekturvorschläge und Emoji-Unterstützung sind ähnlich wie bei Gboard.

SwiftKey unterstützt die gleichzeitige Nutzung von bis zu fünf Sprachen und erlaubt das Anlegen eines sogenannten SwiftKey-Accounts. Mithilfe dieses Kontos wird durch künstliche Intelligenz die Genauigkeit der Wortvorschläge verbessert und der Anwender kann seine Tastatureinstellungen und den Wortschatz über mehrere Geräte hinweg synchronisieren.

Die App ist kostenlos erhältlich und bietet Tastaturthemen als In-App-Käufe an.

Hat man an „malerischen Gesten“ kein Interesse, sondern möchte mit den Fingern tippen und dabei ergänzende Wortvorschläge eingeblendet bekommen, sollte man sich „Minuum“ ansehen. Die Tastatur lässt sich in ihrer Größe anpassen und stellt mit dem Mini Mode eine Variante der Tastatur zur Verfügung, die auf eine Zeile reduziert ist. Ähnlich dem von alten Mobiltelefonen bekannten T9-System sind deren neun Tasten mit mehreren Buchstaben belegt. Die App geht allerdings einen besonderen Weg und versucht, die Tasten nach Nutzungshäufigkeit zu belegen.

Minuum für iPhone ist zum Preis von 4,49 Euro erhältlich. Für Android gibt es eine kostenlose Version, die man 30 Tage lang testen und auf Wunsch per In-App-Kauf zur Vollversion upgraden kann. Alternativ dazu lässt sich die Vollversion direkt erwerben.

In einer ähnlichen Kerbe schlägt „Thumby“ für das iPhone. Die App kostet 2,29 Euro und zeigt eine halbkreisförmige Belegung auf der rechten oder linken Seite des Tastaturfeldes. Die Idee dahinter ist,

dass dieses Layout die Bedienung des Gerätes mit dem rechten oder linken Daumen deutlich vereinfacht. Nicht unerwartet zeigt sich beim Ausprobieren der App, dass sie vor allem auf Geräten mit größeren Displays sehr nützlich ist.

Mehr Komfort bei der Arbeit

Natürlich gibt es neben den bisher erwähnten Produktivitätstastaturen auch solche für spezielle Interessen und Anwendungen. „Hacker’s Keyboard“ für Android ist eine Variante, die sich vor allem für Nutzer anbietet, die von ihrem Mobilgerät aus Softwareentwicklung oder Systemadministration betreiben.

Die Tastatur hat Cursortasten und funktionierende Tasten für Tab und Escape. Gerade wenn man sich per ssh auf entfernten Servern einloggt, erweist sich Hacker’s Keyboard als sehr anwenderfreundlich. Die App ist darüber hinaus unter einer Apache-2-Open-Source-Lizenz auf GitHub erhältlich. (ka@ix.de)

Alle Links: ix.de/ix1810146



Vor 10 Jahren: Gutes von Google

Google hat letztens das großsprecherische „Don’t be evil“ aus seinem Verhaltenskodex entfernt. Dessen Gültigkeit wurde bereits im Editorial der iX 10/2008 angezweifelt.

Vor 10 Jahren dachte der viel zu früh verstorbenen iX-Redakteur Henning Behme über Google nach. Unmittelbarer Anlass des Editorials „Vom Nicht-böse-Sein“ in iX 10/2008 war die Veröffentlichung des neuen Browsers Google Chrome, mit dem die „Suchmaschine“ dem Internet Explorer und Firefox Konkurrenz machte.

Behme bezweifelte, dass das vom Google-Mitarbeiter Paul Buchheit erfundene Firmenmotto „Don’t be evil“ noch seine Gültigkeit habe. Besonders das Engagement der Firma in China zeige, dass Google mit der Einwilligung in die staatliche Zensur die Grenzen zum Bösen verwische. „Immer noch besser, die Chinesen haben Zugriff auf von Google ausgewählte Informationen, als dass ihre Regierung sie ganz vom Internet abschneidet“, diese Argumentation sei ein „Orwellismus“ besonderer Art, schrieb Behme erbost.

Mit großem Tamtam hat Google gerade – am 4. September – seinen 20. Geburtstag gefeiert. Eine neue Version von Chrome erschien und in der Frankfurter

Allgemeinen Zeitung erklärte Andreas von Bechtolsheim, dass Google nach wie vor die beste Suche sei und kein bisschen böse. Schließlich sei niemand gezwungen, Google-Angebote zu nutzen.

Sun-Mitgründer Bechtolsheim hatte vor 20 Jahren einen Scheck über 100 000 US-Dollar auf eine noch nicht existierende „Google Inc.“ ausgestellt, weil er sofort vom Konzept der Suchmaschine überzeugt war. Die Doktoranden Larry Page und Sergey Brin mussten Google gründen, um an das Geld zu kommen.

Sehr wenige Artikel zum Google-Geburtstag beschäftigten sich mit dem Nicht-böse-Sein, sehr viele hingegen mit dem Steuersparmodell des Konzerns und der Milliardenbuße, die die EU-Kommision gegen Google verhängte. Nicht-böse-Sein geht anders.

So wurde denn auch diese moralische Richtschnur aus dem zentralen Verhaltenskodex der Firma entfernt, als Google im März 2018 neue Regeln veröffentlichte. Geblieben ist eine viel unverbindlichere Formulierung ganz zum Schluss:



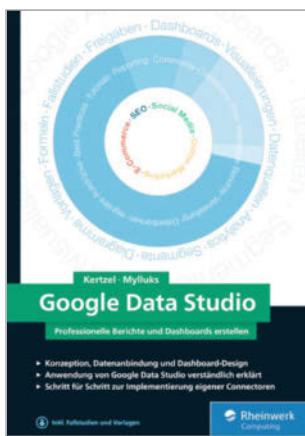
„Erinnere dich ... nicht böse sein, und wenn du etwas siehst, das nicht richtig ist – heraus mit der Sprache!“

Auch der bittere Vorwurf des „Orwellismus“ trifft in dieser Form nicht mehr zu. Bekanntlich zog

sich Google als Suchmaschine ab 2010 aus China zurück, nachdem es fortlaufend Schwierigkeiten mit der Zensur gab. Erst in jüngster Zeit gibt es bei Google Überlegungen, in China eine Suche anzubieten. Schließlich ist Google dort mit einer Niederlassung präsent, offeriert chinesischen Kunden das Machine-Learning-Framework TensorFlow und finanziert in Shanghai einen Lehrstuhl für KI-Forschung.

US-Medien berichteten, dass unter dem Codenamen „Dragonfly“ an einer neuen chinesischen Webpräsenz von „GüGe“ (so der chinesische Name) gearbeitet werde. Am 6. August erschien in der Renmin Ribao, dem Parteiorgan der Kommunistischen Partei Chinas, ein Artikel über die Facebook-Seite der Partei mit einer programmativen Ansage. Man habe in China nichts gegen Facebook und nichts gegen Google. Natürlich würde für beide die strikte chinesische Medienaufsicht gelten.

Detlef Borchers (js@ix.de)



Sascha Kertzel, Sina Mylluks

Google Data Studio

Professionelle Berichte und Dashboards erstellen

Rheinwerk 2018

391 Seiten

39,90 €

ISBN 978-3-8362-6097-8

Data Studio stellt Googles Visualisierungswerkzeuge für jeden zur Verfügung. Die Autoren Kertzel und Mylluks beschreiben das Arbeiten mit dem Berichtsgenerator in vier Schritten: Daten verbinden, aufbereiten, darstellen und teilen. Die Kapitel orientieren sich an dieser Ausrichtung, die Einleitung erklärt oft verwendete Begriffe.

Data Studio erinnert vom Konzept her an Crystal Reports. Das zweite Kapitel beschreibt das Webinterface, das dritte mögliche Datenquellen. Das Werkzeug funktioniert nach Aussage der Autoren mit Tools wie Googles Sheets am besten – die Verbindung mit anderen Diensten erklären sie mit vielen Bildern.

Liegen Daten in einem nicht verwendbaren Format

vor, bietet Data Studio an Tabellenkalkulationen angelehnte Funktionen zur Aufbereitung. Der Text erläutert diese Arbeit in einem rund 70 Seiten umfassenden Abschnitt. Kapitel fünf und sechs stellen die Komponenten zum Visualisieren von Daten vor. Hier geht es auch um die Stärken und Schwächen der verschiedenen Diagrammtypen.

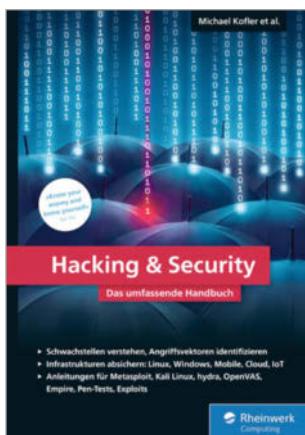
Daten, die nicht der Google-Welt entstammen, lassen sich über Konnektoren in das Werkzeug einbinden. Anhand praktischer Beispiele und eines eigenen kleinen Programms lernt der Leser die verschiedenen Möglichkeiten kennen. Für kompliziertere Aktionen sind allerdings ausgewachsene Programmierkenntnisse gefordert, die das Buch nicht vermitteln kann. Googles Apps Script orientiert sich an JavaScript und dürfte C- und Java-Programmierer nicht abschrecken.

Kapitel acht beschreibt, wie man Informationen mit dem Berechtigungssystem verwaltet und sichert. Es folgt ein Abschnitt, der die Zugriffsrechte für Berichte erklärt – das Einbinden von Google Analytics ist ebenfalls Thema.

Wie man praktische Visualisierungsaufgaben erledigt, ist im Folgenden zu erfahren. Danach stellen die beiden Analysten einige Vorlagen für häufig benötigte Aufgaben bereit, die die Leser in eigenen Reports verwenden können. Weiterhin gibt es Performance-Tipps und Produktivitätshinweise. Am Ende findet sich ein zehnseitiger Appendix mit Links zu weiteren Ressourcen.

Wer keine Skrupel hat, seine Daten mit Google zu teilen, erhält mit Data Studio ein nützliches Tool. Das Buch erklärt alles, was man für die Bedienung braucht.

Annette Bosbach (jd@ix.de)



Michael Kofler et al.

Hacking & Security

Das umfassende Handbuch

Rheinwerk 2018

1067 Seiten

49,90 €

ISBN 978-3-8362-4548-7

Hacker sind nicht immer Unholde. Es gibt auch die Guten, die „White Hacker“, die versuchen, Sicherheitslücken zu finden und zu schließen. Wer Penetrationstests durchführt oder als Sicherheitsforscher Schwachstellen sucht, nutzt dieselben Werkzeuge wie die bösen Hacker. Denn um sich verteidigen zu können, muss man seine Gegner und ihr Equipment genau kennen.

Auf über 1000 Seiten gibt das Autorenteam um Michael Kofler einen Überblick über

ist das betriebssystemübergreifende Denken ein Muss, da sich weder Hacker noch die IT-Sicherheit auf Windows oder Linux beschränke.

Das umfangreiche Werk besteht aus drei großen Teilen: Der erste, „Hacking und Tools“, führt auf 200 Seiten in das Thema ein und erklärt Begriffe wie Hacking, Penetrationstests und Angriffsvektoren. Die Auswahl der Werkzeuge konzentriert sich auf gängige kostenlose Software. Den Anfang macht Kali Linux, eine Art Schweizer Taschenmesser für Security. Auch Nicht-Linuxer können hier lernen, wie sich diese Distribution mit ihrer großen Sammlung an Hacking-Werkzeugen installieren lässt. Für Windows-Anwender stellen die Autoren zum Beispiel PentesBox und die Test- und Lernumgebung Metasploitable vor. Es folgen viele Kommandos, etwa *nmap* (Network Mapper), *hydra* (Network Login Cracker) und Werkzeuge wie *tcpdump* *OpenVAS* (Open Vulnerability Assessment Sys-

tem) und *Burp Suite*. Im zweiten Teil, „Hacking und Absicherung“, erklären die Autoren auf 600 Seiten zunächst Formen des Knackens von Systemen, anschließend die Gegenmaßnahmen. Beispiel: Was kann ein Hacker mit einem verlorenen Notebook anfangen und wie verschlüsselt man seine Festplatte? Weitere Themen: Passwortattacken sowie Angriffe über WLAN, Bluetooth, Software-defined Radios und USB-Schnittstellen. Das Absichern von Linux, Samba-Fileservern und Webanwendungen erklären die Autoren in eigenen Kapiteln.

Im dritten Teil geht es um „Cloud, Smartphones und IoT“. Dazu gehört ein Überblick über Techniken, Anbieter und Risiken. Man erfährt zudem, wie man Android-Apps schützt und IoT-Geräte sicher programmiert. Security-Verantwortliche bekommen mit dem gut geschriebenen Buch viel Material an die Hand, mit dem sie die IT besser sichern können.

Barbara Lange (jd@ix.de)



Joachim Ohser

Angewandte Bildverarbeitung und Bildanalyse

Hanser 2018
301 Seiten
30,00 €
ISBN 978-3-446-44933-6

Bildbearbeitung ist überall präsent: Verkehrsüberwachungssysteme wie SectionControl nutzen sie beispielsweise zum Erfassen von Nummernschildern. Der Hanser-Verlag liefert nun ein Lehrbuch, das die mathematischen Prozesse dahinter zu erklären versucht.

Nach dem Darlegen des inneren Aufbaus einer Bitmap-Klasse folgen mathematische

Grundprinzipien wie die Euler-Zahl. Problematisch könnte sein, dass der Autor ein nicht unerhebliches Grundwissen voraussetzt. Wer das Buch im Eigenstudium durchackert, hätte sich über einige motivierende Sätze sicher gefreut. Am Ende des ersten Kapitels stehen jedenfalls erste lauffähige Algorithmen, die beispielsweise eine Kontrastkorrektur auf Basis von Histogrammen vor-

nehmen. In Joachim Ohsers Buch dreht sich alles um mathematische Transformationen, die erst später zu Klassikern wie Filtern zur Elimination von Bildrauschen kombiniert werden. Die Ausführungen zu Binomialfiltern, Kantendetektion und Co. sind allerdings interessant. Zudem gibt der Autor an dieser Stelle auch Hinweise, wie man die gezeigten Verfahren sauber implementiert.

Während sich das zweite Kapitel mit der „Verbesserung“ des Aussehens von Bildern befasst, präsentiert das folgende Verfahren zur Extraktion von Informationen. Besonderen Fokus legt Ohser auf das Trennen einzelner Objekte in Bildern.

Die im vierten Kapitel vorgestellten Fouriertransformationen sind aus der Elektronik bekannt. Kapitel Nummer fünf vertieft diese Thematik. Als Anwendungsfall dient eine

Kreuzkorrelation, die die Ausbreitung von Borkenkäferbefall analysiert. Weiter geht es mit den Grundlagen der topografischen Rekonstruktion und der Bildanalyse.

Wer mit Mathematik auf Kriegsfuß steht, sollte das Buch lieber nicht kaufen. Der Autor erklärt die Konzepte primär anhand von Formeln. Bilder aus Physik und Metallurgie demonstrieren die Ergebnisse der jeweiligen Algorithmen – Physiker und Materialtechniker sollen sich vorrangig angesprochen fühlen. In jedem Kapitel gibt es Fragen für das Selbststudium. Am Ende des Werks findet sich eine Komplettlösung zum Überprüfen der ermittelten Ergebnisse.

Ohser hat kein Kochbuch geschrieben: Wer schnell schlüssel fertige Algorithmen sucht, wird hier nicht sonderlich gut bedient.

Tam Hanna (jd@ix.de)

iX-Workshop

Parallele Programmierung

Jetzt
anmelden
und
Ticket
sichern

2-tägiger iX-Workshop mit optionalem 3. Tag über Programmierung, Technologie und Architekturen für moderne parallele Anwendungen auf Multicore-Prozessoren

In diesem Seminar wird die parallele Programmierung praxisnah und von Grund auf erschlossen. Es wird von den theoretischen Grundlagen über die klassische Parallelisierung mit Threads hin zu den heute wichtigen Task-Schedulern hin gearbeitet. Dabei wird ersichtlich, wie Synchronisations-Konzepte für die Koordination paralleler Aufgaben am besten genutzt werden und man lernt mit den Memory-Modellen moderner Multicore-CPU's umzugehen. Alle Unterrichtsinhalte werden durch konkrete Programmierübungen vertieft, die wahlweise in Java, C# oder in C++ durchgeführt werden können.

Termin: 5. bis 7. November 2018 in Hannover

Teilnahmegebühr: 1.310,00 Euro

Teilnahmegebühr 3. Tag (optional): 467,00 Euro

alle Preise inkl. MwSt.

Ihr Referent:



Marwan Abu-Khalil ist Senior Software Architekt (SSWA) in der Siemens AG und arbeitet seit über 10 Jahren an der Parallelisierung unterschiedlichster Systeme vom Server-Backend bis zum Embedded-Device. Er ist langjähriger Trainer für Software-Architektur und spricht auf Konferenzen über Parallelisierung.

Eine Veranstaltung von:



Organisiert von:



Weitere Infos unter:

www.heise-events.de/paralleleprogrammierung

www.ix-konferenz.de

Copyright by Heise Medien

STELLENANGEBOTE



KLEINE DETAILS MACHEN DICH WAHNSINNIG?

Du entwickelst Softwareprodukte mit Liebe zum Detail und findest Software muss kompromisslos gut funktionieren?

Jetzt als Software Engineer bewerben.
www.yatta.de/karriere



Fraunhofer IWS

FRAUNHOFER-INSTITUT FÜR WERKSTOFF-
UND STRAHLTECHNIK IWS

WIR BEI FRAUNHOFER BIETEN IHNEN EINE
SPANNENDE TÄTIGKEIT ALS

GRUPPENLEITERIN/ GRUPPENLEITER IT-MANAGEMENT

Die zukünftige Gruppenleiterin/der zukünftige Gruppenleiter ist verantwortlich für die fachliche und disziplinarische Leitung eines derzeit neunköpfigen Teams (inkl. 3 Azubis/BA-Studenten) zur Sicherstellung eines störungsfreien IT-Betriebs, unter Beachtung aller sicherheitsrelevanten Aspekte. Auf Ihrer Agenda stehen die Sicherstellung und Optimierung des operativen Betriebs, die Erarbeitung einer Konzeption für das Anlagennetz sowie die Digitalisierungsstrategie für das gesamte Institut.

Fraunhofer ist die größte Organisation für anwendungsorientierte Forschung in Europa. Unsere Forschungsfelder richten sich nach den Bedürfnissen der Menschen: Gesundheit, Sicherheit, Kommunikation, Mobilität, Energie und Umwelt. Wir sind kreativ, wir gestalten Technik, wir entwerfen Produkte, wir verbessern Verfahren, wir eröffnen neue Wege.

Sie sind interessiert? Die vollständige Stellenausschreibung finden Sie unter: <http://s.fhg.de/4ca>



Heise Gruppe

JAVA-Anwendungsentwickler (m/w) am Standort Hannover

VIELFALT

FREIRAUM

FREUDE

VERANT-
WORTUNG



Werden Sie JAVA-Anwendungsentwickler (m/w) bei Heise!

Sie haben ein Studium der Naturwissenschaften (z. B. Mathematik oder Informatik) oder eine Ausbildung zum Fachinformatiker (m/w) im Bereich Anwendungsentwicklung erfolgreich abgeschlossen. Sie bringen mindestens zwei Jahre einschlägige Berufserfahrung und fundierte Kenntnisse im Bereich Relationale Datenbanken und in der GUI-Entwicklung mit Swing mit. Darüber hinaus wünschenswert sind zusätzliche Erfahrungen in der Web-Entwicklung mit Java sowie Kenntnisse in SAP R/3.

Bitte geben Sie bei Ihrer Bewerbung Ihren frühestmöglichen Eintrittstermin und Ihre Gehaltsvorstellungen an.

Wir freuen uns auf Ihre Bewerbung!

Ihre Ansprechpartnerin

Anika Otten

Teamleiterin Java Anwendungsentwicklung
Tel.: 0511-5352-264

Bitte bewerben Sie sich online über
www.heise-gruppe.de/karriere

Bewerbungen von Menschen mit Behinderung sind erwünscht.



**Neugierig geworden? Lernen Sie
uns im Video kennen!**



Heise Gruppe



Redakteur (m/w) oder Volontär (m/w) Internet und Anwendungen in Hannover

CHARAKTER

IDEEN

ERFOLG

VIELFALT

c't sucht ...

Als Volontär für den Bereich Internet lernen Sie, sich in ein Thema einzuarbeiten und nach gründlicher Recherche Artikel für c't zu veröffentlichen. Als Redakteur setzen wir dieses Können voraus. Sie arbeiten dabei mit Autoren zusammen oder schreiben selbst Testberichte, Praxisanleitungen und Hintergrundartikel. Sie beherrschen HTML, CSS sowie JavaScript und auch das Schrauben an Anwendungen auf dem Server macht Ihnen Spaß. Idealerweise bringen Sie bereits Verlags- oder Redaktionserfahrungen mit, können durch ein abgeschlossenes Studium überzeugen und beherrschen Englisch in Wort und Schrift.

Bewerben Sie sich jetzt! Bitte geben Sie Ihren frühesten Eintrittstermin an.

Ihre Ansprechpartnerin

Dorothee Wiegand
Ressortleiterin c't Redaktion
Tel.: 0511-5352-726

Wir freuen uns auf Ihre Bewerbung!

Bitte bewerben Sie sich online über
www.heise-gruppe.de/karriere

Bewerbungen von Menschen mit Behinderung sind erwünscht.

Heise Medien

REPLY

DEIN JOB IN DER IT SECURITY? REPLY IST DIE ANTWORT!

- Penetration Test
- Ethical Hacking
- IOT & Cloud Security
- Identity & Access Management
- Advanced Security Solutions Implementation



www.reply.de | careers.reply.de | job@reply.de

uvex group

WEITSICHT ERÖFFNET CHANCEN

UNTERNEHMERISCH – einer unserer Führungswerte, der die uvex group in den Bereichen Arbeitsschutz sowie Sport und Freizeit zu einem der führenden Anbieter macht. **protecting people** ist unser Auftrag – hierfür suchen wir Sie, als neue/n Mitarbeiter/in für die UVEX WINTER HOLDING GmbH & Co. KG am Standort Fürth/Bayern als:

SPEZIALIST WORKPLACE

(M/W)

EINIGE IHRER AUFGABEN

- Planung und Implementierung von Enterprise Workplace
- Unterstützung bei Cloud-Themen
- Betrieb von Micro Focus OES (SUSE Linux)
- Lifecycle Management

Verstärken Sie unsere Teams im Konzerninformationsmanagement.

Alle Informationen zu den Aufgaben und Qualifikationen der einzelnen Positionen finden Sie auf unserer Homepage unter uvex-group.de/karriere

Ihre aussagekräftigen Bewerbungsunterlagen senden Sie uns bitte unter Angabe Ihrer Gehaltsvorstellung und des frühestmöglichen Eintrittstermins über unser Online-Bewerberportal.

IHR ANSPRECHPARTNER

Frau Kathrin Kalt
Würzburger Str. 181
90766 Fürth

uvex-group.de/karriere

IT-PROJEKTLEITER

(M/W)

EINIGE IHRER AUFGABEN

- Projektleitung komplexer IT-Projekte mit Schwerpunkt auf technischen Projekten
- Projektreporting, Projektcontrolling und Projektmarketing
- Unterstützung des Projektportfoliomanagements
- Koordination interner und externer Projekttressourcen



protecting people

IMMER EINE IDEE SCHLAUER.



2x Mac & i mit 25% Rabatt testen und Geschenk sichern!

Ihre Vorteile:

- **Plus:** digital und bequem per App
- **Plus:** Online-Zugriff auf das Artikel-Archiv*
- **Plus: Geschenk nach Wahl**, z.B. den Kingston USB-Stick 32 GB (G4) oder einen Bluetooth-Lautsprecher
- **Lieferung frei Haus**

Für nur 16,20 € statt 21,80 €

* Für die Laufzeit des Angebotes.



Jetzt bestellen und von den Vorteilen profitieren:
www.mac-and-i.de/minabo
0541 80 009 120 · leserservice@heise.de

Mac & i. Das Apple-Magazin von c't.





Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover

Redaktion: Telefon: 0511 5352-387, Fax: 0511 5352-361, E-Mail: post@ix.de

Abonnements: Telefon: 0541 80009-120, Fax: 0541 80009-122, E-Mail: leserservice@heise.de

Herausgeber: Christian Heise, Ansgar Heise

Redaktion: Chefredakteur: Jürgen Seeger (js@ix.de) -386

Stellv. Chefredakteur: Dr. Oliver Diedrich (od@ix.de) -616

Ltd. Redakt.: Kersten Auel (ka@ix.de) -367, Alexander Neumann (ane@ix.de) -813,

Bert Ungerer (un@ix.de) -368

Nicole Bechtel (nb@ix.de) -378, Björn Bohn (bbo@ix.de) -373,

Jürgen Diercks (jd@ix.de) -379, Moritz Förster (fogix.de) -374, Alexandra Kleijn (akl@ix.de) -787,

Rainald Menge-Sonnentag (rme@ix.de), Susanne Nolte (sun@ix.de) -689,

Matthias Parbel (map@ix.de) -321, André von Raison (avr@ix.de) -377, Ute Roos (ur@ix.de) -535

Redaktionsassistent: Carmen Lehmann (cle@ix.de) -387, Michael Mentzel (mm@ix.de) -153

Korrespondent Köln/Düsseldorf/Ruhrgebiet:

Achim Born, Siebengebirgsallee 82, 50939 Köln, Telefon: 0221 4200262, E-Mail: ab@ix.de

Korrespondentin München:

Susanne Franke, Belgradstraße 15 a, 80796 München, Telefon: 089 28807480, E-Mail: sf@ix.de

Ständige Mitarbeiter: Detlef Borchers, Tobias Haar, Dr. Fred Hantelmann, Nils Kaczenski, Christian Kirsch, Kai König, Barbara Lange, Stefan Mintert, Dr. Holger Schwichtenberg,

Christian Segor, Diane Sieger, Dr. Jens-Henrik Söldner, Gerhard Völk

Layout und Satz: Madlen Grunert, Lisa Hemmerling, Kirsten Last, Steffi Martens,

Matthias Timm, Ninett Wagner, Hinstorff Media, Rostock

Chefin vom Dienst: Barbara Gückel

Korrektorat: Barbara Gückel; Thomas Ballenberger, Ninett Wagner, Hinstorff Media, Rostock

Fotografie: Martin Klauss Fotografie, Despetal/Barfeld

Titel: Idee: ix; Titel- und Aufmachergestaltung: Dietmar Jokisch, Martin Klauss

Verlag und Anzeigenverwaltung:

Heise Medien GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover; Telefon: 0511 5352-395, Fax: 0511 5352-129

Geschäftsführer: Ansgar Heise, Dr. Alfons Schräder

Mitglieder der Geschäftsleitung: Beate Gerold, Jörg Mühlé

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke -167, E-Mail: michael.hanke@heise.de,

www.heise.de/mediadaten/ix

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 29 vom 1. Januar 2018.

Leiter Vertrieb und Marketing: André Lux -299

Werbeleitung: Julia Conrades -156

Druck: Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel

Sonderdruck-Service: Julia Conrades -156

Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

ix erscheint monatlich

Einzelpreis € 7,90, Österreich € 8,70, Schweiz CHF 12,20, Luxemburg € 9,20

Das Abonnement für 13 Ausgaben kostet: Inland € 93,60, Österreich € 113,10, Schweiz CHF 158,60, restl. Europa € 109,20, sonst. Länder € 113,75; 13 Digitalausgaben im Abonnement kosten weltweit € 93,60; Studentenabonnement: Inland € 55,90, Österreich € 67,60, Schweiz CHF 94,90, restl. Europa € 65,00, sonst. Länder € 68,25; nur gegen Vorlage der Studienbescheinigung, Luftpost auf Anfrage.

ix Plus-Abonnements (inkl. Online-Zugriff auf das ix-Artikel-Archiv und die digitale Ausgabe für Android/iOS) kosten pro Jahr € 13 (Schweiz CHF 16,90) Aufpreis.

Für Mitglieder von AUGE, BvDW e.V., /ch/open, GI, GUUG, ISACA Germany Chapter e. V., JUG Switzerland, Mac e.V., VBIO, VDE und VDI gelten ermäßigte Abonnementpreise (gegen Mitgliedsausweis). Bitte beim Abo-Service nachfragen.

Kundenkonto in der Schweiz: UBS AG, Zürich, Kto.-Nr. 206 PO-465.060.0

Abo-Service:

Heise Medien GmbH & Co. KG, Leserservice, Postfach 24 69, 49014 Osnabrück, Telefon: 0541 80009-120, Fax: 0541 80009-122, E-Mail: leserservice@heise.de

Vertrieb Einzelverkauf (auch für Österreich, Luxemburg und Schweiz):

VU Verlagsunion KG, Meßberg 1, 20086 Hamburg, Telefon: 040 3019-1800, Fax: 040 3019145-1800, info@verlagsunion.de, Internet: www.verlagsunion.de

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Die gewerbliche Nutzung abgedruckter Programme ist nur mit schriftlicher Genehmigung des Herausgebers zulässig.

Honorierte Arbeiten gehen in das Verfügungrecht des Verlages über, Nachdruck nur mit Genehmigung des Verlages. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Sämtliche Veröffentlichungen in ix erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Printed in Germany

© Copyright by Heise Medien GmbH & Co. KG

ISSN 0935-9680



Die Inserenten*

REDAKTIONELLER TEIL

1&1 Internet SE	www.lund1.info	39
aikux	www.aikux.com	19
B1 Systems GmbH	www.b1-systems.de	155
Bundesm. Verteid.	www.bundeswehrkarriere.de	13
BWS Consulting	www.bws-group.de	14
bytec	www.bytec.de	156
Cronon	www.cronon.net	37
dpunkt	www.dpunkt.de	25, 27
G DATA	www.gdata.de	29
Heinlein	www.heinlein-support.de	53
Interxion	www.interxion.com	43
Lufthansa	www.lufthansa-industry-solutions.de	2
Messe Nürnberg	www.it-sa.de	33
mitp-Verlag	www.mitp.de	31
Optima bit	www.optimabit.com	21
Orientation in Objects	www.oio.de	28
pep soft	www.pepfoundation.org	7
Rausch	www.rnt.de	15
Rheinwerk Verlag	www.rheinwerk-verlag.de	11
Thomas Krenn	www.thomas-krenn.com	65
Weber, Fernschule	www.fernenschule-weber.de	20
WIBU-SYSTEMS	www.wibu.de	23
Wortmann	www.wortmann.de	17

itsa-Guide 69-75

iX extra

Endpoint Protector	www.endpointprotector.de	VII
Secunet Security	www.secunet.com	V

STELLENMARKT

Fraunhofer IWS	www.iws.fraunhofer.de	150
Heise Medien	www.heise-gruppe.de	150, 151
Reply	www.reply.de	151
Uvex	www.uvex-group.de	152
Yatta Solutions	www.yatta.de	150

VERANSTALTUNGEN

Parallel 2019	ix, heise developer, dpunkt.verlag	22
IT Jobtag	heise jobs, Jobware	106
Continous Lifecycle / Container Conf.	ix, heise developer, dpunkt.verlag	113
heise devSec	ix, heise security, dpunkt.verlag	115
Cloud Konferenz	ix, heise Event	125
Sammelanzeige Software Quality Lab	ix, Software Quality Lab	137

Diese Ausgabe enthält eine Titelflappe von Alkmene Verlagsgesellschaft, Frankfurt, einen Beihefter von EUROstor, Filderstadt, sowie Beilagen von DOAG, Berlin; Hackattack, Österreich; Swiss Cyber Storm, Schweiz; Unitymedia, Köln und Heise Medien, Hannover.

Wir bitten unsere Leser um freundliche Beachtung.

* Die hier abgedruckten Seitenzahlen sind nicht verbindlich.
Redaktionelle Gründe können Änderungen erforderlich machen.



Android fürs IoT

Mit Android Things hat Google eine modifizierte Version seines verbreiteten und gut dokumentierten Smartphone-Betriebssystems für IoT-Geräte herausgebracht. Was ein Entwickler zu erwarten hat und welche Hürden er meistern muss, in der nächsten iX.

DevOps: Code kontinuierlich testen

Wer DevOps konsequent umsetzt, muss auch Sicherheitstests vollautomatisch in der Delivery-Pipeline verankern. Mit dem Einsatz unterschiedlicher Testarten und Werkzeuge lassen sich Sicherheitslücken im Code vermeiden – bereits während der Entwicklung.



**Heft 11/2018
erscheint am 25. Oktober 2018**

Wie man robuste IT-Systeme schafft

IT-Installationen sollen lange und klaglos funktionieren. Wer beim Einkauf und der Entwicklung keine Fehler machen will, braucht greifbare Kriterien, um am Ende qualitativ hochwertige Anwendungen zu erhalten.

Übersicht: Schwachstellenmanagement

Typische Einfallstore für Angriffe sind falsch konfigurierte oder ungepatchte Server mit veralteter Software. Ein automatisiertes und regelmäßiges Scannen nach Schwachstellen hilft dem Administrator, sie schnell zu erkennen und zu beheben. Welche Tools es hierfür gibt, zeigt die nächste iX.



Container sicher betreiben: drei Ansätze

Als stabile und portable Laufzeitumgebung für Anwendungen bieten Container viele Vorteile. Läuft ein Prozess jedoch Amok, kompromittiert er den Kernel des Hostsystems. Drei aktuelle Projekte wollen dem vorbeugen und verfrachten Container in einen virtuellen Sandkasten.

Kein wichtiges Thema mehr versäumen!

Abonnieren Sie jetzt unseren **Newsletter** oder folgen Sie uns ganz einfach auf **Facebook**. So bleiben Sie immer up to date!

www.iX.de/newsletter



www.facebook.com/iX.magazin



Änderungen vorbehalten



iX kompakt Programmieren heute jetzt im Handel



**Technology Review 10/2018
jetzt im Handel**



**c't 20/2018
jetzt im Handel**



Linux/Open Source mit B1

umfassend & individuell!

Seit 2004 unterstützt B1 Systems deutschlandweit & international Unternehmen jeder Größenordnung bei Konzeption, Betrieb und Management komplexer Open Source/Linux-Landschaften.

Unsere Schwerpunkte:

**Cloud · Containerisierung · System- und Konfigurationsmanagement
Hochverfügbarkeit · Virtualisierung · Monitoring**

Unser Team von ca. 100 festangestellten Mitarbeitern begleitet den gesamten Lebenszyklus eines Projekts vom ersten Proof of Concept bis hin zum Support bestehender Lösungen. Individuelle Trainings-, Consulting- und Support-Konzepte runden unser Angebot ab.



B1 Systems GmbH - Ihr Linux-Partner

Linux/Open Source Consulting, Training, Development & Support

ROCKOLDING · KÖLN · BERLIN · DRESDEN

www.b1-systems.de · info@b1-systems.de

© Copyright by Heise Medien.

Bytec ServiceNet

Always Reliable

Inspired by Vincent van Gogh's *Cafe terrace at night*



The Informatics Network
Bytec GmbH Tel. 07541/585-0 www.bytec.de

bytec