



Anzeige

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

10
OKTOBER
2013

iX extra Security:

**Identity-
Management**

€ 6,40

Österreich € 6,70

Schweiz CHF 10,70

Benelux € 7,40

Italien € 7,40

www.ix.de

Was „Made in Germany“ taugt:

Sicheres Cloud Computing?

Provider-Auswahl, Transport und Verschlüsselung, alternative Cloud-Systeme

Der große Bruder von Windows 8.1:

Windows Server 2012 R2

Arbeitsplätze zentral bereitstellen:

Citrix' XenDesktop 7

Datenbanken verknüpfen:

MariaDB 10 Storage Engine

Webentwicklung:

Web-Apps bauen mit Yeoman

Für Industrie, Schreibtisch und Server:

Linux heute

Softwareentwicklung:

Migration auf Multi-Core-CPUs

Ausblick auf Java 8

Tutorial:

vCenter-Orchestrator

Teil 2: Komplexe Workflows

Runderneuertes Design, vereinfachtes Management:

Was Apples iOS 7 bringt



MARKT + TREND**Hypervisor**

VMworld 2013 US: Auf der Suche nach neuen Märkten

8

Computerspiele

GDC 2013: Mobile Plattformen und neue Bezahlmodelle

12

Open Source

Linux-Kernel: Mehr hauptberufliche Entwickler

22

Security

Empfehlungen zur Datenübermittlung an Drittstaaten

24

Mobile Computing

Smartwatches auf der IFA

26

Recht

Bitcoins als Rechnungseinheit anerkannt

28

Betriebssysteme

Vorschau auf Windows 8.1

33

Wirtschaft

Konzernumbau bei Microsoft

38

TITEL**Cloud Computing**

Cloud-Provider-Auswahl angesichts der NSA-Affäre

COVER
THEMA

42

Cloud-Zugriff

Erfolgreiche Verschlüsselung trotz NSA, GCHQ & Co.

46

Cloud Storage

Dropbox-Alternativen AeroFS und ownCloud

52

REVIEW**Programmiersprachen**

Was Entwickler mit Java 8 erwartet

COVER
THEMA

60

Betriebssysteme

Microsofts Windows Server 2012 Release 2

COVER
THEMA

66

Virtualisierung

Client-Betriebssysteme aus dem RZ mit XenDesktop 7

COVER
THEMA

72

Server

Hochleistungsrechner mit großem Speicher

78

Monitore

NEC MultiSync EA294WMi

84

Datensicherung

Neue Funktionen bei Veeams Backup & Replication v7

86

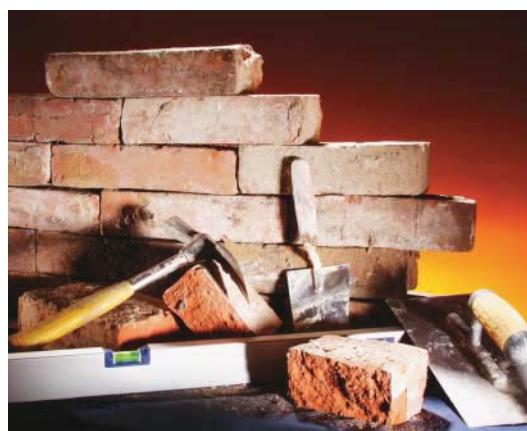
REPORT**Enterprise-Linux**

Linux für den Unternehmenseinsatz

COVER
THEMA

94

Fast eine Major-Release: 8.1-Pendant Window Server 2012 R2



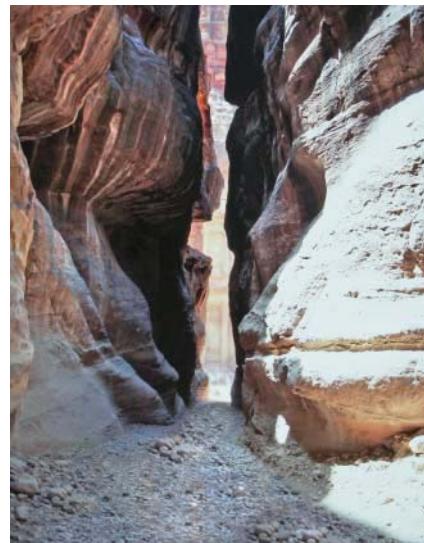
Wenn für den Desktop ein neues Windows erscheint, kann Microsoft die Server nicht darben lassen. Das 8.1-Pendant Windows Server 2012 R2 hat deutlich mehr Neues zu bieten als das verschämt angehängte „R2“ vermuten lässt.

Seite 66

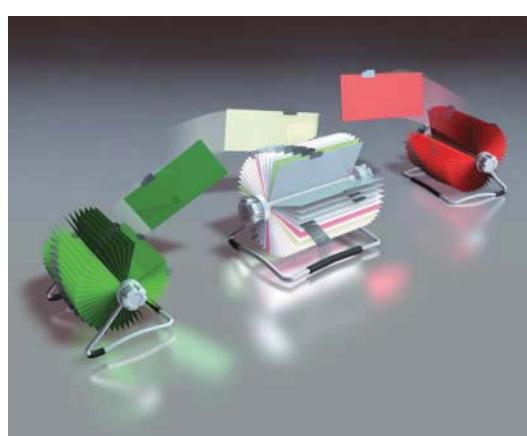
Ante portas: Java 8

Java 8 ist Feature-komplett und kann mit Schmankerln wie Lambda-Ausdrücken zu C# aufschließen. Die finale Release soll im März 2014 erscheinen, einlesen kann man sich ab sofort.

Seite 60



Datenbanken verknüpfen: MariaDB 10 mit neuer Storage Engine



MariaDB, das Oracle-unabhängige MySQL-Spin-off, beinhaltet ab der kommenden Version 10 Storage Engines, die die Verknüpfung heterogener Datenbankformate ermöglichen – egal, ob diese lokal oder remote vorliegen.

Seite 149

Sicheres Cloud Computing?

Provider-Dienste „Made in Germany“ sollen sensible Daten vor NSA, GCHQ und Co. schützen. Doch oft ist in den Paketen weniger „Germany“ drin, als die Anbieter glauben machen wollen. Kritische Tipps zur Provider-Auswahl, eine Beurteilung der Sicherheit von Verschlüsselungsprotokollen und ein Blick auf alternative Cloud-Systeme.

Seite 42, 46 und 52



Was Apples iOS 7 bringt

Das runderneuerte Design von iOS 7 dürfte neben den Anwendern vor allem Entwickler interessieren; Administratoren dürften die neuen Möglichkeiten des Mobile Device Management zu schätzen wissen.

Seite 114 und 120



Embedded-Linux

Linux-Distributionen für eingebettete Systeme

COVER
THEMA

100

Mobile Analytics

Dem mobilen Anwender auf die Finger geschaut

104

Internetzensus

Das Internet scannen und auf Schwachstellen untersuchen

108

WISSEN

Mobile Computing

iOS 7: Was die neue Version für Entwickler bedeutet

COVER
THEMA

114

Mobile Security

Was sich bei iOS 7 in Sachen Sicherheit ändert

120

Software-Tools

Open Build Service für Firmenprojekte nutzen

126

Parallelisierung

Migration auf Multi-Core-CPUs

COVER
THEMA

130

PRAXIS

Webentwicklung

Yeoman: Werkzeugsammlung für Web-Apps

COVER
THEMA

140

Mobile Software

Mobile Oracle-Anwendungen mit APEX

146

SQL-Datenbanken

Neue Storage Engine in MariaDB

COVER
THEMA

149

Remote-Desktop

vCenter-Tutorial, Teil 2: Komplexe Workflows für vCenter Orchestrator

COVER
THEMA

152

MEDIEN

App-Infos

Nachrichten persönlich gestalten

158

Vor 10 Jahren

Der Chip von Fritz im ThinkPad

159

Buchmarkt

CSS3/E-Bücher

160

Rezensionen

Responsive Webdesign, Datenintegration, Die Vernetzung der Welt

162

RUBRIKEN

Editorial

3

Leserbriefe

6

iX extra Security

nach Seite 132

Seminarkalender

164

Stellenmarkt

165

Inserentenverzeichnis

168

Impressum

169

Vorschau

170

Gegen den Strom

Den besonders hell leuchtenden Sternen am IT-Himmel droht wie Sternschnuppen immer das Verglühen. Glaubt man den Worten vieler Journalisten und Analysten, dürfte es in absehbarer Zeit mit Apple so weit sein. Sinkender Marktanteil, fallender Aktienkurs, anscheinend fehlende Innovationsfreude – die Edelmarke steht am Rande des Abgrunds.

Oder auch nicht. Sicher, das iPhone 5s ist technisch ebenso wenig ein großer Wurf wie Nummer 4, das immerhin das damals revolutionär hoch auflösende Retina-Display einführt. Aber interessieren sich Kunden überhaupt dafür, was unter der Haube passiert?

Ein nennenswerter Teil von Smartphone-Eignern weiß aller Wahrscheinlichkeit nach gar nicht, was an technischem Schnickschnack in ihrem Gerät steckt. Und neue technische Fähigkeiten dürften die Kaufentscheidung nicht wesentlich beeinflussen. Das erste iPhone beherrschte nicht einmal UMTS, die Bluetooth-Implementierung ist bis heute verkrüppelt, nicht einmal die Bedienung per Touchscreen als solche war wirklich neu. Nokia hatte seinerzeit wesentlich leistungsfähigere Smartphones im Angebot.

Neu und so gut, dass die Kunden Apple 2007 das erste iPhone aus der Hand rissen, waren hingegen die Bedienmethaphern und die Reduktion auf das Wesentliche. Während man sich anderswo durch zig Menüs klicken musste, um WLAN oder ein Mail-Konto einzurichten, beschränkt sich iOS auf das Unabdingbare. Weshalb es immer noch keinen NFC-Chip im iPhone gibt: Außer fürs mobile Bezahlen braucht man den nicht, und wer braucht mobiles Bezahlen? Das feste Verpartnern von Bedienbarkeit und Reduktion dürfte bis heute der entscheidende Grund für den iPhone-Kauf sein.

Letztlich könnte es den Smartphones so gehen wie vielen Konsumgütern: Handelt es sich um einen reifen Markt, gibt es keine ganz großen Neuerungen mehr. Trotzdem verschwinden weder die Geräte selbst noch ihre Hersteller zwangsläufig – Miele lebt weiter, obwohl es nicht jedes Jahr die Waschmaschine neu erfindet, und Montblanc baut seit über 100 Jahren Füllfederhalter.

Wie Apple verkaufen diese Hersteller nicht nur Produkte, sondern deren hohen Preis selbst: Käufer zeigen, dass sie sich das Teure leisten können. Und allen Apple-Astrologen zum Trotz bleiben iPhones teuer. Auch das neue 5c ist nicht das von ihnen prophezeite Billigerät. Die mit den hohen Preisen verbundene größere Marge führt wiederum dazu, dass der Hersteller trotz sinkenden Marktanteils wesentlich profitabler arbeitet als sein Hauptkonkurrent Samsung: Im zweiten Quartal 2013 erzielte Apple einen Vorsteuergewinn von 9,2 Milliarden US-Dollar, Samsungs Mobilabteilung kam auf 5,64 Milliarden.

Dass Apple keineswegs bald den Weg von Palm, Nokia und BlackBerry beschreiten wird, zeigt ein weiterer Blick in die Bilanzen: Der iPhone-Hersteller hat ein Finanzpolster von 144 Milliarden US-Dollar aufgebaut. Davon sind 100 Milliarden für Dividendenzahlungen und den Rückkauf eigener Aktien vorgesehen. Apple dürfte sich deshalb über deren sinkenden Kurs freuen.

Christian Kirsch

CHRISTIAN KIRSCH



Neueste Technologie von DELTA Computer
mit Intel® Xeon® Prozessoren!



Bis 24 Cores mit
E5-2600 v2 CPUs

**DELTA Ultra-Low-Noise-Workstation:
D20x-RI-ULN**

Maximale Leistung, minimale Geräuschentwicklung:

Gedämmerter Tower, extrem leises Netzteil.

2 Intel Xeon E5-2600 v2 Prozessoren mit 4, 6, 8, 10 und 12 Cores, bis zu 30 MB L3 Cache.

Pro CPU 4 Speicherkanäle mit max. 1866 MHz.

Max. 768 GB DDR3, Modelle mit bis zu 4 GPU/MIC.

	inkl. MwSt.	exkl. MwSt.
Jetzt	4.522,00 €	3.800,00 €

Z. B. mit **2 Intel Xeon E5-2650 v2 Prozessoren** mit insg. 16 Cores mit 2,6 GHz (T.B. 3,4 GHz), 32 Threads, 20 MB L3 pro CPU, 64 GB DDR3 1866 RAM, 2 TB Disk oder 120 GB SSD, DVD-RW, GTX 640, Tast. u. Maus.



**DELTA Double-Twin-Server:
D20-4x-M2-RI**

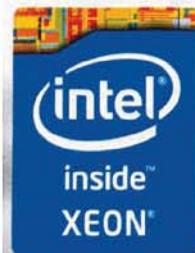
ideal als Mini-Cluster oder Cluster-Knoten:

4 Hochleistungs-Blades mit 2 Intel Xeon E5-2600 v2 Prozessoren teilen sich einen 2 HE Einschub.

Bis zu 16/20/24 Cores mit 3,3/3,0/2,7 GHz pro Rechner. 6x 2,5" oder 3x 3,5" Disk, opt. FDR/QDR IB, 10/40G.

	inkl. MwSt.	exkl. MwSt.
Jetzt	19.516,00 € (4 Rechner)	16.400,00 € (4 Rechner)

Z. B. mit **4 Rechnern mit insgesamt 8 Intel Xeon E5-2670 v2, 80 Cores mit 2,5 GHz** (T.B. 3,3 GHz), 160 Threads, 4x 64 GB DDR3 1866, 4x 1 TB Disk, 2x 1620W red. PS, 2x Gigabit u. BMC pro Rechner.



Steigern Sie nicht nur die Produktivität Ihrer Hardware. Nutzen Sie auch die DELTA Hardware/Software Bundles mit Intel® Software Tools im HPC Umfeld zum Superpreis.

Intel, das Intel Logo, Intel Inside, das Intel Inside Logo, Xeon und Xeon Inside, Xeon Phi und Xeon Phi Inside sind Marken der Intel Corporation in den USA und anderen Ländern.

ELTA Computer Products GmbH

Montgenstraße 4 • 21465 Reinbek bei Hamburg
Tel. 040-300 672-0 • Fax. 040-300 672-11

Nicht nur Webkit

(Webdesign: Hintergrundbilder mit CSS3 gestalten; IX 9/2013; S. 122)

Der entscheidende Nutzen von mehrfachen Hintergrundbildern ist nicht, dass man sich das Bildverarbeitungsprogramm spart, sondern dass man sich dadurch spart, nur für die zusätzlichen Hintergrundbilder weitere HTML-Elemente im Code einzufügen. Denn meist wird man verschiedene Hintergrundbilder flexibel kombinieren und einsetzen wollen.

Für hochauflösende Displays gibt es im Artikel ein Beispiel mit dem Webkit-Prefix: @media (-webkit-min-device-pixel-ratio: 2) { }

Hier sollten aber auch die anderen Browser berücksichtigt werden. Das ist insbesondere wichtig, da die Angaben für andere Browser sich nicht einfach durch Austausch des Präfixes herleiten lassen. Im Artikel heißt es, min-resolution wäre nicht empfohlen. min-resolution ist jedoch die offizielle vom W3C abgesegnete Standardvariante, das im Beispiel aufgeführte device-pixel-ratio ist eine proprietäre Webkit-Erfundung; deswegen sollte man min-resolution unbedingt zusätzlich verwenden.

Wenn background-attachment in einem Artikel zu CSS3 erwähnt wird, sollten nicht nur die Werte aus CSS 2.1 zur Sprache kommen, sondern auch das neu eingeführte background-attachment: local. Es fehlt außerdem im Artikel die Erwähnung der neuen Eigenschaft background-origin, die es neben background-clip gibt.

Übrigens kann man sich bei der Definition der Animation viel Code sparen, denn die Variante mit -moz- ist seit Firefox 16 nicht mehr notwendig und die mit -o- präfigierte Variante bräuchte man nur für den Opera 12.0.

Auch ist die Aussage, dass die Animationsmöglichkeiten mit CSS das Ziel hätten, JavaScript, animierte GIFs, Flash oder Videodateien im Browser zu ersetzen, missverständlich. Durch die CSS3-Animationen kann man einen Teil der Animationen über CSS erstellen – JavaScript beispielsweise wird man aber immer weiter brauchen, eben gerade auch häufig, um die CSS3-Animationen auszulösen.

Und zum Schluss: In einem professionellen Artikel sollte eigentlich kein Link mehr auf W3Schools stehen, denn das erweckt immer den fälschlichen Eindruck, es hätte etwas mit dem W3C zu tun – was es aber in keiner Weise hat, und die Informationen sind auch nicht zuverlässig.

DR. FLORENCE MAURICE, MÜNCHEN

Ideal-Partner Amazon

(Editorial: Girl on Fire; IX 9/2013, S. 3)

Anstatt für BB 10 diesen unsinnigen Fakes mit den portierten/side loaded Android-Apps einzugehen, hätte man bei BlackBerry eine eigene Dalvik VM schreiben sollen. So etwas hat es in den Anfängen von Android auch schon einmal von einer kleinen Firma gegeben, muss also nicht unbedingt der Riesenaufwand sein.

Danach hätte man sich noch den richtigen Partner suchen sollen, für mich wäre das ganz klar Amazon, da die keine Smartphones haben, aber einen eigenen Android App Store; den hätte man dann mit ausliefern können. Und die Amazon Cloud Services hätten super zur schwarzen Beere gepasst, sind ja ebenfalls im Business sehr beliebt. Das hätte BB noch eine minimale Chance gegeben, aber so wie es jetzt aussieht, ist es schlicht zu spät und etwas zu ideenlos ...

ANDREAS LORENZ, REMSCHEID

Endbenutzer überzeugen

(Editorial: Girl on Fire; IX 9/2013, S. 3)

Es ist wichtig, zuerst den Endbenutzer einzubeziehen und von einem Gerät zu überzeugen, das er 24/7 mit sich rumführt und nutzen möchte. Wenn ein Hersteller das geschafft hat, wird er zum IT-Admin kommen und sagen „Mach mir da mal Mail raus“ (O-Ton Volker Weber auf einem Heise-Event).

Auch wir als IT-Dienstleister haben uns auf mobile Endgeräte anderer Her-

Der direkte Draht zu



Direktwahl zur Redaktion: 05 11/53 52-387

Bitte entnehmen Sie Durchwahlnummern und E-Mail-Adressen dem Impressum.

Redaktion IX | Postfach 61 04 07
30604 Hannover | Fax: 05 11/53 52-361
E-Mail: <user>@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 www.ix.de/IXJMMSSS diesem Hinweis können Sie diese URL im Webbrowser aufrufen, um eine klickbare Liste aller URLs zu bekommen.

steller spezialisiert und sehen derzeitig den Trend zu iOS und Android. Nokia Lumia testen wir noch ausgiebig auf Herz und Nieren (sprich Security). Wird aber wirklich bald die dritte Option für Unternehmen werden. Hut ab Nokia – sehr risikantes Manöver, das sich wohl bald auszahlen wird.

Danke auch an Volker Weber! Jetzt muss ich es nicht mehr erklären, sondern kann mit dem Finger auf dieses Editorial zeigen.

ADRIAN WOIZIK, STUTTGART

Marke fürs Leben

(Editorial: Girl on Fire; iX 9/2013, S. 3)

Kommt ein Jünger zu Saturn, schleppt seine Liebste schnurstracks an PCs und Samsungs vorbei zum Apple-Altar:

„Von hier (weist dahin, wo Apple anfängt) bis da (weist dahin, wo Apple aufhört) ist alles für uns. Den Rest kannst Du gleich vergessen!“

So selbst erlebt. Theoretisch mag der Konsument zwar noch Firmenwelten überbrücken können, praktisch kauft er sich eine Hard- und Content-Plattform, die er womöglich Zeit seines Lebens nie mehr verlassen wird. Und das funktioniert nur easy, wenn alles Digitale aus einer Hand kommt.

Vermutlich hat BB das zu spät erkannt, und sie brauchen wirklich eine Zeit der Besinnung, wie das vorhandene am besten zu monetarisieren ist. Genau das hat Steve bei seiner Rückkehr letztendlich auch gemacht und Volltreffer gelandet.

Alicia Keys wird nicht wirklich helfen. Die hat ja angeblich selbst weiter mit dem iPhone gesimst.

FRANK MONDORF,
AUS DEM IX-FORUM

Tragische Geschichte

(Editorial: Girl on Fire; iX 9/2013, S. 3)

Sehr schönes Editorial, vielen Dank, das wurde intern gleich weiterverteilt, die iX gekauft ;-)

Volker Weber beleuchtet eine tragische Geschichte. BB kann genau das, wonach viele Firmen sich sehnen, trotzdem kommen sie nicht mehr zum Zug. Die (früher undenkbar) Risiken werden oftmals hingenommen. Bleibt zu hoffen, dass Android und iOS bald nachziehen, die Ansätze sind in jedem Fall bereits vorhanden.

HUBERT STETTNER, VIA E-MAIL

Genau auf den Punkt

(Editorial: Girl on Fire; iX 9/2013, S. 3)

Herr Weber hat in diesem Editorial alle Probleme genau auf den Punkt gebracht. Meiner Meinung nach war es eine Fehlentscheidung, das Playbook nicht mehr weiterentwickeln. Auch wenn das neue Betriebssystem aufgrund der Hardware-Anforderungen nicht mehr auf den Tablets der ersten Generation lauffähig ist, so wäre es doch ein Leichtes für BlackBerry gewesen, eine stärkere Version nachzuschieben.

Ich hoffe für BlackBerry, dass sie es aus eigener Kraft, oder zumindest mit einem guten Partner, schaffen. Das Unternehmen zu verkaufen und somit das Ruder aus der Hand zu geben, halte ich für den falschen Weg. Auch wenn Herr Heins sicherlich gut daran verdienen würde ...

RALPH HAMMANN, DARMSTADT

Gorbatschow hat Recht

(Editorial: Girl on Fire; iX 9/2013, S. 3)

Toller Kommentar Herr Weber, den man eigentlich komplett unterschreiben kann. Erneut zeigt Gorbatschows Satz „Wer zu spät kommt, den bestraft das Leben“ seine Richtigkeit. RIM hat sich unter Lazaridis zu lange auf seinen Lorbeeren ausgeruht, BB10, Q10 und Z10 sind viel zu spät auf den Markt gekommen. Als überzeugter BB-User tut es mir wirklich leid, dass BB jetzt so übel abstürzt. Aber ich fürchte, wenn keine Unterstützung von einem Partner kommt, ist BB bald Geschichte.

Eigentlich wollte ich mir auch schon längst ein neues Gerät geholt haben. Die Firmenpolitik jedoch lässt mich jetzt noch weiter warten. Man überlegt halt zwei mal, ob man noch in ein Produkt investieren soll, wenn dessen Überleben nicht gesichert ist. Was mich aber noch viel mehr gestört hat, ist der Umgang mit dem Playbook! Denn das hätte ich mir in 2012 im Vorriff auf das nächste Smartphone fast noch gekauft und dabei auf die Zusage vertraut, dass BB10 darauf laufen soll.

Jetzt aber stellt sich heraus, das geht dann doch nicht. Aber statt einer Entschuldigung in dieser Angelegenheit verbreitet Herr Heins jetzt seine exklusive Ansicht, Tablets seien eh nicht wichtig. Das erzähle mal jemand den Vorständen von Dell, HP, Lenovo & Co., deren PC-Verkaufszahlen zurzeit wegen der Tablet-Verkäufe regelrecht einbrechen. Und wer wie etwa Dell und HP keine mobilen Devices im Angebot hat, der sieht richtig alt aus.

DIRK ROEBERS, DÜREN



Hörst Du es summen?

Swarm:

Zusammenarbeit am Quellcode im Flug.

Mit Swarm bietet Perforce eine flexible verteilte Plattform für Zusammenarbeit am Quellcode. Verteilte Teams können schneller agile Arbeitsabläufe und kontinuierliche Auslieferung realisieren.

Schließ Dich dem Schwarm an
info.perforce.com/swarm-ix



PERFORCE

Version everything.

VMworld 2013 US:
Auf der Suche nach neuen Märkten

Um Stellungen

Jens-Henrik Söldner

Trotz aller Erfolge muss VMware sich nach neuer Technik umsehen, bevor Hypervisors wie bei Microsoft als Massenprodukt zur Packungsbeilage verkommen. Auf seiner Hausmesse in den USA war der Veranstanter bemüht, sich neu in Stellung zu bringen.

Für den amerikanischen Virtualisierungsspezialisten wird es zunehmend schwieriger, Kunden ins gelobte Land des vollautomatisierten Software-Defined Data Center zu lotsen, als beim bisherigen Geschäft mit der Software für Server und Desktops. Das Interesse jedenfalls war groß: Mit über 22 000 Teilnehmern an der VMworld in San Francisco konnte VMware Ende August sein 15-jähriges Bestehen mit einem Besucherrekord feiern.

Netz und Speicher ins Virtuelle

Nach einem kurzen Rückblick hat der VMware CEO Pat Gelsinger in seinem Hauptvortrag die Richtung für die nächsten Jahre gewiesen: Ausweiten der Aktivitäten auf das Virtualisieren von Netzwerk und Speichersystemen, das Automatisieren des Rechenzentrumsbetriebs als Ablösung des klassischen IT-Managements und das Bereitstellen hybrider Cloud-Angebote in Konkurrenz zu Amazon und Co.

Als mittelfristiges Ziel gilt das Umstellen des RZ-Managements: Es sollen nicht nur Ressourcen wie CPUs und Hauptspeicher unter der Kontrolle der Virtualisierungssoftware laufen, sondern ebenso Netz und Speichersysteme, die bislang Administratoren vorwiegend manuell einrichten müssen.

Beim herkömmlichen Virtualisieren von Computersystemen kann VMware noch einen Vorsprung mit seiner Technik auf dem Markt halten, obwohl Microsoft und die OpenStack-

Verfechter ihre Stellungen ausbauen, um den Hypervisor zu entzaubern und als Massenprodukt zu degradieren.

VMware verlangt nach wie vor noch hohe Lizenzkosten für seinen vSphere Hypervisor, wohingegen Microsofts Hyper-V samt seiner Enterprise-Features komplett kostenfrei ist. Selbiges gilt für Citrix' XenServer oder KVM.

Jedoch sind „Mehr und mehr VMware-Kunden ... dazu bereit, auf High-End-Funktionen der vSphere-Plattform zu verzichten und auf kostenfreie Alternativen auszuweichen, um Lizenzkosten zu sparen“, erläutert Torsten Volk, Analyst bei Enterprise Management Associates im Gespräch mit iX auf der VMworld. „Die VMworld 2013 hat gezeigt, dass VMware verstanden hat, dass die zukünftigen Wettbewerbsvorteile nicht mehr in der Hypervisor-Plattform selbst, sondern im IT Operations Management (VMware vCOPS) und Automatisieren (VMware vCAC) liegen werden. VMware macht derzeit

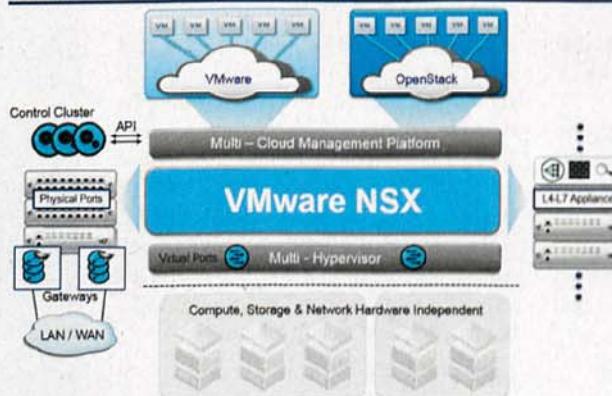
Ernst mit Investitionen in diesen Gebieten, sodass wir einige Innovationen in diesen Bereichen erwarten dürfen“, so der US-amerikanische Analyst.

Weiterhin zementiert ist die Rolle des gemischt beurteilten vSphere Web Client, der auf Dauer den Windows-Client komplett ablösen soll. VMware hat an einem Hauptkritikpunkt gearbeitet: der schwachen Performance des Web-Clients. Wichtige Plug-ins etwa zum Verwalten des „vSphere Update Manager“ oder „Site Recover Manager“ (SRM) fehlen nach wie vor. Dem Administrator bleibt nichts anderes übrig, als mit zwei unterschiedlichen Clients parallel zu arbeiten, da alle neuen Funktionen seit den Versionen 5.1 nur noch über den Web Client anzusteuernd sind.

Das neu angekündigte Produkt vSAN, in einer öffentlichen Beta verfügbar und für das erste Halbjahr 2014 erwartet, stellt VMwares Einstieg in den Software-Defined-Storage dar, ein Bereich, in dem andere Hersteller seit Längerem vertreten sind. Nach Bekunden des Herstellers ist vSAN noch nicht für Speichersysteme mit unternehmenskritischen Daten vorgesehen und daher als Gehversuch des Herstellers in einem neuen Gebiet zu werten.

Für NSX (Network and Security) hat VMware zwei Produkte zusammengeführt: die durch die kostspielige Übernahme von Nicira hinzugekommene „Network Virtualization Platform“ (NVP) und das eigene „vCloud Networking and Security“ (vCNS). Es soll für alle gängigen Hypervisors und diverse Cloud-Management-Plattformen wie OpenStack zur Verfügung stehen.

Introducing VMware NSX – The Network Virtualization Platform



VMware will die Netzwerkdienste in den OSI-Schichten 2 bis 7 komplett per Software steuern und automatisieren. Im Unterschied zur klassischen Virtualisierung von Computersystemen bewirkt NSX keine Einsparungen an Hardware, sondern kann den Aufwand für Administratoren reduzieren. Erhältlich soll es in Q4 sein, allerdings nur über VMwares Consulting-Abteilung.

Von Partnern zu Gegnern

VMware konnte über zwanzig Partner für NSX nennen, darunter die Switch-Hersteller HP und Arista, Firewall- und Sicherheitsspezialisten sowie den Konkurrenten Citrix. Mit dem Netzwerk-Platzhirsch Cisco fehlt jedoch einer der Wichtigsten, den VMware durch die Ankündigung direkt als „Freiheit“ herausfordert.

Beim vCloud Director und Namensgeber der vCloud Suite wird es Änderungen in der Strategie geben. Im Gespräch mit iX hatte vSphere-Produktmanager Michael Adams den Weg angedeutet: „Die bisherige Funktionalität des vCloud Director soll aufgeteilt werden und teilweise in den vCenter Server und, teilweise in das vCloud Automation Center (vCAC) einfließen.“

vCloud Director wird in Zukunft nicht mehr als eigenständiges Produkt verfügbar sein, bisherige Kunden werden eine Migration zum vCAC durchmachen müssen.“ Die Entscheidung zum Verlagern der bisherigen vCloud-Director-Funktionen ins vCAC haben die anwesenden Analysten positiv vermerkt.

Keine Verlautbarungen gab es zu den Produkten für Endanwender im Bereich Virtual Desktop Infrastructure (VDI) wie „Horizon View“. Während Konkurrent Citrix im Mai sein VDI-Flaggschiff XenDesktop 7 vom Stapel ließ (siehe Seite 72), herrscht bei VMware Stille. Wenn es dazu Neuigkeiten geben sollte, muss man sich wohl bis zur „VMworld 2013 Europe“ gedulden, die vom 15. bis zum 17. Oktober in Barcelona stattfindet. (rh)

Kompakte Computing-Plattform NeXtScale von IBM

Im Rahmen einer allgemeinen Auffrischung seiner System-x-Serie hat IBM ein spezielles Produkt hinzugefügt. Jüngster Spross in der x86-Familie ist das NeXtScale System. In einem 19-Zoll-Schrank will der Hersteller in 84 Rechnern 2016 Prozessorkerne betreiben können.

Die hohe Packungsdichte erreicht der Hersteller durch Rechnermodule, von denen zwei nebeneinander eine Höheneinheit belegen (Half-wide 1U). Jedes verfügt über zwei CPU-Sockel, bis zu 128 GByte Hauptspeicher, entweder ein 3,5-, zwei 2,5-Zoll-Laufwerke oder vier 1,8 Zoll große SSDs mit einem Maximalvolumen von 4 TByte, zwei Gigabit-

Ethernet-Anschlüsse on-board und einen PCIe-3.0-Slot (x16). Optional sind zwei Infiniband- oder 10-GbE-Ports verfügbar, die keinen Slot belegen.

Allein durch den Einsatz von Ivy-Bridge-CPUs aus Intels E5-2600-v2-Serie verspricht IBM einen Performance-Zuwachs von 45 % gegenüber dem Vorgänger mit Sandy-Bridge-Architektur. Die Energieaufnahme pro CPU liegt bei bis zu 130 Watt (TDP), die Zahl der Cores bei maximal 12. Zum Erhöhen der Rechengeschwindigkeit können laut IBM Grafikprozessoren (GPUs) oder Intels Xeon Phi dienen.

Das NeXtScale System ist in einem „n1200 Enclosure“ untergebracht. Das 6U hohe

Gehäuse hat zwölf Einschübe für nx360-M4-Server. Für die Stromversorgung sind dort sechs Hot-Swap-Netzteile eingebaut, die Kühlung sollen zehn ebenfalls im Betrieb wechselbare Ventilatoren garantieren. Zum Verwalten und Überwachen aus der Ferne besitzt jeder Server IBMs integrierte Management-Modul Typ 2 (IMM2). Platforms LSF (Load Share Facility) und HPC (High Performance Computing) sollen das Verteilen von Lasten und das optimale Ausnutzen der Rechenkapazität regeln.

Als Betriebssysteme unterstützt IBM für diese Plattform sowohl Windows Server, als auch Enter-

prise Linux von Red Hat und SUSE, außerdem VMwares vSphere Hypervisor (ESXi). Das n1200-Gehäuse kostete 4200 Euro, der Preis für ein x360-Severmodul in der Grundausstattung (eine 2,1-GHz-CPU, 8 GByte RAM, keine Festplatte) liegt bei 2676 Euro netto. Ab Ende Oktober 2013 soll das NeXtScale System allgemein verfügbar sein. (rh)



Kurz notiert



Umzug: 10 Milliarden US-Dollar will das US-Innenministerium (DOI) für das Verlagern seiner IT in die Cloud investieren. Man rechnet damit, dadurch in der Zeit von 2016 bis 2020 jährlich rund 100 Millionen US-Dollar einsparen zu können.

Im Job: Für den Einsatz von Google+ als App im Geschäftlichen unterstützt es das gemeinsame Arbeiten mit mehreren Konten. Außerdem hat das Unternehmen die Google+ Domains API freigegeben.

In a Box: Oracle tritt mit seiner Virtual Compute Appliance gegen NetApp und EMC an. Sie besteht aus x86-Servern samt Speichersystem und der Virtualisierungstechnik für Netzwerke, die sich Oracle 2012 mit dem Kauf von Xsigo Systems ins Haus geholt hatte.

Haltbarkeit: VMware hat die Version 10 seiner Virtualisierungssoftware für Desktops „Workstation“ freigegeben. Zu den neuen Features zählen die Unterstützung aktueller Betriebssystemversionen wie Windows 8.1 und die Möglichkeit, virtuelle Maschinen über ein Verfallsdatum automatisch stillzulegen.

Proxmox VE 3.1 unterstützt SPICE als Preview

Als herausragende Neuerung von Proxmox 3.1 darf die Unterstützung des Simple Protocol for Independent Computing Environments (SPICE) als „Technology Preview“ gelten. Es dient dazu, Desktop-Umgebungen über das Netz bereitzustellen. Als neues Dateisystem-Plugin haben die Entwickler des GlusterFS ihr clusterfähiges Dateisystem hinzugefügt. Außerdem können Anwender ihre VE-Server nun über das WebGUI aktualisieren.

Das Aktualisieren von 3.0 auf 3.1 hat es allerdings an anderer Stelle in sich und löste bereits einen Sturm der Entrüstung in den Proxmox-Foren aus. Bei Version 3.1 existieren die beiden vorherigen Proxmox-Repositories (*pve* und *pve-test*) nicht mehr. Das erste dien-

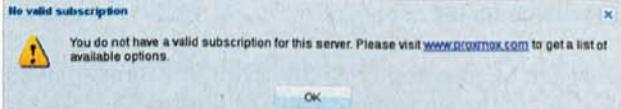
te dazu, alle VE-Server auf dem aktuellen Stand zu halten, im zweiten konnten Nutzer Test- und Beta-Software installieren.

Aufgrund der teilweisen bösen Kommentare im Forum ist der Hersteller ein wenig zurückgerudert und hat das Enterprise-Repository als zusätzliches Extra tituliert, hingegen das No-Subscription-Repository als das vorherige „*pve-stable*“.

Im Zuge der Lizenzänderung hat man bei Proxmox allerdings den Einstiegspreis um mehr als die Hälfte gesenkt: Der Zugriff auf das Enterprise-

Repository kostet als „Proxmox VE Community Subscription“ pro CPU und Jahr 49,90 Euro, einen Rabatt für eine größere Anzahl von CPUs gibt es nicht. Die Preise staffeln sich und liegen beim bisherigen Premium-Support inklusive Unterstützung per SSH-Login bei 796 Euro pro CPU und Jahr. Nach wie vor bietet die Wiener Proxmox Server Solution GmbH ihr Proxmox VE 3.1 unter der GNU Affero General Public License (AGPLv3) als Open-Source-Projekt zum kostenfreien Download an.

Michael Plura (rh)



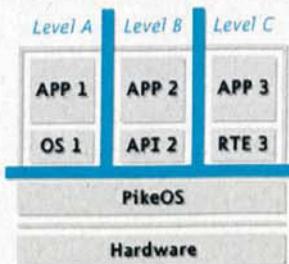
Multicore-Unterstützung für PikeOS

Der Spezialist für Echtzeitbetriebssysteme SYSGO hat mit PikeOS 3.4 den Anwendungsbereich seiner Plattform „Safe

and Secure Virtualization“ (SSV) erweitert. Der auf RTOS (Real Time Operation System) aufgebaute Hypervisor zum Virtualisieren von normalen und Echtzeitbetriebssystemen liefert die Grundlage für eine nach DO-178B zertifizierte Variante von PikeOS. Die Richtlinie gilt für Softwareentwicklungen in der Luftfahrt.

Zu den Neuerungen gehören der Support für IOMMUs (I/O Memory Mapping Units), die Grundlagen für weitere Si-

cherheitszertifikate wie IEC 61508 und EN 50128 SIL 4 (Safety Integration Level), eine native API für PikeOS und anderes mehr. Außerdem hat der Hersteller die mit PikeOS 3.1 eingeführte Multicore-Unterstützung auf neue Architekturen wie Intels Core i7 2655LE ausgeweitet. Ab September soll PikeOS 3.4 verfügbar sein. Die in Klein-Weinheim ansässige SYSGO AG bietet außerdem ELinOS embedded Linux an. (rh)



Citrix veröffentlicht XenClient Enterprise 5

Citrix hat die Version XenClient Enterprise 5 freigegeben. Damit sollen Administratoren per Host oder lokal bereitgestellte virtuelle Desktops zentral verwalten können. Das Unternehmen verspricht erhebliche Erleichterung für das Systemmanagement und einen sicheren Einsatz von Laptops und PCs in Unternehmen.

Für Mitarbeiter bestehen laut Citrix noch nie da gewesene Möglichkeiten, ihren Desktop ihren Wünschen gemäß anzupassen. Dank der Virtualisierung kann die Administration der Desktops aus der Ferne erfolgen. Es ermöglicht Anwendern das Arbeiten von wo aus auch immer und zu jeder Zeit, selbst über langsame, instabile oder unterbrochene Netzverbindungen.

XenClient Enterprise 5 ist Bestandteil von XenDesktop Enterprise und Platinum. Es bietet eine Profile-Synchronisation zwischen lokalen und auf einem Host laufenden vir-

tuellen Arbeitsumgebungen. Die Personal vDisk erlaubt es Anwendern, ihre eigenen Applikationen einzurichten, während die Administratoren weiterhin die Grundkonfiguration überwachen und auf dem neuen Stand halten können.

Das Verwalten des XenClient erfolgt, ohne umstellen



zu müssen, über die Werkzeuge des XenDesktop mit Tools wie Citrix Profile Management

and ShareFile. Der Anbieter stellt per Web eine Testversion zur Verfügung. (rh)

Monotype startet Baseline-Plattform

Speziell für Entwickler hat Monotype seine Baseline-Plattform eröffnet. Wer Anwendungen oder Geräte programmiert, kann dort aus einem Katalog mit über 30 000 Fonts die gewünschten auswählen. Sie lassen sich anschließend über dokumentierte und lizenzierte Schnittstellen zur Programmierung (APIs) einbinden.

Als erster Partner hat Enfocus das Angebot genutzt. Er hat damit seine Software „PitStop 12“ entwickelt, die fehlende oder defekte Fonts in PDF-Dokumenten findet und automatisch korrigiert. (rh)



SICHERE STANDORTVERNETZUNG MADE IN GERMANY

„Auch das beste Schloss bringt nichts, wenn der Einbrecher durch die offene Hintertür kommt.“

Simon Ley,
Entwickler bei Viprinet

China und die USA unterstellen sich heute gegenseitig, zwecks Wirtschaftsspionage mit Hintertüren verschleierte Routertechnik auf den Markt zu bringen. Dank NSA-Affäre herrscht Gewissheit, dass vertrauliche Daten auch bei den Netzbetreibern nicht sicher sind. Das Vertrauen ist bei Unternehmen wie Bürgern zu Recht erschüttert, der Staat zeigt sich überfordert. Wem können Sie noch vertrauen?

Wir sind Viprinet, ein in Deutschland entwickelnder und produzierender Routerhersteller. Die abhörsichere Ende-zu-Ende-Verschlüsselung unserer VPN-Router ist komplett in Ihrer Hand, und nur Sie haben den Schlüssel. Unsere Produkte sind frei von Backdoors, und wir kooperieren nicht mit Geheimdiensten.

Um Ihre Unternehmensstandorte sicher zu vernetzen, nutzen unsere Router mehrere gebündelte günstige Consumer-Medien wie DSL, UMTS oder LTE. Die Daten werden dabei zerteilt und verschlüsselt übertragen. Durch diese Risikoverteilung auf mehrere Zugangsnetze wird Ihre Standortanbindung daher auch noch hochausfallsicher, bei geringen laufenden Kosten – und das selbst an entlegenen oder mobilen Standorten.

Viprinet schafft Ihr wirklich privates Netzwerk. Mit Sicherheit.



GDC 2013: Mobile Plattformen und neue Bezahlmodelle

Das Spiel um Spieler



Hans N. Beck

Geld ist nicht alles – aber ohne Geld ist alles nichts. Schöne Spielideen, brillante Grafiken und riesige Märkte nützen nichts, wenn man daran nicht zu verdienen versteht. Diese Erkenntnis zog sich als roter Faden durch die GDC 2013.

International, breitgefächert und gut besucht: So erlebten Besucher dieses Jahr die wieder in Köln stattfindende Games Developer Conference Europe. 2250 Besucher nutzten die Gelegenheit und informierten sich Ende August drei Tage lang im Kölner Kongresszentrum in weit über 100 Vorträgen über verschiedene Aspekte der Spieleentwicklung und -vermarktung. Dass der Begriff „Computerspiel“ heutzutage sehr weit gefasst ist, belegten die angebotenen Themen: Die Vorträge gliederten sich nach Design, Produktion, Programmierung und Visual Arts. Den geschäftlichen Aspekten der Branche widmete sich eingehend der Themenschwerpunkt Business & Marketing.

Die Märkte sind einem gewaltigen Wandel unterworfen.

Bildeten vor Jahren noch PC und Konsole die Basis für Computerspiele, haben heute Mobilgeräte wie Tablets und Smartphones diese Rolle übernommen. Ross Brockmann von Google brachte es in seinem Vortrag mit seiner Aussage auf den Punkt, dass alle fünf Minuten ein neuer Spieler geboren würde. Dabei geht es nicht um die Bevölkerungsexplosion, sondern die wachsende Zahl der Menschen, die Zugriff auf ein mobiles Endgerät haben.

Der Markt ist offen für Mobiles

Mobile Endgeräte beschäftigen die Menschen bereits mehr als das Web und konkurrieren mit dem TV, wie Guillaume Larrieu von Flurry in seinem Vor-



Quelle: Official GDC

Entwickler gesucht: Viele Aussteller buhlten um talentierte Mitarbeiter, damit sie die zahlreichen Projekte stemmen können (Abb. 1).

trag zum Thema Bewertungsmaßstäbe für Spiele auf mobilen Plattformen ausführte. Beim Marketing und dem Design sei die Tendenz zu berücksichtigen, dass die Nutzer von Tablet und Smartphone auch älter werden. Entgegen dieser Feststellung erklärte John Howard von der BBC, dass sein Arbeitgeber erfolgreich auf die Zielgruppe Kinder setze. Tablets als lohnender Markt bleibt aber auch von Howard unbestritten. Im United Kingdom ist laut Howard der Anteil von Tablet-Besitzern von 12 % im Jahr 2012 auf mittlerweile 24 % gestiegen.

So groß der Markt ist, so viele verschiedene Geräte gilt es zu bedienen. Dieser für die Produktion von Spielen erschwerende Bedingung nahm sich Jani Kahrama (Secret Exit Ltd.) in seinem Vortrag an. Über die Dynamik dieser Märkte, die durch das Erscheinen immer neuer Plattformen geprägt ist, referierte Kaya Tanner von AppLift. Seiner Meinung nach sind aggressives Marketing und ein Know-how-Vorsprung bei der Einführung einer neuen Plattform wesentliche Erfolgsfaktoren. Je länger sie jedoch auf dem Markt sei, desto mehr entscheiden gute Inhalte über den Erfolg.

Spieleproduzenten stehen somit vor der Frage, wie sie diesen Markt erschließen und die Wünsche verschiedener Benutzergruppen erfassen können. Hier offenbarte sich einer der Trends der diesjährigen GDC: Stimme dein Produkt genau auf das Verhalten der Spieler und die Zielgruppen ab. Um das zu tun, muss man folglich wissen, wer wie spielt. Es kommt darauf an, Variablen und Bewertungsmaßstäbe – sogenannte Metriken – zu finden, die Rückschlüsse auf diese entscheidenden Werte erlauben. Guillaume Larrieu (Flurry) erläuterte, dass es möglich sei, solche Metriken zu identifizieren, weil Spieler je nach bevorzugtem Genre sowie Zugehörigkeit zu einer sozialen Gruppe deutliche Muster erkennen lassen. Laut Larrieu kann man sogar Schlüsselmetriken bestimmen, die über verschiedene Spiele eines Genres hinweg gelten – etwa, welche Geräte zum Einsatz kommen, oder wie häufig ein Spiel im Monat aufgerufen wird.

Hat man aussagekräftige Metriken gefunden, muss als Nächstes ein Instrumentarium für deren Messung her. Dies ist eine Paradigmenübersetzung für Google, dessen Mitarbeiter Kristoffer Olofsson erläuterte, wie sich Google Analytics für das Optimieren von Spielen durch das Messen des Nutzerverhaltens einsetzen lässt. „Beobachte wer dein Spiel gerade spielt und wie er das tut“ sind seine ausgewiesenen Ziele. Technisch basiert der Ansatz darauf, Google Analytics mittels eines SDKs über einen HTTP Request anzusprechen. Für das Festhalten der Benutzerdaten hat man das Measurement Protocol entwickelt, das in einer Open Beta vorliegt (siehe „Alle Links“). Über dieses Protokoll und das zugehörige SDK lassen sich mit Google Analytics sogar Abstürze und Einkäufe der Spieler verfolgen. Interessierte finden weitere Hinweise auf Googles Entwicklerseiten.

Die Großen helfen den Kleinen

Aber nicht nur bezogen auf die Spieler ändern sich die sozialen Strukturen, auch die Beziehungen von Produzent, Entwickler und Spieler zueinander befinden sich im Wandel. Eingeleitet durch die Einführung von Apples iPhone steht der Appstore mittlerweile als Symbol für den Erfolg des kleinen Programmierers. Indies oder Independent, also meist kleinere Studios, die ihre Produkte selbst vermarkten, finden so eine Existenzgrundlage. Der Große mit der Infrastruktur hilft dem Kleinen mit den guten Ideen.

Auch Google hat mit Analytics, Playstore, Cloud und weiteren Angeboten eine Menge zu offerieren. Dies mag die Firma veranlassen haben, einen Developer Day zu bestreiten. Ein eigener Track bot eine Fülle von Vorträgen. In „Google for Games: Building a Games Business with the Best of Google“ wurden das Programm und die zentralen Stichwörter dieser GDC deutlich: Infrastruktur und Messwerkzeuge bieten, die die Distribution und die Monetarisierung, also letztlich das Generieren von Umsätzen, unterstützen. Viele weitere Vorträge in diesem Rahmen widmeten sich der Erklärung von Techni-

ken und gaben Tipps, wie man Spiele in diesem Umfeld entwickeln und vertreiben kann.

Microsoft hat ebenfalls die Zeichen der Zeit erkannt, wie Gunnar Lott von flaregames und Kristina Rothe von Microsoft in ihrem Vortrag ausführten. Am Beispiel von „Royal Revolt“, einem Spiel der flaregames GmbH, haben sie die Vorteile des Ökosystems von Microsoft präsentiert. Während in anderen App Stores das Kundeninteresse an einzelnen Apps schnell wachse, aber auch ebenso schnell abklinge, zeigten die Kunden bei Microsoft – so die Vortragenden – ein konstanteres Interesse an einzelnen Anwendungen.

Mit Herz und Verstand dabei sein

Wie man Gewinne erzielt, war ebenfalls häufig Thema. Die Antwort auf die Frage, wie sich Geld mit Spielen im mobilen Markt verdienen lässt, heißt nicht etwa 42, sondern „Free to Play“ (F2). Bei diesem Geschäftsmodell zahlen Spieler nicht für das Spiel selbst, sondern für Inhalte, die ihnen Waffen, Ausrüstung oder einen Zeitvorteil verschaffen. Konsens war, dass dies im Bereich der Apps und Onlinespiele die Strategie der Wahl sei.

Einen guten Überblick über zu berücksichtigende Aspekte gab Chris Williams, VP von Big Fisch Games Inc. Er nannte die relevanten Erfolgsfaktoren und zog einen schönen Vergleich: Ein F2P-Spiel zu betreiben, sei vergleichbar mit dem Führen eines Nachtclubs. Man müsse einem geneigten Publi-

kum täglich ein interessantes Angebot machen. In Bezug auf die Monetisierung betonte Williams, dass der Spieler den Gegen- beziehungsweise Nutzwert seiner Einkäufe erkennen müsse. Ein Handel von Spieler zu Spieler sowie eine gut balancierte virtuelle Währung seien, so Justin Beck von PerBlue Inc., in diesem Zusammenhang bewährte Designmittel.

Emotionales Engagement – damit sprach Chris Williams ein weiteres Schlüsselwort der GDC 2013 an: Will man mit F2P Geld verdienen, müssen die Spieler mit dem Herzen dabei sein, um Ausgaben tätigen zu wollen. Ein witziges, mit netten Cartoons unterstütztes Plädoyer für emotional ansprechende Spiele bot der gut besuchte Vortrag „Stealing Your Heart, Eating Your Brain“ von Timo Dries (Wooga GmbH). Entgegen dem allgemeinen Trend dieser GDC empfahl er, sich nicht nur auf Zahlen und Metriken zu verlassen, um bei den Spielern ein emotionales Engagement zu wecken. Man könne eben nicht alles messen, darum sei Liebe zum Detail und ein Engagement auch auf Seiten der Entwickler unabdingbar. „Heart and Brain bei der Spieleanthropologie“ lautete sein griffiges Schlagwort.

Spieler kann man am besten mit spannenden Inhalten bei der Stange halten. Dies war Inhalt vieler Vorträge zum Thema Spieldesign, wobei auch hier die Häufigkeit des Wortes „Emotion“ auffiel. Direkt angesprochen hat das Heidi McDonald von Schell Games. Auf lockere Weise versuchte sie, die Natur einer Romanze zu erfassen und leitete daraus ge-

stalterische Tipps ab. Dies alles stand in dem Kontext, dass weibliche Spieler auf dem Vormarsch seien. Mit Silicon Sisters Interactive aus Kanada gibt es gar eine Firma, in der Frauen für Frauen Spiele entwerfen.

Vom Design der Spiele zur Technik

Ausschnitte aus erzählenden Filmsequenzen in Spiele einzublenden, hat sich ebenfalls als Stilmittel bewährt. Solche kurzen Videos bauen Atmosphäre auf und binden den Spieler an die Geschichte. Das sei allerdings keine triviale Aufgabe, wie Brian Kindred von Blizzard Entertainment betonte, denn allzu leicht werde ein Spieler ungeduldig, wenn er nicht selbst aktiv ist. Thematik dazu passend konnten die Konferenzteilnehmer in dem gut besuchten Vortrag „Creating an Emotionally Engaging Camera for Tomb Raider“ von Remi Lacoste (Crystal Dynamics) erfahren, wie man das Stilmittel Kamera einsetzen sollte. Die Bewegung einer guten Kamera ist analog zu der einer Spielfigur und erzeugt durch gezielte Nahaufnahmen emotionale Nähe und Identifikation. Physische Einwirkungen müssen sich ebenfalls widerspiegeln.

Wie üblich gab es auch Vorträge zu technischen Fragestellungen. Den Teilnehmer bot sich Gelegenheit, sich über die „PlayStation Shading Language for PS4“ zu informieren. Anhand von Demos zeigten die Sprecher Chris Ho (SCEA) und Richard Stenson (SCEA RandD), welche Effekte man damit erreichen kann. Entwickler kontrollieren Vertex-, Pixel- und Geometry-Shader im Umfeld von Direct 11.2+ sowie OpenGL 4.4. Betont wurde, dass Sony für die Weiterentwicklung der Shading Language auf die Kommunikation mit Entwicklern setze. Details zu OpenGL ES 3.0 waren Thema eines weiteren Vortrags.

Immer komplexere Levels verlangen neue Ansätze für deren Generierung. Spannend ist das dynamische Erzeugen von Inhalten. In dem bis zum letzten Platz gefüllten Vortrag „Designing Games with Procedural Content and Mechanics“ stellte Dr. Ernest Adams (freier Consultant und Gastprofessor

an mehreren Universitäten) die dafür notwendigen Techniken vor. Anhand verschiedener Ansätze illustrierte er die Gratwanderung zwischen Kontrollierbarkeit und Sinnhaftigkeit der generierten Ergebnisse.

Wie erwähnt, sehen sich Entwickler mit einer Vielzahl von Plattformen und somit unterschiedlichen Auflösungen konfrontiert. Oliver Franzke von Double Fine Productions gab in seinem Vortrag Anregungen, diese Herausforderung technisch zu meistern. Der Trick besteht darin, plattformspezifischen Code soweit wie möglich zu vermeiden und von Beginn an zu berücksichtigen, welche Auflösungen welche Szene im Spiel erfordert. Ob man besser von einer hochauflösenden Datenbasis herunterrechnet oder verschiedene Level-of-Details vorhält, bestimmt die Anforderung des Spiels.

Zwar rückt die Notwendigkeit von KI (Künstliche Intelligenz) im Zeitalter der Social Games in den Hintergrund. Dennoch lies es sich John Krzewski (Strange Loop Games) nicht nehmen, die Konferenzteilnehmer darüber aufzuklären, wie sie beginnend bei physikalischer Modellierung über daraus abgeleitete Regelsätze und einer darauf aufbauenden KI eine Spieldynamik entwickeln können.

Konkret bezogen auf die Wii U erläuterten die Nintendo-Mitarbeiter Martin Buchholz und Svyatoslav Pidgornyj, wie sich die Konsole mit HTML und JavaScript programmieren lässt. Gegenüber strebt der Hersteller eine deutliche Vereinfachung für Entwickler an.

Interessant war auch, was es nicht zu sehen gab: So spielten Serious Games kaum eine Rolle. Und obwohl es im Trend liegt, alles Geschehen im Spiel zu messen, waren Datenschutz oder Privatsphäre kaum zu vernehmende Themen. Auch die Cloud als Schlagwort ist aus der ersten Reihe in die Menge der Fachbegriffe abgetaucht.

Wer vor allem technische Neuigkeiten sehen wollte, kam ebenfalls auf seine Kosten. In der begleitenden Ausstellung bot Oculus VR den Konferenzbesuchern die Möglichkeit, den VR-Helm Oculus Rift auszuprobieren. Zahlreiche Neu-



Wer bei Oculus Rift VR im virtuellen Rennwagen mitfahren wollte, musste zunächst ein wenig Geduld in der Warteschlange beweisen (Abb. 2).

gierige haben dieses Angebot in Anspruch genommen, so dass bereits nach kurzer Zeit eine Warteschlange entstand, wie man sie sonst nur von der gamescom her kennt (Abbildung 2). Wer die Wartezeit nicht scheute, konnte in einem virtuellen Rennwagen neben dem Fahrer sitzen und eine Probefahrt machen. Dadurch dass man den Kopf mit dem Helm frei bewegen kann, konnte man als Beifahrer sowohl aus dem Fenster schauen als auch den Fahrer beobachten. Die Grafik war detailliert und ruckelfrei, der Helm recht angenehm zu tragen. Gewicht und optische Eigenschaften will der Hersteller aber noch weiter verbessern.

In dem zugehörigen Vortrag machten Oculus-VR-Mitarbeiter Palmer Luckey und Nate Mitchell deutlich, dass das Programmieren für solche Helme nicht trivial ist. Größe und Maßstab erleben Spielende anders als in der Realität. Eine überzeugende Spieelerfahrung verlangt durchdachte Benutzerschnittstellen. Menüs und Bedienelemente etwa sollte man auf ein virtuelles Gerät oder eine Wand im Spiel projizieren. Die Tatsache, dass die Entwickler Augen und Gleichgewicht der Spieler quasi „austricksen“, erzwingt es, dass sie Bewegungen und Perspektiven so wählen, dass die Anwender weder unter Übelkeit noch unter einer Desorientierung zu leiden haben. Schnelle Änderungen von Höhen oder der Perspektive sollten unterbleiben. Die Vortragenden sehen VR-Helme als Quantensprung in der Spieleentwicklung, weil sie eine neue Qualität einführen.

Ein Technikbonbon der besonderen Art präsentierte OpenNI, ein Konsortium zur Entwicklung von 3D-Messtechnik. Die Kamera für Motion Capture in 3D kann in Gesichtern Mimiken ohne Referenzpunkte erfassen. Möglich ist es auch, einen Raum mit nur einem Schnappschuss maßstabsgetreu zu erfassen, um etwa virtuelle Möbel darin zu platzieren oder im Raum vorhandene Strukturen auf dem Tablet auszumesen. Diese ursprünglich für das israelische Militär entwickelte Technik lässt sich inzwischen mit so kleinen Teilen realisieren, dass sie in ein Tablet eingebaut werden könnte.

Fazit

Spieleentwicklung ist heute ein iterativer und verwobener Prozess, in dem die Hersteller versuchen, das Verhalten und die Wünsche der Kunden zu ermitteln sowie Spiele so zu konzipieren, dass sie den Spieler emotional involvieren. Primäres Ziel ist es, den riesigen Markt mobiler Endgeräte zu nutzen. Geld wird vor allem

durch Bezahlinhalte innerhalb des Spiels verdient.

Neue Benutzergruppen sowie ein verändertes Verhalten der Spieler zwingen Produzenten dazu, ihre Zielgruppe genau zu bestimmen. Für das notwendige emotionale Engagement der Spieler werden die mobilen Angebote multiplayer-tauglich, komplexer und angereichert mit sozialen Elementen.

Wer erfolgreich ein Spiel für ein mobiles Gerät entwickeln will, ist also gut beraten, sich nicht nur um Programmietechniken zu kümmern. Auf der anderen Seite verhelfen Apple, Google und Microsoft mit ihren weltweiten Infrastrukturen auch kleineren Studios zu kommerziellem Erfolg. (ka)

Alle Links: www.ix.de/ix1310012

Alcatel-Lucent 
Enterprise

TOP OF RACK DATA CENTER SWITCH

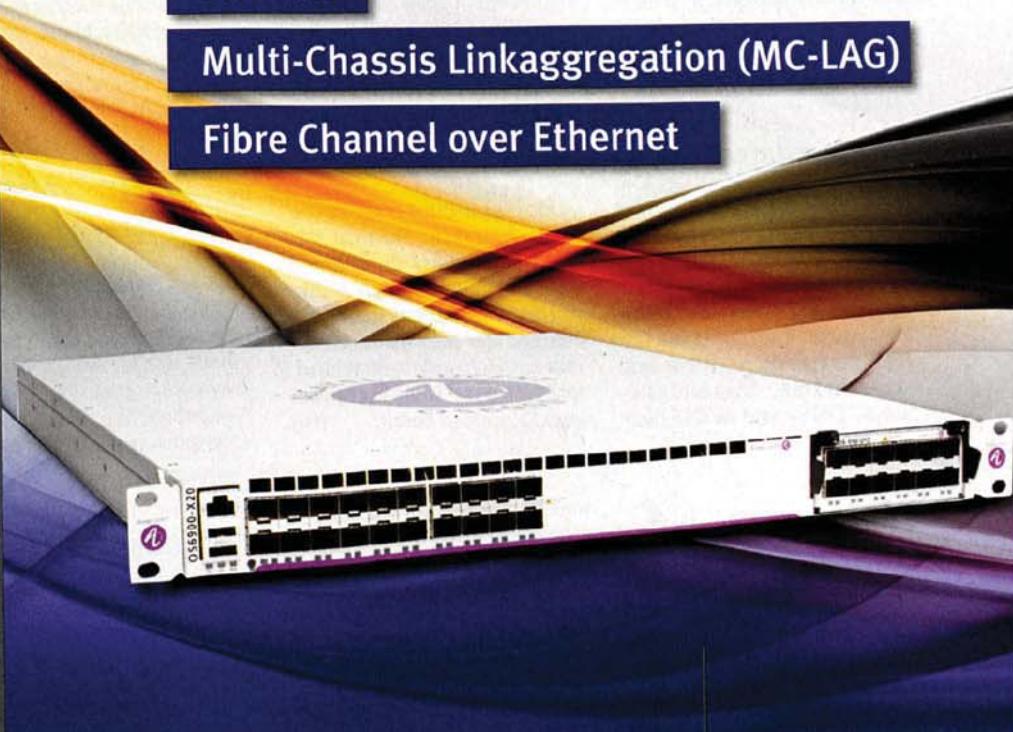
Extrem energiesparend

Bis zu 1,28 Tbit/s Leistungskapazität

Flexibel

Multi-Chassis Linkaggregation (MC-LAG)

Fibre Channel over Ethernet



Ihr Ansprechpartner:

KOMSA Systems GmbH

09231 Hartmannsdorf

Tel.: 03722 713-600

alcatel-lucent@komsa-systems.de


DATA VOICE NETWORKING

iX-Veranstaltungen

Extrem knapp wird es für alle, die bei den Teilnehmergebühren für den **Software QS-Tag** (7. – 8.11.12, Nürnberg) 100 Euro sparen wollen: Nur noch bis einschließlich 27. September gilt der Frühbucherrabatt, ab dann sind statt 850 Euro 950 Euro fällig.

Wenige Tage später, nämlich am 30. September, endet eben diese Frist für die Konferenz **continuous lifecycle 2013** (11. – 13.11.13, Karlsruhe). Dort ist bereits eines der Tutorials ausgebucht – noch ein Grund, sich schnell anzumelden.

Kurz vor Redaktionsschluss wurden auch noch einige Workshops für 2014 auf den Weg gebracht, unter anderem zu C+11, Hadoop, IPv6 und OTRS. Details sind demnächst auf www.ix-konferenz.de zu finden.

Last, but not least: Termin und Ort für den sechsten deutschen **IPv6-Kongress** stehen fest: 22./23. Mai 2014, wieder in Frankfurt/Main im Kino am Eschenheimer Turm. (js)

www.ix-konferenz.de

SAP-Anwender vereinfachen Lizenzmodell

Auf dem Jahreskongress der deutschsprachigen SAP-Anwender (DSAG) gab der Vorstand bekannt, dass es durch intensive Gespräche mit SAP gelungen sei, Bewegung in die Lizenzpolitik der Walldorfer zu bringen. Der Verband sah hier erhebliche Investitionshemmisse, denn kein Unternehmen investiere gern in neue Techniken, wenn es nicht sicher sein könne, die Lizizenzen jemals wieder loszuwerden und nicht aus der Wartung alter Systeme herauszukommen. Nun ist es

möglich, Lizizenzen teilweise stillzulegen. Auch lassen sich Lizizenzen – etwa beim Wechsel von On-Premise-Anwendungen auf Cloud- oder HANA-Varianten – anrechnen.

Vorangekommen sei man auch bei dem leidigen Thema Preisgestaltung, die Kunden als undurchsichtig und verwirrend empfinden. Allein die Preisliste der verschiedenen SAP-Produkte besteht aus 1250 Positionen. DSAG-Mitglieder werden jetzt über Änderungen informiert und es gibt diverse Leit-

Multichannel-VPN-Router für Mobilfunk

Der rheinhessische Routerhersteller Viprinet hat einem mobilen Bündelungsrouter vorgestellt. Der Multichannel VPN Router 510 unterstützt bis zu vier LTE-Verbindungen und DC-HSPA+. Die Daten werden verschlüsselt und mit einer zufallsgesteuerten Verteilung auf die vier WAN-Strecken übertragen.

Für die LAN-Anbindung enthält das Gerät einen GBit-Ethernet-Port sowie einen WLAN-Access-Point (2,4 und 5 GHz). Ein integrierter GPS-Empfänger soll den Router 510 als Arbeitsgerät für Außen Dienst und Transportwesen

prädestinieren. Durch die per Kanalbündelung erzielte hohe Bandbreite und Quality-of-Service-Funktionen soll auch mobiles Video-Streaming möglich sein. Der Listenpreis liegt bei 4990 Euro. (js)



Agil um die Welt

Im Oktober startet zum sechsten Mal die Agile Tour, eine Non-Profit-Veranstaltung zur Förderung der Idee des agilen Programmierens. Aus der 2008 in Frankreich und der Schweiz gestarteten kleinen Konferenzreihe ist mittlerweile eine weltweite Tagungsserie in über 80 Städten auf allen Kontinenten geworden (siehe „Alle Links“).

In Deutschland gastiert die Tour am 16. Oktober in Stuttgart (www.agiletour.de), die Teilnahmegebühr beträgt 72 Euro. (js)

Rechnerdaten von Aagon

Mit NETInfo 4 von Aagon können Administratoren relevante Rechnerdaten automatisch zusammenstellen lassen. Die vierte Ausgabe liefert zusätzlich Informationen zu Netzwerkadapters, IPv4- und -v6-Adressen, Standardgateways, DNS- und WINS-Ser-

vern, Subnetzmasken sowie MAC-Adressen. Da man das Tool nicht extra installieren muss, können es auch wenig technikaffine Mitarbeiter bedienen und die Informationen direkt ans Helpdesk weitergeben. Die Software steht kostenfrei zum Download bereit. (fo)

Kurz notiert



Team-App: Textverarbeitung auf dem Tablet und kollaboratives Arbeiten bietet Quip. Die App ist für iOS und Android erhältlich und für private Nutzer kostenlos. Eine erweiterte Version für Unternehmen kostet 12 US-Dollar pro Monat.

Quark XPress 10 Cocoa-basiert: Die Publishing-Soft-

ware ist in Version 10 mit einer neuen Grafik-Engine ausgestattet, die auch für Retina-Bildschirme ausgelegt ist, und kommt dank Cocoa-Basis ohne Carbon-Bibliotheken aus.

OpenZFS: Verschiedene Projekte und Personen, die am 128-Bit-Dateisystem ZFS beteiligt sind, haben sich zum Projekt OpenZFS zusammengeschlossen. Details sind auf open-zfs.org zu finden.

iX-Umfrage: Kaum Lehren aus der NSA-Affäre gezogen

Um den Einfluss der NSA-Affäre auf die Einschätzungen in Sachen Cloud-Computing abzuschätzen, wurde eine im Februar 2013 auf www.ix.de gelaufene Umfrage wiederholt. Die Frage und die Antworten zeigt die Tabelle.

Quintessenz: Die Unterschiede liegen größtenteils kaum

über der Fehlertoleranz. In den meisten Firmen haben die Verantwortlichen also keine Konsequenzen aus den Snowden-Veröffentlichungen gezogen.

Mit Erscheinen dieser iX-Ausgabe startet eine neue Umfrage, und zwar zum Thema Fachkräftemangel. (js)

Werden in Ihrer Firma externe Cloud-Dienste für Geschäftsdaten genutzt?

	Februar 2013	August/September 2013
Ja, ohne Einschränkungen.	12 %	10 %
Ja, aber nur wenn die Daten Deutschland nicht verlassen.	8 %	7 %
Ja, aber nur wenn die Daten die EU nicht verlassen.	5 %	4 %
Nein, das ist durch firmeninterne Richtlinien generell untersagt.	73 %	77 %

Steigende Budgets für Qualitätssicherung

Die Ausgaben für die Qualitätssicherung belaufen sich auf mittlerweile 23 Prozent der weltweiten IT-Budgets. Der durchschnittliche Anteil ist damit 5 Prozent höher als noch im Vorjahr. Das geht aus dem zum fünften Mal von Capgemini/Sogeti und HP durchgeführten World Quality Report hervor, für den weltweit 1500 IT- und Projektverantwortliche befragt wurden.

Viele Unternehmen verfolgen bei der Qualitätssicherung offenbar einen zunehmend zentralisierten und wirtschaftlichen Ansatz. Waren es im Vorjahr noch 8 Prozent, hätte nun mehr als ein Viertel der Befragten ihre QS-Abteilungen unternehmensweit über Projekte und Sparten hinweg ausgebaut. Fast ein Fünftel der

Studienteilnehmer gab zudem an, ein Testing Center of Excellence (TCOE) eingerichtet zu haben – vergangenes Jahr waren es noch 6 Prozent.

Derzeit investieren deutsche Unternehmen 22 Prozent ihrer IT-Budgets in die Qualitätssicherung, das sind 2 Prozent mehr als 2012. Bei Outsourcing und Testing-Services sind sie anscheinend überdurchschnittlich vorsichtig: Die Hälfte aller Testprojekte werde in Deutschland „in-house“ durchgeführt. Im Vergleich dazu sind es weltweit durchschnittlich 41 Prozent. Nur ein Prozent der deutschen Teilnehmer gab an, dass sie ihr Testzentrum komplett von einem externen Dienstleister betreiben lassen – weltweit sind es in der Studie 9 Prozent. (ane)

Neue Konferenz JavaLand 2014

Am 25. und 26. März 2014 findet zum ersten Mal die JavaLand-Konferenz statt. Sie wird von der DOAG, der Deutschen Oracle-Anwendergruppe, gemeinsam mit dem Heise Zeitschriften Verlag präsentiert und richtet sich sowohl an Java-Einsteiger als auch an Java-Experten. Im Vergleich zu anderen Java-Konferenzen steht hinter JavaLand ein stark von der Community getriebenes Konzept. Deswegen sind die im iJUG e.V. vertretenen Java User Groups eingeladen, die Konferenz mitzustalten.



Ungewöhnlich ist auch der Veranstaltungsort: Der Vergnügungspark Phantasialand in Brühl (in der Nähe von Köln) steht der Java-Community an beiden Tagen exklusiv zur Verfügung. Für zwei Tage sollen die Teilnehmer also in ihrem eigenen Java-Land „leben“ können. Darüber hinaus sind etliche Community-Aktivitäten geplant, die über die „Features“ des Konferenzorts hinausgehen. Noch bis zum 15. Oktober können sich Java-Experten mit einem Vortrag für die Veranstaltung bewerben. (ane)

Neu auf heise Developer

Der von iX betreute Online-Channel hatte schon im August begonnen, zunehmend wichtiger werdende JavaScript-Frameworks vorzustellen. Auf einen Artikel zu Knockout.js folgen nun weitere zu Meteor, Backbone.js und AngularJS. Ein anderer Themenkomplex behandelt das Thema Softwarequalität. So finden Besucher der Website je einen Artikel zur Testautomatisierung und zum Analysewerkzeug SonarQube. Aufmerksamkeit finden darüber hinaus eine Be-

leuchtung des Buchmarkts zu iOS und Objective-C sowie ein Konferenzbericht zur YAPC 2013. Ein Artikel zur Projektmanagementmethode PRINCE2 soll helfen, dass IT-Projekte von Anfang an unter Kontrolle bleiben und sich keine desaströsen Erfahrungen wie bei der Elphilharmonie einstellen. Zu guter Letzt noch der Hinweis, dass man sich nur noch bis 30. September für die Konferenz Continuous Lifecycle 2013 zum Frühbucherprix registrieren kann. (ane)

Kurz notiert

App-Entwicklung: Mit RAD Studio XE5 lassen sich nun auch Apps für Android schreiben. Das Unternehmen sieht sich jetzt als derzeit einzigen Softwarehersteller, mit dessen IDE sich native, von der CPU ausführbare Apps für Android, iOS, Windows und Mac OS X mit derselben C++- oder Delphi-Codebasis entwickeln lassen.

Smart Home: Der Eclipse Foundation liegt mit Eclipse Smart Home ein neuer Projektvorschlag aus dem Umfeld der Heimautomatisierung vor. Hinter ihm stecken die Betreiber des in Java geschriebenen Open-Source-Projekts openHAB (open Home Automation Bus), das das Fernsteuern des elek-

tronischen oder computerisierten Inventars in den eigenen vier Wänden vereinfachen will. Wie openHAB soll Eclipse Smart Home mit einer Integrations-technik die Grundlage schaffen, über sogenannte Bindings unterschiedliche Systeme und Protokolle zentral anzusprechen. Die Finalisierung zum Eclipse-Projekt soll Ende 2013 erfolgen.

Java: Oracle hat planmäßig Java 7u40 veröffentlicht. Das als Feature-Release vorgesehene Update enthält mit Java Mission Control ein Werkzeug zur Überwachung und zum Profiling der JVM sowie Sicherheitsfunktionen wie die sogenannten Deployment Rule Sets, die Java-Anwendungen im Browser besser administrierbar machen sollen.

Neue IDE für Haskell

Das Softwareunternehmen FP Complete hat eine kommerzielle IDE und einen Applicationserver für die funktionale Programmiersprache Haskell veröffentlicht. Die beiden Komponenten, die zusammen das Haskell Center ergeben, sollen die ersten Versuche mit der Sprache erleichtern, da Entwickler so nicht den üblichen Prozess aus Installation, Suche nach Bibliotheken und Ähnlichem durchlaufen müssen. Stattdessen stellt das neue Angebot nach dem Log-in in einem Webbrowser laufende Entwicklungsumgebung bereit, die alle notwendigen Komponen-

ten umfassen soll und darüber hinaus an eine Cloud zum Deployment angebunden ist.

Lizenzen für die IDE sind in drei unterschiedlichen Ausführungen (Community, Standard oder Premium Support) zu haben, die pro Monat oder Jahr zu bezahlen sind (für Einzellizenzen ab 75 US-Dollar pro Monat). Preise für die auf EC2-Instanzen laufenden Applicationserver richten sich nach gewünschter Größe und Support (100 bis 1250 US-Dollar). Eine kostenlose Instanz zum Testen der entwickelten Anwendungen ist jedoch Teil jedes Accounts. (jul)

Hadoop 2.x erreicht Beta-Status

Der 2.x-Release-Strang des unter dem Dach der Apache Software Foundation entwickelten Big-Data-Frameworks hat den Sprung zur Beta geschafft. Das bedeutet offenbar, dass auf dem Weg hin zu einer fertigen Version der nächsten Hadoop-Generation innerhalb der nächsten Wochen nur noch kleinere Fehler zu beseitigen sind. Diese soll dann als Hadoop 2.2.0 über die Ziellinie gehen.

Hadoop 2.x entsteht vor dem Hintergrund, dass sich die Anforderungen und Erwartungen an Flexibilität und Ver-

fügbarkeit bei den Anwendern gegenüber dem Zeitraum der Entstehung des Frameworks 2005 massiv verändert haben. Die kommende Generation des Big-Data-Frameworks enthält deswegen die neue MapReduce-Implementierung YARN (Yet Another Resource Negotiator). Die neue Flexibilität besteht darin, dass sie keine reine MapReduce-Ablaufumgebung mehr ist, sondern andere, verteilte und nicht verteilte Programme demnach im Hadoop-Cluster genauso willkommen sind. (ane)

Neuvorstellungen auf dem EMC-Forum 2013

Im August lud EMC Kunden, Partner und Analysten nach Frankfurt a.M. zur Hausmesse EMC Forum ein. Der Hersteller nutzte die Gelegenheit zu Produktvorstellungen und Ankündigungen.

Runderneut hat EMC die Mid-range-Speicherplattform VNX. Den sechs Hybrid-Modellen steht nun ein reines Flash-System VNX-F zur Seite. Bei allen hat EMC die Architektur für den Einsatz von Flash-Speicher optimiert. Alle unterstützen den block-, file- und objektbasierten Zugriff in beliebiger Mischung. Den Flash-Cache-Bedarf reduzierte EMC durch Deduplizie-

lung. Die Technik MCx soll garantieren, dass die Kerne der Intel-CPUs gleichmäßig ausgelastet sind. Die Preise beginnen bei 30 000 Dollar, die meisten Systeme sind sofort verfügbar.

In Frankfurt erläuterte EMC auch die Rolle der Neugründung Pivotal: Das Unternehmen wird neben VMware und EMC selbstständig agieren und will im vierten Quartal die Cloud-Plattform „Pivotal One“ auf den Markt bringen. Dahinter verbirgt sich eine komplett Umgebung für die Entwicklung, Verwaltung und integrierte Analyse von Daten aller Art ähnlich den Amazon Web Services. Ihre Hauptbestandteile

sind die Module Cloud Fabric, Data Fabric, Application Fabric und die Expert Services. Die Module setzen sich größtenteils aus Open-Source-Software zusammen. Zu ihr gehören die PaaS-Software Cloud Foundry, der Tomcat Application Server samt Webserver, RabbitMQ, das Java-Framework Spring, Redis, Grails, Groovy und die MADlib. Für die Datenanalyse im großen Stil, genannt Big Data, sieht Pivotal unter anderem vor: die kommerzielle Apache-Hadoop-Distribution HD, die Datenintegrations-Appliance DCA, das Social Network Portal Chorus, SQLFire, Analytics- und Monitoring-

Software sowie die Produkte der EMC-Akquisitionen Greenplum und GemFire.

EMC-Geschäftsführerin Sabine Bendick präsentierte die Ergebnisse der jährlichen Anwenderumfrage, an welcher rund 300 Personen teilnahmen. Demnach sind 41 % der Befragten der Meinung, Big Data werde für Sicherheitsapplikationen eine wichtige Rolle spielen. 35 % glauben, dass Big Data über Gewinner und Verlierer in ihren Branchen entscheiden wird. Gleichzeitig sehen 48 % für sich keinen Nutzen in der Technik und 30 % nicht einmal einen Anwendungsfall.

Ariane Rüdiger (sun)

Seagates NAS mit Cloud und Apps

Für kleine und mittlere Unternehmen hat Seagate seine NAS-Linie „Business Storage“ um zwei Rackmount-Modelle erweitert. In die 1-U-Systeme passen vier oder acht Festplatten, allerdings werden die von oben eingebaut (siehe Abbildung). Mit den von Seagate vorgesehenen Constellation ES.3 erreichen sie eine Kapazität von 4 bis 32 TByte. Passend dazu hat der Hersteller sein NAS-OS überarbeitet. Dessen Unterstützung konzentriert sich nach wie vor auf Windows- und Mac-Clients.



Dementsprechend unterstützt das neue intuitive, webbasierte Dashboard die aktuellen Versionen von IE, Firefox, Safari und Chrome.

Darüber hinaus hat der Festplatten-Spezialist eine Anbindung an den Cloud-Speicherdienst Wuala integriert. Den hatte sich Seagate mit der Übernahme des NAS-Spezialisten LaCie im Frühjahr 2012 einverlebt. Daneben liefert Seagate eine Reihe unternehmensorientierte Apps für Windows, Mac OS X, iOS und Android, mit denen Mitarbeiter von unterwegs einen sicheren Zugriff auf Dateien bekommen. Die kostenlosen Wuala-Apps synchronisieren Dateien automatisch und ermöglichen den Zugriff über iPhone, iPad und Android-Geräte. Laut Seagate speichern und übertragen die NAS-Systeme alle Dateien nur verschlüsselt. Preise sind noch nicht offiziell bekannt. (sun)

ZFS-basiertes Unified-Storage

Infortrend erweitert seine Unified-Storage-Familie EonNAS um die Modelle 3012T und 3016RT. Ersteres – ein Update des Modells 3510 – kann zusätzlich zu den 12 internen Platten oder SSDs 108 externe angeschlossene verwalten, mit FC-I/O-Modul erweitert werden und besitzt die üblichen Fähigkeiten der 3000er-Serie: ZFS, die gängigen RAID-Level von 0 bis 60, Snapshots,

WORM, 10-GE-Ports für NAS- und iSCSI-Zugriffe. Sie kooperieren mit LDAP, AD, vSphere, XenServer, Hyper-V.

Das Modell 3016RT arbeitet darüber hinaus mit zwei Controllern, unterstützt bis zu 240 4 TByte große Festplatten, einen Global Namespace, unbegrenzte Snapshots, Remote-Replikation und einen Pool Mirror – beide verschlüsselt – sowie SSD-Caching. (sun)

Backup für virtuelle KMU-Umgebungen

Acronis aktualisiert seine Backup-Software vmProtect 9 für VMwares vSphere-Umgebungen in kleineren und mittleren Unternehmen auf den Markt. vmProtect sichert auf Ebene des Hypervisors, der VMs oder der Anwendungen. Die Version unterstützt Microsoft SQL Server, SharePoint und Active Directory. Über die Weboberfläche lassen sich bis zu 100 VMs für die Sicherung konfigurieren. vmProtect erkennt die üblichen Dateisysteme, über-

springt unnötige Dateien und erstellt mit vmFlashBack virtuelle Maschinen inkrementell. Zudem kann die Software VMs direkt aus einem komprimierten und deduplizierten Image heraus ausführen. Multi-Destination-Backups können die Sicherungen automatisch an mehrere Orte kopieren. Durch die vollständige Integration ins VMwares vCenter lässt sich das Sichern, Wiederherstellen und Replizieren direkt von dort aus verwalten. (sun)

8 TByte auf einem RZ-Band

Mit dem StorageTek T10000D hat Oracle die vierte Generation des RZ-Bandlaufwerks T10000 vorgestellt. Die Kapazität ist auf nativ 8 TByte respektive 8,5 TByte mit eingeschalteter „Maximum Capacity“ gestiegen. Zudem existiert eine 1,6 TByte fassende Sport Cartridge. Den Durchsatz gibt Oracle mit 252 MByte/s ohne Kompression

an. Die Laufwerke lassen sich sowohl über 16-GBit-FC als auch über 10-GBit-FCoE anbinden. Wie bereits sein Vorgänger T1000C beherrscht es das von IBM entwickelte und in die LTO-Standard integrierte Tape-Dateisystem LTFS. Oracle stellt die Treiber als StorageTek LTFS Open Edition und Library Edition bereit. (sun)

Kurz notiert



Eingenommen: Cisco will den All-Flash-Array-Bauer Whiptail für 415 Millionen US-Dollar übernehmen.

Verzahnt: Oracle hat seine ZFS Storage Appliance aktualisiert. Die Modelle ZFS Storage ZS3-2

und ZS3-4 der Multiprotokoll-Systeme sind Bestandteil von dessen Unified Computing-Stra tegie, die von der Hardware zur Anwendung reicht.

Sichergestellt: Tandberg Data hat alle Wechselplatten-, NAS- und Tape-Systeme für Veeams aktuelles Backup & Replication v7 zertifizieren lassen.

Linux-Kernel: Mehr hauptberufliche Entwickler

In der inzwischen fünften Neuauflage der Studie „Linux Kernel Development – How Fast It is Going, Who is Doing It, What They are Doing and Who is Sponsoring It“ haben Jonathan Corbet (LWN.net) sowie die bei der Linux Foundation angestellten Greg Kroah-Hartman und Amanda McPherson die Beiträge zur Kernel-Entwicklung untersucht. Sie konzentrierten sich bei ihrer jetzt auf der amerikanischen LinuxCon in New Orleans vorgestellten Statistik vor allem auf die Kernel-Versionen zwischen 3.3 und 3.10.

Schon in der letzten Auflage im April 2012 war der Trend zu mehr fest angestellten Kernel-Entwicklern aufgefallen. Dieser hat sich auch 2013 weiter gefestigt. Somit sank im Umkehrschluss der Anteil der ungebundenen Patch-Lieferanten von 14,6 Prozent im Jahr 2012 auf nun 13,6 Prozent. Wer sich als Kernel-Entwickler qualifiziert und etabliert habe, müsse sich wohl nicht um eine Anstellung sorgen, schließen Corbet und seine Mitstreiter daraus.

Beim Gesamtanteil an der inzwischen fast 17 Millionen Codezeilen umfassenden Kernel-Entwicklung führen Red Hat mit 10,2 Prozent und Intel mit 8,8 Prozent das Feld der zuliefernden Firmen an. Die Top Ten in dieser Kategorie, zu denen auch Google, IBM und SUSE gehören, verantworten gut 42 Prozent aller Patches. Starke Zuwächse verzeichnen die Mobil- und Embedded-Bereiche: So lieferten beispielsweise Linaro, Samsung, und

Texas Instruments in der Studie von 2012 4,4 Prozent aller Patches; der Anteil hat sich 2013 auf 11 Prozent erhöht. Die Zahlen zeigen, dass Linux in der Industrie angekommen ist und widerlegen deutlich das immer noch gern verwendete Argument vom Hobbyisten-Betriebssystem.

Fast parallel zur Studie veröffentlichte Linus Torvalds die derzeit aktuelle Kernel-Version 3.11. Als Erinnerung an die zwanzig Jahre zuvor erschienene, als erste von Haus aus TCP/IP-fähige Windows-Version änderte er bei der Freigabe den ursprünglichen Codenamen von „Unicycling Gorilla“ auf „Linux for Workgroups“.

Neben den üblichen Bugfixes bietet Linux 3.11 einer Reihe neuer respektive verbesserter Treiber. Die liefern unter anderem Unterstützung für aktuelle WLAN-Chips, besseres Powermanagement bei Radeon-Grafikkarten oder mehr Farbtiefe bei den in Intel-Prozessoren integrierten Grafikkernen.

In Szenarien, bei denen geringe Netz-Latenzen wichtiger sind als die Prozessorlast, lässt sich bei einigen Treibern das „Low-latency Ethernet Device Polling“ aktivieren. Dabei befragt der Kernel das Netz-Device öfter als normalerweise nach eingegangenen Paketen. Ebenfalls neu ist Zswap, bei dem das Memory-Management des Kernels versucht Arbeitsspeicherinhalte zu komprimieren, bevor es sie in den Swap auslagert. Wie gewohnt findet sich eine ausführliche Vorstellung der Neuerungen bei den Kollegen von Heise open (siehe „Alle Links“). (avr)

Linux-Kernel-Statistik

Version	Dateien	Code-Zeilen	Patches	Entwickler	Firmen
3.0	36 788	14 651 135	9153	1131	191
3.1	37 095	14 776 002	8693	1168	189
3.2	37 626	15 004 006	11 780	1316	231
3.3	38 091	15 171 607	10 550	1247	233
3.4	38 573	15 389 393	10 889	1286	245
3.5	39 101	15 601 911	10 957	1195	242
3.6	39 738	15 873 569	10 247	1224	298
3.7	40 912	16 197 233	11 990	1280	228
3.8	41 532	16 422 416	12 394	1258	241
3.9	42 435	16 692 421	11 910	1388	263
3.10	43 029	16 961 031	13 367	1392	243

Quelle: Linux Foundation

Kurz notiert



Abschied: Mit der jetzt freigegebenen ersten Alpha-Release des kommenden FreeBSD 10 haben die Entwickler den GCC-Abschied eingeleitet. Zukünftig will das Projekt LLVM/Clang als Standard-Compiler einsetzen.

Austauschplattform: Das Linux Professional Institut LPI Central Europe (LPI CE) lädt am 17. Oktober zu seiner jährlichen Partnertagung nach München ein. Die bietet mit einem ganztägigen Vortragsprogramm Partnern und Teilnehmern, sich aus-

erster Hand über das LPI und dessen Linux-Zertifizierungen zu informieren.

Zuwachs: Die Open Source Business Alliance (OSBA) – 2001 als Nachfolgeorganisation von Linux-Verband und Linux Solutions Group gegründet – ist auf Wachstumskurs. Allein in diesem Jahr konnte man 20 neue Mitglieder begrüßen, darunter neben den bekannten Open-Source-Dienstleistern Heinlein Support oder SerNet auch Anbieter wie teuto.net, Thomas Krenn sowie kürzlich Branchenprimus Deutsche Telekom.

Juniper goes Open Source

Ende 2012 hatte Juniper das Start-up Contrail Systems gekauft, ein Anbieter von Programmen für Software Defined Networking (SDN). Im Mai hatte man den Betatest für den daraus entstandenen Junos V Contrail Controller gestartet. Den Code hat der Netzwerkspzialist jetzt in das SDN-Projekt OpenContrail eingebracht und ihn unter einer Apache-2.0-Lizenz freigegeben.

Man halte nichts von einem Open-Core-Modell, der Code sei identisch mit dem der kommerziellen Version heißt es bei Juniper. Die Software ist überwiegend in C++ geschrieben. Lediglich für die Schnittstellen haben die Entwickler zu Python gegriffen. Durch die Lizenzierung hofft Juniper auf eine schnelle Anbindung an freie Cloud-Software wie Cloud-Stack und OpenStack. (avr)

GNU feiert 30. Geburtstag

Am 27. September 1983 kündigte Richard Stallman im Usenet den Beginn des GNU-Projekts (GNU – Gnu's Not Unix) zum Bauen einer komplett freien Unix-Alternative an. Zwei Jahre später folgte die Gründung der Free Software Foundation, um dem Projekt eine Körperschaft zur Seite zu stellen. Bis auf den Betriebssys-



temkern – Hurd, der GNU-eigene Kernel ist nach wie vor nicht praxistauglich – kann die FSF Vollzug melden: Auf der Webseite finden sich Links zu GNU/Linux-Distributionen, die die strengen Kriterien erfüllen (siehe „Alle Links“). Klassische Linux-Distributionen finden sich allerdings nicht darunter. (avr)

Mehr Power für Linux on Power

Vierzehn Jahre nach der ersten Ankündigung, eine Milliarde in Linux investieren zu wollen, hat IBM auf der amerikanischen LinuxCon 2013 noch einmal die gleiche Summe zugesagt. Big Blue wollte erneut eine Milliarde US-Dollar in Linux- und Open-Source-Techniken für die hauseigene Power-Serverarchitektur stecken. Kern der Investition wird zum einen ein neues europäisches Power-Systems-

Linux-Zentrum in Montpellier sein. Ähnliche Einrichtungen betreibt IBM in Peking, Austin und New York. Der zweite Baustein ist der Ausbau der Linux on Power Development Cloud, eine Umgebung die ISVs und Open-Source-Entwickler zum Testen ihrer für Power-basierte – einschließlich aktueller POWER7-Syste me – Server kostenlos nutzen können. (avr)

CRYENGINE immer auf dem neuesten Stand

Die Frankfurter Crytek GmbH verzichtet zukünftig darauf, ihre Game Engine mit Versionsnummern auszuzeichnen. Kommerzielle Lizenznehmer der CRYENGINE sollen vielmehr von jetzt an kontinuierlich Zugang zu den aktuellen Entwicklungen der Software haben und nicht mehr auf die nächste Release warten müssen, um neue Funktionen nutzen zu können. Die Game Engine unterstützt die Spieleanthropologie.

für den PC sowie für Konsolen der aktuellen und nächsten Generation (Xbox One, PlayStation 4 und Wii U).

Für die nichtgewerbliche Nutzung bietet der Hersteller seit zwei Jahren zusätzlich ein kostenloses Software Development Kit an. Dieses CRYENGINE SDK hat jetzt ein Update erfahren, das unter anderem einige Beschränkungen bei der Offline-Arbeit aufheben soll. (ka)

Unity mit Cloud und 2D-Werkzeugen

Unity Technologies will Nutzern seiner Game Engine Unity eine Suite von Online-Diensten anbieten, die sie beim Vermarkten von Spielen für mobile Plattformen unterstützen sollen. Dazu zählen Tools für die Analyse des Spielerverhaltens, für das Marketing sowie das Generieren von Umsätzen (Monetarisierung). Für die Nutzung der Unity Cloud, die momentan im Beta-Stadium ist, können Anwender ihren bisherigen Developer Network Account nutzen. Eine native SDK-Integration ist nicht erforderlich.

Darüber hinaus hat die dänische Softwareschmiede bekannt gegeben, dass sie die Version 4.3 der 3D Game Engine, die im Herbst auf den Markt kommen soll, mit neuen Werkzeugen für 2D-Spiele ausliefern will.

Außer den speziell für das Manipulieren zweidimensionaler Szenen konzipierten Tools will der Hersteller für eine bessere Performance und stabilere Simulation die unter der freien zlib-Lizenz stehende Box2D Physics Engine in Unity integrieren. (ka)

MPEG-3D-Audio-Standard kommt

Ein neuer MPEG-Standard soll die effiziente und flexible Übertragung und Wiedergabe von 3D-Audiosignalen gewährleisten. Dafür hat die MPEG-Standardsisierungsorganisation vorab mit kanal-/objekt- sowie szenenbasiertem 3D-Audio zwei Kategorien für deren Codierung und Wiedergabe definiert. Alle Wiedergabesysteme, die 3D-Sound unterstützen, sollen von dem Standard profitieren – vom 3D-Heimkinosystem bis hin zu Tablets und Smartphones.

Durchsetzen konnte sich in umfanglichen Tests gegen diverse internationale Vorschläge der Entwurf des Fraunhofer IIS. Dieser nutzt einen Audio-Codec, der auf dem Extended HE-AAC Codec aufbaut, und kombiniert die kanal-/objektbasierte Technik mit einem 3D-Rendering-Algorithmus.

Im endgültigen Standard, der für das Frühjahr 2015 geplant ist, wollen die Entwickler beide Techniken zusammenführen. (ka)

JavaScript: Ember.js 1.0 stabil für Produktion

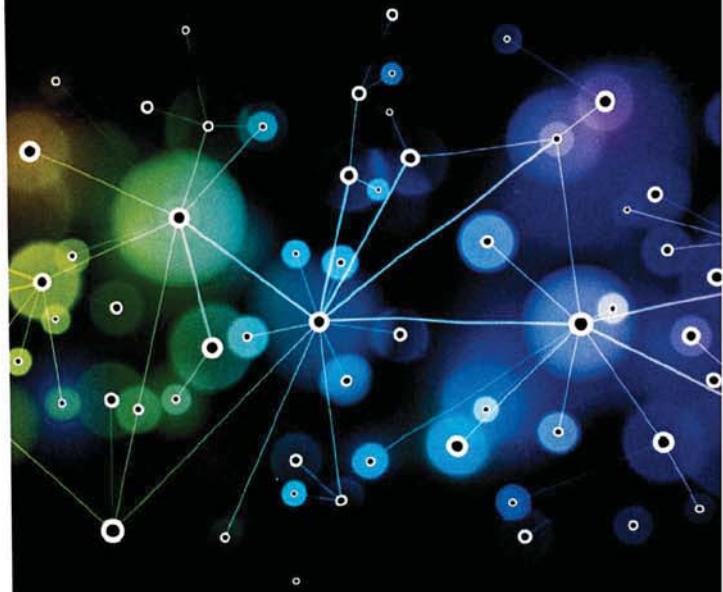
Das das MVC-Paradigma (Model View Controller) umsetzende JavaScript-Framework Ember.js haben dessen Entwickler jetzt in der Version 1.0 veröffentlicht. Es war als eigenständige Weiterentwicklung der von Facebook übernommenen Widget-Bibliothek SproutCore entstanden, die Ende 2011 erst in Ember.js und später in Ember.js umbenannt worden war. Hinter

dem Framework steht unter anderem Yehuda Katz, als Entwickler des Ruby-Frameworks Merb bekannt, das in Ruby on Rails 3.0 aufgegangen ist.

Zu den bekannteren Unternehmen, die Ember.js einsetzen, zählen Groupon, LivingSocial und Square. Ember.js konkurriert mit anderen JavaScript-Frameworks wie Angular.js und Backbone.js. (ane)

MailStore Cloud Edition E-MAIL-ARCHIVIERUNG FÜR PROVIDER

Erweitern Sie Ihr Portfolio und bieten Sie Ihren Kunden alle Vorteile moderner E-Mail-Archivierung as-a-Service. Bereits heute vertrauen über 15.000 Unternehmen auf MailStore.



Softwarelösung für Ihre eigene oder gemietete Server-Infrastruktur



Unterstützt nahezu alle E-Mail-Systeme und Archivierungsmethoden



Bietet umfangreiche Branding- und Scripting-Optionen zur Anpassung an Ihre spezifischen Anforderungen



www.mailstore.co

Performante Next-Generation-Firewalls

Fünf Modelle der neuen TippingPoint Next Generation Firewall stellte HP anlässlich seiner Hausmesse vor. Der Datendurchsatz der Geräte reicht von 500 MBit/s beim kleinsten bis zehn GBit/s beim größten Modell, die Anzahl der gleichzeitig möglichen Verbindungen von 250 000 bis 20 Millionen. Die größten Geräte sind für den Einsatz in Rechenzentren geeignet. Ihre In-

formationen zum Erkennen und Abwehren bekannter und unbekannter Bedrohungen erhalten die Firewalls aus den hauseigenen Labs, der Zero Day Initiative sowie dem HP TippingPoint Reputation Service. Außerdem stellte HP neue Sicherheitsfeatures für das BIOS seiner PCs, Managed Security Services sowie zahlreiche weitere Sicherheitsprodukte vor. (ur)



Datenübermittlung in Drittstaaten

Mitte September veröffentlichte der Düsseldorfer Kreis, ein Zusammenschluss der Behörden für den Datenschutz im nichtöffentlichen Bereich, einen Beschluss zur Datenübermittlung in Drittstaaten (s. „Alle Links“), also Staaten außerhalb des Europäischen Wirtschaftsraums (EWR). Erforderlich ist ihm zufolge eine zweistufige Prüfung. Stufe 1 erfordert gemäß Bundesdatenschutzgesetz (BDSG) das Vorliegen einer schriftlichen Einwilligung des Betroffenen oder eine Rechtsvorschrift, die die Übermittlung legitimiert. Der Beschluss verweist ausdrücklich darauf, dass dieser datenschutzrechtliche Grundsatz auch dann eingehalten sein muss, wenn eine Auftragsdatenverarbeitung vorliegt. Hintergrund ist, dass eine Auftragsdatenverarbeitung nicht

dazu missbraucht werden darf, die zwingenden Voraussetzungen für eine zulässige Datenverarbeitung zu umgehen.

Stufe 2 besteht darin, zu überprüfen, ob in dem betreffenden Land ein angemessenes Datenschutzniveau gemäß BDSG besteht. Nur wenn beide Stufen ein positives Prüfergebnis zur Folge haben, ist die Datenübermittlung zulässig. Dass diese Entschließung mit dem Verweis auf die Auftragsdatenverarbeitung zum jetzigen Zeitpunkt kommt, ist vermutlich kein Zufall. Ein Indiz für den Zusammenhang mit den Datenweitergaben an die NSA ist die kürzlich erfolgte Verlautbarung der Datenschutzbeauftragten des Bundes und der Länder, keine Datenexporte in die USA mehr zu genehmigen, bis die Details der Datenzugriffe geklärt seien. (ur)

Kurz notiert



App-Siegel: Dass ihre App datenschutzfreudlich und seriös ist, können sich Anbieter nach einem umfangreichen Test durch den TÜV Rheinland bestätigen lassen. Verbraucher finden alle Prüfergebnisse im Detail in der Datenbank www.checkyourapp.de.

Zugriffskontrolle: Protiva Cloud Confirm ist eine Software für Multifaktor-Authentifizierung,

die der Hersteller Gemalto „as a Service“ anbietet. Das Produkt ist für Cloud-Anbieter konzipiert, die ihren Unternehmenskunden die sichere Anmeldung an Diensten per Einmalpasswort sowie Token ermöglichen wollen. Im Hintergrund agiert ein mandantenfähiger Authentifizierungsserver.

Patch-Überwachung: Den Corporate Software Inspector CSI, der sämtliche im Unternehmen installierte Software auf Aktualisierungen inspiert, gibt es seit

Entschlüsselungs-Hardware für SSL

Nach der vor Kurzem erfolgten Übernahme von Netronome stellt Blue Coat nun auf der Basis der damit erworbenen Technologie eine Appliance zur SSL-Entschlüsselung vor. Das transparente Proxy-Gerät für SSL-Kommunikation entschlüsselt in Voll duplex-Netzwerken mit 100 Mbps bis 10 Gbps den SSL-Datenverkehr. Die Appliances sollen zudem in inline über einen Tunnel unabhängige Datenströme an bis zu vier Schnittstellen liefern, so dass verschiedene IT-Sicherheitssysteme für die Analyse angeschlossen werden können. Beispiele sind Intrusion-Prevention- oder -Detection-Systeme, forensische oder Sandboxing-Systeme, die Daten aus Angriffen oder bei Datenlecks analysieren können, doch selbst keine Entschlüsselungsfunktion besitzen. Geplant ist, die Technik vollständig in die Blue-Coat-Produkte zu integrieren. Derzeit wird die Appliance noch über zertifizierte OEM-Partner wie Sourcefire vertrieben. Susanne Franke (ur)

„Apps“ für Schwachstellenanalyse

Die neue Version 4.7 des Werkzeugs für Schwachstellenmanagement „SecurityCenter“ des Herstellers Tenable Network Security bietet etliche Erweiterungen. Zu nennen ist hier vor allem ein Katalog mit Hunderten von Analyse-Applikationen für das schnelle Identifizieren und Beseitigen von Bedrohungen ohne Zuhilfenahme von Drittanbieterprogrammen oder Skripten. Auf diese von Tenable „Security App

Store“ genannte Sammlung kann man direkt über die SecurityCenter-Konsole zugreifen. Zu den weiteren Neuerungen gehören vereinfachte Frameworks für das Erstellen von Dashboards, eine erweiterte Abdeckung mobiler Endgeräte, Remediation Reports, die Unterstützung des SCAP 1.2 (Security Content Automation Protocol) sowie die Möglichkeit zur Anpassung von Risikoregeln an eigene Prioritäten. (ur)

Webschwachstellenscanner für HTML5

Der für mittlere und große Unternehmen konzipierte Web Vulnerability Scanner (WVS) von Acunetix legt in Version 9 einen Schwerpunkt auf dynamische Webanwendungen. Mithilfe seiner Deep-Scan-Technik soll der Scanner HTML5- und JavaScript-Code beispielsweise in Ajax-Anwendungen oder Single Page Applications analysieren. Da der WVS die gleiche Rendering Engine benutzt wie die Smartphone-Browser von

iOS, Android und BlackBerry, kann er mobile Webseiten und Applikationen auf Schwachstellen untersuchen. Der Scanning Wizzard zeigt außerdem an, ob gerade die Hauptseite oder eine mobile Seite gescannt wird. Erneuert beziehungsweise verbessert hat der Hersteller außerdem das Erkennen von Sicherheitslücken für Blind Cross-Site Scripting, DOM-basiertes Cross-Site Scripting, Server Side Request Forgery und weitere. (ur)

Anfang September in Version 7. Neu ist unter anderem ein Nutzermanagement mit verschiedenen Rollen und Rechten, eine Web-Konsole (SaaS) für den Zugriff von überall, die Konfiguration von Passwort-Richtlinien sowie ein Add-on für den Alarm bei Zero-Day-Schwachstellen.

Sichere Webanwendungen: Einen Leitfaden zur sicheren Programmierung von Software und speziell Webanwendungen hat das BSI veröffentlicht („Alle

Links“). Er definiert Anforderungen eines Secure Software Development Lifecycle, beinhaltet aber auch Standards und Guidelines der OWASP und vieles mehr.

Bedrohungsabwehr: Die nach eigenen Aussagen erste Sicherheitsplattform, die in Echtzeit Gefahren abwehrt bringt FireEye auf den Markt. Oculus, so der Name des Produkts, kombiniert dazu Virtual-Machine-Techniken, Big-Data-Analysen sowie 24-Stunden-Service und -Support.

Neue Rechner bringen der Herbst

Im Zuge der IFA überarbeiten mehrere Hersteller ihr Laptop-Portfolio. Klassische Notebooks gibt es von Dell und Toshiba. Aus Texas kommen mit dem Latitude 3000 und 5000 Geräte für den Unternehmenseinsatz, die sich durch umfangreiche Sicherheitsoptionen und ein stabiles Gehäuse hervorheben sollen. Aus Japan stammen hingegen Modelle für das multimediale Vergnügen, die sich eher an das private Büro richten. Beide Hersteller wollen jedoch auch etwas vom Ultrabook-Häppchen abhaben: Allzu viel Variation lässt Intel nicht zu, ein Äußeres aus Aluminium muss als Verkaufsargument herhalten. Fujitsu und Lenovo bemühen den am Laptop ungemein beliebten Touchscreen, um Kunden zum Neukauf zu bewegen. Die Chinesen haben zudem die bisher vereinsamten „mobilen Business-Nomaden und Road Warrior“ als potentielle Zielgruppen entdeckt, die sich anscheinend vor allem für die leichten und kleinen Geräte der ThinkPad-X-Reihe interessieren sollen.

Tablets verkörpern momentan den Massenmarkt im Rechner-Geschäft. Neue Modelle unterscheiden sich vor allem in ihrer Größe und der Auflösung des Touchscreens. Unter den Androiden gehören zum Adel noch immer die 10-Zoll-Gerä-

te, wie sie Acer, Asus und PocketBook präsentierten. Einzig das New Transformer Pad von Asus konnte sich abheben, im Innern verrichtet ein Tegra-4-Chipsatz den Dienst, die geballte Masse der 2560 × 1600 Pixel verweist die meisten Desktop-Bildschirme auf die Reservebank. In der Mittelklasse im 8- und 7-Zoll-Bereich führten unter anderem Asus, Lenovo, Huawei und PocketBook neue Modelle vor. Etwas Bemerkenswertes findet sich in Aipteks Projector Pad P100, in dem ein 100-Lumen-Beamer die Präsentation an die Wand funzelt. Huaweis MediaPad 7 und Asus' Fonepad 7 kann man ebenfalls zum Telefonieren nutzen, die „Phablets“ für besonders breite Hände sollen Tablets und Smartphones in einem kombinieren.

Nutzer, die nicht zwischen Tablet und Laptop wählen wollen, könnten in Berlin verschiedene Ansätze für den Spagat in Augenschein nehmen. HPs Split X2 und Toshibas Satellite W30Dt bestehen aus einem Rechner mit ansteckbarer Tastatur. Lenovo setzt beim Yoga hingegen auf 360-Grad-Scharniere, mit denen man die Tasten auf die Rückseite befördert. Auf allen Hybrid-Modellen läuft Windows 8, während sich die reinen Tablets auf Android einschießen. (fo)



Präsentiert: Aiptek Projector Pad P100 ist mit einem 100-Lumen-Projektor ausgestattet.

Updates legen MS-Office lahm

Mehrere Aktualisierungen des September-Patchdays für Microsofts Office paralysieren die Büroumgebung. Der Fehler tritt unter Vista und Windows 7 auf. Windows Update spielt die Pakete KB2760411, KB2760588 und KB2760583 für die 2007er-Ausgabe zunächst automatisch ein, versucht sie jedoch anschließend immer wieder neu zu installieren. Für Abhilfe sorgt ausschließlich, in

der Systemsteuerung das Verhalten in „Updates herunterladen, aber Installation manuell durchführen“ zu ändern.

Auch Nutzer des aktuellen Office 2013 können sich nicht entspannt zurücklehnen: Der Patch KB2817630 lässt die Ordnerliste in Outlook verschwinden. Die kritische Lücke in der Mail-Vorschau der Vorgängerversion behebt das Update jedoch. (fo)



DIE ERFOLGREICHSTE FRAU DER TELEKOM

Das bin ich.

Als Stabsleiterin der T-Systems-Geschäftsführung Delivery halte ich meinem Chef den Rücken frei. Das ist manchmal hektisch – aber immer spannend. Dabei passe ich auf den ersten Blick gar nicht in ein ICT-Unternehmen – schließlich bin ich Kulturwissenschaftlerin. Bei näherer Betrachtung aber ausgesprochen gut. Weil die Telekom für Vielfalt steht. Ich bringe einen anderen Blickwinkel mit als meine technisch geprägten Kollegen. Wir ergänzen uns, lernen voneinander und entwickeln uns so weiter.

Die Telekom ermöglicht mir „Connected Life & Work“. Ich bin „always on“, schaffe mir so aber auch jede Menge Freiräume. Natürlich zählt die Leistung, aber wo und wann ich meine Arbeit erledige, ist zweitrangig. Diese Flexibilität schätze ich sehr und möchte sie nicht mehr missen.

Für mich passt alles zusammen. Deswegen kann ich sagen: Ich bin die erfolgreichste Frau der Telekom.

Auch Lust auf Erfolg?
Bewerben Sie sich jetzt!
Online oder per App.

www.telekom.com/it-jobs
www.telekom.com/jobapp



Neue Smartphones von Apple: Farbig oder schneller

Wie erwartet, hat Apple Anfang September zwei neue Modelle seines iPhones vorgestellt. Das 5c steckt in einem Plastikgehäuse, das in verschiedenen Farben verfügbar ist. Es kostet

etwas weniger als das gleichzeitig präsentierte 5s. Um das von vielen prophezeite „Billig-iPhone“ handelt es sich jedoch nicht: Die kleinere Variante mit 16 GB Speicher kostet ohne

Vertrag gut 500 € netto, für das Modell mit doppelt soviel RAM muss man 588 € hinblättern. iPhone 5s und 5c unterstützen fünf LTE-Frequenzbänder. Damit lassen sich in Deutschland die schnellen Vodafone- und Telekom-Netze nutzen – wie es mit O2 ausseht, ist noch unklar.

Im 5c baut Apple mit der CPU „A7“ erstmals einen 64-Bit-Prozessor ein, die Kamera ist lichtempfindlicher als beim Vorgänger. Bewegungs- und Ortsdaten verarbeitet ein separater Chip („M7“), was die CPU entlasten und Strom sparen soll. In der kleinsten Ausbauvariante mit 16 GB kostet das iPhone 5c ohne Vertrag gut 603 € netto, die 32-GB-Variante kommt auf 670 €.

Alles so schön bunt – das iPhone 5c soll Apple asiatische Märkte öffnen.

Neben der verbesserten Kamera dürfte der in den Home-Knopf integrierte Fingerabdrucksensor die größte für Benutzer sichtbare Neuerung sein. Damit lässt sich das Smartphone entsperren, außerdem können Kunden so ohne Passwort-Eingabe im iTunes-Store einkaufen. Apple verspricht, die Fingerabdruckdaten bleiben auf dem Smartphone. Dort würden sie aber nicht komplett gespeichert, sondern auf dem Telefon liegen lediglich die charakteristischen Merkmale des Abdrucks besonders geschützt und verschlüsselt. Trotzdem warnte der Hamburger Datenschützer Johannes Caspar vor dem Verwenden der Technik: Biometrische Daten sollten Nutzer nur äußerst sparsam verwenden und nicht für triviale Anwendungen wie das Anmelden bei einem Shop herausrücken. (ck)



Quelle: Apple

Smartwatches auf der Internationalen Funkausstellung

Einige Analysten wittern in der „Wearable IT“ bereits das nächste große Ding: Ein cleverer Begleiter reicht nicht aus, smarte Brillen und vor allem Uhren müssen her. Auf der diesjährigen Internationalen Funkausstellung in Berlin hatten die Messebesucher Gelegenheit, Sonys SmartWatch 2, Samsungs Galaxy Gear sowie Modelle von Sonostar und MyKronoz auszuprobieren.

Alle funktionieren ausschließlich in Zusammenarbeit mit dem Smartphone, die Galaxy Gear lediglich mit Modellen des Herstellers. Per Bluetooth oder NFC verbinden sich die Uhren mit dem Handy, das

Informationen zu E-Mails, Twitter, Wetter und eingehenden Anrufen durchreicht. Man kann die Geräte per Touchscreen steuern, das Samsung-Modell unterstützt ebenfalls das hauseigene S Voice. Es enthält zudem als einziges eine Kamera. Das Sony-Gerät zeigt hingegen konstant die Uhrzeit an, sogar wenn das Mobiltelefon mal nicht gekoppelt ist.

Aus Taiwan stammt das Modell Sonostar des gleichnamigen Produzenten. Anders als Sony und Samsung setzt er auf ein E-Ink-Display. Das wirkt sich vor allem auf den Stromverbrauch aus – statt den Chronometer täglich ans Ladegerät

hängen zu müssen, hält das Modell bis zu sieben Tage durch. Ebenfalls einzigartig ist die integrierte Golfkurs-Datenbank.

Etwas mehr Erfahrung beim Bauen von Zeitmessern gibt es in der Schweiz, dem Heimatland von MyKronoz. Die Firma hatte gleich drei Geräte mitgebracht: ZeWatch und ZeBracelet verfrachten die Freisprech-anlage ans Handgelenk und unterscheiden sich im Design, mit der ZeNano kann man zudem Gespräche initiieren.

Aufgrund des variierenden Funktionsumfangs schwanken die Preise deutlich: MyKronoz verlangt für die beiden simp-

leren Modelle 69 €, für das größere 129 €. Sonostar visiert 170 € an, Sony 199 €. Mit 299 € nimmt Samsung den Spitzenplatz ein.

So ganz neu ist das Konzept hingegen nicht. Der PDA-Hersteller Palm kooperierte zum Beispiel 2003 mit Fossil; das Gerät verlagerte den gesamten Assistenten an das Handgelenk und kostete 250 US-Dollar – umso erstaunlicher, dass die jetzt vorgestellten Modelle gerade einmal die Grundfunktionen eines Zeitmessers bieten. Obwohl Kritiker dem Konzept durchaus wohlwollende Worte spendierten, blieb der Erfolg bei den Endkunden bisher aus. (fo)

BlackBerry will sich verkaufen

Mit neuem Betriebssystem und neuen Geräten hat der angeschlagene kanadische Smartphone-Hersteller BlackBerry bisher noch nicht die erhoffte Wende geschafft. Jetzt stellt sich das Unternehmen zum Verkauf, berichtete das Wall Street Journal. Als Interessenten nannte es nordamerikanische Investmentgesellschaften, darunter Brain Capital und das Canada Pension Plan Investment Board. Auch asiatische

IT-Firmen wie Lenovo sollen Interesse an BlackBerry geäußert haben.

Zuvor hatte es Gerüchte gegeben, die Firma wolle ihren erfolgreichen BlackBerry Messenger (BBM) in eine eigene Firma ausgliedern. Der Dienst ermöglicht den direkten, verschlüsselten Austausch von Nachrichten über das Internet. BlackBerry hatte im Mai 2013 iOS- und Android-Clients dafür angekündigt. (ck)

NoSQL: Couchbase für Mobilgeräte

Neben einer klassischen Desktop-Version stellt Couchbase eine mobile Variante seiner dokumentenorientierten NoSQL-Datenbank bereit (s. „Alle Links“). Couchbase lite ist noch im Beta-Stadium und liegt für iOS sowie Android vor. Außerdem gibt es ein Plug-in für das Framework PhoneGap. Zum Programmieren der Datenbank stehen jeweils native iOS- und Android-APIs zur Verfügung. (ck)

Zwei weitere Produkte sollen die mobile Datenbank ergänzen: in der Cloud laufende Couchbase-Server sowie ein Synchronisierungs-Gateway, das die mobilen Datenbanken und die in der Cloud auf demselben Stand hält. Es steht für Linux (Ubuntu und Red Hat) sowie Mac OS X zur Verfügung. Jedes Gateway kann die Synchronisierung mit mehreren Couchbase-Servern und -Datenbanken übernehmen. (ck)

Informatica Feminale: Genderspezifische Fragen und Nachhaltigkeit in der IT

Lasst sie programmieren

Patricia Jung



Bereits zum 16. Mal fand die Informatica Feminal in Bremen statt. Und noch immer bieten Fragen zur Gleichstellung von Mann und Frau im Berufsleben reichlich Diskussionsstoff.

Kann die IT-Wirtschaft auf weibliche Fachkräfte verzichten? Einerseits gelten Vielfalt und daraus resultierende unterschiedliche Sichtweisen in IT-Teams zunehmend als gewünscht, weil sie helfen, den Tunnelblick zu vermeiden. Andererseits schließt die vorherrschende Arbeitswelt mit durchgängiger Büropräsenz und Meetings zu Kindergarten-abholzeiten Mütter und auf Gleichbelastung in der Familienarbeit achtende Väter noch immer weitgehend aus.

Virtuelle Arbeitsformen in der Schweiz

So lag es nahe, dass das Rahmenprogramm des Sommerstudiums für Frauen in der Informatik vom 26. August bis 6. September mehrfach das

Thema „Gender Balance“ aufgriff: Dr. Nadja Ramsauer und Thea Weiss Sampietro von der Zürcher Hochschule für Angewandte Wissenschaften berichteten im Eröffnungsvortrag über ein noch bis Oktober laufendes Projekt, das sich mit virtuellen Arbeitsformen in der Schweizer IT-Branche unter genderspezifischen Aspekten beschäftigt. Zeitliche und örtliche Flexibilität – richtig eingesetzt – erleichtert die Vereinbarkeit von Beruf und Familie, stärkt selbstständiges Arbeiten und Motivation.

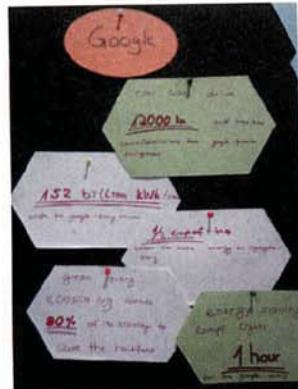
Wie lässt sich aber verhindern, dass der Teamzusammenschnitt schwundet oder das Verschwinden der Grenzen zwischen Berufs- und Privatleben Gesundheit und Wohlbefinden beeinträchtigt? Die im Rahmen des Projekts bei IBM Schweiz erprobten Best Practi-

ses will die Zürcher Hochschule für Angewandte Wissenschaften ZHAW nach Projektabschluss als Handreichung für interessierte IT-Unternehmen publizieren (siehe „Alle Links“). Das halbtägige Jobforum mit seinen Firmenvorträgen und -vorstellungen zeigte denn auch, dass Firmen, die gezielt um technische Mitarbeiterinnen werben, Chancengleichheit, Familienfreundlichkeit und manchmal auch Bio-Frühstück als ausschlaggebend betrachten (Key Selling Points).

Das Sommerstudium selbst bot selbstverständlich wieder Kinderbetreuung während der Lehrveranstaltungen an – vordilicherweise auch, wenn nur ein Kind anwesend war. Und wer den Feuerfeuer sah, mit dem zwei acht- und zwölfjährige Mädchen ihre unter separater Anleitung gebauten und programmierten Lego-Mindstorms-Roboter präsentierten, fragte sich, warum Nachwuchsförderungsinitiativen oft erst einsetzen, wenn die kindliche Begeisterung für technische Themen am Abklingen, wenn nicht bereits sogar erloschen ist.

Klassische Kurse früh ausgebucht

Wieder in Überschreitung mit der Ingenieurinnen-Sommeruni konzipiert, warteten die beiden Sommerstudiengänge mit insgesamt 50 klassischen Lehrveranstaltungen (davon zehn Programmierkurse) auf, von denen viele schon im Mai/Juni ausgebucht waren. Hinzu kamen 25 Exkursionen, Networking-Events und Firmenvor-



Der Kurs „Informatik und Nachhaltigkeit“ war zum zweiten Mal in Folge gut besucht, obwohl oder gerade weil dieses zukunftsrichtige Thema immer noch ein Nischensein fristet.

träge, bei denen sich dieses Jahr nicht nur Firmen, sondern erstmals auch die Bremer Fachbereiche Informatik und Ingenieurwissenschaften vorstellten, darunter das Team des mehrfachen Roboterfußball-Weltmeisters B-Human.

Besonders populär waren die Sommerunis für Bachelorstudentinnen, die über die Hälfte der studentischen Teilnehmerinnen stellten. Mit knapp 190 Anmeldungen (darunter ein knappes Drittel Fachfrauen) blieb die Teilnehmerinnenzahl auf Vorjahresniveau. Gute Aussichten für 2014, wenn Ingenieurinnenuni und Informatica (terminlich wieder eine Woche überlappend) vom 11. bis 29. August stattfinden. (ka)

Alle Links: www.ix.de/x1310027

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: PC-Techniker, Linux-Administrator LPI, Netzwerk-Techniker, Webmaster, Fachkraft Neue Energien

Teststudium ohne Risiko. GRATIS-Infomappe gleich anfordern!

FERN SCHULE WEBER - seit 1959 -
Postfach 21 61 - 26192 Großenkneten - Abt. C98
Telefon 0 44 87 / 263 - Telefax 0 44 87 / 264

www.fern schule-weber.de

DELIVERED!

ge-lie-fert (ugs. für: begeisterte Kunden) | Scrum by borisgloger

Training | Beratung | Zertifizierung
www.borisgloger.com

borisgloger

Bitcoins als Rechnungseinheit anerkannt

Bitcoins sind nach der Auffassung des Bundesfinanzministeriums eine Art „privates Geld“. Juristisch bedeutet dies, dass die digitale Währung als sogenannte „Rechnungseinheit“ rechtlich und steuerlich anerkannt wird. Bereits zuvor hatte das Ministerium klargestellt, dass die durch An- und Verkauf von Bitcoins erzielten Spekulationsgewinne nach einer Haltefrist von einem Jahr steuerfrei sind. Eine Abgeltungssteuer wie bei Aktien- oder Zinsgeschäften wird damit nicht fällig. Bitcoins werfen aber zusätzliche Fragen auf, die noch

nicht abschließend bewertet sind. Insbesondere aus den Vereinigten Staaten kommen Bedenken im Hinblick auf mögliche Geldwäsche mit der digitalen Währung. Zweifelhaft ist es weiterhin, ob der Handel mit Bitcoins der Umsatzsteuer unterliegt. Schließlich sind Fragen des Bankaufsichtsrechts ungeklärt. Müssen mit Bitcoins handelnde Banken eine Genehmigung dafür erhalten oder genügt es, den Handel bei den zuständigen Behörden anzugeben? Erste Banken haben die BAFin angeschrieben, um hier Klarheit zu erhalten. (ur)

Apps versagen im Datenschutztest

19 Datenschutzbehörden haben jüngst in einer konzertierten Aktion des Global Privacy Enforcement Network über 2200 Webseiten und Apps auf ihre Übereinstimmung mit datenschutzrechtlichen Vorgaben überprüft. Insbesondere Apps fielen wegen eklatanter Datenschutzverstöße auf. So habe

man 90 % von ihnen als mangelhaft im Bereich des Schutzes der Privatsphäre der Nutzer eingestuft. Bei den Webseiten beanstanden die Experten nur 50 %, meist wegen der Qualität der Datenschutzerklärungen oder der Erreichbarkeit der Unternehmen im Fall von Datenschutzbeschwerden. (ur)

Verschärzte Regeln gegen Geldwäsche

Die EU-Kommission plant eine Novelle der EU-Geldwäscherechtlinie. Der vorgelegte Entwurf sieht eine Vielzahl von Verschärfungen vor. Kritiker befürchten, dass danach anonyme Bezahldienste nicht mehr angeboten werden dürfen. Der Geschäftsführer des „Prepaid Forum Deutschland“, Hugo Godschalk, mutmaßt, dass in der gesamten EU keine Prepaid-Angebote im E-Commerce mehr eingesetzt werden dürfen.

Dies würde auch zu einem Wegfall der in Deutschland 2011 nach langen Diskussionen eingeführten 100-Euro-Grenze für anonymes E-Geld führen. Dafür hatten sich seinerzeit unter anderem Datenschützer und Anbieter von Prepaid-Zahlungsdiensten stark gemacht. Ähnliche Diskussionen dürften angesichts der geplanten Ausweitung der Identifizierungspflicht für Käufer von Online-Zahlungskarten folgen. (ur)

Kurz notiert



TK-Meldepflicht: Am 25. August ist die EU-Verordnung über die Meldepflicht von TK-Firmen bei Datenschutzverstößen in Kraft getreten. Seither müssen die Unternehmen bei Datenschutzverstößen die jeweiligen zuständigen Behörden informieren. Verstöße werden mit Bußgeldern geahndet.

AGB-Klaus: Wer unerlaubt die allgemeinen Geschäftsbedingungen eines anderen kopiert

und für eigene Zwecke verwendet, ist zum Schadensersatz verpflichtet. Das Amtsgericht Köln (Az. 137 C 568/12) hat einen Rechtsverletzer zur Zahlung von 615 Euro verurteilt.

Behördenauskunft: Seit Einführung einer Meldepflicht bei Datenlecks für Unternehmen im „nichtöffentlichen Bereich“ haben Behörden Hunderte entsprechender Meldungen erhalten. Dabei zeigten sich in einer c't-Recherche die angeschriebenen Behörden unterschiedlich auskunftswillig (s. „Alle Links“).

Erste Urteile wegen Verstößen gegen Buttonlösung

Die 2012 eingeführte sogenannte Buttonlösung sollte Kosten- und Abofallen im Internet wirksam bekämpfen. Der „Verbraucherzentrale Bundesverband“ (vzbv) verweist jetzt auf zwei Urteile, die zeigen, dass in diesem Bereich immer noch einiges im Argen liegt. Es scheint sich dabei um die ersten Urteile zu dieser Gesetzesnovelle zu handeln. Das Landgericht Leipzig (Az. 08 O 3495/12) untersagte einem Onlinenhändler den Vertrieb von Waren an Verbraucher, weil der vorgeschriebene „Kauf-Button“ für die kostenpflichtige Registrierung in den Onlineshop nicht eingebunden war. Ein eher versteckter Hinweis in den AGB des Anbieters, dass sich dieser nur an Unternehmer und nicht an Verbraucher richte, half ihm wegen mangelnder Transparenz nicht.

Ein Urteil des Landgerichts Koblenz beschäftigte sich mit der

Werbung von WEB.DE. Hier erging ein Unterlassungsurteil, weil der Anbieter nicht deutlich genug über Vertragsinhalte wie Laufzeit und Preis aufgeklärt hat. Der vzbv verweist auf 19 weitere Unternehmen, die er in ähnlichen Fällen abgemahnt hat. In acht Fällen ging es um einen fehlenden Bestellbutton, aus dem die Zahlungspflicht deutlich hervorgeht. In einem vergleichbaren Fall bestätigte das Landgericht München I (Az. 33 O 12678/13) die Abmahnung Amazons durch den VerbraucherService Bayern. Es untersagt dem Unternehmen darin, für die kostenpflichtige Prime-Mitgliedschaft durch einen Button mit dem Text „jetzt kostenlos testen“ zu werben. Auch wenn dies für den ersten Monat gilt, muss sich aus der Schaltfläche eindeutig ergeben, dass der Vertrag anschließend kostenpflichtig weiterbestehen soll. (ur)

Kein Personenbezug bei reinen IP-Adressen

Unter Juristen und Datenschützern ist die Frage umstritten, ob dynamische IP-Adressen (mit Zeitstempel) als personenbezogene Daten anzusehen sind. Ist das der Fall, gelten für jede Verarbeitung dieser Daten die Datenschutzgesetze. Bislang haben Gerichte in Deutschland tendenziell eher zugunsten der Datenschützer entschieden und einen Personenbezug angenommen. Jetzt hat das Landgericht Berlin (Az. 57 S 87/08) entschieden, dass dynamische IP-Adressen für sich genommen noch keine personenbezogenen Daten darstellen. Erst wenn weitere Informationen bei der

verarbeitenden Stelle hinzukommen, die einen Betroffenen identifizieren können, ist das Datenschutzrecht anwendbar.

Ausdrücklich zielen die Richter darauf ab, was für die speichernde Stelle konkret machbar ist, und nicht, was theoretisch irgendjemandem möglich wäre. Damit lehnten sie die Ansicht ab, dass über die Log-Files der Internet-Provider – also einer anderen Person als beispielsweise dem Betreiber einer Webseite – eine Identifikation durchführbar sei. Möglicherweise muss sich nun der Bundesgerichtshof mit dieser Thematik beschäftigen. (ur)

Google erweitert Patentlizenzen

Google hat einige Open-Source-Projekte im März 2013 die Nutzung einer Reihe von Patenten gestattet. Jetzt hat der Konzern die Liste dieser Patente, für die die „Open Patent Non-Assertion Pledge“ gilt, auf insgesamt 89 erweitert. Bedeutend ist, dass diese Zusage auch bei einem Verkauf eines der Patente bestehen bleibt. Sie

fällt lediglich weg, wenn der Patentnutzer rechtlich gegen Google vorgehen sollte. Nach Recherchen von heise online umfassen die Patente unter anderem Teile des MapReduce-Algorithmus zum verteilten Rechnen, diverse Verfahren zur Datenübertragung über das Netz, Techniken für Webserver und weitere. (ur)

PostgreSQL verbessert JSON und Sharding

In der jetzt veröffentlichten Version 9.3 der freien SQL-Datenbank PostgreSQL haben die Entwickler die JSON-Unterstützung stark erweitert. Dazu baute Andrew Dunstan den JSON-Parser um und ergänzte ihn um eine Programmierschnittstelle. Dadurch lassen sich Funktionen zum Verarbeiten von JSON einfacher schreiben. So gibt es jetzt etwa `json_agg`, das Datensätze als JSON-Array ausgibt. Die Operatoren `->` und `-->` ermöglichen den Zugriff auf JSON-Objekte innerhalb von PostgreSQL-Feldern. Dunstan hat einen Backport dieser Funktionen als Erweiterung für Version 9.2

veröffentlicht (s. „Alle Links“), die erstmals einen eigenen JSON-Datentyp unterstützte.

Mit den „Foreign Data Wrappers“ (FDW) lassen sich Daten auf entfernten Servern nicht nur lesen, sondern auch ändern – vorausgesetzt, der jeweilige Treiber unterstützt dies. Das gilt bislang nur für externe Redis- und PostgreSQL-Quellen. Der Treiber für die Verbindung zwischen zwei PostgreSQL-Servern soll leistungsfähiger sein als bisher. Abzüge mehrerer Tabellen lassen sich mit `pg_dump` schneller erstellen, wenn man die neue Option `-j njobs` verwendet. (ck)

Mehr SQL bei Google und Cassandra

Ganz so veraltet scheinen SQL und die relationalen Konzepte doch noch nicht zu sein: Google veröffentlichte kürzlich Details zu seiner intern benutzten relationalen Datenbank F1, mit der es einen Datenbestand von 100 TByte für seine AdWords verwaltet. Früher setzte es dafür MySQL ein.

F1 nutzt eine mehrschichtige Architektur auf der Grundlage von Googles Dateisystem BigTable (jetzt Colossus genannt) zum Speichern der eigentlichen Daten. Darüber sitzt „Spanner“, das wesentliche Datenbankfunktionen wie Persistenz, Caching, Transaktionen und Sharding bereitstellt. Die SQL-Abfragen führt der F1-Server aus. Zum parallelen Abarbeiten startet er bei Bedarf Kinder, die jeweils einen Teil der Query abarbeiten. Ein Load Balancer verteilt zuvor die Anfragen der Clients an die ver-

schiedenen F1-Server. Spezielle Vorkehrungen sollen die häufig vorkommenden Master-Detail-Abfragen beschleunigen. Die NoSQL-Technik Map-Reduce lässt sich auch mit F1 nutzen.

Wenig später stellten die Apache-Entwickler Version 2 ihrer NoSQL-Datenbank Cassandra vor. Mit ihren „leichten“ Transaktionen soll sich das Isolation Level „serializable“ traditioneller Datenbanken nachbilden lassen. Auch Trigger ziehen in Cassandra ein, allerdings nur vor der jeweiligen Operation. Die Implementierung der Technik ist noch experimentell und soll sich in Version 2.1 ändern. Cassandras eigene Abfragesprache CQL rüstet auf Protokollebene das stückweise Ausgeben von Ergebnissen nach. Das soll vor Netz- und Speicherüberlastung schützen, wenn sehr große Datenmengen zu übertragen sind. (ck)

Oracle schloss Audit-Lücke heimlich

Einen seit 2011 bekannten Fehler in seiner Audit-Implementierung hat Oracle schon Ende 2012 beseitigt, ohne darauf hinzuweisen. Die Lücke erlaubte es, das Auditing durch den direkten Zugriff auf eine Speicherstelle per `Poke` abzuschalten. Diesen Befehl stellt das nicht dokumentierte Werkzeug `oradebug` zur Verfügung, das Oracle mit allen Versionen seiner Datenbank liefert. Seine Verwendung wird nicht proto-

kolliert, sodass das Abschalten des Audits unbemerkt möglich war. Nun lässt sich der Zugriff mit einem Parameter auf bestimmte `oradebug`-Befehle einschränken.

Auf die Patches wies jetzt der Oracle-Sicherheitsfachmann Alexander Kornbrust in seinem Blog hin (s. „Alle Links“). In den aktuellen Versionen der Reihen 11.2 und 12 der Datenbank ist der Bug ebenfalls behoben. (ck)

JAZOON'13
INTERNATIONAL CONFERENCE FOR THE SOFTWARE COMMUNITY
22 to 23 October 2013
Stage One Zurich Oerlikon

Joe Justice (Wikispeed)
DEVELOPING A 100 MPG CAR USING AGILE METHODS

Heather VanCura (Java Community Process)
JOIN THE JAVA EVOLUTION; JCP & ADOPT-A-JSR

Paul Brauner (Google)
A BACKEND DEVELOPER MEETS THE WEB: MY DART EXPERIENCE

and many more!

Program & tickets available now at:
jazoon.com

Informationen für die Steuerfahndung

Der Bundesfinanzhof hat den Betreiber einer Online-Handelsplattform zur Auskunft über Händler gegenüber der Steuerfahndung verurteilt (Az. II R 15/12). Ziel des Sammelauskunftsersuchens ist es, alle Händler aufzufinden zu machen, die mehr als 17 500 Euro pro

Jahr umsetzen, denn über diese Summe hinaus unterliegen Verkäufe der Umsatzsteuerpflicht. Betroffene Händler auf eBay & Co. müssen sich auf Ermittlungen der Steuerfahndung gefasst machen, wenn sie ihre Waren bislang brutto wie netto verkauften. *Tobias Haar (ur)*

Management von Kundenabrechnungen

Die gerade erschienene Version von Pactas.Itero, einer Management-Plattform zum Verwalten von wiederkehrenden Kundenabrechnungen, bietet Abo-Commerce-Anbietern nun das Auslagern aller administrativer Tätigkeiten über ein neues Self-Service-Produkt an. Jetzt kann der Anbieter seine Geschäfts-, Stamm- und Rechnungsdaten sowie Zahlungsinformationen direkt über eine

verschlüsselte und von Pactas gehostete Seite erfassen. Die Daten werden laut Aussage des Anbieters ausschließlich in Deutschland gespeichert. Pactas.Itero übernimmt zudem das Aktualisieren von Zahlungsinformationen (etwa abgelaufene Kreditkarten et cetera). Außerdem soll sich damit das Debitoren-Management und Mahnwesen komplett automatisieren lassen. *(ur)*

Facebook plant eigenen Bezahlidienst

Laut AllThingsD, dem Blog des Wall Street Journal, plant Facebook einen eigenen Bezahlidienst nach dem Vorbild von PayPal. Der Dienst, dessen Vorbereitung bereits im Gange sein und der als Pilot

bald starten soll, ermöglicht das uneingeschränkte Einkaufen über das soziale Netzwerk. Die Benutzer müssen dafür allerdings ihre Kreditkarteninformationen bei Facebook hinterlegen. *(ur)*

Kurz notiert

Industrie 4.0: Bereits 15 % aller mittelständischen Fertigungsunternehmen setzen selbststeuernde Produktionsprozesse ein, stellt eine Studie der Marktforschungsfirma PAC fest. In Kürze sollen weitere Ergebnisse und zum Jahresende ein kompletter IT-Innovationsindex veröffentlicht werden.

M-Commerce: Mit seinem Software-as-a-Service-Produkt „ShopMatrix“ verspricht das Berliner Start-up-Unternehmen PressMatrix Unternehmen, aus ihren Online-Shops eine native App für Tablets zu generieren. Basis kann jedes Shopsystem sein, im ersten Schritt funktioniert es mit Magento-Shops.

SEPA-Umstellung: Laut einer BaFin-Studie werden die rund 1780 deutschen Zahlungsdienstleister für die SEPA-Umstellung gerüstet sein. Sorgen

bereit der Aufsichtsbehörde allerdings der mangelnde Kenntnisstand der Umsetzung bei den Kunden der Dienstleister sowie die Umsetzung bei externen IT-Dienstleistern.

Shopsoftware: Die jüngste Version des Open-Source-Shopsystems Arcavias hat der Anbieter Metaways vor allem im Frontend ausgebaut. Neben neuen Funktionen für Nutzer stehen erweiterte für den Administrator sowie eine Verwaltung für Cron-jobs zur Verfügung.

Alleskönnen SIM-Karte: Giesecke & Devrient bietet eine neue Plattform für SIM-Karten, mit der sich mehrere NFC-Anwendungen gleichzeitig auf einer SIM-Karte ausführen lassen. Die SkySIM-CX-Familie verfügt über geschützte Bereiche für elektronische Bezahl- und Ticketanwendungen. Das erste Produkt der Familie wurde nun von American Express, MasterCard und Visa zertifiziert.

Defizite im mobilen E-Commerce

Obwohl die Nutzung von Smartphones und Tablets in den letzten Jahren gestiegen ist, sind längst nicht alle Online-Shops gut für den mobilen Einkauf gerüstet. Das ergab eine Studie der UDG United Digital Group GmbH unter den 46 umsatzstärksten Shops Deutschlands. Das größte Defizit stellten die Experten im Bereich „Responsive Design“ fest, also im dynamischen Anpassen der Inhalte an die Displaygröße des jeweiligen Endgeräts oder auch dem schnellen Laden der Seiten. Schlechte

Bewertungen gab es auch für die Darstellung der Allgemeinen Geschäftsbedingungen oder des Widerrufsrechts. Überdies blieb nur bei wenigen Anbietern der Warenkorb über verschiedene Geräte hinweg nach dem Einloggen vorhanden. Zu den Stärken dagegen zählte bei vielen Shops die Erkennbarkeit der Marken, außerdem konnten Nutzer die Funktionen der klassischen Webseite leicht in der mobilen Version wiederfinden. Weitere Ergebnisse liefert eine Zusammenfassung der Studie („Alle Links“). *(ur)*

Aktuelle Studie: Mobiles Einkaufsvergnügen bereits responsive?

Rang	Unternehmen	Punkte*
Top 5		
1	amazon.de	20,68
2	otto.de	18,70
3	mytoys.de	18,65
4	sportcheck.de	18,23
5	zalando.de	18,10
Flop 5		
42	hse24.de	13,80
43	unimall.de	12,93
44	thomann.de	12,88
45	cyberport.de	12,75
46	dell.de	12,35
Durchschnitt von allen 46 Unternehmen		15,36

* maximal erreichbare Punkte: 24

Pilotprojekt soll E-Invoicing vorantreiben

Der größte Versender und Empfänger von Rechnungen hierzu lande ist die öffentliche Hand. Experten gehen von hohen Einsparungen beim Umstellen auf das sogenannte E-Invoicing aus. Ein vom Bundesministerium des Inneren angestoßenes Pilotprojekt soll nun dabei helfen, Erfahrungen zu sammeln, und die elektronische Rechnungslegung sowie das dafür im „Forum elektronische

Rechnung in Deutschland“ entwickelte einheitliche Datenformat (ZUGFeRD-Format, siehe „Alle Links“) vorantreiben. Für das Projekt erfasst der Cloud-Anbieter crossinx alle Eingangsrechnungen des Technischen Hilfswerks und übermittelt sie digital über eine zentrale Schnittstelle zur weiteren Verarbeitung in die Warenwirtschafts-, Archiv- und Workflowsysteme des THW. *(ur)*

Kostenloses Werkzeug für E-Rechnungen

Für Nutzer, die maximal hundert Rechnungen pro Tag bearbeiten, stellt die intarsys consulting GmbH ihre neuen Werkzeuge für elektronische Rechnungsbearbeitung zur freien Nutzung zur Verfügung. Die Software unterstützt den neuen einheitlichen Rechnungsstandard ZUGFeRD, ist für Server und Desktop einsetzbar und

lässt sich – gegen eine einmalige Lizenzgebühr – in ein Enterprise-Content-Management-System einbinden. Mit ihr kann man XML-Rechnungsdaten in PDF/A-3-Dateien einbetten oder aus ihnen extrahieren. Das „intarsys ZUGFeRD Toolkit“ ist auf der intarsys-Homepage oder über www.ferd-net.de erhältlich. *(ur)*

Updates bei Nagios

Gleich für vier Produkte veröffentlicht Nagios Aktualisierungen. Fusion liegt in Version 2012r1.6 vor. Durch ein erweitertes Management der Session lässt sich ein Timeout verhindern; man kann mit Nagios Servern auf Nicht-Standard-

Ports arbeiten. XI 2012r2.3 enthält einige Bugfixes und erweitert die verfügbaren Sprachen um Japanisch. NRPE kann man als Version 2.15 herunterladen, neu ist die Unterstützung für IPv6. Kleinere Fehler behebt Core 3.5.1. (fo)

Aktualisierungen bei SolarWinds

Mit drei Updates bringt SolarWinds seine Software auf den aktuellen Stand. Der Network Configuration Manager (NCM) erkennt nun Geräte älteren Baujahres, sodass Administratoren veraltete Komponenten entdecken können. Die Software bietet zudem globale Geräteverbindungsprofile (Global Device Connection Profiles) zum standardisierten Einrichten von Routern und Switches.

Der Server & Application Monitor (SAM) liegt in Version 6.0 vor. Neu ist AppInsight for SQL zum Überwachen der Datenbankleistung. Der Base-

line-Schwellenwert-Kalkulator dient dem Berechnen von Grenzwerten für Standardabweichungen der Systemleistung. Ein neues Dashboard soll Verantwortlichen dabei helfen, alle Posten der IT-Umgebung wie Hardware-Komponenten oder Garantien im Blick zu behalten.

Am VoIP & Network Quality Manager haben die Texaner ebenfalls gearbeitet. Das Gateway- und Trunk-Monitoring für VoIP zeigt Leistungsmerkmale und Auslastung des PRI-Trunks (Primary Rate Interface) von Ciscos MGCP an. (fo)

Überwachung bei TeamViewer

Für Nutzer der Management Console oder des Client von TeamViewer bietet das Unternehmen ein webbasiertes Monitoring unter dem Namen ITbrain an. Geräte kann man einem Konto zuweisen, um sie aus der Ferne zu überwachen und zu verwalten. Die Software ist in der Lage Speicher-

kapazität, Windows Update, Virenschutz und Firewall im Blick zu behalten und bei Fehlern den Administrator zu alarmieren. Zudem zeigt sie, welches Gerät zuletzt online war. Lizizenzen für ITbrain kalkulieren die Göppinger pro Endpunkt auf monatlicher oder jährlicher Basis. (fo)

Kurz notiert

Updates: Das Modul VIVA für i-doit liegt nun in Version 1.2 vor und enthält neue Assistenten. i-doit pro haben die Entwickler auf 1.1.2 gebracht und sich auf Bugfixes konzentriert.

Anpassen: Von Assmann kommen neue Konsolen für Rechenzentren auf den Markt, bei denen Administratoren vor allem im Bereich der Tastaturen umfangreicher variieren können.

Fernsicht: Administratoren, die Netops Remote Control zum Warten und Steuern von Windows verwenden, können Version 11.5 herunterladen. Die Programmierer haben dem Tool eine Browser-basierte Supportkonsole spendiert.

Mobil: Für Tablets und Smartphones von Apple bietet Materna eine App an, die mit dem System Management Center (MSMC) zusammenarbeitet und grafische Ergebnisse der Netzwerkkomponenten und Server auf den Touchscreen liefert.

Web Hacking Schulungen 2013 / 2014

Sicherheit von Web-Anwendungen aus Angreiferperspektive

Web Hacking Schulung für Entwickler, Administratoren und IT-Sicherheitsverantwortliche mit umfangreichem Praxisteil.
Melden Sie sich an und lernen Sie die Perspektive Ihrer Gegenspieler kennen!

Termine 2013:

- 24. bis 26. September
- 22. bis 24. Oktober
- 19. bis 21. November

Teilnahmegebühr:

2.190,- EUR zzgl. MwSt.

Termine 2014:

- 28. bis 30. Januar
- 11. bis 13. März
- 13. bis 15. Mai
- 16. bis 18. September
- 21. bis 23. Oktober
- 25. bis 27. November

Weitere Informationen und Anmeldung unter:
www.schutzwerk.com/webhacking



Unabhängige Prüfung und ganzheitliche Optimierung
Ihrer Informations- und IT-Sicherheit

Tel. +49 731 / 977 191 0 | info@schutzwerk.com

SCHUTZWERK

Neue App-Art: Offline, ohne Browser

Zum fünften Chrome-Geburtstag hat Google sich etwas Spezielles ausgedacht: Apps, die offline und unabhängig vom Browser laufen. Beim Download der ersten App lädt der Browser für Windows und Chrome OS einen Launcher, den man in der Task-Leiste platzieren kann. Für Mac OS X existiert eine Vorversion ohne Launcher. Linux soll folgen.



Googles C-Bibliothek zum HTML5-Parsen

Mit Gumbo hat Google eine in C geschriebene Programmierungsbibliothek zum Parsen von HTML quelloffen zur Verfügung gestellt. Sie setzt den mit HTML5 standardisierten Parsing-Algorithmus um, hat offenbar alle html5lib-0.95-Tests bestanden und wurde auf 2,5 Milliarden von Google indizierten Seiten getestet. Der Projektbeschreibung zufolge soll sich die Library von vielen Programmiersprachen aufrufen lassen.

Entwickler können die Bibliothek mit Webseiten-Validatoren, bei der statischen Code-Analyse und in Verbindung mit Template-Sprachen sowie Refactoring-Tools verwenden. Als weitere Features sind die Unterstützung des HTML5-Template-Tags und des Parsing von HTML-Fragmenten sowie Bindings in anderen Programmiersprachen geplant. Google hat für Gumbo die Apache Licence 2.0 gewählt. (ane)

Kurz notiert



HTML-Editor: Adobe bietet Brackets, seinen Open-Source-Code-Editor für die Webentwicklung mit HTML, CSS und JavaScript, nun außer für Windows und Mac OS X für Linux-Systeme an. Brackets stellt unter anderem die Basis für Adobes Edge Code dar.

Facebook: Einer bei der Online-Zeitschrift PLOS ONE veröffentlichten Studie von Forschern der Universität Michigan zufolge

geträgt häufiges Nutzen des Facebook-Netzes dazu bei, dass das Wohlbefinden der Anwender sich verschlechtert.

Soziales Netz: Diaspora, das seit einem Jahr von einer Community entwickelte soziale Netz, hat mit Version 0.2 unter anderem die Einzelansicht von Beiträgen überarbeitet.

Type3-Update: Sicherheits-schwachstellen, die Experten der SySS GmbH gefunden hatten, haben die Type3-Entwickler mittlerweile geschlossen; Nutzer sollten Version 6.1.4 installieren.

Chrome 29 verbessert URL-Vorschläge

Google hat Version 29 seines Browsers Chrome für Linux, Windows und OS X veröffentlicht. Gleichzeitig erschien eine Beta mit derselben Versionsnummer für das hauseigene Mobilbetriebssystem Android. Für Anwender dürften vor allem die Neuerungen an der multifunktionalen Adressleiste („Omnibox“) und Benachrichtigungen sowie die Unterstützung für Googles aktuellen Video-Codec VP9 hilfreich sein.

VP9 soll das bisherige VP8 ablösen, das der Internetkonzern ursprünglich als frei propagiert hatte. Mittlerweile hat Google jedoch ein Lizenzabkommen mit dem Patentverwalter MPEG-LA geschlossen, das VP8-Nutzer von Patentansprüchen freistellt. Nokia ist diesem Vertrag nicht beigetreten und hat angekündigt, gegen Verletzer seiner VP8 betreffenden Patente vorzugehen.

Nach Herstellerangaben soll die Omnibox jetzt beim Anbieten von URLs den Verlauf

besser berücksichtigen und zuletzt besuchte Websites bevorzugt vorschlagen. Außerdem des Browser-Fenster angezeigte Benachrichtigungen, etwa über eingetroffene E-Mails, haben ein neues Interface erhalten und erlauben es dem Benutzer, direkt darauf zu reagieren. Dazu gibt es eine API, über die Entwickler von Add-ons und Chrome-Apps diese Benachrichtigungen erzeugen und auf Benutzeraktionen reagieren können.

Weitere neue Schnittstellen sind für die Chrome-Apps vorgesehen: Die Identity-API erlaubt ihnen, OAuth für die Authentifizierung zu nutzen, Bezahlfunktionen binden Googles hauseigene Wallet ein und ermöglichen das Einkaufen aus einer App heraus. Außerdem sind Schnittstellen für Bluetooth, den Zugriff auf lokale Mediendateien und für den Datenaustausch mit nativen Anwendungen hinzugekommen. (ck)

Bootstrap 3.0: Mobile First und RWD

Zum zweiten Jahrestag der Premiere von Bootstrap ist das von Twitter gestartete HTML5-Frontend-Toolkit in Version 3.0 erschienen. Es stellt im Wesentlichen ein HTML- und CSS-Template bereit. Webentwickler können damit unter anderem auf bewährte Frontend-Patterns zurückgreifen, ein Grid-System integrieren, das Styling für typografische Elemente übernehmen, Formulare und Buttons verwenden oder ihre Seiten mit Modal-Boxen, Tooltips und Pop-overs ergänzen.

Das Redesign erfolgte vor dem Hintergrund des Mobile-

First-Ansatzes und der Umsetzung des daraus resultierenden Responsive Webdesigns (RWD). Darüber hinaus weist die Ankündigung auf ein standardmäßig besser zu verwendendes Box-Modell (`box-sizing: border-box`), neu geschriebene JavaScript-Plug-ins, eine neue Glyphicons-Icon-Schrifttype sowie eine responsive Navigationsleiste. Als neue Komponenten sind Panels und Listengruppen dazu gekommen, andere wurden wiederum entfernt. Nicht mehr unterstützt werden Internet Explorer 7 und Firefox 3.6. (ane)

Wer im Netz ist und wer nicht

Laut einer Studie von ARD und ZDF zum Online-Verhalten der Deutschen sind 77,2 % von ihnen mittlerweile online, was gegenüber dem Vorjahr nur eine Steigerung von 1,7 % bedeutet. Im Vergleich zu 2012 stieg die Verweildauer im Netz pro Tag von 133 auf 169 Minuten. Für die Studie waren im Frühjahr 1800 Personen ab 14 Jahre befragt worden.

Gleichsam im Gegensatz dazu hat das Statistische Bundesamt für 2012 mitgeteilt, dass 15 % der Bundesbürger noch nie im Internet waren (je älter, desto mehr Offliner). Im europäischen Mittel sind es sogar 22 %. Seit 2005 ist die Zahl um 14 % gesunken, die wenigsten Nichtnutzer leben in Schweden, den Niederlanden und Finnland (deutlich unter 10 %). (hb)

Vorschau auf Windows 8.1

Zeitnah

Moritz Förster

So ganz fertig ist das Windows-Update noch nicht – seit der Preview im Juni hat sich dennoch schon einiges getan – ästhetisch und unter der Haube.

Während man den Server 2012 R2 längst unter die Lupe nehmen kann, musste man auf die finale Version zum Testen von Windows 8.1 noch etwas warten – obwohl Nutzer das kostenlose Update schon am 17. Oktober herunterladen können. Erst nach heftiger Kritik stellte Microsoft Images zur Verfügung. Die RTM-Ausgabe (Release To Manufacturing) fand dennoch den Weg in die Tauschbörsen.

Zunächst wollen es die Designer der Kacheln den Desktop-gewöhnten Anwendern vereinfachen, sich auf der neuen Oberfläche zurechtzufinden. Erklärende Pfeile in Ecken und an Rändern drängen sich so lange auf, bis man eine bestimmte Aktion mit den Händen respektive der Maus korrekt ausführt. Eine zusätzliche Größe für die Kacheln soll gerade auf kleineren Touchscreens für mehr Übersicht sorgen. Zudem kann man mit dem

Schalter „Weitere Kacheln zeigen“ eine zusätzliche Reihe anzeigen lassen.

Innerhalb der Apps weist der „Minibar“ auf eine Menüleiste hin, die man wie gewohnt durch den Wisch in die Mitte aufruft. Einige vorinstallierte Apps haben die Entwickler überarbeitet, neu hinzugekommen ist Skype. Man kann direkt auf dem Desktop starten, nach dem Beenden von Apps kehrt 8.1 zudem direkt dorthin zurück. Ein „Startknopf“ soll das Wechseln des Interface deutlicher hervorheben.

Die Redmonder liefern alle aktuellen Betriebssysteme mit dem „Defender“ aus. Der Virenschutz enthält mit 8.1 eine Erkennung für verdächtige Verhaltensmuster. Wer sein System beschleunigen möchte, kann auf den erweiterten Support von Hybrid-Festplatten setzen: SSHDs verwenden einen Flash-Pufferspeicher neben den konventionellen Magnetfestplatten. Optimieren soll dies das Hinting-Protokoll, aber derzeit

findet man im Handel keine geeigneten Geräte.

Für professionelle Anwender dürfte die aktualisierte Virtualisierungsplattform Hyper-V der 64-Bit-Pro- und -Enterprise-Versionen einiges bringen. Als Firmware kann auch UEFI zum Einsatz kommen, was sich nach dem Erstellen einer virtuellen Maschine (VM) nicht mehr ändern lässt. In der „Erweiterten Sitzung“ kann man per Remote Desktop Dateien direkt zwischen Wirt und VM austauschen, zudem reicht das System Soundkarte und Drucker durch. Voraussetzung ist jedoch, dass in der VM ebenfalls 8.1 als Pro- oder Enterprise-Version läuft.

Wer das Betriebssystem neu installiert und seinen eigenen lokalen Account pflegen will, muss suchen: Zunächst bietet der Assistent die Option gar nicht an. Lediglich nach dem Entfernen der Internetverbindung oder dem Eingeben einer ungültigen E-Mail-Adresse hat man Zugriff auf den entsprechenden Dialog. (fo)

T3CON13
STUTTGART

3 days, 3 topics
fantastic speakers

The 9th European TYPO3 Conference
October 29 - October 31 // Stuttgart, Germany

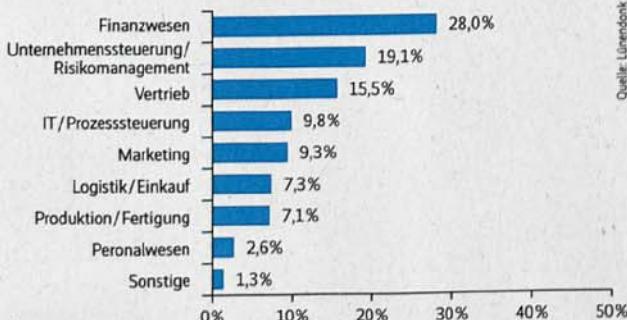
Spezialisierte BI-Anbieter legen zu

Business Intelligence (BI) hat sich 2012 als wachstumsträchtiges Teilsegment im deutschen IT-Markt erwiesen. Während die gesamte ITK-Branche laut ihrem Lobby-Verband BIT-KOM um 1,4 % auf 153 Mrd. Euro zulegte, steuerte das Segment BI-Standardsoftware mit einem von der Lünendonk GmbH geschätzten Marktvolumen von etwa 1,2 Mrd. Euro einen vergleichsweise niedrigen, dafür aber stark wachsenden Teil bei. Im vergangenen Jahr betrug das durchschnittliche Umsatzplus der von der Kaufbeurener Marktforschungsfirma untersuchten BI-Anbieter rund 11,3 % Prozent.

Als Nummer eins im deutschen Markt konnte sich SAS Institute behaupten. Die hiesige Dependance des US-amerikanischen Herstellers erzielte 2012 einen Umsatz von 134,6 Mio. Euro. An zweiter Stelle folgt Teradata mit einem geschätzten Umsatz von 50,0 Mio. Euro, an dritter Position MicroStrategy mit 35,5 Mio. Euro. QlikTech, Informatica und pmOne komplettieren die

Top Fünf der Marktstichprobe, wobei sich Informatica und pmOne mit jeweils geschätzten 16,0 Mio. Euro Umsatz den fünften Platz teilen.

Lünendonk nimmt in die Stichprobe ausschließlich Anbieter auf, die mindestens die Hälfte ihres Umsatzes mit Vertrieb, Einführung und Wartung eigener BI-Software-Produkte erwirtschaften. Damit fallen die großen Mitspieler heraus. SAP, Oracle und Microsoft erzielen hierzulande zwar meist höhere Einnahmen mit BI-Software als die Spezialisten, das Gros ihrer Geschäfte machen sie jedoch mit anderen Programmen, etwa ERP oder CRM. Die positive Nachfrageentwicklung der Spezialisten dürfte sich 2013 fortsetzen. Dem Gesamtmarkt für BI-Software prognostizieren die Analysten ein Wachstum von 11,5 %. Bezogen auf ihr eigenes Unternehmen sind die von Lünendonk untersuchten Hersteller mit einem erwarteten Umsatzwachstum von 21,7 % im statistischen Mittel deutlich optimistischer. (jd)



So verteilt sich der Einsatz von BI-Programmen in der Unternehmenslandschaft.

Kurz notiert



Ausbau: Die Software AG hat JackBe übernommen. Die US-Firma bietet Software zum Visualisieren, Auswerten und Verknüpfen von Daten an. Auf Basis dieser Programme entwickelt die Software AG ihre neue webMethods IBO-Plattform, die sie ab dem vierten Quartal ausliefern will.

BPM-Kumpels: Inspire und Process Gold wollen das klassische Business Process Management

um Process Mining erweitern. Das resultierende Produkt soll helfen, Unternehmensabläufe nach Schwachstellen und Einsparpotenzialen zu durchforschen. Danach folgt das Redesign und das Automatisieren der Abläufe via BPM inspire.

Geschafft: Der Prozessmodellierungsstandard BPMN hat die Weihen der Standardisierungsorganisation ISO/IEC erhalten. Die Spezifikation 2.01 der OMG (Object Management Group) ist nun die offizielle Norm ISO/IEC 19519:2013.

App als Brücke zwischen Programmen

Westaflex hat gemeinsam mit der RWTH Aachen und GS1 Germany eine Android-App für IBMs BladeCenter entwickelt. Das Programmchen soll die Kommunikationslücken zwischen betriebswirtschaftlichen und produktionsnahen Standardanwendungen überbrücken. SQL-Views binden dazu uni-direktional Datenquellen wie ERP, MES, CRM, Qualitätssicherung und Zeitwirtschaft ein. Die App eignet sich

unter anderem zur Personaleinsatzplanung und Auftragskontrolle. Durch das Befolgen des EPCIS-Standards (Electronic Product Code Information Services) lassen sich unternehmensübergreifende Warenflüsse überwachen. Zugehörige Ereignisse werden im Push-Verfahren nach festgelegten Intervallen auf Mobilgeräten angezeigt. Konfigurieren lässt sich die App nach Rollen und Berechtigungen. (jd)

SAPs HANA kommt aus der Cloud

HP bringt SAPs In-Memory-Analyseplattform HANA in einer Software-as-a-Service-Variante (SaaS) heraus. Mit dem Angebot sollen Unternehmen in Echtzeit große Datenbestände auswerten können. Bezahlbar wird per monatlicher Nutzungsgebühr. Im Preis inbegriffen sind die Softwarelizenz, das Applikationsmanagement sowie die nötige Hardware. Das Ganze basiert auf der von SAP zertifizierten virtuellen Appliance HP AppSystem for SAP HANA, die in einer Managed-Cloud-Umgebung läuft. HP hostet die Anwendung in

regionalen Rechenzentren für Unternehmenskunden. HPs Migration Factory for SAP HANA soll die Migration der Kundendaten sicherstellen.

Zunächst will HP das Angebot in Australien und Neuseeland und später weltweit zur Verfügung stellen. Pilotprojekte mit Kunden in Europa sind angeblich schon gestartet. Beim Preis solcher Softwarepakete für Unternehmen halten sich die Anbieter traditionell bedeckt. Die Kunden müssen ihn je nach persönlicher Bedürfnislage aushandeln (siehe „Alle Links“). (jd)

SAP entdeckt den Kunden

Mit SAPs Analyseanwendung „Social Contact Intelligence“ sollen Vertriebler die Diskussionen ihrer Kunden in sozialen Medien besser verfolgen können. Ziel ist, Kampagnen für maßgeschneiderte Angebote zu entwickeln. Mit der Anwendung, die auf der In-Memory-Plattform HANA läuft, schließt SAP eine Lücke in seinem „Customer Engagement Intelligence“. Die Customer-Engagement-Suite

umfasst neben Social Contact Intelligence drei weitere Anwendungen: Audience Discovery and Targeting ermöglicht eine feineren Segmentierung von Zielgruppen bei Marketingkampagnen. Über Customer Value Intelligence lassen sich Vorschläge für Cross- und Up-Selling entwickeln. Und die App „Account Intelligence“ hilft dem Vertriebsmitarbeiter beim Vorbereiten seiner Besuche. (jd)

Dynamics NAV findet Office-365-Anschluss

Microsoft hat Dynamics NAV 2013 R2 vorgestellt. Eine der wichtigsten Neuerungen ist die Anbindung an Office 365. Anwender können so die in Dynamics liegenden Daten mit Excel oder Excel Web Apps bearbeiten. Single Sign-on sowie das einheitliche Look and Feel des Webclients sollen das gemeinsame Nutzen von ERP- und Office-Software verein-

fachen. Zu den weiteren Verbesserungen zählen Funktionen für das Cash-Management und zum Abbilden des SEPA-Zahlungsverkehrs. Dynamics NAV 2013 lässt sich traditionell in Eigenregie oder in der Cloud betreiben. Letzteres geschieht auf Basis von Windows Azure Infrastructure Services. Das Produkt soll ab Oktober verfügbar sein. (jd)

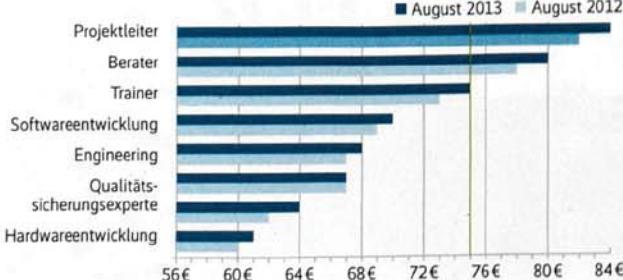
Stundensätze für Freelancer gestiegen

Mit einem durchschnittlichen Stundensatz von 75 Euro stehen IT-Freelancer so gut da wie nie zuvor, schreibt der Personaldienstleiter GULP in seiner jährlichen Stundensatzanalyse.

In der untersucht das Projektportal die Honorarforderungen der im Kandidatenpool registrierten 26 300 Freiberufler. Die Auswertung zeigt ein differenziertes Bild, denn Faktoren wie die Rolle im Projekt, das Land, in dem der Freelancer lebt, Be-

rufserfahrung und das Alter beeinflussen die Honorare stark: Die Spanne reicht von 84 Euro für Projektleiter (Vorjahr 82 Euro) bis 62 Euro für Administratoren (Vorjahr 60 Euro).

Fast die Hälfte der IT-Freelancer sind zwischen 40 und 50 Jahre alt. Ihre Erfahrung scheint zu zählen: Differenziert nach Altersgruppen liegen sie laut GULP mit 78 Euro vorn (Vorjahr 73 Euro) (siehe „Alle Links“). (jd)



Stundensatzforderung der IT/Engineering-Freiberufler nach Position

Kurz notiert

rialien und beantwortet Fragen zu Lizzenzen, zum Urheberrecht und zur Qualitätssicherung (siehe „Alle Links“).

Duales Studium: Unternehmen und Hochschulen, die sich an dualen Studiengängen beteiligen, agieren größtenteils autonom. Über organisatorische Fragen hinaus gäbe es wenig Austausch zwischen ihnen. Zu diesem Ergebnis kommt das Bundesinstitut für Berufsbildung (BIBB) in einer Online-Befragung von 280 Kooperationsbetrieben.

Fernstudium: Zum kommenden Wintersemester gibt es an der Hochschule Anhalt den neuen Master-Fernstudiengang Elektro- und Informationstechnik. Einen Studienschwerpunkt bildet die Entwicklung eingebetteter Systeme.

Offene Bildung: In der Broschüre „Was sind Open Educational Resources?“ informiert die deutsche UNESCO-Kommission über offene Bildungsmate-

Beliebte Jobbörsen für Arbeitgeber

Personalverantwortliche nutzen am liebsten die Arbeitsvermittlungsbörsen Jobware, Stellenanzeigen.de und meinestadt.de. Um das herauszufinden, befragte die Agentur Profilo 1391 HR-Experten. Bei den branchenspezifischen Jobportalen

liegen Hotelcareer, Yourfirm und jobvector vorne. Letztere hat sich auf Naturwissenschaftler, Ingenieure und Techniker spezialisiert. Zu den Bewertungskriterien gehören etwa Kundenbetreuung und unkomplizierte Handhabung. (jd)

MOOCs sind kein Jugendphänomen

Ein Jahr nach dem Start seiner Bildungsplattform openHPI.de hat das Potsdamer Hasso-Plattner-Institut eine erste Zwischenbilanz gezogen. Demnach ist ein typischer Teilnehmer eines Massive Open Online Courses (MOOCs) 30 bis 40 Jahre alt, männlich und seit

über zehn Jahren in einem Beruf mit hohem Anteil an Informationstechnologie tätig. An den fünf durchgeführten Kursen nahmen etwa 50 000 Interessierte teil, rund 8000 erhielten ein Zertifikat, vor allem aus der Altersgruppe der 40- bis 50-Jährigen. (jd)

Zu wenig Frauen in MINT-Fächern

Insgesamt ist die Studiennachfrage nach MINT-Fächern (Mathematik, Informatik, Naturwissenschaft, Technik) zwar gestiegen, das Potenzial wird jedoch wegen der unterdurchschnittlichen Beteiligung von Frauen nicht ausgeschöpft. Die Gründe dafür untersucht das HIS-Institut für Hochschulfor-

schung in seinem Bericht „Bildung und Qualifikation als Grundlage der technologischen Leistungsfähigkeit Deutschlands“. Wichtige Indikatoren für die schlechte MINT-Frauenquote sind mangelnde Förderung schon in der Schule und ein tradiertes Familienbild. (siehe „Alle Links“). (jd)

IT-Freelancing wird Boom-Branche

Vermittler freiberuflicher IT-Experten in Deutschland rechnen laut den Marktforschern von Lünendonk aufgrund einer stabilen Nachfrage mit einem zweistelligen Wachstum von 11,1 % für das Jahr 2013. Damit liegen die Erwartungen deutlich über denen der eben-

falls untersuchten IT-Berater und Systemintegratoren (5 %). Die am häufigsten gesuchten Kompetenzfelder bei IT-Freelancern sind SAP-Know-how und Projekt-/Qualitätsmanagement. Das zeigt eine 1400 Euro teure Marktsegmentstudie 2013 (siehe „Alle Links“). (jd)

Wollen Sie auch, dass NSA und Co die Finger von Ihren Daten lassen?

Grünes Licht für VDSL-Vectoring

Ende August gab die Bundesnetzagentur ihre endgültige Entscheidung für die Rahmenbedingungen zur Einführung der Vectoring-Technik im Netz der Telekom Deutschland bekannt. Mit dem Verfahren lassen sich im Kupferanschlussnetz höhere Übertragungsraten erzielen, als dies mit VDSL (Very High Speed Digital Subscriber Line) allein der Fall ist. Eine Beschleunigung auf bis zu 100 Mbit/s im Down- und bis zu 40 Mbit/s im Upload-Einsatz soll hierdurch möglich sein. Voraussetzung: Die Leitungslänge zwischen Endkundenanschluss und Kabelverzweiger (KVz) muss unter 500 Meter bleiben und Letzterer selbst über Glasfaser angebunden sein. Nach dem Stand der Technik ist dafür allerdings der

Zugriff eines einzigen Unternehmens auf alle Kupferdoppeladern am KVz unumgänglich. Weitere Anbieter könnten die Anschlussleitung dann nicht mehr mitbenutzen.

Die Telekom hatte Ende letzten Jahres erstmals den Wunsch geäußert, die Zugangsmöglichkeiten für Wettbewerber zur Teilnehmeranschlussleitung an den KVz einzuschränken, um Vectoring in ihrem Netz einsetzen zu können. Unter den alternativen Festnetzbetreibern machte seinerzeit schnell der Begriff „Re-Monopolisierung“ die Runde. Diese berechtigte Kritik hat die Bundesnetzagentur zum großen Teil beherzigt und in ihrem ursprünglichen Entwurfspapier entsprechend angepasst.

Nach den jetzigen Rahmenbedingungen muss die Telekom ihren Wettbewerbern auch künftig den Zugang zur Teilnehmeranschlussleitung am KVz gewähren; sie genießen Bestandsschutz. „Unter besonderen Bedingungen“ darf die Telekom den Zugang jedoch verweigern, manchmal auch kündigen, damit sie selbst oder ein anderes Unternehmen dort Vectoring einsetzen kann. Dann muss sie jedoch ein angemessenes Bitstromprodukt als Ersatz anbieten. Die Bundesnetzagentur nahm daher den Ex-Monopolisten in die Pflicht, nun unverzüglich seine aktuellen Verträge für den Zugang zur „letzten Meile“ zu überarbeiten. Die neuen Musterverträge muss er der Behörde zur Prüfung vorlegen. (jd)

Tablet Computer: Wege ins Internet

WLAN, UMTS oder LTE? 65 % der Tablet-Nutzer gehen derzeit ausschließlich via WLAN online, nur ein Drittel surft per Mobilfunk. Dabei kommt meist UMTS (28 % aller Befragten) zum Einsatz. Nur 8 % setzen auf das schnelle LTE (Long Term Evolution). Zu diesen Ergebnissen gelangt

eine repräsentative Befragung von BITKOM Research.

Laut der Umfrage setzt jeder vierte Nutzer (27 %) das Gerät ausschließlich und jeder dritte (34 %) überwiegend in der eigenen vier Wänden ein. Weitere 30 % verwenden es gleichermaßen zu Hause und unterwegs. 8 % gaben an, aus-

schließlich unterwegs mit dem Tablet online zu gehen. Nur 6 % wählen sich mit dem eigenen Mobilfunkmodul ein. 13 % verbinden Tablet und Smartphone, um den Internetzugang herzustellen. Auf öffentliche WLAN-Hotspots greifen 28 % der befragten Anwender zurück. (jd)

AVM mit neuem Spitzenmodell

Die zur CeBIT angekündigte Fritzbox 7490 ist im Handel erhältlich. Das neue Topmodell der Berliner AVM dient als VDSL- und ADSL2+-Router mit Vectoring-Unterstützung. Neben dem WLAN nach den neuen 802.11-AC-Spezifikationen mit bis zu 1300 MBit/s (5 GHz) lässt sich gleichzeitig

ein WLAN-N-Funknetz mit bis zu 450 MBit/s (2,4 GHz) betreiben. Profitieren sollen davon vor allem Breitbandanwendungen wie HD-Videostreaming oder große Downloads.

Das Einrichten eines eingeschränkten WLAN-Gastzugangs (Hotspot) für Freunde und Besucher ist möglich. Ne-

ben den WLANs stehen vier Gigabit-LAN- und zwei USB-3.0-Anschlüsse zur Verfügung. Zur Ausstattung der Box zählen eine DECT-Telefonanlage sowie diverse Funktionen für den Betrieb als Medien- oder NAS-Server. Unverbindliche Preisempfehlung für die Fritzbox 7490: 289 Euro. (jd)

Kurz notiert

Namensgeber: I&I hat mit der ICANN eine Vereinbarung über die Registrierung von neuen Top-Level-Domains unterzeichnet. Voraussichtlich ab Oktober sollen Interessenten via I&I über 700 neue Begriffe als Adresssendung für Domains nutzen können.

Nachzügler: Als letzter unter den vier großen Mobilfunkbetreibern Deutschlands kündigte

Telefónica O2 an, UMTS mit Dual-Carrier-Technik zu beschleunigen. Durch die Kanalbündelung, auch als Dual-Cell-Technik bezeichnet, sind theoretisch Bruttoübertragungsraten von bis zu 42,2 MBit/s im Downstream und bis zu 5,8 MBit/s im Upstream möglich.

Wechselspiele: WBCI (WITA Based Carrier Interface) ist verfügbar. Die Schnittstelle soll bei einem Anbieterwechsel die Abstimmung zwischen den Carriern

automatisieren. Unter www.wbci.de liegen Informationen zu Funktion, Spezifikation und Preisen.

Kabellos: Kabel Deutschland baut das öffentliche WLAN-Angebot in Bayern aus. Bis Ende September 2013 will der TV-Kabelnetz-Betreiber in 70 Städten und Gemeinden über 300 Hotspots installieren. Noch in diesem Jahr sollen Städte in weiteren Bundesländern hinzukommen.

Top-Titel im Oktober



Wireshark 101
Einführung in die Protokollanalyse
Laura Chappell
368 Seiten
ISBN 978-3-8266-9713-5
€ 44,99
www.mitp.de/9713



Einsatz von ERP-Systemen in mittelständischen Unternehmen
Das ERP-Pflichtenheft
Volker Jungbluth
672 Seiten, mit CD-ROM
ISBN 978-3-8266-9487-5
€ 99,99
www.mitp.de/9487



C++ - Das Übungsbuch
Testfragen und Aufgaben mit Lösungen
Ulla Kirch, Peter Prinz
4. Auflage
608 Seiten
ISBN 978-3-8266-9455-4
€ 19,99
www.mitp.de/9455

Konzernumbau

On(c)e Microsoft

Achim Born

Nach dem Vorbild Apple arbeitet Microsoft an einem umfassenden Konzernumbau. Da ist die Übernahme der Handy-Sparte von Nokia konsequent – ein Erfolg der Strategie bleibt zweifelhaft.

Nun also doch: Bereits im Juni soll nach Berichten US-amerikanischer Zeitungen Microsoft mit Nokia über den Kauf der Handy-Sparte gesprochen haben. Seinerzeit gingen die beiden Windows-Phone-Partner ergebnislos auseinander. Anfang September war es dann soweit – der finnische Handy-Konzern verkauft für insgesamt 5,44 Milliarden US-Dollar sein Kerngeschäft nach Redmond. Konkret erhält das weltweit größte Softwarehaus für 3,79 Milliarden die Gerätesparte inklusive Services. Weitere 1,65 Milliarden fallen für ein langjähriges Nutzungsrecht des umfangreichen Patentportfolios an. Im Rahmen der Übernahme überträgt Nokia Microsoft zudem die Lizenz für Qualcomm-Patente. Zusätzlich darf das Unternehmen gegen eine extra zu zahlende Gebühr in den kommenden vier Jahren Nokias HERE-Plattform (vulgo: Kartendienste) nutzen.

Mit dem Einverständnis der Behörden und Aktionäre erhält Microsoft auf einen Schlag 32 000 neue Mitarbeiter. Ihr neuer Chef bleibt der bisherige, denn Stephen Elop, der erst vor drei Jahren von Redmond an die Nokia-Spitze wechselte, leitet künftig die Handy-Sparte und zählt zu den Kandidaten für die Nachfolge von Steve Ballmer. Für den scheidenden Boss selbst kann der Deal so etwas

wie die letzte große Amtshandlung darstellen, bevor er nicht ganz freiwillig den Chefsessel räumt. Bereits im Juli hatte Ballmer mit markigen Worten die Pläne für einen weitreichenden Konzernumbau verkündet. Unter dem Slogan „One Microsoft“ sollen die einzelnen Sparten künftig effizienter zusammenarbeiten. Die bisherigen acht Produktabteilungen will man auf vier reduzieren: Betriebssysteme, Apps, Cloud und Geräte. Das engere Verzähnen und strategische Gleichschalten soll zu schnelleren Innovationen und Kostenersparnissen führen. Einzig die Sparte der betriebswirtschaftlichen Anwendungen (Dynamics) bleibt aufgrund ihrer spezifischen Bedingungen von den organisatorischen Änderungen weitgehend unberührt.

Der Konzernumbau ist eine Reaktion auf den Umbruch in der IT. Mobilität und Internet-Services hebeln die traditionellen Marktregeln im PC-Geschäft aus. Als Folge brechen deutlich erkennbar die Gewinne aus der Windows-Sparte weg, während die Geschäfte mit Online-Services und Geräten vor sich hindümpeln. Die bisherigen Gehversuche im Smartphone- und Tablet-Segment hat man entweder wie bei KIN (beim Kunden durchgefallenes, US-exklusives Mobiltelefon-Projekt) gestoppt oder

sind wie beim noch jungen Surface von Abschreibungen (900 Mio. US-Dollar) begleitet.

Vorbild für die Strategie sind offensichtlich Apple und – mit Abstrichen – Google. In beiden von den Börsianern hofierten Konzernen liegt die Entwicklung der Betriebssysteme für mobile Geräte und PCs in einer Hand. Apple zeigt mit jeder Quartalsbilanz zudem, wie lukrativ das enge Verbinden von Hard- und Software mit Services ist. Selbst Google kopiert mit dem vor zwei Jahren eingeleiteten Kauf von Motorolas Handy-Sparte in Ansätzen das Geschäftsmodell, obgleich es noch an einem vorzeigbaren Ergebnis mangelt.

Microsoft zieht mit dem Übernehmen von Nokias Handy-Geschäft gleich. Mit „One Brand, United Voice“ will man die Folgen des Deals in schönsten Farben malen. Auch wenn das Management das vor zwei Jahren zwischen beiden Firmen gestartete Bündnis offiziell als Erfolg bezeichnet, soll künftig alles (noch) schneller, erfolgreicher und vor allen Dingen profitabler von der Hand gehen. Unter einem Firmendach wollen die Redmonder die Arbeit in der Hard- und Softwareentwicklung besser miteinander koordinieren und das Marketing vereinheitlichen. Außerdem verdient Microsoft nach eigenen Angaben dann statt 10 US-Dollar für die Windows-Lizenz künftig 50 US-Dollar an jedem verkauften Smartphone.

Ob die Akquisition tatsächlich der geniale Schritt ist, wie sie die Beteiligten gerne darstellen, erscheint jedoch zweifelhaft. Auf der Habenseite darf Ballmer sicherlich verbuchen, dass Microsoft deutlich weniger zahlt als Google seinerzeit für Motorola. Zudem ist das Image Nokias erheblich besser. Weniger erfreulich ist indes, dass sich das Handy-Geschäft der Finnen seit Jahren auf dem absteigenden Ast befindet. Al-

lein im zweiten Quartal dieses Jahres sind Umsatz um fast ein Drittel auf 2,72 Milliarden Euro und Absatz um 27 % auf 61 Millionen Geräte eingebrochen. Mit 7,4 Millionen verkauften Lumias folgt man der Konkurrenz von Samsung (über 71 Mio.) oder Apple (32 Mio.) nach wie vor mit gebührendem Abstand. Warum es Microsoft nach den vergeblichen eigenen Anläufen mit der Übernahme nun plötzlich gelingen soll, attraktive Angebote aus einem Guss zu entwickeln, ist eine weitere berechtigte Frage. Offen bleibt zudem, ob die übrigen Hardware-Partner an ihren Windows-Phone-Aktivitäten festhalten.

Nicht wenige Marktbeobachter bemühen daher das Bild zweier Fußlahme, die hoffen, gemeinsam zum Sprinter zu mutieren. Dabei verlieren sie aus den Augen, dass zumindest ein Patient eine bestens gefüllte Kasse besitzt. Allein im Geschäftsjahr 2013 verbuchte Microsoft einen Gewinn von fast 22 Milliarden US-Dollar (+28 %). Im offiziellen Strategie-Papier spricht das Management davon, mit der Akquisition die Zukunft von Windows Phone zu schützen. Dazu passt, dass Nokia in den Labors mit anderen Betriebssystemen (u. a. Android) für Lumia-Smartphones experimentiert haben soll. Wäre das Bündnis 2014 ausgelaufen, hätten die Finnen eine Alternative besessen.

Microsoft leitet das Ende des traditionellen Windows-Geschäftsmodells ein: Das Softwareunternehmen wurde groß und mächtig, weil sein OS die Hardware der diversen Hersteller vor dem Anwender verbarg. Mit der vertikalen Integration will man Windows, aber auch Services zwangsläufig enger an die unterliegende (proprietäre) Hardware binden – und das unabhängig davon, ob künftig lediglich ein einziger Hersteller Smartphones mit dem Betriebssystem ausstatten. (fo)

Microsoft – ausgewählte Bilanzzahlen in Milliarden US-Dollar

Segment	Q4/2013 Umsatz und operativer Gewinn	Q4/2012 Umsatz und operativer Gewinn	2013 Umsatz und operativer Gewinn	2012 Umsatz und operativer Gewinn
Windows	4,411 1,099	4,152 2,422	19,239 9,504	18,400 11,555
Server & Tools	5,502 2,325	5,050 2,040	20,281 8,164	18,534 7,235
Online-Services	0,804 -0,372	0,735 -6,672	3,201 -1,281	2,867 -8,125
Business	7,213 4,873	6,324 4,128	24,724 16,194	24,111 15,832

Kurz notiert



Ausbau: Lexmark kauft die SAPERION AG für circa 72 Millionen US-Dollar. Die US-Firma – ursprünglich eine Ausgründung von IBMs Druckersparte – baut mit der Übernahme des Berliner Spezialisten für Enterprise-Content-Management-Programme ihre Softwaresparte weiter aus.

Einkauf: 33 Millionen US-Dollar lässt Open Text springen, um Cordys zu übernehmen. Mit dem Zukauf der Firma stockt der kanadische Softwarekonzern sein BPM-Portfolio (Business Process Management) auf. Cordys BOP (Business Operations Platform) haben die Niederländer von Grund auf für den Einsatz in der Cloud konzipiert.

Einsatz: IBM setzt die Einkaufstour fort und verleiht sich weiterhin kleinere Softwareschmieden ein. Dieses Mal trifft es Trusteer; die Firma mit Wurzeln in Israel ist im Bereich Sicherheitssoftware aktiv. Als Teil der Übernahme plant IBM, ein Cybersecurity-Labor in Israel mit mehr als 200 Forschern und Entwicklern aufzubauen.

Geldspritz: Goldman Sachs & Co hat in SugarCRM 40 Millionen US-Dollar investiert. Das Unternehmen hinter der gleichnamigen Open-Source-Software für Customer-Relationship-Management (CRM) will mit den Mitteln den internationalen Ausbau vorantreiben.

Rückkauf: Michael Dell darf seine Firma kaufen. Der Gründer plant, den PC-Hersteller von der Börse zu nehmen und zu einem Software- und Service-Anbieter umzubauen.

Entlassung: Trotz Zuwächsen bei Umsätzen und Gewinn im Geschäftsjahr 2013 entlässt Cisco rund 5 % seiner Angestellten. Grund für den Abbau sind die enttäuschenden Aussichten des Konzerns, die Wachstumsprognose musste der Netz-Ausrüster von 7 % auf 3 % bis 5 % reduzieren.

Telekom investiert in den Netzausbau

In diesem Jahr will die Deutsche Telekom 3,4 Milliarden Euro in den Ausbau des Glasfaser-Netzes stecken, 2014 und 2015 sind weitere Investitionen in Höhe von 4,1 Milliarden beziehungsweise 4,3 Milliarden Euro geplant. „Kein anderes Telekommunikationsunternehmen investiert so viel wie die Deutsche Telekom“, lobt der scheidende Chef René Obermann seinen Noch-Arbeitgeber. Im feinsten Marketingdeutsch sprechen die Verantwortlichen des Bonner Konzerns von der „größten Baustelle für Deutschlands Zukunft“ und verweisen

auf die rund 25 600 Gruben für 3500 Kilometer Glasfaser im laufenden Jahr. 2014 sollen Arbeiter auf über 52 000 Baustellen buddeln und mehr als 6250 Kilometer in die Erde bringen.

Derzeit sind rund 12 Millionen Haushalte an das Glasfaser-Netz der Deutschen Telekom angeschlossen, im Zuge des Ausbaus sollen in diesem Jahr weitere 800 000 dazukommen und bis Ende 2016 will man rund 24 Millionen Haushalte mit versorgen.

Das bedeutet jedoch keineswegs, dass die Glasfaser bis zum Gebäude des Normalbüro-

gers (FTTH/FTTB) kommt – sie endet am Kabelverzweiger (Kvz), der sich in den grauen Kästen am Straßenrand befindet. Für die letzte Strecke muss weiterhin die vorhandene Teilnehmeranschlussleitung (Kupfer-Ader) erhalten, die mit Hilfe des Vectoring bis zu 100 Mbit/s Download-Geschwindigkeit bereitstellen soll. An den Plänen für den leistungsstärkeren, kostenintensiveren FTTH-Ausbau hält die Telekom nach eigenem Bekunden zwar fest, der Schwerpunkt läge jedoch auf der Vectoring-Technik. (fo)

Servermarkt in Europa schwächtelt weiter

Die US-amerikanische Marktforschungsfirma Gartner hat für das zweite Jahresquartal Zahlen zum Servermarkt weltweit und in der Region EMEA (Europa, Naher Osten und Afrika) vorgelegt. Danach zählten die Analysten weltweit 2,46 Millionen ausgelieferte Serversysteme. Gegenüber dem Vorjahreszeitraum wuchs der Absatz um 4 %. Von den steigenden Verkaufszahlen profitierten die Hersteller kaum, da gleichzeitig die Einnahmen um 3,8 % auf 12,351 Milliarden US-Dollar schrumpften. Mit anderen Worten: Firmen kaufen vornehmlich preiswerte Modelle. Analyst Jeffrey Hewitt macht den Herstellern wenig Hoffnung, dass sich die konjunkturelle Großwetterlage künftig großartig verändert. „Der weltweite Servermarkt bleibt in relativ schwacher Verfassung“, lautet sein ernüchternder Kommentar. Einzig die Regionen Asien/Pazifik und Kanada wiesen im zweiten Quartal ein Plus sowohl beim Umsatz als auch bei den Auslieferungen auf.

Wie in den vergangenen Quartalen legten x86-Server bei den Stückzahlen (4,5 %) und Einnahmen (2,1 %) zu. Die Geschäfte im Segment der RISC/Itanium-basierten Unix-Server entwickelten sich einmal mehr rückläufig. Die Absatzzahlen brachen hier um 27,2 %, die Erlöse um 25,3 % ein. In guter Verfassung mit einem Umsatzplus von 6,9 % zeigte sich dagegen das Segment der „anderen“ Prozessoren, das Mainframes dominieren.

Spitzenreiter unter den Herstellern nach Einnahmen blieb IBM mit 3,2 Milliarden US-Dollar Umsatz, gerade wegen des starken Mainframe-Geschäftes. Es folgen HP (3,1 Mrd. US-Dollar) und Dell (2,2 Mrd. US-Dollar). Nach Stückzahlen behielt HP die Poleposition mit einem Marktanteil von 23,9 %. Dell rückte bis auf 1,5 Prozentpunkte heran, IBM folgt abgeschlagen mit 8,5 %. In den Top 5 der führenden Stückzahliefieranten taucht mit Inspur ein hierzulande weitgehend unbekannter Name auf. Der chinesische Hersteller verdankt den „Aufstieg“ vor allem einem umfangreichen Ab-

schluss im Hochleistungsrechner-Segment im Heimatland.

Schlechter als der weltweite Gesamtmarkt entwickelten sich die Servergeschäfte in EMEA. Die Hersteller fanden im zweiten Quartal lediglich für rund 550 000 Systeme Abnehmer – knapp 6 % weniger als im Vorjahr. Der Umsatz entwickelte sich ebenso rückläufig und belief sich auf 3,1 Milliarden US-Dollar (-4,6 %). Dell und Fujitsu erzielten unter den führenden Anbietern als Einzige ein Plus bei den Einnahmen, bei den Auslieferungen sind dies Dell und Cisco. In beiden Aufstellungen führt HP die Liste an.

(fo)

EMEA: Serverumsätze in Millionen US-Dollar...

Unternehmen	Q2/2013	Marktanteil	Q2/2012	Marktanteil	Veränderung
HP	1045,013	33,6 %	1212,283	37,2 %	-13,8 %
IBM	834,807	26,8 %	843,044	25,8 %	-1,0 %
Dell	434,887	14,0 %	404,780	12,4 %	7,4 %
Oracle	193,523	6,2 %	221,782	6,8 %	-12,7 %
Fujitsu	175,821	5,7 %	175,424	5,4 %	0,2 %
Übrige	426,488	13,7 %	404,068	12,4 %	5,5 %
Gesamtmarkt	3110,538	100,0 %	3261,401	100,0 %	-4,6 %

... und Auslieferungen

Unternehmen	Q2/2013	Marktanteil	Q2/2012	Marktanteil	Veränderung
HP	222016	40,3 %	243285	41,6 %	-8,7 %
Dell	114057	20,7 %	112997	19,3 %	0,9 %
IBM	47550	8,6 %	56637	9,7 %	-16,0 %
Fujitsu	24325	4,4 %	31945	5,5 %	-23,9 %
Cisco	14484	2,6 %	10300	1,8 %	40,6 %
Übrige	128105	23,3 %	130140	22,2 %	-1,6 %
Gesamtmarkt	550537	100,0 %	585304	100,0 %	-5,9 %

Vodafone verkauft USA-Geschäft an Verizon

Viel Geld in der Hand hat Vodafone durch den Rückzug aus Verizon Wireless. Für die Anteile erhalten die Briten insgesamt 130 Milliarden US-Dollar – umgerechnet rund 100 Milliarden Euro. Von der Summe bezahlt der Mutterkonzern Verizon knapp 59 Milliarden US-Dollar in bar, 60,2 Milliarden

wechseln in Form von Verizon-Aktien den Besitzer. Die restlichen Milliarden wollen die Unternehmen im Zuge kleinerer Finanztransaktionen „tauschen“. Vodafone hatte um die Jahrtausendwende gemeinsam mit Verizon die Mobilfunk-Tochter gegründet und hielt 45 % an dem Joint Ven-

ture. Viel zu sagen hatten die Briten jedoch nicht, obwohl sie sich stets um mehr Mitsprache mühten. Immerhin partizipierten sie an den gut laufenden Geschäften von Verizon Wireless: Rund die Hälfte des operativen Gewinns von Vodafone weltweit stammte von der Beteiligung. Der Gewinnabfluss

war Partner Verizon jedoch stets ein Dorn im Auge. Frühere Versuche sich zu trennen scheiterten an unterschiedlichen Preisvorstellungen beider Firmen. Vodafone will das Aktienpaket sowie rund 24 Milliarden US-Dollar in bar im Frühjahr 2014 unter den Aktiengesellschaften verteilen. (fo)

HP kommt nicht auf die Beine

Auch unter der Regentschaft von Meg Whitman schafft es HP nicht, auf Wachstumskurs zu kommen. Die finanziellen Zahlen des dritten Geschäftsjahresquartals, das am 31. Juli zu Ende ging, fielen alles andere als erfreulich aus: Der Umsatz ging um 8 % auf 27,2 Milliarden US-Dollar zurück. Besonders bitter für den Konzern war, dass er bis auf eine Ausnahme in allen Bereichen einen Einnahmeneinbruch verzeichnete. Selbst die für HPs Revitalisierung als bedeutend eingestuften Geschäftsfelder der Server und Services verbuchten deutliche Rückgänge. Die Einnahmen der Enterprise Group, zu denen das Servergeschäft zählt, fielen mit 5,8 Milliarden US-Dollar gegenüber dem Vorjahr um 9 % niedriger aus, die Service-Sparte schrumpfte ebenso stark auf 5,8 Milliarden US-Dollar Umsatz.

Dabei nahm HP mit anwendungsbezogenen Services 11 % weniger ein, im traditionellen Outsourcing-Segment betrug das Minus 7 %. Die Personal-Systems-Sparte steuerte noch 7,7 Milliarden US-Dollar (-8 %) zum Einsatz bei, der Bereich Druck-Lösungen 5,8 Milliarden US-Dollar (-4 %). Die kostspielig zusammengekauften Softwareabteilung wuchs gerade einmal um 1 % auf knapp 880 Millionen US-Dollar.

Immerhin erzielte HP im Quartal wieder einen Gewinn (1,39 Mrd. US-Dollar). Vor einem Jahr sorgte noch eine Abschreibung für einen gigantischen Verlust von knapp 9 Milliarden US-Dollar: Das Unternehmen sah sich gezwungen, den Buchwert des aufgekauften IT-Serviceanbieters EDS deutlich nach unten zu berichtigen. (fo)



Private Cloud

Unser Angebot:

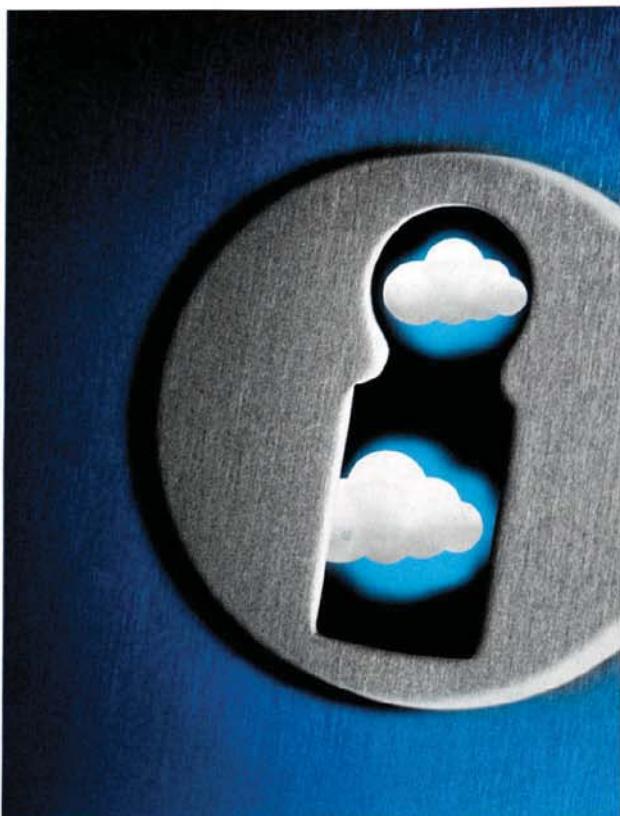
- Konzeptworkshop
- Installation & Konfiguration
- Individuelle Anpassung
- Test der Umgebung
- Übergabeworkshop

OpenStack ist eine offene Infrastruktur as a Service (IaaS) Lösung zur Umsetzung von Public & Private Clouds, welche eine flexible Wahl der Infrastrukturkomponenten wie z.B. die Virtualisierungslösung oder das Storage Backend ermöglicht.

B1 Systems ist an der OpenStack Entwicklung seit 2011 aktiv beteiligt und wir implementieren auch Ihre Umgebung zu einem **Festpreis!**

Gern informieren wir Sie auch zu weiteren Themen wie z.B. Software Defined Networking mit Open vSwitch oder Block & Object Storage mit dem Ceph Storage Cluster.

Bitte schicken Sie uns einen Terminvorschlag für ein persönliches Telefonat an
info@b1-systems.de



Cloud-Provider-Auswahl
angesichts der NSA-Affäre

Kontrolle ist besser

Monika Ermert

Dass US-amerikanische Anbieter nicht den nach deutschem Recht erforderlichen Datenschutz bieten können, hat sich nicht erst seit der NSA-Affäre herumgesprochen. Doch ist Cloud made in Germany die Lösung? Ein paar unbequeme Antworten und aktuelle Überlegungen zur Provider-Auswahl.

Jeden Tag meldet die Initiative „Cloud Services made in Germany“ derzeit ein neues Mitglied. Deutsche Mail-Provider versprechen unter dem Beifall des Bundesamts für Sicherheit in der Informationstechnik eine abhörsichere Mail. Die Enthüllungen des Ex-US-Geheimdienstmitarbeiters Edward Snowden zeigen ganz offensichtlich Wirkung. Aber wie sicher kann die deutsche Wolke angesichts der technischen und wirtschaftlichen Verflechtungen der Anbieter überhaupt sein?

Spätestens seitdem die US-Firmen Lavabit und Silent Circle, beide Anbieter kryptografisch gesicherter E-Mail, das

Handtuch geworfen haben, ist klar, dass in der US-amerikanischen Cloud Sicherheit sehr relativ ist.

Cloud-Anbieter unter US-Recht

Denn Lavabit hatte den Stecker gezogen, nachdem die US-Behörden den Firmengründer Radar Levison per Foreign-Intelligence-Surveillance-Act-Anordnung (FISA) zur Preisgabe der Kommunikationsdaten seiner Kunden, unter ihnen laut Levison auch Edward Snowden selbst, verpflichtet hatten. In einem bemerkens-

werten Interview mit dem Bürgerrechtskanal Democracy Now machte Levison die Situation der US-Anbieter klar, die per FISA-Anordnung nicht nur zur Kooperation, sondern auch zum Stillschweigen darüber verpflichtet sind. Lavabit sei nicht der erste Dienst-Provider, der eine solche Anordnung erhalten habe, und nicht der erste, der sie bekämpfe.

Weil aber sichere E-Mail sein einziges Angebot war, ist damit das Geschäftsmodell zerschlagen. Levison hofft immer noch, dass es in Zukunft für US-Unternehmen wieder möglich ist, einen privaten Cloud-Dienst zu betreiben, ohne zu geheimen Abhörmaßnahmen gezwungen zu sein. Aber – und da wird der Fall über die USA hinaus interessant – auch eine Verlagerung ins Ausland beziehungsweise nur der Betrieb auf Nicht-US-Servern schützt seinen Dienst nicht, solange er seinen Wohnsitz in den USA nicht aufgeben wolle. Denn kein Cloud-Unternehmen mit US-Bezug sei vor den Zugriffen sicher.

Fast jeder US-Bezug kann erpressbar machen

Deutsche Diensteanbieter wittern angesichts dieser Entwicklungen Morgenluft. Nacheinander meldete die Initiative Cloud

TRACT

- Die NSA-Affäre hat noch einmal deutlich gemacht, dass sensible Informationen bei US-amerikanischen Cloud-Anbietern nicht sicher sind.
- Ein Standort der Cloud-Rechenzentren außerhalb der USA ist keine hinreichende Sicherheitsgarantie, der Betreiber darf auch nicht durch finanzielles oder persönliches Engagement in den Vereinigten Staaten erpressbar sein.
- Auch in der Europäischen Union ist der Datenschutz nicht immer ausreichend, und das nicht nur wegen der britischen Sonderrolle.
- Wo „Made in Germany“ draufsteht, ist oft nicht mehr als ein juristisches Versprechen drin. Wichtig sind vertraglich festgelegte Geldbußen beim Bruch der Vertraulichkeit.

Rechtlicher Schutz auch in der EU unzureichend

Die empfohlenen Vorsichtsmaßnahmen sind letztlich auch ein Ausdruck dafür, dass der viel gelobte rechtliche Schutz innerhalb der EU noch zu wünschen übrig lässt. Der dortige Status quo reicht noch nicht aus, um echte Sicherheit in der EU-Cloud zu garantieren. So zumindest das Fazit der Experten eines groß angelegten EU-Projekts zur Sicherheit in der Cloud, SECCRIT (SECure Cloud computing for CRitical infrastructure IT).

Seccrit soll unter anderem die Verträglichkeit der Auslagerung öffentlicher Daten in die Cloud erörtern. Eines der praktischen Beispiele ist der Zugriff auf per Cloud verfügbar gemachte Videoüberwachungsdateien in europäischen Städten. Staatliche Überwachung als eigenes Bedrohungsszenario steht, zumindest bislang, in den Arbeiten eher im Hintergrund. Unter anderem wird überlegt, wie Auffälligkeiten, insbesondere widerrechtliche Zugriffe, erkannt und gerichtsfest dokumentiert werden können.

Im ersten Bericht zu den Rechtsfragen der EU-Cloud verweisen Frank Pallas und Silvia Balaban vom Karlsruher Institut für Technologie (KIT) vor allem auf Mängel bei der Transparenz und Schwächen bei der Zuweisung von Verantwortlichkeiten. Für das typische Ineinandergreifen verschiedener Dienstleistungen im Cloud Computing – Nutzer, Cloud-Anbieter und -dienstleister, weitere Infrastrukturpartner – müssten zusätzliche Regeln gefunden werden, die eine verteilte Verantwortlichkeit abbilden. Der aktuelle Entwurf der künftigen Datenschutzgrundverordnung, der jetzt in die heiße Phase geht, schaffe da keine Abhilfe.

Im Gegenteil: Über die derzeit nach EU-Datenschutzrecht durchaus legale Weitergabe von Daten an Drittstaaten mindestens in der EU

wird noch gerungen. Die Kommission und Teile des Parlamentes drängen laut Beobachtern darauf, dass es der Genehmigung durch den Endnutzer bedarf, die Abrechnung an Dritte auszulagern. Doch diese Ansicht teilen längst nicht alle Straßburger Parlamentarier, und schon gar nicht viele Regierungen und Branchenvertreter der Banken und Versicherungen. Sie wollen keinen harten Ausschluss von Dritten. So gibt es in den weit über 3000 Änderungsanträgen derzeit durchaus Vorschläge, vor allem von konservativer Seite, keine verbindliche Auskunftspflicht etwa über Speicherfristen von Daten vorzusehen. Denn das sei ja für einen Cloud-Provider nicht immer möglich.

Doch mit jedem weiteren Paket aus Edward Snowdens Pandora-Büchse nimmt der Druck auf den EU-Gesetzgeber weiter zu. EU-Vizekommissionschefin und Justizkommissarin Viviane Reding, die sich schon vorher damit unbeliebt gemacht hatte, für in der EU tätige US-Dienstleister auch EU-Datenschutz einzufordern, favorisiert empfindliche finanzielle Strafen. Bußen von bis zu zwei Prozent des Umsatzes sollen im Fall von Verstößen gegen die neue Verordnung fällig werden. Die Lobbyschlacht darum dürfte im Herbst eine neue Runde gehen.

Reding warnte inzwischen eindringlich davor, die finanziellen Strafandrohungen zu verwässern – und erklärte mit Blick auf Großbritannien gleichzeitig, dass man auf Einstimmigkeit nicht mehr setze. Per Mehrheitsentscheid will sie scharfe Bestimmungen durchsetzen. Sollte es am Ende wirklich teuer werden, mit Cloud-Daten zu schlampen oder sie gleich per Backdoor einem US-Geheimdienst zur Verfügung zu stellen? Dass die neue Grundverordnung die Sicherheits- und Datenschutzfragen der „Wolke“ komplett auflöst, mag man kaum glauben.

Services made in Germany die Neumitglieder Terrabit Reutlingen, Stemmer, Olching und den Frankfurter High-Performance-Hoster proLO, die allesamt klassische IT-Infrastruktur-Dienste bieten. Security-Spezialist Ubique Technologies warb vollmundig, man habe die Antwort auf Prism und biete sichere E-Mail à la Lavabit, ohne sich jedoch von US-Unternehmen einschüchtern zu lassen.

Die Deutsche Telekom und United Internet kündigten ebenfalls sichere, verschlüsselte E-Mail an. Doch leider bleibt „E-Mail made in Germany“ auf die Absicherung der Übertragung zwischen den beteiligten Diensten – und innerhalb Deutschlands – beschränkt, inklusive Zwischendurch-Auspicken beim Provider wegen Malware-Scan. Von Ende-zu-

Ende-Verschlüsselung also keine Spur. Dementsprechend erntete das mit großem Marketingaufwand gestartete Angebot in Fachkreisen viel Spott, der Chaos Computer Club sprach vom „Sommermärchen von der sicheren E-Mail“.

Wie deutsch ist die „German Cloud“?

Technische Details sind auch nicht die Sache der Made-in-Germany-Cloud-Initiative. Dem Club kann jeder beitreten, der dem Kunden einen Vertrag nach deutschen Recht, im Klagefall einen deutschen Gerichtsstand und eine deutsche Support-Hotline anbietet. Wo in Anspruch genommene Dienste gehostet sind oder über



AHA-EFFEKT GESUCHT?

Schulungen für Linux-Admins, die durchblicken wollen.

Fachlich und didaktisch kompetente Dozenten, spannende Schulungsthemen, eine lockere Atmosphäre im Kurs und angenehme Unterrichtsräume – all das erwartet Sie bei uns in Berlin an der Heinlein Akademie.

Die nächsten Kurse:

ab 21.10.
HA-Virtualisierungscluster mit KVM

ab 28.10.
Cyrus IMAP-Server

ab 28.10.
Linux Performance Analyse & Tuning

ab 30.10.
Puppet Fundamental Course

ab 04.11.
Bacula / Bareos Administration Level 1

ab 04.11.
Linux Admin Grundlagen

ab 04.11.
IPv6 - Einführung im Unternehmen

heinlein akademie

10 Fragen an den Cloud-Anbieter

Ehe man sich die Mühe macht, ins Detail zu gehen und etwa die im Artikel erwähnte 300-Punkte-Checkliste von René Büst abarbeitet, kann man mit diesen Fragen die Angebote vorsortieren:

1. In welchem Land stehen die für das Cloud Computing genutzten Rechenzentren?
2. In welchen Staaten ist der Cloud-Betreiber selbst beziehungsweise eine Tochter- oder Muttergesellschaft geschäftlich aktiv?
3. Wo ist der Firmensitz des Anbieters?
4. Wo ist der Gerichtsstand?
5. Teilt der Cloud-Betreiber dem Kunden mit, wenn es einen Zugriff von Behörden auf die Daten gab oder gibt?

6. Wird offengelegt, ob und wenn ja welche Drittanbieter für den Dienst in Anspruch genommen werden?

7. Inwiefern wird über Verstöße der Drittanbieter gegen deutsches Datenschutzrecht informiert?

8. Erhält man als Kunde eine vollständige, aktuelle und detaillierte Liste der für den Cloud-Service eingesetzten Hard- und Software?

9. Werden alle Verträge nach deutschen Recht geschlossen?

10. Wie hoch ist die Konventionalstrafe bei einem Verstoß gegen deutsches Datenschutzrecht oder die vereinbarten Vertraulichkeitsbestimmungen?

terstrich Christian Speck vom Reutlinger SAP-Dienstleister Abilis. Dass diese Vorschriften nicht erst seit dem Patriot Act gelten, sondern schon 1978 im Foreign Intelligence Surveillance Act festgeschrieben wurden, ist dabei nur am Rande von Interesse.

Druckmittel gegen EU-Provider?

Eine deutsche oder EU-Cloud wäre ein gutes Label, sagen Experten wie Caspar Bowden, ehemals Datenschutzbeauftragter beim Microsoft-Konzern. Bowden, der mittlerweile als unabhängiger Datenschutzexperte ein skeptisches Auge auf die Branche wirft, hält die Druckmittel einer datengierigen US-Regierung gegenüber Unternehmen mit Geschäftsinteressen in den USA allerdings gleichzeitig für nicht unerheblich. Große, international agierende Telekommunikationsunternehmen seien dem Druck durch US-Behörden besonders ausgesetzt.

„Ein europäisches Mobilfunkunternehmen, das etwa ein rivalisierendes Unternehmen in den USA übernehmen will und dafür die Zustimmung der US-Regierung braucht – da steht einiges auf dem Spiel“, so Bowden gegenüber iX. In einer Anhörung zum Cloud Computing im US-Kongress etwa habe der republikanische Kongressabgeordnete Bob Goodlatte kürzlich eine entsprechende Bemerkung in Bezug auf T-Mobile fallen lassen.

Ein Lobbyist des Information Technology and Innovation Foundation (ITIF) warnte in derselben Sitzung vor der offenen Abwerbung von US-Kunden durch EU-Anbieter. Ausländische Regierungen würden vor US-Anbietern warnen und der US-Wirtschaft schaden. Die deutsche Telekom verweise auf den Patriot Act als Grund, warum Kunden ihre und nicht die Dienste von US-Provider nutzen sollten. Das gefällt US-Politikern natürlich nicht. Verluste in Milliardenhöhe prognostizierte der Lobbyist, und US-Abgeordnete und Journalisten beklagen schon nicht WTO-konforme Handelshemmnisse.

Abgestufter Zugriff für die Dienste

EU-Unternehmen, besonders die strengen Datenschutzbestimmungen gewohnten deutschen Anbieter, würden umfanglichen Hintertüren in ihren Diensten sicherlich ebenso skeptisch gegenüberstehen wie

welche Systeme sie laufen, ist kein Kriterium.

Von einer German Cloud im Sinne einer deutschen Infrastruktur zu sprechen, sei sicherlich Quatsch, meint denn auch Ditmar Tybussek vom Systemhaus Allgeier IT Solutions in einer Interviewsammlung der Initiative. Das Label „Made in Germany“ sichere aber, dass deutsche und europäische Rechtsstandards eingehalten werden. Allgeier bietet die unter anderem vom Bundesamt für Sicherheit in der Informationswirtschaft genutzte Cloud-Anwendung JULIA MailOffice an.

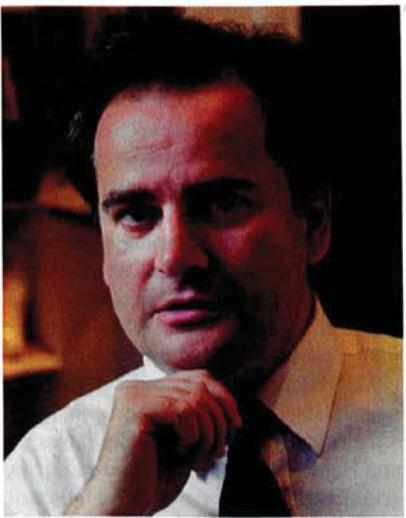
In erster Linie bedeute German Cloud eine Art „Gütesiegel für Sprache, Support und Datensicherheit“, meint Thorsten Lenk, Vorstandsmitglied bei der Darmstädter 5 POINT AG, die unter anderem die Groupware teamspace als Cloud-

Dienst anbietet. Selbst wenn Daten „vielleicht nicht auf deutschen Servern gehalten werden“, sei ein deutscher Anbieter für die Sicherheit der Daten nach deutschen Gesetzen verantwortlich, unterstreicht auch Andreas Schwarze, Leiter Marketing und Business Development von Oventis, die eine in einem TÜV-zertifizierten Rechenzentrum gehostete Beschaffungslösung anbietet.

Eine Reihe der German-Cloud-Mitgliedsunternehmen nennen allerdings eine strikt auf Deutschland beschränkte Datenverarbeitung und -haltung – vorzugsweise in eigenen Rechenzentren – für sensible Informationen als Kernbestandteil eines deutschen Cloud-Angebots. Denn der Patriot Act zwingt US-Anbieter, Daten an das FBI zu geben, selbst wenn diese in europäischen Rechenzentren liegen, un-



Kein Cloud-Unternehmen mit US-Bezug ist sicher: Ladar Levison, Lavabit, mit seinem Anwalt bei Democracy Now (Abb. 1).



Nicht unerhebliche Druckmittel der US-Behörden: Caspar Bowden, Ex-Microsoft-Datenschutzbeauftragter (Abb. 2)

Check aussehen kann, hat der Kieler Analyst und Cloud-Experte Rene Büst aufgeschrieben (siehe „Alle Links“).

Rund dreihundert Fragen zu technischen, rechtlichen, vertraglichen Aspekten legt er Entscheidern nahe, wenn sie einen Cloud-Dienst für ihr Unternehmen auswählen wollen. Neben ganz praktischen Dingen wie Ausfallsicherheit und Transparenz oder Portabilität und gesichertem Löschen von Daten sollten Kunden auch folgende Fragen stellen:

- Kann der Anbieter nachweisen, dass er sich an die Datenschutzbestimmungen hält?
- Wer hat Zugriff auf die Daten, und gibt der Anbieter an, wer Zugriff auf die Daten hat?
- Macht der Anbieter auch transparent, ob ein Staat Zugriff auf die Daten hat?

Gerade durch Gesetze verschiedener Länder geregelte Zugriffe von Behörden werden häufig nicht als Teil des klassischen Bedrohungsszenarios einkalkuliert, unterstreicht auch Bowden. Kunden sollten daher darauf achten, dass bei Audits mögliche Zugriffe ausländischer Behörden oder Strafverfolger (nach dem jeweiligen Landesrecht) mit unter die Lupe genommen werden.

Kontraindiziert sei auf jeden Fall, sich auf Provider zu verlassen, die Datenschutz nach dem Safe-Harbor-Prinzip Cloud-Dienste anbieten. Die Safe-Harbor-Labels, die eher kursorisch zusichern, dass ein US-Provider einen den EU-Datenschutzstandards vergleichbaren Schutz bietet, sind mit den Enthüllungen zu Überwachungsmaßnahmen in den USA endgültig als wertlos in Verruf gekommen.

Bowdens vielleicht wichtigste Empfehlungen sind harte Schadensersatzpflichten für den Fall, dass Daten an ausländische staatliche Stellen weitergegeben werden, eine Garantie, dass der Anbieter keine Session Keys loggt, und eine nachvollziehbare, am besten per Open-Source-Software realisierte Datenlegung über alle Abläufe. (js)

Lavabit, schätzt Bowden. Gezielte Anfragen nach einzelnen Session Keys, der Mailbox oder anderen gespeicherten Daten eines bestimmten Kunden – unter dem jeweiligen nationalen Recht – würden aber wohl auch sie zustimmen, fürchtet der Brite. Das Anzapfen von Datenleitungen per Fasersplit sei aus Sicht mancher Provider möglicherweise sogar das Einfachste.

Am Ende hänge viel von der Integrität und Courage des Managements ab. Große Telekommunikationsunternehmen, die international aktiv sind, würden am ehesten akzeptieren, dass „so das Geschäft in den USA eben läuft“.

Bowden unterstreicht die Notwendigkeit einer klaren Differenzierung zwischen reinen Storage-Lösungen einerseits und den als Cloud-Dienst beworbenen Software-as-a-Service-Angeboten. Für Letztere entfällt die Möglichkeit der durchgehenden harten Verschlüsselung. Traut man einer Microsoft-Software-Lösung noch, gleich ob im deutschen Rechenzentrum gehostet oder nicht, nachdem Snowden das Unternehmen als überaus bereitwillig in der Zusammenarbeit mit US-Behörden geoutet hat? „Trauen sie niemandem“, rät Bowden. Immerhin böten Open-Source-Lösungen in gewisser Weise mehr Schutz vor etwaigen Hintertüren als proprietäre Software.

Vorsichtsmaßnahmen für Cloud-Kunden

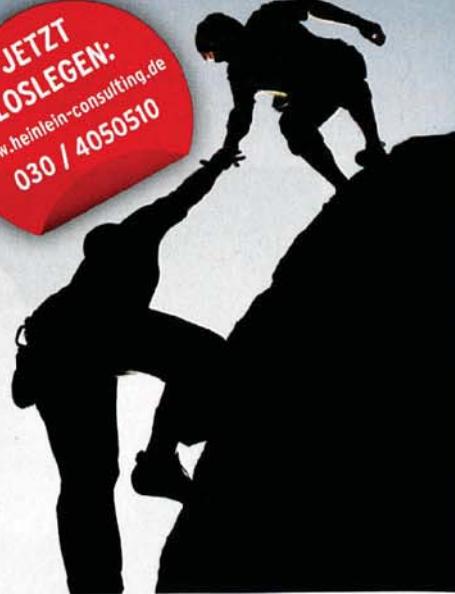
Er rät dazu, die Verträge für Cloud-Dienste sehr genau daraufhin zu prüfen, wie die Datenverarbeitung über die verschiedenen Schichten hinweg – vom direkten Cloud-Anbieter über externe Dienstleister und in Anspruch genommene TK-Anbieter – organisiert ist. Wie ein umfangreicher

Monika Ermert

ist freie Journalistin mit dem Schwerpunkt Internet-Politik.

Alle Links: www.iz.de/iz1310042

JETZT
LOSLEGEN:
www.heinlein-consulting.de
030 / 405050



LINUX SORGENFREI

Linux-Projekte von einem Team, das Sie glücklich macht.

FACHLICH GUT.

„... unterstützt uns seit einigen Jahren fachkundig und rund um die Uhr bei Betrieb und Troubleshooting unserer für den Flugbetrieb wichtigen Linux-Cluster.“

Germanwings, Markus Haake, Head of IT-Infrastructure

EFFIZIENT.

„... lange Diskussionen und Planungen waren unnötig. Die Heinleins haben mit ihrer Erfahrung ein überzeugendes Konzept fertig auf den Tisch gelegt.“

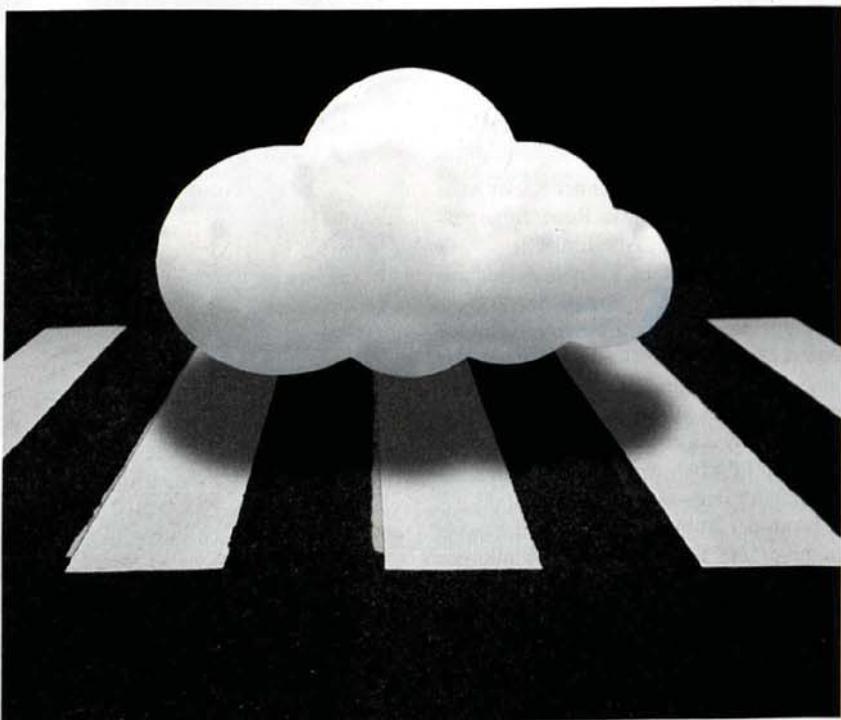
Strato, Marcus Lindner, Head of Corporate Network/Office-IT

ZUVERÄSSIG.

„... innerhalb der recht sportlichen Vorgabe von zwei Wochen wurden alle Punkte umgesetzt.“

XING, Holger Bürger,
Director Site Operations

heinlein
consulting



Erfolgreich verschlüsseln trotz NSA, GCHQ & Co.

Gesicherter Übergang

Michael Hamm, Susanne Nolte

Viel diskutiert ist bisher die Frage, wie sicher die Daten in der Cloud sind, weniger, ob das auch auf die Übertragung zutrifft. Das werden die neuesten Veröffentlichungen über die Entschlüsselfähigkeiten der NSA sicher ändern.

Erst im September enthüllten Guardian, New York Times und ProPublica, in welchem Umfang und mit welcher Systematik sich die US-amerikanische NSA (National Security Agency) und das britische GCHQ (Government Communications Headquarters) der Aufgabe widmen, verschlüsselte Internetdaten auszulesen und zu welchen Methoden sie greifen (s. „Alle Links“). Ziele der Angriffe sind laut Guardian etwa E-Mails, Banking- sowie medizinische Daten. Im Fokus des NSA-Projekts Bullrun und des

GCHQ-Projekts Edgehill stehen SSL/TLS- (Secure Socket Layer/Transport Layer Security) und VPN-Verbindungen (Virtual Private Network), VoIP (Voice over IP) und mobile 4G-Netze [1].

Um die Daten solcher vor allem von Firmen und Behörden benutzten Übertragungen abzuzapfen und zu entschlüsseln, haben laut Guardian die Geheimdienste ein ganzes Arsenal an Techniken zur Hand. Beispielsweise ist die NSA-Abteilung TAO (Tailored Access Operations) darauf spezialisiert, sich Zugang zu Sys-

temen an den End- und Zwischenpunkten der Verschlüsselungsstrecken zu verschaffen, auf denen sie die noch nicht oder nicht mehr verschlüsselten Daten abgreifen. Zu den Methoden zählt nicht nur das Einbrechen in die Zielserver und Ausgangsnetze der Internetkommunikation, sondern etwa auch das Installieren von Weichen an den Knotenpunkten und Hubs der Telekommunikations-Provider.

In einem anderen eigens geschaffenen und mit 250 Millionen US-Dollar pro Jahr finanzierten Programm bindet die NSA verstärkt US- und andere Hersteller ein, um Backdoors oder Trapdoors in deren kommerzielle Verschlüsselungssoft- und Hardware einzubauen, deren Zugänge nur die involvierten Geheimdienste kennen. Zum Vergleich: Das vielzitierte Programm Prism hat einen jährlichen Etat von 20 Millionen US-Dollar. Unter anderem war bereits bekannt geworden, dass Microsoft in Partnerschaft mit der NSA entsprechende Lücken in den E-Mail- und Chat-Dienst Outlook.com eingebaut hat und seine Produkte grundsätzlich so designt, dass sie „existing or future lawful demands“ entsprechen. Zudem hat ein GCHQ-Team Wege entwickelt, den verschlüsselten Datenverkehr der „Big Four“, Hotmail, Google, Yahoo und Facebook, mitzulesen.

Vorsätzlich unsicher

Eine weitere Methode, die Sicherheitsexperten schon lange vermuteten und für die nun erstmals Beweise vorliegen, ist das Einbauen von Schwachstellen in Sicherheitsstandards etwa des NIST (US National Institute of Standards and Technology). Dasselbe gilt für das nachträgliche Entschlüsseln gesammelter Daten per Brute Force auf eigenen Supercomputern.

Laut einem GCHQ-Dokument, das der Guardian zitiert, arbeitet die NSA bereits seit zehn Jahren massiv daran, die Verschlüsselung von Daten auszuhebeln: „For the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet encryption technologies“ [1]. Dieses Zehn-Jahres-Programm habe 2010 zu einem Durchbruch geführt, durch den eine enorme Menge („vast amounts“) Daten, die zuvor verworfen wurden, „exploitable“ sind.

Ursache ist aber nicht, dass NSA & Co. die Verschlüsselungsalgorithmen geknackt hätten, sondern sie die scheinbar starke Sicherheit in Implementierungen abschwächen und sich damit das Entschlüsseln vereinfachen. Grundsätzlich gilt weiterhin: „Encryption works. Pro-

perly implemented strong crypto systems are one of the few things that you can rely on", zitiert der Guardian Edward Snowden. Leicht kompromittierbar sind dagegen lückenhafte Sicherheit und ein fahrlässiger Umgang damit.

Das alles hat nicht nur Auswirkungen auf die Verteidigung der Privatsphäre, sondern vor allem auf Firmen, für die solche Enthüllungen ein neues Licht auf die Möglichkeiten der seit Längerem von den Geheimdiensten betriebenen Wirtschaftsspionage wirft. Und das in einer Zeit, in der Cloud Computing immer mehr Verbreitung findet, vor allem bei Unternehmen und Behörden. Im Februar 2013 stellte etwa die ENISA (European Union Agency for Network and Information Security) in ihrem Bericht „Critical Cloud Computing“ fest, dass in naher Zukunft ein Großteil der Unternehmen und Organisationen in irgendeiner Weise von Cloud Computing abhängig sein werden [2]. Deshalb wird das Kompromittieren oder der Ausfall eines einzigen Dienstes möglicherweise einen massiven Impact auf eine sehr große Zahl von Betroffenen haben.

Möglicherweise werden sich in näherer Zukunft sogar die traditionellen kritischen Infrastrukturen wie Energie- und Wasserversorgung, Finanzmärkte, Transport und Verkehr sowie das Gesundheitswesen teilweise auf Cloud-Ressourcen verlassen. Nach Definition der Europäischen Kommission sind alle IT- und Kommunikationssysteme, die entweder essenziell für die Ökonomie und die Gesellschaft eines oder mehrerer Staaten oder essenziell für die Operation einer kritischen Infrastruktur sind, als kritische

Informationsinfrastrukturen (KII) zu betrachten (s. „Alle Links“).

Einige Anbieter verschlüsseln die Verbindung zum Teil schon per Default oder bieten zumindest die Option. Der Zugang erfolgt meist über den Browser. Dort signalisiert ein <https://> anstelle des <http://>, dass die Verbindung authentifiziert – der Client ist tatsächlich mit der richtigen Website verbunden – und die Sitzung Ende-zu-Ende-verschlüsselt ist. Zumindest die Stationen zwischen Client und Server können die Kommunikation nicht entschlüsseln.

Unsichtbare Verschlüsselungsschicht

Zuständig für Authentifizierung und Verschlüsselung ist in solchen Fällen SSL/TLS. Es schiebt sich zwischen den Network Layer (OSI-Schicht 3) und den Transport Layer (OSI-Schicht 4), also zwischen TCP und IP. Damit steht SSL/TLS auch für andere Transport-Dienste zur Verfügung. Mittlerweile gibt es SSL-Varianten beispielsweise von SMTP (SMTPS), IMAP (IMAPS) und FTP (FTPS), die sich aber noch nicht großflächig durchgesetzt haben.

SSL arbeitet für den Anwender unsichtbar und bietet grundsätzlich eine starke Verschlüsselung der übertragenen Daten und eine starke Authentifizierung des Servers gegenüber dem Browser. Entscheidend ist aber der richtige Umgang damit. Gerade die Transparenz birgt Gefahren, die auf den ersten Blick gar nicht ersichtlich sind.

Eine Tücke liegt beispielsweise im Verhalten der Clients beim Überprüfen des SSL-Server-Zertifikats: Sie müssen online überprüfen, ob das vom Server vorgelegte Zertifikat noch gültig ist oder zurückgezogen wurde. Der Webbrowser nutzt normalerweise das OCSP (Online Certificate Status Protocol), um bei der Zertifizierungsstelle nachzufragen.

Die Implementierung von OCSP in den Browsern ist aber „Defective By Design“. Der Client, der eine SSL-Verbindung aufbaut, muss bei der CA (Certificate Authority) anfragen, ob das vom Server gelieferte Zertifikat noch nicht zurückgezogen wurde. Bekommt der Browser aber die Antwort nicht rechtzeitig, muss er das Zertifikat ungeprüft akzeptieren. Gelingt es also einem Angreifer, die Validierung des Zertifikates zu behindern, kann er den Verbindungsauflauf manipulieren, in dem er beispielsweise in einem Man-in-the-Middle-Angriff dem Client ein kompromittiertes



- Sichern kann man Cloud-Daten nur mit einer Ende-zu-Ende-Verschlüsselung.
- Kompromittiert sind nicht die Verschlüsselungsalgorithmen, sondern deren Implementierungen.
- Sicher ist Verschlüsselungs- und Tunnel-Software nur noch dann, wenn die Quellen verfügbar sind.

PAESSLER
the network monitoring company

PRTG Network Monitor sichert Ihre Private Cloud! Ihr Erfolg steht und fällt mit der Effizienz Ihrer IT-Infrastruktur

Darum überwacht PRTG ...

- die Performance der Verbindung zur Cloud.
- alle Systeme und Verbindungen innerhalb der Cloud.
- alle Dienste und Ressourcen aus Sicht des Nutzers sowie des Servers.

Und: Überlastungen Ihrer Cloud können Sie durch langfristige Planung mit umfangreichen Monitoring-Daten vermeiden.



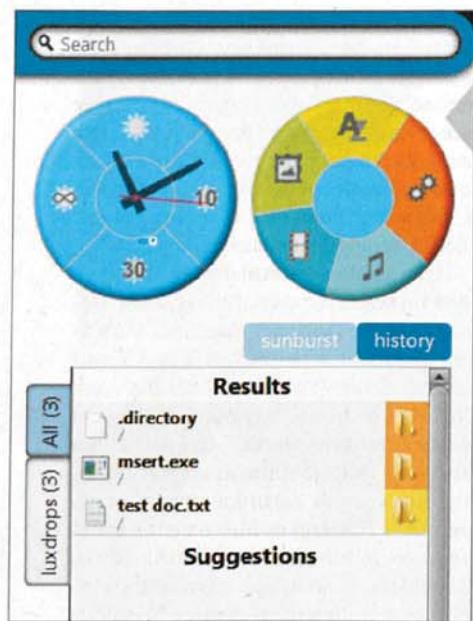
TESTEN SIE PRTG JETZT
KOSTENLOS FÜR 30 TAGE!
www.de.paessler.com/ix-cloud



PRTG
NETWORK
MONITOR

Installiert in Sekunden.
Konfiguriert in Minuten.
Ihr Netzwerk für Jahre im Griff.

Paessler AG • info@paessler.com • www.paessler.de



LuxDrops arbeitet mit einer mehrdimensionalen Suche und mit Ende-zu-Ende-Verschlüsselung, über die der Anwender die volle Kontrolle behält.

und bereits zurückgezogenes Zertifikat unterschiebt.

Ende Juli 2013 veröffentlichte das Online-Magazin CNET die Meldung, dass US-Behörden in Zusammenarbeit mit der NSA massiven Druck auf Internet-Dienst-Anbieter zur Herausgabe des privaten SSL-Schlüssels, des Master Encryption Key ausüben (s. „Alle Links“). Man geht allerdings davon aus, dass große Internet-Firmen dem Druck noch standhalten und die Behörden eine offene Auseinandersetzung vor Gericht scheuen. Kleinere Firmen ohne Rechtsabteilung würden aber vermutlich dem Druck nachgeben müssen.

Zeig mir den Schlüssel

Mit dem privaten Schlüssel können Behörden nicht nur die aktuelle Kommunikation abhören, sondern auch zu einem früheren Zeitpunkt abgefangene Datenströme nachträglich entschlüsseln. Als Schutz davor kennen Verschlüsselungsverfahren, darunter SSL, die Option „Perfect Forward Secrecy“ (PFS), die aber kaum jemand benutzt. PFS verhindert, dass ein Angreifer vergangene Sitzungsschlüssel und damit die Kommunikation rekonstruieren kann, auch wenn er in den Besitz des geheimen privaten Schlüssels gelangt.

SSL benutzt üblicherweise ein symmetrisches Verschlüsselungsverfahren; die zu transportierenden Daten chiffriert es mit

einem temporären Sitzungsschlüssel. Ihn handeln Client und Server für jede Session mit einem Schlüsselaustauschverfahren neu aus. Der Vorteil: Symmetrische Verfahren sind nicht so rechenintensiv und damit auch relativ schnell.

Beim Schlüsselaustausch arbeitet SSL aber mit asymmetrischer Verschlüsselung (Public Key Encryption). Deshalb benutzen viele Implementierungen auch das Private/Public-Paar des Webservers, um direkt den Sitzungsschlüssel mit dem Browser auszuhandeln. Kommt ein Angreifer in den Besitz des privaten Keys, kann er den Schlüsselaustausch, auch von aufgezeichneten Sitzungen, nachvollziehen und damit die jeweiligen Sessionkeys nachberechnen. Liegen die Sitzungsschlüssel vor, ist das Decodieren der aufgezeichneten Daten ein Kinderspiel.

Bei PFS darf SSL den geheimen Key lediglich zum Authentifizieren des Webservers und der Schlüsselaustausch-Daten nutzen. Für den Austausch des symmetrischen Sitzungsschlüssels handeln die Kommunikationspartner hingegen jedes Mal ein neues, temporäres Public/Private-Paar aus. Ist der Schlüsselaustausch abgeschlossen, muss die SSL-Implementierung das temporäre Public/Private-Paar unverzüglich löschen.

Ohne diese temporären Schlüssel sind die aus ihnen erzeugten symmetrischen Sessionkeys selbst mit dem privaten Masterschlüssel nicht mehr rekonstruierbar. Dieses Verfahren ist jedoch deutlich rechenintensiver. Da das mehr Hardware-Ressourcen erfordert, verzichten viele Provider darauf, PFS anzubieten und wählen eine der einfacheren Varianten des Schlüsselaustausches.

Verfahren nach Diffie-Hellman bieten PFS und beginnen in der Webserver-Konfiguration mit „DHE+“. Zwar beherrschen alle gängigen Webserver und Browser „DHE+“, allerdings ist es wesentlich langsamer als der einfache Schlüsselaustausch mit „RSA+“. Der Schlüsselaustausch basierend auf elliptischen Kurven würde die Beeinträchtigungen der Geschwindigkeit beseitigen, setzt allerdings TLSv1.1 voraus und funktioniert nur mit neuen Webbrowsern. Eine Diskussion zum Aktivieren von PFS für Webserver findet sich auf Heise Security (s. „Alle Links“).

Welche Verschlüsselungen zum Einsatz kommen, kann der Anwender beispielsweise im Internet Explorer mit einem einfachen Rechtsklick und dem Auswählen der Seiten-Eigenschaften feststellen. Bei Firefox bekommt man beim Klick auf das HTTPS-Schloss und anschließendem Auswählen von „More Information“ Details über die Parameter der

verschlüsselten Session angezeigt. Informationen zum Schlüsselaustausch sucht man hier aber vergebens. Abhilfe schafft das Add-on Cipherfox, das Firefox um eine Vielzahl an Informationen und Einstellungsmöglichkeiten erweitert. Chrome zeigt die Verschlüsselungsart ohne Hilfsmittel an, Safari nicht.

Auskunft auf vielen Wegen

Sollte sich der Browser zum Verschlüsselungsverfahren ausschweigen, hat man zwei Optionen: Erstens kann man auf die Kommandozeile zurückgreifen und mit den openssl-Tools den Server abfragen:

```
openssl s_client -connect www.google.de:443
```

etwa initiiert eine Verbindung auf dem HTTPS-Port 443. Die Antwort

```
SSL-Session:
  Protocol : TLSv1.2
  Cipher   : ECDHE-RSA-AES128-GCM-SHA256
```

verrät, dass der Server TLSv1.2 verwendet und DHE bevorzugt. Alternativ kann man den Datenverkehr mit Wireshark mitschneiden und die SSL-Sektion des Mitschnitts analysieren.

Vor allem bei Cloud-Speichern bieten viele Provider neben dem Standardzugriff per HTTP/HTTPS alternative Protokolle an. Häufig zu finden ist WebDAV (Web-based Distributed Authoring and Versioning), eine Erweiterung von HTTP/1.1. WebDAV erlaubt es dem Benutzer, auf seine Daten so zuzugreifen, als lägen sie auf einer Online-Festplatte.

Auf der Gegenseite arbeitet ein Webserver mit WebDAV-Erweiterung, etwa ein Apache mit dem Modul „mod_dav“. Es stellt zusätzliche HTTP-Methoden wie COPY und DELETE zur Verfügung. Während einer Client-Anfrage an den Server wird die Ressource mit der HTTP-Methode LOCK gesperrt und mit UNLOCK wieder entsperrt.

WebDAV funktioniert sowohl über HTTP als auch HTTPS. Um auf das Verzeichnis zuzugreifen, gibt man unter Windows im Dateimanager Folgendes in die Adressleiste ein: \server@SSL@port \DavWWWRoot\webdavordner\ . Den Abschnitt @port benötigt man nur, wenn der Dienst nicht am Default-Port 80 (HTTP) beziehungsweise 443 (HTTPS) auf Anfragen wartet. Der Ordner DavWWWRoot ist kein echter Ordner, sondern ein spezielles Schlüsselwort, damit die Windows-Shell den richtigen Treiber aktiviert.

Unter Mac OS X genügt unter „Mit Server verbinden“ die Angabe von http://server:port. Der Konqueror etwa

unter Linux versteht die Angabe `webdav://server:port/`. Alternativ kann man den Browser benutzen, dort lautet die Syntax: `https://server/webdavordner` oder `https://server:port/webdavordner`.

Ebenfalls auf SSL setzt FTPS auf. Allerdings ist FTP über SSL mit einigen Tücken versehen. Zum einen kann der bevorzugte aktive Modus an der Firewall scheitern: In ihm initialisiert der Client eine Control-Session vom eigenen Port >1024 zum Server-Port 21. In der Session teilt der Server dem Client mit, auf welchem Port er eine Verbindung zum Client aufbaut, in der Regel vom Server-Port 20 zum Client-Port >1024. Da der SSL-Layer diese Kommunikation aber verschlüsselt, versteht eine dazwischenliegende Firewall das nicht und kann den entsprechenden Port nicht dynamisch öffnen.

Zum Zweiten sollte man Explicit SSL vermeiden, da die FTP-Session bis zum Authentifizierungs-Befehl unverschlüsselt über den Port 21 läuft. Implicit SSL verwendet hingegen von Anfang an die Ports 990 für passives FTP und den FTP-Control-Kanal sowie 989 für den Datenkanal im aktiven Modus.

Komplett anders arbeitet SFTP, ein Subsystem der SSH mit FTP-Look-and-Feel. Hat man sie eingerichtet, steht auch SFTP zur Verfügung. Damit kann man die starke User-Authentifizierung basierend auf Public-Keys benutzen [3].

Neben dem Datenverkehr kann man mit SSL/TLS den E-Mail-Verkehr absichern. Doch während die Kommunikation über SSL/TLS bei Browsern und Webservern inzwischen zum guten Ton gehört, bleibt die Kommunikation per E-

Mail und Chat bisher größtenteils unverschlüsselt. Will man die verwendeten Server nach ihren Verschlüsselungsmethoden abfragen, variiert man bei der oben beschriebenen Methode mit `openssl` die Port-Angabe, etwa SMTPS (Port 465), IMAPS (Port 993) oder POP3S (Port 995), oder verwendet Wireshark.

Grundsätzlich gelten für E-Mails dieselben Vorsichtsmaßnahmen wie bei Online-Speichern: Da SSL die Daten nur auf dem Transportweg schützen kann, liegen die beim Provider aufbewahrten Daten und Mails dort wieder im Klartext vor und können wieder das Ziel von Schnüffeleien und gezielten Angriffen werden.

Alle Lager abschließen

Wer Wert auf die Sicherheit seiner Daten legt, kommt um eine Ende-zu-Ende-Verschlüsselung nicht herum. Wobei Ende-zu-Ende hier nicht von einem Client-PC zu einem Dienst-Server bedeutet, sondern von Anwendung zu Anwendung. Für E-Mails heißt das, dass man den offenen Standard OpenPGP einsetzt, beispielsweise in der Implementierung von GnuPG.

Bei Dateien würde Ende-zu-Ende bedeuten, dass man sie nur verschlüsselt in die Cloud legt. Die einfachste Methode: Man packt seine Daten in ein passwortgeschütztes ZIP- oder RAR-Archiv. Nützlich sein kann in diesem Fall auch TrueCrypt. Die freie Software funktioniert auf vielen Betriebssystemen und ist einfach zu benutzen, allerdings hauptsächlich dafür bekannt, dass man mit ihr ganze Festplatten oder Partitionen verschlüsseln

kann. Alternativ kann man mit TrueCrypt eine Container-Datei zum Speichern der Daten anlegen. Die Container-Datei lässt sich dann mit TrueCrypt nach Eingabe einer Passphrase, die unbedingt sehr stark sein soll, mounten.

Auch GnuPG eignet sich dazu, Dateien zu verschlüsseln und zu signieren. Zudem kann es verschlüsselte Dateien mit `-armor` oder `-a` ins ASCII-armored-Format umwandeln, vergleichbar `UUencode`. Dadurch sind die verschlüsselten Daten auch mit sehr alten Protokollen, die kein Binär-Format vertragen, kompatibel.

Wesentlich mehr Optionen beim Verschlüsseln haben die Administratoren von Organisationen und Firmen, wenn sie ihre private Cloud etwa mit AeroFS oder OwnCloud betreiben und damit die volle Kontrolle über die eingesetzten Server haben (siehe Artikel „Wolkiges Puzzle“ in diesem Heft auf Seite 52). Sie können dadurch sowohl bei den Transportarten als auch bei den Speichermedien frei über die Verschlüsselungsmethoden entscheiden. Beispielsweise dürfen sie ihre eigenen VPNs einrichten, wodurch dann auch Außendienstmitarbeiter (Road-Warrior) und Außenstellen in den Genuss des organisations- oder firmeneigenen Cloud Computing kämen.

Eine selten benutzte VPN-Variante benutzt die Secure Shell. Die SSH eignet sich zum Bereitstellen von VPN-Tunneln für eine Vielzahl von TCP/IP-Protokollen wie HTTP, SMTP, IMAP, POP3. Voraussetzung ist, dass man die Authentifizierung durch die altbekannte Username-Passwort-Kombination abschaltet und auf die durch Zertifikate umstellt [3].

Anzeige

Agiler und effizienter werden: Modernes BPM im Digital Enterprise

Vier Megatrends aus der IT wirken als Katalysator für die Entwicklung in Richtung Digital Enterprise: Social Collaboration, Mobile Computing, Cloud Computing und Big Data. Diese Megatrends verändern die Art und Weise, wie Menschen miteinander kommunizieren, interagieren und zusammenarbeiten. Das hat Auswirkungen auf Vertriebskanäle, nachgefragte Produkte und Services. Modernes Geschäftsprozessmanagement (BPM) greift die neuen Technologien auf und macht Unternehmen agiler und effizienter.

Als Reaktion auf die ständig neuen Herausforderungen entwickeln Unternehmen ihre internen und externen Prozesse in Richtung des *Digital Enterprise*. Durch die Digitalisierung können sie flexibler auf die wachsende Dynamik und Komplexität reagieren, effizienter arbeiten und gleichzeitig ihren Marktanteil und die Kundenbindung erhöhen.

Die **Innovation World 2013** der Software AG zeigt Ihnen den Weg zum Digitalen Unternehmen. Lassen Sie sich inspirieren! Mit Innovationen und neuen Erkenntnissen schließen Sie die Lücke zwischen traditionellem und digitalem Geschäft.

Kommen Sie zur Innovation World vom 8. bis 10. Oktober in San Francisco:
www.innovationworld2013.com



Weitere Informationen:

Software AG
Uhlandstraße 12
64297 Darmstadt
www.softwareag.de



Anschließend kann der Administrator für die nötigen Dienste einen SSH-Listener einrichten, der die eingehende Verbindung authentifiziert, sich um die Verschlüsselung kümmert und die Kommunikation an den lokalen oder an einen Remote-Dienst weiterleitet [4].

Klassische VPNs setzen im OSI-Modell unterhalb des Layer 3 (IP) an und können damit ein Netz virtualisieren. Verbreitet ist hier noch das Point-to-Point Tunneling Protocol (PPTP), das viele Betriebssysteme wie Windows, Mac OS X, Linux, iOS und Android unterstützen. Es ist zudem relativ einfach einzurichten und zu warten. PPTP sollte aber nicht mehr verwendet werden, da es als geknackt eingestuft wird. Firmen und Behörden, die noch auf PPTP setzen, sollten möglichst schnell auf das wesentlich sichere IPsec oder OpenVPN umsteigen.

IPsec gilt zwar als sicher, stellt aber auch höhere Ansprüche beim Einrichten und Verwalten. Für Administratoren ist das in der Regel mit einem höheren Betreuungsaufwand auf der Client-Seite verbunden. Zudem haben Administratoren bei IPsec mit vielen Produkten unterschiedlicher Hersteller zu kämpfen, die nicht kompatibel untereinander sind.

Nicht sehr viel besser sieht es bei kommerziellen VPN-Produkten aus. Sie sind meist teuer und unterscheiden sich etwa in der Unterstützung der Client-Systeme stark voneinander, bieten aber einen hohen Komfort. Zudem sind kommerzielle Implementierungen von IPsec und VPN angesichts der neueren Enthüllungen nicht sonderlich vertrauenswürdig, da sie eine Black-Box darstellen. Der Kunde kauft die Katze im Sack und kann nicht überprüfen, ob das Produkt versehentlich oder durch Programme wie Bullrun angespornt eine Hintertür offen lässt.

Gerade deshalb erfreuen sich Open-Source-Produkte in letzter Zeit immer größerer Beliebtheit, vor allem auch im Bereich Sicherheit respektive Verschlüsselung. Hier bietet sich beispielsweise als Alternative zu den kommerziellen VPN-Lösungen OpenVPN an. Es errichtet die VPNs auf Basis von OpenSSL und läuft auf allen gängigen Plattformen, darunter auch auf Android und iOS. Es eignet sich sowohl zum Aufbauen eines Site-to-Site- als auch eines Remote-Access-VPN.

OpenVPN unterstützt neben den klassischen Authentifizierungs-Mechanismen Benutzername/Passwort und Pre-Shared Key auch die zertifikatbasierte Authentifizierung mit Private/Public-Schlüsseln und X.509-Zertifikaten. Zwar bedient man es typischerweise auf der Kommandozeile, es existieren aber auch grafische Front-

ends wie OpenVPN GUI für Windows oder Tunnelblick für Mac OS X.

Manche Cloud-Dienste stellen einen Zugang über unverschlüsselte Protokolle wie SMB/CIFS oder rsync bereit. Bei beiden ist auf jeden Fall ein weiteres Verfahren zum Tunnellen der Daten hinzuzufügen. Für rsync eignet sich SSH sehr gut als Tunnelbauer, SMB/CIFS sollte man auf jeden Fall mit einem VPN absichern, da sie als typische LAN-Protokolle für Netze mit identischem Sicherheitsniveau konstruiert sind.

Seit etwa einem Jahr erfreuen sich sogenannte CryptoPartys weltweit wachsender Beliebtheit. Hier treffen sich Experten und Novizen, um sich gegenseitig Verschlüsselungs- und Verschleierungstechniken beizubringen. Teilnahmebedingung ist ein eigener PC und der Wille zum Lernen.

Cryptoparty gegen die Überwachung

Dort kommen Themen wie anonymes Surfen mit dem Tor Browser Bundle, Browser-Plugins zum Erhöhen der eigenen Sicherheit wie NoScript, Alternativen zur Suchmaschine Google, E-Mail-Verschlüsselung mit GnuPG, Privates Chaten mit OTR Messaging (Off-the-Record), sicheres Löschen von Dateien und Full-Disc-Encryption sowie viele weitere Themen zur Sprache. Von einer Cryptoparty der besonderen Art, die im Bundestag für die Abgeordneten und ihre Mitarbeiter stattfand, berichtete kürzlich die Zeit [5].

Insgesamt scheinen die Europäer ihr Vertrauen an die großen US-amerikanischen Internet-Firmen zu verlieren. Die auf den Schutz der Privatsphäre ausgelegte und von cyrptoparty.in empfohlene Suchmaschine Duck Duck Go (duckduckgo.com) berichtet von stark ansteigendem Netzwerkverkehr. Auch der Download von Browser-Add-ons wie „DoNotTrack-Me“ ist offenbar dramatisch angestiegen.

Andere Alternativen wachsen jetzt erst. Beispielsweise arbeitet das Projekt des Forschungsinstituts „Gabriel Lippmann“ aus Luxemburg an einem Cloud-Speicherdiens mit starker Ende-zu-Ende-Verschlüsselung. LuxDrops (luxdrops.lu) – so der Name – schützt die Daten bereits auf der Client-Seite mit symmetrischer Verschlüsselung. Für Daten-Sharing mit anderen Anwendern benutzt es eine asymmetrische Verschlüsselung.

Um LuxDrops zu testen, ist ein Client, basierend auf Java 7 auf einem Windows-System zu installieren. Der Download ist zurzeit noch nicht möglich, da sich das Projekt noch im Testlauf befindet. Nach

Angabe der Entwickler wird noch vor Ende September ein Beta-Client für Mac OS X freigegeben. Nach dem Installieren des LuxDrops-Clients und einem Neustart wird der Benutzer zum Eingeben seiner LuxDrops-Credentials aufgefordert. Es ist aber auch vorgesehen, eine zertifikatsbezogene Authentifizierung zu nutzen.

Fazit

Will man seine Daten weiterhin der Cloud anvertrauen, gibt es nur einen Weg: sie mit starken kryptografischen Verfahren zu verschlüsseln – sowohl auf der Leitung als auch auf den Festplatten des Cloud-Service-Provider. Es reicht also nicht aus, sich auf den Einsatz von SSL/TLS zu verlassen, da das Verfahren nur die Daten unterwegs schützt und sich mit genügend Aufwand unterwandern lässt.

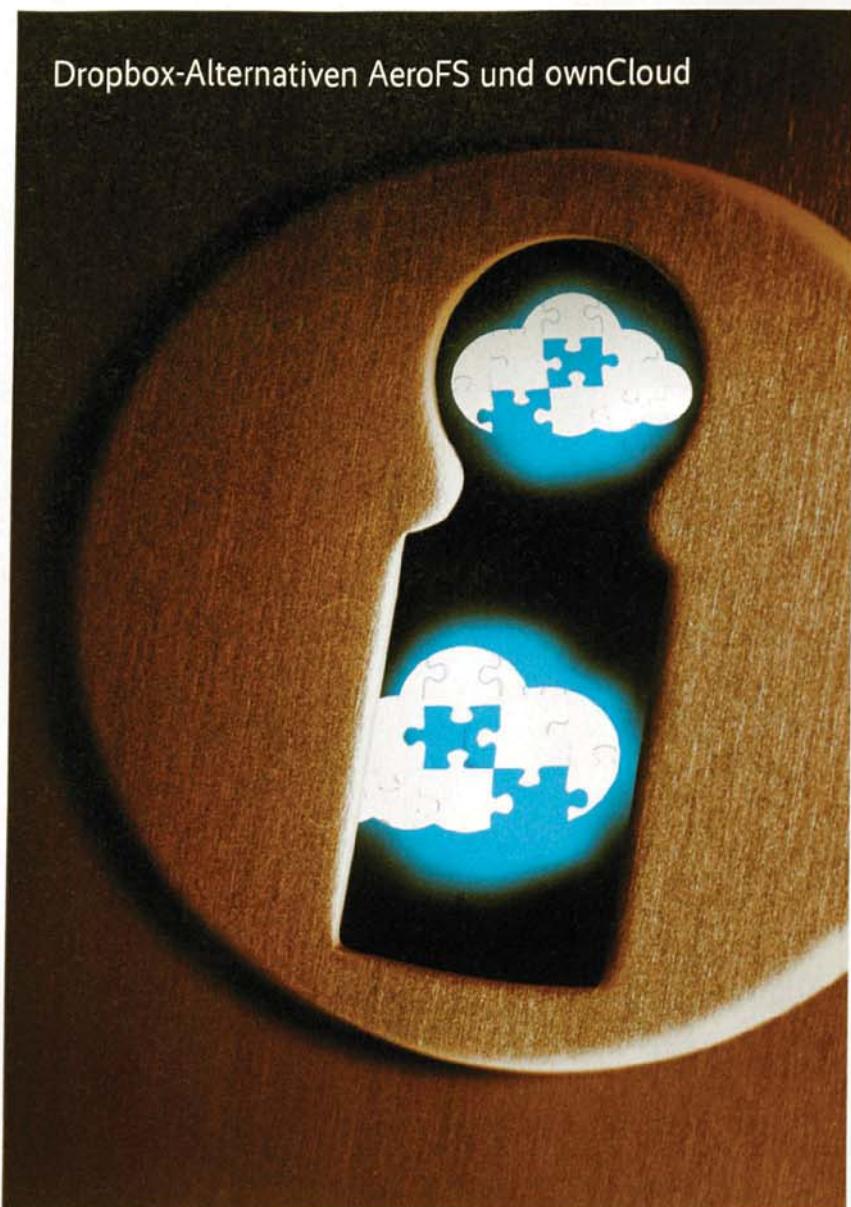
Zudem sind Daten nur dann sicher, wenn deren Besitzer die volle Kontrolle über die Verschlüsselung behält. Das ist – wie CryptoPartys es immer wieder zeigen – für viele Cloud-basierte Dienste für E-Mails oder Storage mit einem vertretbaren Aufwand möglich. Andere Cloud-Anwendungen befinden sich hier noch im Forschungsstadium. (sun)

Michael Hamm

arbeitet als Security Officer bei smile – security made in Luxembourg in Luxembourg.

Literatur

- [1] The Guardian; Revealed: how US and UK spy agencies defeat internet privacy and security; 6.9.2013; www.theguardian.com/world/2013/sep/05/nsa-ghq-encryption-codes-security
- [2] ENISA, Critical Cloud Computing – A CIIP perspective on cloud computing services; www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing
- [3] Michael Hamm; Abwehrmaßnahmen; Gut geraten; Auf Zertifikats-Authentifizierung umsteigen; iX 12/2011, S. 141
- [4] Susanne Nolte; Tools und Tipps; Vielseitig; Komprimieren und Tunnel bauen mit ssh; iX 1/2008, S. 151
- [5] ZEIT ONLINE; Cryptoparty im Bundestag; Hilf dir selbst, bevor der Staat versagt; zeit.de/digital/datenschutz/2013-09/cryptoparty-bundestag-fdp



Dropbox-Alternativen AeroFS und ownCloud

Wolkiges Puzzle

Udo Seidel

Vor dem Hintergrund der NSA-Enthüllungen machen sich IT-Verantwortliche zunehmend auf die Suche nach vertrauenswürdigen Alternativen zu Dropbox & Co. AeroFS und ownCloud versprechen, dass Sicherheit bei ihren Produkten kein Wolkenkuckucksheim ist.

Mittlerweile ist die „Wolke“ fast omnipräsent und dient insbesondere als Datenspeicher. Dropbox ([1], siehe Onlinequellen, [a]) hat einst das Eis gebrochen und das Ablegen der Daten in der Cloud für den Hausgebrauch möglich gemacht. Wem dieser Anbieter nicht geheuer ist, kann auf ownCloud [b] oder AeroFS [c] zurückgreifen. Beide werben damit, die bessere Alternative zu Dropbox zu sein. iX hat sich die Pakete genauer angeschaut.

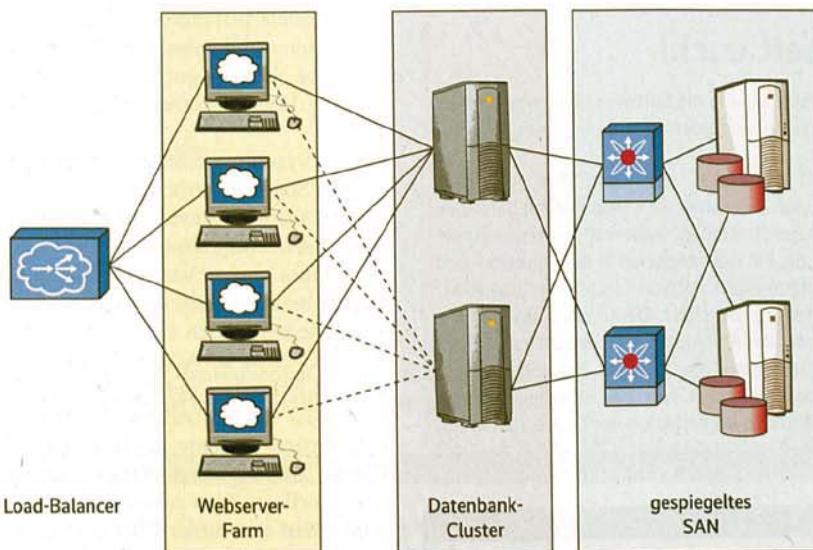
Die Anfänge der eigenen Wolke

Die Geschichte von ownCloud begann im Januar 2010 durch eine Initiative von Frank Karlitschek. Der aus KDE und openDesktop.org [d] bekannte Entwickler machte sich für eine quelloffene Alternative zu Dropbox und Co. stark und legte gleich selbst vor: Schon im Juni 2010 erschien ownCloud 1.0 [e]. Zwei Punkte waren Karlitschek bei diesem Projekt wichtig. Zum einen sollte die Software im Quelltext verfügbar sein. Neben den üblichen Vorteilen von Open-Source-Software muss der Anwender keine versteckten Hintertürchen für Organisationen wie die NSA fürchten. Der zweite wichtige Grundgedanke war, dass die Software selbst unabhängig von externen Dienstleistern ist. Für den rein privaten Gebrauch installiert ein Anwender sie einfach auf einem Server zu Hause, in der Firma kann es erst einmal ein vorhandener Server sein. Der ownCloud-Administrator kann so sehr genau die Kommunikationskanäle für den Datenzugriff festlegen und neugierige Dritte aussperren.

Zu Beginn war das Projekt nur als zentraler Datenspeicher gedacht. Prinzipiell besteht ownCloud aus einem Webserver mit etwas PHP-Code und entsprechenden Berechtigungen. Die interne Benutzerverwaltung greift auf SQLite, MySQL oder PostgreSQL zurück. Die modulare Struktur erlaubt eine einfache Erweiterung durch Plug-ins. Die aktuelle

ownCloud-Storage- Backends

lokales Dateisystem	OpenStack Swift
Amazon S3	SFTP
Dropbox	SMB
FTP	WebDAV
Google Drive	



Für ein ausfallsicheres Setup müssen drei ownCloud-Bereiche hochverfügbar ausgelegt sein (Abb. 1).

Version 5.x (für diesen Artikel kam 5.0.8 zum Einsatz) von ownCloud kann auch Kontakte und Termine verwalten, Musik wiedergeben und vieles mehr – die Auswahl auf der Apps-Seite [f] ist gewaltig. Das Freischalten und Integrieren vieler Funktionen sollte der Anwender dennoch mit Bedacht vornehmen. Das Gesamtsystem wird komplexer und störanfälliger – insbesondere bei Updates.

Ebenfalls im Jahr 2010 liegen die Ursprünge von AeroFS. Knapp sechs Monate nach dem Start der ownCloud-Initiative meldete sich dessen Initiator Juri Sagalow mit dem ersten Blog-Eintrag zu „seiner“ Dropbox-Alternative. Dennoch blieb das Projekt lange Zeit recht geschlossen. Wer im Beta-Test mitmachen wollte, benötigte eine Einladung. Dies änderte sich erst im April dieses Jahres [g]. Zu diesem Zeitpunkt beendete das AeroFS-Team offiziell den Beta-Status der Software. Im selben Beitrag erläuterte Juri Sagalow das Geschäftsmodell, das eine professionelle Nutzung erlaubt. Im Vergleich zu ownCloud wirkt AeroFS dennoch recht zugeknöpft. Die Informationen auf der Hersteller-Website

sind recht dünn und eigenwillig sortiert [h]. Grundlage dieses Artikels ist die Version 0.4.209.

Hinter dem Horizont

Zentrales Element bei ownCloud ist der oben erwähnte Server. Technisch gesehen handelt sich um eine PHP-Anwendung, die unter einem Webserver wie Apache oder IIS läuft. Installationen auf einem NAS-Server von QNAP sind aber ebenso möglich wie auf einem Raspberry Pi mit Nginx. Die PHP-Anwendung ist die zentrale Verwaltungsstelle von ownCloud. Wie erwähnt befinden sich die notwendigen Informationen und Metadaten von ownCloud in einer Datenbank. Die Daten selbst liegen im einfachsten Fall auf der Festplatte des Webservers. Allerdings kann ownCloud auch auf externe Storage-Backends zugreifen. Dafür gibt es zwei Ansätze. Einmal kann der OC-Admin (OC = ownCloud) diese Datenträger an der entsprechenden Stelle im Dateisystem einhängen. Viel eleganter und flexibler erfolgt es aber über sogenannte

Integriertes Management
von mobilen Endgeräten,
PC-Clients und Servern

Wir pflegen Ihre gesamte IT!

www.baramundi.de/it-management



ix-TRACT

- Heute nutzen auch Unternehmen kostenlose Cloud-Speicher-Angebote für den Datenaustausch in verteilten Arbeitsgruppen.
- Mit dem Ziel, die bessere Dropbox-Alternative zu sein, wollen AeroFS und ownCloud vor allem sicherheitsbewusste Anwender überzeugen.
- Anspruch und Wirklichkeit der beiden unterschiedlichen Architekturansätze lassen sich nicht immer in Einklang bringen.

8.-10. Oktober 2013
Halle 12 | Stand 55
itsa 2013

Die IT-Security Messe und Kongress
The IT Security Expo and Congress

Vereinbaren Sie einen Termin und fordern

Daten wechselt euch!

csync ist ein in C geschriebenes Werkzeug zum Synchronisieren von Dateien. Im Unterschied zu *rsync* und Co. arbeitet es bidirektional. Die ursprüngliche Motivation des Projektes von Andreas Schneider war ein Werkzeug zum Abgleich von persönlichen Verzeichnissen unter Linux – analog zu den von Windows bekannten Profilen. Man kann aber beliebige Verzeichnisse synchronisieren. Eine neue oder geänderte Datei registriert die Software über die jeweiligen Metadaten. Die jeweils aktuellen Informationen speichert *csync* in einer lokalen Datei im SQLite-For-

mat. So kann die Software ohne externe Hilfe eventuelle Änderungen feststellen.

Im Konfliktfall, also wenn zwei oder mehr *csync*-Teilnehmer eine Modifikation derselben Datei feststellen, „gewinnt“ die letzte Änderung. Für die Integration in den Anmelde- und Sitzungskonzept von Linux sorgt das PAM-Modul *pam_csync*. Damit alles funktioniert, muss der Administrator es sowohl ins Authentifizierungs- als auch ins Session-Management einbinden. Letzteres ist dabei für die eigentliche Kopieraktion der Daten zuständig.

Listing 1: Ausgabe von tcpdump

```
# tcpdump -N -nn -q -r OC.cap 'host 50.30.33.233' | head
reading from file OC.cap, link-type EN10MB (Ethernet)
21:46:36.363932 IP 192.168.100.100.33922 > 50.30.33.233.443: tcp 0
21:46:36.507290 IP 50.30.33.233.443 > 192.168.100.100.33922: tcp 0
21:46:36.507313 IP 192.168.100.100.33922 > 50.30.33.233.443: tcp 0
21:46:36.519459 IP 192.168.100.100.33922 > 50.30.33.233.443: tcp 201
21:46:36.660070 IP 50.30.33.233.443 > 192.168.100.100.33922: tcp 0
21:46:36.668948 IP 50.30.33.233.443 > 192.168.100.100.33922: tcp 1440
21:46:36.668961 IP 192.168.100.100.33922 > 50.30.33.233.443: tcp 0
21:46:36.669485 IP 50.30.33.233.443 > 192.168.100.100.33922: tcp 1440
21:46:36.669497 IP 192.168.100.100.33922 > 50.30.33.233.443: tcp 0
21:46:36.669503 IP 50.30.33.233.443 > 192.168.100.100.33922: tcp 0
#
```

„Custom Mounts“. Hier können Anwender verschiedene externe Datenspeicher in ihren jeweiligen privaten OC-Bereich einbinden. Der Kasten „ownCloud-Storage-Backends“ listet die wichtigsten unterstützten externen Storage-Backends auf.

Ein HA-Setup ist ratsam

ownCloud steht und fällt mit der Verfügbarkeit des Servers. Zum Minimieren von Ausfällen kommen die üblichen Verfahren zum Einsatz. Wie Abbildung 1 zeigt, unterteilt sich die OC-Plattform im Wesentlichen in drei Bereiche: die Web- und Applikationsserver, die Datenbank sowie der Speicher für die eigentlichen Daten. Für Letzteren wählt der Administrator typischerweise zwischen dem Spiegeln der Daten auf der Serverseite oder dem Synchronisieren zwischen den Storage-Hosts selbst. Analog befindet

sich die Datenbank in einem entweder über externe Cluster-Software oder DB-Replikation verwirklichten Cluster. Die Web- und Applikationsserver schließlich organisiert man als Farm hinter einem Load-Balancer.

Die eigentliche Nutzung von OC-Diensten erfolgt aber über die Clients. Designbedingt kann der Anwender über jeden HTML5-fähigen Browser auf die ownCloud-Daten zugreifen. Wesentlich interessanter sind aber passende Programme für den Desktop und mobile Geräte [i, j]. In allen Fällen authentisiert sich der Client über Benutzername und Passwort. Prinzipiell wäre auch die Verwendung von Client-Zertifikaten für diesen Zweck denkbar und in manchen Umgebungen sogar sinnvoll. Eine entsprechende Anfrage aus der Community scheint aber nicht wirklich etwas zu bewegen. Ebenso fehlt derzeit eine Absicherung gegen Brute-Force-Angriffe. Ohne zusätz-

```
# pwd
/var/www/html/owncloud/data/udo
# ls
cache files_files_trashbin files_versions lucene_index
# find files_files_trashbin/files files_files_versions/
files
files_mytest
files_mytest/myfile.txt
files_trashbin/files
files_trashbin/files/myotherfile.txt.d1377812470
files_versions/
files_versions_mytest
files_versions_mytest/myfile.txt.v1377812109
files_versions_mytest_myfile.txt.v1377812292
#
```

Gelöschte Dateien oder alte Versionen sichert ownCloud für eventuelle Wiederverwendung (Abb. 2).

liche Bastelarbeit protokolliert ownCloud nicht einmal fehlgeschlagene Anmeldeversuche. Diesen gravierenden Mangel will der Hersteller aber in Version 6 beheben.

Das Synchronisieren der Daten beruht auf der Software *csync* ([k], siehe Kasten „Daten wechselt euch“). Damit die Daten auf dem entsprechenden Client aktuell sind, muss er eine Verbindung zum OC-Server besitzen. Eine genauere Analyse zeigt allerdings auch eine Verbindung auf die öffentliche IP-Adresse 50.30.33.233 (siehe Listing 1) – der zugehörige DNS-Name ist „download.ownCloud.com“. Der Grund ist eine Überprüfung des Clients, ob eine neuere Version der Software vorliegt. Zum gegenwärtigen Zeitpunkt lässt sich dieser Check wohl nicht deaktivieren [l].

Per *csync* synchronisiert der Client die Daten mit dem Server. Das lokale Zielverzeichnis kann der Benutzer konfigurieren – Standard ist *ownCloud* im Heimatverzeichnis. ownCloud erlaubt das Wiederherstellen von gelöschten Dateien oder früheren Versionen. Die notwendigen Daten dafür sind auf dem OC-Server in separaten Directories hinterlegt. In Unix-Epoche-Sekunden gemessene Zeitstempel sind Bestandteil des Dateinamens und gewährleisten so die Eindeutigkeit (siehe Abbildung 2). Änderungen an Dateien erkennt *csync* anhand veränderter Metadaten. Das bedeutet, dass sogar ein *touch <Datei>* ein Synchronisieren auslöst. Die Konfigurationsmöglichkeiten der Clients sind allerdings recht eingeschränkt, insbesondere was die Synchronisierungsparameter betrifft. Desktop-Anwender können sich mit manuellen Anpassungen in den Dateien *ownCloud.cfg* und *ocsync.conf* behelfen – benutzerfreundlich ist das aber nicht.

Luftige Architektur

Die Besonderheit – quasi das Alleinstellungsmerkmal – von AeroFS ist die Peer-to-Peer-Architektur. Anders als ownCloud benötigt es keinen zentralen Server. Wie sich später zeigen wird, ist das allerdings nicht so ganz richtig. Das Synchronisieren der Daten erfolgt tatsächlich von Teilnehmer zu Teilnehmer. Eine große Schwäche des Systems ist, dass für den Abgleich zweier AeroFS-Clients beide gleichzeitig online sein müssen. Für globale Kollaboration ist das eher hinderlich. Abhilfe schaffen sogenannte Team-Server. Sie sind ebenfalls Teilnehmer im AeroFS-Verbund, aber ständig erreich-



Support Blog

Install

Sign out

MY AEROFS
Shared Folders
Devices
Invitations
MY TEAM
Team Members
Shared Folders
Team Servers
Settings

Devices

Name	Last seen	Unlink	Erase
GT-I9100	N/A	Unlink	Erase
stderr	N/A	Unlink	Erase
tron	N/A	Unlink	Erase
GT-P751	N/A	Unlink	Erase

Über das Login auf der Homepage von aerofs.com verwaltet man seinen aus Benutzern, Geräten und Servern bestehenden AeroFS-Verbund (Abb. 3).

Listing 2: Das „Client-Zertifikat“ eines AeroFS-Peers

```
$ id
uid=500(cloudy) gid=500(cloudy) Gruppen=500(cloudy)
$ pwd
/home/cloudy/.aerofs
$ openssl x509 -noout -text -in cert
Certificate:
Data:
Version: 1 (0x0)
Serial Number: 137927 (0x21ac7)
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN=AeroFS, C=US, ST=California, L=San Francisco,
O=aerofs.com/emailAddress=team@aerofs.com
Validity
Not Before: Jul 10 23:15:10 2013 GMT
Not After : Jul 11 23:15:10 2014 GMT
Subject: C=US, ST=CA, O=aerofs.com, OU=na,
CN=kommilobckhngoaahlbdaoallpljfcnlfdbfdinphionjcbekgnhppmdhmlp
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:99:0a:7f:ee:9a:20:d9:a7:e7:c7:91:c2:a1:19:
99:80:e5:4a:e5:1a:78:20:4f:bf:2e:30:96:5a:71:
84:cc:a1:3f:ec:8c:46:00:fe:21:a2:3f:a9:50:55:
a5:ec:39:d1:86:37:9c:1e:43:6d:42:c3:a5:dc:13:
...
25:cb:39:ad:e8:d2:c4:e7:c2:0b:cd:ac:a4:de:b7:89:aa:4a:
dd:d6:b2:03:6:05:ee:5a:ac:3c:4e:cf:0:a:0:93:26:6d:59:
30:0d:4b:a2:35:d0:76:6b:e0:fa:e8:9a:af:d0:c4:58:2b:a5:
50:99:08:00:48:6c:ef:15:c5:c8:a6:80:f6:dc:45:7b:ed:
cc:18:63:9b
$
```

bar. Für höhere Verfügbarkeit empfiehlt es sich, mehrere Team-Server aufzusetzen, die dann eine Art Farm bilden.

Sowohl Client als auch Team-Server sind in Java implementiert und bringen alle notwendigen Werkzeuge für Verbindungsauflauf- und -abbau sowie das Synchronisieren der Daten mit. Anders als bei ownCloud existiert zu den Daten keine Webschnittstelle. Für den Download der Software muss man sich bei AeroFS registrieren. Dieser Account erlaubt eine rudimentäre Verwaltung der Benutzer, der beteiligten Geräte und Team-Server (siehe Abbildung 3). Einen Zugriff auf die eigentlichen Daten bietet er jedoch nicht.

Die Tatsache, dass Informationen über den eigenen AeroFS-Verbund beim Softwarehersteller hinterlegt sind, lässt aufhorchen. Eine genaue Analyse zeigt, dass die Peers unter bestimmten Bedingungen Server außerhalb des eigenen Netzes kontaktieren. Für eine erfolgreiche Kom-

munikation der AeroFS-Partner untereinander müssen sie sich gegeneinander ausweisen. Dies erfolgt über ein Gerät zertifikat, das die Setup-Routine anlegt – Listing 2 zeigt ein Beispiel. Die Software lässt sich ohne funktionierende Internetverbindung gar nicht installieren.

Neben dem Herunterladen der eigentlichen Software (siehe „Alle Links“) benötigt das Installationsprogramm einen Kanal zur CA-Infrastruktur von AeroFS. Es generiert beim Setup ein Zertifikat und lässt sich dieses von AeroFS signieren. Um Angriffe Dritter zu erschweren, befindet sich das Zertifikat der Root-CA im Auslieferungsumfang des Clients. Außerdem muss man Benutzername und Passwort angeben, die sich zu diesem Zeitpunkt nur auf AeroFS-Servern befinden. Genau genommen wandert hier aber nicht das Passwort über das Netz und ist als solches auch nirgendwo gespeichert. Alle beteiligten Systeme benutzen einen per script [m] erzeugten Schlüssel. Kon-

Dedicated Marken-Server zum Desktop Preis!

Weltpremiere der neuen AMD Opteron™ 3365 CPU



Premium Server-Features inklusive:

- 8 Core CPU mit jeweils 2,3 GHz Leistung
- Redundantes Netzteil 80+
- Volles Remote KVM Management
- Tier III+ Datacenter in Deutschland
- 24/7 Support & 1.000 Mbit Traffic-Flatrate

Opteron™ S

CPU	AMD Opteron™ 3365 Neu!
Leistung	8 x 2,3 GHz
RAM	16 GB DDR3 ECC
Festplatten	2 x 2.000 GB SATA oder 2 x 64 GB SSD
Erweiterbar bis zu	2 x 4.000 GB oder 2 x 1.000 GB SSD
Anbindung	1.000 MBit Flatrate
IPv4 Adresse Inkl.	✓
IPv6 Subnetz (/64) Inkl.	✓
Betriebssysteme	Debian 7.0 Neu! openSUSE 12.3, Ubuntu 12.04, FreeBSD 9 und Windows 2012 (19,99€ Aufpreis im Monat), inkl. Plesk 11.5 Neu!
Extras	100 GB Backup-Speicher, Monitoring, Reset- und Rescue-System
Vertragslaufzeit	1 Monat
Monatsgrundgebühr ab	39,99 €
Einrichtungsgebühr	0,00 €

Jetzt informieren & bestellen

Tel.: 0211 / 545 957 - 330 www.webtropia.com

Gesucht und gefunden

Peer-to-Peer-Kommunikation klingt verlockend, weil scheinbar nur die beteiligten Partner miteinander kommunizieren können beziehungsweise müssen. Die Schwierigkeit liegt darin, dass die jeweiligen Teilnehmer auch voneinander wissen müssen. Ohne eine Zentralinstanz ist das im Internet eine schwierige Aufgabe. AeroFS behilft sich hier mit einigen Hilfservers und weicht damit vom eigenen Paradigma der Serverlosigkeit ab. Partner im gleichen Netzwerksegment, also in der Regel im LAN, finden sich über IP-Multicast. Das Synchronisieren der Daten erfolgt direkt – also zwischen den Beteiligten. In größeren Netzen und WAN tritt der sogenannte Präsenzserver (x.aerofs.com) auf den Plan. Die AeroFS-Teilnehmer nehmen mit ihm Kontakt auf und erfahren so von den jeweiligen Partnern.

In diesem Szenario kann es durchaus vorkommen, dass mindestens ein Partner sich hinter einem NAT (Network Address Translation) „versteckt“. AeroFS nutzt das in RFC 5389 spezifiziert STUN (Session Traversal Utilities for NAT), um die jeweilige öffentliche IP-Adresse zu bestimmen und mitzuteilen. Als STUN-Server dient stun.l.google.com. AeroFS versucht zunächst eine direkte Verbindung für den Datenaustausch aufzubauen. Ist dies beispielsweise wegen einer Firewall im Netzwerkpunkt nicht möglich, kommt ein weiterer Hilfsserver zum Einsatz – ein Relay. Die AeroFS-Teilnehmer schicken die Daten an relay.aerofs.com, der diese an die jeweils anderen Partner weiterleitet. Laut Aussagen der Leute hinter AeroFS liegen die Daten dem Relay zu keiner Zeit im Klartext vor. Der ultimative Beweis dafür steht aber noch aus.

Tabelle 1: Automatische Verbindungen

Kontakt-Server	Protokoll	aktiv bei Normalbetrieb
x.aerofs.com	HTTPS	nein
verkehr.aerofs.com	HTTPS	ja
sss.aerofs.com	HTTPS	nein
sp.aerofs.com	HTTPS	nein
api.mixpanel.com	HTTPS	nein
nocache.client.aerofs.com	HTTPS	nein
relay.aerofs.com	HTTPS	nein

taktiert nun ein AeroFS-Peer einen anderen, prüfen beide das Zertifikat des jeweils anderen und die Autorisierung für die betreffenden Verzeichnisse. Für beide Vorgänge muss die Software „nach Hause telefonieren“.

Es gibt noch einen weiteren Grund, warum AeroFS-Software Kontakt mit der Außenwelt aufnimmt – die dezentrale

Struktur. Für ein erfolgreiches Synchronisieren aller Daten müssen die Peers voneinander wissen. Ist das beteiligte Netzsegment nicht zu groß, kann man hier mit Broadcasts arbeiten. Im Internet skaliert dieser Ansatz aber überhaupt nicht. Hier kommen verschiedene Infrastruktur-Server zum Einsatz, die unter der Kontrolle von Air Computing Inc. stehen

– der Firma hinter AeroFS. Weitere Information dazu befinden sich im Kasten „Gesucht und gefunden“.

Stille Post im Hintergrund

Bleibt die Frage zu klären, ob die Daten bei ownCloud und AeroFS vor dem Zugriff durch Unbefugte sicher sind. Der Wegfall einer vom Hersteller kontrollierten Serverkomponente schafft schon ein gewisses Grundvertrauen. Eine genaue Sicherheitsanalyse muss im Wesentlichen drei Aspekte abdecken: den Server, den Client und den Transport. Ersterer fällt eventuell bei AeroFS weg – wenn kein Team-Server im Einsatz ist. Bei ownCloud gilt es also, den Webserver genauer unter die Lupe zu nehmen. Im normalen Betrieb gab es keine Auffälligkeiten. Es existieren natürlich Verbindungen von den Clients zum Server, aber das war es auch schon.

Anders bei Team-Server von AeroFS. Bei jedem Start nimmt das Programm über HTTPS Kontakt zu einer Reihe von Servern auf (siehe Tabelle 1 „Automatische Verbindungen“). Der Kanal zu verkehr.aerofs.com bleibt sogar bestehen, solange der Team-Server aktiv ist. Wie oben schon erläutert, dienen diese Verbindungen unter anderem zum Authentifizieren und Auffinden der jeweiligen Kommunikationspartner. Eine genauere Analyse, welche Daten da ins Internet gehen, ist leider noch nicht abgeschlossen. Das scheiterte bislang an der mangelnden Auskunftsfreude der Entwickler und den fehlgeschlagenen Versuchen, den Verkehr mit einem SSL-Proxy umzuleiten.

Für die eigentliche Datenübermittlung greifen beide Dropbox-Alternativen auf Verschlüsselung per OpenSSL zurück. Bei ownCloud setzt das allerdings einen entsprechend konfigurierten Webserver voraus. Sonst erfolgt die Übertragung im Klartext und leider warnt die Software den Benutzer nicht. Hier ist noch etwas Nacharbeit nötig, da die ownCloud-Software zumindest den Anwender auf das mögliche „Abhören“ der Daten hinweisen müsste.

AeroFS nutzt SSL-basierte Verschlüsselung in jedem Fall und fordert das Zertifikat des Kommunikationspartners zum Verifizieren an. Im Unterschied zu ownCloud bringt die Software eigene OpenSSL-Bibliotheken mit. Damit ist AeroFS zwar etwas unabhängiger vom darunterliegenden Betriebssystem. Allerdings müssen die Entwickler nun selbst die Wartung „ihres“ OpenSSL überneh-

Onlinequellen

- | | |
|---|---|
| [a] Dropbox | www.dropbox.com |
| [b] ownCloud | www.ownCloud.com |
| [c] AeroFS | www.aerofs.com |
| [d] openDesktop | opendesktop.org |
| [e] ownCloud 1.0 | blog.karlitschek.de/2010/06/ownCloud-1.0-is-here.html |
| [f] owdCloud-Plug-ins | apps.ownCloud.com |
| [g] offizielle Freigabe | blog.aerofs.com/336/open-for-business |
| [h] AeroFS – technische Informationen | support.aerofs.com/home |
| [i] OC-Desktop-Clients | ownCloud.org/sync-clients |
| [j] OC-Mobil-Clients | ownCloud.com/products/mobileapps |
| [k] csync | www.csync.org |
| [l] Versions-Check | github.com/ownCloud/mirall/issues/588 |
| [m] script | www.tarsnap.com/script.html |
| [n] Update-Problem | github.com/owncloud/core/issues/3417 |
| [o] Forumsdiskussion | forum.owncloud.org/viewtopic.php?f=23&t=10455 |

UNSICHTBARE WLAN POWER

bintec W-Serie

MIMO 802.11n
by bintec



- Gleichzeitiger Betrieb auf dem 2,4-GHz und 5-GHz-Band
- Bruttoübertragungsraten bis zu 2x 450 Mbit/s (802.11n Mimo 3x3)
- Stand-Alone Betrieb oder Betrieb mit bintec WLAN Controller
- 2-Port Gigabit Ethernetanschluss mit PoE (Power over Ethernet)
- Elegantes, unauffälliges Gehäusedesign für Wand- und Deckenmontage
- Integrierte Mimo-Antennen für 2,4- und 5-GHz

Mehr erfahren auf unserer Webseite:
www.teldat.de/wlanpower



Teldat
bintec-elmeg

Teldat GmbH
Südwestpark 94
D-90449 Nürnberg
Telefon: +49-911-96 73-0

Geteilte Meinung

Bei den Anwendern driften die Meinungen bezüglich ownCloud weit auseinander. Diese Aussage beruht auf Wortmeldungen im Internet sowie auf Erfahrungen von Bekannten und Freunden des Autors. Auf der einen Seite gibt es die sehr zufriedenen Benutzer, bei denen auch Updates der Software reibungslos funktionieren. Auf der anderen Seite stehen aber viele Anwender, die nach der Aktualisierung ein kaputtes System hatten. Ein aktuelles Problem – bei dem ownCloud unter bestimmten Umständen im Maintenance-Modus hängt

gen bleibt – erfordert vom Anwender wieder einmal die Manipulation eines PHP-Skript damit das System wieder läuft [n]. Verbesserung soll hier mit Version 6 kommen – zumindest ein Teil der Anwender wartet gespannt darauf. Ein Vorwurf der Community: Bei ownCloud würden neue Features und Funktionen zu schnell und mit heißer Nadel gestrickt im Produkt landen [o]. Hier sind Entwickler und Produkt-Manager gleichermaßen gefragt, dieses Ärgernis aus dem Weg zu räumen.

Tabelle 2: ownCloud und AeroFS im Vergleich

	ownCloud	AeroFS
Speicherplatz	unbegrenzt	unbegrenzt
Client-OS	beliebig (Browser)	Linux, Windows, Mac OS
Anzahl Benutzer (kostenfrei)	beliebig	1-3
Anzahl Benutzer (kostenbehaftet)	beliebig	4 und mehr
Schnittstellen	Web, Clients	Clients
Freigabe von Ordnern möglich	ja	ja
Server nötig	ja	nein
Server-O/S	Linux, Windows, BSD, Mac OS ...	Linux, Windows, Mac OS (Team-Server)
Kommunikation verschlüsselt?	ja	ja
serverseitige Verschlüsselung	ja (AES-256)	nein
„Ausbrechen“ aus Verzeichnissen über Symlinks	nein	nein
lokales Datenverzeichnis konfigurierbar	ja	ja
externer Storage	ja (siehe Text)	ja (Amazon S3)
Versioning (mit automatischen Backup?)	ja (quasi unbegrenzt)	ja (nur letzte Version)
Wiederherstellung gelöschter Dateien	ja	ja

men. Spätestens hier zeigt sich, dass die Leute hinter AeroFS gerne eine gewisse Kontrolle haben. Ihre Software legt die zur Verschlüsselung verwendeten Zertifikate fest und damit das letztlich verwendete Verfahren während der Datenübertragung. Zum gegenwärtigen Zeitpunkt kommt der Advanced Encryption Standard (AES) mit einer Schlüssellänge von 256 Bit zum Einsatz. Eine Übersicht weiterer Eckdaten liefert Tabelle 2.

Fazit

Als reiner Dropbox-Ersatz ist ownCloud gut geeignet. Der Anwender hat volle Kontrolle über die Daten und über ihre Wege. Die Erweiterungs- und Einsatzmöglichkeiten scheinen fast endlos und lassen die Software auch Kontakte und Termine verwalten oder selbst Musik-Dateien abspielen. Hier muss man aber Zugeständnisse bei Stabilität und Update-Fähigkeit machen. Die Enterprise-Variante umfasst professionellen Support und Erleichterungen für den großflächigen Einsatz.

AeroFS ist ambitioniert, muss aber noch gewaltig zulegen. Die Aussage, dass kein zentraler Server nötig ist, ist streng genommen nicht richtig. Die Tatsache, dass unter anderem Informationen zu Benutzern und beteiligten Geräten auf externen Servern liegen, weckt nicht gerade Vertrauen. Die dürftige Dokumentation dazu ist auch nicht hilfreich. (avr)

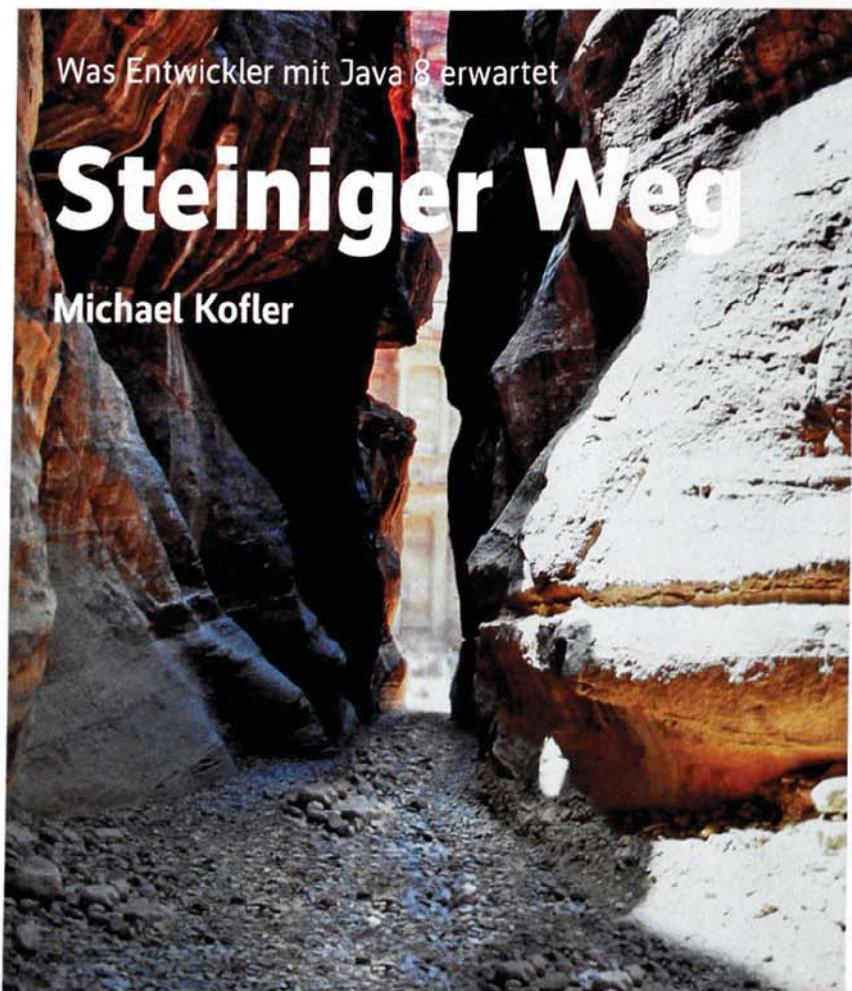
Dr. Udo Seidel

ist studierter Mathe-Physik-Lehrer und leitet eine Unix/Linux-Sysadmin-Gruppe bei der Amadeus Data Processing GmbH in Erding.

Literatur

- [1] Jürgen Seeger; Cloud-Speicher; Verteilt sammeln; Cloud-zentrierte Informationsverwaltung – Dropbox, Evernote, Google Drive; iX 6/2012, S. 66





Nach vielen Verzögerungen ist Java 8 mittlerweile Feature-komplett und befindet sich auf der (ziemlich langen) Zielgeraden. Das Endprodukt ist zwar von Kompromissen geprägt und umfasst weniger Neuerungen als erhofft, kann aber doch mit einigen Besonderheiten aufwarten.

Voraussichtlich im März 2014 wird die neue Version der Programmiersprache mit der Unterstützung von Lambda-Ausdrücken in die Java-Geschichte eingehen. Diese versprechen nicht nur übersichtlicheren Code, sondern auch einfacher parallelisierbare Algorithmen. Daneben soll Java 8 durch viele Detailverbesserungen und neue Bibliotheken überzeugen.

Lambda-Ausdrücke sind eine kompakte Schreibweise zum Formulieren einer anonymen Klasse mit einer Methode. Solche Klassen dienen häufig dazu, funktionale Schnittstellen zu implementieren, also solche, die die Signatur exakt einer Methode definieren. In der Java-Klassenbibliothek gibt es eine Menge derartiger

Interfaces und entsprechend viele Anwendungsmöglichkeiten für Lambda-Ausdrücke.

Das Listing 1 „Hello Lambda!“ zeigt, wie Lambda-Ausdrücke typischen Java-Code vereinfachen können: Ein *FilenameFilter* soll alle PDF-Dateien eines Verzeichnisses ermitteln. Seine Implementierung gelingt mit einem Lambda-Ausdruck wesentlich eleganter als mit einer herkömmlichen anonymen Klasse.

Die Java-Syntax für Lambda-Ausdrücke hat große Ähnlichkeit mit der von C#, wo solche Ausdrücke schon länger erlaubt sind: Einer Parameterliste in runden Klammern folgt ein Pfeiloperator und ein Ausdruck, der die Parameter verarbeitet.

Ein Lambda-Ausdruck kann aus mehreren Java-Kommandos bestehen (siehe Listing 2). In diesem Fall ist er in geschweifte Klammern zu setzen. Wenn der Ausdruck ein Ergebnis liefert, muss das Programm es wie bei einer Methode mit *return* zurückgeben.

In den meisten Fällen kann der Java-Compiler aus dem Kontext den Datentyp der Parameter eines Lambda-Ausdrucks erkennen; dann ist es nicht erforderlich, eine Typbezeichnung voranzustellen. So ist im Listing „Hello Lambda!“ die Variable *pf* als *FilenameFilter* definiert; damit ist für den Java-Compiler klar, dass der Lambda-Ausdruck für die Methode *accept* gilt, also für die einzige Methode der *FilenameFilter*-Schnittstelle. Die Datentypen der Parameter *f* und *s* gehen daher aus der Signatur der Methode *accept* hervor. So viel Compiler-Intelligenz ist übrigens kein Novum in Java: Der in Version 7 eingeführte Diamond-Operator zum typenlosen Aufruf des Konstruktors einer generischen Klasse agiert ähnlich.

Zugriff autorisiert

Lambda-Ausdrücke helfen zwar beim Implementieren anonymer Klassen, sie sind aber mehr als eine Kurzschreibweise hierfür. Für herkömmliche anonyme Klassen gelten nämlich andere Gültigkeitebenen als für Lambda-Ausdrücke: Der Lambda-Ausdruck kann direkt auf Variablen zugreifen, die in derselben Codeebene zugänglich sind, in der er definiert ist. Den entsprechenden Mechanismus bezeichnet man als Variable Capture.

Dabei gibt es allerdings eine wesentliche Einschränkung: Lokale Variablen müssen final deklariert sein oder sich zumindest so verhalten (effectively final); das bedeutet, dass sie nach ihrer ersten Zuweisung nicht mehr verändert werden und der Java-Compiler eine Deklaration mit *final* ohne Fehlermeldung akzeptieren würde.

```
// Lambda-Ausdrücke können auf finale
// Variablen zugreifen
final String pattern = ".pdf";
FilenameFilter pf =
    (file f, String s) -> f.toLowerCase().endsWith(pattern);
```

Auch bei *this* und *super* verhält sich Code in Lambda-Ausdrücken anders als in anonymen Klassen. Normalerweise bezieht sich *this* auf die Instanz der Klasse und *super* auf die Instanz der übergeordneten Klasse. Definiert man also auf herkömmliche Weise eine anonyme Klasse, verweist *this* auf Elemente innerhalb dieser.

In Lambda-Ausdrücken haben *this* und *super* dagegen dieselbe Bedeutung

Listing 1: Hello Lambda!

```
// anonyme Klasse vs. Lambda-Ausdruck
import java.io.*;
...
File basedir = new File(System.getProperty("user.dir"));
...
// FilenameFilter als anonyme Klasse implementieren (Java 7)
FilenameFilter pf = new FilenameFilter() {
    public boolean accept(File f, String s) {
        return s.toLowerCase().endsWith(".pdf");
    }
};

// FilenameFilter als Lambda-Ausdruck implementieren (Java 8)
FilenameFilter pf =
    (f, s) -> s.toLowerCase().endsWith(".pdf");

// FilenameFilter verwenden
File[] pdfs = basedir.listFiles(pf);
for(File f : pdfs)
    System.out.println(f.getName());
```

Listing 3: Default-Methoden

```
... Default-Methoden in Schnittstellen
interface Iterable<T> ... {
    ...
    void forEach(Consumer<? super T> action) default {
        Iterables.forEach(this, action);
    }
}
```

Listing 2: Lambda-Syntax

```
// Lambda-Ausdruck ohne Parameter
() -> 7;
() -> "Ergebnis";

// Lambda-Ausdruck mit einem Parameter
(int i) -> i*i;
(i) -> i*i;
i -> i*i;

// Lambda-Ausdruck mit mehreren Parametern
(int i, String s) -> s.substring(i, i+1);
(i, s) -> s.substring(i, i+1);

// mehrteiliger Lambda-Ausdruck
(i, s) -> {
    kommando1;
    kommando2;
    return ergebnis;
}
```

Listing 4: Methoden-Referenzen

```
// sort-Aufruf mit Methodenreferenzen
import java.util.*;
Double[] x = {1.23, 1.2, 1.29};
Arrays.sort(x, Double::compare);

// sort-Aufruf mit Lambda-Ausdruck
Arrays.sort(x,
    (d1, d2) -> d1==d2 ? 0 : (d1 < d2 ? -1 : 1));
```

wie im Code außerhalb: *this* bezieht sich auf Elemente der Klasse, in der der Lambda-Ausdruck definiert wird, *super* auf deren Basisklasse.

Rückwärtskompatibilität durch Default-Methoden

Es gibt unzählige Schnittstellen in der Java-Standardbibliothek, die prädestiniert für die Anwendung von Lambda-Ausdrücken sind. Das würde allerdings Änderungen an den Schnittstellen erfordern und so die Kompatibilität zu Millionen von Java-Programmen aufs Spiel setzen.

Ein Beispiel ist *Iterable*: Sie wurde in Java 8 um die neue Methode *forEach* erweitert, die einen Lambda-Ausdruck als Parameter erwartet. Eigentlich wäre jetzt der Code jeder Klasse, die von *Iterable* abgeleitet ist, um die Implementierung von *Iterable* zu erweitern. Es gäbe praktisch kein Programm, das durch das Update auf Java 8 und die neue Java-Standardbibliothek nicht grundlegend zu ändern wäre.

Der Ausweg aus diesem Dilemma sind Default-Methoden: Beginnend mit Java 8 können bei der Definition von Schnitt-

stellen einzelne Methoden mit dem Schlüsselwort *default* deklariert und mit Code versehen werden. Beim Implementieren der Schnittstelle hat der Programmierer die Wahl, entweder die Default-Methoden zu übernehmen oder sie durch eigenen Code zu überschreiben.

Das Listing 3 „Default-Methoden“ zeigt die Deklaration der neuen Methode *forEach* für die *Iterable*-Schnittstelle. Dank des Schlüsselworts *default* ändert sich für vorhandenen Java-6- oder Java-7-Code

nichts: Sämtliche Klassen, die *Iterable* implementieren, funktionieren weiterhin. Aber allen Java-8-Programmierern steht nun die neue Methode *forEach* zur Verfügung.

Referenzen auf Methoden

Die Schreibweise *Klasse::statischeMethode* übergibt eine Referenz auf eine statische Methode. Im Listing 4 „Metho-

TRACT

- Die wichtigste Neuerung in Java 8 sind Lambda-Ausdrücke. Sie vereinfachen nicht nur das Formulieren alter Klassen, sondern eröffnen neue Wege zum effizienteren Umgang mit Aufzählungen (Collections).
- Ebenfalls neu in Java 8 sind die Datums- und Zeit-API des Projekts ThreeTen, eine Erweiterung der Annotationssyntax, sowie die wesentlich schnellere JavaScript-Engine Nashorn.
- Die Fertigstellung von Java 8 ist für den März 2014 geplant. Eine Java-8-kompatible Eclipse-Version wird es aber voraussichtlich erst im Sommer 2014 geben.
- Oracle hat das Projekt Jigsaw auf Java 9 verschoben. Es soll bei der Modularisierung von Bibliotheken und der platzsparenden Weitergabe von Java-Programmen helfen.

it-sa Highlight: HS256S



Die neue externe High Security Festplatte HS256S ist durch die ULD-Zertifizierung zur Speicherung personenbezogener Daten zugelassen. (BSI-Zertifizierungs-ID BSI-DSZ-CC-0825)

Neben der bewährten 256-Bit AES-Hardwareverschlüsselung im CBC-Modus und der 2-Faktor-Authentifizierung mittels Smartcard und PIN, bietet die HS256S die Möglichkeit, den kryptografischen Schlüssel unabhängig von PC oder Software auf der Festplatte zu verwalten.

Der Nutzer kann den kryptografischen Schlüssel erstellen, ändern, kopieren und bei Gefahr zerstören.



Besuchen Sie uns auf der it-sa 2013 in Nürnberg

Halle 12, Stand 630

Listing 5: removeIf

```
import java.util.*;

List<Integer> lst = new ArrayList<>();
for(int i=1; i<10; i++)
    lst.add(i);
// alle ungeraden Zahlen entfernen
lst.removeIf(i -> i % 2 == 1);
```

den-Referenzen“ erhält *sort* die statische *compare*-Methode der Double-Klasse. Alternativ lässt sich die Vergleichsmethode, also eine anonyme Comparator-Klasse, auch als Lambda-Ausdruck formulieren. (Selbstverständlich besteht weiterhin die Option, Double-Arrays ohne einen Comparator zu sortieren, weil die Double-Klasse ja ohnedies die Schnittstelle *comparable* implementiert; die Beispiele sollen nur die neuen Syntaxmöglichkeiten verdeutlichen.)

Auch die nicht statischen Methoden von Objekten (also von konkreten Instanzen einer Klasse) lassen sich als Parameter übergeben. Die Schreibweise lautet *objektvariable::instanzMethode*. In der Praxis ist diese Syntax aber selten hilfreich, weil damit zwar eine Referenz auf die Methode übergeben wird, nicht aber das zu bearbeitende Objekt.

Java unterstützt deswegen eine zweite Syntaxvariante, die formal gleich wie bei statischen Methoden aussieht: *klasse::instanzMethode*. Tatsächlich wird dadurch aber ein Lambda-Ausdruck der folgenden Form gebildet:

```
(Klasse obj) -> { obj.instanzMethode(); }
```

Zweckmäßig ist diese Schreibweise zum Beispiel in Kombination mit der neuen *forEach*-Methode diverser Aufzählungsklassen. Sie können nun an *forEach* eine Methode übergeben, die dann auf alle Objekte der Aufzählung angewandt wird:

```
lst.forEach(MyClass::printout);
```

Zum Ziel vormeßeln

Lambda-Ausdrücke eröffnen generell ganz neue Wege im Umgang mit Aufzählungen. Dabei geht es weniger darum, Code eleganter zu formulieren, vielmehr

sollen in Java 8 einzelne Methoden zur Verarbeitung von Aufzählungen besser parallelisiert und erst bei Bedarf vollständig ausgewertet werden (durch sogenannte Lazy Operations). Möglich wird das durch Erweiterungen in den Collection-Klassen der Java-Standardbibliothek.

Für die Schnittstellen *Iterable* und *Iterator* ist *forEach* als Alternative zu herkömmlichen *for*-Schleifen gedacht. Die sogenannte Internal Iteration, die die Methode verwendet, bietet im Vergleich zur traditionellen External Iteration zwei wesentliche Vorteile: Zum einen können Lambda-Ausdrücke komfortabel auf alle Aufzählungselemente angewendet werden, zum anderen lässt sich die *forEach*-Methode so implementieren, dass die Verarbeitung der Elemente parallelisiert erfolgt.

Neben *forEach* gibt es andere neue Methoden, die verschiedene Formen von Lambda-Ausdrücken als Parameter erwarten. Zu deren Deklaration sieht das neue Paket *java.util.functions* diverse Schnittstellen vor (siehe Tabelle „Lambda-Schnittstellen“). Sie kommen zum Beispiel in den Parametern verschiedener Methoden der Collection-Schnittstellen zum Einsatz:

```
Collection.forEach(Consumer)
Collection.removeIf(Predicate)
List.replaceAll(Function)
Stream.anyMatch(Predicate)
```

Das Listing 5 „removeIf“ zeigt den Einsatz der neuen Methode *removeIf*. Sie entfernt alle Elemente einer Aufzählung, die ein bestimmtes Kriterium erfüllen. Hierfür erwartet *removeIf* ein Predicate-Objekt, das sich am einfachsten als Lambda-Ausdruck formulieren lässt.

Die spannendste Neuerung ist aber im Paket *java.util.stream* versteckt. Die dort enthaltenen Schnittstelle *Stream<T>* erweitert die grundlegenden Aufzählungsklassen um ein vollkommen neues Konzept zur funktionalen Programmierung. Die Elemente werden dabei nicht gespeichert, sondern von einer Methode an die nächste weitergereicht (von der Idee her ähnlich wie Pipes unter Unix/Linux) und erst bei Bedarf tatsächlich verarbeitet (La-

zy Operation). Wichtige Methoden sind *filter*, *map*, *reduce*, *fold*, *limit* und *skip*.

Listing 6 „Stream“ zeigt, wie eine Liste von Zeichenketten in einen Stream umgewandelt und dann auf unterschiedliche Weise verarbeitet wird. Bemerkenswert ist die Methode *parallelStream*: Sie liefert einen zur Parallelverarbeitung optimierten Stream.

Datum und Zeit, dritter Aufguss

Der verunglückten Date-Klasse in der Java-Standardbibliothek haben die Entwickler bereits in Java-Version 1.1 die Calendar-Klasse zur Seite gestellt, doch auch sie ist eher eine Notlösung. Als gegenwärtig beste Möglichkeit, diffizile Datumsfragen zu behandeln, gilt die unter der Apache-2-Lizenz verfügbare **Bibliothek Joda Time**.

In Java 8 wagt Oracle mit dem sogenannten ThreeTen-Projekt nun einen weiteren Anlauf, um Daten, Zeiten und ihre unzähligen Sonderfälle innerhalb der Standardbibliothek in den Griff zu bekommen – und versucht gleichzeitig, Designschwächen der Joda-Time-Bibliothek zu beheben. Damit ist schon klar: Java-Entwickler müssen sich auf eine weitere Bibliothek einlassen, die inkompatibel zu allen bisherigen Varianten und mit über 60 Klassen samt Schnittstellen in mehreren *java.time*-Paketen alles andere als übersichtlich ist.

Eine wichtige neue Idee des Projekts ist die Unterscheidung zwischen einer Machine Time Line und einer Human Time Line:

- Die Machine Time Line beschreibt Mechanismen, um einen Zeitpunkt (Klasse *Instant*) beziehungsweise eine Zeitspanne (*Duration*) durch den Computer auf Nanosekunden genau abzubilden. Die *Instant*-Klasse entspricht am ehesten der Date-Klasse.

- In der Human Time Line geht es darum, Datum und Zeit so darzustellen, dass sie sich von Menschen verarbeiten lassen – also zum Beispiel mit einem Monatsna-

Lambda-Schnittstellen im Paket *java.util.function*

Schnittstelle	Funktion
<i>Predicate<T></i>	Überprüft, ob ein Objekt vom Typ <i>T</i> ein Kriterium erfüllt.
<i>Supplier<T></i>	liefert Objekte vom Typ <i>T</i> (zum Beispiel für <i>get</i> -Methoden).
<i>Consumer<T></i>	verarbeitet ein Objekt vom Typ <i>T</i> , gibt kein Ergebnis zurück.
<i>Consumer<T, U></i>	verarbeitet zwei Objekte vom Typ <i>T</i> und <i>U</i> , gibt kein Ergebnis zurück.
<i>Function<T, R></i>	verarbeitet ein Objekt vom Typ <i>T</i> und liefert als Ergebnis ein Objekt vom Typ <i>R</i> zurück.
<i>BiFunction<T, U, R></i>	verarbeitet zwei Objekte vom Typ <i>T</i> und <i>U</i> und liefert als Ergebnis ein Objekt vom Typ <i>R</i> zurück.
<i>UnaryOperator<T></i>	entspricht <i>Function<T, T></i> , das heißt, die zu verarbeitenden Daten und die Ergebnisse weisen denselben Typ auf.
<i>BinaryOperator<T></i>	entspricht <i>BiFunction<T, T, T></i> , das heißt, die zu verarbeitenden Daten und die Ergebnisse weisen denselben Typ auf.

Listing 6: Stream

```
import java.util.*;
String lorem = "Lorem ipsum dolor sit amet, ...";
List<String> lst = Arrays.asList(lorem.split(" "));
// alle Wörter mit mehr als sechs Zeichen ausgeben
// Ausgabe: consetetur sadipscing invidunt aliquyam
//           voluptua. accusam dolores gubergren, ...
lst.stream()
  .filter(s -> s.length() > 6)
  .forEach(s -> System.out.println(s));
// alle Wörter mit mehr als sechs Zeichen zählen (ohne Doppelgänger)
long n = lst.parallelStream()
  .filter(s -> s.length() > 6)
  .distinct()
  .count();
System.out.println(n);
// durchschnittliche Wortlänge
OptionalDouble avg = lst.parallelStream()
  .mapToInt(s -> s.length())
  .average();
System.out.println(avg.getAsDouble());
```

Listing 7: ThreeTen

```
// Anwendung der Zeit- und Datum-Klassen
import java.time.*;
import java.util.*;
import java.time.format.*;

LocalDateTime dt = LocalDateTime.now();
System.out.format("Jahr: %d\n", dt.getYear());
System.out.format("Monat: %d\n", dt.getMonthValue()); // 1-12
// z.B. 2013-06-06T13:29:50.252
System.out.format("Formatiert: %s\n",
  dt.format(DateTimeFormatter.ISO_LOCAL_DATE_TIME));

// der Monatsname
Month m = dt.getMonth();
String s = m.getDisplayName(TextStyle.FULL, new Locale("de"));
System.out.format("Monat: %s\n", s); // z.B. Juni

// das Datum in einem Monat
LocalDateTime dt2 = dt.plusMonths(1);
System.out.format("Formatiert: %s\n", // z.B. 2013-07-06
  dt2.format(DateTimeFormatter.ISO_LOCAL_DATE));
```

men. ThreeTen unterscheidet dabei zwischen lokalen Daten/Zeiten ohne Bezug zu einer Zeitzone (Klassen *LocalDate*, *LocalTime*, *LocalDateTime*), Angaben mit einem fixen Offset (zum Beispiel +01:00; *OffsetDate*, *OffsetTime* und *OffsetDateTime*) sowie Zeitangaben mit voller Zeitzonenerstützung samt Sommer-/Winterzeitumstellung (*ZonedDateTime*).

Standardmäßig verwenden die ThreeTen-Klassen den in Europa üblichen ISO-Kalender (Listing 7). Zum Arbeiten in anderen Kalendersystemen stellen die

Pakete *java.time.chrono* und *java.time.calendars* einige Zusatzklassen zur Verfügung (etwa *MinguoDate* und *MinguoChronology* für den in Taiwan geltenden Minguo-Kalender).

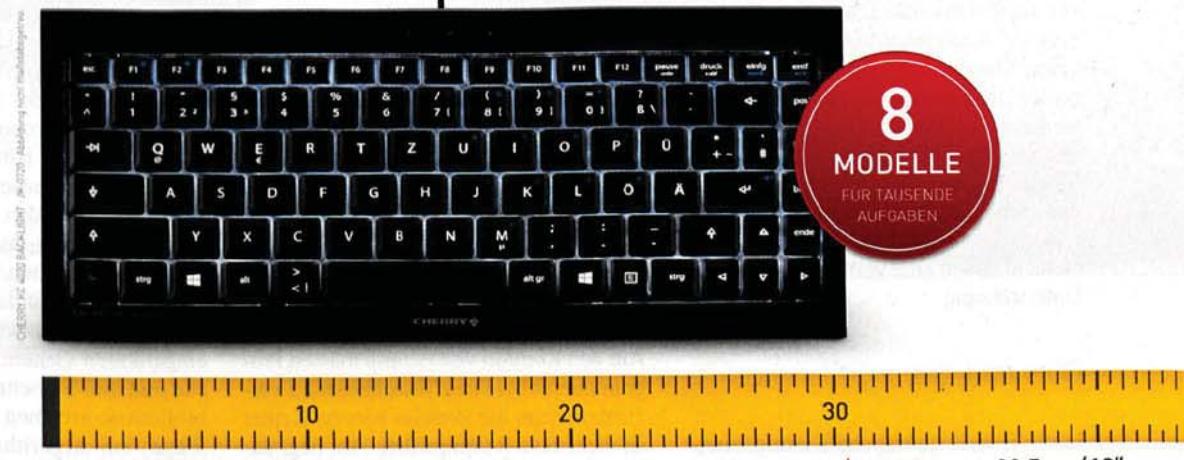
Sonstige Neuerungen

Java 8 erweitert die in Java 5 eingeführten Annotationen: Bisher konnten Entwickler sie nur für Klassen, Methoden, Felder und Variablen verwenden. Ab Java 8 lassen

sich auch alle anderen Java-Typen durch Metainformationen ergänzen, zum Beispiel generische Typen, Arrays, Casting-Operatoren oder *throws*-Ausdrücke.

```
// Annotationen für generische Typen
Map<@NotNull String, @NotEmpty List<String>> mymap;
```

Rund um dieses Thema gibt es noch mehr Änderungen: Eine Annotation lässt sich nun mehrfach auf ein Element anwenden (zum Beispiel *@Author(„name1“) @Author(„name2“)*). Außerdem wurde die



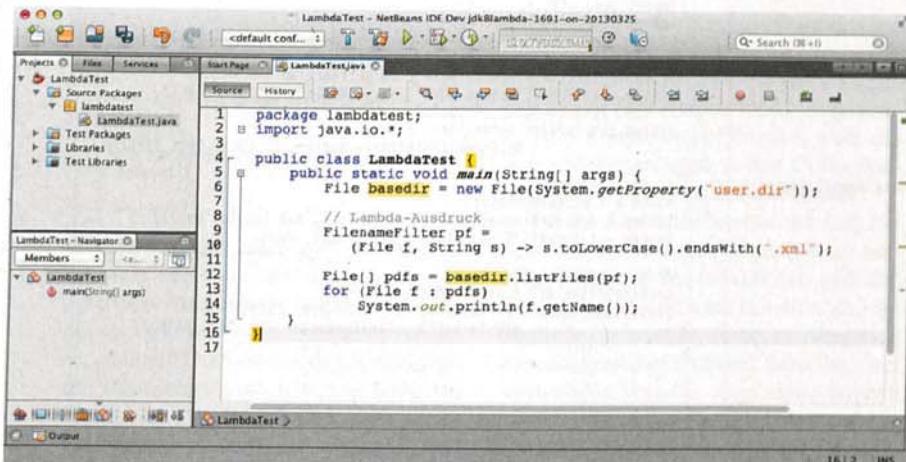
▲ Breite: nur 30,5cm/12"

ORIGINAL CHERRY. AUF KLEINSTEM RAUM.

CHERRY Kompakt-Tastaturen sind unschlagbar. Wegen ihrer sprichwörtlichen Qualität und ihrer Vielfalt an zuverlässigen Tastatur-Modellen und -Varianten in kompakter Baugröße. Wir beraten Sie gern: Telefon +49 [0] 7541 77 499 02*

Tipp: Erleben Sie unsere Raumwunder interaktiv unter cherry.de/kompakt/tastaturen.

CHERRY



Es gibt schon eine Lambda-kompatible Testversion von NetBeans.

Liste der vordefinierten Annotationen um `@FunctionalInterface` erweitert: Sie ist zur Kennzeichnung funktionaler Schnittstellen gedacht. Dabei handelt es sich um solche mit nur einer abstrakten Methode. Beim Verwenden dieser Annotation überprüft der Compiler, ob die Regeln für funktionale Schnittstellen erfüllt sind.

Mit Java 8 wird die in Enterprise- beziehungsweise Server-Anwendungen mitunter eingesetzte JavaScript-Engine Rhino durch die vollkommen neue Implementierung Nashorn ersetzt. Sie soll JavaScript-Code wesentlich schneller ausführen und gleichzeitig sparsamer mit dem Speicherplatz umgehen.

Das Framework JavaFX ist mit Java 8 Bestandteil des JDK, was den Versionsprung von JavaFX 2.2 auf JavaFX 8 begründet. Auch inhaltlich hat sich einiges getan: Zu den wichtigsten Neuerungen zählen 3D-Funktionen, Klassen zur Auswertung von Sensoren, wie sie auf Smartphones häufig zu finden sind, bessere Möglichkeiten zum Formatieren von Text und zum Ausdrucken formatierter Dokumente, das neue TableView-Steuer-element sowie eine verbesserte HTML5-Unterstützung.

Dies und das

In die Rubrik „nützliche Kleinigkeiten“ lässt sich die neue Methode `parallelSort` der Arrays-Klasse einordnen. Sie ist symptomatisch für diverse andere Detailverbesserungen, die Oracle an der Java-Standardsbibliothek vorgenommen hat – etwa die Unterstützung von Unicode 6.2, die Implementierung besserer Verschlüsselungsalgorithmen und sicherere Zufallszahlen. Jede Verbesserung ist für sich kaum der Rede wert, in Summe machen sie die Arbeit mit Java aber produktiver

und die resultierenden Programme – zumindest in manchen Fällen – schneller.

Mit der Fertigstellung des Milestone 7 Ende Mai 2013 ist Java 8 Feature-komplett. Der weitere Zeitplan sieht im September 2013 eine Developer Preview, im Oktober den API/Interface Freeze und im Januar 2014 einen Final Release Candidate vor. Tatsächlich fix und fertig soll Java 8 dann im März 2014 sein. Die vielfachen Verzögerungen haben nicht zuletzt damit zu tun, dass große Teile des Java-Entwickler-Teams seit Monaten damit beschäftigt sind, immer neue Sicherheitslücken in älteren Java-Versionen zu schließen.

Entwickler können den Großteil der neuen Features schon jetzt ausprobieren und wöchentlich neue Early-Access-Testversionen (Builds) von der JDK8-Website herunterladen. Um Konflikte mit vorhandenen Java-Installationen aus dem Weg zu gehen, empfiehlt es sich, dafür eine virtuelle Maschine zu verwenden.

```
java -version
java version "1.8.0-ea"
Java(TM) SE Runtime Environment
(build 1.8.0-ea-b92)
Java HotSpot(TM) 64-Bit Server VM (build
25.0-b34, mixed mode)
```

Auf den Komfort von Eclipse müssen Programmierer bei ihren Tests allerdings verzichten, denn die aktuelle Version Kepler ist nicht Java-8-kompatibel. Das liegt daran, dass sie nicht auf den mit dem JDK mitgelieferten Compiler `javac` zurückgreift, sondern einen eigenen verwendet – und der versteht die Lambda-Syntax noch nicht. NetBeans-Fans haben es besser – für diese IDE existiert bereits eine recht brauchbare Lambda-kompatible Testversion (s. Abb.). Und nicht nur das: Der NetBeans-Editor hilft sogar dabei, anonyme Klassen auf Knopfdruck in Lambda-Ausdrücke umzuwandeln.

Seit Jahren reden Java-Entwickler über die bessere Modularisierung von Java-Programmen und -Bibliotheken. Ein Ziel des der Diskussion zugrunde liegenden Projekts Jigsaw ist es, Java-Programme mit einer minimalen Runtime-Umgebung ausliefern zu können, die wirklich nur die Klassen enthält, die Programme tatsächlich nutzen.

Bitte warten auf Java 9

Obwohl das Projekt Jigsaw weit fortgeschritten ist und ursprünglich als wesentliches Feature von Java 7 (!) gedacht war, musste Oracle seine Fertigstellung nun erneut verschieben – auf die Java-Version 9, für die es noch nicht einmal einen konkreten Zeitplan gibt.

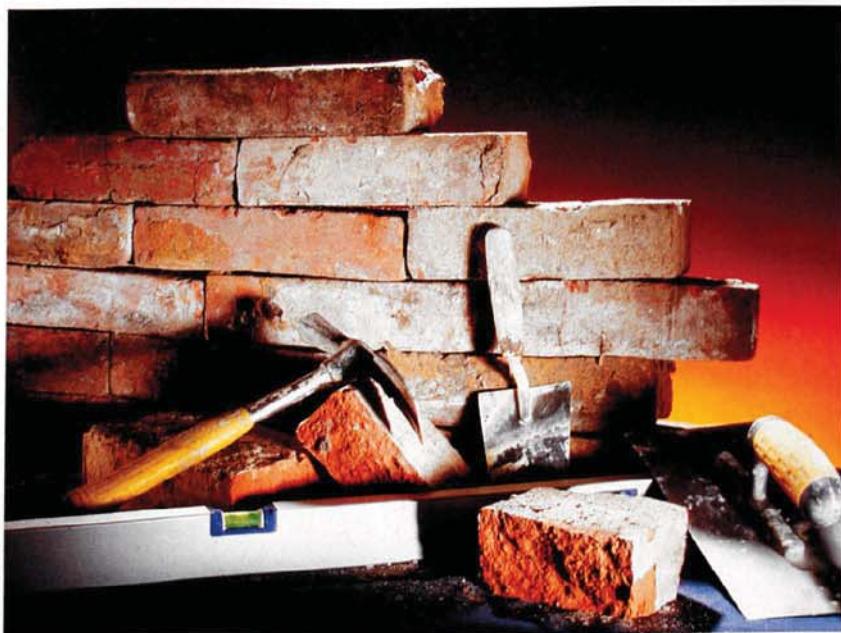
Daneben hat das Unternehmen auf der JavaOne 2012 recht vage einige weitere Ziele für Java 9 formuliert, unter anderem die Fertigstellung einer selbstoptimierenden Java Virtual Machine, die Unterstützung von Tail Calls (also den effizienten Aufruf einer Methode am Ende einer anderen Methode) sowie die bessere Nutzung von Grafikkarten zum Durchführen aufwendiger Berechnungen (OpenJDK-Projekt Sumatra). Wie die Erfahrungen mit Java 7 und 8 gezeigt haben, hat diese Zielvorgabe einen ähnlichen Wert wie ein Brief an das Christkind; welche Features Java 9 tatsächlich bieten wird, dürfen wir erst in einigen Jahren erfahren.

Fazit

Java 8 ist wie jedes andere Softwareprodukt von Kompromissen geprägt. Viele Java-Entwickler hätten sich noch mehr Features für die neue Version gewünscht. Doch selbst mit den verbliebenen Neuerungen kann man Java 8 durchaus als revolutionäre Version bezeichnen, die die Programmierung in Java mindestens ebenso stark verändern wird, wie die in Java 5 eingeführten Generics, Lambda-Ausdrücke und ihre Einbettung in der Standardbibliothek eröffnen vollkommen neue Wege, um Algorithmen mit einfachen Mitteln besser zu parallelisieren. (jul)

Michael Kofler

Ist freier Computerbuchautor und Lehrbeauftragter an der Fachhochschule Kapfenberg. Er hat kürzlich ein E-Book zur Java-Syntax veröffentlicht.



Microsofts Windows Server 2012 R2

Stein auf Stein

Nils Kaczenski

Microsoft hat den Anspruch, mit Windows alle Geräteklassen gleichzeitig zu bedienen: Vom Telefon über das Tablet bis hin zum Server im Rechenzentrum. Getreu dieser Logik muss nun eine neue Serverausgabe erscheinen, da Windows 8.1 ab Mitte Oktober in den Regalen der Händler steht.

Im Schlepptau des neuen Clients mit dem wenig griffigen Namen „Windows 8.1“ legt Microsoft eine neue Fassung seines Server-Betriebssystems vor, das sich wie schon in den letzten beiden Generationen durch das Anhängsel „R2“ als Unterversion der Produktfamilie, hier in der 2012er-Ausgabe, ausgibt. Tatsächlich deuten die Namen seit einiger Zeit nur noch ansatzweise auf den Umfang der Neuerungen hin. Vor drei Jahren etwa galt Server 2008 R2 vielen als veritable Hauptversion, und bei der Management-Suite „System Center“ packten die Redmonder gleich so viel ins Service Pack 1 für die 2012er-Fassung, dass es glatt als eigenes Produkt hätte durchgehen können.

In der aktuellen Runde fügen die Entwickler der verwirrenden Roadmap gleich

ein ganz neues Kapitel hinzu. Während der Client als kostenloses Update daher kommt und scheinbar wie ein Service Pack einfach eine neue Fassung des aktuellen Systems darstellt, handelt es sich beim Server 2012 R2 um ein neues Release, für das die Kunden den vollen Preis zahlen müssen. Zudem haben die Redmonder weit mehr Energie ins „große“ Windows investiert, denn die technischen Änderungen sind umfangreicher als auf der Client-Seite.

So ganz wohl scheint es Microsoft bei der schnellen Abfolge neuer Versionen nicht zu sein: Noch nie gab es schon ein Jahr nach Marktstart einer ihrer Betriebssysteme die nächste Generation. Da entsteht schnell der Eindruck, der Hersteller habe unsauber gearbeitet und müsse nun

korrigieren. Dass der vorherige Server 2012 noch gar nicht richtig am Markt angekommen ist, sieht man auch daran, dass der Hersteller in der Übersicht der R2-Features vieles auflistet, was schon mit der aktuellen Version realisiert ist.

Datenspeicher im Server

Bereits beim Vorgänger spendierten die Entwickler ihrem Server-OS zahlreiche Datenspeicherfunktionen, die man bis dahin lediglich in SAN-Systemen der gehobenen Klasse fand. Kaum zu übersehen, dass die Redmonder damit auf den jahrelangen Trend der Storage-Anbieter reagierten, mehr und mehr Server-Grundfunktionen in ihre eigenen Geräte zu übernehmen. Dies setzt der R2-Server fort und bietet weitere Features für die anspruchsvolle Datenablage.

Mit dem „Storage Tiering“ verschiebt ein Server automatisch die Daten auf schnelle SSD-Platten, auf die man ständig zugreift. Das geschieht auf der Block-Ebene, sodass innerhalb einer großen Datei die „heißen“ Bereiche im schnellen SSD-Bereich liegen, während selten genutzte Teile derselben Datei auf langsameren Festplatten verbleiben. Ein Administrator muss dazu nicht manuell eingreifen. Das Feature erweitert die im Server 2012 eingeführten Storage Pools, die bislang hinsichtlich des Durchsatzes enttäuschten, der weit unter dem herkömmlicher RAID-Arrays lag. So gesehen kann man die Storage Tiers (Tier = Ebene) als Nachbesserung auffassen.

Das aufgebohrte Dateiserver-Protokoll SMB 3.0 (Server Message Block) firmiert im neuen Release als Version 3.1. Wie in der 2012er-Ausgabe konzentrieren sich die Neuerungen auf den Einsatz von SMB als Rechenzentrums-Protokoll, mit dem vor allem Server miteinander kommunizieren. Galt ein Windows-Dateiserver früher als behäbig, geschwätzig und wenig robust, will Microsoft sein Server OS nun ebenfalls als zuverlässiges und skalierbares Storage-Backend positionieren. Der in der Vorversion eingeführte „Scale-out Fileserver“ bietet Dateizugriffe ohne Unterbrechung, selbst falls ein Serverknoten im Cluster plötzlich ausfällt. Das dafür nötige Session-Handling erweitert die R2-Fassung noch einmal und fügt eine verbesserte Lastverteilung hinzu. Unterhielt ein SMB-Client bislang immer eine einzige Sitzung pro Server, so verwaltet Windows nun eine Session pro Freigabe und reicht sie transparent im Cluster weiter. Ein Client, der mehrere Freigaben nutzt, verbindet sich

###Next Generation###

FIRE WAL LS##

####von Clavister####

MAC HEN

##Ihr Netzwerk sicher##
##ohne Abstriche bei##
##der Performance.##

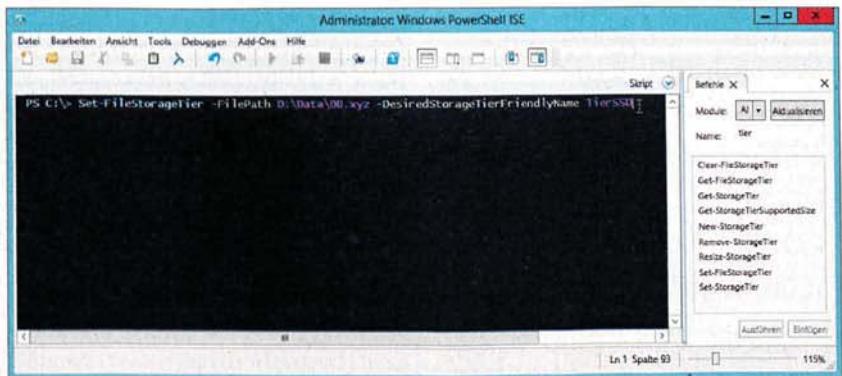
BLÖ D,##

##wer noch keine hat.##

CLAVISTER

WE ARE NETWORK SECURITY

Erfahren Sie mehr darüber,
was Clavister für Sie tun kann.
Und gewinnen Sie mit
etwas Glück ein
Application Security Audit unter
www.clavister.de/quiz



```
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
PS C:\> Set-FileStorageTier -filePath D:\Data\DB.xyz -DesiredStorageTierFriendlyName TierSSD
```

The screenshot shows a Windows PowerShell ISE window. A context menu is open over the command line, with the 'Module' dropdown set to 'AI' and the 'Ausführen' button highlighted.

Entlastet: In Speicher-Pools lassen sich SSDs und Festplatten kombinieren. Der Server erkennt die unterschiedlichen Typen und kann häufig genutzte Daten gezielt auf den schnellen Bereich verschieben (Abb. 1).

immer ausschließlich mit einem Server, doch wenn die Lastsituation es zulässt, verteilt der Cluster diese Zugriffe, sodass mehrere Clusterknoten den Client parallel bedienen.

Ist hier von „Clients“ die Rede, so bezieht sich das nicht vorrangig auf Anwender und ihre PCs. Die neuen SMB-Funktionen zielen auf Server ab, und zwar auch auf solche mit hohen Anforderungen an die Verfügbarkeit. Mittlerweile empfiehlt Microsoft daher als Storage-Backend für Virtualisierungsfarmen unter Hyper-V nicht mehr das Anbinden an einen SAN, sondern den Zugriff auf einen Dateiserver mit SMB 3.1. Da der kaum Anwender versorgt, kann man dort zudem SMB-Version 1.0 abschalten.

Verwaltungsreform per PowerShell

Administratoren eines 2012-R2-Servers profitieren von der erweiterten PowerShell, die in Version 4.0 vorliegt. Neben etwa 3000 neuen Commandlets verbessert sie vor allem den Remote-Zugriff auf andere Systeme sowie die Job-Steuerung. Besonders auf große Netzwerke zielt das Framework „Desired State Configuration“ ab, das Komponenten von Windows-Systemen im Netzwerk regelt. Mit dieser

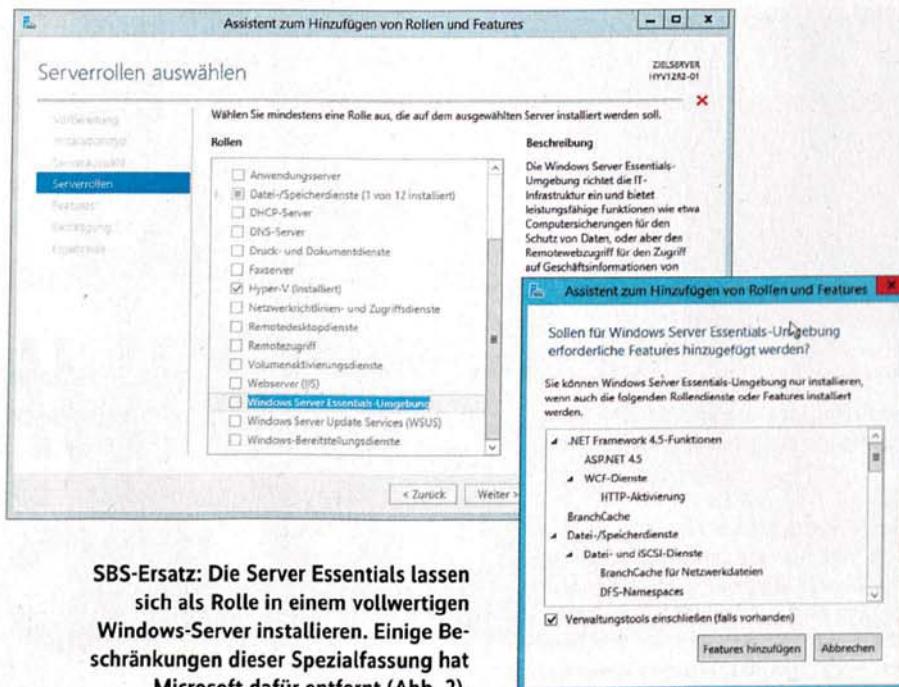
Grundlage soll man die Detailkonfiguration von Servern einfacher überwachen und steuern können. Neben Administratoren, die hier per Skript zugreifen können, dürfte das ein Angebot an Drittanbieter von Verwaltungssoftware sein, die leichter beherrschbare Schnittstellen erhalten.

Failover-Cluster, die eine Applikation beim Ausfall von Hardware am Laufen halten, folgen traditionell dem Quorum-Modell. Das besagt vereinfacht, dass stets eine bestimmte Zahl an Servern im Cluster lauffähig bleiben muss, damit er noch funktioniert. So verhindert das System eine „Split-Brain-Situation“, in der zwischen zwei Teilen eines Clusters (etwa zwischen zwei Servern) das Netzwerk ausfällt, die eigentlichen Server jedoch noch laufen. In dieser Situation muss jeder Teil des Clusters feststellen können, ob er noch die „Mehrheit“ im System hat. Dazu dient das Quorum, das bislang aus einer Festplatte bestand. Der Server, der die Platte ansprechen konnte, blieb in Betrieb, der andere schaltete sich ab, um die Datenkonsistenz nicht durch unkoordinierte Zugriffe zu gefährden.

Da Server 2012 R2 Cluster mit bis zu 64 Knoten unterstützt, ist ein so einfaches Quorum-Modell nicht mehr zeitgemäß. Wie schon in den Vorgängerversionen kann ein Cluster hier verschiedene Varianten nutzen. Neu ist, dass der Cluster



- Windows Server 2012 R2 erscheint gleichzeitig mit Windows 8.1 am 17. Oktober. Der Server ist im Gegensatz zum Client-Update kostenpflichtig.
- Neue Funktionen des Servers gibt es vor allem fürs Rechenzentrum: Storage-Optionen, Verfügbarkeit und Management.
- Der Hypervisor Hyper-V erweitert die Live-Migration und die asynchrone VM-Replikation.



SBS-Ersatz: Die Server Essentials lassen sich als Rolle in einem vollwertigen Windows-Server installieren. Einige Beschränkungen dieser Spezialfassung hat Microsoft dafür entfernt (Abb. 2).

nicht nur Empfehlungen zum Konfigurieren ausspricht (wie im Server 2008 R2), sondern diese gleich umsetzt (wie im Server 2012) und bei veränderten Bedingungen im laufenden Betrieb ändert. Das senkt den administrativen Aufwand und schützt vor Fehlkonfigurationen, da sich das günstigste Quorum-Modell nach automatisierbaren Regeln umsetzen lässt.

Als Ersatz für den entsorgten und beliebten Small Business Server sollten die „Windows Server Essentials“ dienen, eine Art Multifunktionsserver mit reduzierten Lizenzkosten für kleinere Unternehmen. Der Haken: Da Exchange nicht mehr im Paket enthalten ist, verlor das System schlagartig seine Attraktivität. Mit der Alternative, die Mailboxen per Office 365 in der Cloud zu halten, mochten sich bislang wenige Kunden anfreunden.

Im R2-Server rüdert Microsoft zwar nicht zurück, entfernt jedoch einzelne Beschränkungen der Essentials. Weiterhin verwaltet das System maximal 25 Benutzer, aber es darf künftig andere Windows-Server im Netzwerk geben. Zudem kann man die Essentials nun als Serverrolle auf einem „vollwertigen“ 2012-R2-Server aktivieren und so in einem größeren Netzwerk Funktionen wie das automatische Client-Backup oder einige zusätzliche Assistenten verwenden.

Virtualisierung mit Hyper-V

Die schärfste Konkurrenz liefern sich die Redmonder und ihre Mitbewerber der-

zeit auf dem Feld der Virtualisierung. Mit Hyper-V schloss Microsoft zu VMware auf, die mit vSphere jedoch konstant nachlegen.

Entsprechend ist der größte Teil der Entwicklungsarbeit in R2 erneut in den Hypervisor geflossen. Das betrifft insbesondere die Live-Migration, also das Verschieben laufender virtueller Maschinen von einem Hostserver zu einem anderen. Hier konnte Hyper-V in der 2012er-Fassung als erstes kommerzielles Produkt eine „Shared-Nothing Live-Migration“ vorstellen, bei der die Hostserver kein gemeinsames SAN mehr benötigen, sondern lediglich eine LAN-Verbindung. Die R2-Version fügt der Migration nun zwei Methoden zum Beschleunigen hinzu.

In Netzwerken bis 10-Gigabit-Ethernet sorgt eine Kompression der zu übertragenden Daten für einen schnelleren Ablauf. Da das System hierbei den Inhalt des Arbeitsspeichers der virtuellen Maschinen von einem Host auf den an-

Kosten der Lizenzen

- Standard Edition bleibt im Preis etwa gleich
- Datacenter Edition kosten etwa 30 Prozent mehr (4800 statt 6200 Dollar)
- Essentials-Preise steigen um etwa 20 Prozent von 420 auf 500 Dollar
- CALs (Client-Zugriffslizenzen) von Windows 2012 berechtigen zum Zugriff auf 2012 R2; Kunden müssen ausschließlich die eigentlichen Serverlizenzen erneuern

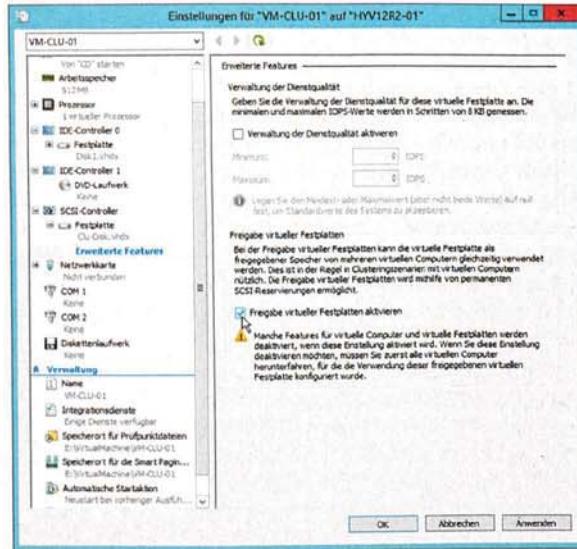
deren kopiert, kann es um erhebliche Datenmengen gehen. Kompression belastet die Host-CPU, daher prüft der Hypervisor laufend, ob Kapazität frei ist. Benötigen die laufenden VMs selbst die CPU-Leistung, verzichtet die Migration auf die Datenreduktion: Das Verschieben dauert dann wieder länger, aber es beeinträchtigt nicht die produktive Performance.

Verfügen die Hostserver über Hochgeschwindigkeits-Netzwerke der 40-Gigabit- oder InfiniBand-Klasse, kann der Administrator über spezielle Netzwerkkarten für noch schnellere Migrationen sorgen. Die RDMA-Adapter (Remote Direct Memory Access), die mit minimalem Protokollanteil und ohne lange CPU-Verarbeitung große Datenmengen direkt ins RAM des Ziel-Hosts schreiben, umgehen schlicht alles, was den Verkehr verzögern könnte. Microsoft berichtete auf seiner Hauskonferenz TechEd von internen Tests mit zwei, drei und vier solchen Adaptern. Konnten die zweite und die dritte Karte den Vorgang noch beschleunigen, gab es bei der vierten parallelen Karte keinen Vorteil mehr. Wie sich herausstellte, ist hier nicht das Netzwerk der Flaschenhals: Der begrenzende Faktor ist die Geschwindigkeit der RAM-Bausteine, die die Daten nicht mehr schneller annehmen können. Übertragungszeiten von unter zehn Sekunden für VMs mit 48 GByte Arbeitsspeicher bringen sicher Flexibilität in große Rechenzentren. Ob der Durchschnittskunde solche Formel-1-Abläufe braucht, steht auf einem anderen Blatt.

Auch die Replikation virtueller Maschinen, eingeführt mit dem Server 2012, hat eine erste Überarbeitung erfahren. Dabei handelt es sich um einen asynchronen Vorgang, der einzelne VMs periodisch auf einen anderen Host kopiert. Das Ziel ist ein schneller Wiederanlauf als „Disaster Recovery“. Anders als manche Mitbewerber erzeugt die Funktion keinen „Spiegel“ der replizierten VM, sondern arbeitet bewusst mit einer gewissen Latenz. Schaltet der Administrator auf das Replikat um, nimmt er einen geringen Verlust der Datenaktualität in Kauf.

So eignet sich die Technik längst nicht für alle schützenswerten Applikationen. Microsoft positioniert sie als kostengünstige Option, ohne hohen Aufwand Notfall-Rechenzentren an entfernten Standorten aufzubauen. Dabei sollen grundsätzlich schmalbandige WAN-Verbindungen für das Kopieren ausreichen. Da der Vorgang eine Delta-Replikation auf Basis von VM-Snapshots darstellt, hängt die tatsächlich anfallende Datenmenge davon ab, wie

Gastgeber: Virtuelle Festplatten im VHDX-Format können als Cluster-Disks dienen. Dadurch benötigen VM-Cluster keine umständliche SAN-Anbindung mehr (Abb. 3).



viel sich an der Quelle ändert. Je mehr Dynamik in den Daten einer Replika-VM herrscht, desto mehr Traffic entsteht. Auch der Bedarf an Disk-I/O auf dem Hostserver an der Quelle ist nicht zu unterschätzen. Die VM-Replikation kann man lediglich als eine nutzbare Technik unter mehreren ansehen, nicht als Allzweckmittel.

Neu im R2-Server ist hier zweierlei: Erstens kann der Administrator das Intervall für die Replikation nun steuern und in der Dauer von 30 Sekunden bis 15 Minuten selbst festlegen. Zuvor war ein Abstand von fünf Minuten fest vorgegeben. Zweitens, und das ist hilfreicher, erlaubt die Replikation nun mehr als nur ein Ziel. So kann man dieselbe VM in ein eigenes Notfall-RZ und parallel mit der Cloud replizieren.

Pinguine in Redmond

Hyper-V arbeitet mit Linux-Gästen, doch das hat sich anscheinend nicht allzu weit herumgesprochen. Dass Microsoft durch die dafür nötigen „Integration Services“ rein zahlenmäßig zu den bedeutenderen Code-Beitragenden des Linux-Kernels zählt, ist eher eine Ironie der Geschichte. Bislang waren Linux-VMs trotzdem eher in der zweiten Klasse der Hyper-V-Gäste zu finden, denn sie mussten auf einige Funktionen des Hypervisors verzichten.

In der 2012-R2-Inkarnation soll sich das ändern. Durch eine neue Fassung der Integration Services reicht Hyper-V praktisch alle Funktionen an den Pinguin durch, die er auch den Windows-VMs anbietet. Dazu gehört vor allem Dynamic Memory: Mit dieser Option kann eine VM im laufenden Betrieb zusätzlichen Arbeitsspeicher vom Host anfordern, um damit ihre Applikationen zu versorgen. Benötigt sie den Speicher nicht mehr, kann die VM

ihm an den Host zurückgeben, damit dieser ihn an andere VMs vergibt.

Eine weitere Funktion ist eine Backup-Integration mit dem Host: Sie kommt den „Volume Shadowcopy Services“ (VSS) von Windows zwar nicht nahe, erlaubt jedoch immerhin eine Dateisystem-Konsistenz. Mithilfe des beteiligten Dienstes kann der Host dem Gast mitteilen, dass ein Backup ansteht, und Linux bringt das Dateisystem in einen definierteren Zustand.

Weitere Detailverbesserungen in Hyper-V betreffen das Clustering: Fährt der Administrator einen Hostserver herunter, kümmert sich dieser ohne weiteren Eingriff darum, zunächst seine VMs auf andere Hosts zu migrieren. Stellt der Hypervisor fest, dass eine VM ihre Netzwerkverbindung verloren hat, kann er ein Live-Migrieren auf einen anderen Host einleiten, sofern der betreffende Netzwerklink dort noch funktioniert.

Zwei Neuerungen im Storage-Stack des Server 2012 R2 kommen direkt den virtuellen Maschinen zugute. Durch „Shared VHDX“ (gemeinsam genutzte virtuelle Festplatten) kann der Administrator nun Gast-Cluster aufbauen, ohne sich um eine SAN-Anbindung der beteiligten VMs kümmern zu müssen. Liegt

X-Wertung

- ⊕ Hyper-V mit schnellerer Live-Migration
- ⊕ Verwaltung von Linux-VMs erweitert
- ⊕ Storage Tiering beschleunigt internen Datenzugriff
- ⊖ unklare Produktstrategie mit Updates und neuen Versionen
- ⊖ neues Server-Release muss man voll lizenziieren
- ⊖ nur ein Jahr Entwicklungszeit seit dem Vorgänger

infotecs

weit über
500 000
Installationen allein in
den letzten 5 Jahren

VIPNet

Eine andere Art VPN

- ▼ Einfache Integration in beliebige Topologien
- ▼ Direkte verschlüsselte Punkt-zu-Punkt-Verbindungen
- ▼ Unbegrenzt skalierbar
- ▼ Transparent für alle Anwendungen und Dienste
- ▼ Soft- und hardwarebasierte Lösungen
- ▼ Hervorragendes Preis-Leistungs-Verhältnis

Eine vollfunktionsfähige Demoversion

unter:
www.infotecs.de
info@infotecs.de
 +49 30 206 43 66-0

Seien Sie unser Guest bei der IT-Sicherheitsmesse
it-sa vom 8.-10. Oktober 2013 in Nürnberg
am Stand 12.0-558 (BITKOM Gemeinschaftsstand).

itsa 2013
Die IT-Security Messe und Kongress
The IT Security Expo and Congress

Für einen kostenfreien Zutritt zur Messe wenden

Erweitern Sie Ihre Cloud

Kenntnisse und Kompetenzen
29. - 30. Oktober 2013
Congress Frankfurt



Powering
THE CLOUD

VIRTUALIZATION WORLD SNW EUROPE DATACENTER TECHNOLOGIES

In diesem Jahr feiern wir 10 Jahre SNW Europe und das 5-jährige Bestehen von Datacenter Technologies und Virtualization World. Wählen Sie aus inzwischen über 130 Präsentationen zum Thema Big Data, Managed Services, Outsourcing, Storage, Virtualisierung, Security, Datacentre u.v.m aus. Networken Sie mit über 1500 Ihrer Kollegen im Herzen Europas und treffen Sie über 70 führende Anbieter und Experten.

2013 Sponsoren



EMULEX



Quantum

Seagate



Sparen Sie die Eintrittsgebühr in Höhe von 120€!
Kostenlose Registrierung mit Aktionscode P54M13

REVIEW | BETRIEBSSYSTEME

die virtuelle Daten-Platte des VM-Clusters auf einem hochverfügbaren Speicher (einem Cluster-Shared Volume im SAN oder einer SMB-3.0-Freigabe), ergibt dies einen gültigen Cluster-Aufbau für anspruchsvolle Applikationen.

Laufen auf dem Hypervisor viele VMs mit I/O-hungrigen Applikationen, kann das Speichersystem in Bedrängnis geraten. Mit „Quality-of-Service“ für Speichersysteme (Storage QoS) versucht Hyper-V dem entgegenzuwirken. Bestimmte VMs kann man bezüglich ihres Speicherzugriffs drosseln, um den verfügbaren Durchsatz für andere VMs nicht über Gebühr einzuschränken. Umgekehrt lässt sich für VMs ein Storage-Minimum vorgeben, damit ein gewisser Datenfluss immer gewährleistet ist.

Vertrauen in der Domäne

Active Directory wartet mit zwei Ergänzungen auf, die unbekannte Geräte besser an Ressourcen des Unternehmens anbinden sollen. Bislang beruhte das Konzept der Windows-Domäne darauf, dass das Endgerät (klassisch: der Firmen-PC) und die Anmeldeserver einander vertrauen. Das wurde durch die Aufnahme des PCs in die Domäne als eine Art Vertrag besiegelt. Wer sich an einem „vertrauenswürdigen“ PC anmeldete, wurde als bekannter Benutzer behandelt und durfte interne Dateien und Dienste nutzen.

Durch den BYOD-Hype (Bring Your Own Device) standen Administratoren vor dem Dilemma, entweder völlig unbekannte Privat-PCs der Mitarbeiter in die Domäne aufzunehmen zu müssen oder den Anwendern den Zugriff zu verweigern. Mit dem „Workplace Join“ gibt es im Server 2012 R2 eine Art Mittelweg. Der Privatrechner eines Mitarbeiters kann so eine Art Gaststatus in der Domäne erhalten und auf einen reduzierten Satz von Ressourcen zugreifen. Das Gerät dient als zweiter Faktor beim Authentisieren, denn beim „Workplace Join“ erhält es ein Zertifikat, das die Kombination aus Benutzer und Gerät bestätigt. Es handelt sich jedoch immer noch um ein Privatgerät außerhalb der Kontrolle der Unternehmens-IT, daher soll es nicht denselben Zugriff wie ein verwalteter (und per Anti-Virus, Gruppenrichtlinien und Firewall geschützter) PC erhalten. Diese Art der begrenzten Aufnahme soll neben Windows-PCs auch RT-Tablets und iOS-Geräten offenstehen; eine Roadmap für Android ist nicht bekannt.

Ein zweiter Ansatz mit ähnlichem Ziel ist der „Web Application Proxy“. Der

Windows-Dienst integriert die vor sieben Jahren eingeführten „Active Directory Federation Services“ (ADFS) leichter mit lokalen Webanwendungen. ADFS waren ursprünglich dazu gedacht, das Anmelden bei Websites externer Dienstleister besser zu steuern. Dazu definieren sie eine Art Vertrauensstellung zwischen dem eigenen und dem fremden Unternehmen. Der „Web Application Proxy“ erweitert das um eine Anbindung an eigene Ressourcen, die etwa als DMZ-Dienste nicht auf das interne Active Directory zugreifen sollen.

Fazit

Gemessen an der Zahl und dem Umfang der Neuerungen darf Server 2012 R2 durchaus als vollwertiges neues Release gelten. Dass Microsoft seine Server abwechselnd als „Hauptversionen“ mit Jahreszahl und als „Unterversionen“ mit angehängtem R2 vermarktet, hat zwar seit einigen Jahren Tradition, nachvollziehbar ist es für Kunden kaum.

Besonders die aktuelle Produktrunde dürfte bei so manchem Einkäufer und vielen Administratoren für mehr als nur Stirnrunzeln sorgen. Seit dem Release des Vorgängers ist gerade mal ein Jahr vergangen, wenn am 17. Oktober dieses Jahres der Server 2012 R2 als neues Betriebssystem in den Handel kommt. Wer die neuen Funktionen nutzen will, muss selbstverständlich neue Lizenzien kaufen.

Diese atemlose Politik aus Redmond sorgt nicht nur bei Kunden für Verwirrung, sondern stellt auch Microsofts Handelspartner und Integratoren vor eine schwierige Aufgabe. Hatten sie gerade erst begonnen, Server 2012 an die Kunden zu verkaufen, hören diese schon jubelnde Ankündigungen des R2-Nachfolgers. Das degradiert das verfügbare Release zur „Zwischenversion“, und so manches Unternehmen stoppt seine Projekte, um auf die nächste Fassung zu warten.

Auf der technischen Seite gibt es durchaus Bemerkenswertes im kommenden Windows Server. Microsoft empfiehlt sein Betriebssystem vor allem für Rechenzentren, indem es die Server-Virtualisierung und die Storage-Funktionen weiterentwickelt. Kleinere Firmen hingegen möchte man in Redmond zunehmend als Cloud-Kunden gewinnen. (fo)

Nils Kaczenski

ist in der Windows-Community als MVP aktiv und leitet das Consulting bei einem IT-Dienstleister in Hannover.





Client-Betriebssysteme aus dem RZ mit XenDesktop 7

Ausgeliefert

Fred Hantelmann, Jens-Henrik Söldner

XenApp gehört in den Bereich serverbasiertes Computing und soll laut Citrix und Microsoft dessen Remote Desktop Services veredeln. XenDesktop bringt Client-Betriebssysteme ins Rechenzentrum und will Vorreiter im Segment virtuelle Desktop-Infrastruktur sein. Mit XenDesktop 7 vereint Citrix nun beide Techniken.

Vor fünf Jahren brachte Citrix XenDesktop in der Version 2.0 auf den Markt. Das Unternehmen verfolgte damit eine neuartige Strategie, Arbeitsplätze zentral bereitzustellen, bestehend aus den getrennt verwalteten Komponenten Betriebssystem, Benutzerprofil und Anwendungen. Erstere sind idealerweise in provisionierbaren Dateien gekapselt, Profile liegen auf Servern im Netzwerk und Applikationen virtualisiert vor, entweder per Stream auslieferbar in Form einer paketierten Anwendung oder veröffentlicht mit Mitteln von XenApp.

Bisher hatten Kunden des XenDesktop ab einer Enterprise-Lizenz automatisch auch eine für XenApp, die ihren Berechtigungen für Benutzer oder Geräte entsprach. Das gilt im Grunde ebenso für XenDesktop 7, jedoch gibt es keine Express Edition mehr zum kostenlosen Betrieb von bis zu 10 virtuellen Desktops

im Gegensatz zur Vorgängerin (Version 5.6). Die Version 7 ist in den Stufen VDI (Virtual Desktop Infrastructure), App Edition, Enterprise und Platinum erhältlich. Die zweite Stufe können Kunden, die einen aktiven Wartungsvertrag der beiden höheren Level besitzen, ohne Weiteres nutzen. Die Migration vom früheren XenApp Advanced aus setzt ein kostenpflichtiges Update über Citrix' Trade-up-Programm voraus.

iX hat die neue Version des XenDesktop Platinum im Labor untersucht. Eine strenge Trennung aller Dienste und Werkzeuge des XenDesktop 7 fand jedoch nicht statt. Dennoch umfasste die Konfiguration immerhin 15 virtuelle Maschinen, betrieben mit VMwares ESX 5.1. Für die Querschnittsdienste kamen oberhalb des Windows Server 2012 ein Domänen-Controller, Zertifikatsautorität nebst Lizenzdienst und ein Streaming-Server für Microsofts „Application Virtualization“ (App-V) sowie ein NAS-Simulator von EMC namens VNX hinzu (VNX steht für Virtual NS- und CX-Plattformen des Herstellers). Das Herz des XenDesktop 7 bildete ein W2K12-Server mit den XenDesktop-Rollen Delivery Controller, StoreFront, Studio und Director.

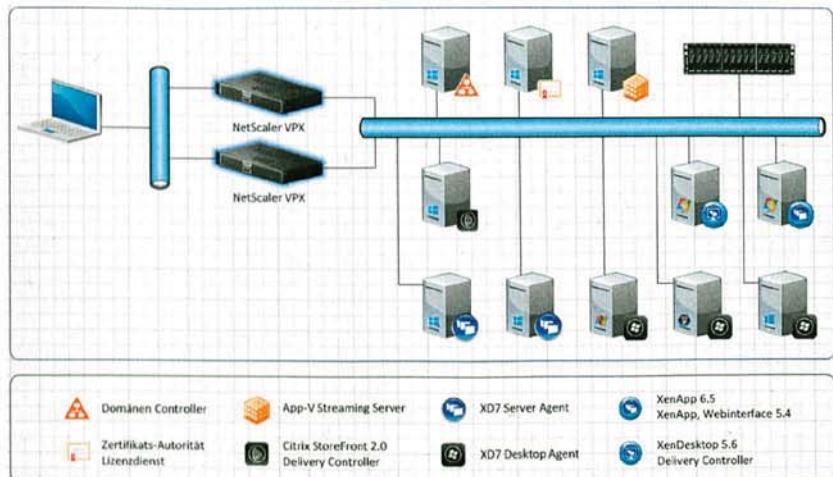
Im Test: Mehrere Windows-Versionen

Zwei weitere W2K12-Systeme mit dem „Delivery Agent für Server OS“ und drei Maschinen mit Client-Betriebssystemen (Windows XP, 7 und 8) samt dort aufgespieltem Delivery Agent für Client OS lieferten Ressourcen zur Veröffentlichung durch XenDesktop 7. Den Zugriff von außen sollte ein hochverfügbares Pärchen bestehend aus NetScaler VPX Appliances regeln. Schließlich kam noch je ein Rechner mit Windows Server 2008 R2, bestückt mit den Basiskomponenten aus XenApp 6.5 und XenDesktop 5.6 hinzu.

Auf Grundlage des XenDesktop 5.6 wirken die Neuerungen auf den ersten Blick kosmetisch. Die Funktionsbausteine heißen nur noch „Delivery Controller“, „Studio“ und „Director“; der frühere Vorname „Desktop“ ist entfallen. Virtuelle Desktops mit Windows XP oder Vista unterstützt Citrix offiziell nicht mehr. Wer die nunmehr von Microsoft nicht mehr gepflegten Varianten dennoch einsetzen möchte, dürfte letztlich eine Enttäuschung erleben: Das Medium zum Installieren enthält den „Virtual Delivery Agent for Windows Desktop OS Version 5.6“ und erlaubt dem Administrator das Instal-

iX-TRACT

- Citrix' XenDesktop 7 dient zum Bereitstellen von Desktop-Betriebssystemen und Applikationen.
- In die Version 7 hat der Hersteller die Funktionen von XenApp 6.5 integriert.
- XenDesktop 7 ist mit Windows Server 2K8R2 und 2K12 sowie den Clients Windows 7 und Windows 8 einsetzbar.



Laboraufbau: Am Test waren außerdem die Vorversionen von XenDesktop 7 beteiligt: XenDesktop 6.5 und XenApp 5.6 (Abb. 1).

lieren auf Windows XP. Registrieren möchte sich das Betriebssystem bei Citrix Studio jedoch nicht. Citrix Desktop Service on Windows XP moniert in seinem Ereignislog „VDA Functional Level too low for Catalog“.

XenApp-Administratoren konfrontiert Citrix bei XenDesktop 7 mit einem Ersatz der über mehrere Generationen gepflegten „Independent-Management-Architektur“ (IMA) durch die „FlexCast-Management-Architektur“ (FMA). Lokaler Host-Cache ist Geschichte, und statt des bisher zweistufigen Installierens von XenApp und anschließendem Farmbeitritt genügt nun das Einrichten eines „Virtual Delivery Agent for Windows Server OS“ nebst Verweis auf den Delivery Controller. Das vereinfacht das Bereitstellen zentral betriebener Applikationen. Jedoch heißt das, seine Kenntnisse über XenApp zu großen Teilen ad acta zu legen und neu lernen zu müssen. Neben dem lokalen Host-Cache gibt es keine Zonen und folgerichtig keine Datensammelpunkte mehr. Diese Elemente sind in XenDesktop 7 in Sites konsolidiert. Das wiederum dürfte XenDesktop-Administratoren seit Version 5.0 des Produkts bekannt sein.

Von langer Hand geplant

Mit XenDesktop 5 verfolgten die Designer das Ziel, eine Architektur zum Bereitstellen zu etablieren, die jenseits der bis dato bekannten Grenzen skaliert. Citrix' CTO Harry Labana skizzierte im Oktober 2010 in einem Interview, dass die erwartete Cloud-Ära möglicherweise Implementierungen für mehrere Hunderttausend Benutzer benötigen werde, die

außerdem mandantenfähig ausgelegt sein sollten. Die Voraussetzungen dazu wolle man mit FMA liefern. Bei der Gelegenheit stellte Labana in Aussicht, dass XenApp zukünftig vielleicht auch oberhalb FMA operieren und Citrix eventuell die Funktionen von XenDesktop und XenApp in einem verschmolzenen Produkt anbieten werde: Das Resultat ist XenDesktop 7.

Einen gravierenden Schnitt erleben die Administratoren beider Produkte beim Anmelden am System: Das althergebrachte Web-Interface hat der Hersteller durch die Komponente „StoreFront“ ersetzt, mit dem Anwender von Citrix' CloudGateway erste Erfahrungen sammeln durften. Es handelt sich um die neue Gegenstelle zum Receiver, die für Authentifikation und das Ausliefern von Ressourcen zuständig ist. Der Authentifikationsdienst prüft Benutzerkennungen und verteilt erfolgreich bestätigte Identitätskennungen an Komponenten der XenDesktop-Site, sodass der Zugriff auf XenDesktop-Ressourcen über einen zentralen Anmeldepunkt stattfinden kann (Single Sign-on).

StoreFront liefert die zentral konfigurierten Veröffentlichungen automatisch als Web- oder Site-Service aus. Beim früheren Web-Interface waren die Dienste zu den beiden Kategorien getrennt zu erzeugen. Citrix' Receiver für Web präsentiert die Publikationen gruppiert in Desktops oder in Applikationen. Während der Administrator beim Konfigurieren den Applikationen ähnlich dem früheren AppCenter von XenApp 6.5 ein beliebiges Icon zuordnen kann, bietet Citrix' Studio für Desktops keinen vergleichbaren Konfigurationspunkt. Wer dennoch seinen Citrix-Desktops individuellen Schliff

Java

Sprache & Programmierung

VIDEO-TRAINING

1 DVD, deutsch
1 gedrucktes Trainingsmanual
224 Seiten/ 4-farbig
ISBN 978-3-95539-052-5
€ 99,95 [D/A]

auch als
**STREAMING-
VERSION**

Einzigartiges didaktisches Konzept

Ideal für Einsteiger und Studierende

opensourceschool.de



KURSE

Programmierung

21.-23.10.	Einstieg in C++
21.-23.10.	Java für Einsteiger
04.-06.11.	Applikationsentwicklung für Android

Webentwicklung

21.-23.10.	TYPO3 für Webdesigner
23.-25.10.	JavaScript
23.-25.10.	OpenLayers

Administration

22.-24.10.	Big Data Anwendungen mit Hadoop
04.-06.11.	Administration von OTRS
11.-14.11.	Linux Performance Tuning

verleihen möchte, muss sich mit den PowerShell-Kommandos des „XenDesktop Software Development Kit“ (SDK) anfreunden (siehe Aufmacher).

Konfigurierte Struktur als App-Kachel

Will jemand eine der veröffentlichten Anwendungen nutzen, muss er sie vorher abonnieren. Der Kontext „Apps“ ist linker Hand mit einem Plus-Zeichen versehen; ein Klick darauf öffnet ein Menü. Dort darf man die vom XenDesktop-Administrator konfigurierte Struktur einzelner Anwendungen auswählen, die StoreFront als Kacheln auf der Seite mit den Apps des Web-Dialogs platziert. Manche der Bildchen sehen allerdings ziemlich verwaschen aus.

Das Grundprinzip der Veröffentlichung von Desktop- oder Anwendungen bei XenDesktop 7 besteht aus dem Bündeln von Maschinen zu Katalogen und anschließendem Erstellen von Liefergruppen (Delivery Groups). Maschinenkataloge entstehen aus vorhandenen oder aus dynamisch angelegten virtuellen oder physischen Maschinen. Jede dieser Aufstellungen enthält gleichartige Maschinen, die jeweils einer der drei Klassen Windows Desktop OS, Windows Server OS oder Remote PC Access angehören. Dynamische Maschinen erzeugt XenDesktop mit den Provisioning Services (PVS) oder Machine Creation Services von Citrix. Letztere interagieren mit einem der unterstützten Hyperviso-

ren ESXi, Hyper-V oder XenServer und zielen auf das Ausrollen virtueller Maschinen ab. Für Administratoren von XenDesktop 5 sind das vertraute Komponenten.

Liefergruppen wirken auf Maschinenkataloge. In XenDesktop 7 deklarieren sie veröffentlichte Desktops und/oder Applikationen. Desktop-Betriebssysteme können selbst Applikationen veröffentlichen, jedoch lediglich eine einzelne zurzeit. Im Test waren von einer virtuellen Maschine mit Windows 8 neben dem Desktop die Anwendungen Putty und Paint veröffentlicht. Sobald jemand eine der Komponenten aktiviert hatte (etwa Paint), war das System blockiert und der am System aktive Anwender konnte keine der anderen zusätzlich starten (weder Desktop noch Putty). Anders als beim Windows Server 2012, der multiverfähig ist, kann Windows 8 keine vorhandene Sitzung erweitern. Citrix' Director protokolliert solche Versuche als „Benutzerverbindungsfehler“.

Beim Veröffentlichen einer Applikation muss der Administrator anders als bei XenApp 6.5 zweistufig vorgehen: Zunächst erzeugt er zu einer ausgewählten Liefergruppe eine Published Application über die Aktion „Add Application“. Ein Wizard zeigt alphabetisch sortiert alles, was er unter „Anwendung“ im voreingestellten Suchpfad auf einem Mitglied des Maschinenkatalogs findet und zusätzlich etwa konfigurierte App-V, die Streaming-Server ausliefern. Das Bildschirmfoto (Abbildung 2) zeigt ein Beispiel. Wer App-V einsetzen möchte, muss auf allen

Mitgliedern des spezifischen Maschinenkatalogs dessen Client (für Remote Desktop) installieren und konfigurieren. Eine manuelle Konfiguration einer Applikation, die der Auswahl dialog nicht präsentiert, ist ebenfalls möglich.

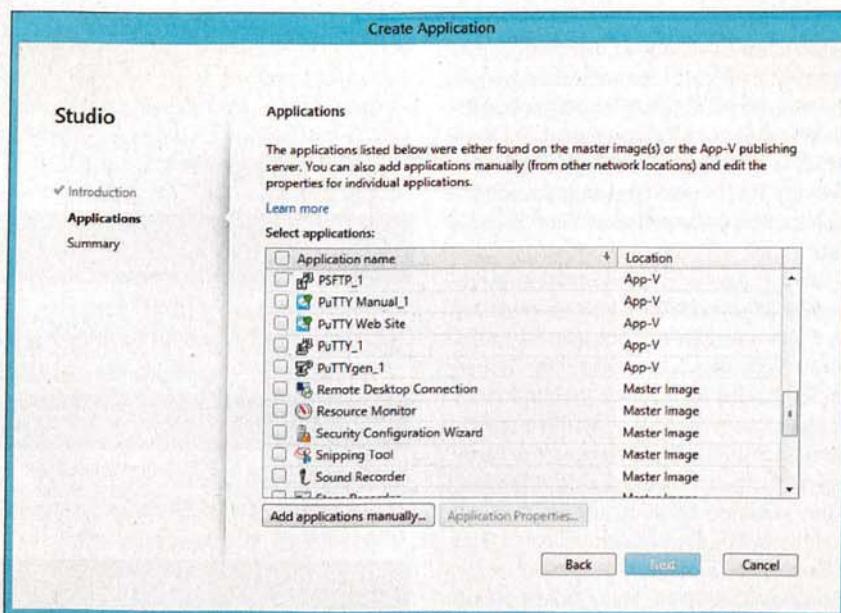
In einem zweiten Schritt geht es ans Einstellen weiterer Feinheiten über einen Eigenschaftskonfigurator für die zuvor veröffentlichte Applikation. Hier stehen zur Wahl die von XenApp 6.5 her bekannten Optionen wie Anpassen des Icons, Zuordnen zu einer Gruppe und damit Darstellen in einem Menü oder Beschränken des Zugriffsrechts auf bestimmte Benutzer und Benutzergruppen. Erweiterte Optionen gemäß AppCenter wie die zum Festlegen des Verschlüsselungsgrads oder der maximalen Farbqualität kennt der Dialog-Vorrat von Citrix' Studio nicht.

Feinarbeiten von Hand erforderlich

Im Test boten die individuellen Publikationen der Anwendungen kleine Herausforderungen. Als Grundlage diente Microsofts Management Console mit einem Snap-in der Group Policy Management Console. Die Anwendung sollte mit eigenem Icon erscheinen. Das stammte aus der innerhalb von `gpmc.msc` als Verweis deklarierten Bibliothek `C:\Windows\System32\gpoadmin.dll`. Die daraus erzeugte ICO-Datei mit den Auflösungsstufen 32, 24 und 16 Pixel Kantenlänge und in RGBA-Farbqualität erkannte der „Select Icon“-Dialog als „Application Settings“ in Studio, jedoch blieb die OK-Taste nach Auswahl des Icons schattiert und damit inaktiv. Erst nach einem Wechsel auf „Choose from Citrix default icons“ und zurück sowie erneuter Auswahl des Bilds klappte das Zuweisen des individuellen Icons.

Weitere Neuerungen in XenDesktop 7: Ein Konfigurations-Logging ist Standard und somit ohne zusätzliche Konfiguration aktiv. Die Administrationsrechte sind durch das Kontextbündel „Rolle“ und „Reichweite“ bestimmt, was eine feinere Granularität als bisher erlaubt. Die Machine Creation Services (MCS) können Betriebssystemaktivierungen über Key Management Services (KMS) beziehen.

Aus Sicht von XenApp zählt das Bereitstellen zusätzlicher Server mit MCS zu den Neuerungen. Das Spiegeln von Benutzern (Shadowing), das heißt, die Assistenz durch Helpdesk-Mitarbeiter, operiert nun oberhalb von Windows Remote Assistance. Für sein hauseigenes Paketierungsprodukt, eventuell bekannt



Liste: Neben den Anwendungen im Suchpfad sind dort konfigurierte App-Vs zu finden (Abb. 2).

Tel. 0 64 32 / 91 39-753
 Fax 0 64 32 / 91 39-711
 vertrieb@ico.de
 www.ico.de/ix



Innovative Computer • Zuckmayerstr. 15 • 65582 Diez

The screenshot shows the Citrix Receiver interface. In the top left, it says "Citrix Receiver". Below that is a sidebar with "Alle Apps" and "Active Directory Tools". Under "Active Directory Tools", there are five items: "Active Directory Administrative ...", "Active Directory Domains and T...", "Active Directory Sites and Servi...", "Active Directory Users and Com...", and "Adsedit".

Kategorie: StoreFront stellt die veröffentlichten Anwendungen strukturiert dar (Abb. 3).

unter „Citrix“ Streaming Server“, hat der Hersteller vor der Markteinführung das „Aus“ verkündet und verweist seither auf App-V 5 als Alternative.

SmartAuditor, bisher nur für Kunden mit XenApp-Platinum-Lizenz zum Aufzeichnen von Sitzungen einsetzbar, fehlt ebenfalls in XenDesktop 7. Eine Rückfrage beim Hersteller ergab, dass der SmartAuditor Code auf IMA basiert und diese nicht mehr Bestandteil von XenDesktop 7 ist. Citrix verweist aktuell auf „Citrix ready“-Produkte von Drittherstellern.

Abschließend seien noch ausgewählte Erfahrungen mit dem Anbinden des NetScaler als Gateway zusammengefasst. SecureGateway aus XenApp 6.5 ist an das Web-Interface gebunden, zudem hat Citrix nun das End-of-Life für den 14. Mai 2015 angekündigt (siehe „Alle Links“).

„Gateway“ hatte Citrix bereits in „NetScaler Gateway“ umbenannt und dessen Lebenszyklus soll spätestens am 31. März 2016 enden. Wer seine Citrix-Infrastruktur absichern will, muss also bald auf NetScaler migrieren.

NetScaler leicht angeschlossen

Die Konfiguration des NetScaler für XenDesktop 7 gelingt manuell oder Wizard-gestützt mit wenigen „erfahrenen“ Handgriffen. Per Wizard richtet der Konfigurator gleich Lastverteiler mit ein, die vorhandene StoreFront- und XML-Broker-Server hochverfügbar beziehungsweise ausfallsicher anbinden. Der Webbrowser im Client kommuniziert mit NetScaler über HTTPS (tcp/443) und Citrix Receiver im Client über ICA (tcp/1594) beziehungsweise Session Reliability (tcp/2598). Letztere Protokolle transportiert ein HTTPS-Tunnel zwischen Client und NetScaler. Das funktioniert aber nur mit einem Zertifikat.

Gängige Praxis ist, aus NetScaler heraus eine Anforderung für ein Zertifikat zu generieren, in einer unternehmenseigenen Zertifizierungsstelle ein passendes zu erzeugen und das Ergebnis zu importieren. Jeder virtuelle Gateway-Server im NetScaler benötigt ein eigenes Zertifikat, und der zugehörige vollqualifizierte Systemname muss netzwerkweit auflösbar sein. Zugreifende Clients und bediente Komponenten des XenDesktop 7 schließlich benötigen das öffentliche Stammzertifikat im Speicher der vertrauenswürdigen Zertifizierungsstellen.

Bei XenDesktop 5.6 und XenApp 6.5 konnten Administratoren den Anmeldepunkt zu ihrer Site beziehungsweise Farm menügestützt wahlweise auf der Seite von NetScaler oder des Web-Interface platzieren. Bei StoreFront 2.0 stellt das Konfigurationswerkzeug keine geeignete Option dazu bereit. In manchen Fällen ist es wünschenswert, das Login außerhalb NetScalers zu positionieren, etwa wenn er als Proxy für mehrere Sites fungieren und jede Site mit individuellem Layout erscheinen soll.

Wer auf der Konfigurationsseite „Authentication“ zum virtuellen Gateway Server die Option „Enable Authentication“ abwählt, dem liefert StoreFront zunächst die Nachricht „Anmeldung kann nicht abgeschlossen werden“. Das kennzeichnet der Hersteller in seiner Online-Dokumentation eDocs als bekanntes Problem von StoreFront 2.0, aber nicht von XenDesktop 7. Im Test gelang das Platzieren des Anmeldepunkts außerhalb des NetScalers durch manuelles Editieren der XML-formatierten Konfigurationsdatei *web.config* des erzeugten StoreFront-Store und anschließenden Neustart der von ihm genutzten Internet Information Services (IIS).

Ein weiteres merkwürdiges Verhalten von StoreFront 2.0 tritt beim Öffnen einer Desktop-Verbindung direkt nach der Benutzeranmeldung auf, falls die konfigu-

Neueste Intel® XEON® E5-Prozessoren – Das Herzstück eines flexiblen und effizienten Rechenzentrums!



XANTHOS R25B 2HE SERVER

- 2x Intel® Xeon® E5-2603v2 1,8GHz 6,4GT 10MB 4C
- 8x 4GB DDR3 RAM
- 2x 1TB 24x7 SATA-2 HDD
- Intel® Remote Management

inkl. MwSt.

1902,-

exkl. MwSt.

1599,-

Art.Nr. Bto-3000532

XANTHOS P45B TOWER SERVER

- 2x Intel® Xeon® E5-2620v2 2,1GHz 7,2GT 15MB 6C
- 8x 4GB DDR3 RAM
- 4x 1TB 24x7 SATA-2 HDD
- Intel® Remote Management

inkl. MwSt.

2378,-

exkl. MwSt.

1999,-

Art.Nr. Bto-3000534

XANTHOS R35A 3HE SERVER

- 2x Intel® Xeon® E5-2620v2 2,1GHz 7,2GT 15MB 6C
- 8x 8GB DDR3 RAM
- 4x 1TB 24x7 SATA-2 HDD
- Adaptec 7805 + NAND BBU
- Intel® Remote Management

inkl. MwSt.

3521,-

exkl. MwSt.

2959,-

Art.Nr. Bto-3000533

Know-how und Tutorial zum C++11-Standard

iX DOSSIER

Einstieg in C++11

Grundlagen, Einschätzung, Tutorial

Spannende und gründlich recherchierte Artikel aus der iX erwarten Sie:

- ✓ Neue Funktionen und bessere Performance
- ✓ Tutorial I: Threads und Synchronisierung
- ✓ Tutorial II: Binder, generalisierte Lambda-Funktionen
- ✓ Tutorial III: Move-Semantik, Zufallszahlen und Netz-I/O
- ✓ Resümee zur Verbreitung des aktuellen Sprachstandards
- ✓ Thread-Programmierung unter C++11

Jetzt als eMagazin für nur 2,99 € laden >

rierte Liefergruppe neben Applikationen genau einen Desktop veröffentlicht. Der zugeordnete Maschinenkatalog bestand aus identisch konfigurierten Serversystemen mit installiertem „Delivery Agent for Server OS“. Das Verhalten konnte eine Modifikation der *web.config* von Store-Web des Store ändern. Dort wurde einfach das Attribut *autoLaunchDesktop* zum Konfigurationsobjekt *userInterface* auf „false“ gesetzt.

Citrix und zahlreiche Blogs bieten ausführliche Anleitungen zum Migrieren von XenApp- und XenDesktop-Installationen auf XenDesktop 7. Für XenDesktop 5.x gibt es ein direktes (in-place) Update des Delivery Controller und der Delivery-Agenten. Der Migrationspfad von Web-Interface zu StoreFront hingegen erfordert eine erneutes Installieren und Konfigurieren.

Fazit

Wer XenApp oder XenDesktop im Einsatz hat, erlebt bei XenDesktop 7 zunächst die Verschmelzung in ein Produkt. Es harmoniert mit Microsofts Windows 8 und Server 2012, was für die Vorgänger nicht gilt. Während für Administratoren des XenDesktop 5.x beim Upgrade nur wenig Neuland zu erkunden ist, heißt es für XenApp-Verantwortliche, das vorhandene Know-how in wesentlichen Teilen durch neues zu ersetzen. Übrigens genügt ein einzelnes System zum Aufbauen einer Umgebung mit XenDesktop 7 App Edition nicht: Delivery Controller und Virtual Delivery Agent for Windows Server OS sind miteinander nicht verträglich.

Während das althergebrachte XenApp helfen konnte, den operativen Aufwand beim Bereitstellen von Applikationen zu reduzieren, liegt der Nutzen von XenDesktop eher in der zentralen Verwaltung und Pflege unternehmweit eingesetzter Clients. Die Datenhaltung im RZ will den Schutz vor Datenverlust verbessern. Das soll gleichermaßen für Offline-Desktops

gelten, wenn sie oberhalb des XenClient arbeiten und der Synchronizer die Änderungen regelmäßig mit dem Bestand im Rechenzentrum abgleichen kann. Diese, in XenDesktop 7 Enterprise und Platinum enthaltenen Komponenten, fanden im Test keine Berücksichtigung. Wer einen ersten Eindruck vom XenDesktop gewinnen möchte, kann eine Demo- und eine Testversion (90 Tage, 99 Benutzer) nach Registrierung bei Citrix herunterladen (<https://www.citrix.com/products/xendesktop/try.html>)

Mittelfristig ist der Umstieg für Bestandskunden mit Wartungsvertrag unumgänglich. Zu XenDesktop 5.6 hat Citrix das letzte Kaufdatum (End of Market EOM) auf den 17.12.2014 gelegt. Zu XenApp 6.5 hat Citrix den EOM-Termin kürzlich auf den 24.02.2016 nach hinten geschoben, sodass XenApp-Kunden mehr Zeit für die Migration bleibt. Der Lebenszyklus endet gemäß Citrix jeweils sechs Monate nach EOM. (rh)

Dr. Fred Hantelmann

ist bei der Silpion IT-Solutions GmbH als Senior IT-Architekt tätig.

Jens-Henrik Söldner

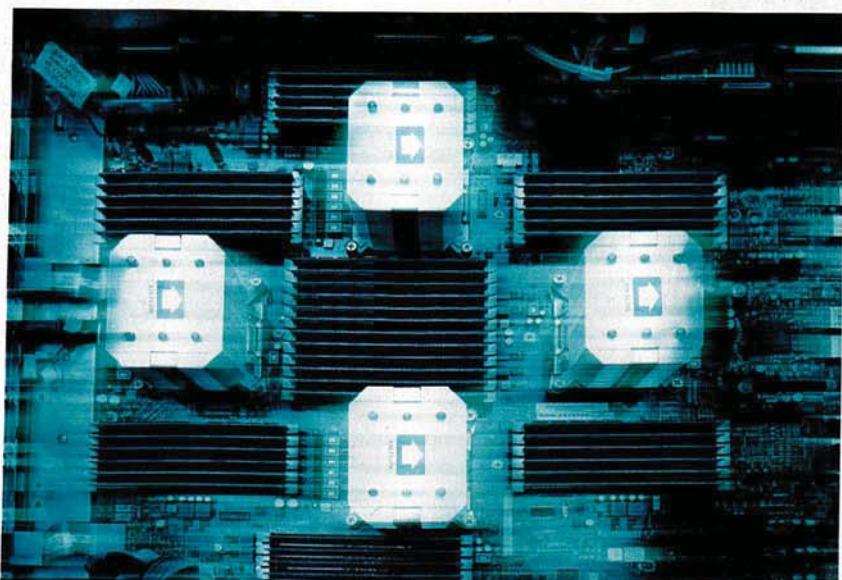
ist Dozent für Wirtschaftsinformatik an der FOM Hochschule für Oekonomie & Management und leitet das Infrastruktur-Consulting bei der Söldner Consult GmbH in Nürnberg.

Literatur

- [1] Fred Hantelmann; Desktops; Vom Tisch; Desktops und Anwendungen im Netz mit Citrix' XenApp 5.0; *iX* 7/2009, S. 62
- [2] Jens-Henrik Söldner; Virtualisierung/Cloud; Nach Belieben; Synergy2012; Apps und Desktops im Mittelpunkt; *iX* 12/2012, S. 14
- [3] Sven Ahnert; Virtualisierung; Geschickt geschachtelt; Pro und contra Virtual Desktop Infrastructure; *iX* 5/2011, S. 94
- [4] Bernd Kretschmer, Achim Schwabehland; Thin Client; Doppelweg; VMwares View 4.5 liefert virtuelle Windows-Desktops; *iX* 2/2011, S. 60
- [5] Fred Hantelmann; Arbeitsumgebung; Frisch zu Tisch; Vier Desktop-Virtualisierer im Vergleich; *iX Special „Cloud, Grid, Virtualisierung“* 2/2010, S. 83

iX-Wertung

- ⊕ bedarfsgerechter Applikationsumfang auf Webschnittstelle durch Anwender konfigurierbar
- ⊕ kompatibel mit ESXi, Hyper-V und XenServer
- ⊕ vollständige App-V-Integration
- ⊖ SmartAuditor nicht mehr enthalten
- ⊖ einige Konfigurationsoptionen nur über PowerShell API möglich



Hochleistungsrechner mit großem Speicher

In die Vollen

Ralph Hülsenbusch

Bei Servern in Rechenzentren geht es nicht immer nur um Rechenleistung. Spätestens seit SAPs HANA und Apaches Hadoop sind große Hauptspeicher attraktiv, weil gewaltige Datenmengen zu verarbeiten sind. Grenzen setzt die Zahl der Memory-Slots, die wiederum von der Zahl der Prozessorsockel abhängt. Was da möglich ist, zeigt ein Vierwegeserver von der DELTA Computer Products GmbH.

Terabyte an Hauptspeicher waren noch vor wenigen Jahren eine unvorstellbare Größe, die wenn, nur mit speziellen Tricks zu realisieren war. Denn das Limit bildet in erster Linie die Zahl der Slots, und das ist durch die Bauart der Prozessoren begrenzt. Für Server verwendbare CPUs von Intel und AMD mit ihren integrierten Memory Controllern verfügen über eine festgelegte Zahl von Speicherbussen, die wiederum nur eine definierte Menge an Slots ansteuern können.

Aktuelle Xeons der E5-Serie von Intel (Sandy und Ivy Bridge) haben einen integrierten Memory Controller mit vier Kanälen. Jeder Bus kann bis zu drei Spei-

chermodule bedienen, allerdings nicht ohne Nebenwirkungen: Bei voller Bestückung sinkt die maximale Zugriffsgeschwindigkeit von 1600 MHz auf 1066 MHz, da sich die Module den Bus teilen müssen.

Prozessoren setzen Speichergrenzen

Ein Sockel kann somit zwölf Memory-Slots bereitstellen. Damit sind 384 GByte pro Sockel bei einer Bestückung mit 32 GByte großen Riegel realisierbar. Ein System mit vier Sockeln durchbricht damit die 1-Terabyte-Grenze. Die Kosten

belaufen sich jedoch auf rund 500 Euro pro 1600-Modul – da kommen über 24 000 Euro allein für den Hauptspeicher zusammen. Ein weiteres Dilemma entsteht durch die Menge der Module, denn mit ihr steigt die Wahrscheinlichkeit für Fehler. Bei 48 DDR3-Riegeln kann schon mal eins mit Mängeln dabei sein. Jeden Prozessor flankieren je sechs Slots rechts und links (siehe Aufma-cher).

Zwar ist die Ausstattung mit Terabyte-großem Hauptspeicher nicht neu, jedoch waren bei den früheren Systemen mit Westmere-Technik spezielle Tricks erforderlich, die Riesenspeicher aufzubauen. Wie iX in der Februarausgabe 2013 berichtet hat, verwendet IBM in seiner MAX5 dazu eine Board-Erweiterung. DELTA Computer hat dazu sein Modell D80x im Programm, das acht Sockel für Westmere-Ex-Prozessoren vom Typ E7-8000 besitzt [1]. Das senkt zwar die Kosten für den Speicherumbau (6340 Euro), dafür hat die Serverplattform mit 27 990 Euro aber einen höheren Preis. Dank der Entwicklung bei Intel erlauben die integrierten Memory-Controller der Sandy- und Ivy-Bridge-Architektur inzwischen den Anschluss von drei Slots statt zwei und die Hersteller von Speicherriegeln bieten größere Module als früher.

Zum Test schickte die Hamburger DELTA Computer Products GmbH einen Hochleistungsserver mit neuer Technik. Im Unterschied zu dem im vorigen Jahr bereitgestellten Acht-Wege-Server für großen Hauptspeicher mit Xeons aus der E7-8000er-Serie genügen jetzt Systeme mit vier Sockeln, um die Terabyte-Grenze zu durchbrechen. Die Ausstattung mit Intels Xeons E5-4600 lässt dank der 48 DIMM-Steckplätze den Ausbau auf 1,5 Terabyte zu.

DELTA Computer Products aus Reinbek bei Hamburg wirbt mit einer kostengünstigen Variante, die mit 16-GByte-Modulen bestückt ist. Das System mit dem sprechenden Namen D44X-M4-RS-27-16-768-6x300GB – die Kürzel und Ziffern bezeichnen die Ausbaustufen – war mit 768 GByte Hauptspeicher bestückt, bestehend aus 48 DDR3-DIMM-ECC, registered. Die vier Sandy-Bridge-EP-Prozessoren Xeon E5-4650 arbeiten im 2,7-GHz-Takt mit 20 MByte großem L3-Cache. Sie bedienen den Speicherbus mit bis zu 1600 MHz. Die CPUs drehen im Turbo-Mode auf bis 3,3 GHz hoch. Für die sechs 300 GByte großen SAS2-Festplatten mit je 64 MByte Cache war ein MegaRAID-927i-SAS2-Controller von LSI eingebaut. Die Mannschaft bei DELTA hatte das System vor



Zugänglich: Beim D44x-Server von DELTA braucht man keine Umwege zur Rückseite, um Tastatur, Maus und Monitor anzuschließen. Es bleibt sogar ein USB-Anschluss frei (Abb. 1).

dem Versand einem 48 Stunden dauernden Stress-Test unterzogen.

Das Motherboard von Supermicro mit Intels C602-Chipset hat zweimal 1-Gigabit-Ethernet on-board, gesteuert von Intels i350. Vier SATA2- und zwei SATA3-, zwei USB-2.0-Anschlüsse und ein serieller sind integriert. Auf dem Board sind unter den neun PCIe-3.0-Slots – für einen Server ungewöhnlich – vier für GPUs (16x) vorgesehen. Leider war das mangels passender Karten nicht Gegenstand des Testes. Für die Fernwartung ist ein IPMI-2.0-kompatibler Board Management Controller (BMC) über ein separates Netz erreichbar.

Auf der Frontseite bietet der Server Zugang zu dreimal USB und VGA. Dort sind die acht Wechselplatten und das CD-Laufwerk erreichbar. Zusätzlich ist noch ein 5,25-Slot frei, etwa für ein Bandlaufwerk.

Testplattform als Dauerläufer

Im iX-Labor war der Rechner mehrere Monate in Betrieb und diente während der Untersuchung auch als Entwicklungs-



Vielfach: Der Server bietet eine große Zahl von Erweiterungssteckplätzen und ist mit vier Netzteilen gut versorgt. Fürs Management gibt es einen eigenen Ethernet-Port (Abb. 2).

plattform für die Testprogramme zum Messen der Speicher-Performance. Übliche Benchmarks können einer solchen Konfiguration – im konkreten Fall mit 768 GByte – nicht gerecht werden. SPECs CPU2006 etwa, losgelassen auf 64 Cores mit einem Appetit von bis zu 128 GByte, knabbert kaum am Speicher. Deshalb kamen die Tests der c't für Hauptspeicher, entwickelt von Andreas Stiller, zum Zuge, die jedoch angesichts des Microsoft Server 2012 einer Überarbeitung bedurften.

Die Memory-Benchmarks auf dem E5-4650 ergaben für den lokalen Hauptspeicher eine Performance bei einer Latenz von 66 ns bis hinauf zu 14 GByte/s single-threaded und 27 GByte/s bei acht Threads. Beim Zugriff auf den Speicher benachbarter CPUs jedoch liegt die Performance, erstaunlicherweise ohne größere Unterschiede zwischen den Sockeln, mit einer Latenz von 275 bis 300 ns zwischen 2,9 und 3,1 GByte mit einem, bei 3,3 und 3,5 GByte/s mit acht Threads.

Zum Vergleich: Ein Westmere EX (E7-4870) mit 128 GByte RAM ist lokal zwar langsamer (24 GByte/s und 140 ns Latenz bei zehn Threads), kann aber mit seinen vier QPI-Links dank der Direktverbindung zum entfernten Speicher mehr rausholen: 10,9 GByte/s mit circa 200 ns Latenz. Jedoch kann dieser Prozessortyp ohne Memory Buffer nur mit 32 Speicher-Slots aufwarten. Maßgeblich für die Speicher-Performance ist die Aus-

stattung der Prozessoren mit Quick Path Interfaces (QPI).

Fazit

Als Resümee mag gelten, dass Kompro misse eingehen muss, wer große Hauptspeicher nutzen will. Von den technischen Daten her, die Intel für die Westmere-CPUs herausgibt, wäre ein Vier-Wege-Server mit dem E7-4870 auf bis zu 2 Terabyte ausbaubar, wozu jedoch 64 GByte große Memory-Module erforderlich sind – sofern erhältlich, ein teures Vergnügen. Bei der Rechenleistung schneidet der E5-4650 insgesamt besser ab, wovon Anwendungen profitieren. An Intels Adresse geht die Kritik, dass das Einsparen an QPIs trotz Beschleunigung der Speicher-Performance nicht zugute kommt.

Aus der zur Drucklegung aktuellen Preisliste von DELTA geht hervor, dass die Grundausstattung mit 128 GByte RAM 16 854 Euro kostet. Der Ausbau auf 768 GByte wie im Test schlägt mit 5800 Euro zu Buche. Wer 1 TByte braucht, muss stattdessen 16 400 Euro auf den Tisch legen – letztlich fast dieselbe Summe, wie bei der Basis. Zum Vergleich: Eine Blade vom Typ ProLiant BL660c Gen8 von HP mit derselben CPU, aber nur 128 GByte Hauptspeicher gibt es für 20 933 Euro. IBMs System x3750 M4 8722 mit zwei Prozessoren und 16 GByte RAM ist ab 14 629,40 Euro zu haben. Zwar sind die anderen Angebote nur bedingt vergleichbar, zeigen aber, dass die Preise bei DELTA attraktiv sind. (rh)

Literatur

- [1] Ralph Hülsenbusch, Andreas Stiller; Rack-mounted Server; Angekoppelt; System mit Hauptspeichererweiterung: IBMs MAX5; iX 2/2013, S. 68
- [2] Ralph Hülsenbusch; Rack-Server; Zwillingsturm; AMDs Piledriver gegen Intels Sandy Bridge; iX 8/2013, S. 74

X-Wertung

- ⊕ solide Verarbeitung
- ⊕ performantes System

Daten und Preise

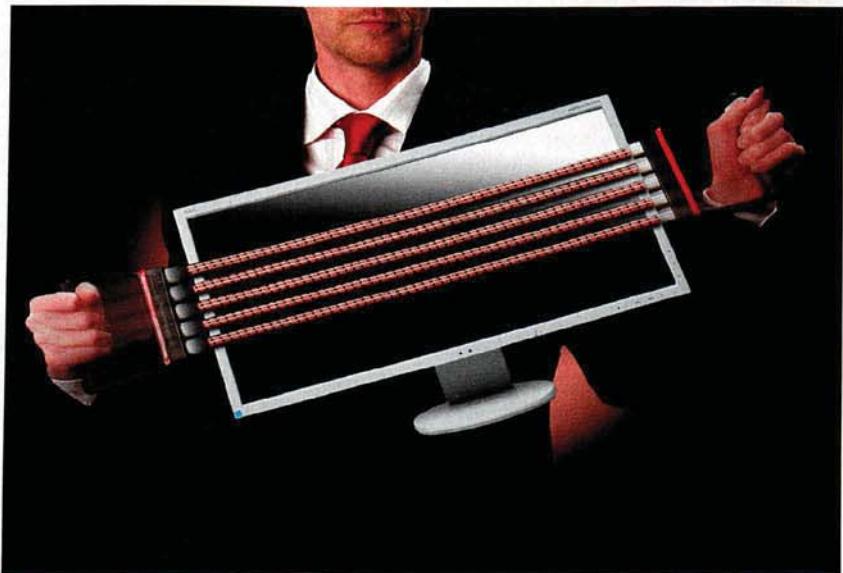
DELTA D44x-M4

Hardware: vier Xeon E5-2650, 2,7 GHz (max. 3,3 GHz), 20 MByte L3-Cache; 768 GByte DDR3-ECC-RAM (1600); LSI MegaRAID 9271-8i SAS2; sechs HDD 300 GByte, 7200 UPM, 64 MByte Cache; 48 DIMM-Slot, Anschlüsse für: zwei Gigabit-Ethernet, vier SATA2, zwei SATA3, neun PCIe 3.0 (vier x16, ein x8 in x16, zwei x8, ein x4 in x8, ein x8 (Quanta mezzanine cards)), fünf USB 2.0, ein serieller; IPMI 2.0 mit eigenem LAN-Port; Aspeed AST2300 8 MByte DDR3 4HE-Rack-Chassis, vier redundante 1100 Watt Netzteile, acht HotSwap-Einschübe 2,5", Slim Line DVD

Software: Windows Server 2012

Anbieter/Hersteller: DELTA Computer Products GmbH, Reinbek, www.deltacomputer.de

Preis: 22 654 Euro (Teststellung ohne OS)



NEC MultiSync EA294WMi

Expander

Moritz Förster, Dieter Michel

Die ersten Ultra-Widescreen-Displays im *iX*-Test eigneten sich nur eingeschränkt für das Büro. Nun versucht mit NEC ein weiterer Hersteller sein Glück.

In vielen Büros stehen an einem Arbeitsplatz mehrere Monitore, mit denen Administratoren ihre Systeme im Blick behalten oder dem Web 2.0 folgen wollen. Offensichtlich ist manchen ein Widescreen-Bildschirm nicht breit genug, erste Hersteller bringen Displays im 21:9-Format mit 2560 × 1080 Pixeln auf den Markt. Im *iX*-Test konnte man auf diesen

zwar den Desktop deutlich ausdehnen, jedoch haperte es am Zusammenspiel mit den Betriebssystemen und der Verarbeitung der Gehäuse [1].

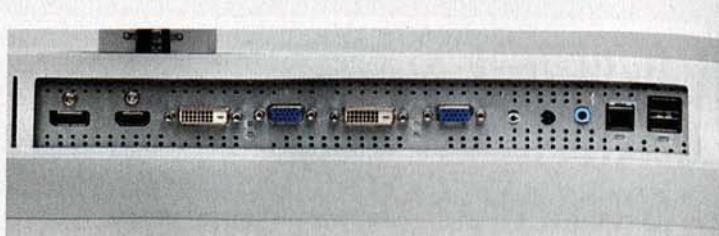
Nun stellt sich der MultiSync EA294WMi von NEC denselben Herausforderungen. Zunächst fällt die Farbe auf: Ein hellgraues Gehäuse findet man eher im Büro denn im Heimkino. Zudem hat

der Hersteller daran gedacht, dass es Größenunterschiede bei Menschen gibt – das Display lässt sich in der Höhe verstehen und schont so den Rücken. Im Monitorfuß ist eine Drehscheibe integriert. Für das Ordnen der Kabel besitzt das Standbein auf seiner Rückseite eine leicht zugängliche Kabelführung.

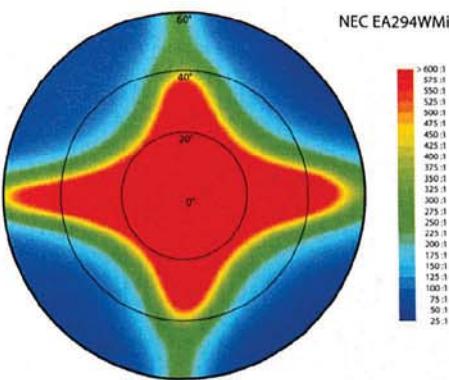
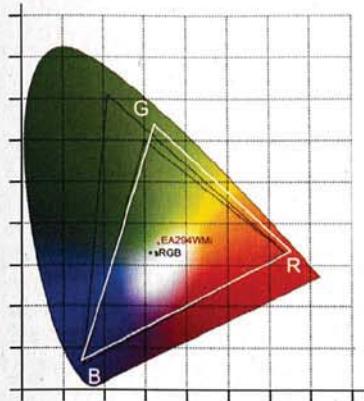
Um die untere rechte Ecke des vorderen Rahmens verteilen sich die Touch-Buttons zum Bedienen des On-Screen-Menüs. Die Symbole auf dem Gehäuse sind lediglich aufgedruckt, für einige Anwender mag die Anordnung etwas gewöhnungsbedürftig sein, das Mittelgrau auf Hellgrau erschwert das Erkennen der Beschriftung. Im Menü selbst muss man sich durch Symbole und Untermenüs kämpfen, jedoch ist alles durch die starken Kontraste klar erkennbar.

Unter dem Bildschirm befinden sich die Schnittstellen. Hier hat NEC nicht gespart: Mit je zwei DVI-D- und VGA-Eingängen sowie je einer DP- und HDMI-Buchse hat man im Alltag genügend Auswahl. Hinzu kommen Audio- und USB-2.0-Eingang. Will man statt der integrierten Boxen lieber Kopfhörer verwenden, findet man den Klinken-Ausgang am linken Rand des Gehäuses in einem klar abgegrenzten Bereich. Hier lassen sich ebenfalls zwei USB-Medien anschließen. Zwei weitere Schnittstellen für fest installierte USB-Geräte wie Tastatur und Maus verstecken sich im Portfeld unter dem Bildschirm. Obwohl das Netzteil integriert ist, besitzt das Gerät keinen separaten Schalter zum Trennen vom Stromnetz.

Der Farbraum des EA294WMi ist nah am sRGB-Standard, mit um eine Idee gesättigteren Primärfarben Grün und Rot. Auch ohne Softwarekalibrierung dürfte man Fotos und Videos frei von sichtbaren Farbverschiebungen wiedergeben können, solange man keine erweiterten Farbräume wie Adobe RGB benutzt. Passend zum ausgeprägten Querformat ist der horizontale Einblickwinkel größer als der vertikale. Das Fremdlichtkontrastverhal-

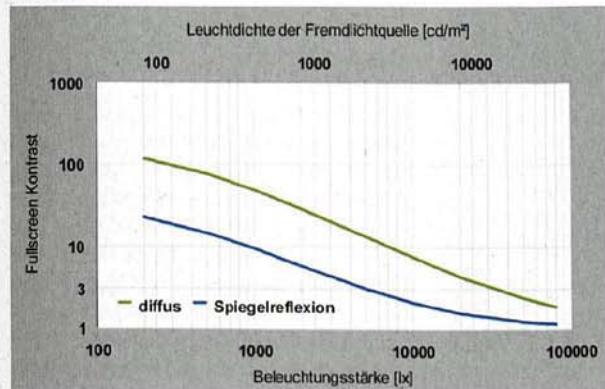


Umfangreich: Unter dem Gerät befinden sich die meisten Anschlüsse, zwei USB-Medien und Kopfhörer kann man am linken Rand anschließen (Abb. 1).



Picture in Picture (PiP) beherrscht das Gerät nicht.

Wie den 298P4QJEB von Philips im ersten Ultra-Widescreen-Test kann man den NEC hochkant in den Pivot-Modus drehen, der in der neuen Position die Nackenmuskulatur fordert. Über den analogen Eingang boten alle Testrechner die volle Auflösung von 2560×1080 Pixeln, ein älterer Computer mit Linux versteifte sich beim Nutzen des DVI-D auf das 16:9-Format. Abstürze oder Artefakte wie bei der Konkurrenz gab es keine.



Standard: Das Panel erfüllt die Erwartungen an einen matten Bildschirm für das Büro (Abb. 2).

ten ist typisch für Monitore mit matter Displayoberfläche.

Eine Schwachstelle der Konkurrenz ist die Verarbeitung des Gehäuses. Insgesamt ist das Modell von NEC stabil, lediglich der obere und untere Rahmen lassen sich etwas abziehen. Auf Letzterem befinden sich zwei Sensoren für das Erfassen der Helligkeit und Anwesenheit des Nutzers, wodurch das Gerät die Leuchtkraft anpasst beziehungsweise in den Stand-by-Modus wechselt. Was genau die Sensoren wann auslösen, kann man im Menü kon-

figurieren; sitzt man nicht vorm Bildschirm oder bleibt still sitzen, bekommt man gleich angezeigt, wie viel Prozent Strom man nun einspart.

Besonders interessant dürfte für viele professionelle Anwender der Picture-by-Picture-Modus (PbP) sein, der mehrere Geräte auf einem Display ausgibt. Auf beiden Anzeigen kann man mit einer Auflösung von 1280×1024 Pixeln im 4:3-Format arbeiten – in vielen Fällen dürfte sich der verfügbare Platz auf dem jeweiligen Desktop also verringern.

Fazit

Insgesamt bietet der MultiSync EA294 WMi einiges für das Büro. Gerade die vielen Schnittstellen, der durchdachte Aufbau und Sensoren zum Stromsparen dürften viele ansprechen, die täglich viele Stunden mit dem Bildschirm arbeiten. Das Anzeigen mehrerer Rechner funktioniert nahtlos, einzige die oft geforderten Touch-Buttons des Menüs dürften mechanischer sein.

(fo)

Dieter Michel

arbeitet als freier DV-Journalist und ist Chefredakteur der Fachzeitschrift Prosound.

Literatur

- [1] Dieter Michel, Susanne Nolte; Monitore; Extrabreit; 29"-Ultra-Widescreens für den Schreibtisch; iX 6/2013, S. 60



Innovation und Kontinuität im Software-Schutz

Einmal Schützen - Mehrfach liefern:
- Wibu-Systems Konzept seit 1989

Höchste CodeMeter-Sicherheit:
- Smart Card Chips und AES/ECC seit 2003,
Aktivierung CmActLicense oder CmDongle

Zukunftssicher und einfach zu nutzen:
- Remote-Updates, abwärtskompatibel, treiberlos seit 2003,
USB 3.0, Windows 8, .NET: kein Problem für CodeMeter



20+ Years

MEDIA
ACCESS

www.wibu.com
sales@wibu.com

WIBU



Neue Funktionen bei Veeams Backup & Replication v7

Parallelisiert

Jörg Riether

Im August brachte Veeam die Version 7 seines Backup & Replication auf den Markt. Bereits die letzten beiden Major-Releases überraschten mit einem großen Sack neuer Fähigkeiten.

Als Veeam im Oktober 2010 die fünfte Generation seines Backup & Replication auf den Markt brachte, schuf es damit erstmals die Möglichkeit, die Sicherungskopien virtueller Gäste auf ihre tatsächliche Lauffähigkeit zu überprüfen. Das eigentliche Backup trat damit in den Hintergrund und machte Platz für automatisierte Prüfverfahren und Testlabore. Etwa ein Jahr später brachte man mit der Version 6 verteilte Backup-Architekturen ins Spiel und verwandelte das reine VMware-Produkt in eine Hybridvariante, geeignet, um von einem zentralen Punkt aus sowohl ESXi-, als auch Hyper-V-Gäste zu sichern (siehe Kasten „Aufbau von Veeam Backup & Replication“).

Wieder ein Jahr später, die Rede ist von Oktober 2012 und der Version 6.5, stieg Veeam erstmals ungewohnt tief in

die Applikationsebene herab, namentlich in Microsofts Exchange-Datenbankstrukturen. Auch in der Hardwarefokussierung gab es einen kleinen Sprung – und zwar in Richtung HP. Durch tiefe Einblicke in die Architektur und Arbeitsweise von HPs Storage-Systemen konnte Veeams Software Backups von einem SAN-Snapshot wiederherstellen. Die Frage, ob die Version 7 in puncto Neuerungen mit ihren Vorgängern mithalten kann, hat Veeam nun beantwortet.

Nachdem sich vor drei Jahren der Standard- eine Enterprise-Lizenz hinzugesellt, präsentiert Veeam nun eine weitere – die Königslizenz „Enterprise Plus“. Eine komplette Gegenüberstellung der neuen Lizenzklassen inklusive der Listenpreise findet man auf der Website des Herstellers (siehe „Alle Links“).

Er befreist nach Sockeln und Lizenzklassen. Nach wie vor existiert eine kostenlose Lizenz, die im Funktionsumfang stark eingeschränkt ist. Darüber hinaus bietet Veeam ein Essentials-Paket sowie eine Suite – alles außerordentlich ähnlich zu der Lizenzgestaltung von VMware. Schließlich gibt es noch eine Cloud-Edition, die Backups zu diversen Cloud-Speicher-Anbietern transferieren kann.

Funktionen nicht für jedermann

Für seine höchste Lizenzklasse hat sich Veeam im Wesentlichen zwei markante neue Funktionen als Exklusivausstattung ausgesucht. Zum einen hat man erstmals einen eigenen WAN-Beschleuniger entwickelt und integriert. Dieser lässt sich, ähnlich wie die hauseigene Proxy-Architektur, direkt über die grafische Oberfläche lokal oder entfernt ausrollen.

WAN-Beschleuniger arbeiten grundsätzlich als Pärchen zwischen Quelle und Ziel zusammen. Im Fall von B&R v7 ist die einzige System-Voraussetzung ein 64-Bit-Windows. Danach können sie als Quelle, als Ziel oder als beides zugleich agieren. Hauptsächlich arbeitet Veeam mit einem gemeinsamen Cache-Speicher und Deduplizierung, um Durchlaufzeiten auf WAN-Strecken zu optimieren.

Größe und Ort der Cache sind für jeden WAN-Beschleuniger frei konfigurierbar. Nachdem man den Cache etabliert hat, muss er erst einmal lernen. Es ist also unwahrscheinlich, dass die Geschwindigkeit bereits beim ersten Durchlauf zunimmt. Als Empfehlung gibt Veeam eine Cache-Größe von 100 GByte an. Wenn aber ein Ziel-Beschleuniger mit mehreren Quell-Beschleunigern zusammenspielen soll, muss seine Cache-Größe zwangsläufig um die Größe jedes zusätzlichen Quell-Beschleunigers wachsen.

X-TRACT

- Mit jeder neuen Version erweitert Veeam die Feature-Liste seiner Software Backup & Replication deutlich.
- Auch B&R v7 bringt einiges an Neuerungen mit.
- Zugleich sind es die Verbesserungen im Detail, die vor allem die Performance der Backup-Jobs steigern und die Hardware-Ressourcen entlasten.

Aufbau von Veeam Backup & Replication

2008 veröffentlichte Veeam seine speziell für virtuelle Umgebungen konzipierte Backup- und Replikations-Software unter dem Namen Veeam Backup 1.0. Sie arbeitet argenlos von einem – physischen oder virtuellen – Windows-Server aus mit VMwares ESX(i)-Hypervisoren zusammen. Dazu diente zuerst das NBD-Protokoll (Network Block Device), später gesellten sich der direkte SAN-Zugriff (Storage Area Network) und SCSI-Hot-Adds als weitere Zugriffsmethoden hinzu. Erst mit der Version 6 kam die Unterstützung für Hyper-V hinzu.

Bereits in ihrer ersten Version beherrschte Veeam Backup das Wiederherstellen einzelner Dateien in virtuellen Maschinen, indem sie – mit entsprechenden Dateisystemtreibern ausgestattet – die Backup-Kopien der VM-Image-Dateien öffnete und aufs darin befindliche Dateisystem zugriff. Inzwischen reicht die Liste von FAT, NTFS, ReFS über ext, ReiserFS, JFS, XFS, UFS, HFS und NSS zu ZFS samt allen Nachfolgern [k].

Ein großer Unterschied zur klassischen Backup-Software: Veeams B&R sichert grundsätzlich VM-Images auf Festplatten. Erst in die aktuelle Version 7 hat die Unterstützung von Bandlaufwerken Eingang gefunden. Sie erlaubt aber nur das nachträgliche Kopieren der Backup-Images auf ein weiteres Sicherungsmedium.

Ebenfalls der Enterprise-Plus-Lizenz vorbehalten ist ein neues Verfahren, von Snapshots, die Disk-Arrays aus dem Hause HP angefertigt haben, direkte Backups anzulegen. Dies erfordert eine direkte und weitreichende Interaktion mit den Storage-Subsystemen. Anders als der bereits mit Veeam 6.5 eingeführte Explorer für Snapshots durch die Speichersysteme beinhaltet die mit Version 7 eingeführte Technik einen gänzlich anderen Ansatz: Erstmals kann man einen solchen Snapshot automatisch erzeugen und anschließend direkt über ihn eine Sicherungskopie erstellen. Das funktioniert momentan aber ausschließlich in VMware-Umgebungen.

Kein Weg am ESXi-Snapshot vorbei

Wer allerdings jetzt glaubt, dies mache einen Snapshot auf VMware-Hypervisor-Ebene endlich obsolet, der irrt leider. Den muss man nach wie vor zusätzlich auf Hypervisor-Ebene durchführen, kann ihn aber im Gegensatz zum gewohnten Standard-Verfahren per vStorage APIs for Data Protection (VADP) gleich im Anschluss wieder entfernen. Das Storage-System muss lediglich die Ausführung des Snapshots bestätigt haben. Beim herkömmlichen VADP-Verfahren darf man den

Voraussetzung für das Installieren ist ein x86-64-System mit Windows 7 SP1, Windows Server 2008 SP2 oder höher. Auf ihm läuft die zentrale Software, der Veeam Backup & Replication Server. Dort oder auf einem anderen System arbeitet auch der Backup Repository Server, der das Lager mit den Backups verwaltet. Er darf unter Linux oder Windows laufen.

Für größere und verteilte Umgebungen sind die Backup-Proxy-Server gedacht, die man vom Backup & Replication Server aus ausrollen kann. Sie komprimieren die Backup-Daten beispielsweise bereits in den Randzonen des Firmennetzes, bevor sie ihren langen Weg zum eigentlichen Backup-Ziel antreten. Ebenfalls optional sind die neuen WAN Accelerator Server, die pärchenweise an den Endpunkten einer WAN-Strecke angesiedelt sind und ein 64-Bit-Windows-System ab XP oder Server 2003 benötigen.

Will man Mitarbeitern oder Kunden das Suchen nach und Wiederherstellen von ganzen VM-Backups oder einzelnen Dateien innerhalb der Gäste erlauben, benötigt man den Backup Enterprise Manager, der übrigens mit mehreren Backup & Replication Servern zusammenarbeiten kann. Ihm zur Seite stehen Agents zum Indizieren der Guest-Systeme und bei größerem Umgebungen optional Veeams Backup Search Server, der auf Microsofts Search Server aufsetzt.

Hypervisor-Snapshot hingegen erst am Ende der eigentlichen Sicherung wieder entfernen.

Um die Frage zu beantworten, warum man bei Veeam und anderen Herstellern derartige Anstrengungen für ESXi-Server unternimmt, muss man sich deren Arbeitsweise vergegenwärtigen: Snapshot-Operationen müssen die virtuellen Maschinen (VM) vereinfacht gesagt zu Beginn und zum Ende des Schnappschusses kurz einfrieren, was jeweils zu einem kurzen Aussetzer im Antwortverhalten der VM führen kann – beim Anlegen des Snapshots und beim Zurückschreiben der Änderungen seit seiner Erzeugung in die eigentliche VMDK-Datei. Bei stark gewachsenen Snapshots kann sich der Moment des Rückschreibens massiv verlängern. Solch große Snapshots entstehen vor allem bei besonders I/O-lastigen Anwendungen in VMs. Konsolidiert man durch Veeams Unterstützung der Storage-Hardware-Snapshots aber den VMware-Snapshot direkt nach seiner Erzeugung wieder, kann dies zu massiven Leistungsgewinnen im Vergleich zum herkömmlichen VADP-Verfahren führen.

Bislang gibt es diese tiefe Disk-Array-Integration aber ausschließlich für Produkte von HP, genau genommen für StoreVirtual VSA, StoreVirtual sowie StoreServ-Speichersysteme. Eine Weiter-

NETWAYS SCHULUNGEN

WENN OPEN SOURCE - DANN MIT NETWAYS

PUPPET FUNDAMENTALS



3 TAGE | NÜRNBERG | ZÜRICH

- Einführung in Puppet
- Arbeiten mit Modulen
- Viele Praxisbeispiele

PUPPET ADVANCED



3 TAGE | NÜRNBERG | HAMBURG

- Reporting und Auditierung
- Einstieg in MCollective
- Optimierung und Skalierung

EXTENDING PUPPET



3 TAGE | NÜRNBERG

- Grundlagen von Ruby
- Custom Handlers, Types und Providers
- Modultest mit RSpec & Mocha

netways.de/schulungen



Puppet Camp

discover > configure > manage™

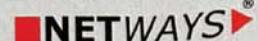
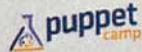
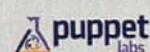
[Save the Dates]

[Munich] [Nov 28th 2013]

[Berlin] [Apr 11th 2014]

netways.de/puppetcamp

presented by



entwicklung, die diese Option auf Disk-Systeme anderer Hersteller ausdehnt, ist wünschenswert. Grundsätzlich wäre es außerdem dringend an der Zeit, dass sich Storage-Hersteller, Entwickler von Backup-Software und VMware gemeinsam an einen großen Tisch setzen und eine untereinander standardisierte Backup-Methode schaffen, die etwaige Snapshots auf Hypervisor-Ebene völlig obsolet macht – träumen darf man ja wohl noch.

Auf den Wunschlisten der Administratoren, aber nicht auf der Liste künftiger Funktionen stand vor der Veröffentlichung von B&R v7 die parallele Verarbeitung innerhalb eines Backup-Auftrags.

Auch im Management-GUI versteckt sich diese Funktion gut hinter den globalen Optionen und dort nochmals im Karteireiter „Advanced“. Vor der Version 7 musste man die zu sichernden virtuellen Maschinen innerhalb eines Backup-Auftrags sequenziell abarbeiten und für eine parallele Ausführung mehrere Aufträge gleichzeitig ausführen.

Aktualisiert man frühere Versionen, muss man die Funktion explizit aktivieren. Im Test deaktivierte die Software sie nach dem Update von Version 6.5 auf 7. Dies ist beabsichtigt: Nach einem Update möchte man zunächst die bisherige Konfiguration vorfinden.

Zusätzlich zu VMs verarbeitet B&R v7 virtuelle Festplatten parallel: Ist eine zu sichernde VM mit mehreren vDisks ausgestattet, kann B&R v7 Letztere nun parallel anstatt sequenziell sichern. Damit lassen sich innerhalb eines Jobs selbst im alten und langsamen NBD-Modus (Network Block Device), also ohne direkten SAN-Zugriff oder SCSI-Hot-Add, respektable Durchsatzwerte erzielen. Im Test waren es über eine 10-Gigabit-Ethernet-Verbindung knapp 400 MByte/s.

Allerdings lässt sich die parallele Verarbeitung nur global ein- oder ausschalten. Ist sie aktiviert, gilt sie ohne Einschränkung für jeden konfigurierten Backup-Job. Momentan unterscheidet B&R v7 dabei auch nicht zwischen VMs und vDisks. Grundsätzlich lässt sich aber die maximale Zahl paralleler Jobs sowohl je Backup-Proxy-Server für den eigentlichen Transport, als auch je Repository für das Ablegen der Backups individuell konfigurieren.

Kompression überarbeitet

Ein weiterer Grund für den Performance-Zuwachs von Version 6.5 zu 7 ist die Überarbeitung des Kompressionsverfahrens. Mit der aktuellen Version hat Veeam eine neue Standard-Kompressionsstufe eingeführt. Waren zuvor die vier Stufen None, Dedup-friendly, Optimal, Extreme wählbar, gibt es jetzt derer fünf. Die alte Stufe Optimal heißt nun High; die hinzu gekommene „Optimal“-Stufe beherbergt einen neuen proprietären Kompressionsalgorithmus, der seine Effizienz vor allem der Verwendung des SSE-Befehlsatzes von x86-CPUs verdanken soll. Zwar verringert sich laut Veeam durch den neuen Algorithmus die Kompressionsleistung um etwa 10 %, dafür soll er aber nur ein Zehntel der CPU-Leistung für sich beanspruchen.

Da Backup-Jobs mit Kompression die CPUs erfahrungsgemäß massiv beschäftigen, ist dieser Schritt durchaus sinnvoll, insbesondere bei dem hohen Grad der Parallelisierung, den B&R v7 nun erlaubt. In dieser Version frisch erstellte Aufträge erhalten automatisch die Stufe Optimal zugewiesen. Alte Backup-Jobs, die noch aus früheren Versionen stammen, muss man händisch auf den neuen Algorithmus umstellen, sonst verwendet B&R weiter den leistungshungrigeren High-Algorithmus – auch hier behält die Software nach dem Upgrade sicherheitshalber die bislängige Konfiguration bei.

Im direkten Vergleich mit einem zuflüssig ausgewählten Test-Job mit 260,5 GByte zu lesenden Netto-Quelldaten bei



Während die Kompressionsstufe High mit dem alten Algorithmus Intels Xeon-Prozessoren mit je acht Kernen gut beschäftigt (oben), haben sie mit der neuen Standard-Stufe Optimal samt neuem Kompressionsalgorithmus weit weniger zu tun (unten, Abb. 1).

ES-2016WSS NAS 32 TB

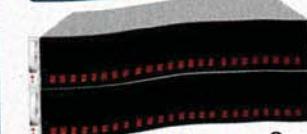
NAS

- teilbestückt:
8 x 4 TB SAS Nearline Enterprise Disks 24x7
 - opt. SAS/SATA bis 4 TB auf Hardware Contr.
 - 4 x 1 Gbit Ethernet Port
 - Windows Storage Server 2012
 - Xeon Quad Core E3
 - 3 HE im Rack
 - redundante Netzteile
- inkl. MwSt. **5.938,-** exkl. MwSt. **4.990,-**

ES-2824 Nexenta ZFS

iSCSI
NAS

- teilbestückt:
12 x 600 GB SAS 15K
 - alternativ: SAS Nearline bis 4 TB (mischbar)
 - 4 x 1 Gbit Hostinterface für iSCSI und NAS (opt. mehr)
 - opt. SSD ZIL Cache mit bis zu 130.000 IOPS
 - Quad Xeon
 - redundante Netzteile
- inkl. MwSt. **8.913,-** exkl. MwSt. **7.490,-**

ES-8700 iSCSI Cluster

iSCSI
open-e
PARTNER GOLD

- Cluster aus 2 x 24 Slot 2.5" Systemen
 - teilbestückt:
je 12 x 300 GB SAS 10K
 - alternativ:
SAS bis 1,2 TB, SATA bis 1 TB (mischbar)
 - RAID 0, 1, 10, 5, 6, 50, 60 auf Hardware Controller
 - Erweiterung per JBOD
 - 4 x 1 Gbit zum Host
- inkl. MwSt. **11.769,-** exkl. MwSt. **9.890,-**

alle Preise in €

EUROstor GmbH
Hornbergstr. 39
D-70794 Filderstadt

RAID 6
Dual Parity

aktivierter Veeam-Deduplizierung erzeugte der – alte – Algorithmus der Kompressionsstufe High eine 108,9 GByte große Sicherungskopie und der neue Optimal-Algorithmus ein 110,4 GByte großes Backup. Gleichzeitig konnte man beobachten, wie sich die Auslastung der beiden maximal 2,9 GHz schnellen 8-Kern-CPUs Xeon E5-2690 von durchschnittlich etwa 50 % bei 2,26 GHz auf etwa 15 % bei 1,16 GHz reduzierte (siehe Abbildung 1).

Weg vom einfachen Backup to Disk

Sicherheitsbewussten Backup-Verantwortlichen dürfen die neuen Funktionen Backup Copy Job und Backup-to-Tape-Integration ins Auge springen. Wollte man bislang seine mit B&R erzeugten Backup-Images nach dem Backup-to-Disk auf ein Band schreiben lassen, etwa um es zusätzlich in einem anderen Brandabschnitt lagern zu können oder um die Aufbewahrungszeit zu erhöhen, war der Einsatz einer zusätzlichen Software unumgänglich, zu der zahlreiche Backup-Verantwortliche auch tatsächlich gegriffen haben.

Version 7 bringt erstmals einen eigenen Backup-to-Tape-Mechanismus mit, der grundsätzlich mit allen Bandgeräten oder Wechslern spricht, die Windows sehen und ansteuern kann. Die Bandgeräte müssen vom Veeam Backup-Server aus über SCSI, SAS, FC oder iSCSI erreichbar sein. Neben einfachen Bandgeräten unterstützt B&R v7 physische und virtuelle Tape Libraries. Im Test erkannte es zwei an das System angeschlossene LTO-6-Laufwerke von IBM ohne Murren.

Der eigentliche Backup-to-Tape-Job stellt sich innerhalb der GUI in gewohnter Manier dar. Wie bei normalen Backup-Aufträgen kann man den Fortschritt, die übertragene Datenmenge sowie die Geschwindigkeit in Echtzeit überwachen.

Darüber hinaus kann man die Sicherungskopien auftragsbasiert wegschreiben. Als Quellenangabe können einzelne Veeam-Backup-Aufträge oder ganze Repositorien herhalten. Wer will, kann B&R zusätzlich dazu missbrauchen, sich agnostisch zur hauseigenen Backup-Logik zu verhalten und schlicht Dateien in angegebenen Ordnern zu sichern. Etwaige Dateifilter lassen sich je Pfad konfigurieren.

Schließlich kann sich jeder seine eigene Backup-Logik mit Skripten kreieren. Die Powershell-Commandlets hat Veeam entsprechend um Funktionen zur Bandsicherung erweitert. Ein Blick in die neue Referenz lohnt sich allemal (siehe „Alle

Links“). Skript-Bastlern sei an dieser Stelle ein Blick auf neue Commandlets wie *Get-VBRTapeMedium* oder *Erase-VBRTapeMedium* ans Herz gelegt.

Auch sei darauf hingewiesen, dass eine Datei-Bandsicherung mit NTFS-Hardlinks umgehen kann. Im Test sicherte ein Datei-auf-Band-Job, der einige mit *mklink /h* erstellte Hardlinks hingeworfen bekam, anstandslos die verknüpften Backupdateien. B&R v7 kann darüber hinaus Medien einlesen und wiederherstellen, die Drittanbieterprodukte geschrieben haben, sofern sie das Microsoft Tape Format (MTF) verwenden.

Neu ist ebenfalls die Funktion Backup Copy Jobs. Mit ihr lassen sich Backup-Images nachgeschaltet auf ein weiteres Disk-Backup-System übertragen, idealerweise in einem anderen Brandabschnitt gelegen. Bislang musste man für diese und zahlreiche ähnliche Unternehmungen selbstgeschriebene Skripte einsetzen.

Backups per Auftrag kopieren

Außerdem war das nicht gerade ressourcenschonend, da zum Großteil einfach nur gigantische Datenmengen übers Netz von A nach B gingen – wohlgemerkt ohne jegliche logische Integration in das eigentliche System. Dies ändert Veeam nun in der aktuellen Version. Ab sofort kann B&R etwaige Backups mit einem Copy-Job auf einen weiteren konfigurierten Datenspeicher übertragen, und zwar nicht etwa durch einfaches Vergleichen und Kopieren, sondern innerhalb der Veeam-Backuplogik. Die Aufträge arbeiten es wie bisherige Backup-Jobs ab. Einzelne VMs holt es blockweise aus den Quell-Backup-Dateien und überträgt sie zum Zielsystem.

Eine parallele Verarbeitung beherrscht es an dieser Stelle aber noch nicht. Auf dem Zielsystem legt es stets eine vorwärtsgerichtete inkrementelle Backup-Kette an, selbst dann, wenn man im Quellsystem mit rückwärts gerichteten Inkrementen (reverse incremental) gearbeitet hat. Auch lassen sich, wie man es vom bisherigen Backup gewohnt ist, auf Wunsch Deduplikation und Kompression einschalten.

Ein neuer Auftrag erzeugt zunächst am konfigurierten Zielort ein Vollbackup und im Anschluss vorwärts gerichtete Inkremeante. Je nachdem, wie man seine Aufbewahrungsrichtlinien für das Ziel konfiguriert hat, räumt B&R dort zu gegebener Zeit auf. Dieser Prozess verdient eine genauere Betrachtung, beispielsweise was

passiert, wenn die Aufbewahrungsrichtlinie am Ziel sieben Tage beträgt und man ein sechs Tage altes Vollbackup nebst sechs Inkrementen dort liegen hat. Löschte man das Vollbackup, wäre die Kette zerstört. B&R injiziert stattdessen bei Überschreiten der konfigurierten Aufbewahrungszeit das älteste Inkrement des Jobs in das Vollbackup. Anschließend löscht es das Inkrement, da es nun Bestandteil des Vollbackups ist.

Es erklärt sich von selbst, dass das Vollbackup mit der Zeit durch Fragmentierung unnötig stark wachsen könnte. Daher empfiehlt es sich, in den Konfigurationsoptionen des Copy Jobs unter *Target -> Advanced* einen sich regelmäßig wiederholenden Zeitpunkt auszuwählen, an dem B&R das Vollbackup neu komprimieren soll. Wichtig zu wissen: Momentan funktioniert diese Art der zeitgesteuerten Kompression des Vollbackups bei den Copy Jobs nur dann, wenn man eine einfache Aufbewahrungsrichtlinie konfiguriert hat. Bei komplexen Großvater-Vater-Sohn-Szenarien ist das zeitgesteuerte Neukomprimieren noch nicht möglich.

Auf Wunsch kann man den Backup Copy Job über den normalen Veeam-Transportmechanismus oder über die neue WAN-Beschleunigung laufen lassen. An dieser Stelle sei angemerkt, dass mit dem jetzigen Releasestand der Backup Copy Job der bislang einzige gesetzte Weg ist, die neue WAN-Beschleunigung zu nutzen.

Virtuelle Labs auch für Hyper-V

Admins, die mit VMwares ESX(i)-Sternen und Veeams B&R arbeiten, kennen und schätzen die Möglichkeit, Backups in einer durch B&R etablierten Sandbox-Laborumgebung zu testen oder sie automatisiert auf ihre tatsächliche Lauffähigkeit hin überprüfen zu können. Auch universelle Wiederherstellungsmechanismen waren dadurch in den Bereich des Machbaren gerückt, da bereits die Version 5 durch die Kombination eines speziellen virtuellen Proxy-Filtersystems und der Gast-Isolation streng kontrollierte In-

teraktionen zwischen Sandbox und Produktivumgebung erlaubte.

Das Hyper-V-Lager dagegen musste bislang ohne diese Funktionen auskommen. Dies ändert Veeam mit der Version 7. Erstmals bringt B&R Virtual Labs und damit SureBackup auch für Hyper-V mit. Momentan kann man Virtual Labs allerdings nur mit einem Windows Server 2012 mit aktivierter Hyper-V-Rolle etablieren.

Nach wie vor sind die ESXi-Nutzer bei Veeam technisch im Vorteil. Eine häufig nachgefragte Funktion hat es nun in die Version 7 geschafft: Virtual Labs für VMDK-Replikate (VMwares Virtual Machine Disk Format). Bislang konnte man diese Funktion nur für die Backups benutzen, nicht aber für Replikate, die nicht auf einem von B&R verwalteten Datenspeicher, sondern direkt auf dem ESXi-Datenspeicher liegen. Indem Veeam hier Abhilfe geschaffen hat, hat es auch die SureBackup-Funktion auf die Replikate ausgedehnt. Man nennt das Kind Sure-Replica.

Für Hoster und Provider

Vor allem für größere Hoster ist die Unterstützung von VMwares vCloud Director wichtig. Backup & Replication 7 nutzt die vCloud Director API. Mit ihr vermag die Software die vCloud-Director-Strukturen direkt in der GUI darzustellen und in den Aufträgen zu hervorheben. So lassen sich vApps inklusive deren Metadaten sichern und wiederherstellen. Bei den Metadaten ist Obacht angesagt: Man muss den Backup-Auftrag explizit als vCD-Job konfigurieren, andernfalls bleiben die Metadaten ungesichert zurück.

Ebenfalls für Hosting-Umgebungen sind die beiden neuen Funktionen zur Delegation gedacht: die individuelle rechtegesteuerte Self-Service-Wiederherstellung für Kunden und eigene Web-Implementierungen, etwa mit REST (Representational State Transfer). Die gute Nachricht: Beides führt Veeam mit der Version 7 ein. Die schlechte: Beides verlangt die Enterprise-Plus-Lizenz. Die zugehörige RESTful API Referenz kann man sich bei Veeam herunterladen (siehe „Alle Links“).

Letztes Jahr integrierte Veeam die Unterstützung von Exchange-2010-Datenbanken. Die erweitert der Hersteller nun auf den Exchange Server 2013. Darüber hinaus kommt erstmals mit der Version 7 eine SharePoint-Integration hinzu. B&R unterstützt SharePoint 2010 Foundation,

Standard und Enterprise. Der neue Veeam Explorer for SharePoint vermag SharePoint-Datenbankdateien mithilfe eines sogenannten Staging-Servers zu öffnen. Letzterer benötigt einen Microsoft SQL Server größer gleich der Version der gesicherten SharePoint-Datenbank.

Man kann selbstredend hierzu auch den SQL Server Express 2008 R2 SP1 benutzen, den B&R v7 mitbringt. Dabei muss man aber die Datenbankgröße im Auge behalten. Ist die zu öffnende SharePoint-Datenbank größer als 10 GByte, reicht die kostenlose Express Edition des SQL Server nicht mehr aus. Genau wie beim Explorer for Exchange ist der Explorer for SharePoint in jeder Lizenzklasse, sogar der kostenlosen Variante, enthalten. Für ein automatisiertes Wiederherstellen direkt an den Ursprungsort in der Produktionsumgebung bedarf es jedoch jeweils der Enterprise oder Enterprise-Plus-Lizenz.

Zum bloßen Überwachen der Backup- und Replikations-Jobs kann man seit der Version 7 in VMware-Umgebungen auch deren vSphere-Web-Client benutzen. Das erforderliche Plug-in kann man über den Veeam Enterprise Manager aktivieren. Es arbeitet mit dem vSphere Web Client v5.1.0 build 880146 oder neuer zusammen.

Fazit

Veeams Backup & Replication v7 überzeugt durch sinnvolle neue Ideen, eine verbesserte Gesamtperformance sowie Stabilität. Vor allem die kleinen Dinge wie die parallele Verarbeitung und der neue Kompressionsalgorithmus können insbesondere in größeren und verteilten Umgebungen für deutliche Verkürzungen der Backup-Zeiten sorgen. (sun)

Jörg Riether

ist spezialisiert auf die Bereiche IT-Sicherheit, Hochverfügbarkeit und Virtualisierung. Er arbeitet als Abteilungsleiter der IT bei der Vitos Haina gemeinnützige GmbH.

Literatur

- [1] Jörg Riether; Datensicherung; V-Formation; Veeam Backup & Replication v5 Enterprise Edition; IX 1/2011, S. 60

-Wertung

- ⊕ neue Optionen für VMware-Snapshots
- ⊕ native Unterstützung für Bandlaufwerke
- ⊕ SureBackup für Hyper-V
- ⊕ parallele Verarbeitung
- ⊖ Hyper-V-Unterstützung hinkt hinterher



Linux für den Unternehmenseinsatz

Distributions-dschungel

André von Raison

Wer in der eigenen IT-Abteilung auf fundiertes Linux-Know-how zurückgreifen kann, dem bietet das Umfeld des freien Betriebssystems ein breites Spektrum an Distributionen. Auf andere wirkt die Vielfalt wie ein Blick in einen fast undurchdringlichen Urwald.

Sieht man sich die Palette der potentiellen Linux-Einsatzgebiete an, kann dem unbedarften Betrachter schon mal der Kopf schwirren. Von Embedded Devices wie Industriesteuerungen oder Smartphones über Tablets, Notebooks, PCs und Server bis hin zu Mainframes und HPC-Clustern deckt Linux ein extrem breites Spektrum ab. Für den Unternehmenseinsatz lässt sich der Markt in zwei große Segmente aufteilen: die klassische IT sowie den Bereich des Embedded

Computing. Ersteres ist Thema dieses Beitrags, während sich der Artikel „Vorher-sagbar“ ab Seite 100 Letzterem widmet.

Ein wenig Zahlenjonglage

Bei den x86-Servern bescheinigte IDC Systemen, die mit vorinstalliertem Linux ausgeliefert werden, im zweiten Quartal 2013 weltweit einen kostenmäßigen Marktanteil von 23,2 Prozent (siehe „On-

linequellen, [a]). Da die Marktforscher Windows-Systemen knapp 50 Prozent zugestehen, liegt die Vermutung nahe, dass die fehlenden knapp 27 Prozent ebenfalls unter Linux beziehungsweise einem BSD-Derivat ihren Dienst versehen oder als Virtualisierungsplattform beispielsweise für Webserver dienen.

In diesem Segment ordnet W3Techs 66 Prozent aller Webserver einem unixoiden Betriebssystem zu (Stand 10. September 2013, [b]) von denen der Löwenanteil ein Linux-Derivat sein dürfte. Das Supercomputing ist hingegen fest in Linux-Hand: In der derzeit aktuellen TOP500-Liste vom Juni 2013 laufen 95,2 Prozent aller Supercomputer unter dem freien System [c]. In diesen Trend passt auch IBMs Ankündigung, von seiner neuen Mainframe-Familie zBC12, eine Linux-only-Variante zu vertreiben (siehe „Alle Links“).

Eine von SUSE beauftragte, kürzlich veröffentlichte Studie hat rund 200 IT-Verantwortliche von Firmen mit mehr als 500 Mitarbeitern zum Einsatz von Linux in ihren Unternehmen befragt (siehe „Alle Links“). Dass 83 Prozent Linux im Betriebssystem-Portfolio haben, ist nicht allzu verwunderlich. Bemerkenswert ist aber, dass weit über 60 Prozent der Befragten angaben, Linux als Plattform für unternehmenskritische Software wie Datenbanken, Data-Warehousing- oder Business-Intelligence-Anwendungen einzusetzen respektive in den kommenden Monaten nutzen zu wollen. Dabei nannten sie als zentrale Argumente für das Open-Source-Betriebssystem geringere Kosten, bessere Performance sowie das Vermeiden eines Vendor Lock-in, der Abhängigkeit von einem Anbieter.

Große Auswahl oder verwirrende Vielfalt

Auf den ersten Blick scheint sich die Vielfalt der potenziellen Plattformen und Einsatzgebiete potenziert in der Auswahl der verfügbaren Linux-Distributionen niederschlagen. Eine erste Produkt- respektive Projektübersicht kann DistroWatch.com [d] liefern. Die populäre Seite beherbergt in ihrer Datenbank Namen von rund 760 Distributionen, von denen rund 300 den Status aktiv haben. Rechnet man die diversen BSD- und Solaris-Abkömlinge heraus, bleibt dennoch ein recht unübersichtliches Namenskonglomerat.

Strukturierter geht das Team um den Schweden Andreas Lundqvist an die Aufgabe heran. Es hat Informationen zu insgesamt fast 500 Distributionen zusammengetragen und in der „GNU/Linux

Linux von großen Hardware-Anbietern

Von allen großen Hardware-Anbietern fasst Big Blue die Linux-Eignung seiner Produkte am kürzesten: Das freie Betriebssystem ist für alle IBM-Systeme zertifiziert. Darüber hinaus bietet man einen Software-Stack mit über 500 Paketen für unterschiedliche Aufgaben an und untermauert das Ganze mit einem passend zugeschnittenen Dienstleistungsangebot.

Fujitsu hat Oracle Linux, RHEL und SLES für die Primergy-Server-Familie eine vollständige Freigabe erteilt. Darüber hinaus arbeitet der Hersteller auch mit externen Dienstleistern zusammen, um auch freie Distributionen zu unterstützen und in die hauseigene Server Management Suite zu integrieren. Weiter finden sich bei Fujitsu für CentOS, Debian und Ubuntu detailliertere Dokumente.

HP hat viele seiner Server für den Betrieb unter Oracle Linux, RHEL, SLES und Ubuntu zertifiziert. Darüber hinaus gibt es Success-Stories für Asianux, CentOS, Debian, Fedora und openSUSE. HP bietet für Ubuntu LTS (10.04, 12.04) auf der hauseigenen Hardware auch Support an.

Dell verfügt ebenfalls über ein großes Linux-Portfolio. Das reicht von klassischen Servern über Appliances, Cloud- und Storage-Ansätzen bis hin zu Workstations und Business-Clients. Wie HP arbeiten die Texaner dabei mit den „klassischen“ Distributionsanbietern Canonical, Oracle, Red Hat und SUSE zusammen. Als weiteren Baustein gibt es das Dell-Enterprise-Linux-Wiki, in dem sich Anwender und Dell-Ingenieure direkt austauschen können.

Distribution Timeline“ (GLDT, [e]) zu- einander in Beziehung gesetzt. Bei Wikipedia findet sich eine Variante, die Googles Android einbezieht. Allerdings liegt die letzte Aktualisierung inzwischen fast ein Jahr zurück.

Einer der am weitesten zurückreichenden Zweige ist der, dessen Wurzeln auf Slackware zurückgehen – die älteste derzeit noch aktiv betreute Linux-Distribution. Hierzu gehört auch SUSE mit seinen

Derivaten Astaro, openSUSE, SLED oder SLES. Den größten Teilbaum hingegen bildet das vor zwanzig Jahren ins Leben gerufene Debian mit seinen weit über Hundert Derivaten. Von denen stellt die Ubuntu-Familie inzwischen mit rund 70 aktiv gepflegten Mitgliedern den Löwenanteil. In ähnlicher Stärke präsentiert sich der dritte große Teil, dessen Wurzeln auf Red Hat mit seinem Enterprise Linux (RHEL) zurückgehen.

Allerdings lassen sich mit solchen genealogischen Betrachtungen nur bedingt Aussagen treffen, ob ein Projekt für den Unternehmenseinsatz taugt oder nicht – zumal ein Großteil der verfügbaren Distributionsvarianten eher aus persönlichen Bedürfnissen einiger Anwender heraus entstanden sind und sich somit nicht für einen generischen Einsatz in Firmen eignet.

Bei der Entscheidung für eine Distribution spielen mehrere Fragen eine Rolle. Die erste betrifft die gewünschte Hardware-Plattform. Sollen topaktuelle Geräte zum Einsatz kommen, ist im Vorfeld zu prüfen, ob für alle Komponenten auch passenden Linux-Treiber existieren.

Eher konservativ ausgerichtete freie Vertreter wie Debian oder Slackware, aber auch kommerzielle Anbieter wie Red Hat oder SUSE müssen hierbei gegebenenfalls passen. Letztere bieten im Gegenzug nicht nur ausgereifte Treiber, sondern auch Zertifizierungsprogramme. Die stellen sicher, dass das Zusammenspiel mit Server-Hardware der großen Hersteller sowie mit einer Reihe vor allem in größeren Unternehmen verbreiteter 3rd-Party-Programme, beispielsweise SAP oder Datenbanken, reibungslos funktioniert. Wer unternehmenskritische Workloads unter Linux auf IBMs Power-Systemen oder Mainframes betreiben möchte, kommt um RHEL oder SLES vermutlich nicht herum.

Unternehmens-Linux

Hersteller	Distribution	Web
bitbone AG	bitkit SOLUTIONS	www.bitbone.de/bitkit-SOLUTIONS.2.0.html
Canonical	Ubuntu LTS	www.ubuntu.com
CERN	Scientific Linux (RHEL-Clone)	www.scientificlinux.org
ClearCenter	ClearOS	www.clearcenter.com/Software/clearos-professional-overview.html
Collax	Business Server, Platform Server	www.collax.com/produkte
Debian-Projekt	Debian	www.debian.org
Fixstars Solutions	Yellow Dog Linux	www.yellowdoglinux.com
JM Consulting Group	SME Server	www.smeserver.net
Klaus Knopper	Knoppix (Debian Derivat)	www.knopper.net
LIS AG	CoreBiz, RedBiz	www.linux-ag.com/produkte/
Mandriva S.A.	Mandriva Business Server	www.mandriva.com/de/solutions/corporate-governmental/
natural COMPUTING	natural DESKTOP	www.natural-computing.de/sites_d/produkte.html
Oracle	Oracle Linux	www.oracle.com/de/technologies/linux/overview/
Red Hat	Red Hat Enterprise Linux	www.redhat.com/rhel/
Slackware Inc.	Slackware	www.slackware.com
SUSE Linux	SUSE Linux Enterprise Server	www.suse.com/de-de/products/server/
Univention	Univention Corporate Server	www.univention.de/produkte/ucs/
Zorin Group	Zorin OS	zorin-os.com

IX-TRACT

- Mehrere Hundert Linux-Distributionen buhlen um die Gunst der Anwender.
- Für die Unternehmens-IT wichtige Rahmenbedingungen beschränken die Auswahl auf ein übersichtliches Maß.
- Bei fehlendem Know-how stehen professionelle Dienstleister bereit, Firmen bei Einführung und Betrieb von Linux-Systemen zu begleiten.

Langfristig stabile Schnittstellen

Gerade in dieser Kategorie Software sind für einen geordneten Betrieb stabile System- und Kernel-APIs und -ABIs erforderlich. Auch hier können die „großen“ kommerziellen Anbieter mit ihren langen Produktlebenszyklen für ihre Distributionen punkten. Beispielsweise bietet Red Hat für die beiden letzten RHEL-Releases 5.x und 6.x – natürlich gegen zusätzliche

Bezahlung – über den „normalen“ zehnjährigen Produktzyklus hinaus drei weitere Jahre Extended Lifecycle Support.

Bei SUSE endet der „normale“ Support nach sieben Jahren und lässt sich ebenfalls um drei Jahre erweitern. Canonical garantiert beim Ubuntu LTS Server für einen Zeitraum von fünf Jahren Security-Patches sowie Backports von Treibern und aktuellerer Software aus den Desktop-Versionen.

Wer mit etwas geringeren Produktlebenszeiten auskommt, könnte sich aber auch bei einem der weniger prominenten Anbieter umsehen. Gerade etwas kleinere Firmen, die über kein Linux-Know-how in ihrer IT-Abteilung verfügen, finden hier individuell zugeschnittene Beratungs- und Supportangebote. Und die dort auffindbaren Distributionen ändern sich auch nicht im Sechs-Monats-Rhythmus.

Ein paar Pfade in den Dschungel

Sicherlich sind Red Hat und SUSE die bekanntesten Vertreter kommerzieller Linux-Angebote. Beide stellen mit ihren Enterprise-Distributionen RHEL und SLES schon seit vielen Jahren ihre Tauglichkeit für die Unternehmens-IT unter Beweis – wobei sie sich auch preislich in für dieses Marktsegment üblichen Regionen bewegen. Das Produktangebot geht weit über die reine Linux-Distribution hinaus und dank eines breit gestreuten Partnernetzes können sie auch Wünsche nach individueller Betreuung samt Beratung erfüllen. Bei Bedarf liefern sie den 3rd-Level-Support dazu. Oracles RHEL-Clone bietet für seine Linux-Familien 5.x und 6.x mit dem „Unbreakable Enterprise Kernel Release 2“ einen speziell auf den Einsatz der hauseigenen Produkte zugeschnittenen Kernel an. Der basiert auf Linux 3.0.16 und glänzt unter anderem mit Ksplice für Kernel-Updates ohne Reboot sowie die Dateisysteme Btrfs, OCFS2 und XFS.

Ebenfalls mit einem Partneransatz bietet Canonical Ubuntu-Nutzern ein professionelles Dienstleistungsspektrum. Selbst für das als reine Desktop-Variante mit KDE statt Gnome ausgerichtete Kubuntu gibt es Unterstützung: Die britische Firma Emerge Open liefert kommerziellen Support und zwar sowohl für die Desktop- als auch für die Server-Variante. Beim Geschäftsmodell schimmert der Community-Gedanke durch: Die Gewinne aus dem Angebot fließen ans Kubuntu-Projekt.

Bei ihrem auf Debian basierenden Corporate Server (UCS) arbeitet die Univation GmbH ebenfalls mit Partnern zusam-

NOTFALL

HELP

Ist Ihre IT fit für den NOTFALL?

Mit dem iX Notfallmanagement steuern Notfallbeauftragte in kleinen und mittleren Unternehmen Notfälle gründlich und stoßen entsprechende Prozesse zur Schadensbehebung an.

Basierend auf der Portal-Software Intrexx von United Planet präsentiert iX ein **Notfallkit für Windows, Linux und Mac** und einer Runtime-Lizenz für 1 Jahr mit folgenden Highlights:

- das exklusive iX-Sonderheft „Notfallmanagement“ im Wert von 9,90 Euro **kostenlos**
- ein **komplettes Ticketsystem** für die IT-Abteilung
- **unverzichtbare News** rund um das Thema Notfallmanagement

Bestellen Sie jetzt das wichtige Notfallmanagement-Toolkit bis zum 31.12.2013 zum Sonderpreis von 99,- Euro.

www.iX.de/notfall



Ausgewählte Linux-Dienstleister

Anbieter	Dienstleistungsangebot	Web
B1 Systems	Consulting, Entwicklung, Schulung, Support	www.b1-systems.de
bcs kommunikations-lösungen	Debian-Systeme	www.b-c-s.de/html/index.html
creativ	Open Source Support Center	www.creativ.de
DASEQ	Red Hat, Consulting, Schulung	www.daseq.de
dass IT	Red Hat, UCS, Consulting, Schulung, Support	www.dass-it.de
DECOIT	Full Service, Ergänzungen UCS	www.decoit.de
DELTA Computer Products	vorinstallierte Systeme, Support	www.deltacomputer.de/loesungen/loesungen_index.shtml
FOX Elektronix – Fux	vorinstallierte Debian-Systeme	www.asimplecomputer.com/index.php
GONICUS	Open-Source-Services, Debian-Support	www.gonicus.de
G-TEC Open Source Solutions	IBM-Systeme mit Debian oder GRML	www.g-tec.co.at
Heinlein Consulting	Administration, Consulting, Schulung, Support	www.heinlein-support.de/linux-consulting
Intevation	Open Source, Debian	www.intevation.de
LINET Services	UCS	www.linet-services.de
LinSoft	vorinstallierte Systeme	www.linsoft.de/engine/productG/systemhaus
MSD Computer-systeme	Open Source, Debian, Ubuntu	www.msddnet.de/linux/
NETWAYS	Consulting, Managed Services, Schulung, Support	www.netways.de/de/units/managed_services/
SerNet	Open Source, Debian, RHEL, SLES	www.sernet.de
Sybuca	Debian, Fedora, Gentoo, openSUSE ...	www.sybuca.de
teuto.net	Ubuntu-Server-Hosting	www.teuto.net
Thomas Krenn	vorinstallierte Server (Debian)	www.thomas-krenn.com/de/produkte/server-systeme.html

Weitere Anbieter siehe „Alle Links“

men. Die Bremer waren die ersten, die mit ihrer Distribution dank integriertem Samba 4 quasi Out-of-the-Box Active-Directory-Verzeichnisdienste für Windows-Clients erlaubten. Über das in die grafische Managementkonsole integrierte App Center stehen eine Reihe von 3rd-Party-Paketen bereit, beispielsweise Backup, Dokumenten-Management, ERP, Groupware oder VoIP. Für Linux-Desktops haben die Bremer mit dem hauseigenen Corporate Client ein passendes Angebot.

Ursprünglich setzte die Münchener Linux Information Systems AG (LIS AG) auf Debian für ihre CoreBiz-Server-Suite, die schon im iX-Labor ihre Fähigkeiten unter Beweis stellen konnte [1, 2]. Vor einigen Jahren wechselte man beim Unterbau auf Ubuntu LTS. Kern der Produktfamilie ist der Base-Server, der unter

anderem einen zentralen, LDAP-basierten Authentifizierungsdienst sowie die Core-Biz Management Console umfasst. An diesen lassen sich je nach Einsatzgebiet weitere Module andocken – inklusive vollständiger Integration ins Basissystem. Als neueste Variante arbeiten die LIS-Entwickler daran, ihre CoreBiz-Architektur auch auf einem Red-Hat-Unterbau anzubieten. Unter dem Label RedBiz 6 sind der Basisserver sowie die Module Groupware und Datensicherung bereits verfügbar.

Einen ähnlichen Ansatz verfolgt Collax. Die haben einerseits mit ihrem Business Server ein auf den KMU-Sektor zugeschnittenes Komplettspaket im Angebot. Auf der anderen Seite bieten sie mit dem Collax Platform Server ein Basissystem, dass sich mit derzeit 16 Modulen um spezifische Funktionen erweitern lässt. Auf

Wunsch liefern die Ismaninger ihre Software als vorinstallierte Komplettspäckte inklusive passender Hardware.

Ein Platzhirsch im Verborgenen

Darüber hinaus gibt es noch einige ebenfalls kommerziell ausgerichtete Distributionen, deren detailliertere Vorstellung den Rahmen sprengen würde. Die Tabelle „Unternehmens-Distributionen“ listet – ohne Anspruch auf Vollständigkeit – einige davon auf.

Ein weiterer Kandidat kam bislang nur am Rande vor: Debian. Das Community-Linux mit professionellem Anspruch an Stabilität und Qualität der Distribution erfreut sich vor allem bei denjenigen großer Beliebtheit, die das erforderliche Know-how bereits im Unternehmen haben. Allerdings kann, wer das nicht hat und im Betrieb nicht auf Zertifizierungen von Hardware oder gar Software-Stacks angewiesen ist, für eine Debian-Nutzung auf eine ansehnliche Schar von Systemhäusern oder Dienstleistern zurückgreifen. Eine exemplarische Auswahl findet sich in der Tabelle „Ausgewählte Linux-Dienstleister“.

Fazit

Dass Linux generell für den Einsatz in der Unternehmens-IT taugt, muss es nicht unter Beweis stellen. Eine Liste erfolgreicher Beispiele ließe sich fast beliebig füllen. Wer das für den Betrieb sinnvolle Know-how nicht im eigenen Haus hat, kann auf ein breites Dienstleistungsangebot zurückgreifen. Wer allerdings glaubt, professionelle Services für das Open-Source-Betriebssystem zum Nulltarif zu bekommen, irrt gewaltig. Die gibt es zu marktüblichen Konditionen, sodass das dafür erforderliche Budget je nach Funktions- und Betreuungsbedarf variiert. Aber die durch die Linux-Nutzung gewonnene Freiheit ist gegebenenfalls unbezahltbar. (avr)

Literatur

- [1] André von Raison; Collaboration; Talentvielfalt; Groupware und mehr Komplettangebote für KMU; iX 11/2010, S. 86
- [2] Christian Böttger; Linux SBS; Linux en miniature; Arbeitspferde für kleinere Unternehmen; iX 6/2008, S. 48

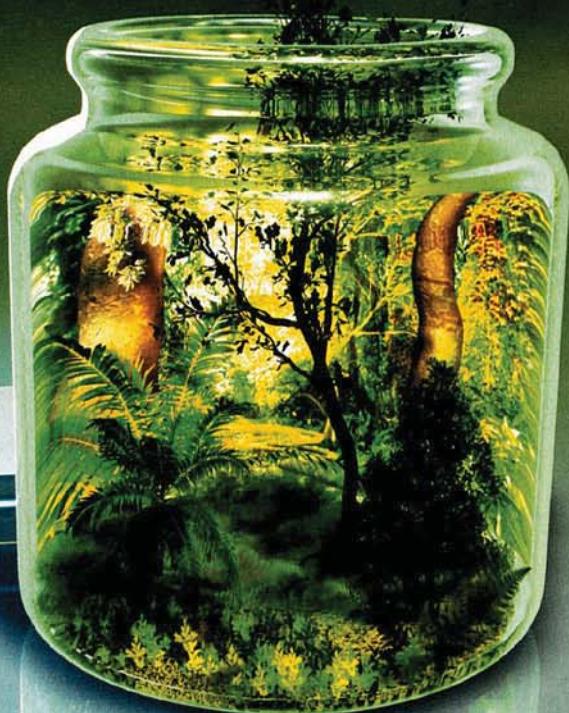
Onlinequellen

[a] IDC-Servermarkt Q3/2013	www.ix.de/-1944664
[b] W3Techs	w3techs.com/technologies/overview/operating_system/all
[c] Top 500	www.top500.org
[d] DistroWatch	www.distrowatch.com
[e] GLDT	futurist.se/gldt/

Alle Links: www.ix.de/ix1310094



Linux-Distributionen für eingebettete Systeme



Vorhersagbar

Barbara Lange

Zu den besonderen Anforderungen, die Embedded-Anwendungen an ihre Betriebssysteme stellen, gehört die Echtzeitfähigkeit. Durch die Integration des „Realtime Preemption Patch“ kann Linux diese Aufgabe erfüllen. Ein Überblick, mit welchen Embedded-Linux-Distributionen die Betriebssystemhersteller Unternehmen beim Entwickeln eingebetteter Systeme unterstützen wollen.

Echtzeit, Sicherheit und die begrenzten Hardware-Ressourcen stecken den groben Rahmen ab, der für eingebettete Systeme in besonderem Maße gilt. So geht das Spektrum der eingesetzten Architekturen über die im Desktop-Bereich bekannten CPUs hinaus. Außerdem verfügen Embedded-Systeme in der Regel über geringe Hardware-Ressourcen. Daher ist es wichtig, dass Entwickler sich ein kleines, auf die definierte Aufgabe hin zugeschnittenes System zusammenstellen können.

Nicht zu unterschätzen ist weiterhin der Support. Im Unterschied zu Linux im Server- und Desktop-Markt muss Embedded-Linux über lange Zeit den Support gewährleisten, denn in der Industrie sind Maschinen durchaus 25 Jahre oder länger in Betrieb.

Letztlich muss, wer „Embedded“ sagt, auch „Echtzeit“ sagen. Jedenfalls stellen viele Anwendungsbereiche diese Anforderung, die eine garantierte Reaktionszeit auf externe Ereignisse verlangen. Linux kann das seit der Kernel-Version 2.6 erfüllen, als Linus Torvalds mit der Integration des „Realtime Preemption Patch“ den Linux-Kernel um Echtzeitfunktionen erweiterte.

Damit ist der Kernel präemptibel geworden, das heißt, mit entsprechender Priorität ausgestattete Anwendungsprozesse können das Betriebssystem jederzeit unterbrechen. Die Integration musste nachträglich erfolgen, da das offene Betriebssystem ursprünglich nicht für Echtzeitaufgaben konzipiert war.

Attraktivität für die Industrie nimmt zu

Maßgeblich beteiligt an dieser Entwicklung ist die Genossenschaft „Open Source Automation Development Lab“ (OSADL), die sich seit Jahren um das Anpassen von Linux für den industriellen Einsatz im Maschinenbau und in der Automatisierungsindustrie kümmert und jetzt das PREEMPT_RT-Echtzeit-Linux pflegt.

In der Industrie sehe er keine Alternative zu Linux, so Carsten Emde, OSADL-Geschäftsführer, auf dem LinuxTag 2013. Er schätzt, dass in diesem Jahr zwei Drittel der neu entwickelten Embedded-Systeme mit Linux laufen; insgesamt liege der Anteil bei allen Geräten und Maschinen derzeit bei etwa 15 Prozent (siehe „Onlinequellen“, [a]).

OSADL hat mittlerweile über 40 Mitglieder, darunter Firmen wie ELTEC Electronic, Kontron, TRUMPF, Homag Holzbearbeitungssysteme, Intel oder Te-

Wind River Linux 5 unterstützt Yocto und ist damit auf zum Projekt kompatiblen Entwickler-Boards lauffähig. Yocto stellt einen Baukasten zur Erstellung von Distributionen zur Verfügung (Abb. 1).



xas Instruments. Von der Seite der Betriebssystemhersteller ist seit einigen Jahren SYSGO dabei, seit einigen Monaten auch Wind River.

Im Jahr 2012 hat die Genossenschaft die Echtzeitfähigkeit von Linux experimentell in seiner „Embedded Farm“ nachgewiesen. Ausgewertet wurden 73 Milliarden automatisierte Testzyklen von über 50 Rechnern mit Mainline-RT-Kernel verschiedener CPU-Plattformen.

Industrie-Unternehmen, die Linux nutzen wollen, müssen sich bei der Wahl mit diversen Vor- und Nachteilen von Open Source auseinandersetzen. Zum einen besitzt die Entwickler-Community rasch Fehler, man ist unabhängig von Softwareherstellern und besitzt die Kontrolle über die Funktion des Systems, da der Quellcode offenliegt. Im Unterschied zu proprietären Systemen kann Linux nicht mal eben abgekündigt werden. Diese Eigenschaften sind für Unternehmen viel wichtiger als potenzielle Kostenersparnisse durch das offene System, so Emde gegenüber iX.

Zu den Nachteilen gehören Fragen, die das Betriebsgeheimnis betreffen. Hier ist die Meinung in der Welt der Distributionsanbieter einhellig: Wenn mehrere Firmen gemeinsam Treiber entwickeln und diese offenlegen, können alle von der Zusammenarbeit profitieren und sich ver-

stärkt auf ihre Kernkompetenz konzentrieren, deren technische Interna sie natürlich für sich behalten.

Single oder Dual Kernel

Neben dem direkt in den Mainline-Kernel integrierten „Realtime Preemption Patch“ existiert ein zweites Verfahren, die Echtzeit-Funktionen zu realisieren. Hierbei übernimmt ein zweiter Kernel (Dual Kernel) die Echtzeit-Aufgaben. Er führt die Echtzeit-Tasks aus und muss den ersten Linux-Kernel daher jederzeit unterbrechen können, dominiert ihn somit. Genau diesen Ansatz nutzt das Projekt Xenomai.

Im Einsatz ist es zum Beispiel in der Linux-Distribution SCALE-RT von Cossatot, die auf dem Debian-Kernel basiert und durch die Xenomai-Real-Time-Erweiterung Echtzeitfunktionen wahrnehmen kann. Einsatzbereich von SCALE-RT sind Echtzeitsimulationen bei der Entwicklung von Automobil-Software.

Harte und weiche Echtzeit

Ein weiteres Anwendungsbeispiel für Xenomai ist die vierbeinige Roboterkatze

Cheetah-Cub, ein Forschungsprojekt des Biorobotics Laboratory der École polytechnique fédérale de Lausanne (EPFL) aus der Schweiz. Auf dem darin eingesetzten RoBoard RB-110 läuft ein echtzeitfähiges Xenomai-Linux [b].

In vielen Embedded-Anwendungen gelten hohe Sicherheitsanforderungen. Man denke nur an Airbags, medizinische Geräte, Maschinen oder Motoren. Unzuverlässige Software würde hier Menschenleben gefährden. Das wollen Normen für die funktionale Sicherheit wie IEC 61508 sowie abgeleitete branchenspezifische Normen wie ISO 26262 für die Automobilindustrie oder DO-178B für die Luftfahrt so weit wie möglich ausschließen [1].

Linux soll zertifiziert werden

Die Normen beschreiben unter anderem ein systematisches Vorgehen, mit dem Entwickler die Ziele erreichen können. Sogenannte Sicherheits-Integritätslevel (SIL) legen die einzuhaltenden Konstruktionsprinzipien fest, die das Risiko einer Fehlfunktion minimieren sollen.

Betriebssystemhersteller wie SYSGO oder Wind River bieten zertifizierte Werkzeuge für sicherheitskritische Anwendungen an. So nutzt Betriebssystemhersteller SYSGO in seinem Linux-Betriebssystem ELinOS den OSADL-Kernel. Der funktioniere zwar sehr gut, erfüllt jedoch nicht harte Echtzeitanforderungen in Bereichen, in denen Menschenleben auf dem Spiel stehen. Daher setzt SYSGO für solche Anwendungen lieber auf sein Echtzeit-Betriebssystem PikeOS und empfiehlt ELinOS für den Einsatz bei Netzwerk- oder grafischen Benutzerdiensten. Auch Wind River verwendet für sicherheitskritische Anwendungen, die harte Echtzeit erfordern, sein Betriebssystem VxWorks,

TRACT

- Embedded-Linux unterscheidet sich von den Standarddistributionen, denn es muss Echtzeit-Anforderungen erfüllen, mit begrenzten Hardware-Ressourcen klarkommen und eine große Prozessoren-Palette unterstützen.
- Seit der Kernel-Version 2.6.24 sind große Teile des „Real Time Preemption Patch“ Bestandteil des Linux-Kernels.
- Embedded-Linux-Distributionen kann man entweder in fertiger Form kaufen oder mithilfe freier Projekte selbst zusammenstellen.

vor allem, wenn sie Zertifizierungen vorweisen müssen. Denn damit kann Linux bislang noch nicht dienen.

OSADL will diese Sicherheitslevel mit dem Projekt SIL2LinuxMP aber auch in Linux einführen. Dessen Ziel ist das Zertifizieren der Basiskomponenten eines Embedded-GNU/Linux-Echtzeitsystems, das auf Einzel- oder Mehrkern-Boards läuft, nach den Vorgaben des „IEC Safety Integrity Level 2“ (SIL2). Zu den Basiskomponenten gehören zum Beispiel Bootloader, das Root-Dateisystem und der Linux-Kernel. Damit soll die quelloffene Software für den Einsatz im Safety-Bereich gerüstet sein.

Generell ist eine solche Zertifizierung nicht so einfach, da Linux nicht den Vorgaben des SIL entsprechend entwickelt worden ist und sich die auch nicht nachträglich einführen lassen. Laut Emde erlaubt aber eine Änderung der Norm IEC

61508 eine Zertifizierung auch von Systemen wie Linux (siehe „Alle Links“). Hier arbeitet die Genossenschaft mit dem TÜV Rheinland zusammen. Für einen Projektstart steht die Finanzierung noch aus, zurzeit sucht man noch Teilnehmer.

Plattformübergreifende Distributionen bauen

Wer ein Embedded-Linux in seinem Unternehmen nutzen will, kann entweder eine fertige Distribution kaufen, den aktuellen Kernel herunterladen oder sich selbst eine Betriebssystemumgebung bauen. Auf das eigenständige Zusammenstellen setzt das im Jahr 2010 ins Leben gerufene Yocto, ein Open-Source-Projekt der Linux-Foundation.

Hier entsteht eine Art Baukasten namens Poky, aus dem sich Embedded-Ent-

wickler mit Werkzeugen und Methoden bedienen können, um eingebettete Linux-Systeme für verschiedene Prozessorarchitekturen wie ARM, MIPS, PowerPC und x86 zu erhalten. Yocto stellt einen Baukasten zum Erstellen von Distributionen zur Verfügung. Geplant ist eine vollständige Entwicklungsumgebung. Zu den Teilnehmern von Yocto zählen vonseiten der Betriebssystemhersteller Mentor Graphics, Wind River, Monta Vista und ENEA.

Daher bildet Yocto die Grundlage einiger kommerzieller Angebote, zum Beispiel Wind River Linux 5. Diese aktuelle Betriebssystemversion unterstützt die Open-Source-Entwicklungsinfrastruktur des Projekts und ist damit auf Yocto-kompatiblen Entwickler-Boards lauffähig. Außerdem hat Wind River Yocto-Komponenten in seine „Platform for Infotainment“ eingebunden.

SYSGO setzt nicht auf Yocto, sondern hebt als Vorteil seiner Distribution ELinOS besonders die Geschwindigkeit hervor, mit der Anwender mit diesem „Out-of-the-Box-System“ loslegen können. Das sei mit dem selbstständigen Zusammenstellen einer Distribution aus verschiedenen Komponenten so nicht möglich, heißt es bei SYSGO.

Zwischen dem Yocto-Projekt und der GENIVI-Allianz [c] gibt es ebenfalls eine Verbindung. Das Konsortium besteht aus über hundert Firmen aus der Automobil- und Softwareindustrie. Es wurde 2009 auf Betreiben von BMW gegründet. Zu den Mitgliedern gehören die Betriebssystemhersteller Mentor Graphics und Wind River. Ziel ist es, eine einheitliche Plattform für Auto-Infotainment-Systeme (IVI – In-Vehicle-Infotainment) zu entwickeln, die auf Linux basiert und die Grundlage für eigene Lösungen bildet. Im IVI-Bereich geht es vor allem darum, mit den kurzen Zyklen in der Unterhaltungselektronik halbwegs mithalten zu können. Die Linux-Distribution „Yocto GENIVI Baseline“ schafft die Verbindung zwischen Yocto und GENIVI.

Ein weiteres Projekt, mit denen man Distributionen bauen kann, ist zum Beispiel das Open-Source-Framework Kael-Os. Mit ihm können Konstrukteure Linux-Distributionen für Embedded-Geräte herstellen. Es ist in Yocto integriert und wird mit OpenEmbedded generiert.

Dass binäre Distributionen zu unflexibel für Embedded-Systeme sind, findet Pengutronix. Daher baut das Unternehmen mit dem System PTXdist das Ziel-System direkt aus den Original-Sources. Außerdem bietet die Hildesheimer Firma einige inoffizielle Debian-Pakete, die

Embedded-Linux-Distributionen

Hersteller	Distribution	Web
Cosateq	SCALE-RT	www.scale-rt.com
Enea	Enea Linux	www.enea.com/solutions/Enea-Linux/
Mentor Graphics	Mentor Embedded Linux	www.mentor.com
MontaVista	Monta Vista Linux	www.mvista.com
OSADL	Real-time Linux	www.osdl.org
Red Hat	Red Hat Enterprise MRG	www.redhat.com/mrg/
SUSE Linux GmbH	SUSE Linux Enterprise Server 11 SP3 Real Time Extension	www.suse.com/de-de/products/realtime/
SYSGO AG	PikeOS, ElinOS	www.sysgo.com
Ubuntu RealTime	Echtzeit-Weiterentwicklungen	wiki.ubuntu.com/RealTime
Wind River Systems	Wind River Linux	www.windriver.com/de



Das Embedded-Betriebssystem ELinOS von SYSGO nutzt den „Realtime Preemption Patch“ von Linux (Abb. 2).

man noch nicht offiziell bei Debian finden kann, vor allem den RT-Preempt-Kernel.

Echtzeit Erweiterungen für Linux

Auch Anbieter wie Red Hat oder SUSE nutzen Erweiterungen, um ihren Enterprise-Linux-Distributionen Echtzeitfähigkeit zu verschaffen. So bietet Red Hat ein Add-on namens Enterprise MRG (Messaging, Realtime und Grid), das den Determinismus der „normalen“ Serverversion steigert: Garantierte Reaktionen auf Ereignisse sind innerhalb von acht Mikrosekunden möglich, so Red Hat. Außerdem ist die Echtzeit-Variante mit der Standardversion kompatibel. Unternehmen können nach Herstellerangaben Anwendungen, die unter Red Harts Enterprise Linux laufen, ohne Änderungen oder erneutes Übersetzen mit dem MRG-Realtime-Kernel betreiben.

Echtzeit gibt es auch bei SUSE mit der Linux Enterprise Server Real Time Extension. Sie zeichnet sich nach Herstellerangaben dadurch aus, dass sie dasselbe Kernel-Release verwendet wie die Standardversion. Die Variante ist unter anderem im Einsatz bei der Deutschen Börse in Frankfurt, bei der NASA und bei der Deutschen Flugsicherung in Langen bei Frankfurt. Dort versorgt sie die Controller an 19 Towern mit Informationen für einen sicheren und geordneten Flugablauf. Der Bildschirm der Controller darf niemals länger als fünf Sekunden leer bleiben, heißt es bei SUSE.

Onlinequellen

[a] Bericht LinuxTag 2013
www.ix.de/-1867455

[b] RoBoard RB110
biorob.epfl.ch/cheetah

[c] GENIVI-Allianz
www.genivi.org

Auswahl freier Linux-Echtzeitprojekte

KaeRTOS
www.kaertos.com

Linaro
www.linaro.org

Open Embedded
www.openembedded.org

PTXdist
ptxdist.de

Realtime for Debian
debian.pengutronix.de

Ubuntu RealTime-Erweiterungen
wiki.ubuntu.com/RealTime

Xenomai
www.xenomai.org

Yocto
www.yoctoproject.org

Yocto GENIVI baseline
projects.genivi.org/GENIVI_Baselines/meta-ivi/home

Außerdem unterstützt die Nürnberger Linux Enterprise Server Real Time Extension das Unternehmen ThyssenKrupp Electrical Steel bei der Kontrolle der Fertigungsprozesse. Für jeden produzierten Meter Stahl sind dort 200 verschiedene Messungen erforderlich, und dabei muss es schnell gehen: Einige der Fertigungsstraßen bewegen sich mit einer Geschwindigkeit von 18 Metern pro Sekunde, das heißt, die 200 Messungen müssen garantiert innerhalb von 50 Millisekunden erfolgen.

Fazit

Diverse Hersteller unterstützen den Einzug von Linux in die Echtzeit-Welt. Aber auch freie Projekte wie Yocto stellen Baukästen zur Verfügung, mit denen sich Entwickler eine eigene Distribution zusammenstellen

können. Für sicherheitskritische Anwendungen, die eine Zertifizierung verlangen, ist Linux bislang noch nicht geeignet. Zurzeit laufen Bestrebungen, auch Linux nach den Vorgaben von „IEC Safety Integrity Level 2“ (SIL2) zu zertifizieren. (avr)

Barbara Lange

ist IT-Journalistin und Inhaberin des Redaktionsbüros kurz und einfach in Lengede.

Literatur

[1] Lange, Barbara; Alles richtig; Standards regeln die Softwareentwicklung; iX extra 2/2012; S. I ff.

Alle Links: www.ix.de/ix1310100



Zukunft.Dynamisch.Entwickeln.

3. Deutsche Python-Konferenz

14. Okt. Tutorialtag
15.-17. Okt. Vorträge
18. Okt. BarCamp > Eintritt frei! · 18.-19. Okt. Sprints



14.-19. Oktober · Köln

Goldspender

PROUNIX
skoobe
blueyonder



LINUX
ADMIN

O'REILLY

Silbersponsor

DIVIO
Python Academy
PAYMILL

pymove3D

Bronzespender

GU GU Cyrus AG
der Partner für IT-Schulungen
transcode
Wir bauen Ihre Mauer in Code
IMMOBILIEN
SCOUT24

JÜLICH
FORSCHUNGSZENTRUM

ORBI TEAM
WIR VERARBEITEN DAS WISSEN IN CODE

billiger.de

IMMOBILIEN
SCOUT24

billiger.de

Veranstalter

py cologne
Python Software Verband e.V.
DLR Deutsches Zentrum für Luft- und Raumfahrt e.V.



70131.de/pycon/de/de/3724

Mein Ticket sichern...

Jetzt registrieren!

Dem mobilen Anwender auf die Finger geschaut



Tracking-Tour

Frank Puscher

Nutzer mobiler Endgeräte agieren deutlich anders als solche, die mit einem stationären PC ins Netz gehen. Damit Website-Betreiber ihre Seiten und Apps entsprechend anpassen können, müssen sie zuvor das Verhalten der Zielgruppen differenziert untersuchen.

Im Jahr 2014 werden erstmals mehr Webseiten von Smartphones und Tablets aufgerufen als von Desktop-PCs. Das zumindest meint eine Studie von Adobe. Fragt man bei Onlinehändlern nach, liegt deren mobile Zugriffsquote zwischen 20 und 30 Prozent, Tendenz stark steigend (siehe Kasten „Mobiles: Daten und Fakten“).

Nach etlichen Jahren des Experimentierens gewinnt der Mobilsektor ökonomische Relevanz. Um den Bedürfnissen des mobilen Webnutzers auf die Spur zu kommen, müssen die interessierten Kreise zunächst ihre Analysesysteme so einrichten, dass sie das Verhalten der Klienten überhaupt sauber messen können (siehe Kasten „Apps nicht überfrachten“).

Für die sogenannte Onsite-Messung (siehe „Alle Links“) stellt das Tracking

keine größere Hürde dar. Das Verfolgen der eigenen Webseiten geschieht mit in die Seiten eingebundenem Tracking-Code. In den meisten Fällen wird ein Zählpixel eingebaut, ein unsichtbares Bild, dessen Aufruf darauf hindeutet, dass jemand die zugehörige Seite betrachtet oder zumindest geladen hat. Der Server speichert sodann die Daten des Clients, der das Pixel angefordert hat.

Dabei interessiert den Server nicht, ob der Aufruf von einem mobilen oder stationären Gerät kommt. Mobile Clients lassen sich jedoch besser vermessen (siehe Kasten „Werbung beschränken“). Der Browser kann je nach Konfiguration zusätzlich die Positionsdaten des Nutzers übermitteln. Für eine Anwendung mit Ortsbezug ist das unter Umständen eine wichtige Information. So könnte die Navigator-App der deutschen Bahn den

Startbahnhof entsprechend dem aktuellen Standort vorgeben.

Pixelmessung ist mit Fehlern behaftet. Die Platzierung des Zählpixels im Seitenquelltext kann bewirken, dass das Pixel gezählt wird, obwohl der Nutzer die Seite noch gar nicht vollständig geladen hat. Und auch das Laden in einem Tab oder Fenster, das derzeit nicht im Fokus steht, wird mitgerechnet, obwohl der User die Seite gar nicht ansieht. Bei sogenannten Pop-unders, Werbefenstern, die nach einer Nutzeraktion irgendwo im Hintergrund starten, ist das ein gängiger Messfehler.

Das quantitative Messen kämpft ebenso wie das qualitative mit methodischen Schwierigkeiten. Will man die exakte Nutzung eines Mobilangebots abbilden, geht kaum ein Weg an Eyetracking vorbei. Das System beobachtet dabei nicht nur die Fingertipper auf dem Bildschirm, sondern auch den Blickverlauf des Anwenders, um zu sehen, wohin dessen Aufmerksamkeit geht.

Maus-Tracking hingegen bringt wenig, da der Proband den Finger nicht von einem Interaktionselement zum anderen über den Bildschirm bewegt. Dafür gibt es eine ganze Reihe weiterer Ereignisse, die sich im mobilen Umfeld messen lassen. Zum Tap (Klick) kommen noch der Doppel-Tap sowie die Vergrößerungsgesten Pinch und Zoom – wobei die Testumgebung idealerweise den Ausschnitt zeigt, den der Anwender auf dem Bildschirm sieht. Das Scrollen will ebenfalls eingefangen werden und zwar vertikal und horizontal. Schließlich kommt zur Lagedeknung (Portrait vs. Landscape) noch das Feststellen einer Lageveränderung. Letzteres erfolgt häufig, wenn der Nutzer auf ein Formular trifft, in das er etwas eingeben soll. Er wechselt dann meist in die Breitansicht, da dort die Bildschirmtastatur größer und leichter zu bedienen ist.

Mobiles Verhalten im Labor nicht testbar

Die methodisch größte Schwierigkeit des Usability-Tests mit Mobilgeräten ist allerdings der mangelnde Nutzungskontext. Während sich ein Büroarbeitsplatz nachstellen lässt, gibt es im Mobilsegment zahlreiche unterschiedliche Szenarien, die den User mehr oder weniger ablenken. Ein Abbruch in einem Formular könnte in der Realität durch Bedienungsprobleme bedingt sein, oder dadurch, dass gerade der Bus kommt, auf den der Benutzer gewartet hat. Der Labortest kann nur die erste Variante feststellen. „Labortests sind für mobile Anwendun-

Mobiles: Daten und Fakten

Zweimal jährlich untersucht die Arbeitsgemeinschaft Online Forschung (AGOF) die Verbreitung und Reichweite mobiler Endgeräte. Demnach gibt es 60 Millionen Nutzer in Deutschland. 21,3 Millionen haben im 30-tägigen Erhebungszeitraum mit ihrem Smartphone oder Tablet eine Website oder eine App mit Internetanbindung aufgerufen. Das entspricht einer Steigerung von 25 % im Vergleich zu 2011. Der männliche Anteil überwiegt (58 % zu 42 %). Die meisten sind zwischen 20 und 29 Jahre alt (28,5 %).

Bereits 15,6 % der Befragten verwenden den mobilen Zugang als Ersatz für den stationären. 70 % betrachten die mobile Option nur als Ergänzung. Die Schwerpunkte liegen bei E-Mail, Social Media und Onlinespielen. Immerhin 36,1 % machen einmal pro Woche Onlinebanking (siehe Abbildung). Die beliebtesten Webseiten sind Gutefrage.net und Bild.de.

„Bei vielen Endgeräten kann man nicht mehr unterscheiden, ob es primär mobil oder stationär genutzt wird. Das ist für die AGOF eine der größten Herausforderungen“, erklärt Steffen Bax, stellvertretender Vorsitzender der Sektion Mobile. Aus diesem Grund will die Arbeitsgemeinschaft ihre Studien mobile Facts und Internet Facts zusammenlegen (siehe „Alle Links“).

Etwas tiefer in die qualitative Marktforschung wagte sich das Reiseportal HRS vor. Jeder dritte Smartphone-Besitzer hat bereits ein Hotelzimmer mit dem Gerät gebucht, ermittelten die Forscher vom Göttinger Usability-Dienstleister eResult für HRS.

Wenig überraschend zeigt sich die Nutzungsverteilung: Männliche Geschäftsleute domi-

nieren bei der Hotelbuchung. Fast jeder zweite hat das bereits hinter sich. Die Studie fand auch heraus, dass für die Hotelsuche die App besser funktioniert als eine mobile Website. „Das liegt vor allem an der Integration mit dem Endgerät, zum Beispiel dem Verwalten der Buchung in Apples Passbook oder der Erinnerungsfunktion im Kalender“, so Björn Krämer, Director Mobile & New Media bei HRS.

Ich nutze das mobile internetfähige Gerät mindestens einmal in der Woche für Folgendes:



Immerhin fast jeder fünfte Besitzer eines Mobilgeräts kauft einmal in der Woche online ein.

gen kompletter Quatsch. Das funktioniert nur für die Entwicklung von Prototypen in einer frühen Projektphase“, meint Julianne Hartmann vom Dresdner Analyse-spezialisten m-pathy.

Für die Verhaltensmessung in Apps gelten im Wesentlichen die gleichen Regeln wie für Websites und für Mobilgeräte angepasste Angebote. Hier lassen sich ebenso Tracking-Pixel in den einzelnen Seiten unterbringen, sofern es sich um eine App handelt, die mit dieser Seiten-Metapher arbeitet. Für komplexe Anwendungen mit vielen interaktiven Ele-

menten gibt es Software Development Kits (SDKs). Eins der populärsten kommt von der Analysefirma Flurry. Deren Ansatz ähnelt dem von Google Analytics: Die Einstiegsversion ist kostenlos. Freilich ist der App-Entwickler genötigt, auf diese Form des Trackings hinzuweisen.

Neben der Vielzahl zusätzlicher Parameter, die messbar, jedoch nicht für jede Anwendung wichtig sind, existieren zwei besondere Hürden im Zusammenhang mit Apps. Zunächst ist es für viele Entwickler wichtig zu wissen, wie die Interessenten auf eine App gestoßen sind. War es

ein Banner, ein direkter Link oder vielleicht eine Bewertungsseite im App-Store?

Das in Seattle ansässige Unternehmen HasOffers hat sich auf derartige Fragen spezialisiert. Es schließt Verträge mit Werbenetzwerken, damit der Tracking-Code im jeweiligen Werbemittel hinterlegt werden kann, und wertet es in der App aus. Hierzu erstellt der Code einen sogenannten Fingerprint, eine Kombination aus Hardware-Parametern, die so differenziert ist, dass es die meisten Konfigurationen nur ein einziges Mal gibt.

Der Tracking-Code in der App macht praktisch das Gleiche. Nun kann der Server das Betrachten des Banners sowie das Öffnen der App verbinden und feststellen, woher der Nutzer kam. Darüber hinaus bietet ein Tool namens MobileAppTracking das Messen der User-Bewegungen und -aktivitäten innerhalb der App an. Einschränkung: Das Partner-Netzwerk ist aus europäischer Sicht noch zu dünn.

„Beim Tracking mobiler Apps ist die Messung anders, insofern auch die Offline-Nutzung relevant ist. Daher braucht man hier Verfahren, die diese Offline-Aktivitäten puffern und bei der nächsten Online-Verbindung übertragen“, erklärt Olaf Brandt, Director Produktmanagement beim Hamburger Analysespezialisten etracker.

IX-TRACT

- Werbetreibende und Onlineshops sind daran interessiert, das Verhalten von Internetnutzern minutiös zu vermessen.
- Hauptsächlich geht es ihnen darum, ihre Angebote passgenau auf einzelne Nutzer zuzuschneiden.
- Messverfahren vor allem im mobilen Umfeld haben mit methodischen und technischen Schwierigkeiten zu kämpfen. Allein ihre Kombination verspricht aussagekräftige Einschätzungen.
- Nicht jeder will sich ständig von Tracking-Diensten verfolgen lassen. Auf dem PC kann man sich gut schützen, bei Mobilgeräten ist die Sache schwierig bis unmöglich.

Derzeit integriert eTracker ein solches Modul in die eigenen Suites.

Einen Schritt weiter ist der Berliner Wettbewerber Webtrekk mit Mobile Insights. Es enthält die asynchrone App-Analyse, die Offline-Benutzung messen kann und die Daten bei der nächsten Netzverbindung an den Server ausliefert.

Etwas komplizierter geht es zu beim Tracking von Werbemaßnahmen. Das klassische Cookie-basierte Nachverfolgen funktioniert ähnlich wie im stationären Web. Moderne Smartphones-Browser erlauben das Setzen und Lesen temporärer Textdateien. Google beendete vor einem Jahr feierlich die Unterstützung älterer Browser, die das nicht können, für die Android-Plattform.

Für Diskussion sorgt derzeit die Frage, ob nur die gerade aufgerufene Website

Cookies setzen darf (First Party) oder ob Drittanbieter – in der Regel die Werbenetzwerke oder die Werbetreibenden selbst – dies ebenfalls tun dürfen (Third Party). Nach EU-Direktive ist Letzteres nur nach explizitem Einverständnis des Users erlaubt. Vorausschauende Analyseanbieter setzen hier mindestens zusätzlich auf das Fingerprint-Verfahren.

Apple kocht eigenes Süppchen

Apple kocht unterdessen sein eigenes Süppchen. Derzeit schmeißt der Anbieter immer mehr Apps aus dem App Store, die versuchen, Cookies zu setzen, was gegen die hauseigenen allgemeinen Geschäftsbedingungen verstößt. Es hat sich

der Trick eingebürgert, aus der App heraus eine normale Website im Browser zu laden, die dann das Cookie platziert.

Inzwischen bietet Apple ein eigenes Tracking-Format namens IDA beziehungsweise IDFA an (Identifier For Advertisers) an. Es funktioniert ähnlich wie Cookies, der Anbieter behält aber die Fäden über Implementierung, Laufzeit und Datentiefe in der Hand. Einige US-Experten erwarten, dass IDFA künftig für den mobilen Safari-Browser eingeführt wird.

Aus Sicht der „User Experience“ ist allerdings das Betrachten der einzelnen Plattformen und Systeme reines Stückwerk. Was, wenn ein Cookie einen Surfer auf dem Desktop erkannt hat und er im Rahmen einer personalisierten Website spezielle Inhalte serviert bekommt? Der selbe Nutzer ruft die Site später mit sei-

Bedienbarkeit leidet unter überfrachteten Apps

Vincent Schlecker, Analysespezialist bei Mindlab Solutions beantwortet Fragen zum mobilen Tracking.

iX: Wie integriert sich Mobile Analytics heute in die Webanalyse?

Schlecker: Da sich das Geschäftsmodell einer App oftmals mit dem einer Website deckt, ist die Durchführung von professionellem Mobile Analytics wie auch eines umfassenden Web-Controlling unerlässlich. Wenn beide Analysen mit einem System umgesetzt werden, können die individuellen Reportings aufeinander abgestimmt und die Ergebnisse so direkt miteinander verglichen werden.

iX: Hat man im mobilen Umfeld dieselben Daten zur Verfügung, um zum Beispiel die Absprungrate zu messen?

Schlecker: Viele Daten beziehungsweise Kennzahlen sind beim Mobile Tracking dieselben wie im Web-Controlling. Jedoch gibt es beim Tracking spezifische Daten, zum Beispiel die Nutzungsanalyse einer App im Quer- oder Hochformat. Auch der Erfolg eines Buttons kann im mobilen Umfeld anders bewertet werden als im Desktop-Bereich, dies hängt dann von den unterschiedlichen, individuellen Zielsetzungen des Website- und App-Betreibers ab.

iX: Wie gestaltet sich das Usability-Testing idealtypisch. Geht man mit Prototypen ins Labor? Wie steht's mit Eyetracking? Oder gründet sich alles auf A/B-Tests und Co.?

Schlecker: Ein Eyetracking ist bei großen Nutzerzahlen nicht zielführend, da man sich zu sehr auf wenige Nutzer konzentriert. Da der Darstellungsbereich kleiner ist, gibt es auch weniger Varianz bei den Nutzerpräferenzen. Ein A/B-Testing auf Grundlage von Reports, die das Verhalten aller Nutzer einheitlich zusammenführen, ist eine von mehreren Möglichkeiten, die Usability-Optimierung einer App erfolgreich zu betreiben. Andere Optionen sind beispielsweise die Verbesserung in Prozessen auf Grundlage von detaillierten Prozessanalysen sowie die ständige Überwachung, ob es zu Benutzerfehlern oder Abstürzen der

App kommt. Diese sollten dann möglichst schnell behoben werden, damit man keine User verliert.

iX: Gibt es grundlegende Unterschiede im Bereich Testing/Messung zwischen App, Web-App und mobiler Website?

Schlecker: Lediglich bei der Datenerfassung muss zwischen Apps und mobilen Websites unterschieden werden. Da Apps unter Umständen häufig auch offline genutzt werden können, muss die Erfassung der Nutzungsdaten, etwa durch eine Tracking Library, auf dem Gerät der Nutzer selbst erfolgen. Dann kann man sie später bei bestehender Internetverbindung des Clients komprimiert an den Server schicken. Nur dann sind die Daten über Nutzeraktivitäten zu 100 Prozent genau und vollständig.

iX: Was ist der häufigste Fehler in der Usability, und was wird bei der Konversionsoptimierung auf der mobilen Seite gerne übersehen?

Schlecker: Aus Angst, Content an der einen oder anderen Stelle in der App zu entfernen, wird die App häufig mit zu viel Inhalt überladen, was der Usability schadet. Bei der Konversionsoptimierung ist es wichtig, nicht nur die Conversion-Rate als Grundlage zur Erfolgsbewertung zu nehmen, sondern bei der Analyse und Optimierung einen Schritt nach dem anderen zu machen, indem man beispielsweise erst einmal versucht, die Anzahl der aktiven App-Nutzer zu erhöhen.



Vincent Schlecker präferiert A/B-Tests mit vielen Nutzern vor Eyetracking und ähnlichen Einzeltests.

Werbung beschränken

nem Tablet auf und sieht komplett andere Angebote.

Kein Problem damit haben Dienste, die ein Login erfordern, allen voran Google und Facebook. Da die meisten Nutzer aus Komfortgründen das automatische Login zulassen, können die Dienste genau feststellen, welcher Nutzer wann welches Gerät benutzt. Onlinesysteme von Dritten, die ebenfalls das Facebook-Login nutzen, können dies ebenso, geben aber die Daten zusätzlich gleichzeitig an Facebook weiter. Auch hierfür verlangt der deutsche Datenschutz eine explizite Einverständniserklärung. Mit dem einfachen Einbau der Facebook-API ist es nicht getan.

Auch Mails werden gemessen und gewogen

Dienste, die direkt mit Personalisierung arbeiten, sind ebenfalls in der Lage, ein geräteunabhängiges Profil zu erzeugen und auszulesen. Das gilt etwa für E-Mails. So wohl transaktionsbezogene Mails (im Zusammenhang mit einem Kauf, einer Registrierung et cetera) als auch Newsletter bekommen eine persönliche ID, die in den Links übergeben wird. Somit weiß der Webserver genau, wer auf was in einem Newsletter reagiert hat. Sie ist nicht nur mit dem Tracking-Pixel verbunden, sondern ebenso mit der Landeseite, die beispielsweise aus einem Newsletter verlinkt ist. Das Tracking-Pixel zählt die Öffnung der Mail, die Landeseite die Klickrate. Beide können messen, welches Gerät Letztere ausgelöst hat und dies an das Analysesystem melden.

Yvonne Perdelwitz von der Heidelberger Agentur postina.net hat den Newsletter des Marketingportals ABSOLIT.de untersucht. Er erreicht 30 000 Empfänger im B2B-Segment. Sie testete im Juni 2012 und im Juni 2013. „Die Unterschiede sind augenfällig. Insbesondere die Klickrate ist bei mobilen Abrufen frappierend um 60 % geringer“, so Perdelwitz. Ihrer Annahme zufolge hat das etwas mit schlechten Ladezeiten und geringen Bandbreiten zu tun.

Für den Marketingberater Frank Strzyzewski aus Offenbach hat eine solche Analyse grundlegende Bedeutung für die E-Mail-Strategie. „Das Wissen um die wechselnde Benutzung von mobilen und stationären Clients ist besonders wichtig, um die optimale Öffnungsrate zu erreichen. Es geht um den bestmöglichen Zeitpunkt für das Verschicken eines Newsletters. Erreicht der den Nutzer am stationären Rechner, so ist die Klickwahrscheinlichkeit zweimal bis dreimal so hoch.“

Wer gern personalisierte Reklame bekommt und nichts dagegen hat, sich der Werbewirtschaft glänzen zu präsentieren, muss diesen Beitrag nicht lesen. Es könnte jedoch sein, dass nicht jeder mit Angeboten bombardiert werden will, auch nicht mit speziell zugeschnittenen.

Sich vom stationären PC aus gegen Tracking zu wehren, ist relativ einfach. Das Browser-Add-on Ghostery unterbindet das Nachverfolgen effektiv, und Ad-Blocker tun ein Übriges. Die Suchmaschine ixquick alias Startpage speichert weder IP-Adressen noch irgendwelche Surf-Verläufe und gibt keine Daten an Dritte weiter. Wer solche Programme einsetzt, bekommt kaum noch Werbung zu sehen. Die wackeren Datenschützer vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein haben einige Tipps zum Schutz vor Tracking zusammengetragen (siehe „Alle Links“).

Selbst Facebook-Anwender können Werbung, Spieleanfragen und ähnlich Nervtötendes ausblenden, und zwar mit F.B. Purity. Via Facebook lässt sich der Link auf die entsprechende

Seite nicht posten, er wird als Spam abgewiesen. Aus Sicht der Macher des sozialen Netzes ist das einigermaßen verständlich, denn das Tool greift ja deren Geschäftsmodell direkt an. Hier muss man abwarten, wie lange das Ganze noch gutgeht. Den Programmierer der Browser-Extension hat Facebook schon rausgeschmissen, und die Rechtsabteilung des Konzerns versucht, dem Werkzeug den Garaus zu machen.

Auf Mobilgeräten gestaltet sich das Eindämmen von Tracking erheblich schwieriger. Ortungsdienste lassen sich zwar sowohl unter iOS als auch Android deaktivieren, allerdings funktionieren dann die auf diesen Informationen aufbauenden Dienste nicht mehr oder nur noch eingeschränkt. Mit iCab Mobile existiert ein Browser für iOS, der unter anderem Anzeigen unterdrücken kann. Einige Hinweise und Artikel zu diesem Spannungsfeld erhält man über „Alle Links“. Ganz entkommt man dem Tracking im Mobilbereich leider nicht, wer jedoch seinen PC dichtmacht, verhindert zumindest das Kreuznutzen mobiler und stationärer Websites.

Jürgen Diercks

Frank Strzyzewski kennt einen einfachen Trick für die Festlegung des besten Versandzeitpunkts. „Man kann auch den Zeitpunkt der Newsletter-Anmeldung nehmen. Da die meisten Registrierungen aus stationären Endgeräten erfolgen – es ist nervig, auf mobilen Endgeräten zu tippen – sind die Anmeldezeitpunkte in der Regel auch Zeitpunkte stationärer Endgerätenutzung.“

Wer die Kreuznutzung von Website und mobiler Website mit unterschiedlichen Geräten analysieren möchte, ist darauf angewiesen, dass sein Tracking-Anbieter den entsprechenden Code in allen Plattformen hinterlegen kann. Die Analystiker von m-pathy verwenden dafür JavaScript. Dieser Code ist in der Lage, nicht nur den Seitenaufruf zu protokollieren, sondern ebenso die jeweilige Interaktion. „Zunächst haben wir mit Koordinaten-Tracking experimentiert, aber das hat wegen der Vielzahl an Endgeräten nicht funktioniert. Inzwischen machen wir im Hintergrund Screenshots“, erläutert Managing Director Juliane Hartmann.

In ihren ersten Analysen hat Hartmann überraschende Fehler festgestellt. „Tatsächlich vergessen viele Site-Betreiber, die Telefonnummer in der mobilen Website so zu codieren, dass man durch Drauftippen anrufen kann. User drücken acht Mal hintereinander den Home-Button, um die Telefonnummer abzutippen.“ Außerdem sollte in Formularfeldern, wo nur Zahlen zugelassen sind, die Soft-Tastatur entsprechend umschalten. „Zu große Formularfelder sind übrigens auch schlecht, da sie

hen die Nutzer nicht, wie es weitergeht“, so die Dresdnerin. Aus den aufgezeichneten Daten erstellt MPathy Videos, die die Aktionen des Anwenders zeigen.

Ein Verfahren allein reicht nicht

Wer herausfinden will, wo Smartphone-User anders agieren als die Benutzer stationärer Rechner, kommt um die differenzierte Analyse des mobilen Verhaltens nicht herum. Eine einzelne Tracking-Methode reicht nicht aus. Alle vier gängigen Messverfahren – Cookies, Zählpixel, In-App Tracking und die Verfolgung eines technischen Fingerprints – müssen kombiniert und anonymisiert laufen. Der erste Schritt ist zweifellos das Auswerten der vorhandenen Daten. Angesichts der zahlreichen messbaren Parameter scheint es dringend geboten, sich vor der Untersuchung ernsthafte Gedanken zu machen, welche Werte tatsächlich relevant sein könnten. Sonst erstickt der Analyst in den Daten. Jim Sterne, Gründer von Target.com und Online-Marketer der ersten Stunde bringt es auf den Punkt: „Please think before you analyse.“ (jd)

Frank Puscher

arbeitet seit 20 Jahren als Berater, Autor und Journalist im Onlinemarketing.



Das Internet scannen und auf Schwachstellen untersuchen

Inventur

**Sebastian Schinzel,
Maximilian Thünemann**

Mit nicht ganz legalen Mitteln hat ein Hacker eine Art Bestandsaufnahme des heutigen Internets gemacht und die Daten komplett ins Netz gestellt – eine Fundgrube für Forscher.

Sicherheitslücken in Internetanwendungen, seien es Webanwendungen oder E-Mail-Dienste wie SMTP oder IMAP, gehören längst zum Alltag, und um kein Opfer von Angriffen zu werden, sollte man die Dienste immer auf dem aktuellen Stand halten. So weit die Theorie. In der Praxis lassen manche Administratoren die Dienste über Jahre hinweg ohne Updates im Internet stehen.

Eine andere Ursache für die Angrifbarkeit von Diensten ist, dass der Administrator in vielen Fällen keinen vollständigen Überblick darüber hat, was alles über das Internet erreichbar ist. Eine kleine Unachtsamkeit bei der Konfiguration, ein Tippfehler in den Firewallregeln und schon ist der Dienst aus dem Internet erreichbar. Und in einer schnell gewachsenen IT-Infrastruktur ist dem Administrator vielleicht noch gar nicht der Gedanke

gekommen, dass das ehemals vertrauenswürdige Intranet, in dem man vor Jahren noch jeden beim Vornamen kannte, mittlerweile mehrere Hundert oder Tausend Benutzer zählt, von denen möglicherweise nicht alle vertrauenswürdig sind.

Aus Sicht eines Angreifers sind das gute Nachrichten, da er bereits vorgefertigte Angriffsksripte (Exploits) für bekannte Schwachstellen in solchen Anwendungen verwenden kann, um diese zu kompromittieren. Das Metasploit-Framework liefert beispielsweise rund 1100 solcher Exploits, die selbst Laien über eine einfache Kommandozeilen-Schnittstelle gegen ein Zielsystem einsetzen können. Aber wie findet der Angreifer mögliche Ziele? Im IPv4-Adressbereich gibt es theoretisch 2^{32} IP-Adressen, das heißt rund 4 Milliarden potentielle Ziele, wobei es für jedes Ziel 2^{16} (rund 65 000)

mögliche Ports gibt, auf denen ein anfälliger Dienst laufen könnte. Zusammengekommen sind das zu viele IP/Port-Kombinationen, als dass ein einzelner Angreifer auf der Suche nach anfälligen Diensten alle durchprobieren könnte.

Zumindest war das die gängige Meinung, bis Unbekannter im letzten Jahr einen Datensatz veröffentlichten, der genau das dokumentierte: einen vollständigen Scan aller öffentlichen IPv4-Adressen mit den gängigen Ports, auf denen typische Internetdienste laufen. Wie hat der Unbekannte das angestellt?

Mächtiges Scan-Werkzeug: Das Carna-Botnetz

Ausgangspunkt für die Scans war, dass der Unbekannte eine große Anzahl von Telnet-Diensten im Internet ausgemacht hatte, auf die man mit Standard-Zugangsdaten wie Benutzername root und Passwort root oder Benutzername admin und Passwort admin zugreifen konnte. Meldet man sich auf diesen Systemen an, bekommt man vollen Zugriff auf den Rechner, auf dem der Telnet-Dienst läuft. Der Unbekannte hat daraufhin das Internet nach solchen Telnet-Diensten durchsucht und mehrere Hunderttausend dieser Dienste gefunden, teilweise auf kleinen Heimroutern, teilweise in Industrieanlagen, teilweise auch in ausgewachsenen BGP-Routern (Border Gateway Protocol).

Zusammengekommen hatte er damit eine große Anzahl an Rechnern und deren Ressourcen zur Verfügung, mit denen es möglich war, den IPv4-Adressbereich zu scannen. Er nannte diesen Rechnerzusammenschluss „Carna-Botnetz“. Er erstellte daraufhin ein Programm auf Basis des bekannten Netzwerkscanners Nmap, das er auf die kompromittierten Rechner kopierte und mit dem diese wiederum den IPv4-Bereich scannen. Da die eigentlichen Funktionen der Rechner nicht beeinträchtigt werden sollten, wurde das Programm nur im flüchtigen Speicher abgelegt und war somit nach einem Neustart restlos entfernt. Weiterhin achtete der Unbekannte nach eigener Angabe darauf, die Ressourcen der gekaperten Rechner nicht zu sehr zu beanspruchen, das heißt die Anzahl der gleichzeitig gescannten IP-Adressen war auf zehn pro Sekunde beschränkt.

Auch das Design des Carna-Botnetzes unterscheidet sich deutlich von der Architektur klassischer Botnetze. Diese nutzen üblicherweise einen zentralen Command-&-Control-Server, der dem Bot bekannt ist und zu dem sich infizierte Systeme verbinden. Da jedoch sämtliche

Systeme direkt aus dem Internet erreichbar sind, kann man diese Kommunikation umkehren, sodass ein zentraler Server den Kontakt zu einem infizierten System aufnehmen kann. Dadurch ist es möglich, die Verwaltung und Administration von einem Rechner auszuführen, der sich hinter einem NAT-Gateway (Network Address Translation) befindet.

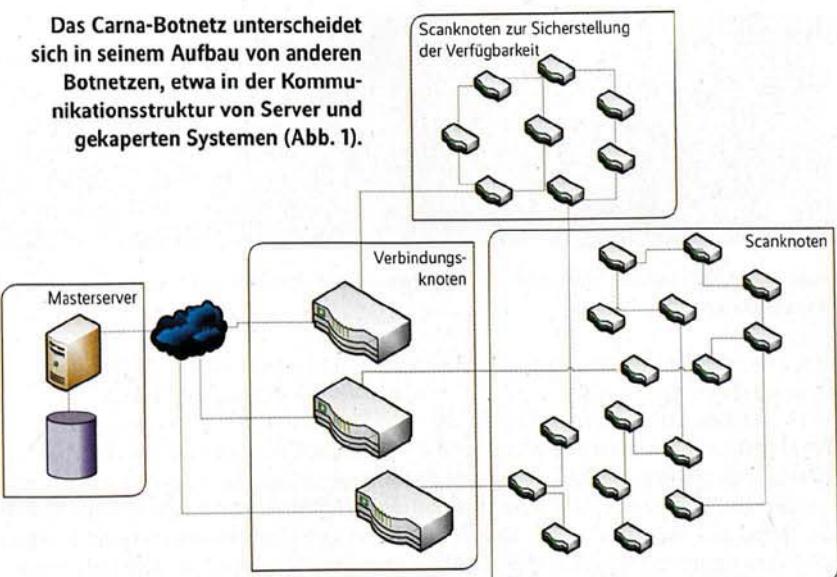
Abbildung 1 zeigt die Infrastruktur des Carna-Botnetzes. Diese besteht aus einem Masterserver und einer Vielzahl von infiltrierten Systemen, die entweder als Scanknoten oder als Vermittlungsknoten fungieren. Der Masterserver dient dazu, Scanaufträge zu verteilen und zu koordinieren sowie das Botnetz zu administrieren. Zusätzlich verwaltet er eine zentrale Datenbank mit den IP-Adressen aller infizierten Systeme.

Via Telnet für Nachschub sorgen

Diese Datenbank kann allerdings aufgrund eines Neustartes eines infizierten Systems oder neu vergebener IP-Adressen nicht mehr erreichbare Systeme enthalten. Um die Anzahl falscher Eintragungen gering zu halten, setzte der Unbekannte daher etwa 9000 Scanknoten ausschließlich dazu ein, den gesamten IPv4-Addressbereich nach offenen Telnet-Logins zu durchsuchen und bei Erfolg den Bot dort erneut zu installieren. Hierdurch erreichte eine durchgehende Verfügbarkeit von nahezu 85 % aller Clients.

Der größte Teil der Scanknoten diente aber dazu, die im Rahmen des Internetzensus durchgeführten Scans auszuführen. Hierzu weist der Masterserver die Scanaufgaben zu. Dies erfolgt durch Übermittlung einer Identifikationsnummer, der Start- sowie der Ziel-IP-Adresse und einer Schrittweite. Aus diesen Informationen generieren die Scanknoten die eigentli-

Das Carna-Botnet unterscheidet sich in seinem Aufbau von anderen Botnetzen, etwa in der Kommunikationsstruktur von Server und gekaperten Systemen (Abb. 1).



chen Scanaufträge und führen sie aus. Die Ergebnisse melden sie an die Vermittlungsknoten zurück, die diese wiederum dem Masterserver zum Download bereitstellen. Der Masterserver legt die Vermittlungsknoten fest und wechselt sie regelmäßig, um eine übermäßige Netzwerkauslastung zu vermeiden. Es wählt dafür diejenigen Systeme aus, die über die meiste Rechenleistung verfügen.

Nach ersten eigenen Analysen hat der Unbekannte den kompletten Datensatz auf der Projekthomepage als BitTorrent-Download zur Verfügung gestellt. Dieser trotz Komprimierung insgesamt 568 GByte umfassende Download enthält neben den Rohdaten des Scans zusätzlich die Ergebnisse der auf der Homepage veröffentlichten Auswertungen [a], eine Offline-Kopie der Projektwebseite sowie eine Reihe von Skripten. Eines dieser Skripte dient zur verteilten Dekompression der Daten auf einem Rechencluster. Mit einem weiteren Skript kann man die Service-Probe-Datensätze

mithilfe einer modifizierten Nmap-Version auswerten. Nach vollständiger Dekompression aller Archive beträgt die Größe des Datensatzes etwa 9 TByte.

Wer etwas in dem Datensatz stöbern will ohne gleich einen Stapel Festplatten zu kaufen, kann das über die Weboberfläche eines Sicherheitsforschers [b] tun. Hier kann man im Datensatz bequem ein beliebiges /24-Netzwerk nach offenen Ports durchsuchen oder sich alle IP-Adressen mit einem bestimmten offenen Port anzeigen lassen. Damit kratzt man jedoch nur an der Oberfläche. Wer mehr wissen will, sollte sich doch zusätzlichen Plattenplatz anschaffen und die Daten entpacken.

Die Rohdaten des Scans liegen strukturiert vor. Die Daten sind in eigenen Unterordnern nach Art des Scans organisiert, das heißt es gibt je einen Ordner für die Datensätze des ICMP Ping Scan, die Host Probes, die Reverse-DNS-Abfragen, die Traceroutes und die Service Probes. Jeder dieser Unterordner, ausgenommen der Service-Probe-Ordner, enthält jeweils die Scandaten für jedes /8-Netz zwischen 1.0.0.0/8 und 223.0.0.0/8 als komprimierte ZPAQ-Archive.

Der Service-Probe-Ordner weist eine weitere Besonderheit auf. Hier sind die Rohdaten zunächst nach der Art des Service Probe und dem getesteten Port zu einem tar-Archiv zusammengefasst, das wiederum die nach /8-Netzen geordneten Rohdaten enthält. Diese Strukturierung ermöglicht eine sehr genaue Auswahl der Daten, da hierdurch bestimmte Netzbereiche unabhängig voneinander analysierbar sind. Zusätzlich bietet diese Organisation den Vorteil, dass man die Ergebnisse verschiedener Scanarten losgelöst voneinander betrachten kann, ohne

TRACT

- Mithilfe gekappter Systeme wurden alle IPv4-Adressen im Internet auf gängige Ports und Dienste gescannt und zahlreiche Daten über die Standorte der ungesicherten Geräte gesammelt.
- Die als „Internetzensus 2012“ bekannt gewordenen Informationen sind frei verfügbar und für Sicherheits- und Internetforscher aller Art eine aufschlussreiche, automatisiert analysierbare Datensammlung.
- Informationen nutzen den „Guten“ wie den „Bösen“: Während Erstere mit ihnen zu einem sichereren Internet beitragen können, ist es Letzteren möglich, ihre Angriffe und kriminellen Aktivitäten zu optimieren – zumal mit neuen, performanten Werkzeugen. Dagegen hilft nur, die eigenen Systeme abzusichern und aktuell zu halten.

```

124.2.40.24 1355510700 5
124.2.40.24 1355535900 5
124.2.40.34 1343256300 3
124.2.40.40 1355589900 5
124.2.40.44 1343205900 1 HTTP/1.1 20500 20Internal 20Server 20Error 0D 0AConnection: 20close 0D 0ADate: 20We
4, 2025 20Jul 202012 2008:52:58 20GMT 0D 0AContent-Type: 20text/html 0D 0AExpires: 20Wed, 2025 20Jul 202012 2008:51:58 20GMT 0D 0ASet-Cookie: 20ASPSESSIONIDC
CDTBHQ3DAHFNUDGACDFEAOMCHMPG; 20path=/ 0D 0AContent-Control: 20private 0D 0A 0D 20<font 20face: 3D" B1 BC B8 B2" 20
size: 3D> 0A<p>Microsoft 20VBScript 20 B7 B1 C5 BB C0 D3 20 BF C0 B7 F9</font> 20<font 20face: 3D" B1 BC B8 B2" 20size: 3D>
BF C0 B7 F9 20'800a0009'</font> 0A<p>- 0A<font 20face: 3D" B1 BC B8 B2" 20size: 3D> C3-B7-C0-DA 20-BB-E7-BF-E8-C0-CC 20-C0-DE
-BB-F8-B5-C7-BE-FA-BD-C0-B4-CF-B4-D9.: 20'Inumber: 2001'</font> 0A<p>- 0A<font 20face: 3D" B1 BC B8 B2" 20size: 3D>index.htm
</font><font 20face: 3D" B1 BC B8 B2" 20size: 3D>, 20-C1-D9-2023</font>-20

```

Auszug aus den Service Probes des Internetzensus: Die durchdachte Struktur der Datensätze ermöglicht eine zielgenaue Auswahl und Untersuchung (Abb. 2).

dass eine vollständige Dekompression des Datensatzes erfolgen muss.

Die Rohdaten der Scans liegen als Textdateien vor, in denen zeilenweise mit Tabulatoren getrennt im Klartext die ge-scannte IP-Adresse und der Timestamp des Scans gespeichert sind. Je nach Art des Scans folgen die Resultate auf die IP-Adresse und den Timestamp in unterschiedlicher Form. Bei den Service Probes folgt ein Indikator für den Zustand des Ports und ein Teil der vom getesteten Ziel zurückgegebenen Antwort. Das heißt bei einem HTTP-GET-Request ist ein Teil der HTTP-Response des Ziels im Datensatz hinterlegt (Abbildung 2).

Zum Entpacken des Datensatzes kommt das Kompressionstool ZPAQ zum Einsatz. Es ist für Windows sowie für Linux-Plattformen als Open Source verfügbar und in den Repositories der am meisten verbreiteten Linux-Distributionen bereits vorhanden. Es empfiehlt sich allerdings der Einsatz der jeweils neuesten Version, in den Repositories befinden sich häufig veraltete Werkzeuge.

Zum Entpacken gibt man über die Kommandozeile den Befehl `zpaq x Archiv.zpaq [-threads n]` ein. Die Dauer des Vorgangs ermittelte das Linux-Kommandozeilentool `time`: Es ergab sich für die Dekompression mit Version 6.41 ei-

ne Dauer von etwa 163 Minuten bei einer Verteilung auf vier Threads.

Da es sich bei den Datensätzen um Textdateien handelt, kann die Verarbeitung der entpackten Scandaten durch Skripte automatisiert erfolgen. Zu diesem Zweck bietet sich eine dreistufige Verarbeitungskette an, bestehend aus den Teilschritten Sammeln, Bereinigen und Auswerten. Im ersten Teilschritt durchsucht das entsprechende Skript die Dateien des Internetzensus zeilenweise auf das Vorkommen eines bestimmten Strings. Findet es ihn, speichert es die zu diesem Datensatz gehörige IP-Adresse. Eine Bereinigung der Daten im Anschluss an diese Suche ist notwendig, da jeder Scan mehrfach durchgeführt wird und IP-Adressen daher doppelt in den Ergebnissen auftauchen können. Abschließend kann man anhand dieser Daten Auswertungen durchführen.

Auf der Suche nach „SAP“

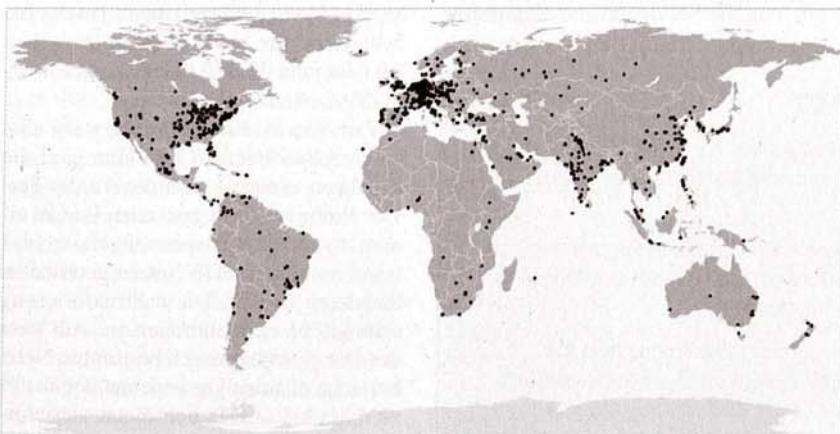
Im Rahmen dieses Artikels haben die Autoren beispielhaft die Datensätze der Service Probes auf SAP-Serverinstallationen untersucht. Zum Einsatz kam eine Sammlung von Skripten, die der vorgeschlagenen Verarbeitungskette folgen. Zunächst durchsuchten sie rekursiv aufsteigend von einem angegebenen Ordner

jede Datei zeilenweise auf das Vorkommen des Suchstrings „SAP“. Nachdem die Skripte alle IP-Adressen, deren Antwort das Pattern „SAP“ beinhaltet, identifiziert und bereinigt hatten, wurden die Adressen mit der Lite-Version der Geo-IP-Datenbank der Firma MaxMind [c] lokalisiert und mit dem World map tool der Nagoya University Graduate School of Law auf einer Weltkarte eingetragen [d].

Abbildung 3 zeigt sämtliche gefundene SAP-Serverdienste weltweit. Zusätzlich ermittelten die Skripte die Häufigkeit der einzelnen Serverversionen. Abbildung 4 zeigt einen Auszug aus der Auswertung der gefundenen Service-Versio-nen. Er enthält die zehn am häufigsten entdeckten Serverflags mit der relativen Häufigkeit ihres Vorkommens abhängig vom untersuchten Port. In diesem Rah-men haben die Autoren die sechs gän-gigsten HTTP-Ports sowie HTTPS-Port 443 untersucht. Auf der Testhardware dauerte das Durchsuchen aller HTTP-GET-Requests über TCP auf Port 80 nach dem Stichwort SAP insgesamt etwa 11 Minuten. Diese Dauer ist allerdings stark abhängig von der Anzahl der Suchergebnisse. Dieselbe Suche nach Versionen des Apache Webservers auf Port 80 dauerte etwa 2 Stunden. Die zu diesem Zweck eingesetzten Skripte befinden sich auf Github [e].

Wie man sieht, kann der Datensatz sehr einfach dazu verwendet werden, bestimmte Softwareversionen im Internet zu suchen und deren geografische Verteilung herauszufinden. Natürlich handelt es sich dabei lediglich um eine momentane Be-standsaufnahme und der Datensatz ist im Grunde bereits veraltet. Es ist wenig wahr-scheinlich und vermutlich auch nicht er-strebenswert, dass jemand regelmäßig in große Mengen von Rechnern eindringt, um das Internet zu scannen. Doch man kann das Internet auch selbst durchsuchen.

Forscher der University of Michigan haben kürzlich auf dem Usenix Security Symposium den Portscanner ZMap vor-gestellt [f], der gezielt dafür gebaut wurde, sehr schnell große Netzwerke nach offenen Ports zu scannen. Die Forscher



Anhand der IP-Adressen lässt sich die weltweite Verteilung spezieller Dienste ermitteln, im vorliegenden Beispiel der SAP-Serverdienste (Abb. 3).

Liste von Serverflags

	80	443	8000	8001	8008	8080	8081
SAP NetWeaver Application Server / ABAP 702	3,9923%	0,2974%	17,4230%	10,8541%	3,3333%	10,2041%	7,7778%
SAP Web Application Server	2,7688%	43,5455%	1,8442%	4,6263%	5,5556%	6,1224%	1,1111%
SAP J2EE Engine/7.00	12,6529%	0,6544%	8,2019%	10,3203%	4,4444%	13,4694%	2,2222%
SAP NetWeaver Application Server 7.20 / ICM 7.20	21,9897%	0,1785%	1,8927%	1,4235%	2,2222%	8,5714%	4,4444%
SAP J2EE Engine/7.01	8,5319%	0,3569%	9,6336%	7,6512%	6,6667%	6,1224%	3,3333%
SAP NetWeaver Application Server / ABAP 701	3,0908%	0,2380%	12,7396%	16,1922%	6,6667%	4,0816%	2,2222%
SAP NetWeaver Application Server (ICM)	5,4411%	28,5544%	1,4550%	1,6014%	0,0000%	5,7143%	2,2222%
SAP Web Application Server [1.0;700]	2,3181%	0,1190%	13,5889%	11,7438%	8,8889%	6,5306%	4,4444%
SAP Web Application Server [1.0;701]	1,3522%	0,1785%	7,6680%	10,4982%	55,5556%	2,4490%	3,3333%
SAP Web Application Server (ICM)	9,7875%	7,0791%	0,2427%	1,0676%	1,1111%	8,5714%	4,4444%

Diese zehn SAP-Serverversionen sind momentan am meisten verbreitet (Abb. 4).

sind damit in der Lage, über eine 1-Giga-bit/s-Leitung in nur 45 Minuten einen bestimmten Port im gesamten IPv4-Bereich zu scannen.

ZMap erreicht diese atemberaubende Performance durch einige Designentscheidungen, die ihn grundsätzlich von anderen Portscannern unterscheiden. Beispielsweise scannt er die IP-Adressen nicht fortlaufend, sondern wählt die Reihenfolge der Adressen so, dass möglichst keine Pfade auf dem Weg zu den Zielsystemen überlastet werden. Eine weitere Eigenart ist, dass ZMap die Pakete über Raw-Sockets aussendet und lokal nicht den Status der einzelnen Verbindungen hält. Es gibt einen Thread, der die Pakete versendet, und einen zweiten, der die Antwortpakete empfängt. Beide kommunizieren kaum, sodass der sendende Thread beispielsweise nicht „weiß“, ob ein Antwortpaket hereinkam oder nicht. ZMap kennt daher auch keine Timeouts und wiederholt folglich keine Messungen. Überraschenderweise schätzen die ZMap-Autoren, dass ihr Scanner trotzdem 98 % der offenen Ports findet und zwar selbst dann, wenn er mit maximaler Geschwindigkeit scannt. Unter dem Strich ist ZMap um das 1300-Fache schneller als Nmap in der schnellsten Konfiguration.

ZMaps Autoren sind sich der Brisanz ihres Werks bewusst. Der Scanner bietet einerseits viele Forschungsmöglichkeiten, zum Beispiel Sicherheitsexperten und IT-Fachleuten einen Überblick über große Netzwerke und deren Verfügbarkeit zu verschaffen, die Verteilung neuer Protokolle im Internet zu beobachten oder

eben auch, viele anfällige Dienste zu finden – was andererseits in den falschen Händen missbraucht werden kann. Wie geht man mit diesen Daten verantwortungsvoll um?

Es ist nicht realistisch, jeden Betreiber hinter einer IP-Adresse um Erlaubnis fragen zu wollen, ob man diese scannen darf. Für die andere Seite gibt es auch noch keine automatisierte Möglichkeit, mitzuteilen, dass man nicht gescannt werden möchte, wie es die *robots.txt*-Datei im Web erlaubt. Über diese Datei kann man Web-Crawlers anweisen, welche Teile indexiert werden sollen und welche nicht. Als Nutzer von Werkzeugen wie ZMap sollte man trotzdem mindestens die Möglichkeit bieten, dass Betroffene herausfinden können, wofür die Scans durchgeführt werden, und wie sie künftige Scans verhindern können. Das kann man über eine Standard-Webseite mitteilen, die auf der gleichen IP-Adresse läuft wie der Scanner.

Vorbereitungen für den ZMap-Einsatz

Weiterhin muss man sicherstellen, dass die eigene Infrastruktur die Scans aushält. Das bedeutet, die Benutzer sollten die lokalen Netzwerkadministratoren in die Planung einbeziehen und sie über die Zeitpunkte der Scans informieren. Überdies sollte man sich auf ein erhöhtes E-Mail-Aufkommen der abuse@-E-Mail-Adressen einstellen. Die ZMap-Autoren wurden im Laufe ihrer Scans 145-mal kontaktiert, wobei die meisten Schreiber

um Aufklärung bat. 15 Antworten waren feindselig, das heißt drohten mit Anzeigen oder Denial-of-Service-Gegenschlägen.

Eine „Warnung“ an dieser Stelle: Niemand sollte sich darauf verlassen, dass Cyberkriminelle sich an den ethischen Richtlinien der ZMap-Autoren orientieren. Der Scanner ist frei verfügbar und Angreifer werden ihn für ihre Zwecke anpassen und verwenden.

Fazit

Die Zeiten, in denen Update-faule Administratoren deshalb davongekommen sind, weil kein Angreifer ihre anfälligen Dienste gefunden hat, sind vorbei. Der Datensatz erlaubt es, offline nach anfälligen Diensten zu suchen, die 2012 im Internet standen. Daraus lässt sich leicht eine Liste von IPs erstellen, die der Angreifer dann nochmals auf Aktualität prüfen kann. Darauf hinaus ist man mit dem ZMap-Scanner erstmals in der Lage, in wenigen Minuten den gesamten IPv4-Adressraum nach bestimmten offenen Ports zu scannen. Damit sind Cyberkriminelle in der Lage, sich ein stundenaktuelles Abbild möglicher Angriffsziele zu verschaffen.

Man könnte diese Erkenntnisse als weitere Motivation dafür nehmen, endlich IPv6 großflächig auszurollen. Schließlich ist der IPv6-Adressraum mit 2^{128} wesentlich größer und kann nicht mehr vollständig durchsucht werden. Doch auch wenn der Wechsel zu IPv6 jetzt zügig stattfindet, die Anzahl der tatsächlich benutzten IP-Adressen wird wohl auch weiterhin gleichmäßig steigen, genauso wie die Rechnerressourcen und die verfügbare Netzwerkbandbreite. Man sollte sich also nicht darauf verlassen, dass Forscher nicht doch noch eine pfiffige Idee haben werden, wie man eine Liste der verwendeten IPv6-Adressen erstellt. Sichere Softwareentwicklung und zeitnahe Ausrollen von Updates und Patches sind auch weiterhin der einzige Weg, eine IT-Infrastruktur abzusichern.

(ur)

Onlinequellen

- [a] Internetzensus 2012 internetcensus2012.bitbucket.org/paper.html
- [b] Weboberfläche zum automatisierten Suchen www.exfiltrated.com/querystart.php
- [c] MaxMind GeoLite City Database geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz
- [d] Nagoya University Graduate School of Law World Map Tool law.nagoya-u.ac.jp/en/appendix/software/worldmap
- [e] Sammlung der Analyseskripte <https://github.com/MThuene/seminarcensus>
- [f] ZMap zmap.io

Sebastian Schinzel

ist Professor für IT-Sicherheit an der FH Münster.

Maximilian Thünemann

studiert Informationstechnik an der FH Münster.



iOS 7: Was die neue Version für Entwickler bedeutet



Facelift

Markus Weyerhäuser

iOS 7 kommt in runderneuertem Design daher. Tiefe, Struktur und Dynamik charakterisieren das neue Look & Feel. Ein Blick hinter die Kulissen zeigt die Techniken, auf denen das neue Design fußt.

Apple hat die siebte Version seines Mobil-Betriebssystems fertiggestellt; mit der finalen Version ist am 18. September zu rechnen. Drei wesentliche Prinzipien bilden die Grundlage des neuen Designs: Klarheit (clarity), Rücksicht auf die Nutzer (deference) und Tiefe (depth). Klarheit heißt, die wichtigen Dinge hervorzuheben beziehungsweise selbsterklärende Funktionen zu fordern. Dadurch ergeben sich eindeutige

Richtlinien, die das UI zusammen und konsistent halten (siehe Apples „iOS 7 UI Transition Guide“ und die „iOS Human Interface Guidelines“ in „Alle Links“).

Vorrang für Tiefe und Dynamik

Rücksicht lässt übermäßige Ornamentierung nicht den Blick auf das Wesentliche verstellen. Beispiele für die An-

lehnung von Software an Alltagsgegenstände (Skeuomorphismus) wie beim Adressbuch oder der Notizen-App findet man in iOS 7 nur noch subtil.

Ziel des neuen Designs ist vor allem, Tiefe und Dynamik zu zeigen. Der Blick auf das Hintergrundbild durch Hin- und Herbewegen der Icons, Unschärfe und Transparenz sowie ausgefeilte Animationen ersetzen die aus iOS 6 bekannten Farbverläufe, Schatten und Schnittlinien. Leisten (Status Bar, Navigation Bar, Tab Bar) sind nun standardmäßig durchsichtig, wodurch der Inhalt durchscheint. Buttons reduzieren sich auf ein Minimum inklusive eines Verzichts auf den äußeren Rahmen. Statt Icons hebt farblich anders gestalteter Text klickbare Objekte ab. Um die neuen visuellen Effekte zu ermöglichen, hat Apple iOS 7 mit mehr als 100 neuen Klassen ausgestattet. Insbesondere das neue Text-Kit-Framework und etliche Erweiterungen und Verbesserungen im UIKit

ermöglichen die Effekte und das dynamische Verhalten der Objekte.

Dynamik in einer Benutzeroberfläche nachzubilden ermöglicht die Annäherung der Benutzerführung an die reale Welt. Dadurch fühlt sich eine Interaktion „echt“ an, und die Anwendung ist intuitiver und leichter benutzbar. Das erfordert die Simulation wesentlicher physikalischer Eigenschaften. Hierzu gehören beispielsweise Schwerkraft, Kollisionen, Elastizität, Massen und Partikelsysteme. Zur Simulation der physikalischen Eigenschaften von Objekten verwendet Apple in iOS 7 eine neu entwickelte Physik-Engine. Über sie legen Entwickler Gesetzmäßigkeiten und Regeln zur Interaktion zwischen Objekten fest.

Die grundlegenden Klassen der Physik-Engine liefert das UIKit-Framework mit. Klassen, die das *UIDynamicItem*-Protokoll unterstützen, bezeichnet man als „dynamische Elemente“. Sie beschreiben die Eigenschaften, die UIKit zur Animation des Elements benötigt. Damit man die Physik-Engine nutzen kann, muss dies Protokoll implementiert sein. Ab iOS 7 gehört auch die zentrale *UIView*-Klasse zu den „dynamischen Elementen“ und damit jede von ihr abgeleitete. Die meisten Controls lassen sich dadurch in die Physik-Engine einbinden.

Von Haus aus liefert Apple unterschiedliche dynamische Verhaltensweisen mit. Beispielsweise kann ein Entwickler über das *UIAttachmentBehavior*-Objekt eine Verbindung zwischen zwei dynamischen Elementen herstellen. Bewegt sich eins, so bewegt sich das zugeordnete andere mit. Die Verbindung ist nicht vollkommen statisch. Durch Spezifizieren des Dämpfungs- und Schwingungsverhaltens der Verbindung lassen sich sehenswerte Effekte erzeugen. Über das *UICollisionBehavior*-Objekt können Entwickler Kollisionen verschiedener dynamischer Elemente abbilden. Ein

UIGravityBehavior-Objekt definiert einen Gravitationsvektor für verschiedene dynamische Elemente, mit dem sie sich in eine Richtung und mit einer definierten Beschleunigung bewegen lassen.

Graue Eminenz im Hintergrund ist der *UIDynamicAnimator*, der die Schnittstelle zur Physik-Engine und den zu animierenden Objekt bildet. Ein einziges dynamisches Element kann mehrere Verhaltensweisen besitzen, jedoch muss das selbe *UIDynamicAnimator*-Objekt sie alle koordinieren.

Wer dynamische Effekte in eigenen Apps verwenden will, konfiguriert zunächst eine oder mehrere dynamische Verhaltensweisen wie ein *UIAttachmentBehavior*. Anschließend ordnet er dynamische Elemente – beispielsweise eine *UIView* – diesen dynamischen Verhaltensweisen und diese danach einem *UIDynamicAnimator*-Objekt zu.

Texte leichter und flexibler layouten

Um vorgefertigte Inhalte mit einem bestehenden Layout darzustellen, bietet sich *UIWebView* an. Will man den dargestellten Inhalt manipulieren, um beispielsweise einige Textstellen herauszuheben oder aber eine Grafik einzufügen, die den Text umfließt, ist dies mit bisherigen iOS-Boardmitteln nur aufwendig realisierbar. Version 7 vereinfacht die Manipulation von Text und Typografie mit dem neuen Text-Kit-Framework,

eine Text und Layout Rendering Engine, die auf Core Text aufsetzt. Das neue Framework ist komplementär zu WebKit zu sehen; sein Einsatz empfiehlt sich immer, wenn man Texte über Programmcode manipulieren oder Texte in anderen Controls wie einer *UIScrollView* einbetten will.

Damit lässt sich beispielsweise ein Textblock leicht in Absätze, Spalten und Seiten formatieren. Text kann um beliebige Regionen wie Grafiken herumfließen. Die typografische Darstellung wie Kerning (überlappende Zeichen) und Ligaturen (Zusammenfassung verschiedener Zeichen) beherrscht Text Kit ebenso wie die Darstellung komplexer Schriftarten. Alle textbasierten UIKit-Controls verwenden Text Kit. So hat Apple beispielsweise *UITextView*, *UITextField* und *UILabel* neu implementiert. Damit verfügen sie über erweiterte Fähigkeiten, beispielsweise die Darstellung von Kerning und Ligaturen. iOS 7 erlaubt außerdem den direkten Zugriff auf den Textspeicher. Neben einigen neuen Klassen wie *NSTextStorage* und *NSTextContainer* sind bestehende wie *NSAttributedString* erweitert, um neue Attribute zu unterstützen.

Mit iOS 7 hat Apple semantische Beschreibungen für die Verwendungen von Schriften eingeführt. Unterschiedlichen Verwendungsarten sind Konstanten zugeordnet wie *UIFontTextStyleHeadline1*, *UIFontTextStyleBody* oder *UIFontTextStyleSubheadline1*. Sie stellt auch Xcode 5, Apples

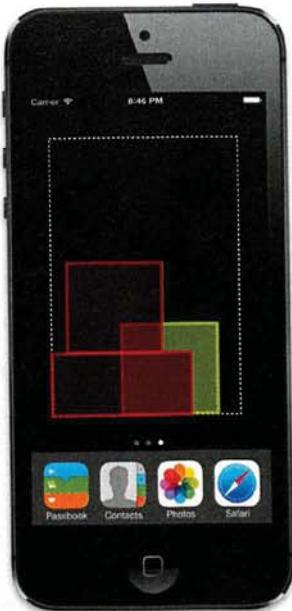
Objekten lassen sich mehrere Verhaltensweisen zuordnen: Rote Views kollidieren mit roten – aber nicht mit den grünen. Mit der Begrenzung jedoch kollidieren alle Views (Abb. 1).

Entwicklungsumgebung, zur Verfügung. Welche Schriftart zur Laufzeit tatsächlich verwendet wird, hängt von einer Reihe von Faktoren ab. Beispielsweise kann der Benutzer die Größe in den Systemeinstellungen vorgeben, sodass iOS 7 alle Oberflächen, die die neuen Konstanten verwenden, entsprechend anpasst. Dieser dynamische Mechanismus verbessert die Lesbarkeit – setzt aber voraus, dass die Benutzeroberfläche mit wechselnden Schriftgrößen umgehen kann. Die Verwendung von Auto Layout bietet sich hier zwingend an.

Sprite Kit verleiht ein bisschen Flügel

Das Sprite-Kit-Framework bietet ein hardwarebeschleunigtes Animationssystem, optimiert für Erstellen von Spielen in 2D und 2,5D (simulierte 3D). Das Framework nutzt die oben erwähnte Physik-Engine. Sprite Kit stellt eine Basisinfrastruktur zur Verfügung, die für die gängigen Spieleanforderungen ausreichend sein dürfte und die Bereiche Grafik-Rendering, Animationen und Ton-Wiedergabe einschließt. Innerhalb von Sprite Kit sind vor allem GPU-nahe Algorithmen implementiert. Das setzt zum einen Spezialwissen voraus und kostet zum anderen viel Entwicklungszeit. Über beides verfügen Spieleentwickler in der Regel nicht. Die Integration mit den unterschiedlichen Bewegungssensoren von iPhone und iPad dürfte jedoch die Akzeptanz bei Spieleentwicklern erhöhen.

Das Kit kann Sprites darstellen, Objekte animieren und physikalische Effekte berech-



nen. Eine auf dem Sprite Kit aufbauende App ist in Szenen organisiert, denen texturierte Objekte, Videos, pfadbasierte Formen, Core Image Filter und andere Spezialeffekte angehören können. Einzelne Objekte lassen sich über explizite Aktionen animieren. Alternativ können Entwickler Animationen über die Physik-Engine steuern. Physikalisches Verhalten wie Schwerkraft und Anziehungskraft lässt sich dadurch simulieren.

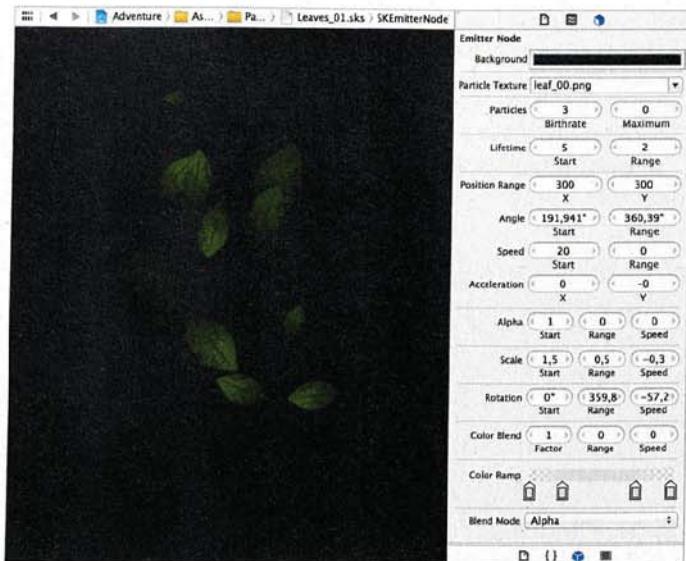
Xcode 5 verfügt über einen neuen integrierten Editor zum Erstellen und Simulieren von Partikeleffekten. Über einen Partikelemitter kann man bestimmte Punkte eines View ansprechen und bewegte Bilder erzeugen – beispielsweise Regen-, Schnee- und Feuereffekte. Mehrere Texturen lassen sich in einem großen Bild (einem Atlas) zusammenfassen. Das verbessert die Zugriffsgeschwindigkeit bei der Darstellung zur Laufzeit. Das Erstellen und Verwalten eines solchen Atlas erfolgt ebenfalls in Xcode 5.

Multitasking mit Mobilitätshürden

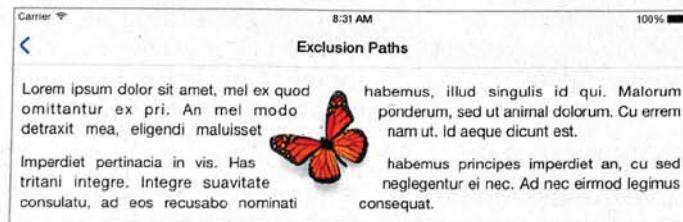
Wegen der begrenzten Batterielaufzeit eines mobilen Geräts wird die Ausführung von

TRACT

- Apple hat sein Mobil-Betriebssystem iOS einer General-Überholung unterzogen und in Version 7 vieles von Grund auf neu aufgebaut.
- Beispielsweise dient die neu entwickelte Physik-Engine dazu, Gesetzmäßigkeiten und Regeln aus der Welt zur Interaktion zwischen Objekten festzulegen.
- Die IDE Xcode, die jetzt als Version 5 vorliegt, hat Apple samt dem Interface Builder eher unauffällig überarbeitet.



Der in Xcode 5 integrierte Partikelemitter-Editor erlaubt die Modifikation wichtiger Parameter und deren Live-Preview direkt aus der Entwicklungsumgebung heraus (Abb. 2).



Das neue iOS 7-Text-Kit-Framework ist eine leistungsfähige Text Rendering Engine, die komplexe Layout-Vorgaben flexibel umsetzen kann (Abb. 3).

Apps im Hintergrund zum Balanceakt. In den ersten iOS-Versionen durften nur Apples eigene Apps im Hintergrund laufen. Später erlaubte der Hersteller Apps von Drittanbietern, gewisse Dinge im Hintergrund auszuführen. iOS 7 unterstützt zwei weitere Modi.

Apps, die in regelmäßigen Abständen neue Inhalte laden, kann das System jeweils wecken, sodass sie Inhalte unbedeutend laden. Davon profitieren Apps für soziale Netze, Nachrichten oder E-Mail. Dem Benutzer stehen beim Start der Anwendung die neuen Inhalte gleich zur Verfügung. Um den optimalen Zeitpunkt für das Wecken der App zu ermitteln, beobachtet iOS das Nutzerverhalten und zieht andere Rahmenbedingungen ebenfalls mit in Betracht – et-

wa ob das Gerät beispielsweise schon aktiv oder die Netzverbindung gerade gut ist. Apps, die Push-Benachrichtigungen verwenden, um den Benutzer über die Verfügbarkeit neuer Inhalte zu informieren, können auf eine solche Meldung hin Download-Vorgänge im Hintergrund einleiten. Und zwar bevor die Nachricht an den Benutzer gesendet wird. Die `NSURLSession`-Klasse vereinfacht das Herunterladen von Inhalten im Hintergrund deutlich. Sie stellt eine einfache, Task-basierte Schnittstelle für die Abarbeitung mehrerer `NSURLRequest`-Objekte zur Verfügung.

AirDrop ermöglicht Fotos, Dokumenten, URLs und anderen Daten mit in der Nähe befindlichen Geräten zu teilen. Seit iOS 7 gibt es dafür eine Erweiterung der `UIActivity`-

`ViewController`-Klasse. Mit Xcode lassen sich außerdem die unterstützten Dokumenttypen einer App spezifizieren. Daran erkennt das System zur Laufzeit, welche Dokumenttypen die App verarbeiten kann. Empfängt das System eine neue Datei, ruft es eine passende Methode im `Application Delegate`-Objekt auf. Empfangene Files speichert es verschlüsselt in einem Unterordner des Heimatverzeichnisses (`Home/Documents/Inbox`). Die App kann darauf nur schreibend oder löschen zugreifen. Zum Modifizieren der Datei muss man daher das Gerät entsperrt und die Datei in ein anderes Verzeichnis verschoben haben.

Eine weitere flexiblere Art, Geräte in der unmittelbaren Nähe aufzufinden, ist Aufgabe des Multipeer-Connectivity-Framework. Die direkte Kommunikation (WLAN, Peer-to-Peer und Bluetooth) zwischen ihnen funktioniert ohne eine Internet-Verbindung. Über das neu in iOS 7 bereitgestellte Framework lassen sich Multipeer-Sitzungen einfach erstellen und Daten in Echtzeit mit benachbarten Geräten austauschen. Das iOS 7-SDK bietet eine programmatische und eine UI-basierte Option zum Auffinden und zur Verwaltung von Netzdiensten. Die Klasse `MCBrowserViewController` lässt sich in die Benutzeroberfläche der eigenen App integrieren, und das User Interface zeigt Geräte in der Nähe des Benutzers an. Apps können Einladungen zu einer Sitzung verschicken und akzeptieren. Alternativ können sie über die Klasse `MCNearbyServiceBrowser` nach Services suchen, die in der Nähe befindliche Geräte anbieten. Diese Klasse bringt zwar kein eigenes UI mit, dafür kann man nach Servicetyp filtern.

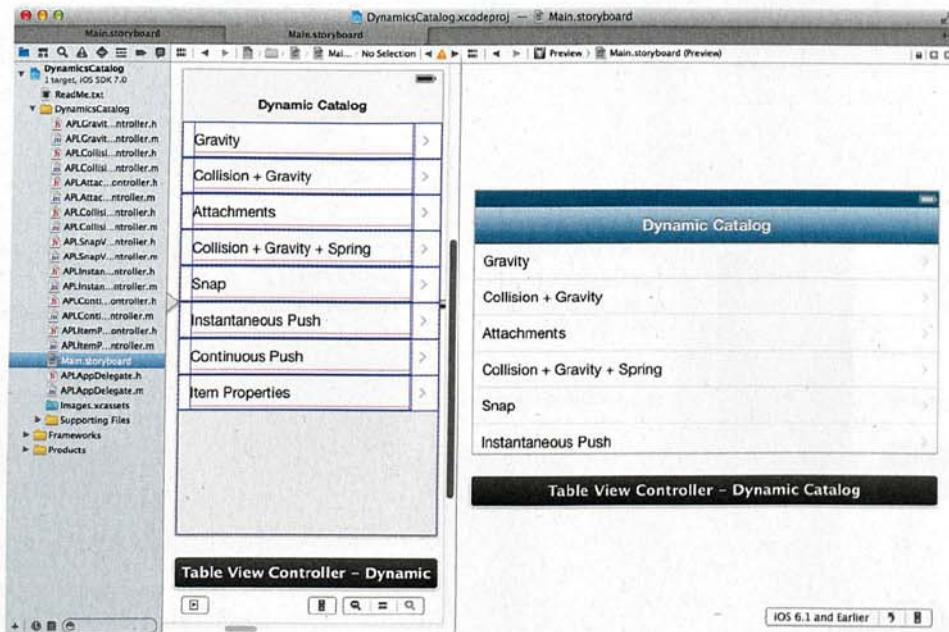
Mit iOS 7 kennt das Audio-Unit-Framework eine Inter-App-Audiofunktionalität, was dem Austausch von MIDI-Befehlen und Audio-Streams zwischen Anwendungen auf demselben Gerät dient. Da-

durch kann der Anwender beispielsweise Musik in einer App aufnehmen und an eine andere App zur Weiterbearbeitung senden. Damit unabhängig voneinander entwickelte Apps sich zur Laufzeit finden und austauschen können, hat Apple einen Discovery-Mechanismus entwickelt. Um Audiodaten der eigenen App anderen zur Verfügung zu stellen, muss die Software eine `AURemoteIO`-Audio-Komponente publizieren, die für andere Prozesse sichtbar ist, sodass sie auf die Daten zugreifen können.

Da die bisherige Implementierung von Core Data in Zusammenhang mit iCloud schlichtweg als unbrauchbar galt, gelobte Apple Besserung. So konzentrierte sich die Firma mit iOS 7 auf Zuverlässigkeit und Qualität bestehender APIs und stellte neue Funktionen hintan. Eine Tonne von Bugs habe man gefixt, so Andreas Wenter, Apples Senior Director für OS X Platform Experience. Ein Schritt in die richtige Richtung ist zunächst die Unterstützung von iCloud Debugging in Xcode 5. Außerdem hat der iOS-Simulator nun Zugriff auf in iCloud gespeicherte Daten.

Xcode 5: An der Oberfläche gekratzt

Xcode 5 präsentiert sich ebenfalls mit einer aufgeräumteren Benutzeroberfläche. Im Vergleich zu iOS 7 fallen die Änderungen allerdings eher marginal aus. So ist die Toolbar beispielsweise jetzt etwas schmäler gestaltet. Dies lässt insbesondere auf kleineren Monitoren mehr Platz für Wichtiges. Die Controls sind prägnanter und deutlicher zu erkennen. Das Dialogfeld für „Open Quickly“ ist überarbeitet und nun einfacher zu bedienen. Unter der Haube hat Apple einen stärkeren Matching-Algorithmus implementiert, der Ergebnisse schneller und mit mehr Inhalt zurück liefert. Über den runderneuerten



Über eine Preview-Funktion lässt sich das in Bearbeitung befindliche UI im Interface Builder in verschiedenen Ausrichtungen und iOS-Versionen darstellen (Abb. 4).

Such-Navigator sind alle Optionen und Einstellungen auf einen Blick ersichtlich. Durch direktes Anklicken der Suchoptionen können Entwickler verschiedene Eingrenzungen wie den Suchbereich verschiedener Projektordner einstellen. Die Ergebnisse fließen nun in die nächsten Zeilen, sodass mehr Informationen schnell erkennbar sind.

Interface Builder in Xcode 5 unterstützt das Erstellen neuer Interface-Objekte in iOS 7, und der Auto-Layout-Editor bietet deutlich mehr Flexibilität beim Gestalten der Benutzeroberfläche. Viele der aus früheren Versionen bekannten Kinderkrankheiten sind behoben. Objekte müssen nicht mehr zwingend über Constraints verfügen. Interface Builder fügt sie nicht mehr automatisch hinzu. Neue Constraints können Entwickler über Control-and-Drag anlegen. So lässt sich beispielsweise schnell ein Constraint von einem Button zu seiner Super View einfügen. Der Interface Builder kann durch Markieren aller Objekte automatisch alle fehlenden Constraints ergänzen beziehungsweise komplett neu anlegen. Die Analyse potenzieller Feh-

lersituationen hat Apple ebenfalls verbessert.

Der Assistenzeditor stellt Benutzeroberflächen im iOS 6 und iOS 7 Look & Feel dar. Der Haupteditor kann dabei eine andere iOS-Version präsentieren als der Assistenzeditor. Dies vereinfacht die Entwicklung von Versionen für iOS 6 und 7 deutlich. Wer nur für eine Version etwas erstellen will, kann in den beiden Editoren Portrait- und Landscape Mode parallel darstellen.

Ein neuer Asset-Katalog verwaltet Bilder und Symbole in verschiedenen Auflösungen. Dort lassen sich zentral grafische Elemente für verschiedene Plattformen, Geräte und Skalierungsfaktoren speichern. Der Katalog zeigt die je nach Plattform benötigten Bilder. Dazu gehören die Launch Images und App Icons. Diese mussten Entwickler bisher umständlich über Namenskonventionen manuell ablegen, sodass die unterschiedlichen Geräte und Bildschirmauflösungen ersichtlich waren. Statt Namenskonventionen hat Apple die Klasse *UIImage* erweitert, sodass der direkte Zugriff auf den Asset-Katalog möglich ist. Mit Xcode 5 kann man sich damit im Wesentlichen auf das

Erstellen der Grafiken konzentrieren.

Ein ebenfalls nützliches Werkzeug ist ein neuer Editor zum Teilen und Schneiden von Grafiken, die zur Laufzeit ihre Größe anpassen sollen. Beispielsweise ein mit einem Hintergrundbild belegter Button, dessen Größe sich horizontal verändern kann. Xcode 5 erleidet die Aufteilung des Hintergrundbildes für den erwähnten Button auf Wunsch sogar automatisch.

Immer besser: Manuell war gestern

Eine App nach der Entwicklung im AppStore zur Verfügung zu stellen, bedurfte bisher einiger zeitraubender Nacharbeiten. Mit Unterstützung einer automatischen Konfiguration hat Apple einen Teil des Aufwands reduziert. Apple-IDs des Developer-Programms, Source Code Repositories und Integrationsserver können Entwickler nun direkt aus Xcode heraus zentral verwalten. Ein Provisioning Profile kann Xcode 5 direkt aus den angegebenen Informationen wie Signing Identity und Capabilities erzeugen beziehungsweise unterstützt beim Auffinden fehlerhafter Konfigurationen. OS X Server bringt einen neuen Dienst mit, sodass dieser als Build und kontinuierlicher Integrationsserver genutzt werden kann. Plattformspezifische Fähigkeiten, wie iCloud, Game Center, Passcode und Karten sind bequem über eine Projekteinstellung in Xcode zu konfigurieren.

Zum Erhöhen der Softwarequalität kommen kontinuierliche Integrationsprozesse immer häufiger zum Einsatz. Bisher mussten sich Objective-C-Entwickler aus unterschiedlichen Open-Source-Werkzeugen ihren eigenen Integrationsserver und Prozess bauen. Xcode 5 unterstützt den neuen Xcode-Service von OS X Server 10.9, um einen Integrationsserver standardmäßig zur Verfügung zu stellen. Der Dienst automatisiert das Ausführen von Integrationsprozessen zum Bau, zur Analyse, zum Testen und zur Archivierung der App. Was genau dieser Integrationsprozess tun soll, definiert man innerhalb von Xcode in der lokalen Entwicklerumgebung. Die Ausführung sogenannter Bots erfolgt in der Regel auf einem dedizierten Integrationsserver. Sie lassen sich beispielsweise so bauen, dass jeweils nach einem erfolgreichen Commit auf dem Git-Repository des Servers ein Integrationslauf startet. In größeren Entwicklergruppen dürfte man stattdessen auf feste Intervalle zurückgreifen. So lässt sich schnell erkennen, warum ein Build-Prozess oder eine Reihe von Tests nicht erfolgreich durchliefen. Die Ergebnisse eines Bot-Laufs kann Xcode 5 anzeigen und analysieren.

Fester Bestandteil von Xcode 5 ist ein neuer Navigator, der einen Überblick über alle Tests im aktuellen Workspace bietet. Über ihn können Entwickler neue Targets und Klassen hinzufügen; außerdem können sie einzelne Tests oder ganze Sammlungen ausführen. Und über neue Käte-

Verstrickt?

Wir schaffen Durchblick.

gorien (Test Callers und Classes) können sie außerdem Source Code und Tests Seite an Seite im Haupt- und im Assistant-Editor anzeigen.

Fazit

Obwohl das neue Look & Feel es vermuten lässt: Ein radikal neues System ist iOS 7 nicht. Vielmehr hat Apple wie üblich ein evolutionär weiterentwickeltes System geliefert. Alte Zöpfe hat der Hersteller trotzdem abgeschnitten. So ist die Umstellung auf die LLVM-Technik abgeschlossen, und der GNU-Compiler/Debugger ausgemustert.

Abgesehen von gänzlich neuen Funktionen haben sich Konzepte und APIs verändert. Je nach Anwendungstyp und Komplexität bringt das Änderungsaufwand mit sich. Bestehende Anwendungen lassen sich mit Xcode 5 in iOS 7 transformieren. Sie unterstützen auf Knopfdruck das neue Look & Feel. Nicht bei allen Apps dürfte das reichen. Je nachdem wie tief Programmierer in die Trickkiste gegriffen haben, ist der Umstellungsaufwand höher. Dies gilt vor allem für die Benutzeroberfläche und Gestaltung der App. (hb)

Markus Weyerhäuser

ist IT-Berater und Autor. Seine Beratungsschwerpunkte liegen in der Konzeption und Realisierung von (mobilen) Unternehmensanwendungen sowie der Planung und Durchführung komplexer IT-Transformationsprojekte.

Literatur

- [1] Markus Weyerhäuser; iOS-Entwicklung; Werkzeug-Update; Erfahrungen mit Auto Layout und Social-Media-Framework; iX 5/2013, S. 104

Alle Links: www.iz.de/ix1310114



Wann lohnt sich ein Server statt NAS? Welche Server-Software brauche ich wirklich?
Warum Virtualisierung und welche?

Antworten auf diese und noch mehr Fragen gibt Ihnen die neue c't-Sonderausgabe Netzwerke. Das 172 Seiten umfassende Kompendium versorgt Sie mit inhaltlichen und rechtlichen Grundlagen, vermittelt aktuelles Praxiswissen und gibt nützliche Kauftipps für Ihr Heim oder Büro.

» Inklusive c't Netzwerkzeugkasten als Download-Paket
mit 57 Tools zur Diagnose und Reparatur

Gleich mitbestellen und
mehr als 10 % sparen!

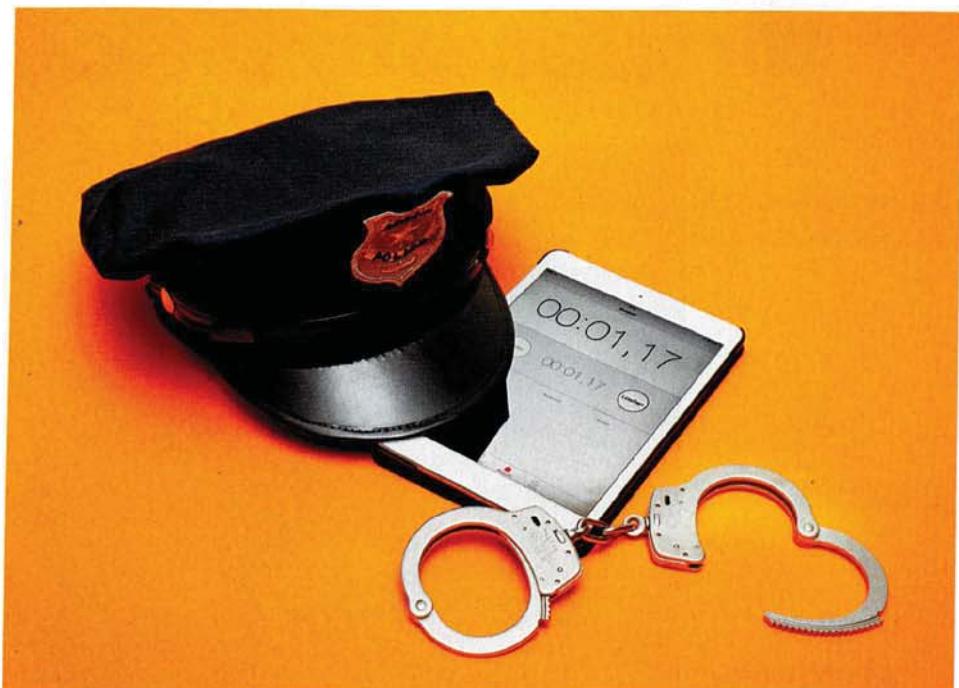
c't computerversteher Shirt
statt 17,90 Euro nur 15,90 Euro



Bestellen Sie Ihr Exemplar für 9,90 €
portofrei bis 24.11.2013*

shop.heise.de/ct-netze service@shop.heise.de
0 21 52 915 229

heise shop



Was sich bei iOS 7 in Sachen Sicherheit ändert

Sicherheitskontrolle

Mark Zimmermann, Philip Kuß

Zwar stehen Entwicklern mit iOS 7 viele neue Features zur Verfügung, teilweise werfen jedoch genau diese neue Sicherheitsprobleme auf. An den Bordmitteln in Sachen Sicherheit hat Apple auch gearbeitet.

Mit dem gerade veröffentlichten iOS 7 hat Apple bei Weitem nicht nur das Erscheinungsbild des beliebten mobilen Betriebssystems angepasst, sondern dessen Unterbau ebenfalls kräftig überarbeitet. Dadurch stehen Entwicklern neue Möglichkeiten offen, die das OS vor allem für den Unternehmenseinsatz interessant machen (siehe auch Artikel „Face-Lift“ Seite 114). Insbesondere stehen für Unternehmen Aspekte wie Sicherheit, Performance sowie die Inte-

grierbarkeit in bestehende Infrastrukturen im Vordergrund. Die Integration in die Infrastruktur von Unternehmen war bereits mit iOS-Geräten seit Version 4.0 effizient und einfach möglich. Auch verschlüsselte E-Mails, MDM (Mobile-Device-Management) und VPN (Virtual Private Network) unterstützt das Betriebssystem seit Längerem. Apple baut diesen hohen Integrationsstandard bei iOS 7 nun deutlich aus.

Auch beim Mobile-Device-Management gab es weitrei-

chende Änderungen. Mit dem neuen iOS 7 lassen sich nicht nur die Smartphones oder Tablets verwalten, sondern auch Apple-TV-Endgeräte. Das ermöglicht es, dass man sie auf die Whitelist der erlaubten Geräte setzt und Mitarbeiter sie beispielsweise für Präsentationen nutzen können.

MDM der nächsten Generation

Des Weiteren hat Apple mit iOS 7 das Aufnehmen neuer Geräte in das MDM stark vereinfacht. Der Administrator eines Unternehmens kann sie bei Apple direkt registrieren und in die eigene MDM-Lösung einbinden. Bei Inbetriebnahme eines Gerätes durch den Anwender stellt der Einrichtungsassistent fest, dass es

registriert wurde, und das MDM bestückt es „over the air“ automatisch mit den dafür vorgesehenen Profilen. Diese Profile können Unternehmensrichtlinien sowie unternehmensübliche Konfigurationen enthalten. Auf diese Weise ist sichergestellt, dass das Gerät den aktuell gültigen Sicherheits- und Konfigurationsstandard erhält.

Die beschriebene Verwaltung erfolgt durch MDM-Profile über Webprotokolle. Apple hat hier viele neue Kommandos, Abfragen und Konfigurationsmöglichkeiten eingefügt, die ein differenzierteres Administrieren der Geräte ermöglichen (s. Kasten „MDM-Optionen für ge- managte Apps“).

Dieses neue Konzept dient dazu, die Privatsphäre von Anwendern zu schützen, Unternehmen abzusichern sowie unerwünschten Datenabfluss zu verhindern und ist Apples Antwort auf die Problematik BYOD/HYOD (Bring Your Own Device/Here is Your Own Device). Anbieter wie Samsung mit seinem Knox oder BlackBerry mit Balance setzen auf das Separieren des privaten und geschäftlichen Workspace. Apples iOS 7 dagegen auf Schutz und Separieren der Daten in ihren jeweiligen App-Sandboxen. Letzteres soll Anwendern ein angenehmeres Arbeiten bescheren, da sie nicht zwischen unterschiedlichen Workspaces umschalten müssen.

Wie im Kasten „MDM-Optionen ...“ zu sehen ist, unterstützt iOS 7 den sogenannten „Supervised Mode“ bei Mobilgeräten. Dieser Modus war bis iOS 6 ausschließlich über das Apple Configuration Utility zu realisieren. Dazu musste allerdings der lokale Administrator die zu betreuenden Geräte via Kabelanbindung in den entsprechenden Modus versetzen und die Konfigurationsprofile verteilen. Mit iOS 7 ist das nun auch kabellos über das MDM möglich. Der Modus erlaubt dem Administrator tiefegehende Konfigurationsan-

passungen, zum Beispiel das Abschalten des Lightning-/Dock-Connectors, die Silent-Installation von Anwendungen (also ohne Dialogfenster) und einiges mehr.

MDM-Interaktion mit Apps

Seit iOS 7 können Administratoren die Apps auf den Geräten über das MDM-Protokoll mit Konfigurationsinformationen versorgen, unabhängig davon, ob diese gerade aktiv sind oder nicht. Entwickler können Neuerungen einfach wie folgt in ihre Apps integrieren. Erhält eine App per MDM eine aktualisierte Konfigurationsinformation, kann der Entwickler sie über die bereits aus den App-Settings bekannte Funktion

```
[[NSUserDefaults standardUserDefaults] objectForKey:@"com.apple.configuration.managed"]
```

auslesen. Erhält eine Anwendung ein geändertes Konfigurationsprofil, wird für die betroffene App eine Notification ausgelöst, auf die der Entwickler in seinem Code reagieren muss. Hierzu kann er die Notification mit dem Callback `NSUserDefaultsDidChangeNotification` abfangen (siehe Listing 1).

Diese gesendeten Konfigurationen (zum Beispiel UI-Einstellungen, URL-Listen, De-/Aktivierung von iCloud) dürfen keine sicherheitsrelevanten Informationen beinhalten, da diese innerhalb ei-

nes ungeschützten Objekts auf dem Gerät (Schutzklasse *NSFileProtectionNone*) gespeichert und hier von Dritten ausgelesen werden können. Das MDM darf daher auf diesem Weg nur Konfigurationen und keine Nutzdaten versenden.

Den Rückkanal aus den Apps zum MDM kann der Entwickler wie folgt umsetzen und nutzen. Die Funktion des App-Feedbacks ermöglicht es zum Beispiel im Support- und Requestfall, Informationen zu einem Problem oder auch Feature-Requests direkt aus der App heraus an das MDM des Unternehmens zu senden. Dieses kann die Informationen entgegennehmen und kanalisierten. Um einen Feedback an das MDM-System zu senden, muss der Entwickler die zu übermittelnden Werte in einem *NSDictionary*-Objekt sammeln und über den Aufruf *NSUserDefaults* mit dem Key *com.apple.feedback.managed* an das MDM-System senden (siehe Listing 2).

**Erhöhte
App-Sicherheit**

Zur Trennung des privaten vom geschäftlichen Bereich trägt eine entsprechende Beschränkung in der „Open In“-Einstellung für das Share Sheet maßgeblich bei. Diese Option bewirkt, dass lediglich durch den Administrator definierte Apps Daten austauschen können. Man kann etwa den Datenabfluss zu einem

MDM-Optionen für gemanagte Apps	
Aktion	Neu in iOS 7
Installieren von Apps	
Löschen von Apps	
Deaktivieren von iCloud-Anbindungen	
Installieren ohne Nutzerinteraktion (nur bei „supervised“ Geräten)	✓
App-Konfiguration	✓
App-Feedback	✓
verwaltetes „Open In“	✓
Single Sign-on	✓
Per-App-VPN	✓

Listing 1: Auslesen der Konfiguration

```
//Funktion zum Auslesen der empfangenen Einstellungen.  
- (void)readValues {  
    NSDictionary *serverConfig =  
        [NSUserDefaults standardUserDefaults]  
            dictionaryWithForKey:@"com.apple.configuration.managed"];  
    NSString *Konfigurationsinhalt = serverConfig[@"Configurationstitle"];  
}
```

Listing 2: App-Feedback via MDM

```
- (void)sendFeedback {
    ...
    NSMutableDictionary *feedback =
        [[[NSUserDefaults standardUserDefaults]
            dictionaryForKey:@"com.apple.feedback.managed"] mutableCopy];
    if (!feedback) feedback = [NSMutableDictionary dictionaryWithDictionary:[NSmutableDictionary dictionary]];
    feedback[@"successCount"] = @"FEEDBACK";
    [[NSUserDefaults standardUserDefaults]
        setObject:feedback forKey:@"com.apple.feedback.managed"];
    ...
}
```

Dropbox et cetera dadurch unterbinden, dass man die „Open In“-Weitergabe an Dropbox nicht explizit erlaubt (Whitelisting).

Eine zusätzliche Maßnahme zur Erhöhung der Sicherheit führt iOS 7 im Umfeld der Standardverschlüsselung ein. Ab iOS 7 werden alle Apps standardmäßig nach FIPS 140-2 mit *NSFileProtectionCompleteUntilFirstUserAuthentication* verschlüsselt. Das kann der Entwickler weder erzwingen noch deaktivieren.

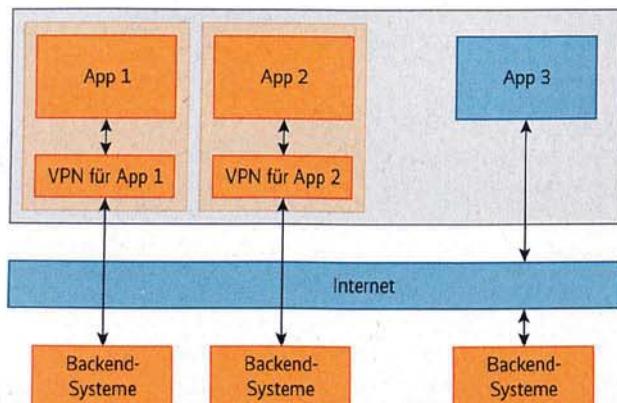
ren. Die Folge ist, dass nach einem Reset oder Neustart des Telefons die Applikationen erst nach erfolgreichem Entsperren durch den Anwender zugänglich sind. Dieselbe Vorkehrung trifft das Betriebssystem beim Speichern von Werten in die Keychain, indem es auch hier intern auf *kSecAttrAccessibleAfterFirstUnlock* umstellt.

Zentraler Ort
für Geheimnisse

Unter iOS 7 müssen alle Zugriffe des Entwicklers auf die Keychain über die API *SecItem* erfolgen. Die Keychain ist unter iOS – ebenso wie unter OS X – der zentrale Ort zum Ablegen von Geheimnissen unterschiedlicher Art (Zertifikate, Kennwörter und so weiter). Sie ist eine Datenbank, in der jede Tabelle eine Spalte besitzt, in der die Daten verschlüsselt stehen. Diese Daten sind mit einem gerätespezifischen Schlüssel ver-



- Mit dem neuen iOS 7 setzt Apple den Weg zu mehr Datenschutz und -Sicherheit insbesondere in Bezug auf den Unternehmenseinsatz mobiler Geräte fort. Auch Performance und Integrierbarkeit in bestehende IT-Strukturen stehen im Vordergrund.
 - Mit ausgefeilten Optionen des Mobile-Device-Management reagiert Apple auf die Herausforderungen und Risiken, die das aus Unternehmen nicht mehr wegzudenkende „Bring Your Own Device“ mit sich bringt.
 - Vorsicht, Falle: Zwar gibt es zahlreiche neue Sicherheitsfeatures, andere Neuerungen reißen dafür neue Sicherheitslücken auf, die die Entwickler und Administratoren kennen und stopfen müssen.



Im Gegensatz zu einem systemübergreifenden ist das Per-App-VPN ressourcensparend und beeinträchtigt nicht die Laufzeit der Geräte (Abb. 1).

sehen, der den transparenten Zugriff auf sie auf das jeweilige Gerät einschränkt.

Mit iOS 7 führt Apple das Single Sign-on ein. Nun ist es App-übergreifend möglich, sich an einem Authentifizierungsserver (Kerberos) einmalig anzumelden und das Login für alle zugelassenen Apps zu verwenden. Wird eine App genutzt, die eine noch nicht vorliegende Authentifizierung benötigt, so fordert künftig das OS selbst die Authentifizierung des Anwenders an, um ein Sitzungsticket zu erzeugen. Es kann dann in anderen Anwendungen genutzt werden. Ob es sich um selbst entwickelte oder um fremd erstellte Apps handelt, spielt keine Rolle. Gültige SSO-Sitzungen können in

Apps automatisch genutzt werden, wenn der Entwickler für die Kommunikation die Klassen *NSURLConnection* beziehungsweise *NSURLSession* nutzt. Eine individuelle Implementierung für einzelne Apps ist somit nicht mehr notwendig.

Die SSO-Authentifizierung konfiguriert der Administrator über das MDM mit Konfigurationsprofilen. Anschließend steht SSO nicht nur den Apps, sondern auch dem Browser von iOS (Safari) zur Verfügung.

Reine VPN-Verbindungen sind schon länger Bestandteil von iOS. Mit iOS 7 steht nun ein sogenanntes Per-App-VPN zur Verfügung – also die Möglichkeit, pro App eine VPN-Verbindung (Abbil-

dung 1) zu definieren. Das erfolgt ebenfalls per MDM in Form von Konfigurationsprofilen. Diese Erweiterung bietet den Vorteil, dass sie die Akkulaufzeit nicht beeinträchtigt, anders als das systemweite VPN, das in der Praxis den Energieverbrauch der mobilen Geräte stark erhöhte und deren Laufzeit um ein Vielfaches reduzierte.

Außerdem steht der Zugriff auf das VPN-Netzwerk in der jetzigen Version nur noch vom Administrator festgelegten Anwendungen zur Verfügung. Beim systemweiten VPN bestand noch der Nachteil, dass auch nicht explizit dafür freigegebene Apps es nutzen konnten. Um Per-App-VPN einzusetzen, ist lediglich die entsprechende Infrastruktur im Unternehmen notwendig, keine individuelle Implementierung durch den Entwickler oder durch Dritte in den jeweiligen Apps. Es reicht hier ebenfalls, die erwähnten Klassen *NSURLConnection* und *NSURLSession* für die Kommunikation zu nutzen.

Nativer Code und JavaScript

Mit iOS 7 stellt Apple Entwicklern die neue Bibliothek *JavaScriptCore Library* zur Verfügung, die es ermöglicht,

aus JavaScript heraus auf Objective-C-Funktionen zuzugreifen. Ein globales Objekt für die Ausführung von JavaScript-Code steht mit *JSContext* bereit.

JSValue ist hierbei eine Referenz auf das Ergebnis der JavaScript-Operation und lässt sich im Objective-C-Code weiterverarbeiten. Die Ergebnisse können auch an JavaScript zurückgegeben werden. Entwickler können mit der Funktion *evaluateScript* JavaScript-Code ausführen, der ihr zum Beispiel in Form eines *NSString* als Parameter zu übergeben ist:

```
JSContext *context = [JSContext alloc] init];
//JavaScript-Klasse initialisieren
JSValue *result = [context evaluateScript:@“4 + 8”];
//den JavaScript-Code in
//Objective-C durchführen
```

JavaScript-Fragmente liegen im Klartext im App Bundle und sind somit jederzeit „einschubar“. Daraus folgt, dass Entwickler keine sicherheits- oder datenschutzrelevanten Informationen oder Routinen in diesen Methoden ablegen sollten. Der Zugriff auf ein JavaScript, das per HTTP geladen wird, ist mit der neuen JavaScript Library ebenfalls möglich (Listing 3).

Und das ist noch nicht alles, auch der Aufruf von Objective-C-Code aus JavaScript heraus ist für Entwickler nun möglich. Gerade im Hinblick auf zunehmende HTML5-Entwicklungen gibt es ihnen die Option, ihren Code großteils wiederzuverwenden. Unter dem genannten Aspekt der Sichtbarkeit des Codes sollten Entwickler aber darauf achten, welche Komponenten sie in diesem Kontext wiederverwenden. Betrachtet man den JavaScript-Code, kann man Rückschlüsse auf Objective-C-Methodennamen ziehen. Hier muss der Entwickler dafür Sorge tragen, dass der Methodename nichts über den Funktionsinhalt verrät. Dank dieser Neuerungen ist es nun auf einfache Art und Weise möglich, bestehende Webanwendungen im Kon-

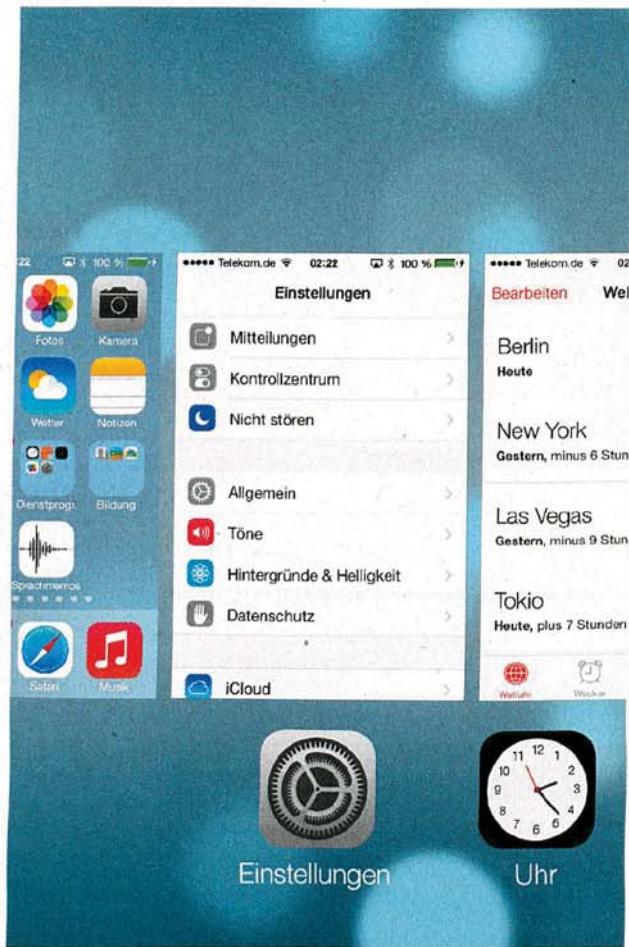
Listing 3: JavaScript und Objective-C

```
//Objective-C-Code (App)
-(BOOL)webView:(UIWebView *)theWebView shouldStartLoadWithRequest:(NSURLRequest *)theRequest
navigationType:(UIWebViewNavigationType)navigationType {
    NSString *requestStr = [[theRequest URL] absoluteString];
    NSArray *requestComponents = [requestStr componentsSeparatedByString:@":"];

    if ([requestComponents count] > 1 &&
        [(NSString *)[requestComponents objectAtIndex:0] isEqualToString:@"meineApp"]) {
        if([(NSString *)[requestComponents objectAtIndex:1] isEqualToString:@"meineFunktion"])
        {
            [[<Objekt> shared] ObjectiveCFunktion]; //ruft die Objective-C-Funktion auf
        }
        return NO;
    }
    return YES; //Rückgabewert YES, damit nach der individuellen Bearbeitung der normale Request weiterläuft.

}

//JavaScript-Code (Web Server)
function myFunction(event)
{
    document.location = "meineApp:" + "meineFunktion:" + param1 + ":" + param2;
}
```



Beim Taskmanager ist Datenschutz gefragt: Damit kein Unbefugter vertrauliche Informationen erhascht, sollte man gegen den standardmäßig erstellten App-Screenshot aktiv werden (Abb. 2).

text einer nativen App zu betreiben und mit dieser interagieren zu lassen.

Jetzt auch mit Biometrie

Mit Veröffentlichung von iOS 7 und dem neuen Spitzmodell iPhone 5S stellt Apple erstmalig eine Option zur biometrischen Authentifizierung bereit: einen Fingerabdruck-

sensor namens TouchID. Die Funktion ist vorerst dem System selbst vorbehalten, Entwickler haben keinen Zugriff darauf. Der Benutzer kann mit ihr das Gerät entsperren, iTunes-Einkäufe autorisieren und Kennwörter ersetzen. Die sicherheitsbezogenen Daten des Sensors werden lokal in einem neuen Sicherheitsbaustein des ebenfalls neuen 64-Bit-Prozessors vom Typ A7 vorgehalten.

Es bleibt aber zu beachten, dass es sich dabei nur um eine Einfaktor-Authentifizierung handelt, mit allen Vorteilen und Nachteilen. Unternehmen sollten dieses Feature im Auge behalten, da zu hoffen ist, dass es in Folgeversionen auch Entwicklern zur Verfügung stehen wird.

Zu einer eher kleinen Neuerung gehört die Einstellung, ob eine Anwendung das mobile Datennetz des Endgerätes nutzen darf. Mit `urlRequest.allowsCellularAccess = NO` schränkt der Entwickler die Datenkommunikationen ausschließlich auf WLAN ein. Entwickler sollten diese Einstellung wählen, wenn der Benutzer mit großen Datenmengen arbeiten muss.

Dem Diebstahl von Endgeräten setzt Apple das neue Feature „Activation Lock“ entgegen. Es verlangt selbst nach einem kompletten Zurücksetzen vom Anwender die AppleID des letzten Besitzers samt Kennwort, um wieder in Betrieb zu gehen. In den USA haben die Staatsanwaltschaft und Sicherheitsbehörden nach einem Test diese Funktion positiv bewertet.

Neue Features, neue Herausforderungen

Apple stellt mit dem neuen iOS 7 eine Vielzahl neuer Optionen und Funktionen bereit. Mit den neuen Features gehen teilweise aber auch neue Sicherheitsprobleme einher. Die wichtigsten sowie einige Schutzmaßnahmen seien im Folgenden kurz angesprochen.

Screenshots: iOS 7 nutzt für seine Animationen und

vor allem für den neuen Taskmanager (Abb. 2) weiterhin Screenshots der jeweiligen App, die das Betriebssystem beim Verlassen einer Anwendung automatisch erstellt. Da diese künftig unmittelbar im Taskmanager zur visuellen Orientierung angezeigt werden, empfiehlt es sich, sie in kritischen Apps zu unterdrücken, zu löschen oder durch ein Standardhintergrundbild zu ersetzen. Andernfalls könnten Unbefugte beim Durchwischen des Taskmanagers vertrauliche Informationen sehen [1].

Vorsicht geboten ist manchmal auch, wenn der Anwender selbst von vertraulichen Informationen oder Dateien einen Screenshot erstellen will. Damit ein Entwickler das je nach Unternehmens-Policy beispielsweise unterbinden oder einen Alarm auslösen kann, bringt iOS 7 ein neues Event mit. Es kann als `Event-Listener` im `AppDelegate` der App hinterlegt werden, ein Beispiel zeigt Listing 4.

Code Injection: Durch die beschriebenen Zugriffsmöglichkeiten von Objective-C auf JavaScript und umgekehrt sind nicht nur die genannten Datenschutzverletzungen möglich. Vielmehr entstehen Risiken der Code Injection und potentieller Manipulation des bestehenden Codes durch Dritte, wie man sie von den „klassischen“ Webanwendungen her kennt.

Da diese Option in iOS 7 neu ist, muss der Entwickler dafür Sorge tragen, dass Zugriffsmethoden zwischen den Stacks verschleiert sind, eindeutige Parameterprüfungen stattfinden und Parameter – etwa durch ASCII-Entsprechungen – entschärft („escaped“) werden. Auf diese Art kann er gängige Cross-site-Scripting-Angriffe unterbinden [2].

Verstärkung der Standardverschlüsselung: Finden sich in Anwendungen besonders vertrauliche Daten, muss der Entwickler zusätzliche Verschlüsselungsmechanismen einbauen. Die Autoren emp-

Listing 4: Screenshot EventHandler

```
- (BOOL)application:(UIApplication *)application didFinishLaunchingWithOptions:(NSDictionary *)launchOptions
{
    [[NSNotificationCenter defaultCenter] addObserver:self selector:@selector(screenshotAusgelöst:)
                                              name:UIApplicationUserDidTakeScreenshotNotification object:nil];
}

- (void)screenshotAusgelöst{
    //Screenshot löschen und ggf. weitere Events auslösen.
}
```

BIG DATA –

Große Datenmengen
richtig speichern
und effizient verarbeiten

Redaktionelle Fachkonferenz

Big Data
in Zeiten von
Prism & Co.

heise
Netze

Die diesjährige, rein redaktionelle Fachkonferenz von heise Netze steht ganz im Fokus des bedeutenden Themas Big Data.

AUSZUG AUS DEM PROGRAMM:

- **Big Data – Was'n Hype?!**
Volker Weber, freiberuflicher Systemarchitekt und Fachautor
- **Sicherheit im Big Data Umfeld – Big Data = Big Problem?**
Christoph Wegener, freiberuflicher Berater, wecon.it-consulting
- **Datenanalyse für Big Data –**
Mehr Sicherheit durch „Prism yourself“
Sebastian Mondial, freier investigativer Datenjournalist, Norddeutscher Rundfunk und ARD/ZDF-Medienakademie
- **Big Data: Möglichkeiten und Grenzen aus rechtlicher Sicht**
Joerg Heidrich, Justiziar & Datenschutzbeauftragter, Heise Zeitschriften Verlag

DIE HEISE NETZE TOUR

- 100% unabhängig
- hochkarätige Experten
- praxisorientiert
- Networking

Jetzt 15%
Frühbucherrabatt
sichern!

TERMINE:

- 7. November, Köln
- 14. November, Hamburg
- 19. November, Frankfurt
- 21. November, München

Frühbuchergebühr:
485,- Euro (inkl. MwSt.)

Teilnahmegebühr:
570,- Euro (inkl. MwSt.)

Partner:

EMC² Isilon

Software, Systeme und Dienstleistungen
Fritz & Maczki

MicroStrategy

concat AG
IT SOLUTIONS

Organisiert von:
heise
Events
Conferences, Seminars, Workshops

Kooperationspartner:

future thinking
26./27.03.2014

DEUTSCHE RECHENZENTRUMSPREIS
2014

Bexx

ecos

Weitere Informationen unter:

fehlen dafür die Nutzung von Keys, die nicht im System hinterlegt sind, sondern zufällig generiert werden. Eine gute Methode ist es, solche Keys aus Hashes unterschiedlicher zufälliger Komponenten zu erzeugen, zum Beispiel dem *identifierForVendor* zusätzlich einer zufälligen UUID [2].

Hintergrund-Downloads: Bei der Nutzung von *NSURLSession* muss der Entwickler dafür Sorge tragen, dass die Möglichkeiten zur separierten und privaten Speicherung der Download-Daten, die *NSURLSession* bereitstellt, zum Einsatz kommen. Das soll eine Kompromittierung der Nutzerdaten während des Herunterladens unterbinden.

Geändertes FileSystem/JailBreaktests: In iOS 7 ist ein modifiziertes Berechtigungskonzept für das FileSystem eingezogen. Es schützt das Betriebssystem vor direkten Zugriffen auf bekannte Partitionen/Mountpoints (zum Beispiel */var*). Nutzt eine App Funktionen, die darauf basieren, muss man sie für iOS 7 separat betrachten. Auch wenn aktuell noch keine JailBreaks für iOS 7 bekannt sind, müssen Entwickler auf diese Anpassung bei iOS 7 mit Vorsicht reagieren.

Mit Abfragen wie *contentsOfDirectoryAtPath: @"/Applications/"* könnten sie bei iOS 6 noch prüfen, ob beispielsweise Anwendungen wie Cydia vorhanden sind, die Rückschlüsse auf einen Jailbreak zulassen. Die Zuverlässigkeit solcher Prüfungen auf Anwesenheit bestimmter Dateien ist mit iOS 7 somit nicht mehr gegeben, die Prüfung damit nicht mehr ausreichend.

Fazit

Apple hatte mit iOS 6 bereits wichtige Schritte für den Betrieb der Plattform im Unternehmensumfeld eingeleitet. Mit iOS 7 wird dies nun konsequent fortgesetzt. Die neu-

en Features sollen sowohl anwenderfreundlich sein als auch die technischen und sicherheitsrelevanten Anforderungen von Unternehmen erfüllen.

Des Weiteren zeichnet sich die neue Betriebssystemversion durch neue Funktionen zum Schutz vertraulicher Geschäftsdaten, der Wahrung der Privatsphäre sowie ausgeweitete Optionen eines Mobile-Device-Management inklusive gängigen Szenarien eines Verlustfalls oder eines barrierefreien Zugangs aus. Das MDM ermöglicht theoretisch sogar, die Daten einer App eines verlorenen Gerätes wieder anzufordern, bislang ein Alleinstellungsmerkmal dieser Plattform. Das setzt allerdings die Kooperation von MDM-Anbieter und Entwickler voraus. (ur)

Mark Zimmermann

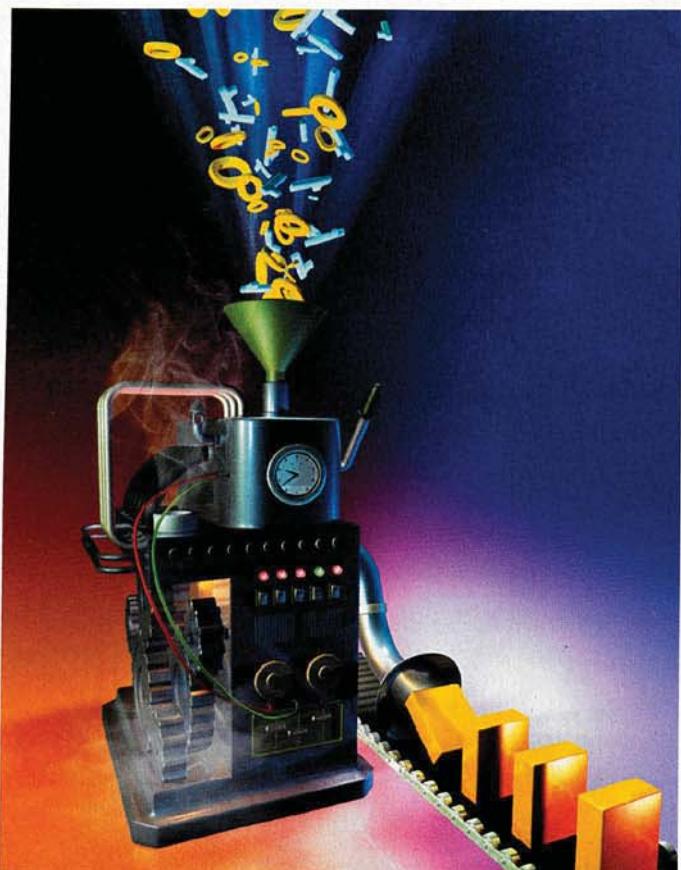
ist bei der EnBW Energie Baden-Württemberg AG in Karlsruhe als Teamleiter tätig. Das Aufgabenfeld in dem von ihm verantworteten Team umfasst unter anderem die Entwicklung von mobilen Applikationen für den internen Einsatz sowie für Endkunden der EnBW.

Philip Kuß

ist bei der EnNo Consulting GmbH in Münster als Softwareentwickler und -architekt tätig. Sein Aufgabenfeld umfasst die Konzeption, Architektur und Entwicklung individueller Applikationen.

Literatur

- [1] Ronny Sackmann, Mark Zimmermann; App-Hilfe; Sichere iOS-Programmierung im Unternehmensumfeld; *iX* 2/2012, S. 44
- [2] Daniel Schabunow, Mark Zimmermann; Mobility; Appgeschottet; Mehr Sicherheit für iOS-Unternehmensanwendungen; *iX* 9/2013, S. 96



Open Build Service
für Firmenprojekte nutzen

Baukasten

**Christian Schneemann,
Stefan Seyfried**

Als Build-Umgebung der openSUSE-Distribution gestartet, kann der Open Build Service heute deutlich mehr als „nur“ Pakete für Linux-Distributionen zu bauen. Firmen können darüber bequem Installationspaket-eigener Produkte oder im Unternehmen genutzter respektive entwickelter Tools sowie Skripte erstellen und zentral verwalten. Im eigenen Haus gehostete Instanzen bieten dafür umfangreiche Funktionen und mehr.

Keine Firma kommt heutzutage ohne IT aus. Und wo eine IT-Abteilung ist, finden sich auch selbstentwickelte Skripte, Tools, die den Administratoren die tägliche Arbeit erleichtern oder 3rd-Party-Applikationen und -Module, die die jeweiligen Hersteller als einfache Archive ausliefern. Mit wachsender Anzahl von Tools wächst auch der Aufwand, den Überblick zu behalten. Ein erster Schritt ist hier die Pflege der geschriebenen Skripte in einem Versionsverwaltungssystem wie Subversion oder Git. Neben der Pflege der Skripte selbst nimmt auch die Installation der aktuellen beziehungsweise freigegebenen Versionen auf den einzelnen Servern viel Zeit in Anspruch.

Hier kann der Open Build Service (OBS) helfen. Mit ihm lassen sich auf einfache Art und Weise aus identischen Quellen Pakete für RPM-basierte Distributionen bauen, beispielsweise SUSE Linux Enterprise Server (SLES), Red Hat Enterprise Linux (RHEL), openSUSE, Fedora oder CentOS, um nur einige zu nennen. Darüber hinaus unterstützt OBS deb-basierte Distributionen wie Debian oder Ubuntu sowie das PKGBUILD-System von Arch Linux. Selbst Windows-Software kann man mit dem OBS bauen und paketieren.

Vom Distributions- zum Community-Tool

Entstanden ist der Dienst im Rahmen des openSUSE-Projekts als Plattform, um der Community den Bau eigener Pakete und später auch die Mitarbeit an der Distribution zu ermöglichen. Seit 2006 ist die bis dahin noch openSUSE Build Service genannte Software als Open Build Service unter der GPL als Open-Source-Lösung verfügbar.

Die wohl bekannteste und größte OBS-Installation dürfte build.opensuse.org sein. Dort bauen und betreuen die Ent-

wickler des openSUSE-Projekts ihre Distribution. In einer ähnlichen (privaten) Instanz verwaltet SUSE seine Enterprise-Linux-Produkte.

Obwohl der Ursprung des Open Build Service in der openSUSE-Community liegt, bietet er inzwischen viele Features für den Unternehmenseinsatz. Diese lassen sich nur in einer eigenen Installation, einer sogenannten privaten Instanz, aktivieren und nutzen. Der weitere Text geht daher bei der Vorstellung der Features und den zugehörigen Beispielen immer von einer privaten Installation aus.

Vielschichtiges Innenleben

Unter der Haube besteht der OBS aus verschiedenen auf jeweils eine Aufgabe spezialisierten Einzeldiensten. Der Source-Server verwaltet den Quellcode der zu bauenden Pakete in einer Art Versionsverwaltung. Der Source Server ermöglicht das Ausführen von Skripten, sogenannter Services, die die Quellen des zu bauenden Pakets verändern oder aktualisieren können, beispielsweise indem sie den Code aus einer Versionsverwaltung auschecken. Pro Architektur existiert ein Scheduler-Dienst, der die abzuarbeitenden Aufgaben als Job generiert, die der Dispatcher wiederum an die sogenannten Worker verteilt. Sie sind die eigentlichen „Rechenknechte“, die den Quellcode übersetzen und daraus die Pakete bauen.

Ein Repo-Server hält die zum Aufbau der jeweiligen Build-Umgebung benötigten Pakete zum Download bereit. Nach dem erfolgreichen Bau der Pakete versieht der Sign-Server sie mit einer GPG-Signatur. Anschließend kommt der Publisher zum Einsatz: Er erstellt die Installations-Repositorien mit den fertigen Paketen und kann dabei auch eigene Skripte ausführen. Auf diesem Weg lässt sich bei-

spielsweise das Repository auf einen anderen Server spiegeln. Für die Interaktion bietet der OBS eine API, über die Benutzer per Webfrontend oder den Kommandozeilen-Client *osc* mit dem System kommunizieren können.

Unterstützung kollaborativer Arbeit

Im OBS erfolgt die Gliederung der einzelnen Software-pakete in Projekte. Aus diesen erstellt die Software dann Repositories für die Installation. OBS-Benutzer können in einem Projekt durchaus verschiedene Rollen einnehmen. Beispielsweise können sie „Maintainer“ oder „Reviewer“ sein und somit spezielle Rechte wahrnehmen. Ein Maintainer besitzt volle Schreibrechte auf ein Projekt/Paket. Diese Rolle darf im Bezug auf ein Paket beispielsweise die Sources verändern. Auf ein Projekt gesehen kann ein Maintainer auch Pakete anlegen. Ein Reviewer hat keine Schreibrechte, kann jedoch Commit-Requests für die Projekte oder Pakete, denen er zugeordnet ist, sehen und kommentieren.

Wer ohne die Maintainer-Rolle zu besitzen Änderungen an einem Paket vornehmen möchte, kann einen Branch erstellen, ihn wie gewünscht bearbeiten und anschließend per *commit* in das ursprüngliche Projekt zurückfließen lassen. Hat eine festgelegte Anzahl von Reviewern ihr Okay zu den vorgenommenen

Änderungen gegeben, kann ein Maintainer den Commit annehmen und die Änderungen in das ursprüngliche Projekt integrieren.

Ein typischer Anwendungsfall in Unternehmen ist das Aufnehmen von Softwareänderungen in die nächste Produktversion. OBS organisiert die Bestandteile respektive Pakete für das Produkt in zwei Arten von Projekten: eins, in dem die Entwicklung stattfindet, und eins, das das fertige Projekt beziehungsweise das nächste Release des Produktes festhalten soll. Hat ein Paket im Entwicklungsvorprojekt einen Release-fähigen Status erreicht, können die Entwickler es in das Produktprojekt einreichen. Hier entscheiden dann die Release-Verantwortlichen über die Aufnahme.

Eine weitere Funktion ist die Option, Zugriffe auf Projekte zu beschränken und dadurch den Zugang auf den dort vorgehaltenen Sourcecode zu kontrollieren. Ebenfalls nützlich ist die Option, sogenannte Publish Hooks auf Projektbasis zu definieren. Dabei handelt es sich jeweils um ein Skript, das OBS aufruft, wenn er alle Build-Jobs eines Projekts abgearbeitet hat. Auf diesem Weg kann man unmittelbar Einfluss darauf nehmen, was mit den fertigen Paketen passiert, nachdem OBS sie ins Download-Repository geladen hat. Die Optionen reichen hierbei vom Kopieren und Verteilen auf Mirror-Systeme bis hin zum

```

1 # 
2 # spec file for package nagios
3 # Copyright (c) 2013 SUSE LINUX Products GmbH, Nuernberg, Germany.
4 #
5 # All modifications and additions to the file contributed by third parties
6 # remain the property of their copyright owners, unless otherwise agreed
7 # in writing. The license for this file, and modifications and additions to the
8 # file, is the same license as for the pristine package itself (unless the
9 # file's license is the same license as for the pristine package in which
10 # case the license is the MIT License). An "Open Source License" is a
11 # license that conforms to the Open Source Definition (Version 1.9)
12 # published by the Open Source Initiative.
13 #
14 # Please submit bugfixes or comments via http://bugs.opensuse.org/
15 #
16 #
17 #
18 Name:          nagios
19 Summary:       The Nagios Network Monitor
20 License:      GPL-2.0+
21 Group:        System/Monitoring
22 Version:     3.5.0
23 Release:      0
24 Url:         http://www.nagios.org/
25 Source0:      %{name}-%{version}.tar.bz2
26 Source1:      rcs{name}
27 Source2:      convertcfg_8
28 Source3:      %{name}.sysconfig
29 Source4:      suse_de-nagios
30 Source5:      nagios_8
31 Source6:      nagiosstats_8
32 Source7:      nagios-htpasswd.users
33 Source8:      mini_epn_8
34 Source9:      new_mini_epn_8
35 #
36 #

```

Die Weboberfläche bietet einen Texteditor mit Syntaxhervorhebung, um schnell Änderungen am Quellcode vornehmen zu können (Abb. 1).

Verteilen und automatischen Installieren auf Testsystemen.

Publish Hooks lassen sich detailliert an die Prozesse in der jeweiligen Abteilung anpassen. Ein Beispiel für ihren Einsatz folgt später im Anwendungsbeispiel „Continuous Integration mit OBS“.

Bedienung per GUI oder Kommandozeile

Über das Web-GUI lässt sich der Open Build Service bequem steuern. Hier können Anwender auf einfache Art und Weise das Projektmanagement erledigen: Projekte und dazugehörige Pakete anlegen, editieren und natürlich auch wieder löschen. Quellen für Pakete lassen sich entweder direkt hochladen oder

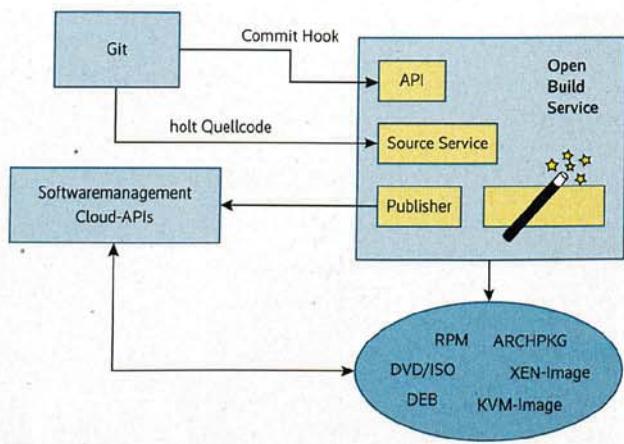
einzelne Paketdateien direkt in einem Editorfenster editieren. Auf Informationsseiten wie in Abbildung 1 hat man den Überblick über die Pakete eines Projekts.

Die OBS-Kollaborationsfunktionen sind für die einfache Benutzung ebenfalls in die Weboberfläche integriert. So kann ein Benutzer per Knopfdruck einen Branch erzeugen, das heißt eine Kopie in einem Unterprojekt seines Home-Projektes anlegen. In dieser Kopie kann er die gewünschten Modifikationen durchführen und anschließend die Änderung per Knopfdruck vorschlagen. Der oder die jeweiligen Maintainer des Ursprungspakets erhalten auf ihrer Webseite einen entsprechenden Hinweis und können die Änderungen im Browser direkt anschauen, übernehmen oder mit Kommentaren und Nachbesserungswünschen ablehnen.

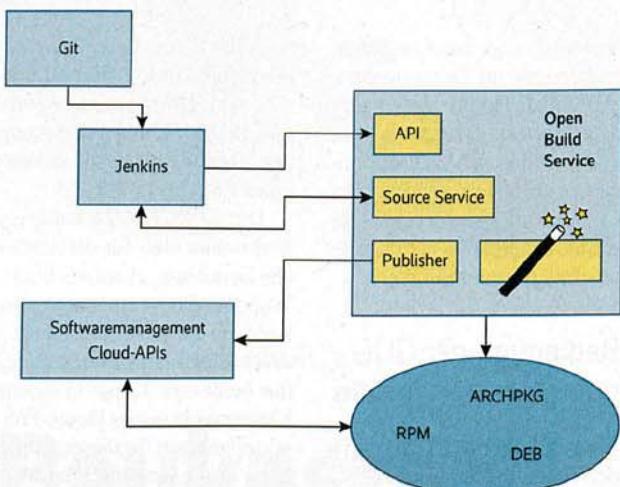
Mit dem Kommandozeilentool *osc* kann ein Anwender sämtliche im OBS anfallenden Arbeiten auch auf der Konsole durchführen. Über Skripte lassen sich Aufgaben einfach automatisieren. Die Bedienung von *osc* lehnt sich an die von Subversion an. Die Befehle zum Auschecken eines Pakets oder Projekts, zum Hinzufügen von Dateien oder zur Anzeige von Unterschie-

TRACT

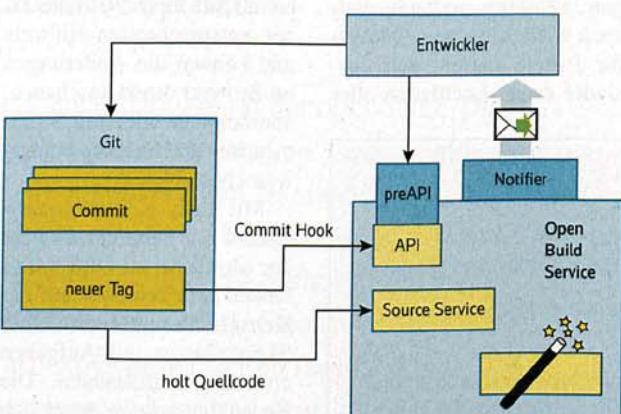
- Ursprünglich für das openSUSE-Projekt an den Start gegangen, lassen sich über den Open Build Service heute Pakete für viele Linux-Distributionen und sogar Windows bauen.
- Neben der Software kann der OBS auch Konfigurationen sowie Skripte verteilen und so den Wildwuchs in der IT eindämmen.
- Lokale OBS-Instanzen lassen sich gut in vorhandene Infrastrukturen einbinden und bieten die Option, die Vorteile des OBS zu nutzen, ohne jedem die Sources der eigenen Produkte offenlegen zu müssen.
- Die Kombination mit Git und Jenkins erlaubt Entwicklern, weiterhin in ihrer vertrauten Umgebung zu arbeiten.



Git-/Cloud-Anbindung: Ein Commit Hook aus Git informiert den OBS via API darüber, dass neue Versionen zum Bauen vorliegen. Der Source Service holt sie und baut sie im OBS, während der Publisher wiederum die Cloud-APIs über neue Images informiert (Abb. 2).



Continuous Integration: Zwischen Git und OBS führt Jenkins Tests mit dem Sourcecode durch und reicht diese erst an den OBS weiter, wenn die Ergebnisse den Kriterien entsprechen (Abb. 3).



Minimalkontakt: Hier arbeiten Entwickler nur mit Git und checken ihre Änderungen dort ein. Im Hintergrund erfolgt automatisch die Übergabe an den OBS. Bei Fehlern informiert der Notifier die Entwickler per Mail darüber (Abb. 4).

den zwischen lokalem Dateisystem und der Version auf dem Server sind identisch, sodass ein Administrator sich hier schnell heimisch fühlt. Außerdem gibt es OBS-spezifische Kommandos, um die Metadaten eines Projekts oder Pakets anzusehen und zu ändern, das Paket testweise lokal auf dem Entwicklerrechner zu bauen (empfehlenswert bei komplizierteren Paketen, beispielsweise zum Ausschließen von Tippfehlern) sowie zum Herunterladen der auf dem Server gebauten Pakete. Die Kollaborationsfunktionen lassen sich natürlich auch mit *osc* vollständig nutzen.

anbinden. Auf diesem Weg führen Änderungen an den Sources der Tools oder den Konfigurationen umgehend zu Installationspaketen für die Installation neuer Systeme oder das Update vorhandener Systeme in den Repositories.

Continuous Integration mit OBS

Abbildung 2 zeigt den schematischen Ablauf dieser Anbindung. Im Versionsverwaltungssystem (im Beispiel Git) ist ein Post-Hook zu konfigurieren, der auf neu angelegte Tags reagiert. Ein Tag ist sozusagen ein eindeutiger Name für einen bestimmten Stand der Entwicklung. Tags sollte man nutzen, damit OBS nur bestimmte Versionen baut und nicht jede kleine Änderung, die eventuell nur Teil mehrerer Commits ist und einzeln nicht funktioniert. Dies schließt ungewollte und sinnlose Bauversuche von vornherein aus.

Pakete auch für Konfigurationen

Das Erstellen von Installationspaketen ist aber nicht nur etwas für Softwareprodukte. Auch intern geschriebene und genutzte Skripte lassen sich mit RPM/DEB-Paketen sauber auf Serversystemen verteilen. Darauf hinaus kann man fertige Konfigurationen, sprich fertig angepasste Konfigurationsdateien, mithilfe von Installationspaketen distributieren. Im Fehlerfall lässt sich dann mit einfachen Bordmitteln überprüfen, warum auf einem Server etwas nicht funktioniert, obwohl auf den ersten Blick niemand etwas geändert hat. Ein Aufruf von *rpm --verify*, wie exemplarisch in Listing 1 zu sehen, zeigt auf einem zu überprüfenden System sofort an, welche Dateien nicht mehr im ursprünglichen Zustand sind. So lassen sich Fehler durch manuelle einseitige Änderungen ohne großes Suchen direkt auf den Systemen finden und einfach durch Neuinstallation des Pakets beheben.

Ein weiterer Punkt ist, dass OBS sich gut in bestehende Infrastrukturen einbinden lässt. Pflegt man seine internen Tools und Skripte bereits in einem Versionsverwaltungssystem wie Git oder Subversion, lassen sich diese an den OBS

konfigurierte Hook spricht die API des OBS an und schreibt dort eine neue Service-Datei. Diese enthält die Konfiguration der Abläufe, die der OBS automatisch vor dem Start eines Build-Jobs durchführen soll, zum Beispiel das Herunterladen von Dateien von Webservern oder aus einem Versionsverwaltungssystem. In diesem Fall enthält die Service-Datei Informationen zum neu erstellten Tag sowie zum Git-Repository und sorgt dafür, dass der passende Source Service ausgeführt wird. Ein Source Service ist ein Skript, das ein spezieller Dienst (Source Service Server) auf dem OBS Backend ausführt und das die Sources für ein Paket vor dem Bauprozess verändern/erweitern kann. Danach ersetzt er die Paketquellen, durch die hinter dem Tag befindliche neue Version. Da sich der Inhalt der Service-Datei geändert hat, stößt der OBS einen neuen Build-Job an und wertet den Inhalt der Servicedatei aus. Danach

checkt er die hinter dem Tag genannte Version aus dem Versionsverwaltungssystem aus und speichert sie als komprimiertes Tar-Archiv. Anschließend übergibt der Server den Build-Job an einen Worker, der das eigentliche Paket baut. Hat der das Paket fertig gestellt, überträgt er es zurück an das OBS Backend. Das legt es in das passende Repository und führt den für das Repository konfigurierten Publish Hook aus. Dieser signalisiert beispielsweise dem Softwaremanagement-Tool, dass neue Pakete vorliegen, was wiederum die Neuinstallation von Testsystemen auslöst.

Softwaretests mit Jenkins

Leider sind die Testmöglichkeiten durch einen bloßen Build-Job nur begrenzt auswertbar. Zwar kann man innerhalb des Bauvorgangs Tests durchführen, jedoch kann das Ergebnis eines Build-Jobs nur erfolgreich oder nicht erfolgreich sein. Möchte man noch detailliertere Tests durchführen, lässt sich ein Continuous-Integration-Tool wie Jenkins zwischen Git und OBS schalten (s. Abb. 3). Dieses führt dann Checks für die Codeanalyse oder API durch, bevor es den Quelltext an den OBS übergibt.

In einem solchen Szenario kontaktiert der im Git-Repository konfigurierte Post-Hook dann nicht die OBS-API, sondern die API von Jenkins und stößt hier einen vorher erstellten Job an. Hat dieser Jenkins nach den definierten Kriterien erfolgreich durchlaufen, hat man zwei Möglichkeiten, den Build-Job für das neue Paket im OBS erstellen zu lassen:

Entweder man lässt, wie im vorherigen Beispiel ohne Jenkins, eine Service-Datei erstellen mit Verweis auf den getesteten Git-Tag und lädt die Sources direkt aus dem Git-Repository. Oder man lässt das von Jenkins erstellte Archiv in das passende OBS-Projekt hochladen.

Open Build Service im Verborgenen

Hat man den OBS wie vorhergehend beschrieben direkt oder über Tools wie Jenkins an die im Unternehmen genutzten Versionsverwaltungssysteme angeschlossen, ist zu überlegen, ob wirklich jeder Entwickler/Administrator, der etwas in diesen Systemen (Git oder Subversion) ändert, auch als Benutzer Zugriff auf den OBS benötigt.

Zum Steigern der Akzeptanz lässt sich die „Komplexität“ des Konstrukts von den meisten Mitarbeitern fernhalten. Für den Großteil der Nutzer reicht es in den beschriebenen Abläufen aus, weiterhin ihre Änderungen lediglich in das genutzte Versionsverwaltungssystem zu „committen“ und anschließend das passende Installationspaket in einem Repository vorzufinden. Die Arbeit direkt im OBS kann man einem Team überlassen, das die Aufgaben des initialen Packagings neuer Projekte übernimmt.

Damit die jeweiligen Entwickler interner Tools dennoch Informationen über auftretende Fehler im Bauprozess erhalten, kann man auf eine weitere OBS-Schnittstelle zurückgreifen: den Notifier. Den ruft OBS nach dem Ende eines Build-Jobs auf und übergibt ihm Informationen wie das Er-

Listing 1: Systemänderungen per rpm --verify finden

```
# rpm -ql apache-vhost-example.org
/etc/apache2/vhosts.d/example.org.conf
# rpm --verify apache-vhost-example.org
# vi apache-vhost-example.org
# rpm --verify apache-vhost-example.org
...T.... /etc/apache2/vhosts.d/example.org.conf
# zypper in --force apache-vhost-example.org-1-9.1.noarch.rpm
# rpm --verify apache-vhost-example.org
```

Listing 2: Beispiel einer Servicedefinition

```
<services>
<service name="tar_scm">
<param name="url">http://example.de/foo.git</param>
<param name="scm">git</param>
<param name="revision">v0.23.5</param>
</service>
<service name="recompress">
<param name="compression">gz</param>
<param name="file">*foo*tar</param>
</service>
<service name="download_url">
<param name="protocol">https</param>
<param name="host">b1-systems.de</param>
<param name="path">/master/foo.spec</param>
</service>
</services>
```

gebnis des Jobs. Hier kann man ein Notify-Skript nutzen, das nur auf fehlgeschlagene Build-Jobs reagiert und den passenden Entwickler per Mail darüber informiert. Diese Mail enthält beispielsweise einen Link zum Build-Log des fehlgeschlagenen Jobs. So kann der Entwickler Fehler nachvollziehen und beheben.

Abbildung 4 zeigt das Vorgehen genauer. Die dort beschriebene „preAPI“ stellt nur eine Zwischenschicht zwischen den Entwicklern und der OBS-API dar. Auf diesem Weg können Entwickler, ohne sich an der API authentifizieren zu müssen, auf bestimmte Funktionen des Build Service zugreifen, beispielsweise das Abrufen des Build-Logs bei der Fehlersuche. Bei einem derart gestalteten Setup kommen die Entwickler nur wenn nötig mit dem Open Build Service in Berührung und arbeiten den Großteil ihrer Zeit mit ihren gewohnten Werkzeugen wie IDEs und Versionsverwaltungssystemen.

Fazit

OBS bietet Unternehmen ein mächtiges Werkzeug, um den Wildwuchs in ihrer Systemlandschaft einzuschränken. Skripte, Konfigurationen und Software werden nicht mehr von Hand verteilt und gewartet, sondern zentral im OBS

verwaltet. Softwareherstellern erlaubt der OBS schnell und einheitlich Pakete für unterschiedlichste Distributionen bereitzustellen.

Da OBS ein Open-Source-Projekt ist, steht kein Hersteller mit kommerziellem Support hinter dem „Produkt“. In diese Breche springen Dienstleister aus dem Open-Source-Umfeld, die kommerziellen Enterprise-Support rund um OBS im Programm haben [c]. Für einen intensiveren Einstieg bietet die Firma der Autoren eine vorkonfigurierte Appliance zum kostenlosen Download an [d]. Damit können Interessierte OBS nach Herzenslust ausprobieren. (avr)

Stefan Seyfried

arbeitet bei der B1 Systems GmbH als Linux Consultant & Developer und verwendet den OBS seit Beginn als openSUSE-Community-Mitglied, bei Kunden und zum Bauen von B1-Paketen.

Christian Schneemann

unterstützt als System Management & Monitoring Architect bei der B1 Systems GmbH mehrere Kunden bei der OBS-Einführung und implementiert von diesen gewünschte Features in OBS.

Alle Links: www.iz.de/ix1310126

Onlinequellen

- | | |
|------------------------|--|
| [a] OBS-Projektseite | www.open-build-service.org |
| [b] größte OBS-Instanz | build.opensuse.org |
| [c] Enterprise-Support | www.open-build-service.org/support |
| [d] OBS-Appliance | www.b1-systems.de/loesungen/obs |

Migration auf Multi-Core-CPUs



Nebeneinander

Marwan Abu-Khalil

Wer die Leistung moderner Multi-Core-Prozessoren ausreizen will, muss vorhandene Software parallelisieren. Wie man dabei vorgeht und was es zu beachten gilt.

Prozessoren werden heute nicht mehr wesentlich schneller, stattdessen erhöht sich fortwährend die Zahl der Kerne in den CPUs. Daher ist Parallelisierung mittlerweile das nahezu wichtigste Mittel, die Performance von Softwaresystemen sicherzustellen. Besondere Bedeutung kommt dabei der Migration von Legacy-Software zu, da sich viele Systeme nicht von Grund auf neu schreiben lassen. Solche Migrationsprojekte stehen etwa dann vor besonderen Herausforderungen, wenn die Softwarearchitektur sich implizit darauf verlässt, dass der Prozessor Threads nie gleichzeitig ausführt – was jedoch nur bei Single-Core-CPUs der Fall ist.

Der vorliegende Artikel resümiert die Erfahrungen aus einem Parallelisierungsprojekt, dessen Ziel die Portie-

rung eines Realtime-Embedded-Systems von einem Single-Core-PowerPC auf einen ARM-Prozessor mit zwei Kernen war. Die dabei getroffenen Design-Entscheidungen lassen sich jedoch auf viele Parallelisierungsprojekte übertragen. Auch die verwendeten Techniken sind nahezu universell.

Abbildung 1 zeigt die ursprüngliche Architektur des portierten Systems. Ein dedizierter IO-Thread empfängt in regelmäßigen Intervallen Messwerte aus der Außenwelt. Die Business-Logik läuft in mehreren eigenen Threads (BL-Threads). Sie berechnet in Echtzeit Steuersignale, die der IO-Thread ausgibt. Letzterer kommuniziert mit den BL-Threads über Ringpuffer.

Da die Ausgangsarchitektur für eine Single-Core-CPU entworfen wurde, verlässt sie sich an vielen Stellen darauf,

dass Threads niemals gleichzeitig laufen. Das Realtime-OS garantiert, dass stets der Thread mit der höchsten Priorität die CPU erhält. Ein sogenanntes implizites Synchronisationsmodell ist durch Deaktivieren der Interrupts realisiert. Diese Technik ist in Embedded-Systemen weit verbreitet, jedoch nicht auf Multi-Core-Hardware übertragbar.

Threads an die Leine nehmen

Will man die Performance des Systems signifikant erhöhen, muss man die Software so restrukturieren, dass Threads gleichzeitig auf mehreren Prozessorkernen laufen können. Dazu ist es notwendig, von impliziter auf explizite Thread-Synchronisation umzustellen. Außerdem muss man sicher-

stellen, dass die CPU-Kerne eine konsistente Sicht auf den gemeinsam genutzten Hauptspeicher haben.

Das ausgewählte Zielsystem ist ein klassisches symmetrisches Multiprozessorsystem (SMP), in dem alle Threads einen gemeinsamen Adressraum nutzen. Das Betriebssystem – hier Wind Rivers VxWorks – verteilt die Threads normalerweise automatisch auf die vorhandenen CPU-Kerne. Um die Umbaumaßnahmen zu begrenzen, kann es jedoch sinnvoll sein, die Threads fest an bestimmte Cores zu binden (CPU Affinity), da so das ursprüngliche Scheduling-Verhalten teilweise erhalten bleibt.

Im konkreten Fall bekam der performancehungrige IO-Thread einen eigenen Prozessorkern fest zugewiesen (Core 1), während alle BL-Threads an den anderen gebunden wurden (Core 0). Das hat unter anderem den Vorteil, dass sich das Laufzeitverhalten der Business-Logik nicht ändert – was wiederum die Migration vereinfacht.

Allerdings kann durch die starre Bindung der Threads an einen Core die Situation entstehen, dass einer dieser Threads zwar lauffähig ist, er jedoch nicht zur Ausführung kommt, obwohl auf einem anderen Core Rechenleistung zur Verfügung stünde. Ein weiteres Defizit ist die mangelnde Skalierbarkeit: Die gewählte Architektur (siehe Abb. 2) kann nicht mehr als zwei CPU-Kerne nutzen. Zwar lässt sich das beheben, doch nur mit einem Mehraufwand.

In der Ausgangsarchitektur sind Critical Sections im Code durch die Thread-Prioritäten und Annahmen über das Scheduling des Betriebssystems geschützt (implizite Synchronisation). Ein Thread, der eine Critical Section ausführen möchte, deaktiviert Interrupts, die zu einem Thread-Wechsel führen könnten. Somit kann kein anderer Thread die CPU erhalten. Das Modell ist jedoch nicht auf Multi-Core-Prozessoren übertragbar, da dort

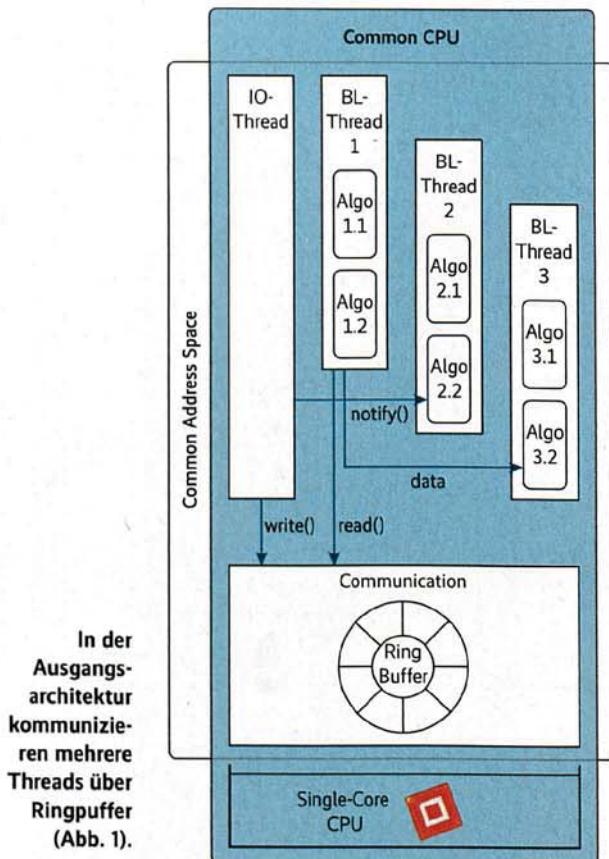
weitere Threads auf anderen CPU-Kernen laufen können.

Wie die meisten Betriebssysteme bietet VxWorks zwei explizite Synchronisationsmittel an: Semaphore und Spinlocks. Semaphore sind das klassische blockierende Synchronisationsmittel schlechthin; die Schlüsselwörter *synchronized* in Java und *lock* in C# etwa arbeiten mit Semaphoren. Nur eine vorgegebene Anzahl Threads – meist nur einer – kann einen Semaphore gleichzeitig akquirieren. Alle übrigen müssen warten, bis der „Eigentümer“ das Semaphore wieder freigibt. Zuständig für den geregelten Ablauf ist der Scheduler des Betriebssystems. Im Gegensatz dazu verwenden Spinlocks das sogenannte „Busy Waiting“: Ein Thread, der auf die Zuteilung eines Spinlocks wartet, führt pausenlos CPU-Befehle aus, die prüfen, ob das Spinlock mittlerweile frei ist.

Werkzeuge zum Synchronisieren

Semaphor-Operationen sind vergleichsweise teuer, da sie Systemaufrufe und Scheduling-Entscheidungen des Betriebssystems erfordern. Dafür benötigt ein wartender Thread bei sogenannter Contention – mehrere Threads versuchen gleichzeitig, einen Semaphore zu akquirieren – keine Rechenzeit und der Scheduler kann den CPU-Kern einem anderen Thread zuteilen.

Akquirieren und Freigeben von Spinlocks hingegen sind schnelle Operationen, die auf spezielle Prozessorbefehle zurückgreifen, ohne das Betriebssystem in Anspruch zu nehmen; bei ARM-Prozessoren sind das exklusive Load- und Store-Operationen. Allerdings gibt es einen wartenden Thread seinen CPU-Kern nicht frei, sodass der sich nicht von einem anderen Thread nutzen lässt. Je nach Anwendungsfall ist mal die eine, mal die andere Technik besser geeignet.



Für die Kommunikation zwischen IO- und BL-Threads sind im vorliegenden System Ringpuffer zuständig. In der ursprünglichen Architektur sind sie durch einen simplen „Lock-freien“ Algorithmus geschützt, der aber nur für den Single-Core-Betrieb geeignet ist. Im Multi-Core-System kommen Semaphore zum Einsatz, da sie in diesem Szenario Spinlocks überlegen sind. Der Grund: Da IO-Thread und BL-Threads auf unterschiedlichen Cores laufen, wollen sie mit sehr hoher Wahrscheinlichkeit gleichzeitig auf den Ringpuffer zugreifen (Contention). Wenn in diesem Fall ein BL-Thread auf die Zuteilung des Semaphors wartet, kann ein anderer den Prozessorkern nutzen, was mit Spinlocks nicht möglich wäre. Der beim Akquirieren und Freigeben des Semaphors eventuell eintretende Thread-Wechsel amortisiert sich, da pro Ringpuffer-Zugriff viele Daten übertragen werden und der Zugriff entsprechend lange dauert.

Untereinander kommunizieren die BL-Threads durch eigene Datenstrukturen, die in der Ausgangsarchitektur durch implizite Synchronisation geschützt sind. Dazu verwendet die Software den VxWorks-Systemaufruf *intLock()*, der auf Single-Core-Systemen Interrupts deaktiviert und so einen Thread-Wechsel verhindert. Auf einem Multi-Core-System kommen als Ersatz Semaphore, Spinlocks oder der Systemaufruf *intCpuLock()* in Frage, der Interrupts auf einem einzelnen Core unterbindet. Im vorliegenden Fall haben sich Spinlocks als die tragfähigste Lösung erwiesen, da alle BL-Threads an denselben CPU-Kern gebunden sind und der IO-Thread nur selten auf die BL-Datenstrukturen zugreift.

Bei einem Datenaustausch zwischen zwei BL-Threads kann keine Contention entstehen, da die Threads nacheinander auf demselben Core ablaufen. Das Spinlock muss also lediglich den Thread-Wechsel verhindern; es ver-



Jetzt 15%
Frühbucherrabatt
für München
sichern!

Hyper-V mit Windows Server 2012

Zwei-Tages-Seminar (zweiter Tag optional)

Mit der aktuellen Fassung von Hyper-V zielt Microsoft auf anspruchsvolle Kunden und Enterprise-Netzwerke. Höhere Skalierbarkeit, bessere Performance und Funktionen für mehr Verfügbarkeit bilden die Grundlage. Vor allem aber hat der Hersteller die Funktionen für virtuelle Netzwerke drastisch erweitert.

Der Workshop beleuchtet den Stand der Technik aus Redmond aus prinzipieller und aus praktischer Sicht. Am ersten Tag stehen neben einem umfassenden Blick auf die technischen Funktionen einige strategische Kernfragen auf dem Programm: Wie lässt sich Virtualisierung sicher betreiben? Was sollte ein Unternehmen beim Projekt-Design beachten?

Der optionale zweite Tag widmet sich der praktischen Umsetzung mit „Hands-on“-Übungen. Jeder Teilnehmer hat ein Notebook zur Verfügung und wird Hyper-V dort einrichten und konfigurieren. Am Ende des Tages verfügt das Workshop-Netzwerk dann über eine anspruchsvolle Cluster-Architektur mit Hyper-V unter Windows Server 2012.

Termine:
5. - 6. November, Köln
5. - 6. Dezember, München

Teilnahmegebühr:
1-Tages-Ticket:
599,00 Euro zzgl. MwSt.
(712,81 Euro inkl. MwSt.)

2-Tages-Ticket:
1.349,00 Euro zzgl. MwSt.
(1.605,31 Euro inkl. MwSt.)

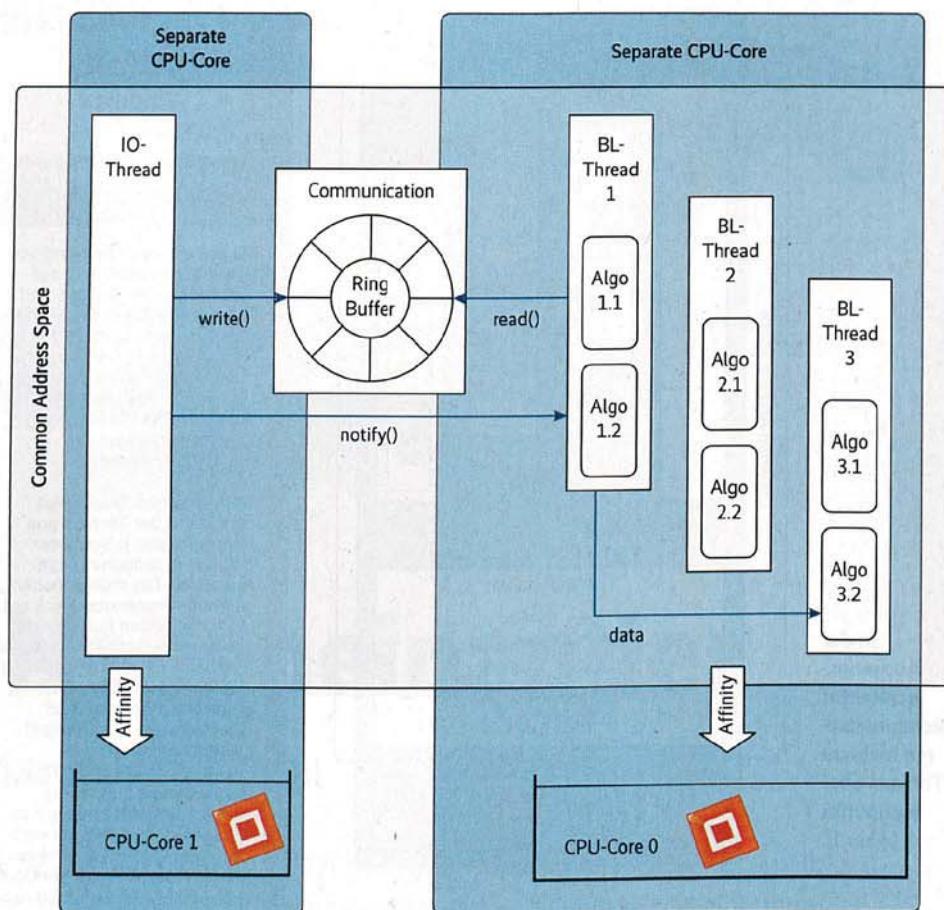
www.heise.de/hyperv2013

Referent



Nils Kaczenski verfügt über fast 30 Jahre IT-Erfahrung. Seit Mitte der Neunzigerjahre ist er als Consultant für Windows-Netzwerke tätig und berät Firmen in technischen und strategischen Fragen.

Eine Veranstaltung von: Organisiert von:
 heise Events
Conferences, Seminars, Workshops



Die neue Architektur reserviert einen CPU-Kern für den performancehungrigen IO-Thread (Abb. 2).

hält sich Core-lokal wie ein Interrupt-Lock und ist mit diesem Mechanismus implementiert (Aufruf von `intCpuLock()`).

Wollen zwei Threads auf verschiedenen Cores – der IO-Thread und ein BL-Thread – gleichzeitig das Spinlock aquirieren, sind zwei Fälle zu unterscheiden. Gewinnt der BL-Thread, muss der IO-Thread warten (Busy Waiting). Da jedoch aufgrund der eingesetzten CPU-Affinity kein anderer Thread den Core des IO-Thread nutzen kann, geht lediglich Rechenzeit verloren, aber keine Performance. Gewinnt hingegen der IO-Thread, verhindert der auf das Spinlock wartende BL-Thread, dass auf Core 0 ein anderer Thread zum Zug kommt. Dieser Fall tritt jedoch so selten auf, dass der Performanceverlust im Rahmen bleibt. Außerdem sind die Critical Sections und damit die Wartezeit relativ

kurz, da jeweils nur ein einzelner Wert übertragen wird.

Unterschiedliche Perspektiven

Generell bieten sich Spinlocks dann an, wenn eine geringe Wahrscheinlichkeit für Contention besteht und die Critical Sections relativ kurz sind. Ein Thread-Wechsel, wie er beim Einsatz von Semaphoren stattfinden kann, amortisiert sich in solchen Fällen nicht. Die Entscheidung gegen Semaphore hatte jedoch im beschriebenen Projekt noch einen anderen Grund: Sie können zu zusätzlichen Thread-Wechseln innerhalb der Business-Logik und dadurch zu einem veränderten Verhalten führen, was einen größeren Umbau der Software-Architektur erfordert hätte. Die Funktion `intCpuLock()` wäre aufgrund der CPU-Affinity eine Alternative zu Spinlocks,

würde jedoch längerfristig die Skalierung auf mehr als zwei CPU-Kerne behindern.

Moderne Multi-Core-Prozessoren nehmen sich einige Freiheiten beim Umgang mit Schreib- und Leseoperationen im Hauptspeicher. So kann etwa die CPU oder die Cache-Hierarchie die Reihenfolge der Operationen ändern. Das kommt der Performance zugute, kann jedoch dazu führen, dass ein Thread Zuweisungen an Variablen in einer anderen Reihenfolge „sieht“, als der schreibende Thread sie ausführt. Ein solches „relaxed consistent memory model“ findet man bei diversen Prozessoren, unter anderem bei der im Zielsystem eingesetzten ARM-CPU.

Im vorliegenden System steuert der IO-Thread den Arbeitszyklus, indem er beim Eintreffen neuer Daten einen Zykluszähler im Speicher aktualisiert. Da die BL-Threads

auf dem anderen Core laufen, kann es vorkommen, dass der lesende BL-Thread zwar den korrekten Wert aus dem Zykluszähler liest, aber veraltete Daten sieht. Deshalb stellt der Prozessor sogenannte Memory-Barrier-Instruktionen bereit, die das Umordnen der Speicherzugriffe einschränken: Mit ihnen kann man etwa die CPU zwingen, alle ausstehenden Zugriffe vor der „Barriere“ abzuschließen, bevor sie neue in Angriff nimmt. Das Einfügen solcher Memory-Barsiers bei den Zugriffen auf den Zykluszähler und die zu übertragenden Daten stellt sicher, dass der lesende und der schreibende Thread eine konsistente Sicht auf den gemeinsamen Speicher haben: Der lesende Thread sieht immer zusammengehörende Werte des Zykluszählers und der Daten.

Fazit

Parallelisierung von Legacy-Software erfordert zunächst eine genaue Analyse der vorhandenen Softwarearchitektur, die implizite Annahmen über zeitliche Abläufe aufdeckt. Die notwendigen Redesign-Maßnahmen lassen sich grob in drei Bereiche unterteilen: Parallelisierung, Synchronisation und Handhabung des Memory-Modells.

Generell gilt es, einen Kompromiss zwischen der Performance und dem Aufwand für den Umbau zu finden. Bei der Wahl der Synchronisationsmittel muss man deren spezifische Eigenschaften in puncto Performance und Einfluss auf das Scheduling genau betrachten. Außerdem sollten Entwickler mit den Eigenheiten der Zielhardware vertraut sein, damit sie die Implikationen auf die eigene Anwendung einschätzen können. (mr)

Marwan Abu-Khalil

arbeitet als Softwarearchitekt für Parallelisierung und verteilte Systeme bei der Siemens AG.



extra Oktobe
2013

Security

Dienste und Werkzeuge zum Identity-Management

Identity-Management
und die Cloud

Sichere Identitäten
für alles und alle

Seite II

Vorschau: Storage

Speicher aus der Cloud

Seite VII



iX extra zum Nachschlagen:

www.ix.de/extra

Sichere Identitäten für alles und alle

Identity-Management und die Cloud

Identity- und Access-Management (IAM) für unternehmensinterne Benutzer und interne Anwendungen reicht heutzutage nicht mehr aus. Cloud-Anwendungen, externe Benutzer, mobile Zugriffe und „Social-Logins“ erfordern neue Ansätze. IAM-Lösungen in der Cloud und für die Cloud liefern Antworten.

Wie so oft in der IT gibt es nicht die eine richtige Antwort, um die Herausforderungen eines „Identity-Management für die Cloud“ zu meistern. Identity-Management für die Cloud, und hier muss zwingend „Access-Management“ hinzugefügt werden, macht nur einen Teil der zu lösenden Probleme aus. Die dafür Verantwortlichen hatten nämlich bisher meist hauptsächlich auf interne Anwendungen und eine begrenzte Gruppe von Benutzern – Mitarbeiter und ein paar Geschäftspartner – ausgerichtete IAM-Infrastrukturen zu

verwalten. Natürlich gibt es in vielen Firmen auch Lösungen für externe Benutzergruppen, etwa Geschäftspartner und Kunden. Doch die stehen häufig weitgehend isoliert von der Kern-IAM-Infrastruktur zur Verfügung. Diese „Punktlösungen“ reichen jetzt aber nicht mehr aus, und der Veränderungsdruck auf die IT ist in diesem Bereich hoch.

Unternehmen müssen immer mehr Geschäftsprozesse umsetzen, in die externe Benutzergruppen wie neue Geschäftspartner und Kunden einzubinden sind (Abb. 1). In vielen

Organisationen fordern die Beteiligten ein schnelles „Onboarding“ und sicheres „Offboarding“ etwa von Externen, weil im Zuge der Veränderung von Geschäftsmodellen, Geschäftsprozessen und Vertriebswegen beispielsweise schnell Kooperationen mit externen Vertriebspartnern aufgebaut, aber auch beendet werden müssen.

Es gibt kaum noch Firmen, in denen nicht die Forderung nach Nutzung von Cloud-Diensten wie salesforce.com oder Microsoft Office 365 als SaaS-Anwendung (Software as a Service), oder die AWS (Amazon Web Services) als IaaS-Infrastruktur (Infrastructure as a Service) besteht. Selbst wenn sich dieser Trend als Folge der NSA-Affäre vielleicht etwas verlangsamt, bleibt doch die grundsätzliche Notwendigkeit bestehen, auch für solche Infrastrukturen IAM-Dienste anzubieten.

Neue Herausforderungen für das IAM

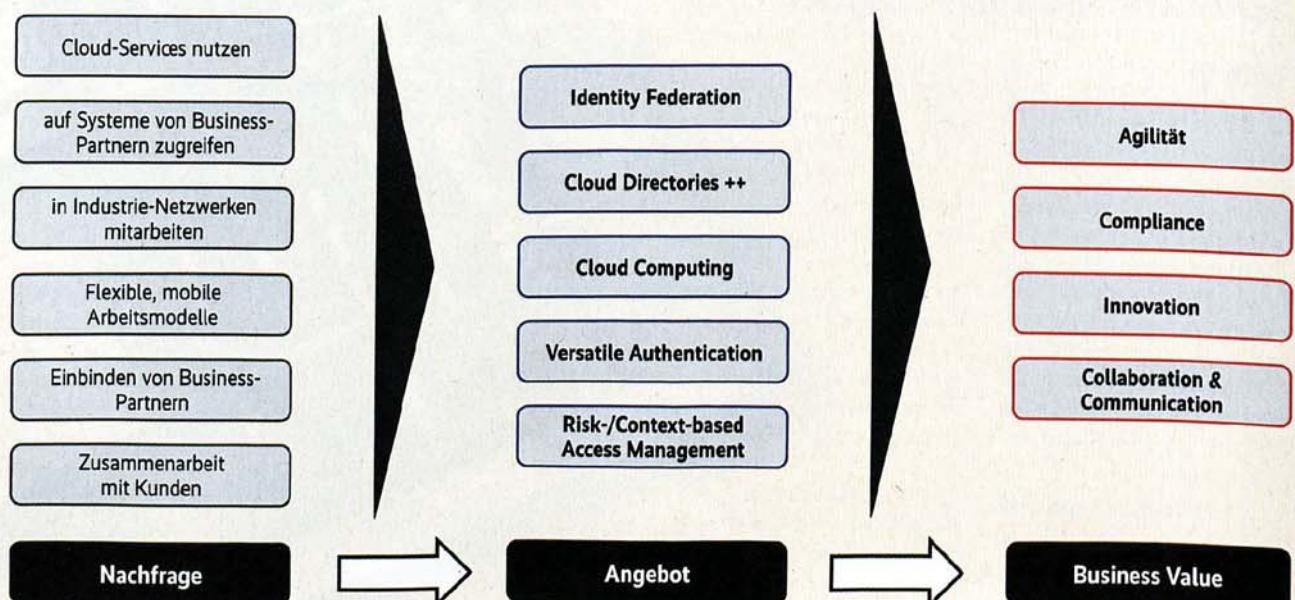
Darüber hinaus muss die IT in der Lage sein, mit immer mehr Identitäten umzugehen. BYOI (Bring Your Own Identity) heißt das Stichwort und es soll den Nutzern ermöglichen, vorhandene digitale Identitäten für den Zugriff zu nutzen. Ein Kunde

soll beispielsweise sein Facebook- oder Google-Login verwenden können, um sich zu authentifizieren. Falls er dann aber etwas kauft, muss auch ein möglichst reibungsloser Wechsel auf eine andere, stärkere Identität oder eine direkte Registrierung möglich sein.

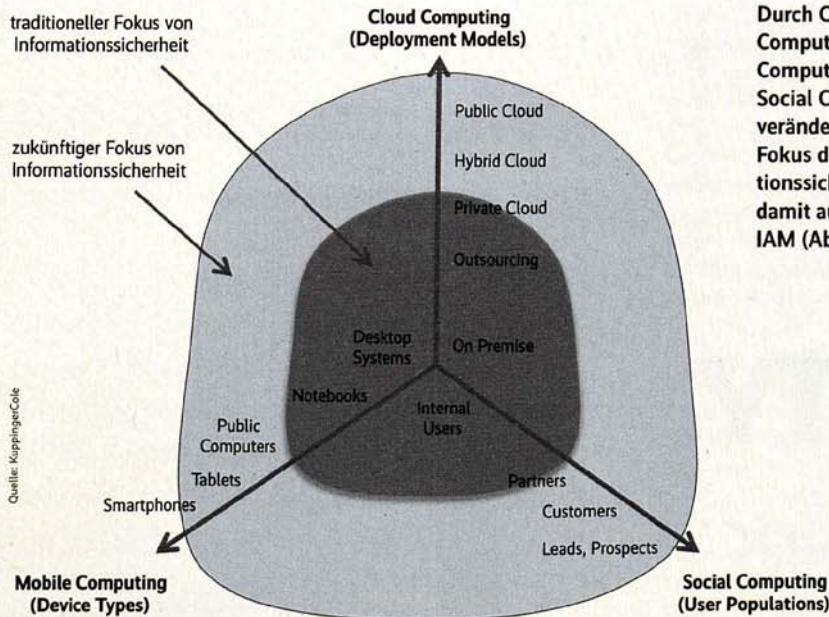
Manche Dienste lassen sich on Premise überhaupt nicht mehr umsetzen: Wenn der Geschäftspartner oder Kunde eines Unternehmens auf einen Cloud-Dienst zugreift, den dieses Unternehmen bereitstellt, dann hat er zunächst keinen direkten Bezugspunkt mehr mit der internen IT des Unternehmens – der Zugriff erfolgt direkt vom Nutzer auf die Cloud.

Generell ist die Erfordernis zur Anpassung des IAM groß, weil die sogenannte „Computing Troika“, bestehend aus Cloud Computing, Mobile Computing und Social Computing in Kombination mit dem Wettbewerbsdruck bei den Unternehmen neue Lösungen erzwingen (Abb. 2).

Wie immer, wenn sich neue Trends abzeichnen, gibt es viele Produkte, die Abhilfe für die anstehenden Probleme versprechen. Und ebenso gilt, dass die meisten zwar durchaus einen Teil der Herausforderungen meistern können, dass es aber doch nicht die sprichwörtliche



Die IT muss externe Benutzer und Dienste unterstützen, um die Anforderungen des Business zu erfüllen (Abb. 1).



„eierlegende Wollmilchsau“ gibt.

Die Schwierigkeit im Bereich IAM besteht vor allem darin, dass es eben nicht eine spezielle Technologie gibt, sondern dass IAM der Überbegriff für eine Vielzahl von Technologien für das Management von (Benutzer-)Identitäten und Zugriffs-berechtigungen ist. Dazu gehören Verzeichnisdienste, in denen Identitätsdaten gespeichert sind, und Provisioning, um Änderungen auf verschiedene Verzeichnisse zu verteilen.

IAM: Mehr als nur Benutzermanagement

Des Weiteren macht Access Governance einen wichtigen Bereich aus, den mit ihr kann man Zugriffs-berechtigungen verwalten und analysieren. Single Sign-on, um Benutzern mit nur einer Anmeldung Zugriff auf viele Anwendungen zu geben, gehört ebenso dazu wie die Identity Federation, wobei ein Identity Provider (IdP) die Authentifizierung mit standard-konformen Mechanismen übernimmt, während ein Service Provider (SP) oder eine Relying Party (RP), die dem IdP vertraut, die Autorisierung durchführt. Web-Access-Management – eine Art Gateway für die Authentifizierung und Au-

torisierung von Zugriffen von Benutzern auf bestehende Webanwendungen – ist ebenfalls ein Teil von IAM.

Neben dieser keineswegs vollständigen Aufzählung der Kernelemente gibt es viele weitere Technologien rund um das IAM. Ansätze für die starke Authentifizierung, PKIs (Public Key Infrastructures), Information Rights Management (IRM) und auch Technologien, bei denen die physische Authentifizierung beispielsweise beim Zugang zu einem Unternehmen und die logische Authentifizierung beim Zugriff auf IT-Systeme kombiniert werden, spielen eine Rolle. Und selbst nationale ID-Karten sind zumindest ein Randthema des IAM.

Diese Vielfalt an Technologien rund um das Thema Identitäten macht deutlich, dass es keine einfachen Antworten auf die Frage geben kann, wie Identity-Management für die Cloud „richtig“ aufzusetzen ist. Das gilt umso mehr, als die Antwort keineswegs in einem Identity-Management für die interne IT und einem für Cloud-Dienste mit voneinander getrennter Verwaltung zu suchen ist. Vielmehr geht es darum, die bestehende IAM-Infrastruktur so weiterzu entwickeln, dass sie auch die neuen Herausforderungen meistern kann (Abb. 3).

Durch Cloud Computing, Mobile Computing und Social Computing verändert sich der Fokus der Informationssicherheit und damit auch von IAM (Abb. 2).

durchzuführen ist, oder ob es eine standardisierte Lösung ist, mit der der Kunde schnell starten kann, weil er auf Best Practices für Prozesse et cetera zugreifen kann.

Grundsätzlich gilt, dass das Angebot hier immer reichhaltiger und besser wird und die Möglichkeiten, IAM-Infrastrukturen in die Cloud auszulagern, auch. Achtung: Da hier zwangsläufig personenbezogene Daten involviert sind, sollten die Verantwortlichen die datenschutzrechtliche Problematik nicht unterschätzen.

SSO und Zugriffsmanagement

Neben dieser Verlagerung von Kernfunktionen in die Cloud passiert vor allem in einem Bereich des IAM aus der Cloud einiges: Es betrifft Single Sign-on und die Zugriffssteuerung für verschiedene Cloud-Dienste. Hier haben sich schon früh einige Start-ups wie Symplified und Okta positioniert. Inzwischen sind aber auch viele der etablierten Anbieter in diesem Marktsegment aktiv.

Die Grundidee dahinter ist, den Benutzern ein Single Sign-on für Cloud-Dienste zu ermöglichen. Das geht prinzipiell auch auf Basis etablierter, interner Enterprise-Single-Sign-on-Lösungen (E-SSO), weil Cloud-Dienste aus Sicht der Benutzer nichts anderes sind als Webanwendungen. Allerdings lassen sich mit E-SSO die Zugriffe externer Benutzer nicht oder nur eingeschränkt verwalten.

Anbieter wie Ping Identity mit PingOne oder RSA mit Adaptive Federation bieten Cloud-Dienste an, mit denen Benutzer über ein Portal auf „ihre“ Cloud-Dienste zugreifen können. Die Dienste arbeiten mit bestehenden Verzeichnisdiensten zusammen und können Benutzer authentifizieren. Sie verbinden diese dann mit den Cloud-Diensten und liefern über die Federation-Standards wie SAML v2 (Security Assertion Markup Language) die Bestätigung für die erfolgreiche

Security

Die Authentifizierung von Benutzern und das Management von Zugriffen wird mit der Cloud komplexer (Abb. 3).

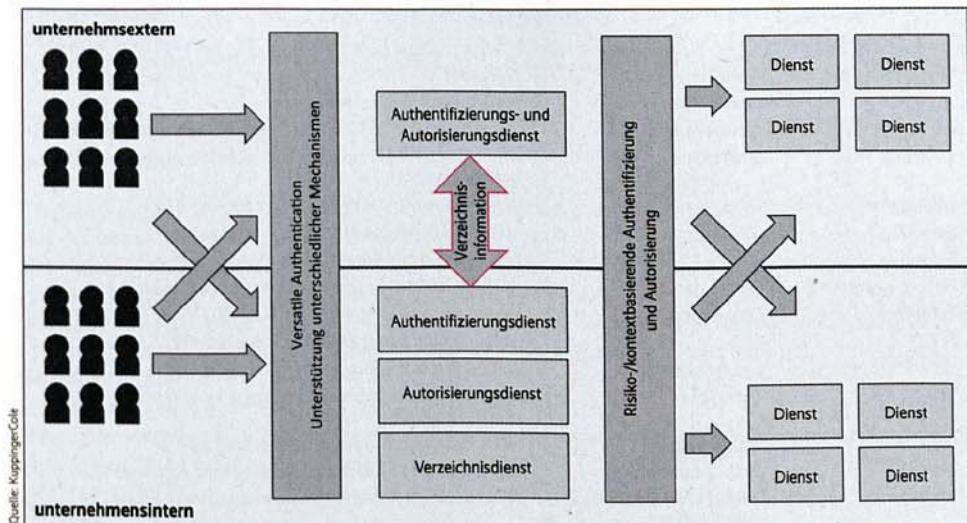
Authentifizierung und bei Bedarf weitere Attribute.

Dieser Markt ist einigermaßen unübersichtlich, nicht zuletzt weil die Zahl der Anbieter sowohl durch neue Start-ups als auch durch neue Angebote der etablierten Hersteller wächst.

Starke Authentifizierung aus der Cloud

Es gibt auch Anbieter, die zunächst mit Angeboten für die starke Authentifizierung in der Cloud gestartet sind, inzwischen ihre Funktionen ausweiten und zusätzlich das Management von Benutzern sowie die Federation mit Cloud-Diensten unterstützen. Ein Beispiel in diesem Bereich ist SecureAuth, die ursprünglich eine Zwei-Faktor-Authentifizierung als Cloud-Dienst anboten, um einen sicheren Zugriff auf Cloud-Dienste sowie auf On-Premise-Anwendungen zu ermöglichen.

Daneben gibt es aber auch eine Reihe von spezialisierten Lösungen für eine starke Authentifizierung als Cloud-Dienst. Dazu gehören sowohl etablierte Angebote als auch die zahlreichen Start-ups. Kaum ein anderer Bereich des



IAM weist derzeit eine vergleichbare Dynamik auf. Hintergrund dafür ist wohl die inzwischen allgemein akzeptierte Erkenntnis, dass Kennwörter für die Authentifizierung nicht ausreichend sicher sind. Des Weiteren gibt es im Zusammenhang mit BYOI viele neue Angebote, die versprechen, eine sichere Authentifizierung ohne den logistischen Aufwand der Verteilung und des Managements beispielsweise von Hardware-Tokens als Cloud-Dienst bereitzustellen. Hier wird es zweifelsohne interessant sein, zu sehen, welche Verfahren und Hersteller sich am Ende durchsetzen können.

Zwei Schwergewichte auf dem Markt

Den größten Einfluss auf die weitere Entwicklung von IAM

für die Cloud und aus der Cloud dürften aber neue Angebote zweier Schwergewichte im Markt haben: salesforce.com und Microsoft. Während Microsoft schon lange mit Verzeichnisdiensten im Bereich des On-Premise-IAM aktiv ist (schon seit der Einführung des LAN-Managers, noch lange vor der Einführung des Active Directory), ist salesforce.com ein Anbieter, den man in diesem Markt bis vor Kurzem eher nicht erwartet hätte.

salesforce.com setzt darauf, von seiner Plattform aus die Funktionen für das Verwalten und Speichern von Benutzern (Verzeichnisdienste) und die Federation-Dienste zu anderen Plattformen anzubieten. Der Hersteller möchte damit seine starke Position im Bereich der Interaktion von Unternehmen mit ihren Kunden nutzen und

ausbauen – das Management von Identitäten und Zugriffen wird als strategisches Thema betrachtet.

Kreative Ideen aus Redmond

Den potenziell größten Einfluss auf den IAM-Markt insgesamt und Cloud-IAM im Speziellen hat aber wohl Microsoft. Seit Kurzem ist das Azure Active Directory (AAD) offiziell verfügbar. Ganz neu ist das AAD allerdings nicht, weil es schon seit einiger Zeit als Backend-Infrastruktur für Microsoft Office 365 und Microsoft Intune verwendet wird. Dieser Ansatz ist deshalb so wichtig, weil er die hohe Skalierbarkeit des AAD belegt – und Skalierbarkeit ist beim Cloud-IAM, vor allem wenn Unternehmen die Zugriffe von potenziell Millionen von



FSP

SOFTWARE & CONSULTING
Wettbewerbsvorteile aus einer Hand.

Congress@it-sa: FSP GmbH Software & Consulting

Access Management: Umsetzung und Zertifizierung

9. Oktober 2013 13 bis 17 Uhr

Praxisberichte:

- Integration eines Access Management Systems in eine bestehende Systemlandschaft
- WebSecurity: Realisierung eines ganzheitlichen IAM-Konzepts für einen Versicherungskonzern
- Access Governancekonzepte und Re-/Zertifizierungskonzepte



Besuchen Sie uns in
Halle 12, Stand 109

Jetzt kostenlose
Kongresstickets
sichern

Informationen unter:
messe.fsp-gmbh.com



Anbieter von Identity- und Access-Management für die Cloud

Hersteller	Produkt	Website
Aveksa	IAM Platform	www.aveksa.com/products/cloud/
CA	CloudMinder	www.ca.com/us/lpg/cloud-minder-microsite/ca-cloud-minder
Courion	CourionLive	www.courion.com/products/cloud-based-identity-access-management.html
DELL Software	Quest One Identity	www.quest.com/identity-administration/
EmpowerID	SSO Platform	www.empowerid.com/solutions/singlesignon
Evidian	Identity & Access Manager	www.evidian.com/iam/identity-access-manager/
Fischer International	Fischer Identity	www.fischerinternational.com/competencies/overview.htm
ForgeRock	Open Identity Stack	forgerock.com/category/products-services/
FSP	ORG	www.fsp-gmbh.com/de/softwareprodukte/org/
Hitachi ID Systems	Identity Manager	hitachi-id.com/identity-manager/
IBM	Tivoli Suite	www-01.ibm.com/software/tivoli/governance/security/identity-access-mgmt.html
Identropy	SCUID Platform	www.identropy.com/products/scuid-platform/
McAfee	Cloud Identity Manager	www.mcafee.com/de/products/cloud-identity-manager.aspx
Microsoft	Forefront Identity Manager & Access Platform	www.microsoft.com/en-us/server-cloud/identity-access
NetIQ	Identity Manager	https://www.netiq.com/de-de/products/identity-manager/advanced/
Omada	Identity Suite	www.omada.net/omada-identity-suite-417.aspx
Oracle	Identity Management	www.oracle.com/technetwork/middleware/id-mgmt/overview/index.html
Ping Identity	PingFederate	https://www.pingidentity.com/our-solutions/SSO-and-Federated-Identity.cfm
RMS Software	IdM	www.rm5software.com/products/rm5idm/overview
SailPoint	IdentityIQ	www.sailpoint.com
SecureAuth	SecureAuth Identity Provider	www.secureauth.com/identity-governance/identity-management/
Simeio Solutions	Enterprise IAM	www.simeiosolutions.com/
Stonesoft	A2Cloud	www.stonesoft.com
ViewDS	Identity Solution Suite	www.viewds.com/products.html

Die Übersicht erhebt keinen Anspruch auf Vollständigkeit.

Kunden verwalten wollen, eine Kernanforderung.

AD und AAD im Doppelpack

Auch wenn das AAD den Begriff „Active Directory“ im Namen trägt, handelt es sich nicht einfach um die Portierung des

klassischen Active Directory in die Cloud. Das wird schon daran deutlich, dass das AAD einerseits keine LDAP-Schnittstelle hat (die sich aber potenziell implementieren lässt), andererseits aber auch Identity Federation und die Autorisierung von Zugriffen auf Cloud-Dienste unterstützt.

Das AAD kann in bestehenden Active-Directory-Infrastrukturen über ADFS (Active Directory Federation Services) oder Synchronisierungswerzeuge integriert werden (Abb. 4). Die Absicht dahinter ist, dort Benutzer wie Kunden und Geschäftspartner zu verwalten, die das Unternehmen nicht im Active Directo-

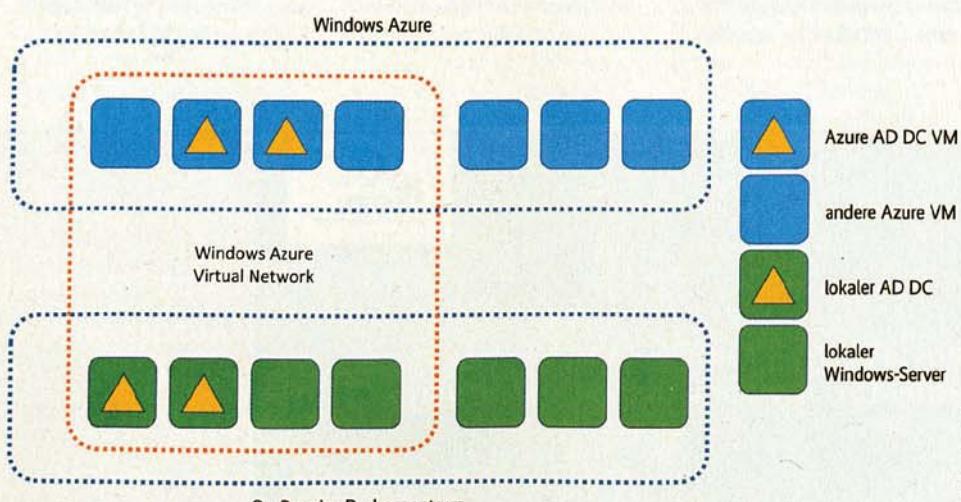
ry verwalten möchte oder kann. Die Verwaltung externer Benutzer ist sowohl unter dem Aspekt der Sicherheit als auch des Designs der Verzeichnisstruktur bisher eine große Herausforderung für Active-Directory-Verantwortliche gewesen. Das ändert sich nun, weil das AAD genau darauf ausgelegt ist. Viele Administratoren werden sich sicher auch darüber freuen, dass das Schema des AAD hochflexibel ist – bisher lässt der Begriff „Schema-Änderung“ ja bei ihnen eher die Alarmglocken läuten.

Mit dem AAD hat Microsoft nun eine Lösung, die das Active Directory in die Cloud erweitert, externe Benutzer verwaltet und Zugriffe auf Cloud-Applikationen steuert. Mit einer Graph API kann das AAD über REST-API-Informationen einfach durchsucht werden.

Darüber hinaus gibt es auch für diesen Bereich Service Provider, die zum Teil schon seit vielen Jahren im Markt aktiv sind, etwa Exostar und Covisint, beide bereits in der Zeit der damaligen „New Economy“ vor der Jahrtausendwende im Zuge der damals aufkommenden B2B-Marktplätze entstanden. Sie bieten für verschiedene Branchen, zum Beispiel die Automobilindustrie, Dienste an, mit denen Hersteller und Zulieferer die Identitäten der Benutzer verwalten können, die auf Dienste von Geschäftspartnern zugreifen müssen.

IRM: Ein wichtiger Randbereich

Ein Randthema bei IAM in der Cloud, das aber gerade in Folge der aktuellen Diskussionen um die Rolle der NSA wieder verstärkt ins Blickfeld rückt, ist das Information Rights Management (IRM), das dabei hilft, Dokumente zu verschlüsseln und mit Zugriffsberechtigungen zu versehen. Nur authentifizierte Benutzer können diese Dokumente wieder entschlüsseln. Die Anwendungen – soweit sie für IRM aktiviert sind – setzen dann die definierten Zugriffs-berechtigungen durch.



Windows Azure kann auch klassische Active-Directory-Domänencontroller hosten (Abb. 4).

Der Vorteil von IRM ist die Ende-zu-Ende-Sicherheit beim Austausch von Informationen, was sowohl mit Blick auf die Informationssicherheitsrisiken im Internet – wer hört mit und wo landen die gesammelten Daten – als auch vor dem Hintergrund der steigenden Compliance-Anforderungen wichtig ist.

Bisher ist IRM nicht sehr häufig im Einsatz, trotz der offensichtlichen Vorteile als Technologie, die Informationen beim Speichern, Übertragen und Nutzen durchgängig schützt. Die größten Hürden waren bisher die eingeschränkte Unterstützung von Anwendungen, das Einbinden von externen Kommunikationspartnern und die hohe Komplexität bezüglich Implementierung und Betrieb.

Auch hier hat Microsoft Pläne und wird mit Azure RMS eine Weiterentwicklung der etablierten Windows RMS (Rights Management Services) herausbringen. Die Lösung liefert eine viel breitere Unterstützung von Anwendungen und Geräten als bisher und legt viele Funktionen in die Cloud, sodass externe Kommunikationspartner einfach eingebunden werden können und der Aufbau der Infrastruktur vereinfacht wird. Gleichzeitig kann man die Schlüssel auch on Premise in einem HMS (Hardware Security Module) verwalten. Azure RMS hat überdies das Potenzial, diesen Markt zu verändern und das Zugriffsmanagement nicht mehr nur auf System- und

Dienstebene, sondern auch auf Dokumentenebene zu etablieren.

Ohne IAM-Strategie geht es nicht

Die gute Nachricht ist: Es tut sich viel bezüglich IAM in der Cloud und für die Cloud. Die schlechte Nachricht, es gibt nicht den einen Lösungsansatz, den Unternehmen brauchen. Der Markt ist noch stark in Bewegung und die Marktsegmente sind noch nicht so klar definiert, wie es im klassischen

IAM bei Identity Provisioning oder Access Governance der Fall ist, wo es Lösungen gibt, an denen Unternehmen kaum vorbeikommen.

Deshalb sind für Anwender zwei Aspekte besonders wichtig. Einerseits sollten Anwender Unternehmen taktische Punktlösungen vermeiden. Der Zugriff von unterschiedlichen Benutzergruppen sowohl auf interne als auch externe Anwendungen ist eine strategische Herausforderung für die Informationssicherheit. Das führt zum zweiten Aspekt: Unternehmen

müssen eine Strategie entwickeln, die verschiedene heute bestehende und zu erwartende Szenarien identifiziert, um dann einen Lösungsansatz zu entwickeln, mit dem sich die bestehende IAM-Infrastruktur entsprechend weiterentwickeln lässt. Das ist heute schon möglich und lässt Anwender die nötigen Schritte gehen und gleichzeitig strategisch die Cloud-IAM-Infrastruktur für die Zukunft aufzubauen. (ur)

Martin Kuppinger ist Gründer und Principal Analyst bei KuppingerCole.

In iX extra 11/2013 Storage: Speicher aus der Cloud

Beweggründe, Daten in die Public Cloud zu verlagern, gibt es viele: Die einen nutzen die Angebote für Backups, die nächsten lagern ihre digitalen Archive dorthin aus, andere stellen dort Daten an Dritte bereit, wieder andere nutzen die Cloud als Zwischenlager bei kurzzeitigen Engpässen und manch einer denkt darüber nach, die eigene Storage-Hardware durch Cloud-Angebote zu ersetzen. Doch

ganz so trivial, wie es auf den ersten Blick erscheint, ist das Abgeben von unternehmenseigenen Daten an Dritte nicht und nicht jeder Anbieter eignet sich für jeden Kunden.

Wohl auch deshalb kommt jetzt neben der Public Cloud mit ihren mietbaren Ressourcen die Private Cloud in Fahrt, die Firmen intern und ausschließlich für eigene Zwecke aufsetzen, um ihren Speicherzoo in

den Griff zu bekommen und ihm einen neuen Anstrich zu geben. iX extra gibt einen Überblick über die für Firmen tauglichen Angebote und Trends und geht der Frage nach, worin der Wandel vom Storage Area Network zur Private Cloud eigentlich besteht und was sich dadurch ändert.

Erscheinungstermin:
24. Oktober 2013

Die weiteren iX extras:

Ausgabe	Thema	Erscheinungstermin
12/13 Networking	Gigabit-WLAN – Konkurrenz fürs Kabel?	21. 11. 13
01/14 Security	Lösungen gegen Malware-Angriffe	19. 12. 13
03/14 Security	Endpoint-Sicherheit	Februar 2014



dpunkt.verlag präsentiert

Programmieren mit Android



Einstieg in die Programmierung von Android-Apps

Anhand von praxisnahen Beispielen mit vielen Übungen wird gezeigt, wie man Android-Apps entwickelt, die sowohl auf dem Smartphone als auch auf dem Tablet laufen. Die Teilnehmer lernen, wie man den Emulator richtig nutzt und welche Werkzeuge wirklich weiterhelfen. Vom Anlegen eines Projekts bis zum lauffähigen Programm werden die Komponenten von Android vorgestellt und ihr Einsatzzweck erklärt. Die Teilnehmer lernen das Arbeiten mit dem Android-SDK kennen und die wichtigsten Klassen der Android-API zu verwenden. Von der Oberflächengestaltung über Hintergrund-

prozesse und Persistenz bis zu Location Based Services werden die wichtigsten Komponenten von Android implementiert und im Emulator getestet.

Zielgruppe:

Android-Anfänger, Java-Programmierer
Die Teilnehmerzahl ist auf 20 Personen begrenzt!

Termin: 10. - 11. Oktober in Heidelberg

www.dpunkt.de/workshop_android



Yeoman: Werkzeugsammlung für Web-Apps

Ein Auge drauf

Roland Eckl

Gute Webwerkzeuge erfreuen sich großer Beliebtheit. Das von Google stammende Paket Yeoman enthält mehrere Open-Source-Tools und hilft unter anderem durch klare Strukturierung, Arbeitszeit zu sparen.

Zu den immer wichtigeren mobilen Anwendungen gehören nicht nur native Apps, sondern darüber hinaus Web-Apps, die aus HTML5, CSS und JavaScript bestehen. Webentwickler können sie gleich für mehrere Plattformen umsetzen. Hilfe bietet die Tool-Sammlung Yeoman.

Hat man früher oft lediglich ein paar Zeilen JavaScript-Code für die eigene In-

ternet-Präsenz in die Tastatur gehackt, etwa um kleine Mouseover-Effekte oder eine relativ einfache Überprüfung der Nutzereingaben vorzunehmen, so liegen heute ganze in der Sprache geschriebene Anwendungen vor. Der Anteil des professionellen JavaScript-Codes wächst beständig und bekommt nun die Rolle einer Basistechnik, statt sich mit der netten Dreingabe für diverse Spielereien begnü-

gen zu müssen. Denn wer heute noch in seinem Browser JavaScript deaktiviert, blickt auf vielen Seiten in die Röhre.

Damit einhergehend stellen Anwender nun an Webanwendungen andere Ansprüche. Das bezieht sich auf die Entwicklung wie auf die Umsetzung. Für Erstere sollten Tools und Bibliotheken gut aufeinander abgestimmt sein. Darauf hinaus muss die Qualität der Ergebnisse stimmen. Zum Glück gibt es für fast alles schon das eine oder andere Werkzeug im Netz, man muss sie sich nur erst zusammensuchen. Und genau hier greift Google mit Yeoman an, indem es einen ganzen Technik-Stack, die geschickte Integration ausgesuchter Tools, in Form eines Open-Source-Projekts zur Verfügung stellt. Selbst Neulinge in der JavaScript-Welt sind dadurch in der Lage, aus dem Stand heraus etablierte Entwicklungswerzeuge einzusetzen.

Das Team um Paul Irish und Addy Osmani präsentierte die erste Version vor über einem Jahr auf der hauseigenen Google-I/O-Konferenz. Sie zeigten, wie einfach man mit Yeoman neue Anwendungen anlegen und Bibliotheken samt Abhängigkeiten komfortabel hinzufügen und verwalten kann (zu Video-Clips siehe „Alle Links“). Von Anfang an haben sie an das Optimieren, Bauen und Testen der Anwendungen sowie zahlreiche weitere Facetten der Webentwicklung mit JavaScript gedacht.

Nicht ohne die Werkzeuge Bower, Grunt und Yo

Als Grundlage dienten damals Grunt (siehe dazu den *iX*-Artikel [1]) und Bower (zu allen Werkzeugen versammeln „Alle Links“ die Verweise). Ersteres ist ein sogenannter Task-Runner für alles, was nur im Entfernen einem Build-Prozess ähnelt, quasi das *make* für JavaScript. Bei Bower handelt es sich hingegen um ein Package Management System, ursprünglich von Twitter entwickelt. Es hilft mitunter, die verschiedenen JavaScript-Bibliotheken über einen zentralen Weg zu finden und deren Abhängigkeiten untereinander zu meistern. Beide Tools, wie Yeoman selbst, laufen in der Node.js-Runtime (siehe wiederum einen *iX*-Artikel, [2]) und sind vollständig in JavaScript geschrieben.

Anfangs gab es einige Kritikpunkte an Yeoman; erstaunlicherweise ging es dabei häufig um eine vielleicht gar zu tiefe Integration. So schreckten die Macher von Yeoman nicht davor zurück, die einzelnen Teile so zurechtzubiegen, dass sie ih-

re ganz individuellen Vorstellungen umsetzen konnten. Insbesondere Grunt haben sie dermaßen verändert und erweitert, dass man von Kompatibilität zum Original-Tool nur noch bedingt sprechen konnte. Wollte man später gar nicht (mehr) auf alle Optionen von Yeoman zurückgreifen, war ein Umstieg auf Grunt nur mit Mühen oder eben nicht realisierbar. Selbst Ben Alman, der kreative Kopf hinter Grunt, war alles andere als begeistert und ließ beispielsweise im Diskussionsforum von Yeoman seinem Frust darüber freien Lauf. So tat er kund, dass viele Entwickler ihm Fehler gemeldet hätten, die allerdings nur auf die Google-Anpassung zutrafen. Die Verwirrung war deshalb groß, denn auf der Verpackung stand Grunt, und damit etwas anderes, als tatsächlich enthalten war.

Aber Google hat den Kritikern gut zugehört und mit der eben erschienenen Version 1.0 wieder eine saubere Trennung von Tools und Komponente hergestellt. Statt veränderter Klone kommen nun deren offizielle Releases zum Einsatz. Grunt und Bower werden weiterhin in selbstständigen Projekten entwickelt, aber die verschiedenen Entwickler-Teams tauschen sich nun regelmäßig untereinander aus. Das soll maximale Kompatibilität und Interoperabilität gewährleisten. Frühere Anpassungen sind inzwischen entweder in das neue und separate Projekt Yo gewandert oder aber stellen gültige Plugins für Grunt dar. Gerade der letzte Punkt ermöglicht es nun endlich, einzelne Funktionen aus dem Yeoman-Projekt in einem davon unabhängigen Grunt-Build zu verwenden. Yeoman komplett zu installieren kann man sich gegebenenfalls sparen. So partizipieren nun andere Entwickler von Googles Entwicklung, ohne deren ganzen Stack einsetzen zu müssen.

Im Folgenden soll es um die drei Kern-Tools des Stacks gehen. Vorab ein paar Worte zum Installieren. Zunächst muss NodeJS auf dem Rechner vorhanden sein. Ist es installiert, reicht folgender

```
D:\Workspaces\Playground\ix>yo webapp
Welcome to Yeoman,
ladies and gentlemen!
out of the box I include HTML5 Boilerplate, jQuery and Modernizr.
[?] Would you like to include Twitter Bootstrap for Sass?: No
[?] Would you like to include RequireJS (for AMD support)?: No
[?] Would you like to use autoprefixer for your CSS?: No
create Gruntfile.js
create package.json
create .gitignore
create .gitattributes
create .bowerrc
create bower.json
create .jshintrc
create .editorconfig
Ready
```

Alle Yeoman-Tools werden von der Kommandozeile aus bedient. Hier stellt Yo Fragen für die Web-App, bevor es das Projekt anlegt (Abb. 1).

Befehl in der Kommandozeile aus, der den Node Package Manager (NPM) beauftragt, Yo sowie ein schmales Kommandozeilen-Interface für Grunt und zu guter Letzt Bower zu installieren.

```
npm install -g yo grunt-cli bower
```

Der Parameter `-g` steht für „global“, das heißt die neuen Node-Anwendungen sind systemweit über die Kommandozeile verfügbar.

Alles übers Anlegen von Projekten

Los geht's mit Yo, dem jüngsten Spross in der Yeoman-Familie. Er kümmert sich um alles, was mit dem Anlegen neuer Projekte zu tun hat. Man spricht im Fachjargon gerne von Scaffolding. Früher hatte man sich hierfür oft sogenannter Boilerplates bedient. Dieser Begriff, ursprünglich aus den Medien beziehungsweise dem Druckwesen stammend, steht für gleichbleibende Textblöcke, die keinen direkten Bezug

zur tatsächlichen Publikation aufweisen. Ähnlich verhält es sich bei der Programmierung; man erhält eine statische Zusammenstellung von Bibliotheken, die beispielsweise von einer gemeinsamen HTML-Datei aus referenziert werden. Im Grunde handelt es sich schlicht um eine Vorlage, die schon bewährte Frameworks wie jQuery und Co enthält. Der nach wie vor bekannteste Vertreter in diesem Bereich ist HTML5 Boilerplate.

Scaffolding bedeutet hingegen, Projekte viel dynamischer zu erzeugen. Bei Yo stehen hierfür einige Generatoren zur Verfügung, die die verschiedenen Bedürfnisse bedienen sollen. Ob es sich dabei um eine einfache Web-App handelt, oder um eine komplexere mit Frameworks wie AngularJS oder vielleicht eher Backbone.js, an der Auswahl mangelt es nicht.

Generatoren sind wie die Kern-Tools über den Node Package Manager zu beziehen. Sie sind mit dem Keyword `yeoman-generator` versehen und beginnen in der Regel mit dem Prefix `generator-`. Möchte man etwa mit der Entwicklung für das neue FirefoxOS loslegen, lädt man den entsprechenden Generator per `npm install generator-firefox-os` nach. Für Backbone wäre es hingegen `npm install generator-backbone` und für die einfache Web-App ohne große Spezialitäten `npm install generator-webapp`. Wer sich erst umsehen möchte, findet eine vollständige Auflistung auf der Site für Node Package Modules (in „Alle Links“).

Will man einen Generator gleich mehrfach nutzen, kann man wieder das Flag `-g` für die systemweite Installation verwenden. Um beim nächsten Projekt jedoch nicht mit einer alten Vorlage zu

TRACT

- Das von Google im vorigen Jahr erstmals vorgestellte Paket Yeoman unterstützt die Webentwicklung durch das Zusammenspiel von Yo, Grunt und Bower – alleamt Open Source.
- Yeoman, das auf Node.js aufsetzt, hilft beispielsweise, JavaScript-Bibliotheken über einen zentralen Weg zu finden und deren Abhängigkeiten untereinander zu meistern.
- Vom Scaffolding übers Testen bis hin zum Deployment können Webentwickler ihre Arbeit Yeoman verrichten lassen.

Einzelschritte zu und mit Yeoman

Kommando	Aktionen
<code>npm -g yo grunt-cli bower</code>	systemweite (-g) Installation der drei Tools
<code>mkdir mywebapp; cd mywebapp</code>	Anlegen des Web-App-Verzeichnisses und Wechsel dorthin
<code>npm install generator-webapp</code>	lokale Installation des Generators für eine Web-App
<code>yo webapp</code>	Anlegen des Projekts
<code>grunt build</code>	Build der Anwendung
<code>grunt server</code>	Starten der Web-App über internen Webserver

arbeiten, ist es eher zu empfehlen, den Generator für jedes Projekt erneut zu ziehen. Vorlagen landen immer im Verzeichnis `node_modules` relativ zum gegenwärtigen Pfad.

Um ein neues JavaScript-Projekt anzulegen, braucht es danach nicht mehr viel. Man teilt Yo den gewünschten Generator mit, den Rest fragt das Werkzeug in einem verständlichen Dialog ab (siehe Abb. 1).

Ist dieser Schritt getan, erhält man im obigen Fall mehrere Verzeichnisse und Dateien. Im `app`-Ordner liegen die HTML- und JavaScript-Dateien der kommenden Anwendung. Daneben findet sich noch ein Ordner für Tests sowie die Dateien `bower.json`, `package.json` und `Gruntfile.js`. In der ersten Datei verwaltet Bower die Abhängigkeiten der eingesetzten Bibliotheken, die beiden anderen gehören zu Grunt und konfigurieren den Build-Prozess; dazu später mehr.

JavaScript auf dem Server erwünscht

In Zukunft dürfte es immer mehr Generatoren für die Backend-Seite geben, denn die Nachfrage steigt; viele wollen beiderseits durchgehend JavaScript einsetzen können. Ein vielversprechendes Beispiel findet sich für Express.js (ein Web Application Framework für die Node.js-Runtime) auf der Server- und AngularJS auf der Browser-Seite mit dem sogenannten Express-Stack. Bei diesen neuen Generatoren dürfte sich die Serverseite rein auf JavaScript beschränken – eben Node.js, außerdem vielleicht Helma oder RingoJS. Für alle anderen Sprachen, etwa PHP oder ASP.NET, könnte der Stack zwar die initiale Vorlage liefern, aber bei allen weiteren Schritten fehlt die Unterstützung. Vom propagierten ganzheitlichen Workflow über das Anlegen hinaus wäre man daher meilenweit entfernt.

Ist man über das Anlegen eines Projekts hinaus, kommen spätestens jetzt weitere Komponenten ins Spiel. Ein Geflecht von Abhängigkeiten will verwaltet sein. Vorweg sei nochmals daran erinnert, dass es in JavaScript kein klassisches Modularisierungskonzept gibt, wie man

es aus anderen Hochsprachen kennt. Das Paketieren oder gar Versionieren von Code und Ressourcen ist ebenfalls nicht Teil des Standards. Mit der Active Module Definition (AMD) haben Entwickler die Option, Module nachzuempfinden und zur Laufzeit Abhängigkeiten aufzulösen. Ein Modul entspricht hier einer einzelnen JavaScript-Datei.

Bündel von Dateien und mehr verwalten

Bower kümmert sich nicht um die Laufzeitspekte und beschränkt sich nicht auf Quellcode. Es handelt sich um ein Package Management System für die Entwicklung, vergleichbar mit dem Node Package Manager. Dabei spielt es keine Rolle, wie viele Dateien ein Paket ergeben und was letztlich deren konkreter Inhalt ist. Bower kann daher sowohl AMD-konforme Module (beispielsweise das weitverbreitete jQuery), Bündel von HTML- und CSS-Dateien oder eine Sammlung von Icons in Form von Paketen verwalten. Deshalb ist das Werkzeug ideal für Yeomans Zwecke, da es die aus den Generatoren erzeugten Projekte wiederum als Pakete behandeln kann und nur auf weitere Pakete zu verweisen braucht. Andere Package Manager wie Jam kümmern sich dagegen ausschließlich um JavaScript-Code und wären hier nur bedingt tauglich.

Der Node Package Manager setzt ebenfalls voraus, dass die Pakete oder Module gültige Node-Anwendungen sind beziehungsweise von solchen geladen werden können. Aber Bower stellt eine Online-Datenbank zur Verfügung, in der man beliebige Pakete und ihre Versionsstände eintragen und abfragen kann. Die bekannten Frameworks aus der Java-

Script-Welt sind hier fast vollständig enthalten, eigene Pakete können Entwickler ohne Weiteres registrieren. Momentan liegen knapp 3000 Einträge vor.

Bower funktioniert zunächst so, dass das `search`-Kommando Pakete und verschiedene Versionen findet. So listet `bower search jquery` alle registrierten Varianten und Versionen der Bibliothek auf. Wer sich nur umsehen möchte, kann im Netz stöbern (siehe „Alle Links“). Das eigene Entwicklungsprojekt wird ebenfalls schlicht als Paket behandelt und seine Abhängigkeiten sind in der JSON-Datei namens `bower.json` hinterlegt. Listing 1 zeigt eine Komponente, die ausschließlich jQuery in der aktuellen Version benötigt – `bower update` würde jQuery übrigens auf die gegebenenfalls neue Version aktualisieren.

Beim Einsatz dieser Komponente in verschiedenen Anwendungen fände sich dort in den jeweiligen `bower.json` wiederum ein Verweis auf die eigene Komponente. Das kann am eigenen Rechner über die volle Pfadangabe anstelle des Paketnamens geschehen, oder aber man registriert seine Komponente bei `bower` und stellt sie online und jedermann zur Verfügung; in diesem Fall sollte sie allerdings von ausreichend öffentlichem Interesse sein.

Grunt: Alles für den Entwicklungsprozess

Bei Grunt dreht es sich nicht um Frameworks, sondern alles rund um den Entwicklungsprozess: ein umfangreiches Build-System, das es erlaubt, fast alles zu automatisieren. Der manuelle Aufruf unterschiedlicher Tools für wiederkehrende Aufgaben gehört der Vergangenheit an; und so setzen nicht mehr nur Open-Source-Projekte Grunt erfolgreich ein, sondern es fasst schrittweise auch im kommerziellen Bereich Fuß.

Wie eingangs erwähnt kann man vom `make` der JavaScript-Welt sprechen. Dabei geht es weniger ums Kompilieren und Linken als vielmehr um das Ausführen verschiedener Tasks. Dies kann neben Unit-Tests oder einer statischen Code-Analyse schlicht das Zusammenfügen und Minifizieren von JavaScript-Dateien sein. Letzteres ist Standard, wenn es um das Ausliefern des eigenen Codes geht, sodass im Browser am Ende nicht viele einzelne JavaScript-Dateien mit zur Ausführung unnötigen Zeichen und Kommentaren ankommen.

Anders als in der vorangegangenen Version liefert das Projekt-Team Grunt nicht mehr mit einigen fest eingebauten

Listing 1: Einfache Bower-Konfiguration

```
{
  "name": "MyComponent",
  "version": "1.0.0",
  "main" : "./main.js",
  "dependencies": {
    "jquery" : "latest"
  }
}
```

Listing 2: Typisches Gruntfile

```

1 module.exports = function(grunt) {
2   grunt.initConfig({
3     // Metadaten
4     pkg: grunt.file.readJSON('package.json'),
5     banner: '/* <%= pkg.title || pkg.name %> <%= pkg.version %>
6                 Copyright (C) Roland Eckl
7                 <%= grunt.template.today("yyyy") %>.
8                 All Rights Reserved. */\n',
9   });
10    // Concatenation-Task
11  concat: {
12    options: {
13      banner: '<%= banner %>',
14      stripBanners: true
15    },
16    dist: {
17      src: '/src/**/*.js',
18      dest: 'dist/<%= pkg.name %>.js'
19    }
20  },
21
22  // Minification-Task
23  uglify: {
24    options: {
25      banner: '<%= banner %>'
26    },
27    dist: {
28      src: concat.dist.dest,
29      dest: 'dist/<%= pkg.name %>.min.js'
30    }
31  },
32
33  // Linting-Task
34  jshint: {
35    gruntfile: {
36      src: 'gruntfile.js'
37    },
38    source: {
39      src: ['src/**/*.js']
40    }
41  };
42 });
43
44 // Die folgenden Tasks wollen wir verwenden.
45 grunt.loadNpmTasks('grunt-contrib-jshint');
46 grunt.loadNpmTasks('grunt-contrib-concat');
47 grunt.loadNpmTasks('grunt-contrib-uglify');
48
49 // Die folgenden Aliase haben wir.
50 grunt.registerTask('debug', ['concat', 'uglify']);
51 grunt.registerTask('release', ['jshint', 'debug']);
52
53 grunt.registerTask('default', 'debug');
54 };

```

Tasks aus. Zwar sind weiterhin hauseigene Tasks verfügbar, und das Grunt-Team um Ben Alman pflegt sie weiterhin; Entwickler müssen sie aber bei Bedarf zunächst installieren. Überhaupt beschränkt sich Grunt beim Installieren inzwischen auf ein schmales Command-Line-Interface (CLI), das im Grunde nur den Befehl *grunt* systemweit zur Verfügung stellt; daher enthielt die NPM-Installationszeile oben *grunt-cli* und nicht *grunt*. Erst im Nachgang installiert man nun Grunt selbst, jedoch relativ zum Projektpfad, deshalb ohne das *-g*-Flag. Das erlaubt es, mehrere Projekte in verschiedenen Grunt-Versionen zu fahren. Bei einem Update ist man auf diese Weise nicht mehr gezwungen, sofort alle Projekte und insbesondere deren jeweiligen Build-Prozess aktualisieren zu müssen.

Tasks findet man leicht, denn der offizielle Internetauftritt hat dafür eine Extra-Seite: gruntjs.com/plugins. Dort liegt eine umfangreiche Liste, und man kann nach Stichworten recherchieren. Auf Wunsch lassen sich die Ergebnisse auf sogenannte *contrib-tasks* einschränken; dies sind die offiziell vom Grunt-Team gepflegten Helferlein, falls man den unzähligen (und teils tatsächlich nicht immer ausgereiften) Tasks der Allgemeinheit nicht so ganz vertrauen mag.

Anlegen neuer Projekte über Templates

Wer Grunt ohne Yeoman und die zugehörigen Generatoren einsetzen möchte, findet momentan allerdings keine eingebaute *init*-Task vor. Und wer beim Scaffolding unbedingt ohne Yeoman arbeiten möchte, findet gegebenenfalls in *grunt-*

init eine Alternative. Im Grunde ermöglicht Letzteres, vergleichbar zu Yo, das Anlegen neuer Projekte über Templates, die man ähnlich zu vorherigen Generatoren separat nachinstallieren kann. Wie bei Yo werden Entwickler mit zahlreichen Fragen zu neuen Projekten konfrontiert. Man erhält danach auf diesem Wege neben den vorlagespezifischen Dateien stets die für Grunt typischen Dateien *package.json* und *Gruntfile.js*. Die Bower-Unterstützung hingegen fehlt in der Regel.

package.json ist das Pendant zu *bower.json*, kommt allerdings ursprünglich aus dem Node.js-Universum. Neben Meta-Informationen wie Projektname, Version und Autor finden sich hier *devDependencies*, Abhängigkeiten der individuellen Entwicklungsumgebung und nicht solche der zu entwickelnden Anwendung selbst. Dies sind beispielsweise alle verwendeten Grunt-Plug-ins. Hier kann man weitere Abhängigkeiten eintragen. Ein Aufruf von *npm install* (ohne Angabe eines konkreten Moduls) weist den Node Package Manager an, alle fehlenden Abhängigkeiten (etwa neu eingetragene Tasks) herunterzuladen. Diese landen wie die Yo-Generatoren im *node_modules*-Verzeichnis. Selbst gezielt mit *npm* statt über den direkten Eintrag in der JSON-Datei installierte Tasks können über die zusätzliche Angabe des *--save-dev*-Flags automatisch in das *package.json* als *devDependency* eingetragen werden.

In *Gruntfile.js* wiederum liegt die Konfiguration des Build-Prozesses vor; sie startet mit dem Methodenaufruf *grunt.initConfig*, wobei man die individuellen Einstellungen für jede Task in Form eines JavaScript-Objektliterals über gibt. Listing 2 zeigt das. Was wie zu kon-

figurieren ist, offenbaren die Tasks im *Readme*-Bereich ihrer jeweiligen NPM-Seite, die über die zuvor erwähnte Plug-in-Suche ebenfalls erreichbar ist. Damit die jeweiligen Tasks funktionieren, lädt *grunt.loadNpmTasks* (Zeilen 45 bis 47 im Listing) diese anschließend. Dabei unterscheidet man grundsätzlich zwischen einfachen und sogenannten Multi-Tasks. Zuerst genannte weisen nur eine einzige Konfiguration auf, Letztere erlauben es, mehrere Konfigurationen für die gleiche Task anzulegen. Für gewöhnlich sind Tasks eher vom letzten Typ.

Während Entwickler einfache Tasks ausschließlich über ihren Namen referenzieren können, erlauben Multi-Tasks die Angabe der jeweiligen Konfiguration nach einem Doppelpunkt. Ohne die Angabe einer solchen spezifischen Konfiguration arbeitet Grunt einfach alle nacheinander ab.

Alias-Tasks bündeln Einzelaufgaben

Es lassen sich weiterhin Ziele hinzufügen, die keiner konkreten Task entsprechen. Stattdessen bündeln sie weitere Ziele und/oder Tasks; man spricht hier von Alias-Tasks. So lassen sich bequem ganze Sequenzen zusammenfassen. Die Zeilen 50 und 51 von Listing 2 enthalten einen Release- und Debug-Build, die unterschiedlich viele Tasks ausführen. In Zeile 53 wird lediglich eine einzelne Task mit einem anderen, zusätzlichen Namen versehen. Dieser Alias (*default*) kommt zum Tragen, wenn Grunt ohne Angabe irgendeiner konkreten Task startet.

Da die Konfiguration im Gruntfile letztlich nur ein JavaScript-Objektliteral

ist, lassen sich einzelne Elemente untereinander referenzieren. Zeile 28 zeigt das. Sollen die Werte innerhalb von Strings verwendet werden, können die Referenzen mit sogenannten Direktiven in spitzen Klammern erfolgen. In den Zeilen 5 ff. wird beispielsweise ein Wert für ein Text-Banner zusammengesetzt – mit dem Namen der Anwendung.

Um den Build anzustoßen, muss man im Verzeichnis mit dem zugehörigen Gruntfile ihn aufrufen. Danach startet automatisch die unter *default* beziehungsweise *debug* angegebene Kette. Gibt eine der Tasks einen Fehler oder einen Warnung aus, bricht Grunt ab. Mit dem Flag *--force* kann man das Programm allerdings dazu bewegen, bei Fehlern die nächsten Tasks dennoch auszuführen.

Das Zusammenspiel der drei Tools

Einzelne Tasks lassen sich ebenfalls aufrufen. *grunt jshint* etwa unterzieht Quellcode und Gruntfile einer statischen Code-Analyse. Da es sich dabei um eine Multi-Task handelt, können Entwickler wie beschrieben bei Bedarf eine der Unterkonfigurationen auswählen, etwa *grunt jshint:source*.

Im kombinierten Einsatz von Yo, Bower und Grunt soll zunächst eine simple Web-App ohne große Spezialitäten entstehen – vom Anlegen eines einfachen Projektes über das Hinzufügen von Abhängigkeiten bis hin zum Build. Sie soll die Nutzereingaben lediglich stets rückwärts anzeigen. Da die drei Kern-Tools systemweit installiert sind, ist nur noch ein Verzeichnis für die Anwendung anzulegen. Dort spielt *npm install generator-webapp* einen Generator ein. *yo webapp* legt das Projekt an. Zu beantworten sind ein paar Fragen, etwa ob das Twittersche Bootstrap oder RequireJS zum Einsatz kommen sollen. Hier genügt momentan ein „No“ in allen Fällen.

Daraufhin liegen die Dateien für Bower (*bower.json*) und Grunt (*Gruntfile.js*, *package.json*) im Projektverzeichnis vor. Yo fordert im Nachgang automatisch Bower und den Node Package Manager auf, die fehlenden Pakete und Module zu installieren. Schließlich enthält das Anwendungsverzeichnis drei Unterordner. Im ersten, *app*, liegen alle HTML-, JavaScript- und sonstige Ressourcen, aus denen die Web-App bestehen soll. Die Abhängigkeiten sind im Unterordner *bower_components* zu finden. Zwar legt Bower sie in einem Ordner namens *components*, aber Yeoman hat den Pfad über die Einstellungsdatei *bowerrc* geändert. Der nächste Ordner

heißt *test*; hier liegen erste, erweiterbare Unit-Tests bereit. Als Test-Framework kommt Mocha zum Einsatz. Und der letzte Ordner, *node_modules*, enthält die Grunt-Tasks und weitere zur Entwicklung nützliche Sachen, wie LiveReload. Dazu später mehr.

Damit existiert eine funktionierende, zugegebenermaßen aber rudimentäre Anwendung für das Web. Sie lässt sich schon testen und bauen – per *grunt build*. Infolgedessen werden nun die Dateien verkleinert und teilweise zusammengefügt, überflüssige Kommentare entfernt, Bilder optimiert, und so weiter. Das Ergebnis landet in einem vierten Ordner namens *dist*, dessen Inhalt letztlich auf einem Webserver residieren muss. Für das Optmieren von Cascading-Style-Sheets wären noch zwei weitere Installationen fällig (Ruby und Compass); darauf sei hier verzichtet. Grunt bricht zwar mit einer Warnung ab, aber über das zusätzliche *--force* lassen sich alle Warnungen ignorieren.

Außer dem Ziel *build* stehen noch einige zur Verfügung, etwa *test* und *jshint*, das Ausführen der Mocha-Unit-Tests und die statische Code-Analyse. Diese Ziele führt Grunt automatisch bei der Default-Task vor dem tatsächlichen Build aus. Beim Starten von *grun* ohne weitere Angaben durchläuft er alle Schritte, und wenn zuvor keine Fehler bei der Qualitätssicherung auftreten, sind die Dateien für das Deployment das Ergebnis.

JavaScript und HTML verbandeln

Schließlich sei noch eine Bibliothek in die Anwendung integriert: Knockout, ein Framework für das Model-View-View-Model-Pattern (MVVM), wie man es aus der .NET/WPF-Welt kennt. Es ermöglicht Datenbindung zwischen Markup (hier meist HTML) und Business-Logik (JavaScript). *bower install knockout* lädt das Framework, trägt es in *bower.json* ein und legt es ins richtige Verzeichnis.

Vor dem Einbinden von Knockout in den Quellcode ein kurzer Blick auf ein weiteres Tool: LiveReload. Mit ihm betrachtet man über einen Test-Server das Ergebnis seiner aktuellen Entwicklungstätigkeit im Browser. Bei jeder Änderung am Quellcode (gleichgültig, ob es sich um CSS, HTML, JavaScript, und so weiter handelt) aktualisiert das Tool den Browser wie von Geisterhand.

LiveReload findet sich dank Yeoman schon unter den Entwicklungsabhängigkeiten im *node_modules*-Verzeichnis. Um es zu nutzen, müssen Entwickler

Listing 3: HTML-Code von index.html mit Data-Binding

```
<!doctype html>
<html>
  <head>
    <title>My Web App</title>
    <!-- Place favicon.ico and apple-touch-icon.png in the root directory -->
    <link rel="stylesheet" href="styles/main.css">
    <!-- build:js scripts/external/knockout.js -->
    <script src="bower_components/knockout.js/knockout.js"></script>
    <!-- endbuild -->
  </head>
  <body>
    <div class="container">
      <div class="hero-unit">
        <h2>Reverse it, baby!</h2>
        <input data-bind="value: Original, valueUpdate: 'afterkeydown'" size="30"/>
        <p><span data-bind="text: Reversed"></span></p>
      </div>
    </div>

    <!-- build:js scripts/main.js -->
    <script src="scripts/main.js"></script>
    <!-- endbuild -->
  </body>
</html>
```

Listing 4: JavaScript-Code mit Knockout-ViewModel

```
/*global ko*/
(function () {
  'use strict';
  var ViewModel = function () {
    this.Original = ko.observable('This is actually reversed!');

    this.Reversed = ko.computed(function () {
      return this.Original().split('').reverse().join('');
    }, this);
  };

  ko.applyBindings(new ViewModel());
})();
```



grunt server eingeben, wonach der Test-Server startet und ein Browser-Fenster öffnet.

Übrig bleibt die Aufgabe, *index.html* zu öffnen und anzupassen. Da die Web-App die Nutzereingaben rückwärts ausgeben soll, ist ein Texteingabefeld sowie Platz für die Ausgabe erforderlich. Den Quellcode zeigt Listing 3. Welche IDE für die Programmierung zum Einsatz kommt, ist für LiveReload irrelevant, Grunt beobachtet die Projektverzeichnisse und merkt, wenn sich etwas ändert. Sobald ein Entwickler speichert, erscheint die aktualisierte Ansicht (siehe Abb. 2). Der Nutzer kann nun zwar in das Eingabefeld schreiben, aber viel mehr passiert noch nicht. Da helfen die Data-Binding-Deklarationen in Listing 3 nicht viel. Dazu ist es notwendig, den JavaScript-Code in *main.js* anzupassen. Ein *ViewModel* ist in Listing 4, mit *applyBindings* scharf gestellt. Das nächste Speichern aktualisiert den Browser; nach einer Texteingabe zeigt er sie bei jedem Tastenanschlag sofort rückwärts im Ausgabefeld an. Das hier vorgestellte Anwendungsbeispiel liegt auf dem FTP-Server der iX zum Download bereit.

Schließlich ist es erforderlich, die App auf den Server zu kopieren. Lokal lässt sich das über die *grunt-contrib-copy*-Task erledigen (Teil des Projekts). Für einen Transfer per FTP stünde mit *grunt-ftp-deploy* ebenfalls eine Task zur Verfügung; die müsste man allerdings nachinstallieren.

Mobile Endgeräte können auf die Web-App zugreifen, aber wer sie in den

AppStore bringen will, braucht noch PhoneGap oder einen anderen nativen Wrapper. Für das Erzeugen der mobilen App können Entwickler PhoneGap Build nutzen, den Cloud-basierten App-Generierungsdiensst. Das Installieren und die Pflege der nativen SDKs für alle Zielpлатformen entfallen. Einen (kostenlosen) Account bekommt man derzeit unter build.phonegap.com. Und wie zu erwarten, gibt es hierfür längst eine Task.

Fazit

Yeoman unterstützt ohne besondere Anlaufschwierigkeiten beim Entwickeln von Anwendungen für die neue HTML5-Welt. In der Praxis können die drei Tools Yeoman, Grunt und Bower überzeugen. Höchstens bei den Generatoren mangelt es manchmal an der wünschenswerten Flexibilität, sodass man letzten Endes wohl eher auf einen vertrauten Satz selbst zusammengestellter Bibliotheken, Frameworks und Tasks zurückgreifen möchte, statt die teilweise etwas überfrachteten Vorlagen zu nutzen.

Ein großer Teil der Entwicklergemeinde kommt vermutlich ohne Yeoman (oder konkreter Yo) aus und konzentriert sich eher auf Grunt und Bower für die alltäglichen Aufgaben. Dank der zwischenzeitlich sauberen Trennung der vorgestellten Werkzeuge lassen sich aber dennoch alle Beigaben der Yeoman-Macher problemlos verwenden. Ebenso kann man das eine oder andere Tool nach- oder wieder

deinstallieren. Wer dennoch Wert auf Scaffolding legt, kann einen Blick auf *grunt-init* werfen.

Insgesamt fehlt eine saubere IDE-Integration. Zwar kann man Yeoman in die Entwicklungsumgebung seiner Wahl einbinden; aber für eine richtige Integration wäre etwas mehr notwendig. Denn von Task zu Task sind die Ausgaben unterschiedlich formatiert und deshalb kann eine IDE sie nur schwer interpretieren.

Ein guter Build-Prozess ist allerdings selbst ohne Anpassung an eine IDE hilfreich und wertvoll. Vielleicht macht genau das die Stärke und Beliebtheit von Yeoman aus: Jeder kann die Tools nutzen, gleichgültig in welchem Editor man sich zu Hause fühlt. (hb)

Roland Eckl

arbeitet als Softwarearchitekt im Fokusfeld Mobile and Social Computing der Corporate Technology der Siemens AG. Neben Forschung und Technologie-Transfer ist er beratend für die Siemens-Sektoren tätig.

Literatur

- [1] Roland Eckl; Webentwicklung; Reine Routine; Grunt: Command-Line-Build-System für JavaScript; *iX* 12/2012, S. 76
- [2] Sebastian Springer; JavaScript; Gordische Welt; Professionelle Applikationsentwicklung mit Node.js; *iX* 10/2012, S. 58



Mobile Oracle-Anwendungen mit APEX

Wie hausgemacht

Peter Raganitsch

Ähnlich wie für den Desktop kann man mit aktuellen APEX-Versionen auch HTML-Anwendungen für Mobilgeräte erstellen. Das geht dank jQuery Mobile schnell und flexibel.

Oracle Application Express (APEX) ist seit Jahren als Rapid Application Development (RAD) Tool zum Erstellen datenbankbasierter Webanwendungen bekannt. Sein Fokus liegt auf der Ein- und Ausgabe von Daten sowie einfachem Reporting, etwa Listenauswertungen, Charts et cetera. Zum einen beinhaltet es ein deklaratives Baukastensystem mit einer Menge vorgefertigter Komponenten, zum anderen kann man Plug-ins einbinden oder selbst erstellen. Ein Markt von Plug-in-Anbietern hat sich bereits etabliert.

Mit der im Oktober 2012 erschienenen Version 4.2 kamen Funktionen für das

Entwickeln mobiler Anwendungen hinzu. Denn auch bei Business-Anwendungen werden die Rufe nach mobilen Applikationen und dem Zugang zu wichtigen Geschäfts- und Kundendaten von unterwegs lauter. Aber nicht jeder Mitarbeiter verwendet das gleiche Smartphone; oft sind in Firmenlandschaften alle Hersteller und Preisklassen der Telefone vertreten. Eins aber haben sie alle gemeinsam: So ziemlich jedes aktuell verkauftes Smartphone verfügt über einen Internetzugang und einen Browser.

Das passt gut zu APEX, denn mit dieser Umgebung erzeugt man HTML-Seiten direkt aus der Oracle-Datenbank. Für

das Erstellen von Smartphone-Oberflächen ist jQuery Mobile in APEX 4.2 integriert, und Entwickler erhalten Unterstützung durch zahlreiche Wizards [a].

Die Programmiersprache innerhalb von APEX ist SQL und PL/SQL, mit der sich ein Datenbankprogrammierer schnell einarbeiten kann. Da APEX in einer Oracle-Datenbank installiert ist, sollte sie als Hauptquelle der Anwendungsdaten fungieren. Über verschiedene Kanäle wie Database-Links, Webservices und externe Tabellen kann man auch andere Quellen anbinden. Einen Überblick bietet der Onlineartikel bei heise Developer [b].

Zurzeit liegt APEX in Version 4.2.2 vor. Für Version 5.0 nennen die Entwickler weitere mobile Features sowie neue Komponenten für den Desktop-Browser-Betrieb. Auf der öffentlichen Demo-Plattform [c] kann man sich kostenfrei einen Workspace besorgen und testen, ohne eine lokale Installation vornehmen zu müssen.

Wie von APEX gewohnt, erstellt man mobile Anwendungen im sogenannten Application Builder. Dort ruft man mit dem Button *Create* den Anwendungs-Wizard auf. Wichtigste Einstellung darin ist das „User Interface“. Der Wert *jQuery Mobile Smartphone* optimiert die Anwendung für den mobilen Gebrauch (siehe Abbildung 1).

Vorgefertigte Ansichten

Auf den weiteren Seiten folgen allgemeine Einstellungen wie die zu Datumsformaten und Benutzer-Authentifizierung, die hier keine Rolle spielen. Ein Klick auf *Create Application* überspringt sie. Die Anwendung ist nun erstellt und lässt sich bereits (idealerweise auf einem Smartphone bzw. -simulator) ausführen. Man kann sich bei ihr anmelden und landet danach auf einer noch leeren Navigationsseite, die bereits eine Kopfleiste mit einem Home- und Logout-Button zeigt. Daraus entsteht später das Startmenü.

Zurück im Application Builder startet *Create Page* den Wizard zum Erstellen einer neuen Seite. Darin wählt man *Form* und danach *Form on a Table with List View* und vergibt den Seitennamen „Kunden“. Als Tabelle kommt *DEMO_CUSTOMERS* mit *CUST_LAST_NAME* als Anzeigespalte zum Einsatz. Alle anderen gewünschten Spalten wählt man durch Verschieben in die rechte Box. Für die restlichen Formularfelder akzeptiert man die Vorschlagswerte und schließt den Wizard mit *Create* ab.

Auf der so erstellten Seite 2 der Anwendung ist bereits ein funktionierender und durchsuchbarer Listview zu sehen (siehe Abbildung 2).

Das Prinzip ist klar und von anderen Smartphone-Anwendungen her bekannt: Man blättert sich durch Listen; das Aktivieren eines Elements führt zur nächsten Ebene. Im vorliegenden Fall ist dies ein Formular zum Bearbeiten der Kundendaten.

Aber zurück zur Liste und ihren Einstellungsmöglichkeiten: Im Application Builder öffnet man die Seite im Bearbeitungsmodus und wählt dort die Region „Kunden“. Am ersten Tab zeigt sich das vom Wizard erstellte *SELECT*-Statement, das man nun nach Belieben ändern und erweitern kann. Für Erste seien eine Sortierung und eine neue Spalte für den Anfangsbuchstaben des Nachnamens hinzugefügt. Das gesamte Statement sieht dann wie folgt aus:

```
select a.ROWID as "PK_ROWID",
       a.*,
       SUBSTR(a.CUST_LAST_NAME,1,1)
       as CUST_INITIAL
  from "#OWNER#."#DEMO_CUSTOMERS" a
 order by a.CUST_LAST_NAME
```

Apply Changes speichert die Änderung und öffnet die Region nochmals zur Bearbeitung, so man die Checkbox „Return to Page“ vor dem Speichern aktiviert hat. Ein Wechsel zum Tab *Region Attributes* enthüllt diverse Einstellungsmöglichkeiten, die sich auf die Darstellung der Liste auswirken.

Für einen ersten Test setzt man ein Häkchen bei *Show List Divider* und wählt die neue Spalte *CUST_INITIAL* als *List Divider Column*. Nach dem Speichern und Ausführen der Seite zeigt sich das Resultat: eine sortierte Liste mit alphabetischen Trennzeilen zwischen den jeweiligen Anfangsbuchstaben der Nachnamen (siehe Abbildung 3).

Der Listview bietet weitere deklarative Einstellungsmöglichkeiten. Wenn sie zur visuellen Gestaltung der Liste nicht ausreichen, kann man die Option *Advanced Formatting* aktivieren und ein



Ein vorgefertigter Listview zeigt die ausgewählte Spalte einer Tabelle an (Abb. 2).

Alphabetische Trennzeilen fügt APEX auf Wunsch ein (Abb. 3).

HTML-Gerüst für eine Listenzeile definieren. Damit unterstützt APEX alle Listview-Optionen, die jQuery Mobile anbietet. Details der Gestaltungsmöglichkeiten enthält dessen Referenzdokumentation [d].

Erweiterte Formatierungen

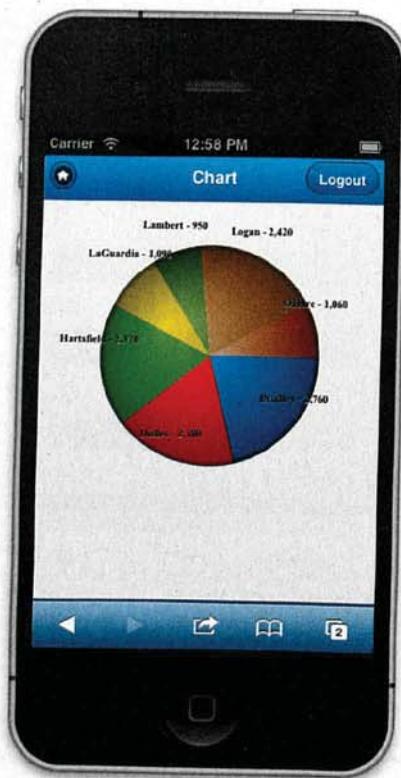
Das Handling von Formularen ist in der mobilen Variante einfacher, als man das von APEX für den Desktop gewohnt ist, denn jQuery Mobile übernimmt die optimale Positionierung und Darstellung der Beschriftungen. Bietet der Bildschirm ausreichend Platz, steht das Label vor dem Feld, sonst springt es darüber. Das ist zumeist bei Smartphones im Hochkant-Modus zu sehen.

Eine wichtige Forderung bei mobilen Anwendungen ist die möglichst einfache Eingabe von Daten. Da die meisten Smartphones keine physische Tastatur mehr haben, kommt stattdessen eine virtuelle zum Einsatz. Allerdings kennen sie nicht nur ein Keyboard, sondern eine ganze Reihe spezieller Tastatur-Layouts, je nachdem, ob man Text, Zahlen, Telefonnummern, Mailadressen, URLs und so weiter eingeben will.

Damit das Smartphone die richtige Tastatur wählt, muss man bei jedem Feld bestimmen, welche Art von Daten es akzeptieren soll. Dies geschieht über die APEX-Einstellung des *Subtype* für das Formularfeld. Wie genau die Tastatur aussieht, hängt vom jeweiligen Endgerät und dem Betriebssystem ab. Durch die Einstellung des Feldtyps hat der mobile Browser jedenfalls die nötige Information und entscheidet selbst, was er damit macht.

Für Charts setzt APEX – wie bisher – auf die Anychart Library, diesmal in Version 6. Sie ergänzt die bisherigen Flash-um HTML5-Diagramme. Zwischen den beiden Formaten wählt man beim Erstellen des Chart, wobei APEX Flash als Präferenz interpretiert: Ist auf dem Client kein passender Player installiert, kommt HTML5 zum Einsatz. Als HTML5-Variante sind schon einige, aber leider noch

Der Create Application Wizard führt den Entwickler durch die jQuery-Elemente (Abb. 1).



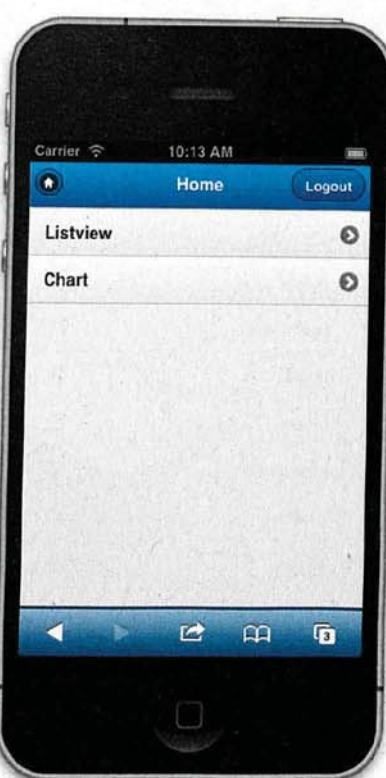
Einige Chart-Typen hat Apex bereits in HTML5 implementiert (Abb. 4).

nicht alle Chart-Typen implementiert, dies will Oracle mit APEX-Patchsets und der nächsten Version nachbessern.

Aus dem Application Builder erstellt man eine neue Seite vom Typ *Chart* mit dem Create Page Wizard, wählt eine 2D-Torte und gibt folgende Abfrage an:

```
SELECT NULL AS LINK
, C.CUST_LAST_NAME AS LABEL
, SUM(O.ORDER_TOTAL) AS VALUE
FROM DEMO_CUSTOMERS C
, DEMO_ORDERS O
WHERE O.CUSTOMER_ID = C.CUSTOMER_ID
GROUP BY C.CUST_LAST_NAME
```

Bei allen anderen Settings nimmt man die Default-Werte und bestätigt durch *Create*. Das erste Resultat dieses Chart auf einem Smartphone sieht noch etwas



Ein Listview ermöglicht das Navigieren zu den anderen APEX-Seiten (Abb. 5).

klein aus, ist aber durch Einstellungen der Chart-Region einfach anpassbar (siehe Abbildung 4).

Bisher fehlt das Startmenü auf Seite 1, die immer noch leer ist. Sie soll die Navigation für die bisher erstellten Seiten enthalten. Dazu wechselt man im Application Builder auf Seite 1 und von dort über das kleine Zahnrad-Symbol rechts oben auf die *Shared Components*. Im Bereich Navigation wählt man *Lists* und erstellt eine namens „Navigation“ mit *Create*. Sie soll statisch sein und zwei Einträge enthalten: „Listview“ mit der Target-Page 2 und „Chart“ mit der Target-Page 4. Auf der nächsten Wizard-Seite wählt man die Option *Create list*

region on current page..Page Template Body (3)“ legt die Region auf die Standardposition fest. Die Auswahl des Templates „List View“ bestimmt, dass die Liste als JQM Listview angezeigt wird. Bei erneutem Ausführen der Anwendung erscheint nun auf der ersten Seite ein Menü (siehe Abbildung 5).

Kommt eine neue Seite zur Anwendung hinzu, braucht man dafür nur noch einen neuen Listeneintrag hinzuzufügen, damit das Menü aktuell bleibt.

Auch für Kalender stellt Oracle eine mobile Version bereit. Sie beziehen ihre Daten aus einer Tabelle oder einem View und zeigen eine Monatsübersicht an. Tage mit Terminen oder Ereignissen sind mit einem blauen Punkt markiert. Ein Klick darauf zeigt die Details oder führt auf eine Seite zur Bearbeitung – je nach Kalendereinstellung.

Erweiterungen

Damit ist der Funktionsumfang der mobilen Unterstützung in APEX längst nicht ausgereizt; die bisher erwähnten Möglichkeiten entsprechen lediglich dem Lieferumfang. Wer keine Angst vor HTML hat, kann durch Bearbeiten von Templates noch mehr aus jQuery Mobile herausholen und die Anwendung visuell aufpeppen. Ein praktisches Werkzeug zum Anpassen der verwendeten Farben ist der Theme-Roller [e]. Darin klickt man sich die Farben für die einzelnen Elemente wie Texte, Buttons, Hintergründe, Kopf- und Fußleisten zusammen und bekommt am Schluss eine CSS-Datei zum Download. Die installiert man auf dem APEX-Webserver und bindet sie in die Anwendung ein.

Eine weitere wichtige Möglichkeit, den Funktionsumfang von APEX – mobile wie Desktop – zu erweitern, sind Plug-ins. Auf den Plattformen im Internet gibt es sie teilweise kostenfrei. Ist ein Plug-in einmal in die Anwendung importiert, kann man es wie jede andere Komponente mit Wizards erstellen und anpassen. So finden sich alle Arten von Maps – etwa Google Maps, Oracle eLocation service oder OpenStreetMap – und Charts sowie mobile Date-Picker und andere Kostbarkeiten. (ck)

Peter Raganitsch

entwickelt seit 2008 Webanwendungen auf Basis von APEX.

Storage Engines sind eine Besonderheit von MySQL und damit von dessen Abkömmling MariaDB. Solche Engines speichern die jeweiligen Daten einer Tabelle. Welche von ihnen zu verwenden ist, definiert die Option *ENGINE* im *CREATE TABLE*-Befehl. Fehlt sie, verwendet der Server die Variable *default_storage_engine*, die seit MySQL 5.5 auf *InnoDB* steht. Die bekanntesten Storage Engines sind das klassische MyISAM und das transaktionsfähige InnoDB. Daneben sind etwa Partitionierung und das Binär-Log von MySQL derart implementiert. Einen kleinen Überblick über die Storage Engines einer Datenbankinstanz erhält man mit

```
SELECT PLUGIN_NAME
  FROM information_schema.plugins
 WHERE PLUGIN_TYPE='STORAGE ENGINE';
```

Im Folgenden geht es um das von dem ehemaligen IBM-Mitarbeiter Olivier Bertrand geschriebene Connect. Diese Storage Engine enthält der freie MySQL-Abkömmling MariaDB ab Version 10.0. Sie ermöglicht den Zugriff auf Quellen im lokalen Dateisystem oder Datenbanken auf anderen Servern. Für letzteren Anwendungsfall benutzt Connect ODBC oder die Client API von MySQL. Der ODBC-Zugriff erfolgt in der aktuellen Version nur lesend. Beim Zugriff per MySQL-API sind lediglich *INSERT*- und *SELECT*-Befehle zulässig. So eignet sich Connect, das keine Transaktionen bietet, zwar nicht für OLTP-Anwendungen, jedoch für Reporting oder Migrationsaufgaben.

Lokale Dateien mit MySQL lesen

Neu ist die Idee nicht, fremde Formate zu unterstützen: MySQL kann schon seit Version 4.1.4 eine CSV-Datei nutzen. Connect unterstützt daneben unter anderem XML, BIN, DBF (dBASE) und INI.

Mit dem Statement

```
CREATE TABLE csv
  ENGINE=CONNECT
  TABLE_TYPE=CSV SELECT * FROM aha ;
```

erstellt man eine CSV-Tabelle für Connect, die der Server mit den Daten der Tabelle *aha* füllt. Er erzeugt in diesem Fall automatisch die Datei *csv.csv*. Existiert bereits eine CSV-Datei, macht man sie mit Connect für *SELECT*-Kommandos zugänglich:

```
CREATE TABLE hallo (id int, id2 int)
  ENGINE=CONNECT TABLE_TYPE=CSV
  FILE_NAME='csv.csv';
```



Neue Storage Engine in MariaDB 10

Fremde Federn schmücken

Erkan Yanar

Mit der Storage Engine Connect kann der MySQL-Spross MariaDB sowohl lokale strukturierte Dateien etwa im CSV- oder XML-Format lesen als auch auf Tabellen in anderen Datenbanksystemen zugreifen.

Zu beachten ist, dass hier die Spaltendefinition die Struktur der CSV-Tabelle angibt. Bei *hallo* handelt es sich um eine virtuelle Tabelle, die keine Daten speichert. Sie beschreibt lediglich den Zugriff auf die angegebene Datenquelle. Wird die eigentliche Datenquelle gelöscht, geht der Zugriff auf die Daten ins Leere:

```
DROP TABLE csv;
...
SELECT * FROM hallo;
...
SHOW WARNINGS;
```

warnt folglich, dass die Datei *csv.csv* nicht existiere.

Connect ermöglicht für lokale Datenquellen das Erstellen von Indizes, jedoch nicht für via MySQL oder ODBC angebundene Server. Der Server kann Abfragen auf solche indizierten Quellen beschleunigen, indem er sich des „Index Condition Push-down“ bedient: Dadurch nutzt bereits die Storage Engine den Index für die Auswahl der benötigten Zeilen, sodass der Server weniger Daten zu verarbeiten hat. Dazu muss

```
optimizer_switch='engine_condition_pushdown=on'
```

als Konfigurationsoption gesetzt sein. Ohne Index durchläuft MariaDB immer

Installation von MariaDB

Bislang enthält keines der Linux-Repositories MariaDB 10, sodass man es manuell nachinstallieren muss. Eine Anleitung dafür findet man online (s. „Alle Links“). Dort gibt es neben den Quellen und tar-Archiven auch fertige Pakete für einige Linux-Distributionen. Wenn die Connect Engine in einem eigenen Paket steckt, wie bei Ubuntu, muss man es ebenfalls herunterladen und installieren. Folgende Konfigurationsoption sollte gesetzt sein:

```
[mysqld]
optimizer_switch='engine_condition_pushdown=on'
```

Der `optimizer_switch` verbessert die Performance beim Zugriff auf entfernte Rechner. Wenn der Datenbankserver Connect nicht automatisch einbindet, hat dies noch zu erfolgen:

```
install plugin CONNECT soname 'ha_connect.so';
```

Ein anschließendes `SHOW ENGINES` sollte die Engine zeigen.

Engine, die Tabellen anderer MySQL-Server zugänglich macht. Sie wird jedoch nicht mehr gepflegt und ist im Default nicht aktiviert. Connect macht dort weiter, wo dieser Vorgänger stehen blieb. So kann man damit auf ODBC-Quellen zugreifen, was die Anbindung nahezu jedes anderen Datenbankservers an MariaDB erlaubt und das Reporting in heterogenen Umgebungen vereinfacht.

Automatische Analyse der Fremd-Tabelle

Gerade beim Zugriff auf große Tabellen hilft der Index Condition Pushdown von Connect. Während ein per Federated angebundener Server die gesamte Tabelle schickt und die lokale Instanz sie nach der `WHERE`-Bedingung filtert, überträgt Connect diese Bedingung an die Gegenseite. Dadurch kann nicht nur ein hoffentlich existierender Index seine Stärke zeigen, sondern es sinkt auch die Netzlast. In einem einfachen Test brauchte Federated für die Suche nach einer von 10 000 Zeilen 33,8 Sekunden (1000 Durchläufe), während Connect nach 2,7 Sekunden fertig war. Noch hat Connect gegenüber Federated jedoch entscheidende Nachteile: Wer Daten auf einem anderen Server ändern oder löschen will, muss die ältere Technik verwenden, denn Connect erlaubt nur `SELECT`- und `INSERT`-Statements.

Ein weiterer Vorteil von Connect ist die Tabellenstruktur, die es bei mit MySQL und ODBC angesprochenen Quelltabellen selbst analysiert. Dadurch muss man bei der Tabellendefinition keine Spalten angeben:

```
keyname varchar(50) flag=2,
value char(200)
ENGINE=CONNECT TABLE_TYPE=ini
FILE_NAME='/etc/mysql/my.cnf'
OPTION_LIST='layout=Row';
```

macht diese Datei für `SELECT`-Befehle zugänglich:

```
SELECT * FROM mycnf
WHERE section='mysqld'
AND keyname like 'innodb%';
```

könnte eine Ausgabe ähnlich der in Listing 1 liefern.

Die genaue Bedeutung der Spaltenoption `flag` jeweils bedeutet, hängt vom jeweiligen `TABLE_TYPE` ab. Für INI-Tabellen definiert `flag=1` die Spalte für den Abschnitt und `flag=2` beim zeilenorientierten Layout die Schlüsselspalte. Dieses zeilenorientierte Layout bietet sich für Dateien an, deren Abschnitte unterschiedliche Schlüssel haben können. Auf diese Weise kann man per Datenbankzugriff die MariaDB-Konfiguration abfragen. Verhinderten nicht die Zugriffsrechte des Betriebssystems dies, könnte man sie per SQL-Kommando auch ändern.

Interessanter als der Zugriff auf lokale Datenquellen ist die Verwendung von Tabellen auf anderen Maschinen. Mit Federated kennt MySQL zwar eine Storage

```
CREATE TABLE remote
ENGINE=CONNECT TABLE_TYPE=mysql
DBNAME='app' TABNAME='personen'
OPTION_LIST='user=apache,host=my.host'
```

Für den Tabellentyp `mysql` können der Datenbank- (`DBNAME`) und der Tabellename (`TABNAME`) der Zieltabelle angegeben werden. In der `OPTION_LIST` stehen die Authentifizierungsdaten und die Adresse des Remote-Server.

Per ODBC ist der Zugriff noch einfacher:

```
CREATE TABLE nachoracle ENGINE=CONNECT
TABLE_TYPE=ODBC TABNAME=sales
connection='DSN=oracle'
```

wobei man die Daten für den Parameter `DSN` mit den entsprechenden Tools definieren, unter Linux etwa `unixODBC`.

Mit dem Parameter `srcdef` kann man Connect ein `SELECT`-Statement für die

Spider: Eine Alternative zu Connect

MariaDB enthält ab Version 10.0.4 die Storage Engine Spider. Kurz gesagt, kombiniert sie die Partition- mit der Federated-Engine. Bei Spider-Tabellen kann jede Partition auf einen anderen Server verweisen. So lassen sich zum Beispiel Terabyte große Datenbanken auf mehrere Server verteilen und dort im Speicher halten. Die Applikation selbst greift über nur eine Tabelle darauf zu.

Das Verteilen großer Datenmengen auf mehrere Server ist eine übliche Praxis, genannt Sharding. Hierzu mussten die Daten in disjunkte Mengen teilbar sein, und Transaktionen

die gesamte Tabelle, um die gewünschte Zeile zu finden. Das zeigt `EXPLAIN SELECT * FROM hallo WHERE id=11;` Existiert kein Index, liest der Server alle 6966 Zeilen. Ist mit

```
CREATE INDEX 'idx' ON hallo(id);
```

ein Index angelegt, liest die Datenbank nur noch die eine benötigte Zeile.

MariaDB liest die eigene Konfiguration

Im zweiten Beispiel sei der Zugriff auf die Konfigurationsdatei des Datenbank-servers gezeigt (`my.cnf`). Sie liegt im INI-Format vor: in Abschnitte unterteilte Zeilen der Form `Schlüssel = Wert`.

```
CREATE TABLE mycnf (
section char(20) flag=1,
```

Listing 1: `SELECT` liest `my.cnf`

section	keyname	value
mysqld	innodb_buffer_pool_size	256M
mysqld	innodb_log_buffer_size	8M
mysqld	innodb_file_per_table	1
mysqld	innodb_open_files	400
mysqld	innodb_io_capacity	400
mysqld	innodb_flush_method	0_DIRECT

6 rows in set (0.00 sec)

Auswahl der erwünschten Daten übergeben – sozusagen ein Remote-View:

```
CREATE TABLE onlineuser ENGINE=CONNECT
  TABLE_TYPE=ODBC TABNAME=user
  connection='DSN=games'
  srcdef='SELECT * FROM user WHERE online=1'
```

Anschließend gibt `SELECT * FROM onlineuser` die Zeilen der Tabelle `user` zurück, bei denen `online` den Wert 1 hat. So kann man mit Connect zum Beispiel die Daten für das Reporting bestimmen.

Connect adaptiert und erweitert zudem die Fähigkeiten der Merge Storage Engine, die MyISAM-Tabellen derselben Struktur zu einer neuen kombiniert. Anders als das Vorbild beschränkt sich Connect jedoch nicht auf MyISAM-Tabellen: Das Zusammenfassen zu einer neuen, virtuellen Tabelle funktioniert auch mit Connect-Tabellen selbst. Das Ergebnis heißt Table-List-Tabelle (TBL), beim `CREATE TABLE` ist deshalb `TBL` als `TABLE_TYPE` anzugeben. Optionen legen fest, wie viele Subtabellen höchstens fehlen dürfen (`MAXERR`), dass in Subtabellen fehlende Spalten als `NULL` erscheinen (`ACCEPT`) und dass Connect Subtabellen parallel abfragen soll (`THREAD`).

Ein weiteres Connect-Feature – nicht nur für TBL-Tabellen, aber hier besonders nützlich – sind „Special Columns“. Diese Spalten füllt Connect mit internen Informationen, und Anwendungen können nach ihnen filtern. Die relevanten sind `TABID` (Tabellenname) und `SERVID` (Name des Servers).

```
CREATE TABLE alle
  (filename varchar(30) special=TABID,
  id int flag=1, id2 int flag=2)
  engine=connect TABLE_TYPE=tbl
  table_list='abc,aha,remoteconnect'
```

Hier steht `flag=2` für die zweite Spalte. Danach liefert die Abfrage

```
SELECT filename, SUM(id2)
  FROM alle GROUP BY filename
```

die Ausgabe in Listing 2. In `filename` steht der Name der Subtabelle.

Listing 2: Connect nennt interne Informationen

filename	sum(id2)
abc	5974
aha	19510
remoteconnect	20054

hier erneut auftreten. So speichert derzeit das Backup einer Connect-Tabelle auch alle von ihr referenzierten Daten – dasselbe tat Federated in einer frühen Version.

Der Zugriff auf nahezu beliebige Datenquellen vereinfacht Migrationsprojekte von und nach MySQL und das Reporting. Wesentlich andere Einsatzgebiete sollte man schon allein deshalb nicht suchen, weil die Engine keine Transaktionen bietet. (ck)

Fazit

Zwar ist der Storage Engine Connect der Alphastatus noch anzumerken, aber die Entwicklungsgeschwindigkeit und Reaktionszeit auf Bugs beeindrucken, selbst wenn Kinderkrankheiten anderer Engines

Erkan Yanar

ist freiberuflicher Berater, am liebsten für und mit MySQL und LXC.

Alle Links: www.ix.de/ix1310149



Werkzeuge für Software-QS und -Test

Jetzt anmelden!

7. bis 8. November 2013 in Nürnberg

So vielseitig wie heute war das Angebot an Werkzeugen zu Software-Qualitätssicherung und -Test noch nie!

Ob für agiles Testen, Testmanagement oder -automatisierung: Der Software-QS-Tag 2013 liefert Ihnen einen Blick über den Tellerrand auf die gegenwärtige Tool-Landschaft – und zeigt das Potenzial der Werkzeuge.

Bekannte Tool- und Testexperten präsentieren Ihnen Fachvorträge als auch Workshops und Tutorials in denen Sie selbst die Werkzeuge genauer unter die Lupe nehmen können.

Seien Sie am 21. Software-QS-Tag dabei und erfahren Sie, was Test-Tools heute können!

Die Veranstaltung von Experten für Experten!

Weitere Informationen unter:
www.ix-konferenz.de

**Software
QS-TAG
2013**



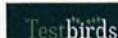
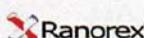
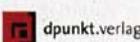
eine Veranstaltung von:



in Zusammenarbeit mit:



Es stellen aus:



vCenter-Tutorial, Teil 2: Komplexe Workflows für den vCenter Orchestrator

Etüde



**Guido-Arndt Söldner,
Jens-Henrik Söldner**

VMwares vCenter Orchestrator ist ein bei vSphere mitgeliefertes Werkzeug zum Automatisieren von IT-Prozessen in virtualisierten Umgebungen. Der zweite Teil des Tutorials beschäftigt sich mit dem Erstellen von Workflows, die komplexe Prozesse abbilden und steuern können.

Im ersten Teil des Tutorials ging es nach einer Einführung in die Architektur des vCenter Orchestrator (vCO) von VMware um den konkreten Einsatz. Der zweite Teil zeigt aus welchen grundlegenden Elementen Workflows aufgebaut sein können.

Ein erster eigener Workflow

Von Haus aus bietet der vCO eine große Zahl vorgefertigter Workflows und Aktionen. In der Regel sind Erstere dafür ausgelegt, mit genau einer Elementinstanz (etwa einer virtuellen Maschine) zu interagieren und sie zu ändern. Darüber hinaus kann es sinnvoll und praktisch sein, mehrere virtuelle Maschinen (VMs) auf einmal zu ändern. Typische Szenarien sind, dass alle virtuellen Maschinen, die in einem bestimmten Ordner oder im Resource Pool abgelegt sind, modifiziert werden sollen.

Aktionen hingegen stellen elementare Bausteine dar, die in Workflows als Funktionen fungieren können. Sie dienen etwa dazu, zu überprüfen, ob ein Windows-Betriebssystem in einer VM läuft, eine IP-Adresse gültig ist oder man verwendet sie, um einen Ordner im VirtualCenter anzulegen oder Benutzerkonten im Active Directory einzurichten. VMware liefert vCO mit Hunderten fertiger Aktionen, die letzten Endes die Mächtigkeit des Systems zu großen Teilen mit ausmachen.

Das Ziel des ersten Workflows liegt auf der Hand: Er soll von jeder VM einen Snapshot erzeugen. Dazu erhält er als Eingabeparameter die Namen der virtuellen Systeme.

Damit man die eigenen Workflows im Auge behalten kann, empfiehlt es sich, im vCO in der Designansicht zunächst einen neuen Ordner anzulegen. Danach führt ein Rechtsklick auf den Ordner zur Option, einen neuen Workflow anzulegen – im Rahmen des Tutorials bietet sich als Name „Create Snapshots“ an. Daraufhin lässt sich die Workflow-Design-Maske mit ihren Registerkarten (siehe Abbildung 1) öffnen.

In der ersten Registerkarte „General“ erscheint der Name des Workflows sowie dessen Beschreibung samt Version.

Ein wichtiger Bestandteil des Workflow-Konzeptes von vCO sind Attribute. Sie dienen innerhalb eines Workflows als globale Variablen und ermöglichen es, Informationen zwischen den einzelnen Schritten auszutauschen. Wenn eine Workflow-Komponente die Attribute lesen oder schreiben soll, ist es jedoch wiederum unumgänglich, die betroffenen Attribute als Ein- oder Ausgabeparameter der aufzurufenden Komponente zu definieren. Falls ein Attribut mit der Markierung „Read-only“ versehen ist, gilt es als Konstante. Zusätzlich darf man die Attribute mit Werten vorbelegen.

Für den ersten Workflow sind zwei Attribute erforderlich:

- Das Attribut *vmNB* speichert zuerst die Gesamtzahl der zu erstellenden Snapshots bedingt durch die Zahl der VMs. Nach jedem Snapshot soll es der Workflow um eins verringern, bis 0 erreicht ist.
- Mit dem Attribut *currentVM* erhält der Workflow eine Referenz auf die aktuell zu bearbeitende VM.

Beim Anlegen von Attributen oder Ein- und Ausgabeparametern verlangt vCO eine Angabe des Typs der Variablen. Dabei gibt es folgende Typen:

- Basisdaten wie String, Number oder Boolean,
- für JavaScript wie Date oder RegExp,
- generische (wie Any, Properties),

X-TRACT

- Mit dem vCenter Orchestrator können Administratoren Workflows anlegen, ohne sich spezielle Programmierkenntnisse aneignen zu müssen.
- Das Festlegen der Parameter geschieht über die grafische Oberfläche.
- Zusätzlich lassen sich über Skripte Logs generieren, die bei der Fehleranalyse helfen.

- Composite – darunter fasst vCO Attribute beziehungsweise Eingabeparameter unterschiedlichen Typs zusammen, die aber als logische Einheit gruppiert sind.
- vCO-interne Daten wie Workflows, Actions oder Workflow-Tokens und
- Daten, wie sie Plug-ins bereitstellen.

Beim Benennen der Variablen folgt Orchestrator der „CamelCase“-Schreibweise (siehe „Alle Links“). Variablen dürfen keine Leerzeichen und sollten tunlichst keine Sonderzeichen enthalten.

Unter „Attributes“ im unteren Teilbereich des Menüs erscheint als Erstes die Variable *vmNB*. Sie soll den Datentyp *number* erhalten, die zweite *currentVM VC:VirtualMachine*. Dazu klickt man jedes Mal auf „Type“, gibt im Feld „Filter“ das gesuchte Muster ein und wählt den passenden Datentyp anschließend aus der Liste aus (siehe Abbildung 2).

Dem Namen nach

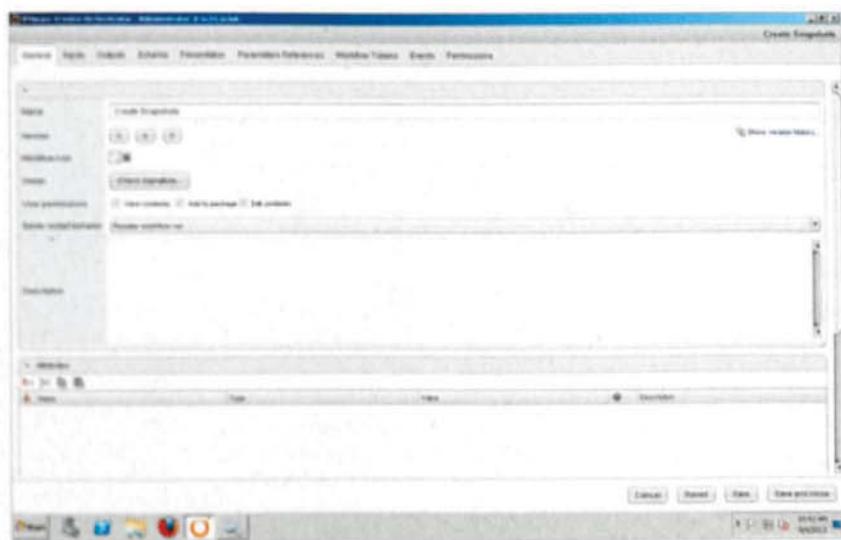
Damit der Workflow Snapshots erstellen kann, benötigt er die Namen der VMs. Diese Information akzeptiert er als Eingabeparameter. Der Benutzer kann sie entweder manuell eingeben, oder der Workflow kann sie von einem anderen, ihn aufrufenden oder einem externen System erhalten. Wie bei einem Attribut besteht jeder Eingabeparameter aus Namen und Datentyp.

Für das Beispiel soll die Registerkarte „Inputs“ den Eingabeparameter *vms* vom Typ *Array/VC:VirtualMachine* erhalten. Hier heißt es aufpassen, dass wirklich ein Feld aus virtuellen Maschinen entsteht (siehe Abbildung 3).

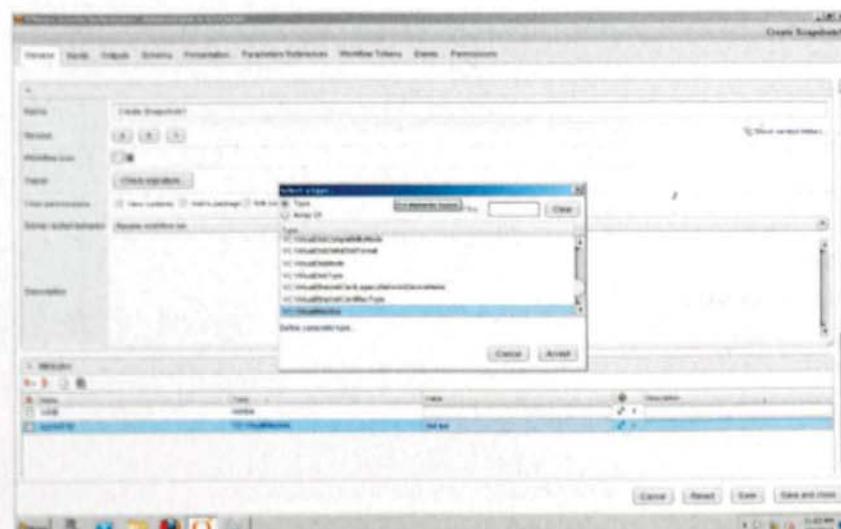
Nach diesen Vorbereitungen führt der nächste Schritt zum Implementieren der Logik, wozu ein Wechsel auf die Registerkarte „Schema“ erforderlich ist (Abbildung 4).

Eine erste Skript-Komponente initialisiert die übergebenen Variablen und stellt die Anzahl der zu erzeugenden Snapshots fest. Eine „Custom Decision“ dient daraufhin dazu, die Aufträge abzuarbeiten. Sind für alle virtuellen Maschinen Snapshots erzeugt, endet der Workflow.

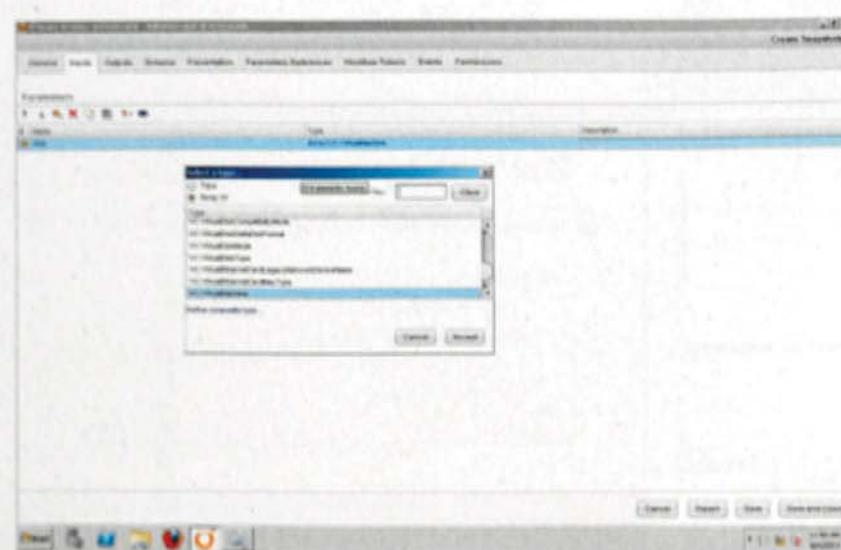
Dabei zählt die Komponente *Decrease Counter* in jedem Schleifendurchlauf die Variable *vmNB* herunter. Eine weitere legt die zu bearbeitende virtuelle Maschine fest. Und der letzte Schritt in der Schleife erzeugt schließlich den Snapshot.



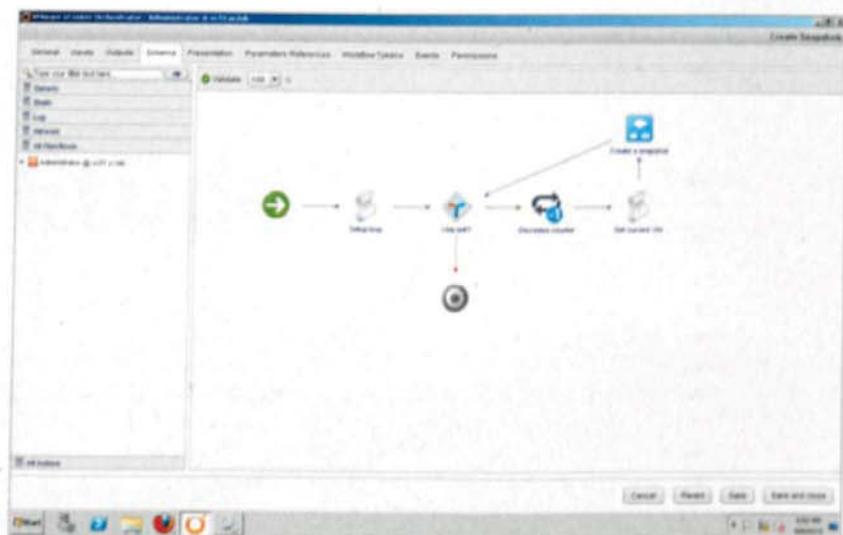
Taufe: In der „General“-Ansicht kann man dem Kind einen Namen geben und die Versionshistorie einsehen (Abb. 1).



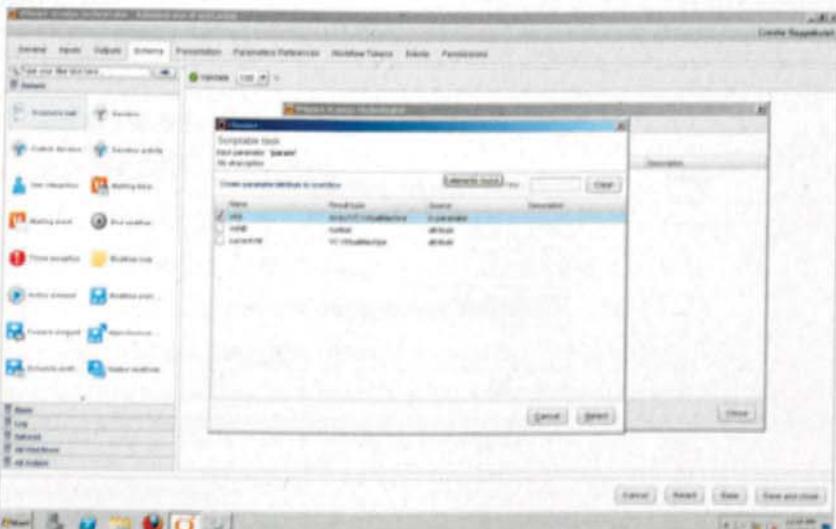
Typ gesucht: Der vCenter Orchestrator zeigt hier alle Datentypen an, die sich auf VirtualCenter beziehen (Abb. 2).



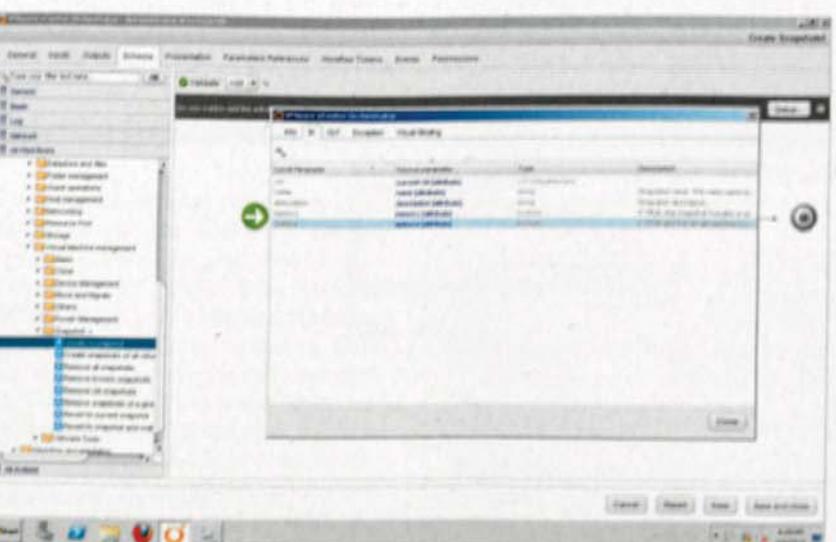
Eingabe: Das Array *VC:VirtualMachine* soll die Namen der virtuellen Maschinen aufnehmen (Abb. 3).



Ablauf: Die Logik des Workflows stellt vCO in einem Diagramm dar, im Zentrum die „Custom decision“ „VMs left?“ (Abb. 4).



Anlagen: Für den Eingabeparameter `vms` ist hier als Quelle der Array `VC:VirtualMachine` gewählt (Abb. 5).



Nach der konzeptionellen Besprechung des Workflows geht es ans schrittweise Einrichten des Workflows: Als Erstes bedarf es der Skript-Komponente (*scriptable task*) zum Initialisieren der Variablen. Diese lässt sich mit Drag & Drop vom linken Teilbereich zwischen den Anfangs- und Endknoten ziehen. Um sie einzurichten, fährt man mit dem Mauszeiger über das Element und aktiviert das Stiftsymbol, woraufhin vCO den Editiermodus öffnet. Auf der ersten Registrierkarte „Info“ hinterlegt man gleich einen passenden Namen für die Komponente wie „Setup loop“. Da es die Aufgabe der Skript-Komponente ist, die Variable `vmNB` zu setzen, braucht sie die entsprechenden Ein- und Ausgabeparameter. Auf der Registerkarte „IN“ aktiviert man dazu das „Bind to workflow parameter/attribute“-Icon und wählt den zuvor erstellten Eingabeparameter `vms` aus (siehe Abbildung 5).

Komponente konfigurieren

Ähnlich geht man mit dem Ausgabeparameter auf der Registrierkarte „OUT“ vor – die Zahl der virtuellen Maschinen soll im Attribut `vmNB` stehen. Zum Abschluss fehlt noch das auszuführende Skript, das man auf der Registrierkarte „Scripting“ eingibt. Es lautet einfach:

```
var vmNB = vms.length;
```

und belegt die Variable `vmNB` mit der Länge der `vms`-Arrays.

Die nächste zu konfigurierende Komponente lautet „Custom decision“. Deren Aufgabe ist es, die Schleifensteuerung zu übernehmen. Wie in Abbildung 4 zu erkennen, hat sie zwei Ausgänge:

- Falls vCO für alle VMs Snapshots erzeugt hat, folgt der Kontrollfluss dem roten Pfeil: Der Workflow ist beendet.
- Sind dagegen noch Snapshots zu erstellen, kehrt der Ablauf dem blauen Pfeil folgend in den Rumpf des Workflows zurück.

Nachdem man die „Custom decision“ in den Workflow gezogen hat, muss man sie noch konfigurieren. Auf der Registerkarte „IN“ kann man wie oben beschrieben die Eingabeparameter binden, in diesem Fall das Attribut `vmNB`. Als Nächstes folgt der Wechsel zur Karteikarte „Scripting“. Dort gibt man ein:

```
return vmNB > 0;
```

Unterpunkt: Das Erzeugen von Snapshots gehört zu den vorgefertigten Workflows (Abb. 6).

Danach kann man das Dialogfeld der „Custom decision“ schließen, nachdem man der Bedingung auf dem Karteireiter „Info“ noch einen Namen verpasst hat, etwa „VMs left?“.

Jetzt fehlt noch das Implementieren des Schleifenrumpfes. Er braucht für das Übungsbeispiel zuerst die Aktion „Decrease counter“. Man erzeugt sie, indem man das vorgefertigte Element „Decrease counter“ aus dem Inventarbereich links aus der Kategorie „Basic“ auswählt und in den Workflow zwischen dem grünen Pfeil nach der Custom Decision und dem Endelement per Drag & Drop einfügt.

Die vorgefertigte Aktion verfügt über eine lokale Variable namens *counter*, die mit *vmNB* als In- und Out-Parameter verbunden sein muss, was man unter den Karteireitern „IN“ beziehungsweise „OUT“ direkt unter der Spalte „Source parameter“ erledigen kann. Auf der Registerkarte „Visual Binding“ lässt sich das Ergebnis noch mal optisch überprüfen.

Nachdem man den Zähler dekrementiert hat, muss als Nächstes das Attribut *currentVM* gesetzt sein. Hier behilft man

Local Parameter	Source parameter	Type	Description
<i>vm</i>	not set	VC.VirtualMachine	Virtual machine of which to create a snapshot
<i>name</i>	not set	string	Snapshot name. The name need not be unique for this virtual machine.
<i>description</i>	not set	string	Snapshot description.
<i>memory</i>	not set	boolean	If TRUE, the snapshot includes a dump of the internal state of the virtual machine.
<i>quiesce</i>	not set	boolean	If TRUE and the virtual machine is powered on when the snapshot is taken, the snapshot is created while the virtual machine is in a quiescent state.

Bindungen: Die benötigten Parameter lassen sich hier an Attribute koppeln (Abb. 7).

sich wieder mit der inzwischen bekannten Skript-Komponente „Scriptable task“ aus dem Inventarbereich „Generic“ und zieht diese hinter das Element „Decrease counter“ in den Workflow. Als Name für die Komponente bietet sich zum Beispiel „Set current VM“ an. Damit sie ihre Aufgabe erfüllen kann, erhält sie die Attribute *vms* und *vmNB* als Eingabeparameter auf der Registerkarte „IN“. Da *currentVM* im Anschluss die richtige virtuelle Maschine speichern soll, bindet man das Attribut in einem zweiten Schritt noch unter der Registerkarte „OUT“. Zum Schluss fehlt noch unter „Scripting“:

```
currentVM = vms[vmNB];
```

Nun kann man als Nächstes das Erzeugen der Snapshots konfigurieren. Hier

kommen die bereits erwähnten vorgefertigten Workflows des Orchestrators ins Spiel, die man entweder direkt oder von einem anderen Workflow aus aufrufen kann. Für das Übungsbeispiel ist der Workflow „Create a snapshot“ relevant, der sich im grafischen Workflow-Editor in der Kategorie „All Workflows“ und dann unter „Library -> vCenter -> Virtual Machine management -> Snapshot“ befindet. Man zieht ihn einfach hinter die „Set current VM“-Komponente in die Designer-Pane.

Etwas aufwendiger als zuvor ist das Konfigurieren. Wieder geht es ans Binden der Eingabeparameter an die Workflow-Attribute, die lokale Variablen innerhalb des Workflows darstellen (siehe Abbildung 6). Der lokale Parameter *vm* kommt



Dr. Scott Meyers' Development Days 2013

Der weltweit führende C++-Spezialist

Jetzt
buchen!

Bereits im achten Jahr, und dieses Jahr zum letzten Mal in Deutschland, veranstalten wir in Zusammenarbeit mit dem Softwaretestspezialisten, QA Systems, Seminare mit Scott Meyers.

Alle Seminare finden zweitägig in Stuttgart statt und werden in Englisch vorgetragen.

Termine 2013:

- 11. - 12. November: **An Overview of the New C++ (C++11)**
- 14. - 15. November: **Effective C++11 Programming **NEUES SEMINAR****
Dieses Seminar ist die Fortsetzung des Overview-Seminars, also C++11 für Fortgeschrittene bzw. Teilnehmer mit Vorkenntnissen. Jeder Teilnehmer erhält gratis zum neuen Seminar einen Gutschein für Scott Meyers' neues Buch „Effective C++11“.
- 18. - 19. November: **Effective C++ in an Embedded Environment**

Die Teilnahmegebühr pro Workshop beträgt:

Frühbucher: 1.650,- Euro zzgl. MwSt.
(2.201,50 Euro inkl. MwSt.)

Standard: 1.990,- Euro zzgl. MwSt.
(2.368,10 Euro inkl. MwSt.)

Aktionspreis für beide C++11 Seminare:

Frühbucher: 3.250,- Euro zzgl. MwSt.
(3.867,50 Euro inkl. MwSt.)

Standard: 3.500,- Euro zzgl. MwSt.
(4.165,- Euro inkl. MwSt.)

Alle Teilnahmegebühren verstehen sich inklusive Verpflegung und Seminarunterlagen.

Weitere Infos unter: www.ix-konferenz.de

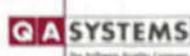


Dr. Scott Meyers

Eine Veranstaltung von

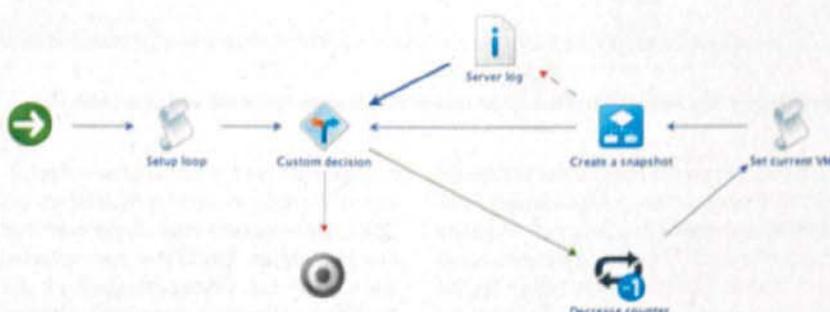


in Zusammenarbeit mit



Info	IN	OUT	Exception	Visual Binding
Output exception binding – <u>errorCode</u>				

Ausnahmen: Die Behandlung von Fehlern sollte mit berücksichtigt sein (Abb. 8).



Ausweg: Für die Fehlerbehandlung zieht man einfach „Serverlog“ auf „Create a snapshot“ und erhält einen hinausführenden Pfad (Abb. 9).

zum Attribut *currentVM*. Für die anderen lokalen Parameter (*name*, *description*, *memory*, *quiesce*) existieren jedoch noch keine Attribute im Workflow.

Um das nachzuholen, klickt man einfach in der Spalte „Source parameter“ auf „not set“ und folgt im sich daraufhin öffnenden Dialogfeld dem Link „Create parameter/attribute in workflow“. Daraufhin kann man das neue Attribut im äußeren Workflow unter dem gleichen Namen wie das lokale Attribut erzeugen, indem man die Standardwerte gesetzt lässt und über OK die Auswahl verlässt (siehe Abbildung 7).

Dieses Vorgehen wiederholt sich, bis alle noch fehlenden Attribute gesetzt sind. Auf der Registerkarte „OUT“ verknüpft man mit der gleichen Vorgehensweise anschließend den Rückgabewert des „Create a snapshot“-Workflows an ein ebenfalls neu erstelltes Attribut, selbst wenn Workflow ihn nicht weiter verwendet. Ist er vom Typ *VC:VirtualMachineSnapshot*, wäre es möglich, im Nachgang noch weitere Aktionen mit dem Snapshot durchzuführen. Das Dialogfeld zum eingebundenen „Create a snapshot“-Workflow kann man nun mit „Close“ schließen.

Nun geht es zurück zur Registerkarte „General“ des Gesamt-Workflows. Sie erwartet die Standardwerte für die gerade eben erzeugten Attribute. Die Boolean-Variablen *memory* und *quiesce* erhalten den Wert „No“, für die Snapshot-Namen unter *name* und die Beschreibung bei *description* trägt man etwas Passendes ein, etwa beide Male „vCO-TestSnapshot“.

Zu guter Letzt muss der Kontrollfluss noch geändert werden, sodass er nach dem aufgerufenen „Create a snapshot“-Workflow zurück zur Schleifenbedin-

gung „VMs left?“ springt. Das erreicht man, indem man das nach dem „Create a snapshot“ folgende Zielelement einfach auf das „VMs left?“-Entscheidungselement zieht und zur Übersichtlichkeit den „Create a snapshot“-Teil nach oben verschiebt. Der Gesamt-Workflow sollte danach wie in Abbildung 4 aussehen.

Nun ist das Erstellen des Workflows abgeschlossen. Beim Speichern validiert vCO ihn automatisch, die Prüfung lässt sich aber auch separat aufrufen. Beim Starten fragt der Orchestrator ab, welche virtuellen Maschinen er übergeben soll. Dazu stellt man menügeführt eine Verbindung zum vCenter-Server her und wählt die gewünschten aus.

Bei Fehlern Workflow fortsetzen

An dieser Stelle sei noch darauf hingewiesen, dass die ganze Ablaufsteuerung theoretisch in einem einzigen Skript implementierbar wäre. Trotzdem ist es sinnvoll, den Workflow wie beschrieben einzurichten. Denn der Orchestrator setzt während der Ausführung Checkpoints in seiner Datenbank und zwar jedes Mal, wenn er eine Aufgabe im Kontrollfluss bearbeitet hat. Der Benutzer kann somit im Fehlerfall den Workflow an der abgebrochenen Stelle weiter fortsetzen.

Tutorialinhalt

Teil 1: Einrichten des vCenter Orchestrator, erster Workflow

Teil 2: Komplexe Workflows

Teil 3: Das Anbinden von Fremdsystemen



Berichte: Durch das Hinzufügen der Funktion „Send Notification“ erhält man Nachrichten über die Ereignisse im Workflow (Abb. 10).

Nichtsdestotrotz ist es darüber hinaus noch wünschenswert, im Workflow zusätzlich eine Fehlerbehandlung zu implementieren, was wichtig ist, wenn das Erzeugen des Snapshots fehlschlägt. In dem Fall sollte vCO den Fehler protokollieren und den Workflow mit der nächsten virtuellen Maschine forsetzen.

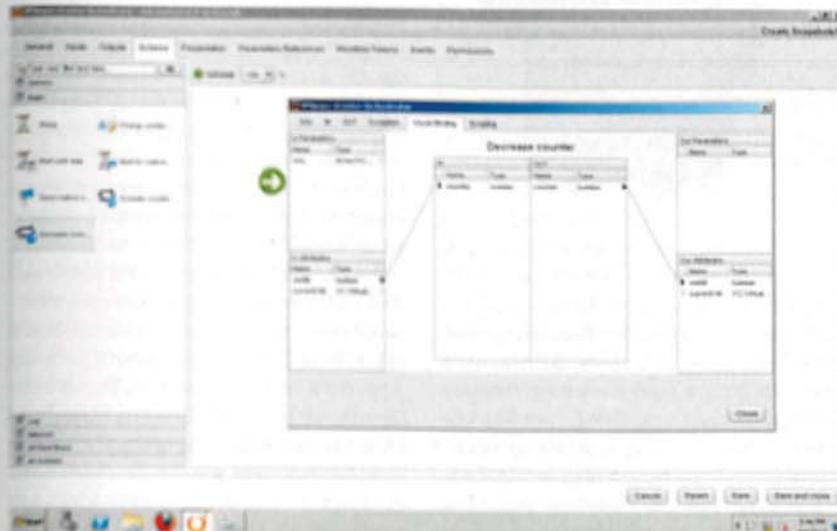
Falls ein Fehler beim untergeordneten Workflow auftritt, der den jeweiligen Snapshot erzeugt, folgt der Kontrollfluss dem roten Pfeil in Abbildung 9. Um das in den Workflow einzubauen, zieht man einfach die Komponente „Serverlog“ aus der Kategorie „Log“ auf das Element „Create a snapshot“. Daraufhin erzeugt der vCO den Pfad für die Fehlerbehandlung. Um den Kreis der Schleife im Workflow wieder zu schließen, muss man noch den ausgehenden blauen Pfeil von der „Serverlog“-Komponente zurück zum Entscheidungselement „VMs left?“ ziehen.

Damit die Log-Komponente die von der Snapshot-Komponente generierte Exception lesen kann, muss man die Snapshot-Komponente so konfigurieren, dass sie im Fehlerfall die Ursache in einem Attribut speichert. Hierzu wechselt man auf die Karteikarte „Exception“ (Abbildung 8) und verwendet den „Not set“-Link, um ein Attribut auszuwählen, das die Exception speichern kann. Nun möchte vCO ein neues Attribut *errorCode* erzeugen, das im Workflow bislang noch nicht vorhanden ist. Wenn man dem Link „Create parameter/attribute in workflow“ folgt und das folgende Dialogfeld mit OK bestätigt, erzeugt vCO es.

Jetzt stellt man noch die „Serverlog“-Komponente ein, damit sie die entsprechenden Werte auslesen und ins Log übertragen kann. Um das zu erreichen, legt man bei „IN“ die Parameter *text* und *object* fest. Im ersten Fall handelt es sich um ein generisches Fehlerattribut, dem man einen vordefinierten Wert, zum Beispiel „Error during snapshot creation“ ge-

Listing: Die Berichtsfunktion

```
var logText;  
for(i in vms){ var vm = vms[i]; if(vm.runtime.connectionState.value == "connected" && !vm.config.template)  
{  
    var actionResult = System.getModule("com.vmware.library.vc.vm.snapshot").getAllSnapshotsOfVM(vm);  
    if(actionResult.length > 0)  
    {  
        System.log("VM name: " + vm.name + " Number of snapshots : " + actionResult.length);  
        logText = "VM name: " + vm.name + " Number of snapshots : " + actionResult.length;  
        content = content + "<br>" + logText;  
    }  
}  
}  
var vmsLength=vms.length; System.log("VMs have snapshots: " + vmsLength); subjects = "VMs have snapshots: " + vmsLength;
```



Zusammenhang: Die Zuordnung der Variablen an die Ein- und Ausgabe stellt vCO grafisch dar (Abb. 11).

ben kann. Dem zweiten Parameter weist man das Attribut „errorCode“ zu. Zum Schluss kann man die Log-Ausgabe in der Designansicht mit der „Custom decision“ verbinden, damit der Kontrollfluss wieder an die Schleifensteuerung zurückgeht.

Auflisten von vorhandenen Snapshots

Der Workflow ist damit fertiggestellt. In der täglichen Praxis will man jedoch wissen, wie viele Snapshots existieren, schließlich belegen sie Speicherplatz und bedürfen einer regelmäßigen Kontrolle. Deshalb könnte man den hier vorgestellten Workflow um eine Berichtsfunktion ergänzen, realisiert durch zwei weitere Komponenten: eine Protokollierungskomponente als *scriptable task*, hier „Log Snapshots“ genannt und einen im vCO mitgelieferten Workflow zum E-Mail-Versand, der im Workflow-Selektor als „Send notification“ abrufbar ist und in der Bibliothek „Library/Mail“ liegt (Abbildung 10).

Alternativ bietet sich das Erstellen eines eigenen separaten Workflows an, der

einen Bericht mit allen vorhandenen Snapshots erzeugt und per E-Mail verschickt. Dank der im vCO eingebauten Scheduling-Funktion kann man diesen Bericht dann regelmäßig erzeugen und verschicken lassen.

Der Quellcode für die Skript-Komponente steht im Listing-Kasten und kann als Ausgangspunkt für eine eigene Umsetzung dienen, die hier nur skizzenhaft besprochen wird.

Um die Liste aller Snapshots zu generieren, erzeugt der Workflow zuerst ein Array, in dem er die VMs mit Snapshots speichert. In einer For-Schleife durchläuft er die Liste der virtuellen Maschinen. Falls eine VM im vCenter sichtbar und zugreifbar ist per

```
vm.runtime.connectionState.value == "connected"
```

und es sich um kein Template handelt, kann vCO die Liste aller Snapshots laden.

Im Folgenden veranlasst das Skript das Speichern der Informationen in den Variablen *content* und *subjects*. Da die E-Mail-Komponente dieselben Informationen benötigt, müssen die Variablen an entsprechende Workflow-Attribute

gebunden sein. Als Eingabeparameter dient wiederum die Variable *vms*. Der letzte Schritt im Workflow besteht darin, die Komponente „Send notification to mailing list“ in den Workflow einzubauen. Dabei müssen die Betreffzeile (*subject*) und der Inhalt (*content*) an die vorher erzeugten Attribute gebunden sein. Zusätzlich muss man die anderen benötigten Attribute (etwa für den Mailserver oder -adresse) erzeugen und mit entsprechenden Werten füllen. Damit ist der Teil des Workflows zum Übermitteln von Nachrichten über den Verlauf eingebaut.

Dem Erzeugen von Workflows folgt in der nächsten Ausgabe ein weiterer Schritt: Das Einbinden von Fremdsystemen in den vCenter Orchestrator. (rh)

Dr. Guido-Arndt Söldner

ist Dozent für Wirtschaftsinformatik an der FOM Hochschule für Oekonomie & Management und beschäftigt sich mit den Themen Automatisierung und Programmierung bei der Söldner Consult GmbH in Nürnberg.

Jens-Henrik Söldner

ist Dozent für Wirtschaftsinformatik an der FOM Hochschule für Oekonomie & Management und leitet das Infrastruktur-Consulting bei der Söldner Consult GmbH in Nürnberg.

Literatur

- [1] Jörg Riether; Servervirtualisierung; Doppelsteuerung: Versionsschritte in vSphere 5.1; iX 11/2012, S. 66
- [2] Sven Ahnert, André Dannbacher, Mathias Ewald, Jörg Riether, Jens-Henrik Söldner; Virtualisierung; Alles in allem; Aufwand und Kosten der Hypervisors: Hyper-V, XenServer, vSphere und KVM; iX 8/2012, S. 82

Nachrichten persönlich gestalten

Brief-Deko

Diane Sieger

Am Anfang war die Textnachricht, manchmal aufgepeppt durch Smileys. Heute kann man mit den richtigen Tools Nachrichten leicht durch Bilder, Fotos oder Videos einen persönlicheren Anstrich geben.



Viele erinnern sich bestimmt noch an den Beginn der Mobiltelefonie, als die ersten Handys für Privatpersonen auf den Markt kamen und preislich langsam erschwinglich wurden. SMS-Kurznachrichten fanden nur kurze Zeit später ihren Weg in die Geräte. Zunächst konnten einige Mobiltelefone zwar Kurznachrichten empfangen, jedoch nicht versenden, was heutzutage nur noch schwer vorstellbar ist. Seither hat sich im Bereich der SMS eine Menge getan – die einfache Aneinanderreihung von Buchstaben wird, insbesondere beim Versenden privater Messages, inzwischen oft als langweilig angesehen. Zum Glück gibt es eine Reihe von iOS- und Android-Anwendungen, die beim Verschönern mobiler Texte helfen.

ASCII-Art passt (fast) immer

Nostalgiker schwelgen gern in Erinnerung an ASCII-Art. Bei dieser Kunstform nutzt der Verfasser Buchstaben, Ziffern und Sonderzeichen, um kleine Piktogramme oder ganze Kunstwerke zu zaubern. Das funktionierte auch in mobilen Kurznachrichten, es dauerte jedoch je nach Motiv lange, bis die Handarbeit fertig war. Zudem gab es keine Garantie, dass ein Piktogramm auf dem Empfängerbildschirm exakt so aussah wie beim Verfasser – unterschiedliche Auflösungen und Zeilenumbrüche machten aus manchem Werk eine unübersichtliche Ansammlung willkürlicher angeordneter Zeichen. Heutzutage gibt es aber Apps, die Piktogramme bereits versandfertig zur Verfügung stellen.

Ein gelungenes Beispiel ist die iOS-App „Text Pics“ zum Preis von 0,89 Euro.

Aus einer umfangreichen Sammlung von Kategorien (Tiere, Feiern, Musik etc.) wählt der SMS-Künstler ein vorgefertigtes ASCII-Bildchen aus, das er per Knopfdruck direkt an einen Kontakt aus dem Adressbuch verschicken oder in die Zwischenablage des Mobiltelefons speichern kann. Letzteres empfiehlt sich, wenn er das Piktogramm noch verändern oder Text hinzufügen möchte. Zusätzlich kann er Lieblingsbilder als Favoriten sichern; eigene Kreationen kann er ebenfalls in den Speicher übernehmen und, wenn er will, mit den Machern der Anwendung teilen.

Android-Nutzern steht als Alternative „Text smileys and Emoticons“ zur Verfügung. Leider ergibt sich bei dieser App regelmäßig das altbekannte Problem mit ASCII-Bildern: Aufgrund unterschiedlicher Bildschirmgrößen und verschiedener Zeilenumbrüche in der Vielfalt der Android-Versionen kann es vorkommen, dass das Bildchen beim Empfänger nicht korrekt erscheint.

Kurztexter, die ihre Nachrichten nicht mit ASCII-Bildchen, sondern mit ansprechendem Design aufpeppen möchten, können ebenfalls auf ein großes Angebot zurückgreifen. Beispielsweise mit poppigen Hintergrundbildern oder Text in bunten Farben und verschiedenen Schriftarten. Für iOS-Geräte empfiehlt sich „Color Text Messages+“. Die Bedienung ist denkbar einfach: Hintergrund, Schrifttyp und -farbe auswählen und Nachricht eintippen, anschließend auf den Pfeil zum Versenden drücken. Dadurch wird die Nachricht als Bild in der Zwischenablage gespeichert und das Nachrichten-Programm geöffnet. Als Nächstes den Empfänger eingeben, das zwischengespeicherte Bild in das

Textfeld einfügen und auf „Senden“ drücken. Der Empfänger erhält nun die Nachricht als Image im Gesprächsverlauf.

Kleine Warnung: Die kostenlose Version, die bereits über mehr als 40 verschiedene Hintergrundbilder verfügt, nervt mit Werbeeinblendungen für andere Anwendungen des Herstellers. Da diese als Pop-up fast die gesamte Bildschirmfläche einnehmen und manuell geschlossen werden müssen, ist es unmöglich, sie zu ignorieren. Sobald man jedoch 48 zusätzliche Hintergrundmuster als In-App-Kauf zum Preis von 0,89 Euro erworben hat, fallen diese Werbeeinblendungen weg. Als Alternative bietet sich auch „Color Text Message HD Pro“ an. Die Anwendung bietet im Grunde genommen dieselben Funktionen wie die zuvor genannte App, kostet ebenfalls 0,89 Euro und ist stellenweise sogar etwas einfacher zu bedienen.

Ist der Text zu lang für eine SMS, soll aber trotzdem als etwas Besonderes wahrgenommen werden, lohnt sich ein Blick auf „Email Themes Stationery“ – eine App, die iOS-Nutzer für 0,89 Euro bei der Gestaltung von E-Mails unterstützt. Zwar ist die Bedienführung nicht die nutzerfreundlichste, wer jedoch den Anweisungen folgt, wird in der Lage sein, Mails mit verschiedenen Hintergründen von nett bis kitschig zu versenden. Ob Blumenfelder, abstrakte Muster oder Feiertagsmotive, hier ist für jeden Anlass etwas dabei.

Emoticons für alle Fälle

Sollten die zuvor genannten Möglichkeiten für das Design nicht ausreichen, heißt die Rettung „TextCutie“. Die App bietet eine umfangreiche Sammlung schöner Hintergrundbilder und Schriften zur Gestaltung von Nachrichten. Die Images kann der Anwender direkt aus TextCutie heraus zu Instagram hochladen oder in den Fotostream speichern und von dort aus in Kurznachrichten oder E-Mails einfügen. Zusätzlich können die Bilder in WhatsApp-Chats integriert und in zahlreiche Cloud Services (beispielsweise Dropbox, Evernote oder Google Drive) gespeichert werden. TextCutie gibt es gratis für iOS und Android. Für iOS vereint zusätzlich eine Pro-Version zum Preis von 4,49 Euro alle zur Verfügung stehenden In-App-Käufe.

Leser, denen die Auswahl von Hintergrundbildern, Schriftarten und -farben nach zu viel Arbeit klingt, die jedoch nicht darauf verzichten möchten, ihre Nachrichten durch das Hinzufügen von kleinen Bildern mehr Nachdruck zu verleihen, sollten sich die iOS-App „Emoji

Emoticon-Kunst“ anschauen. Die Anzahl verfügbarer Emoticons ist riesig, und umfasst unter anderem Smileys in allen emotionalen Zuständen (glücklich, traurig, verliebt, wütend etc.), aber auch Herzen, Tiere und weitere Symbole, die eine Nachricht visuell aufpeppen. Denbar einfach ist das Einfügen der Emoticons in Kurzmitteilungen, WhatsApp-Nachrichten oder Twitter- und Facebook-Updates: Das gewählte Symbol wird in der Zwischenablage gespeichert und kann durch anhaltenden Klick in das Nachrichtenfeld der gewünschten Anwendung kopiert werden. Zusätzlich zu den Mini-Symbolen verfügt die App über einen Word Maker, der gewünschte Worte aus Smileys zusammenbaut. Außerdem gibt es aus Emoticons zusammengestellte Szenen und Bilder, die man als Sticker versenden kann. Die Auswahl geht weit über das in iOS ab Version 5.0 integrierte Emoji-Keyboard hinaus.

Besonderes Gimmick für die iOS-APP „Emoji“ ist die Funktion „Emoji und Spaziergang“. Um das sichere Texten während des Spaziergangs zu gewährleisten, legt die App das Textfeld über die im iPhone integrierte Kamera. Der Anwender kann so durch das Mobiltelefon hin-

durchschauen und während des Laufens Nachrichten verfassen, ohne einen Laternenpfahl im Weg zu übersehen.

Das Sprudeln der Schorle

Sollten Emoticons und flippige Designs nicht ausreichen, um der eigenen Persönlichkeit in Kurznachrichten und E-Mails Ausdruck zu verleihen, hilft die kostenlose iOS-App „Animotions for iMessages“ weiter. Mit ihr kann man kurze Videoaufnahmen produzieren, die automatisch in animierte Gif-Dateien umgewandelt werden. Die Mini-Movies lassen sich innerhalb der App speichern, mit Text versehen und per iMessage oder E-Mail versenden, oder zu Tumblr, Twitter, Facebook oder imgur hochladen. Wer sich selbst in verschiedenen Stimmungen aufnimmt, etwa mit einem breiten Grinsen oder vor Wut kochend, braucht nicht mehr auf anonyme Smileys zurückzugreifen, um Freunden, Bekannten oder Familienmitgliedern den eigenen Gemütszustand mitzuteilen. Natürlich lassen sich auch andere Dinge mit „Animotions for iMessages“ aufzeichnen, das Gähnen des Stubentigers beispielswei-

URLs auf einen Klick

Die App-Infos gibt es auch online:
www.heise.de/ix/online/app-infos/



se oder das Sprudeln der prickelnden Apfelschorle am heißen Sommertag. Der Fantasie sind keine Grenzen gesetzt.

Wer statt der integrierten Kurzmitteilungs-Anwendung lieber den „WhatsApp Messenger“ – gratis zu haben sowohl für iPhones als auch für Android-Geräte – zum Chatten nutzt, kann inzwischen ebenfalls eine Reihe interessanter Zusatzangebote nutzen. Um seinem Gesprächspartner beispielsweise eine Zeichnung zu schicken, kann man auf „DrawTo“ zurückgreifen. Die Nutzung der App ist denkbar einfach: kleines Kunstwerk auf der Freifläche erstellen und an WhatsApp (wahlweise auch iMessage, Facebook, Twitter oder E-Mail) senden. Es stehen zwei Optionen zur Verfügung: Entweder, man schickt dem Chat-Partner einen Link, den dieser anklicken muss, um das Mini-Kunstwerk und dessen Erstellung im Browser anzuschauen, oder man fügt das Bild direkt in den Gesprächsverlauf ein. Beides sollte gut ankommen.

(ka)

Vor 10 Jahren: Der Chip von Fritz im ThinkPad

In zwei Jahren soll TPM für Windows 8.x obligatorisch werden. Einen PC mit dem dazu eingebauten Fritz-Chip konnte iX erstmals 2003 im Augenschein nehmen.

Ab 2015 müssen alle Rechner und Smartphones, die Microsoft Windows 8.x als Betriebssystem einsetzen, einen Fritz-Chip 2.0 besitzen. Ein Trusted Platform Module (TPM 2.0) soll dann beim Hochfahren des Geräts prüfen, ob beispielsweise das Betriebssystem unverändert ist. Das ist die Aufgabe des Fritz-Chip 2.0. Seine Funktion soll abschaltbar sein, doch ist der Chip selbst zwingende Voraussetzung dafür, dass der Gerätsteller das Logo „Windows 8 Compatible“ verwenden darf. Mit der TPM-Unterstützung setzt Microsoft den Ansatz des Trusted Computing um, den die Fachwelt vor 10 Jahren intensiv diskutierte.

Der Fritz-Chip geht auf einen Vorschlag des demokratischen US-Senators Ernest Frederick Hollings zurück, der sich mit einer ganzen Reihe von Gesetzesinitiativen für ein Digital-Rights-Management einsetzte. Unter anderem schlug er einen Chip vor, mit dem jedes

digitalisierte Musikstück auf einem Computer eine Seriennummer bekommt. Aus diesem Ansatz entwickelte die Trusted Computing Platform Alliance (TCPA) ab 1999 das Konzept des Trusted Computing, eine „Sicherheitskette“ von Kontroll- und Freigabevorgängen vom Booten des Rechners bis zum Starten autorisierter Software, bei denen ein Chip eine wichtige Rolle spielt. Das TCG-Mitglied Microsoft versprach seinerzeit, ab Windows Vista (Codename Palladium) Trusted Computing zu unterstützen.

Vor 10 Jahren kamen die ersten Rechner mit Fritz-Chips auf den Markt. Ein solchermaßen ausgerüstetes ThinkPad T30 von IBM (heute Lenovo) testete iX in Ausgabe 10/2003 unter Windows und Linux. Viel war es nicht, was man testen konnte. Ein sicheres Login des Nutzers und (nur unter Windows) die rudimentäre Verschlüsselung von Dateien. Das iX-tract des Testers fiel entsprechend nüchtern aus: „Eine solch hardwaregestützte Verschlüs-



selungstechnik nach den Vorschlägen der Trusted Computing Group birgt das Risiko einer ausfernenden Fremdkontrolle.“ Während die Fritz-Chips und ihre Nachfolger ihren Weg in die PCs fanden, wurde es ziemlich still um Trusted Computing.

Wir schreiben 2013. Die Nachrichten über Machenschaften der NSA reißen dank der Enthüllungen von Edward Snowden nicht ab. Viele Verschlüsselungsverfahren sind nicht vor dem Geheimdienst sicher, unter anderem, weil sie Zufallsgenerator benutzen, die kaum Zufälle kennen. Einer der Verdächtigen ist der Generator der Fritz-Chips. Auf „Zeit Online“ erscheint ein Artikel, in dem behauptet wird, dass die NSA auch den Standard TPM 2.0 kontrolliert. „Die NSA ist einverstanden“, dieser Satz soll in einem Treffen der Trusted Computing Group gefallen sein. Wenige Tage später wurde der Artikel gesperrt.

Zeit Online hatte außerdem behauptet, dass das BSI Risiken beim Einsatz von Windows 8 sieht, eben wegen der Unterstützung von Trusted Computing 2.0. Dagegen legte Microsoft erfolgreich Beschwerde ein. Wir leben in interessanten Zeiten.

Detlef Borchers (js)

Bevor es in diesem Monat nur noch ums Elektronische am Buchmarkt geht, seien ein paar papiere Bände vorgestellt, die sich mit den Cascading Stylesheets (CSS) beschäftigen – sowie einer, der ausschließlich als E-Buch vorliegt. Da es sich um Werke handelt, die erst kürzlich erschienen sind, behandeln sie die Stylesheets allesamt unter Einbeziehung der zum großen Teil noch in Entwicklung befindlichen Version 3. Moderne Browser unterstützen davon allerdings schon einiges, so dass Webdesigner vieles, teilweise noch mit Hersteller-Präfix, verwenden können.

Kai Laborenz' bei Galileo veröffentlichtes Handbuch zu CSS (siehe iX 5/2012) liegt jetzt in der zweiten Auflage vor und behandelt wie schon die erste CSS2 und CSS3. Wie es einem Handbuch kommt, geht der Autor gründlich von den Anfängen bis hin zu spezielleren Themen vor, die etwa Transformationen und Animationen beinhalten. Die Online-Version, nicht zu verwechseln mit den kostenlosen Openbooks, kommt fünf Euro preiswerter.

O'Reillys Pendant zu diesem Band, eins der bekannten „fehlenden Handbücher“, hat der Verlag Anfang des Jahres erneut veröffentlicht. Autor David Sawyer McFarland hat sein „CSS3“ überarbeitet und HTML5 einbezogen. Meist geht der Autor wie Laborenz vor, indem er implizit die Neuerungen von CSS3 in die Kapitel integriert. Gelegentlich, wie bei Transformationen und Animationen, sieht er ein eigenes Kapitel vor oder widmet sich Aspekten wie der Verwendung von (Web) Fonts, die bei Laborenz nicht vorkommen. Den englischsprachigen Band können Käufer außer auf Papier als PDF, Epub oder Mobi bekommen, für 6,50 Euro weniger.

Ausschließlich als E-Buch (PDF, Epub oder Mobi) hat die Open Source Press Peter Kröners „Einstieg in CSS3“ herausgegeben. Er hatte 2010 für denselben Verlag ein frühes Buch zu HTML5 geschrieben. Zwar hat die CSS3-Einführung nur 48 Seiten, dafür kostet sie lediglich 4,99 Euro. Eben nur ein Einstieg. Der Verlag beabsichtigt, demnächst weitere Bände „zu spe-

MEHR KBYTES

CSS3/E-Bücher

zifischen technischen Fragestellungen rund um CSS3“ zu veröffentlichen.

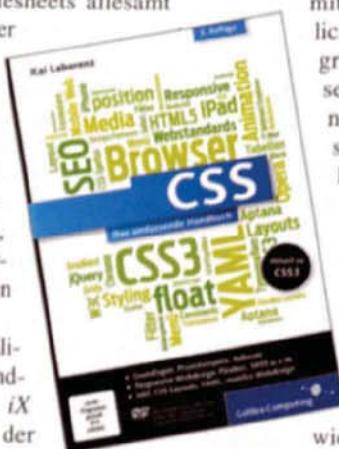
Zum E-Markt. Wer seine elektronischen Bücher als Epubs selbst verwaltet, nutzt

mit recht großer Wahrscheinlichkeit ein Open-Source-Programm namens Calibre, das seit Jahren in einer 0.x benannten Version vorlag, aber stabil arbeitete. Im August kam der magische Moment: Version 1.0 kann MS-Word-Dokumente konvertieren, Schriftarten einbetten und enthält eine Cover-Ansicht der vorhandenen Bücher. Außerdem haben die Entwickler das Datenbank-Backend neu geschrieben, sodass es erheblich schneller geworden ist. Und Anwender können ihre Bestände in virtuelle Bibliotheken unterteilen.

Mittlerweile liegt Version 1.3 vor, denn seit August wurden etliche Fehler beseitigt und neue Eigenschaften hinzugefügt (siehe „Alle Links“).

Carta statt Pearl. Amazons neuer E-Bookreader Paperwhite beinhaltet als erster die neue Version von E-Ink. Mit Carta wirds noch kontrastärker, und dank „Regal“ genannter Technik können die Reader die alten Pigmente besser entfernen, was das Invertieren vor dem neuen Darstellen nicht mehr erfordert. Der neue Paperwhite soll als WLAN-Version 130 Euro kosten, mit 3G-Modul 190. Lieferbar ab Oktober beziehungsweise November. Klar dass Kobo und Sony ihre Lesegeräte vor der IFA ebenfalls noch einem Update unterzogen haben, wenn auch (noch) ohne Carta.

Ein wahrscheinlich auf den deutschen Buchmarkt kaum anwendbares Projekt hat Amazon unter dem Namen Kindle MatchBook ins Leben gerufen. Für den



Peter Kröner; Einstieg in CSS3; Standards und Struktur; München (Open Source Press) 2013; 48 Seiten; 4,99 € (Epub/Mobi/PDF)

Kai Laborenz; CSS; Das umfassende Handbuch; Bonn (Galileo) 2013; 2. Auflage; 791 Seiten zzgl. DVD; 39,90 € (gebunden); 34,90 € (Online)

David Sawyer McFarland; CSS3; the missing manual; Sebastopol, CA (O'Reilly) 2013, 3. Auflage; 638 Seiten; 29,- € (Paperback); 22,45 € (E-Buch)

US-Markt hat Amazon Verträge mit einigen Verlagen geschlossen, die bedeuten, dass Kunden Bücher, die sie jetzt kaufen oder seit 1995 gekauft haben, für'n Appel

und 'n Ei zusätzlich als E-Buch bekommen können: zwischen kostenlos und 2,99 US-\$ Davon können Europäer nur träumen.

Der deutsche Kulturrat, der Börsenverein des Deutschen Buchhandels sowie zwei französische Verbände von Handel und Verlagen warnen in einer gemeinsamen Erklärung vor der Dominanz von Amazon, Google und anderen nichteuropäischen Konzernen. Ihre Deklaration zur Zukunft des Buches erschöpft sich allerdings darin, die Buchpreisbindung vor internationalen Handelsabkommen schützen zu wollen, die ermäßigte Mehrwertsteuer

für E-Bücher zu fordern und das Autorenrecht zu betonen. Ob das allein die europäische Buchkultur vor US-Firmen zu retten vermag, sei hiermit be zweifelt.

Wie weit digitales Lesen in Deutschland gekommen ist (und wie weit nicht), zeigt unter anderem die Shortlist für den Deutschen Buchpreis, das Pendant zu Prix Goncourt und Man Booker Prize. Vier der sechs ausgewählten Romane können Leser außer auf Papier in elektronischer Variante lesen. Hanser und der Luchterhand Literaturverlag beschränken sich auf traditionelle Papier.

E-Literatur außerhalb des Buchmarkts diskutierten Protagonisten schon in den 90er-Jahren als „Netzliteratur“. Rowohlt will mit Andreas Winkelmanns „Deathbook“ ab dem 24. September (nach Redaktionsschluss) einen multimedialen Neuanfang innerhalb des Buchmarkts versuchen: zehn E-Bücher, wöchentlich als Fortsetzung ausgeliefert. Verlag und Autor haben Facebook, Twitter, Blogs sowie Videos „in die Handlung integriert“, Leserreaktionen sollen in die Handlung zurückfließen, und eine gecastete Bloggerin erweitert den Figurenreigen. Im Dezember will Rowohlt eine gedruckte Version veröffentlichen. Ein bisschen Buchmarkt muss noch sein.

Hennig Behme (hb)

[Alle Links: www.iX.de/ix220160](http://www.iX.de/ix220160)



Jonas Hellwig

Responsive Webdesign

Das umfassende Praxistraining

Bonn 2013
Galileo Computing
Lehrprogramm (Video)
39,90 €
ISBN 978-3-8362-2312-6

Responsive Webdesign ist die Kunst, Webseiten so zu gestalten, dass sie sich automatisch an die Darstellungsgröße des Browsers anpassen, sei es ein Desktop, sei es ein mobiles Gerät. Startet man bei der Entwicklung der Seite mit dem Design für den Desktop und vereinfacht es anschließend für eine optimale Darstellung auf mobilen Geräten, heißt der Vorgang

„Graceful Degradation“, während man den umgekehrten Weg „Mobile First“ nennt.

Jonas Hellwig zeigt in seinem Videotraining beides. Er beginnt mit einer Einführung, die statisches Design versus Responsiv Design diskutiert, und demonstriert anschließend mit einer Beispieldatei, wie Webdesigner statisches Layout in ein flexibles überführen können. Dieses Praxisbeispiel

weckt Lust auf mehr. Und so gelingt es Hellwig, genügend Spannung aufzubauen, um den Zuschauer in den folgenden Kapiteln mitzunehmen und intensiver in die einzelnen Bereiche einzutauchen. Dabei geht er sowohl auf den denkbaren Workflow der Entwicklung als auch auf die Anlage der Projekte, die Gestaltung einzelner Blöcke und Typografie ein, vergisst dabei aber Fehlersuche und Optimierung nicht.

Er unterlegt seinen Vortrag immer wieder mit Beispieleseiten aus dem Web. Ebenso zeigt er zahlreiche Seiten, die dem Entwickler nützliche Tools bieten, sei es zur Umrechnung von Pixeln in Prozent oder Boilerplate-Code. Allerdings erwähnt er einige interessante Seiten nur kurz und benennt die URLs nicht. In solchen Situationen wird die Pause-Taste zum wichtigen Instrument, um die gezeigte URL tatsächlich nutzen zu können.

Mit dem erworbenen Wissen geht es an zwei Projekte, mit denen der Trainer „Graceful Degradation“ und „Mobile First“ noch mal im Detail vorführt. Bei Letzterem hat sich ein technisches Problem eingeschlichen: Die Konzeption kommt dem Zuschauer allzu bekannt vor. Hier sieht er die Beispiele aus dem ersten Kapitel wieder. Das korrekte Kapitel bietet Jonas Hellwig auf seiner Site zum Download an, sodass dieser Fauxpas nicht übermäßig ins Gewicht fällt.

Anschließend geht er auf die Besonderheiten des Designs in Bezug auf Retina-Displays ein. Den Abschluss bildet ein spezielles Kapitel zu Adobes Edge Reflow. Trotz sprachlicher Wiederholungen bietet Hellwig insgesamt ein kurzeiliges und informatives Training, das es erlaubt, das Gesehene schnell in die Praxis umzusetzen.

Michael Müller (hb)



Ines Rossak (Hrsg.)

Datenintegration

Integrationsansätze, Beispielszenarien, Problemlösungen, Talend Open Studio

München, Wien 2013
Hanser
226 Seiten
29,99 €
ISBN 978-3-446-43221-5

Es könnte alles ideal sein. Man nehme die Idee für eine Unternehmensanwendung und lasse hierfür ein wunderbares Datenmodell ohne Redundanzen und Widersprüche entstehen. Über den Lebenszyklus vielleicht noch hie oder da eine kleine Anpassung, aber prinzipiell ist alles in Ordnung. Weit gefehlt. Plötzlich erfolgt die Fusion mit dem Unternehmen Foo, dessen Datenmodell mit dem eigenen nicht übereinstimmt. Und da gibt es den neuen Vorstand Bar, der für HR und

CRM auf andere Software setzen will. Und die Revision stellt fest, dass sich über die Jahre Insellsungen auf Basis von Tabellenkalkulation und Desktop-Datenbank gebildet haben, die ihre Daten über hervorragende manuelle Eingaben oder Copy and Paste austauschen.

Wie das Bereinigen einer solchen Situation aussehen könnte, zeigt Ines Rossak als Herausgeberin. Im Rahmen des Masterstudiengangs „Angewandte Informatik“ haben sich fünf ihrer Studenten ent-

schlossen, dieses Thema für ein Buch aufzubereiten. Ziel der Bemühungen war eine Einführung in die Datenintegration sowie ein Lösungsansatz auf Basis des Open-Source-Tools Talend Open Studio. Und so führt das Grundlagenkapitel in die typischen Einsatzfelder ein, die im operativen und im analytischen Bereich liegen. Weiter behandeln die Autoren ausführlich die Integrationsherausforderungen, Ebenen, Architekturen und Aufgaben, was dem Leser einen umfassenden und bis dahin technikneutralen Einblick verschafft.

Im dritten Kapitel thematisieren sie die Technik, kommerzielle Anbieter knapp und etwas umfangreicher Produkte aus dem Open-Source-Sektor. Detaillierter geht es im Rahmen des Praxisbeispiels zu. Zwei Kapitel stellen die Installation und Konfiguration der Datenbanken vor.

Kapitel 7 konzentriert sich auf das Talend Studio for Data Integration. Es bildet die Basis für das Projekt, das sich im

Folgenden auf über 60 Seiten erstreckt. Dabei kommen eine Vielzahl von Screenshots, Diagrammen und Tabellen zum Einsatz, sind teilweise jedoch zu klein. Ebenso geht durch den starken Bezug auf das Werkzeug einiges an Grundlagen verloren. Den Abschluss bilden der Import und Export von Projekten, eine Zusammenfassung und Schemadiagramme der drei Datenbanken.

Datenintegration ist in der Tat ein spannendes Thema und die Harmonisierung von Datenmodellen nicht trivial. Die Einführung in dieses Gebiet gelingt den Autoren anschaulich, die Diagramme erleichtern das Verständnis. Mit dem Einstieg in die Welt der Werkzeuge und in das Beispielprojekt ändert sich das Bild leider. Das Ziel, eine Vielzahl visueller Hilfsmittel einzusetzen, ist prinzipiell gut. Nur leider eignen sich Screenshots hier weniger. Und der starke Bezug auf ein konkretes Tool lenkt vom Thema ab. Das trübt den Eindruck des Buchs etwas.

Frank Müller (hb)

Die Vernetzung der Welt

Ein Blick in unsere Zukunft

*Eric Schmidt
Jared Cohen*

Eric Schmidt, Jared Cohen

Die Vernetzung der Welt

Ein Blick in unsere Zukunft

Reinbek bei Hamburg 2013
Rowohlt
Übersetzt von Jürgen Neubauer
441 Seiten
24,95 €/E-Buch 21,99 €
ISBN 978-3-498-06422-8

Das „größte Anarchismusexperiment aller Zeiten“ nennen Google-Chef Eric Schmidt und sein Mann für Ideen Jared Cohen in ihrer Einleitung das Internet. Und in sieben Kapiteln stellen sie anschließend dar, was die Zukunft für die Menschen, Staaten, Revolutionen, den Terrorismus, Konflikte/Kriege, Wiederaufbau sowie Identität, Zivilgesellschaft und Journa-

lismus bereithalten dürfte. Schmidt und Cohen sehen „Grund zum Optimismus“, was die Effekte der Technikentwicklung auf das physische Umfeld angeht, und sie beschreiben teilweise jene schöne neue Welt, die allen mehr Freiheit und Wohlstand bringen soll. Allerdings verschließen sie nicht die Augen davor, dass Technik gleichzeitig mehr Schnüffelei, Überwachung und

Einschüchterung ermöglicht: „Alles, was ein Regime zum Aufbau einer schlagkräftigen Digitalpolizei benötigt, ist heute auf dem Markt erhältlich“. heißt es beispielsweise.

Als Warner Bros. nach dem 11.9.2001 die Premiere des Schwarzenegger-Films „Collateral Damage“ verschob, war von Online-Überwachung nicht die Rede. Hier schreiben die Autoren: „Der Kollateralschaden dieser Überwachung besteht [...] vor allem im drohenden staatlichen Missbrauch und in Fehleinschätzungen durch die Internethüter.“

Sätze wie, dass Menschen sind, was sie tweeten, und Marketing nicht mit Information gleichzusetzen ist, gehören zu den weniger erhellenden Aussagen, aber insgesamt zieht ein leicht kritischer Wind durch den Band; etwa der Konflikt zwischen dem Schutz der Privatsphäre und der inneren Sicherheit.

Regierungen stellen nicht das einzige Gefahrenpotenzial, weswegen der Band ein ganzes Kapitel zum Terrorismus enthält. Positives sehen Schmidt und Cohen vor allem für Phasen des Wiederaufbaus nach einem Krieg oder einer Katastrophe. Handys für Milizionäre im Austausch gegen Waffen sowie allgegenwärtige Smartphones als Mittel, sich mit anderen und Aufbauwendungen zu vernetzen und sich einzumischen, erachten die Autoren als kleine Schritte auf dem Weg nach vorn.

Geschrieben im Jahr vor Snowden, hat der mit reichlich Hintergrundlinks versehene Band selbst danach genügend Inhalt, um eine nachdenklich stimmende Lektüre zu bieten. Und sei es nur wegen des Fazitelsatzes: „Wenn wir uns nicht für unsere Privatsphäre einsetzen, werden wir sie verlieren.“

Henning Behme (hb)



Scrum Master Zertifizierung (CSM) Jeff Sutherland

Zwei-Tages-Scrum Workshop

Dr. Jeff Sutherland wird seinen Workshop „Certified Scrum Master“ auch dieses Jahr bei uns in Deutschland durchführen. Lernen Sie von der Person, die das erste Scrum Team ins Leben gerufen hat und zusammen mit Ken Schwaber als die Begründer von Scrum gelten. Profitieren Sie von seinen Erfahrungen, die er in unterschiedlichen Unternehmen erlangt hat und genießen Sie die Anekdoten von denen der wohl erfahrenste Scrum Trainer zu berichten weiß.

Nutzen Sie diese einmalige Gelegenheit den „geistigen Vater“ von Scrum zu treffen und werden Sie „Certified Scrum Master certified by Jeff Sutherland“.

TERMIN: 10. - 11. Oktober 2013 in München

Die Teilnehmeranzahl für dieses Scrum Training ist begrenzt.
Melden Sie sich am besten noch heute an.
Das Scrum Seminar wird in englischer Sprache abgehalten.

Alle Teilnehmer erhalten im Vorfeld eine E-Mail mit allen wichtigen Eckdaten zum Certified Scrum Master Training. Vorläufiger Zeitplan des CSM:

- erster Tag: (8:30 Registrierung) 9:00 - 17:00 Uhr
- zweiter Tag: 9:00 - 17:00 Uhr

Weitere Infos unter: www.ix-konferenz.de und www.scrum-events.de

**Jetzt
buchen!**



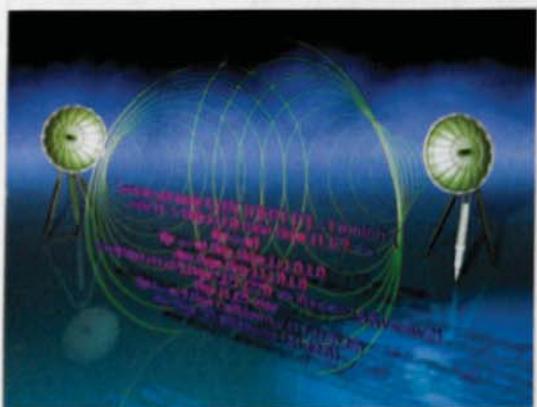
Dr. Jeff Sutherland ist der Mitbegründer von Scrum und ein erfahrener Scrum Consultant. Er entwickelte Scrum zusammen mit Ken Schwaber zu Beginn der 90ziger Jahre. Zu seinen Referenzen zählen weltweit führende Unternehmen wie Cisco, Google, Yahoo, Microsoft, IBM, Oracle, MySpace, Adobe, Siemens, Sony/Ericson und Accenture.

Eine Veranstaltung von:



In Zusammenarbeit mit:





Video-Konferenzen zwischen Browsern

Direkte Echtzeitkommunikation zwischen Webbrowsern hat das World Wide Web Consortium schon seit zwei Jahren in Arbeit. Die Spezifikation befindet sich zwar noch wie vor im Entwurfsstadium, doch es gibt bereits Dienste wie palava.tv von der Dresdner Innovavailable, der plug-in-freie Videokonferenzen zwischen WebRTC-fähigen Browsern wie Firefox und Chrome erlaubt.

SonarQube analysiert Codequalität

Zur Softwareentwicklung gehört kontinuierliches Testen. Ob sich der Code so verhält wie gewünscht, zeigen in der Regel Unit-Tests. Die sagen aber nicht unbedingt etwas über die strukturelle Qualität des Quellcodes aus. Hier zeigt das Maven-Projekt SonarQube seine Stärken: Die Webanwendung stellt Projekte und deren Qualitätsmetriken in allen gängigen Browsern dar.

Firewalls der nächsten Generation

Mit dem Schlagwort „Next Generation“ preisen viele Hersteller ihre aktuellen Firewalls an. Einbinden mobiler Geräte, umfangreicheres Rechtemanagement, Daten auf dem Applikations-Layer untersuchen – die Produkte sollen gerade im Unternehmenseinsatz mehr Sicherheit schaffen. Was die Angebote unterscheidet, klärt die Marktübersicht in der nächsten iX.

Heft 11/2013
erscheint am 24. Oktober 2013

Kein wichtiges Thema mehr versäumen!

Abonnieren Sie jetzt unseren **Newsletter** oder folgen uns ganz einfach auf **Facebook**. So bleiben Sie immer up to date!

www.iX.de/newsletter



www.facebook.com/iX.magazin



AMD Notebooks: 3D-Power für kleines Geld

PC-Fernwartung vom Android-Tablet
Sat to IP: Netzwerk statt Antennenkabel

E-Mail privat: Provider-Wahl, Konfiguration, Verschlüsselung

Heft 22/13 ab 7. Oktober am Kiosk

Technology Review



Die Welt in zehn Jahren: So stellen sich Technologiepioniere unsere Zukunft vor.

Hirnstimulation: Eine Stromtherapie fürs Gehirn verspricht die Linderung von Gesundheitsproblemen.

Heft 10/13 ab 26. September am Kiosk



Freies Cloud-Computing mit Open Stack: Grundlagen, Installation und Betrieb eines eigenen Cloud-Systems

29. - 30. Oktober 2013 in Hamburg