FÜR IT-ENTSCHEIDER
com! professional

All for One Steeb AG

Suchbegriff 1. All for One, -Steeb AG

Verlag Neue Mediengesellschaft Ulm mbH, URL: www.nmg.de
Redaktion com! professional Redaktion, Tel.: 089 74117 302, E-Mail: redaktion@com-magazin.de

Ausgabe 01.08.2017 • Nr. 8/2017
Seite 40
Rubrik

Medientyp Special Interest
Erscheinungsweise monatlich
Branche IT Allgemein
Bundesland Überregional

Publikation	verkauft	verbreitet	gedruckt	Reichweite Mio	Medien-Nr.
com! professional	16.320	19.165	30.234	0,11	88283

ARGUS DATA INSIGHTS® Deutschland GmbH
Gneisenaustr. 66, 10961 Berlin | T +49 30 203 987-0 | F +49 30 203 987-77 | E sales@argusdatainsights.de | www.argusdatainsights.de

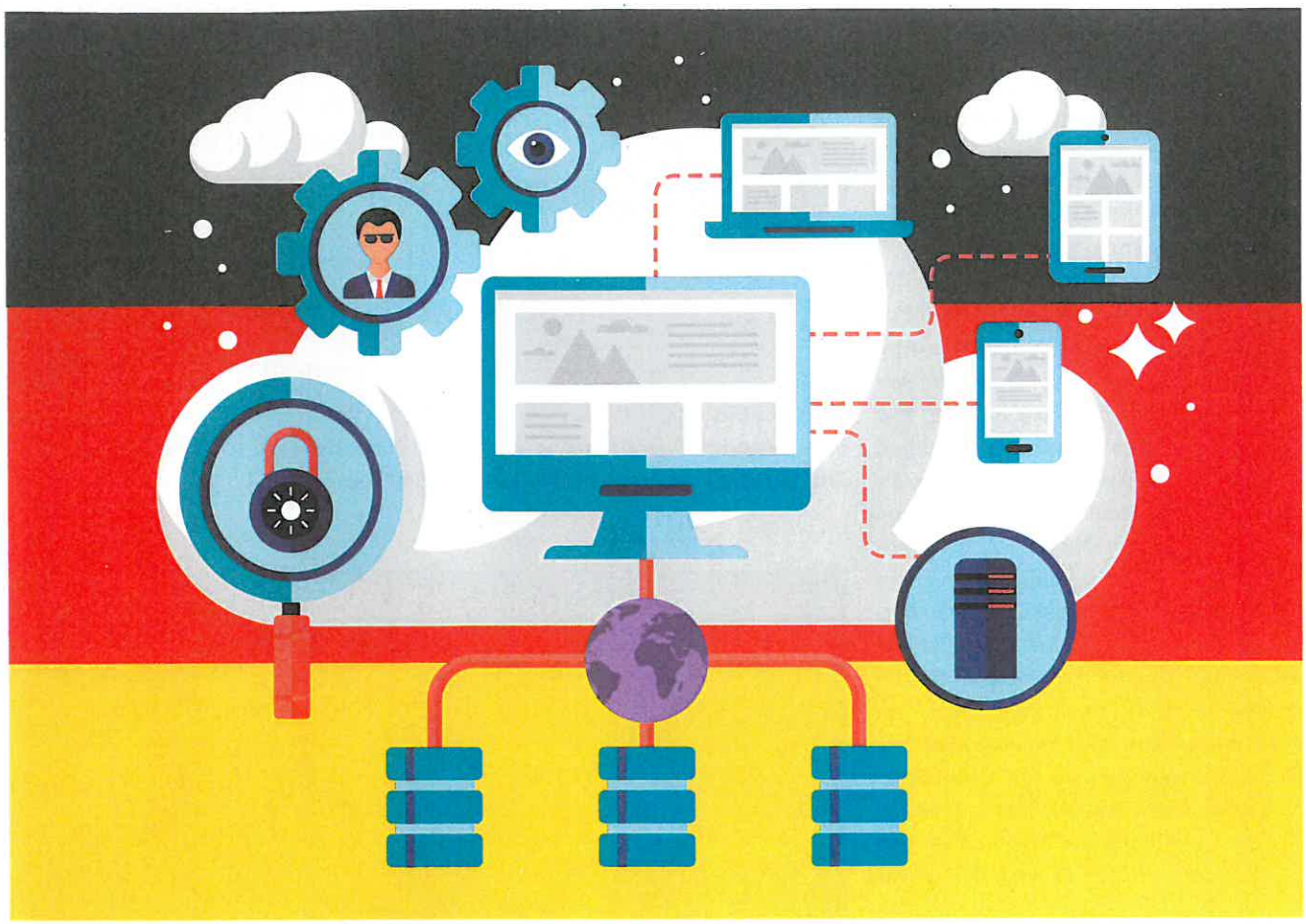


Foto: Shutterstock / girafchik

Schutz für Daten und Dienste

Public Clouds made in Germany

Mit Cloud-Services aus deutschen Rechenzentren behalten Unternehmen die Kontrolle.

Cloud-Computing ist für einen Großteil der Unternehmen unverzichtbar geworden. Da sind sich die Marktforscher einig. „Cloud-Computing ist als Kernkomponente in den deutschen Unternehmen gesetzt. Die Mehrheit der Unternehmen beschäftigt sich intensiv mit diesem Thema", sagt beispielsweise Björn Böttcher, Senior Analyst & Data Practice Lead beim Analystenhaus Crisp Research. „Nur bei knapp 15 Prozent der Unternehmen zählt Cloud-Computing noch nicht zum Portfolio ihrer IT-Strategien." Zu einer ähnlichen Einschätzung kommt der „Cloud-Monitor 2017", den das Beratungshaus KPMG in Zusammenarbeit mit Bitkom Research erstellt hat. Danach nutzten 2016 über 80 Prozent der deutschen Unternehmen Cloud-Dienste oder hatten konkrete Pläne, dies zu tun – 11 Prozent mehr als im Vorjahr.

Cloud-Skepsis

Allerdings haben Firmen in Deutschland klare Vorstellungen, was den Speicherort und den Schutz ihrer Daten in einer Cloud betrifft. Laut Cloud-Monitor bestehen 77 Prozent auf einem Provider mit Hauptsitz im Rechtsgebiet der Europäischen Union. An die 71 Prozent der Cloud-Nutzer halten Rechenzentren in Deutschland für unverzichtbar, 60 Prozent bevorzugen sogar einen Anbieter, dessen Firmensitz in Deutschland liegt. Den Hauptgrund für diese vorsichtige Haltung kennt Olaf Köppe, Partner und Head of IT Compliance bei KPMG: „Die größten Bedenken gegenüber öffentlichen Cloud-Diensten haben deutsche Unternehmen beim Datenschutz. Sie befürchten, dass Cloud-Computing die Einhaltung von Compliance-Anforderungen gefährdet."

Vor allem die neue Datenschutz-Grundverordnung (DSGVO) der Europäischen Union veranlasst Unternehmen, ihre Cloud-Strategie zu überprüfen. Die DSGVO muss ab dem 25. Mai 2018 umgesetzt werden. Sie sieht unter anderem vor, dass auch ausländische Cloud-Service-Anbieter die Vorgaben der Grundverordnung beziehungsweise General Data Protection Regulation (GDPR), so der englische Begriff, erfüllen müssen. Wer einen Cloud-Dienst nutzt und damit sensible Daten bearbeitet, etwa Kundeninformationen oder Gesundheitsdaten, muss prüfen, ob sein Provider die Datenschutz- und Datensicherheitsregeln einhält. Hinzu kommen erweiterte Dokumentationspflichten in puncto Datenschutz für den Provider und den Cloud-Service-Nutzer sowie verschärfte Meldepflichten und Strafen bei einem Datenleck.

Nach Einschätzung von Rechtsanwalt Jens Eckhardt, Vorstand Recht & Compliance bei EuroCloud Deutschland_eco e. V., stellt die DSGVO für Provider aber keine unüberwindbare Barriere dar. Er empfiehlt ihnen, proaktiv auf ihre Auftraggeber zuzugehen und die neuen Vorgaben bereits jetzt in den gemeinsamen Verträgen umzusetzen. „In den meisten Fällen ist es ausreichend, sich auf andere Vertragstexte zu einigen. Eine Änderung an den Service-Prozessen allein wegen der DSGVO wird in den seltensten Fällen notwendig sein", so der Jurist.

Foto: KPMG

„Deutsche Unternehmen befürchten, dass Cloud-Computing die Einhaltung von Compliance-Anforderungen gefährdet."

Olaf Köppe
Partner und Head of IT Compliance bei KPMG
https://home.kpmg.com/de

Gefahr durch US-Gesetze

Vor dem Hintergrund der DSGVO haben sich alle führenden Cloud-Service-Anbieter aus den USA dazu verpflichtet, diese Vorgaben einzuhalten. Dazu zählen Amazon Web Services (AWS), Google, IBM, Microsoft und Oracle. Auch dem Wunsch deutscher Unternehmen, Daten ausschließlich in Rechenzentren auf dem Boden der Bundesrepublik zu verarbeiten, kommen sie nach. AWS, IBM und Microsoft haben bereits Datacenter in Deutschland eröffnet. Google und Oracle wollen das noch 2017 tun. Allerdings droht von anderer Seite Gefahr: US-Präsident Donald Trump hat angekündigt, dass er die Maßnahmen erweitern wird, die dem Schutz der USA dienen. Darunter fällt auch ein reduzierter Datenschutz für Bürger ausländischer Staaten. Einen entsprechenden Erlass unterzeichnete Trump am 25. Januar dieses Jahres. Er tangiert jedoch (noch) nicht Bürger von EU-Staaten. Vielmehr garantiert das EU-US-Privacy-Shield-Abkommen von 2016 für Daten von EU-Bürger einen vergleichbaren Schutz wie in Europa. Unklar ist derzeit aber, ob diese Vereinbarung Bestand haben wird.

Foto: Deutsche Telekom AG

Geschützt wie eine Festung: Das Zwillings-Rechenzentrum der Deutschen Telekom in Biere bei Magdeburg.

Viele Anbieter zur Wahl

Wer einen Cloud-Service aus der Hand eines Anbieters mit Sitz in Deutschland oder der EU ordern möchte, der zudem Daten des Nutzers ausschließlich in Rechenzentren in der EU speichert, hat mittlerweile eine Fülle von Optionen. Der Lösungskatalog der „Initiative Cloud Services Made in Germany" führt mehr als 200 Angebote auf. Allerdings fehlen dort etliche relevante Anbieter, etwa die Telekom mit der Open Telekom Cloud, T-Systems, Strato oder QSC. Auch das Beratungshaus ISG (ehemals Experton Group) verzeichnet in seinem „Cloud Vendor Benchmark 2016" mehr als 200 Anbieter.

Welchen Cloud-Service-Provider ein Unternehmen benötigt, hängt von seinen Anforderungen sowie der Service-Palette des Anbieters ab. Das mit Abstand umfangreichste Angebot von Public-Cloud-Diensten stellen Amazon Web Services AWS und Microsoft bereit, gefolgt von Google, Oracle und IBM. Anbieter mit einem vergleichbaren Produktportfolio, die zudem ihren Hauptsitz in einem Mitgliedsland der Europäischen Union oder in Deutschland haben, sind dünn gesät.

11,7 Mrd.
Dollar gaben Unternehmen in Westeuropa 2016 für SaaS aus

Quelle: IDC

In der Liga der großen Cloud-Service-Provider wollen Deutsche Telekom und 1&1 mitspielen. Gleiches gilt für Fujitsu mit seiner K5-Cloud. Dieser Anbieter verweist trotz seiner japanischen Muttergesellschaft gern auf seine deutschen Wurzeln, Stichwort Fujitsu-Siemens.

Zudem haben Systemhäuser wie Bechtle, Cancom/Pironet, Allgeier oder All for One Steeb die Cloud als Geschäftsfeld entdeckt. Sie verfügen über Datacenter in Deutschland und konzentrieren sich vor allem auf gemanagte Cloud-Services. Das heißt, die Cloud-Dienste werden vom Systemhaus über eigene Datacenter oder gemietete Ressourcen in Rechenzentren mit Sitz in Deutschland bereitgestellt. Die Verwaltung und Abrechnung der Dienste sowie die Anbindung die IT-Umgebung des Nutzers übernimmt das Systemhaus.

Hinzu kommt eine Vielzahl von Spezialanbietern. Der Berliner Service-Provider Profitbricks etwa fokussiert sich auf preisgünstige IaaS-Dienste (Infrastructure as a Service); Strato, Web on Drive oder Hornetdrive stellen Online-Speicherdienste für geschäftliche Nutzer in den Vordergrund. ▶

Public Clouds aus Deutschland

Zunächst ein Blick auf die Anbieter von Public-Cloud-Diensten, die sich an Amazon Web Services, Microsoft und Co. orientieren.

Open Telekom Cloud (OTC): Die Cloud-Plattform der Deutschen Telekom ist in Deutschland seit einem Jahr verfügbar. Die Rechenzentren in Biere bei Magdeburg und Frankfurt am Main, die von der Telekom-Tochter T-Systems gemanagt werden, nutzt auch Microsoft für seine Deutschland-Cloud-Services, etwa Office 365 und Azure. Angeboten werden bei OTC Cloud-Dienste für Infrastruktur (IaaS), Plattform (PaaS) und Software (SaaS).

Das Beratungshaus ISG/Experton Group attestiert OTC eine große Auswahl an unterstützten Plattformen und Services sowie Kostentransparenz. Hinzu kommen das hohe Sicherheitsniveau und der laut ISG „exzellente" Kunden-Service. Im Bereich Rechenleistung hat der Nutzer beispielsweise die Wahl zwischen „Elastic Compute"-Diensten auf Basis virtueller Maschinen und einem Auto-Scaling-Angebot, das sich an wechselnde Lasten anpasst. Zudem sind dedizierte Hosts verfügbar, sprich separate Virtual Machines.

Ein weiterer Pluspunkt von OTC ist, dass das Angebot auf das Open-Source-Cloud-Framework OpenStack setzt. Dadurch entfällt die Bindung an herstellerspezifische Ansätze. Zudem erleichtert OpenStack die Migration von Workloads in die Open Telekom Cloud oder zu anderen Cloud-Plattformen.

Daniel Klemm, Senior Analyst bei Crisp Research, sieht bei OTC allerdings Nachholbedarf in puncto Services, die für Start-ups und Unternehmen wichtig sind, die native Cloud-Anwendungen entwickeln und nutzen. So fehle es an Diensten wie „Function as a Service", die für Serverless Computing wichtig sind. Auch eine NoSQL-Datenbank und ein API-Gateway sind laut Klemm im Gegensatz zu AWS, IBM oder Microsoft Azure nicht verfügbar.

Fujitsu K5: Die Cloud-Plattform K5 hat Fujitsu hierzulande im Frühjahr dieses Jahres an den Start gebracht. Der deutsch-japanische Konzern unterhält in Deutschland zwei für die K5-Cloud reservierte Rechenzentren. „Nutzer unserer K5-Cloud können vorgeben, wo Datenbestände gespeichert werden, etwa ausschließlich in den Cloud-Rechenzentren in Deutschland", betont Uwe Scheuber, Director Business Development Cloud & Hybrid IT bei Fujitsu. Ebenso wie die Telekom bietet Fujitsu K5 IaaS-, PaaS- und SaaS-Dienste an.

Das Software-Angebot fristet allerdings bislang noch ein Schattendasein. Doch das ändere sich, so Uwe Scheuber: „K5 liefert bereits SaaS-Services, etwa Database as a Service. Der weitere Ausbau der Angebote auf Basis unserer K5-Plattform findet kontinuierlich statt – sei es direkt oder über Partner, die eigene Angebote auf Basis von K5 offerieren können." Die Partnerschaften, teilweise auch mit Spezialanbietern wie dem Telekommunikationsunternehmen Nfon, führt ISG/Experton Group als einen der Vorteile von Fujitsu an. Das Unternehmen stellt zudem branchenspezifische Cloud-Plattformen (Industry Clouds) zur Verfügung, etwa für die Industrie, den Handel oder die Finanzbranche.

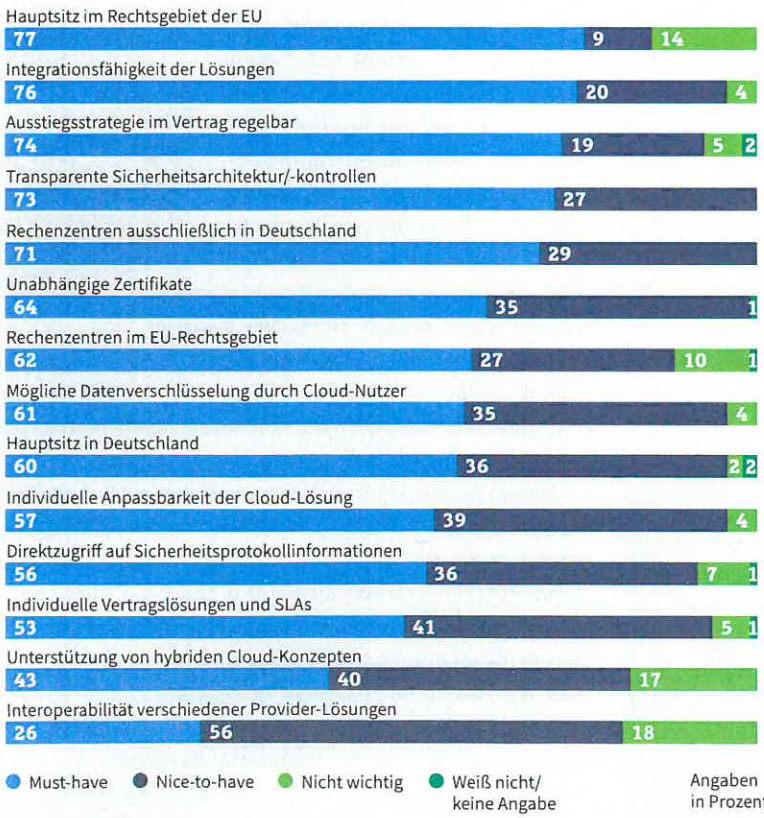
Ebenso wie die Open Telekom Cloud nutzt Fujitsu K5 OpenStack: „Ein entscheidender Punkt ist die Offenheit, unter anderem durch den Einsatz von OpenStack: Kunden haben mit K5 keine Einschränkungen durch einen Vendor-Lock-in", so Fujitsu-Manager Scheuber. Als weitere Besonderheit führt er die Bereitstellungsmodelle an.

Foto: EuroCloud Deutschland

„Eine Änderung an den Service-Prozessen wegen der DSGVO wird in den seltensten Fällen notwendig sein."

Jens Eckardt
Vorstand Recht und Compliance von EuroCloud Deutschland_eco e. V.
www.eurocloud.de

Anforderungen an Cloud-Anbieter



Cloud-Monitor 2017: Unternehmen aus Deutschland bevorzugen Service-Provider, die hierzulande Rechenzentren unterhalten und ihren Sitz in Deutschland haben.

com! professional 8/17

Quelle: KPMG (2017) (n = 489)

Neben den klassischen Public- und Virtual-Private-Hosted-Ansätzen bietet K5 die Möglichkeit eines dedizierten Modells in Rechenzentren von Fujitsu oder beim Kunden vor Ort. „Als Basis für alle Modelle kommt immer die gleiche Technologie zum Einsatz. Das ermöglicht eine Kombination verschiedener Cloud-Modelle", so der Fujitsu-Fachmann:

Ob es sich bei Fujitsu um einen „deutschen" Cloud-Anbieter handelt, ist jedoch strittig. Formalrechtlich hat die japanische Muttergesellschaft die Oberhoheit über die Aktivitäten der deutschen Tochter. Allerdings weisen die Datenschutzregeln in Japan ein mindestens ebenso hohes Niveau auf wie die in der EU. Anfang 2017 hat die japanische Regierung diese Vorgaben nochmals verschärft. Daher ist es für deutsche Unternehmen kein besonderes Risiko, die K5-Cloud zu nutzen. Eine größere Unsicherheit, so ISG/Experton Group, sei die Sprunghaftigkeit von Fujitsus Cloud-Strategie in den vergangenen Jahren

Foto: Microsoft

„Kunden können weiterhin unsere (...) Cloud-Lösungen nutzen oder sich dafür entscheiden, unsere Services aus deutschen Rechenzentren zu beziehen und den Zugang zu ihren Daten durch einen deutschen Treuhänder kontrollieren zu lassen."

Satya Nadella
CEO von Microsoft
www.microsoft.de

Microsoft-Cloud: Wer ein iPhone oder iPad besitzt, kennt die Herkunftsbezeichnung auf der Rückseite der Systeme: „Designed by Apple in California – Assembled in China". Im übertragenen Sinn lässt sich das auch auf Microsofts Cloud-Plattform in Deutschland anwenden: Entwickelt werden die Angebote von Microsoft, also einem amerikanischen Anbieter. Die Bereitstellung der Dienste erfolgt allerdings über zwei Rechenzentren in Deutschland – nämlich die bereits erwähnten in Biere nahe Magdeburg und in Frankfurt am Main. Wichtiger ist jedoch, dass für die Verwaltung der Nutzerdaten und der Informationsbestände von deutschen Usern mit T-Systems ausschließlich ein Unternehmen mit Sitz in Deutschland zuständig ist.

3,6 Mrd.
Dollar investierten Unternehmen in Westeuropa 2016 in IaaS
Quelle: IDC

„Kunden können weiterhin unsere öffentlichen, privaten und hybriden Cloud-Lösungen nutzen oder sich dafür entscheiden, unsere Services aus deutschen Rechenzentren zu beziehen und den Zugang zu ihren Daten durch einen deutschen Datentreuhänder kontrollieren zu lassen", erklärte Microsofts CEO Satya Nadella im November 2015 in Berlin bei der Präsentation der Cloud-Strategie seines Hauses für Deutschland.

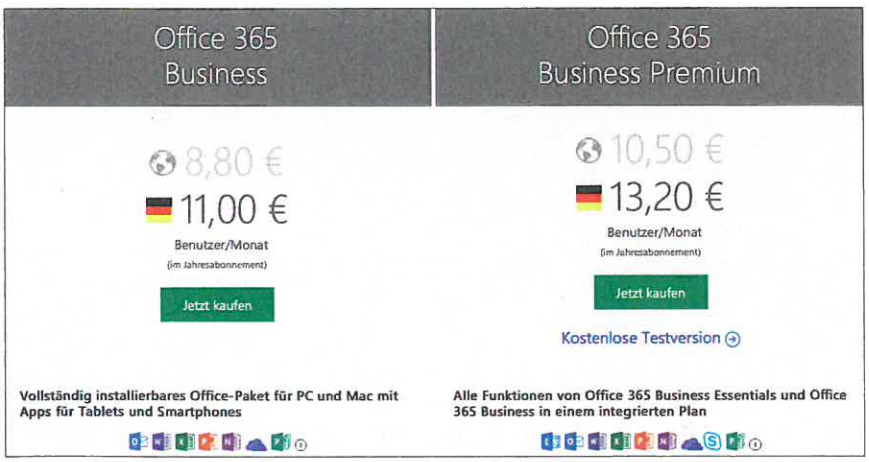
Der Schachzug von Microsoft, deutsche Versionen von Azure und Office 365 aufzusetzen, hat für deutsche Nutzer Vorteile. Denn sollten amerikanische Behörden den Zugriff auf Daten deutscher Kunden einfordern, kann sich Microsoft auf die Treuhänder-Vereinbarung mit T-Systems berufen und die Herausgabe von Daten verweigern.

So reichhaltig wie bei den internationalen Versionen ist die Palette der Services in Deutschland noch nicht. Microsoft ergänzt jedoch sukzessive die deutsche Version seines Cloud-Angebots. Als in Deutschland gehostete Versionen sind Office 365 und Azure verfügbar, seit dem 1. Juni 2017 außerdem Dynamics 365.

Die Kröte, die Nutzer der deutschen Microsoft-Cloud schlucken müssen, ist ein Aufpreis von rund 25 Prozent. So kostet die preisgünstigste Business-Version von Office 365 mit Outlook, Word, Excel, Powerpoint, One Note, Access und Publisher beispielsweise 11,00 Euro pro Nutzer und Monat. Die nicht in Deutschland gehostete Ausgabe kommt auf 8,80 Euro monatlich – allerdings im Jahresabonnement. Für 10,50 Euro monatlich bietet Microsoft Office 365 Business Premium an, inklusive Skype, SharePoint, Exchange und dem Social-Collaboration-Dienst Yammer. Aus der deutschen Cloud kostet diese Variante 13,20 Euro.

Der höhere Preis ist zum einen auf das Treuhändermodell zurückzuführen, sprich T-Systems möchte für seine Bemühungen entlohnt werden. Laut einem Systemhaus, das mit Microsoft zusammenarbeitet, spielen zudem die hohen Strompreise in Deutschland eine Rolle. Sie verteuern den Betrieb der Rechenzentren.

1&1: Als „Rising Star" unter den Anbietern von IaaS- und SaaS-Cloud-Diensten stufte ISG/Experton Group 2016 1&1 ein. Das Unternehmen mit Sitz in Deutschland fokussiert sich derzeit auf die Bereitstellung von Servern via Cloud, also auf IaaS-Dienste. Nutzer haben die Wahl zwischen eigenen („dedicated") Systemen, virtuellen Servern, die dem Nutzer exklusiv zur Verfügung stehen („Virtual Server Cloud") und Cloud-Servern, die sich mehrere User teilen. Ein von 1&1 gehosteter und verwalteter Cloud-Server unter Ubuntu 16.04 ▶



Aufpreis: Wer Office 365 aus der Deutschland-Cloud beziehen will, muss 25 Prozent mehr bezahlen als Firmen, die sich mit der „normalen" Microsoft-Cloud begnügen.

ist ab 9,99 Euro monatlich verfügbar, ein System mit Windows Server 2012 kostet 5 Euro mehr.

Eine Besonderheit ist, dass der Nutzer dank einer minutengenauen Abrechnung der gewählten Konfiguration nur für die Ressourcen bezahlt, die er tatsächlich nutzt. Die virtuellen Maschinen lassen sich zudem im laufenden Betrieb ohne Abschaltung erweitern. Ohne Zusatzkosten können User darüber hinaus festlegen, in welchem Rechenzentrum ihre virtuellen Server vorgehalten werden. Neben Datacentern in Deutschland steht auch ein Cloud-Rechenzentrum in den USA zur Auswahl.

Ein weiterer Pluspunkt des 1&1-Cloud-Angebots ist das Baukasten-Prinzip. Es ermöglicht beispielsweise, bei Bedarf zu einem Server-Cluster weitere Systeme hinzuzufügen und diese wieder herunterzufahren, wenn die Rechenleistung nicht mehr benötigt wird. Die Analysten von ISG/Experton Group loben zudem die gut dokumentierte Programmierschnittstelle, über die sich weitere Cloud-Dienste und Microservices andocken lassen.

Speziell für kleine und mittelständische Unternehmen hilfreich ist das Cloud-App-Center von 1&1. Dort finden sich mehr als 100 Applikationen, meist auf Open-Source-Basis. Dazu zählen etwa Content-Management-Lösungen, Datenbanken, E-Mail-Tools, Groupware-Programme und einige Anwendungs-Server.

Systemhäuser als Broker

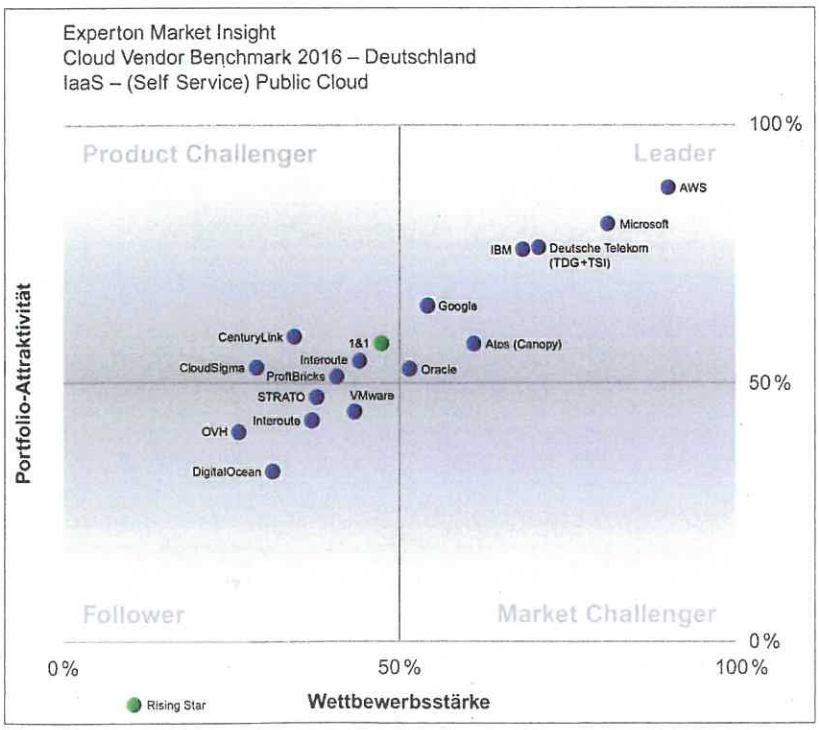
Anwender, die vorzugsweise auf gemanagte Clouds aus deutschen Rechenzentren Wert legen, haben eine weitere Option: Sie können auf die Angebote von Systemhäusern und IT-Dienstleistern zurückgreifen. Sie alle verfügen über Rechenzentren in Deutschland und haben ihren Firmensitz in der Bundesrepublik. Als Beispiele dafür stellen wir Bechtle und Cancom/Pironet vor. Weitere Anbieter mit diesem Zuschnitt sind etwa die schon erwähnten Dienstleister QSC, Allgeier oder All for One Steeb

Foto: Fujitsu

„Nutzer unserer K5-Cloud können vorgeben, wo Datenbestände gespeichert werden, etwa in Cloud-Rechenzentren in Deutschland."

Uwe Scheuber
Director Business Development Cloud & Hybrid IT bei Fujitsu
www.fujitsu.com/de

Bechtle: Das Systemhaus Bechtle definiert sich als „Multi-Cloud-Provider". Das heißt, Bechtle bietet eigene Cloud-Dienste an und bezieht auf Wunsch externe Cloud-Services in sein Angebot mit ein. Das sind Services von AWS oder Microsoft. „Aus zahlreichen Projekten wissen wir, dass Cloud-Services einen erheblichen Wertbeitrag für die IT unserer Kunden liefern können, sei es als dedizierte Lösung etwa für Entwicklungs- und Testaufgaben, sei es als Bestandteil hybrider IT-Architekturen. Hier knüpft die erweiterte Partnerschaft mit Microsoft an", erklärt Michael Guschlbauer, Vorstand IT-Systemhaus & Managed Services bei Bechtle. Als Partner im Cloud-Solution-Provider-Programm von Microsoft übernimmt Bechtle nicht nur die Vermarktung von Cloud-Diensten des US-Unternehmens. Das Systemhaus tritt als Berater des Nutzers auf und ist außerdem für die Bereitstellung und den technischen Support der Microsoft-Cloud-Services zuständig. Nach dem gleichen Muster arbeitet Bechtle mit AWS zusammen. Für Anwender hat das den Vorteil, dass sie nur einen Ansprechpartner haben, der die Dienste aller Cloud-Service-Provider koordiniert. Das gilt auch für das Speichern und Bearbeiten von sensiblen Daten in einer Cloud. Wenn der Nutzer dies vorgibt, bleiben solche Informationen im Rechenzentrum des Systemhauses und wandern nicht in ein US-Cloud-Rechenzentrum eines Service-Providers.



Quelle: Experton Group

Benchmark: Unter den führenden IaaS-Anbietern in Deutschland befanden sich 2016 mehrere einheimische Anbieter, etwa Telekom, Strato, 1&1 und Profitbricks.

Cancom/Pironet: Das Unternehmen Cancom/Pironet verfügt über zwei Rechenzentren in Deutschland. Darüber bietet Cancom/Pironet unter anderem Services anderer Anbieter wie Microsoft und SAP „as a Service" an. Außerdem stellt der Provider digitale Arbeitsplätze (Workplaces) aus der Cloud zur Verfügung. Die Zielgruppe sind traditionell Mittelständler.

Gerade für mittelständische Unternehmen hat ein solches Modell eines „One-Stop Shops" Vorteile. Denn: „Viele Unternehmen haben das Thema Cloud-Computing in den vergangenen Jahren opportunistisch vorangetrie- ▶

ben", sagt Matthias Zacher, Manager Research & Consulting beim Beratungshaus IDC Deutschland. „Fachabteilungen entscheiden sich immer häufiger für SaaS-Lösungen und fordern nachträglich deren Integration in die Unternehmens-IT. Damit ergibt sich in vielen Fällen ein Sammelsurium aus Public-, Dedicated- und Hosted-Private-Cloud-Services sowie hybriden Szenarien, die nebeneinander und ohne übergreifenden Ansatz existieren."

Kurzum: Das Risiko, dass in einem solchen „Sammelsurium" Daten nicht entsprechend den Vorgaben der DSGVO in Cloud-Umgebungen gespeichert werden, steigt. Diese Einschätzung teilt Felix Höger, Vorstand Technologie und Operations, COO/CTO, beim deutschen IT-Haus und Cloud-Service-Provider QSC: „Die Nachfrage nach einfach konsumierbaren Public-Cloud- oder auch Software-as-a-Service-Angeboten hat in letzter Zeit rasant angezogen. Jedoch ist das Management der unterschiedlichen Cloud-Angebote ein mitunter komplexes Unterfangen." Ein neues Angebot von QSC sind daher Beratungsleistungen in puncto Multi-Cloud.

Die Komplexität einer Multi-Cloud-Umgebung lässt sich reduzieren, wenn ein Profi mit ins Boot geholt wird, etwa ein IT-Haus mit Erfahrung auf dem Gebiet Cloud und Cloud-Service-Management. Die Kehrseite der Medaille: Der Nutzer muss für diesen Service bezahlen.

Dennoch geht der Trend eindeutig in Richtung Multi-Cloud. Der Einstieg erfolgt in vielen Fällen nach folgendem Muster: Hoch wichtige Daten, etwa Entwicklungsunterlagen und brisante Geschäftsdokumente, verwaltet ein Unternehmen in einer Private Cloud im hauseigenen Rechenzentrum.

Foto: Bechtle

„Aus zahlreichen Projekten wissen wir, dass Cloud-Services einen erheblichen Wertbeitrag für die IT unserer Kunden liefern können."

Michael Guschlbauer
Vorstand IT-Systemhaus & Managed Services der Bechtle AG
www.bechtle.de

Weniger kritische Informationen, wie Standard-E-Mails und Office-Applikationen, werden aus einer oder aus Gründen der Redundanz besser aus zwei Public Clouds bezogen. Wer auf der sicheren Seite sein möchte, bevorzugt dabei Provider mit Rechenzentren in Deutschland. Eine solche Hybrid Cloud, also eine Mischung aus Private- und Public-Cloud-Infrastruktur, erfreut sich laut IDC und KPMG gegenwärtig bei deutschen Unternehmen besonderer Beliebtheit.

Private-Cloud-Eigenbau

Wer keine Scheu hat, selbst Hand anzulegen, kann sich im eigenen Server-Raum oder Rechenzentrum eine Private oder Hybrid Cloud einrichten. Dafür gibt es zwei Optionen.

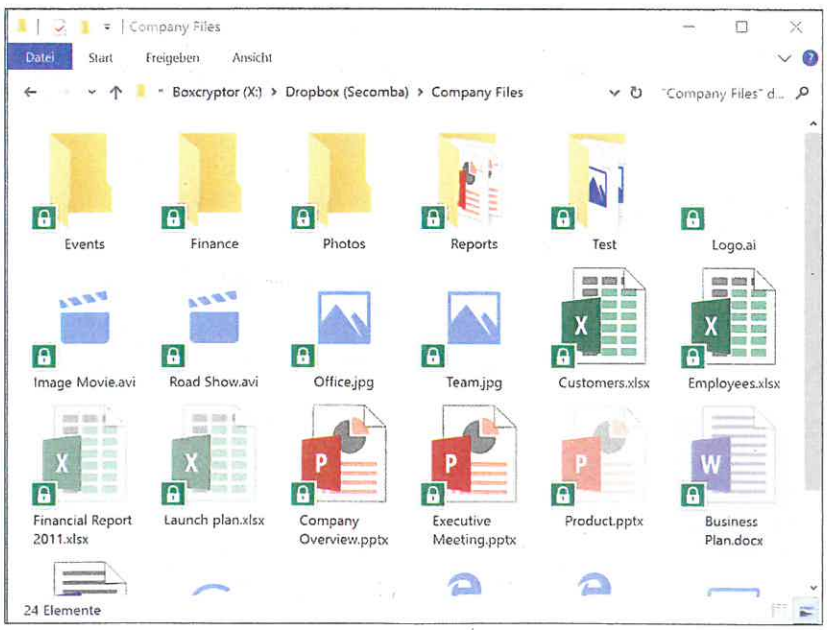
Erstens: Relativ preisgünstige Plattformen wie ownCloud und deren Ableger Nextcloud. Sie eignen sich auch für kleine und mittelständische Unternehmen.

Zweitens: Größere Private-Cloud-Plattformen wie etwa Helion von HPE, vCloud Air von VMware, Enterprise Private Cloud von Dell EMC oder Oracles Cloud Platform und Microsofts Azure Stack. Solche Angebote kommen primär für größere Organisationen mit einer entsprechend umfangreichen IT-Abteilung in Betracht.

ownCloud beziehungsweise Nextcloud laufen auf Webservern, auch solchen auf einem NAS-System. Allerdings ist ein NAS als Basis nur für kleine Unternehmen akzeptabel. Besser ist ein ausgewachsener Server, auf dem sich die Software als Virtual Appliance installieren lässt.

Sowohl ownCloud als auch Nextcloud stellen primär Funktionen für das Teilen und gemeinsame Bearbeiten von Content bereit, also von Dateien, Bildern oder Videos. Gegen Aufpreis lassen sich weitere Funktionen hinzufügen, vom Outlook-Add-in über SIP-Gateways (Session Initiation Protocol) bis hin zu Office-Suiten wie Collabra. Die jüngste Ausgabe von Nextcloud verfügt zudem über eine Funktion für Video- und Audio-Chats.

Die Standard- beziehungsweise Basis-Version für Unternehmenskunden für 50 User kostet bei ownCloud 3000 Euro pro Jahr, bei Nextcloud 1900 Euro. Zudem gibt es kostenlose Community-Editionen beider Software-Pakete. Deren Funktionsumfang ist allerdings eingeschränkt, weswegen sie eher für private Nutzer oder Kleinstunternehmen in Betracht kommen.



Sicher ist sicher: Boxcryptor verschlüsselt Daten, die Anwender in Cloud-Speichern ablegen. Selbst AWS empfiehlt den Einsatz solcher Tools.

Schlüsselfertige Cloud

Wer ownCloud oder Nextcloud nicht selbst implementieren will, kann auf eine gehostete Version zurückgreifen. Sie wird von Cloud- oder Web-Hosting-Unternehmen bereitgestellt. Nextcloud hat mehr als 30 solcher Partner in Deutschland, zum Beispiel oCloud.de,

OwnCube, PortKnox und Netways. Auch ownCloud arbeitet mit solchen Providern zusammen, etwa mit oCloud.de.

Welches der beiden Software-Pakete das bessere ist, lässt sich schwer sagen. Der Funktionsumfang beider Lösungen ist in etwa gleich. Den etwas innovativeren Eindruck macht derzeit Nextcloud. So stehen seit Version 12 Collaboration-Funktionen wie Videoanrufe und Push-Nachrichten zur Verfügung. In Online-Foren wird zudem immer wieder das Argument angeführt, dass Funktionen, die bei Nextcloud kostenlos sind, bei ownCloud den kostenpflichtigen Versionen vorbehalten sind. Dafür verfügt ownCloud über eine größere installierte Basis.

Datenwege kontrollieren

Auch sicherheitsbewusste Nutzer von Cloud-Diensten übersehen oft einen Faktor, nämlich dass Daten auf dem Weg vom hauseigenen Rechenzentrum zu dem eines Cloud-Service-Providers möglicherweise Routen nutzen, die außerhalb Deutschlands verlaufen. Dies ist durch die maschenartige Struktur des Internets bedingt. Doch dieser Umstand erleichtert es Hackern und Geheimdiensten, solche Daten abzufangen und zu entschlüsseln.

2 Mrd.
Dollar gaben Unternehmen in Westeuropa 2016 für PaaS aus

Quelle: IDC

Einen Ausweg bietet – gegen Aufpreis – der Service DirectCloud von DE-CIX (Deutscher Commercial Internet Exchange). Er bindet die Datacenter von Service-Providern und Unternehmen über ein virtuelles LAN (Virtual Local Area Network) an den Internetknoten in Frankfurt an. „Für den Kunden ist das praktisch ein lokales Netzwerk, das in die Cloud verlängert wird", sagt Thomas King, Chief Innovation Officer bei DE-CIX. Auch können Nutzer von DirectCloud ihre eigenen IP-Adressen verwenden und brauchen keine „Übersetzungsverfahren". Nutzer des Dienstes haben zudem die Gewähr, dass ihre Daten auf dem Weg zum Cloud-Service-Provider nur über Verbindungen innerhalb Deutschlands laufen. Das ist auch dann von Vorteil, wenn man Cloud-Dienste von AWS, IBM, Google oder Oracle nutzt. Der Datentransfer vom und zum Cloud-Rechenzentrum dieser Anbieter wird nicht über Connections gelenkt, die sich der Kontrolle des Nutzers beziehungsweise von DE-CIX entziehen.

Ob dieser Aspekt von DirectCloud für eine Firma wichtig ist, hängt letztlich von deren Sicherheitsanforderungen ab. Für Unternehmen aus Hightech-Branchen wie Chemie, Maschinenbau und Automobilindustrie, die besonderen Wert auf den Schutz unternehmenskritischer Daten legen, kann der Dienst durchaus von Nutzen sein.

Foto: QSC

„Die Nachfrage nach einfach konsumierbaren Public-Cloud- oder Software-as-a-Service-Angeboten hat in letzter Zeit rasant angezogen. Das Management der unterschiedlichen Cloud-Angebote ist jedoch mitunter ein komplexes Unterfangen."

Felix Höger
Vorstand Technologie und Operations, COO/CTO, bei QSC
www.qsc.de

Verschlüsseln!

Bereits 2015 betonte Werner Vogels, Chief Technology Officer von Amazon Web Services, wie wichtig es sei, Daten zu verschlüsseln, und das mit eigenen Schlüsseln, die sich der Kontrolle des Service-Providers entziehen. Dadurch wird es Unbefugten, inklusive Hackern und Geheimdiensten, erschwert, Informationen „abzusaugen", die Unternehmen in einer Public Cloud speichern oder bearbeiten.

Eine Möglichkeit, Cloud-Daten zu verschlüsseln, bietet das Tool Boxcryptor des Augsburger Software-Hauses Secomba. Es steht in Versionen für Teams, Kleinfirmen und Unternehmen zur Verfügung. Die Software bietet eine durchgängige, also Ende-zu-Ende-Verschlüsselung von Daten, die Nut- ▶

Trusted Cloud: Cloud-Provider finden

Unternehmen, die Cloud-Services von deutschen Providern bevorzugen, können einen Blick auf die Webseite des Kompetenznetzwerks Trusted Cloud e. V. werfen (www.trusted-cloud.de/de/projekt). Der Verein vergibt das Trusted-Cloud-Label für vertrauenswürdige Cloud-Services für die Wirtschaft. Die Zielgruppe sind vor allem mittelständische Unternehmen. Trusted Cloud ging 2015 aus dem gleichnamigen Technologieprogramm des Bundesministeriums für Wirtschaft und Energie (BMWi) hervor.

Über ein Webportal (www.trusted-cloud.de/de/cloud-service-suche) können Interessenten nach Cloud-Service-Providern und Anbietern von Beratungsdiensten suchen. Die Auswahlmaske ist relativ grobkörnig. So können Nutzer Cloud-Angebote suchen, die in Form von IaaS-, SaaS- oder PaaS-Diensten (Infrastructure, Software oder Platform as a Service) bereitgestellt werden.

Kompetenznetzwerk Trusted Cloud: Der vom Bund geförderte Verein vergibt ein neutrales Gütesiegel.

Zudem lässt sich vorgeben, dass die Dienste über Rechenzentren in Deutschland angeboten werden und über welche Zertifikate der Anbieter verfügen muss.

Ein Manko von Trusted Cloud: Die Zahl der Angebote ist noch überschaubar. Die Suche nach Cloud-Services im Bereich Backup ergab beispielsweise ganze zwei Treffer.

zer bei Public-Cloud-Storage-Diensten speichern. Unterstützt werden nicht nur Dropbox, Box und SugarSync, sondern auch Services, die in Deutschland oder der EU beheimatet sind. Dazu gehören GMX, Secure Data Space, Strato, Telekom Magenta Cloud und Web.de.

Boxcryptor ermöglicht unter anderem das gemeinsame Bearbeiten von Daten durch Gruppen. Die Dateien werden dabei verschlüsselt und sind für Externe unzugänglich. Das Tool unterstützt die gängigen Betriebssysteme Windows, iOS, Android, Mac OS und Chrome. Der Preis für die Teamversion beträgt 72 Euro pro Jahr. Die Ausgabe für Unternehmen kostet ab 6,40 Euro pro Nutzer und Monat.

Gateway steuert Zugriff

Einen anderen Ansatz verfolgt das Darmstädter IT-Security-Unternehmen Eperi. Es hat ein Gateway entwickelt, mit dem sich sensible Daten selektiv verschlüsseln lassen. Zudem behält der Nutzer die Schlüssel und damit die Hoheit über seine Daten – auch wenn diese in einem Cloud-Rechenzentrum lagern. Das Gateway arbeitet wie ein transparenter Proxy, der einer Anwendung vorgelagert ist. Alle Daten, die ein Nutzer mit dieser Anwendung bearbeitet, werden in Echtzeit automatisch verschlüsselt, sobald sie das Gateway passieren.

Die Gateway-Software hat Eperi als Open Source auf seiner Webseite offengelegt. Somit kann jeder Anwender die kryptografischen Grundlagen sowie das Rollen- und Benutzermanagement überprüfen. Eine spezielle Variante, das Eperi-Gateway for Cloud Apps, ist für Cloud-Anwendungen konzipiert. Unterstützt werden Office 365 und Salesforce.com. Word-Dokumente, die ein Nutzer zum Beispiel mit Office 365 bearbeitet, werden verschlüsselt, bevor sie auf OneDrive oder SharePoint landen. Auf dieselbe Weise werden E-Mails und andere Daten geschützt, die ein Nutzer auf Cloud-Plattformen ablegt.

Auch Datenbanken lassen sich mit dem Gateway verschlüsseln, etwa IBM DB2, MariaDB, Microsoft SQL Server und Oracle 11gR2 bis 12c. Implementiert wird Eperi als Image in einer Cloud oder als virtuelle Appliance beziehungsweise Virtual Machine im eigenen Rechenzentrum. Eine dritte Möglichkeit ist, das Gateway auf einem hausinternen Java-Application-Server laufen zu lassen.

Für Firmen, die Public-Cloud-Dienste nutzen wollen, aber nur bei minimalem Risiko, sind Lösungen wie das Eperi-Gateway eine interessante Option. Denn sie bieten gewissermaßen eine Extraportion Sicherheit, selbst in per se unsicheren Umgebungen wie einer Public Cloud.

Foto: IDC

„In vielen Fällen ergibt sich ein Sammelsurium aus Public-, Dedicated- und Hosted-Private-Cloud-Services sowie hybriden Szenarien, die nebeneinander existieren, ohne übergreifenden Ansatz."

Matthias Zacher
Manager Research & Consulting bei IDC Deutschland
www.idc.de

Fazit

Unternehmen, die sicherstellen möchten, dass vertrauliche Daten nicht bei ausländischen Behörden oder Hackern landen, müssen keinen Bogen um die Cloud machen, auch nicht um Public-Cloud-Dienste. Nach derzeitigem Stand erfüllen auch Anbieter mit Hauptsitz in den USA die Vorgaben der Datenschutz-Grundverordnung, sofern sie Rechenzentren in Deutschland betreiben und garantieren können, dass Daten von Kunden ausschließlich dort verarbeitet werden.

Ein Unsicherheitsfaktor bleibt jedoch: Die US-Regierung könnte Provider wie AWS, Google oder IBM dazu nötigen, solche Informationen auch dann herauszugeben, wenn sie in Frankfurt am Main oder Hamburg lagern. Offen ist, ob sich ein amerikanisches Unternehmen auf Dauer diesem Druck widersetzen könnte. Daher ist es für Anwender durchaus eine Überlegung wert, zumindest als Backup einen Cloud-Service-Provider mit Hauptsitz in Deutschland in petto zu haben. Dies umso mehr, als eine solche Multi-Cloud-Strategie die Abhängigkeit von einem Anbieter verringert.

Keine tragfähige Alternative ist es dagegen, Public Clouds zu meiden. Services, wie sie über solche Cloud-Umgebungen verfügbar sind, in Eigenregie zu implementieren, ist schlichtweg unrentabel. Hinzu kommt, dass viele Unternehmensrechenzentren nicht die gleichen Sicherheitsstandards aufweisen wie Cloud-Datacenter von Providern.

Wichtig und praktikabel sind dagegen Sicherheitsverfahren wie Datenverschlüsselung. Denn nicht erst seit Edward Snowden ist bekannt, dass Geheimdienste und Hacker mit einer starken Verschlüsselung massive Probleme haben. ■

Bernd Reder/js
js@com-professional.de

Der BND liest mit

Am 1. Januar 2017 haben sich in Deutschland die Gegebenheiten geändert – zulasten des Datenschutzes. An diesem Tag trat das „Gesetz über den Bundesnachrichtendienst", kurz BND-Gesetz, in Kraft (www.gesetze-im-internet.de/bndg) . Es räumt dem Bundesnachrichtendienst das Recht ein, am Internetknoten DE-CIX in Frankfurt am Main Daten von ausländischen Internetnutzern abzugreifen und auszuwerten. Dazu reicht es aus, wenn die „Handlungsfähigkeit der Bundesrepublik Deutschland" gewahrt werden soll oder es notwendig ist, „frühzeitig Gefahren für die innere oder äußere Sicherheit der Bundesrepublik Deutschland" zu erkennen. Diese schwammigen Passagen geben dem BND die Möglichkeit zu weitreichenden Datensammel-Aktivitäten.

Es ist nicht auszuschließen, dass der BND auch Informationsbestände von deutschen Staatsbürgern und Unternehmen am DE-CIX abfängt und analysiert, etwa solchen mit Handelsbeziehungen zu Firmen im Mittleren Osten oder Asien. Vertreter des DE-CIX haben beim Bundesverwaltungsgericht in Leipzig Klage gegen das BND-Gesetz eingereicht. Das Unternehmen möchte die Fernmeldeüberwachung durch den BND einer „gerichtlichen Prüfung" unterziehen.