iX extra Juli 2015

Cloud-Computing

Eine Sonderveröffentlichung der Heise Medien GmbH & Co. KG

Geschäftskritische Daten absichern

Marktübersicht: Backup in die Cloud

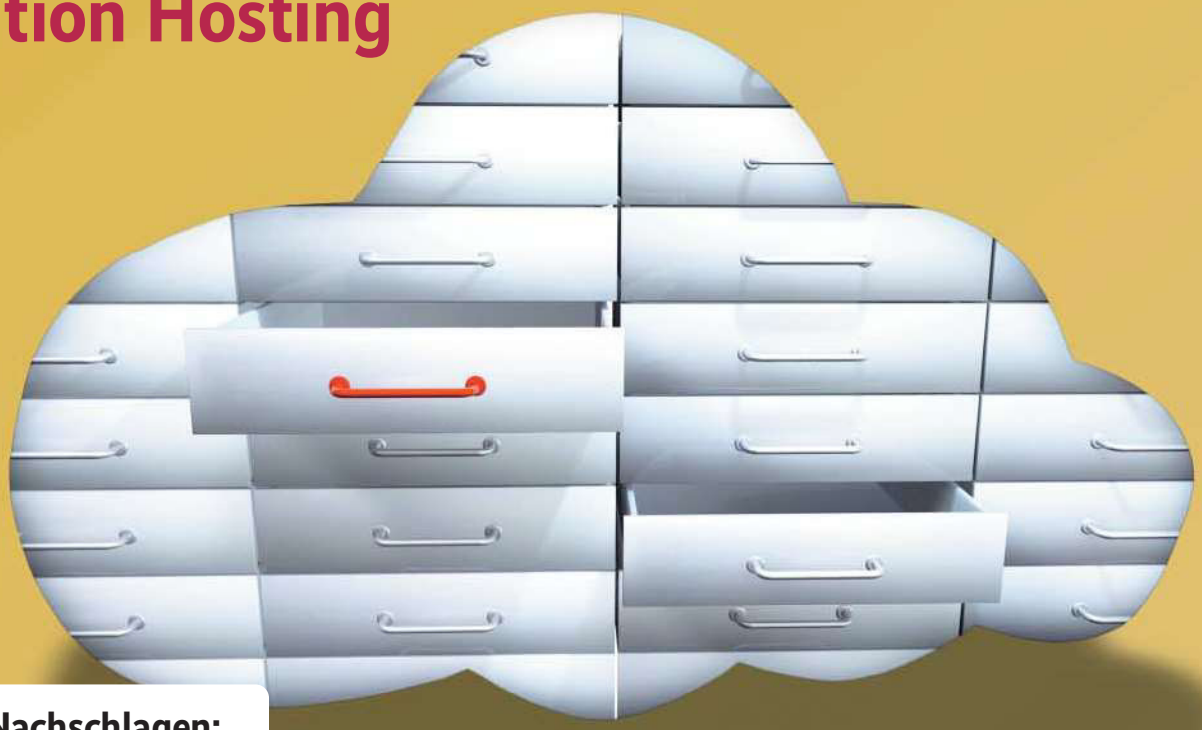
Immer ein Ass im Ärmel

Seite I

Vorschau: Webhosting

Application Hosting

Seite IX



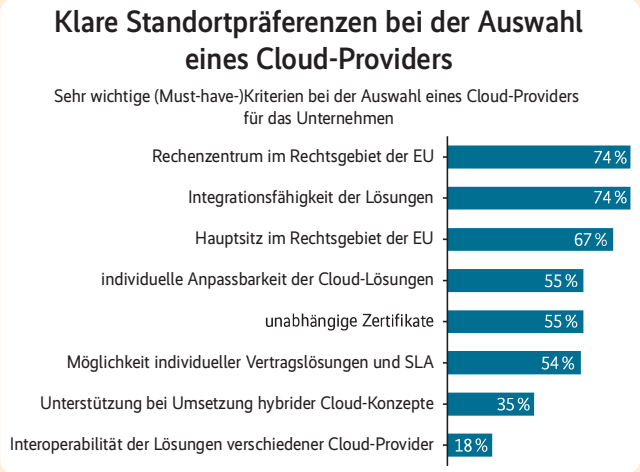
iX extra zum Nachschlagen:
www.ix.de/extra

Immer ein Ass im Ärmel

Marktübersicht: Backup in die Cloud

Datensicherung ist ungeliebt, da die damit verbundenen Tätigkeiten zumindest vordergründig keinen neuen Umsatz bringen. Aber wenn der Schadensfall eintritt, zeigt sich der Stellenwert einer gut durchdachten Notfallvorsorge, denn häufig hängt die Existenz von Unternehmen an der Verfügbarkeit geschäftskritischer Daten. Deshalb muss man sie schnell wieder einspielen können, wenn Hardwaredefekte, Feuer, Wasser, Unbefugte oder Viren das Material unbrauchbar gemacht haben.

Quelle: BITKOM



Der Standort des Rechenzentrums gehört zu den wichtigsten Kriterien bei der Auswahl eines Cloud-Providers. Basis: Unternehmen ab 20 Mitarbeitern, die Private bzw. Public Cloud nutzen, den Einsatz planen oder diskutieren (Abb. 2).

Backups brauchen viele Ressourcen an Hard- und Software. Sie erfordern einen besonders für kleine und mittlere Unternehmen schwer zu realisierenden administrativen Aufwand. Gerade KMUs können aber mit Online-Backups ein Sicherheitslevel erreichen, das mit Bordmitteln nur schwer realisierbar ist. Wie erforderlich das ist, hat die Initiative „Cloud Services Made in Germany“ Ende 2014 in einer Umfrage unter Managern und Geschäftsführern in 100 mittelständischen Unternehmen herausgefunden: 95 Prozent geben an, dass sie ohne Daten ihre Prozesse nicht mehr in der gewohnten Art und Weise weiterführen können. Bei 51 Prozent der Unternehmen droht gar ein vollständiger Stillstand der Organisation.

Zwar haben die meisten Befragten (87 %) Maßnahmen zur Sicherung und Wiederherstellung implementiert, aber über die Hälfte (67 %) weiß nicht, ob das Zurückspielen der Daten im Ernstfall korrekt funktioniert. Auf externe Dienstleister greifen 21 Prozent zurück, 53 Prozent lehnen ein Backup über die Cloud ab. Eine Schwierigkeit deckte die von NetApp beauftragte Studie auf: Viele Unternehmen sehen Backup und Disaster Recovery als zwei getrennte Bereiche an, obwohl viele Dienstleister beides anbieten.

Besonders kleinen Firmen stellt sich daher die Frage, ob sie ihre Backups einem der zahlreichen Dienstleister überlassen – entweder komplett oder ergänzend zu eigenen Sicherungen. Solche Anbieter übernehmen alle Aktivitäten: zum einen das regelmäßige Sichern der Daten in die Cloud, zum anderen das Wiedereinspielen im Extremfall. Sie können sich vollständig auf die Aufgaben konzentrieren und stellen die erforderliche Hard- und Software samt Beratung zur Verfügung.

Mit Online-Datensicherungen in die Cloud entfallen Anschaffungskosten für ein eigenes Backup-System – besonders in Zeiten schnell wachsender Datenmengen (und ständiger Updates) ein wichtiges Kriterium. Durch das dynamische Zu- und Abbuchen von Ressourcen bleiben Unternehmen flexibel, die Kosten, die entstehen, bleiben überschaubar und den Administratoren bleibt Arbeit erspart. Sie müssen sich beispielsweise nicht mehr um das Aufbewahren und ständige Prüfen der Sicherungen kümmern – oder mit einem schlechten Ge-

Quelle: NetApp

Mit Online-Backups können besonders kleine Unternehmen ihre eigene IT-Abteilung entlasten (Abb. 1).

wissen leben, wenn sie es versäumen. Ein weiterer Aspekt: Durch Online-Backups liegen die Daten physisch getrennt von den Originalen im Unternehmen.

Standort Rechenzentrum

Wer Online-Backups nutzt, gibt seine geschäftskritischen Daten zwangsläufig aus dem Haus und muss dem Anbieter vertrauen, dass der sorgsam mit ihnen umgeht.

In der Marktübersicht sind Online-Backup-Anbieter aufgeführt, die ein deutsches Rechenzentrum nutzen – wie immer ohne Anspruch auf Vollständigkeit. Wie wichtig der Standort des Rechenzentrums ist, hat der Branchenverband BITKOM im Cloud-Monitor 2015 ermittelt (www.bitkom.org/de/publikationen/38338_82139.aspx).

Für 74 Prozent der Befragten gehört das Rechenzentrum im Rechtsgebiet der EU zu den unerlässlichen Kriterien bei der Auswahl eines Cloud-Providers. Für 67 Prozent muss sich der Hauptsitz des Anbieters im Rechtsgebiet der EU befinden (siehe Abbildung 2). Für die von der KPMG AG Wirtschaftsprüfungsgesellschaft beauftragte Studie wurden 458 Personen in deutschen Unternehmen mit mindestens 20 Mitarbeitern befragt.

Unabhängige Zertifikate spielen für 55 Prozent der Studienteilnehmer eine große Rolle. Viele in der Marktübersicht genannten Anbieter nutzen zertifizierte Rechenzentren, vor allem nach der internationalen Norm ISO 27001.

Zum Beispiel hat der TÜV Rheinland das gesamte Unternehmen Uptime inklusive

Virenschutz aus der Cloud

Für die Sicherheit geschäftskritischer Daten ist es außerdem wichtig, dass Virenscanner Schädlinge schnellstens erkennen und abwehren. Neue Viren, Trojaner oder Malware verbreiten sich in einem rasanten Tempo, sodass lokale Rechner die geeigneten Gegenmittel gar nicht schnell genug nachladen können. Außerdem entstehen täglich Hunderte neuer Computerviren und Trojaner.

Hersteller von Sicherheitssoftware setzen daher vielfach auf die Cloud, um Schädlingen besser auf die Spur zu kommen: Dort können sie eine große und ständig aktuelle Signaturdatenbank vorhalten, die zudem die Ressourcen des Unternehmens schont. Auf Basis der gesammelten Antivirenscans sind sie schneller in der Lage, Schaden abzuwehren.

Kaspersky verlagert den Arbeitsort der Antivirenprogramme auf einen Server in der Cloud. Die Nutzer brauchen nur noch ein kleines Client-Programm auf einem Desktop zu installieren, der eine Verbindung zum Webdienst des Sicherheitsanbieters herstellt. Er analysiert die Daten aus den Antivirenscans und informiert den Rechner des Anwenders über geeignete Gegenmaßnahmen.

Allerdings kann das System ohne Internetverbindung keine Schädlinge erkennen, denn der lokale Client kann das System nur scannen, stand-alone nicht aber die Ergebnisse interpretieren.

Avira integriert in seinen frei nutzbaren Virenschutz „Free Antivirus“ für Windows seine „Protection Cloud“, die den digitalen Fingerabdruck verdächtiger ausführbarer Dateien auf dem PC mit Echtzeit-Malware-Daten in der Cloud abgleicht. Wenn das System eine unbekannte Datei findet, lädt es diese zur Überprüfung hoch und stuft sie anschließend als sauber oder infiziert ein. Laut Anbieter beansprucht das Programm nur einen Bruchteil der Systemleistung, die für die lokale Analyse einer Datei nötig wäre.

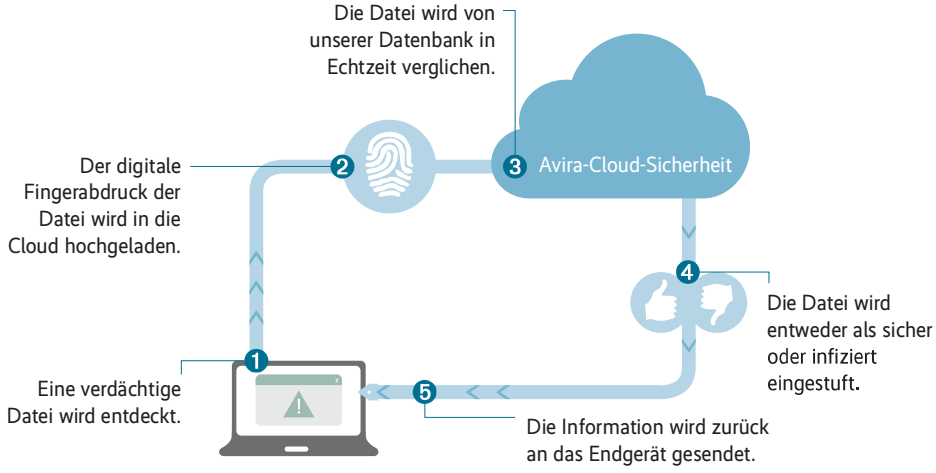
Symantec reduziert mit seinem „Global Intelligence Network“ den Client um 80 bis 90 Prozent, belegt damit entsprechend weniger Speicher und eignet sich laut Hersteller für Embedded-Systeme. Der Schutz vor Angriffen aus dem Netz analysiert eingehende Datenströme und blockiert Bedrohungen.

Die meisten Anbieter wie G DATA, F-Secure, McAfee, Sophos oder Symantec offerieren Cloud-Ansätze. Sie protokollieren und übermitteln etwa die vom Nutzer besuchten Websites an einen Server in der Ferne, wie AV-Comparatives, eine Organisation, die Sicherheitssoftware testet, ermittelt hat (http://www.av-comparatives.org/wp-content/uploads/2014/04/avc_datasending_2014_en.pdf). Wer das nicht möchte, kann die Cloud-Option abschalten, etwa bei Emsisofts „Anti-Malware Network“.

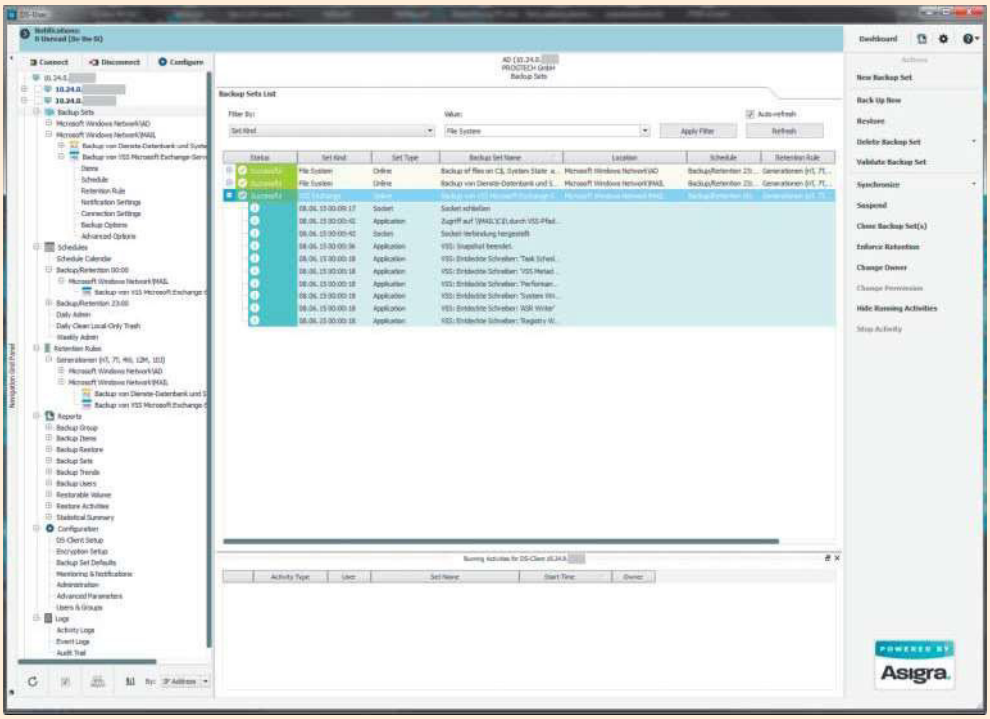
Panda Security etwa bietet seinen „Cloud Cleaner“ an, ein Antivirusprogramm, das sowohl mit der Cloud als auch lokal ohne Internetverbindung funktioniert. Volle Kraft erreicht das Programm aber nur mitsamt den Rechnern in der Wolke. Nur hier können alle Kunden davon profitieren, wenn die Systeme irgendwo eine neue Bedrohung identifiziert haben.

Laut Panda Security analysiert und klassifiziert das System jeden Tag Tausende neuer Malware-Muster aus der als „Collective Intelligence“ bezeichneten User Community. Ständig aktualisierte Whitelists mit über 10 Millionen Dateien sorgen dafür, dass „gute“ Dateien nicht gescannt werden müssen.

Trend Micro bietet ebenfalls ein Modell, das im internen und im externen Netz verwendbar ist: Hierbei müssen sich Kunden nicht zwischen einer lokalen oder einer Cloud-Installation entscheiden, sondern können beides kombinieren und die gewählte Option jederzeit ohne Auswirkungen auf die Lizenz ändern.



Avira nutzt die Cloud als „kollektive Intelligenz“. Jeder in die Cloud hochgeladene digitale Fingerabdruck einer Datei erweitert eine kontinuierlich wachsende Datenbank (Abb. 3)



Quelle: PROGTECH

PROGTECHs Backup-Produkt unterstützt unter anderem VMwares Virtual Machine Replication und Geolocation von mobilen Endgeräten (Abb. 4).

Rechenzentrum nach ISO 27001:2013 zertifiziert. Das umfasst unter anderem die physikalische und logische Sicherheit in den Rechenzentren sowie den Umgang mit Kundendaten. Nach Unternehmensangaben sind alle Prozesse und Systeme dokumentiert, Verantwortlichkeiten und Benutzerrechte klar definiert.

Für die Sicherheit der Daten organisiert Uptime außerdem sein Risikomanagement nach den Vorgaben der Norm ISO 31000 und nutzt dafür die für ISO 27001 weiterentwickelte OCTAVE-Methode. Dabei geht es nicht nur um IT-spezifische Gefahren wie das Hacking oder technische Pannen, sondern auch um menschliches Versagen, Katastrophen oder höhere Gewalt.

Zu den Nutzern zertifizierter Rechenzentren zählen außerdem unter anderem Concat,

Anbieter für Backup in die Cloud

Hersteller	Webseite	Produkt
Acronis	www.acronis.com/de-de/business/backup	Acronis Cloud Backup
AHD Hellweg Data	https://www.ahd.de	ahd Managed Backup
BUSYMOUSE Business Systems GmbH	www.busymouse.de	BUSYMOUSE Online Backup
blackpoint GmbH	www.back2web.de	Back2Web
Cema GmbH	www.cema.de	Online Backup Service
Concat AG	www.concat.de	Backup2net
Continum	www.continum.net	Online-Backup
cratchmere.com GmbH	www.netzdrive.de	netzdrive cloudcollaboration
cubos Internet GmbH	www.cubos-internet.de	Online-Backup
DATEV eG	www.datev.de	DATEV Datensicherung online
Datis IT-Services	https://www.datis.de	Online-Backup
dogado GmbH	www.dogado.de	dogado Online Backup
Elabs AG	www.elabs.de	HighSecurity-Backup
epcan	www.epcan.de	Online-Backup
GEOTEK Datentechnik GmbH	geotek.de	Online-Backup
intrusys	www.intrusys.de	Online-Backup
inforsacom Informationssysteme GmbH	www.inforsacom.com	Backup as a Service
IT works!	www.itworks-hh.de	Online-Backups
Janz IT AG	www.janz.it.de	Backup as a Service
levigo	www.levigo.de	levigo.managed.backup
Macnetix GmbH	www.macnetix.de	Backup as a Service
matrix technology AG	www.matrix.ag/baas	matrix Backup as a Service
Mindtime Backup	www.mindtimebackup.de	Mindtime Backup
netclusive GmbH	www.netclusive.de	netclusive Online Backup
netcos AG	www.reback.de	ReBack Remote Backup Services
Oberdieck Online GmbH	www.oberdieck-online.de	Online-Backup
PROGTECH GmbH	www.progtech.net	BAYERN BACKUP
SpaceNet	www.space.net	SpaceNet Online-Backup
SSP Europe GmbH	www.ssp-europe.eu	SSP Secure Online Backup
teamix GmbH	www.teamix.de	FlexVault
TeamViewer GmbH	www.airbackup.de	airbackup
Terrabit GmbH	www.terrabit.de	Backup as a Service
Uptime	www.uptime.de	Uptime BaaS
Web2know GmbH	www.webattachedbackup.de/	WebAttachedBackup Professional

SSP Europe, matrix technology und Datis IT-Services.

Wer Online-Backups einsetzen will, sichert seine Daten physisch an einem anderen Ort. Um noch mehr Redundanz zu erreichen, speichern einige Anbieter wie Uptime, Concat und Terrabit die Daten ihrerseits auf einem zweiten System oder in einem weiteren, physisch getrennten Rechenzentrum.

Cloud Services Made in Germany

Einige der Betreiber gehören zu den mittlerweile über 160 Mitgliedern der Initiative „Cloud Services Made in Germany“, darunter BUSYMOUSE, Uptime, NetApp, matrix technology, teamix, Concat, Terrabit, dogado, PROGTECH, Datis IT-Services.

Als Aufnahmekriterien für Unternehmen gelten: in Deutschland gegründet und Hauptsitz dort. Das ist wichtig, denn nach amerikanischer Rechtsprechung können US-amerikanische Cloud-Anbieter zur Herausgabe von Kundendaten gezwungen werden, selbst wenn die in Europa lagern.

Außerdem vereinbaren die Mitglieder der Initiative mit ihren Kunden Verträge mit Service Level Agreements (SLA) nach deutschem Recht. Der Gerichtsstand für alle vertraglichen und juristischen Angelegenheiten ist Deutschland. Zudem stellt der Anbieter einen lokal ansässigen, deutschsprachigen Service und Support zur Verfügung.

Neben dem Standort des Rechenzentrums und dem Stammsitz des Anbieters gehört das Verschlüsseln zu den unbedingten Voraussetzungen für Sicherheit, besonders, wenn es sich um geschäftskritische Daten handelt. Das versteht sich nach dem Aufdecken der Überwachungsaktionen diverser Geheimdienste inzwischen von selbst. Sowohl Übertragungswege als auch die Daten müssen verschlüsselt sein, um den Zugriff für Unbefugte auszuschließen.

Als verbreitete Methode zum Kodieren der Daten hat sich derzeit der 256-Bit Advanced Encryption Standard (AES) durchgesetzt. Seine Verwendung versprechen die meisten der in der Marktübersicht gelisteten Anbieter, ebenso wie einen gesicherten Transport mit dem Verschlüsselungsprotokoll Secure Sockets Layer (SSL).

Ein weiterer Sicherheitsaspekt ist zudem die Frage, wer auf den Schlüssel zugreifen kann: nur der Kunde oder auch der Anbieter. Viele Cloud-Provider versprechen, dass ausschließlich der Kunde im Besitz des Schlüssels bleibt, darunter blackpoint und TeamViewer. Das Produkt von NetApp legt den Schlüssel entweder nur beim Kunden oder zusätzlich beim Anbieter ab, wenn jener den Restore-Prozess übernehmen soll.

Ob es sich bei einer verschlüsselten Datei noch um personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes handelt, hat Concat den Hessischen Datenschutzbeauftragten gefragt. Seiner Meinung nach sind es für den Dienstleister keine personenbezogenen Daten mehr, wenn er keine technischen Mittel hat, sie zu entschlüsseln. Als Voraussetzung dafür muss der Schlüssel unter alleiniger Kontrolle des Auftraggebers sein. Außerdem sind die Verschlüsselungsalgorithmen so zu wählen, dass sie nach dem Stand der Technik sicher sind, und der Anbieter muss die Algorithmen im Produkt korrekt implementiert haben. Wenn das Verfahren eines Tages nicht mehr wirksam ist, etwa weil es gehackt wurde, muss der Kunde die Daten beim Dienstleister komplett datenschutzgerecht löschen können (www.concat.de/wp-content/uploads/2013/01/Hessischer_Datenschutzbeauftragter_zu_Backup2Net.pdf).

Die Datenmenge klein halten

Technisch gesehen offerieren Anbieter unterschiedliche Methoden beim Sichern der Daten, um die Datenmenge klein zu halten und die Übertragungszeiten auf ein verträgliches Maß zu reduzieren. Bei großen Datenmengen kann man schließlich nicht in kurzen Intervallen immer

wieder den kompletten Bestand speichern. In der Regel ändert sich aber nur ein relativ kleiner Teil pro Tag. Bei kleinen Datenmengen hingegen kann man die Online-Backups über eine bestehende Internetverbindung im laufenden Betrieb durchführen.

Daten per Kurier

Differenzielle und inkrementelle Sicherungen setzen eine einmalige vollständige Datensicherung voraus. Dabei fallen große Datenmengen an – daher unterstützen viele Dienstleister eine spezielle Methode: das Speichern des ersten Backups auf einer eigenen Festplatte, die per Kurier ins Rechenzentrum geht (Seeding). Das bietet etwa Datis IT-Services an.

Sämtliche folgenden differenziellen Sicherungen enthalten nur neue Daten oder solche, die sich seit dem letzten vollständigen Backup geändert haben. Dabei bezieht sich die differenzielle Sicherung immer auf die Vollsicherung.

Im Unterschied dazu beinhalten inkrementelle Sicherungen nur Daten, die sich von der vorherigen inkrementellen Sicherung unterscheiden. Das heißt, die Backups sind miteinander verknüpft. Bei einem Restore muss sich das System den Bestand aus mehreren Sicherungen zusammenstellen. Das benötigt zwar eine noch geringere Menge als bei den differenziellen Sicherungen, das sukzessive Einspielen verketteter Sicherungen stellt sich jedoch oft als langwierig und fehlerträchtig dar [1].

Back2Web von blackpoint nutzt für veränderte Dateien eine Block-Level-Delta-Übertragung: Sie besteht nur aus Änderungen gegenüber dem letzten Backup, dafür soll ISDN oder eine UMTS-Verbindung genügen.

Im hybriden Backup kann man herkömmliche und Online-Backups verbinden. Solche Angebote sind ebenfalls in der Marktübersicht zu finden, wie die von Acronis, TeamViewer und PROGTECH. NetApp hat sein Backup as a Service (BaaS) um hybride Sicherungen erweitert. Eine Appliance namens AltaVault überträgt Daten, die der Anwender vorher mit herkömmlicher Backup-Software gesichert hat, in die Cloud eines autorisierten Partners von NetApp. Das Produkt nutzt eine Passwortverschlüsselung und eignet sich laut Anbieter daher auch für Unternehmen, die nach § 203 StGB keine unverschlüsselten Daten an Dritte auslagern dürfen. Diese Verschwiegenheitspflicht gilt für bestimmte Berufsgruppen, darunter Ärzte und Rechtsanwälte.

NetApp vertreibt sein BaaS-Produkt über zehn zertifizierte Provider und Reseller, darunter überwiegend lokale Anbieter wie Advanced Unibyte, AHD Hellweg Data, Datis IT-Services, IT works!, Janz IT, teamix, matrix und SHD.

VMs mit erfasst

Virtualisierte Systeme gehören mittlerweile zum Backup. Einige Anbieter, darunter Macnetix, nutzen zum Sichern virtueller Umgebungen von VMwares vSphere und Microsofts Hyper-V die Software Veeam. Das Unternehmen erzeugt mit einer Snapshot-Technik mindestens einmal am Tag ein Backup und gleicht es mittels Veeam mit dem Backup-Bestand ab.

Veeam ist ebenfalls bei Uptime im Einsatz. Das Unternehmen setzt auf IBMs Tivoli Storage Manager (TSM), mit dem Anwender das Sichern und Wiederherstellen von virtuellen, physischen und Cloud-Umgebungen jeder Größenordnung zentral verwalten können. Damit will der Anbieter kleineren Unternehmen einen Zugang zu einer Technik geben, die bisher nur in großen Firmen zum Einsatz kam.

Anbieter PROGTECH sichert ebenfalls sowohl traditionelle On-Premise-Systeme als auch virtuelle Umgebungen mit VMwares vSphere, Microsofts Hyper-V oder Citrix' Xen als Ganzes. Er unterstützt außerdem ein Virtual Disaster Recovery (VDR) in Form einer virtuellen Maschine, die sowohl virtualisierte als

auch physikalische Systeme speichert.

Acronis nutzt ein Bare-Metal Recovery, das ein gesamtes System auf beliebiger Hardware wiederherstellt. Alle dafür erforderlichen Komponenten gehören zum Backup, inklusive Betriebssystem.

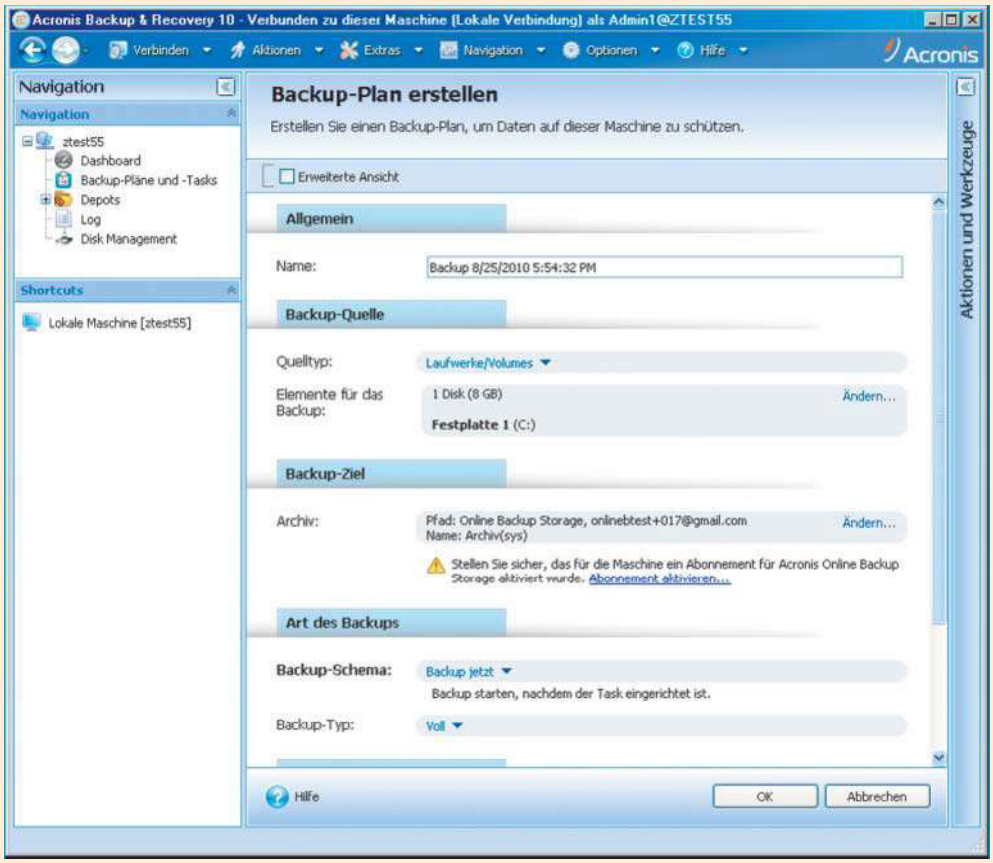
Nicht vernachlässigen sollten Anwender außerdem Backups für ihre mobilen Geräte wie Notebooks, Smartphones oder Tablets. Angebote dieser Art findet man unter anderem bei PROGTECH, cubos Internet und matrix.

Webkonsole für den Administrator

Bei einem vollständigen Datenverlust versendet blackpoint das gesamte Backup-Set verschlüsselt auf einem Datenträger. Concat wirbt damit, dass jeder autorisierte Mitarbeiter die Client-Software bedienen kann. Auf der Konsole für den Administrator des Produkts airback von TeamViewer kann man alle Geräte und Datensicherungen zentral verwalten und konfigurieren. Wenn der Administrator das Backup eines Servers starten möchte oder den Systemstatus eines Arbeitsplatzcomputers wiederherstellen muss, kann er dies auch remote tun. Fehler zeigt die Konsole sofort an oder schickt eine E-Mail.

Die Anbieter der Backup-Dienste rechnen oft nach Datenmenge pro Monat ab. Dabei kommt es darauf an, welches Stadium als Maßstab für die Menge gilt: vor oder nach Kompression und Deduplizierung. Letzteres reduziert die Volumen, indem es redundante Daten vor dem Speichern erkennt. NetApp und teamix etwa rechnen pro belegtem Terabyte ab – der Kunde zahlt nur für die Datenmenge, die nach dem Deduplizieren übrig geblieben ist.

Quelle: TeamViewer



Administratoren können ihren Backup-Plan selbst erstellen (Abb. 5)

Fazit

Zahlreiche externe Dienstleister bieten Online-Backup-Produkte an, die physische und virtualisierte Systeme sichern und wiederherstellen. Dabei setzen sie Sicherheitstechniken ein, die Cloud-Dienste ihren Reiz verleihen: ein Rechenzentrum in Europa beziehungsweise Deutschland, eine Zertifizierung sowie eine Ende-zu-Ende-Verschlüsselung von Daten und Transportwegen.

Wer nicht komplett auf externe Anbieter setzen möchte, kann mit einem hybriden Konzept einen Mittelweg gehen. Ob man Online-Backups als einzige oder zusätzliche Methode einsetzt, hängt von der Unternehmensgröße, vom Vertrauen in externe Dienstleister und der Kraft der eigenen IT-Abteilung ab, für die Backups in die Cloud auf jeden Fall eine Entlastung bedeuten dürften. (rh)

Barbara Lange ist IT-Journalistin und Inhaberin des Redaktionsbüros kurz und einfach in Lengede.

In iX extra 09/2015

Webhosting: Application Hosting – Software außer Haus

Die Idee, statt eines Servers doch gleich die gehostete Software zur Verfügung zu stellen, ist nicht neu. In der Vergangenheit standen Begriffe wie ASP oder SaaS für diese Angebote. Aber erst eine ausgereifte Virtualisierung und mandantenfähige Software erlauben es, das Prinzip auf nahezu jede Anwendung zu übertragen und kundenspezifische Services zu entwickeln. Am weitesten verbreitet sind Webshops, CRM-Systeme und Groupware. Im Gegensatz zu manchen Cloud-Services, die ähnliche Ziele verfolgen, garantiert Application Hosting eine Datenhaltung in Deutschland nach nationalem Recht.

Erscheinungstermin:
27. August 2015

Ausgabe		Thema	Erscheinungstermin
10/15	Security	Trends und News 2015	24.09.2015
01/16	Cloud-Computing	Verfügbarkeit sicherstellen: Cloud-Speicher überwachen	17.12.2015

Literatur

[1] Tilman Wittenhorst; Doppelte Leitung; Online-Backup für Unternehmen; *iX* 3/2015, S. 50