



IT-Grundschutz

Informationsdienst

Praxis und Anwendungen

Buyers Guide Online-Back- up für den Mittelstand

Seite 9



Quelle: Stockphoto/Alex Slobodkin

NEWS

Weltweite Studie zu Banken und Finanzinstituten Seite 2

Sophos Threat Monitor für Apple Seite 2

Viele Deutsche geben Passwörter weiter Seite 2

Rubriken

Editorial Seite 2

Impressum Seite 15

IT und Recht

Sicherheit für E-Mails korrekt umsetzen Seite 3

Workshops

Ordnungsgemäßes Löschen und Vernichten von Daten Seite 6

Praxis und Anwendungen

Buyers Guide Online-Backup für den Mittelstand Seite 9
Backup in der Cloud Seite 13

Studien und Analysen

Endspurt für Grundschutz-Studie Seite 12

So fern und doch so nah

Buyers Guide Online-Backup für den Mittelstand

Elmar Török, bits+bites

Seit Bandbreiten und Flatrates die DSL-Anschlüsse in veritable Datenautobahnen verwandeln, gewinnt die Datensicherung bei einem Backup-Provider immer mehr Anhänger. Die richtigen Überlegungen im Vorfeld erleichtern die Wahl des besten Anbieters.

Das Thema Backup ist gleichermaßen unbeliebt wie wichtig. Seit es Computer gibt, existieren auf deren Speichermedien wichtige Daten, die geschützt werden müssen. Und mindestens genau so lange wird dieser Schutz vernachlässigt. Sei es aus Kostengründen, weil es zu kompliziert ist oder schlicht, weil Menschen Fehler machen: Es kommt zu Datenverlusten, die es doch eigentlich zu verhindern gilt.

Naturgemäß haben große Unternehmen geringere Probleme mit der korrekten Sicherung. Sie verfügen über das Personal und die Budgets, um Hard- und Software zu kaufen und zu pflegen. Zudem sind sie oftmals durch Compliance-Vorgaben dazu verpflichtet, ihre Datensicherung nach hohen Standards durchzuführen. Anders kleine und kleinste Firmen. Bei ihnen ist das Backup eine ungeliebte Zusatzaufgabe, die nur nebenher wahrgenommen wird oder oftmals komplett unter den Tisch fällt.

Laut einer europaweit durchgeführten Studie (1) benötigen 56 Prozent der deutschen Unternehmen nach IT-Störfällen zwischen einem Tag und einer Woche um den Geschäftsbetrieb wieder aufzunehmen. Zwei Prozent der befragten Organisationen sind gar nicht in der Lage, ihre Daten und Systeme wiederherzustellen.



Widrige Umstände im Weg

Die Gründe, warum es seit Jahr und Tag mit dem Backup nicht klappen will, sind vielfältig. Zum einen wird bei der Investition gespart, schließlich trägt Datensicherung ohne den Ernstfall nicht zum Betriebsergebnis bei. Zum anderen verursacht die Bedienung und regelmäßige Kontrolle der Sicherungsvorgänge Aufwand. Nutzt man dafür ein Magnetband, muss es gewechselt und rechtzeitig erneuert werden. Dazu kommen unter Umständen Kosten für die Reinigung des Magnetkopfes und die Lagerung der Bänder in einer klimakontrollierten Umgebung, damit die Alterung der Tapes möglichst verlangsamt wird. Eine externe Festplatte kommt ohne Wechsel aus, darf aber – wie

die Bänder – nicht nur im Büro stehen, um Diebstahl, Feuer- oder Wasserschäden vorzubeugen.

Das Auslagern von Bändern und Platten ist ebenfalls mit Aufwand und Risiken verbunden. Zudem generiert die Software Protokolle, die man kontrollieren und nach Fehlern durchsuchen muss. Oft gibt es keinen Zuständigen für diese Pflichten, wenn doch, hat er zusätzliche Aufgaben, die regelmäßige Kontrolle des Backups wird gern verdrängt.

Ganz ohne den leidigen Bandwechsel und Off-Site Lagerung kommt eine Form des Backups aus, die erst in den letzten drei Jahren maßgeblich an Bedeutung gewonnen hat. Die Datensicherung auf Speicherressourcen im Internet ist bei Weitem nicht so stark verbreitet wie herkömmliche Methoden

Bildquelle:
iStockphoto/
Henrik Jonsson

mit Magnetband und Festplatte. Doch die praktisch durchgehende Verfügbarkeit breitbandiger DSL-Anschlüsse in Kombination mit günstigen Flatrates macht den Einsatz von Online-Backups zumindest technisch problemlos möglich.

In Deutschland haben ADSL-Anschlüsse üblicherweise eine maximale Upload-Geschwindigkeit von 1 Mbit/s. Damit können theoretisch 450 Megabyte pro Stunde oder 10,5 Gigabyte pro Tag übertragen werden. Für ein großes Unternehmen reichen solche Mengen nicht aus, selbst wenn man nur geänderte Dateien mit dem Online-Vault synchronisiert. Doch kleine und mittelständische Firmen könnten diese Backup-Alternative als Ergänzung und Erweiterung in ihr Datensicherungskonzept einbinden.

Unerreichbar für Desaster

Der offensichtliche Vorteil eines ausgelagerten Sicherungsorts ist die Entkoppelung von physischen Schäden, die den Firmenstandort treffen könnten. Auch für Notebooks kann die Methode einen Sicherheitszuwachs bedeuten. Ihre Dateien werden nicht mehr nur dann gesichert, wenn sie eine ausreichend schnelle Verbindung mit dem Firmennetz haben, sondern sobald sie online sind. Kleine Firmen verfügen in der Regel nicht über die Infrastruktur um das Backup von mobilen Clients per VPN zentral sicher zu stellen.

Zahlreiche Anbieter haben mittlerweile Dienstleistungen im Umfeld der Online-Datensicherung im Programm. Deren Funktionen, Zielgruppen und Preisstruktur unterscheiden sich ebenso wie das primäre Einsatzfeld. So gibt es Provider, die den Fokus eher auf die Zusammenarbeit im Team legen und die Dateien online für mehrere Benutzer zugänglich machen. Andere Anbieter zielen ausschließlich auf Backup ab und bieten dedizierte Client-Software sowie umfangreiche Sicherheitsmaßnahmen.

Wer sich für Online-Backup entscheidet, muss im Vorfeld ein paar Eckdaten abklären. So staffelt praktisch der Anbieter den Preis seiner Dienstleistung nach der gewünschten Online-Speicherkapazität. Eine grobe Übersicht, welche Daten schützenswert sind und wie viel Kapazität diese, mitsamt Änderungen, über einen bestimmten Zeitraum belegen, gehört zu den Hausaufgaben, die man als potenzieller Kunde erledigen muss. Die Preisstrukturen können auch Überraschungen im Kleingedruckten verbergen. So sind Einrichtungsgebühren ebenso möglich wie eine Gebühr für das vollständige und sichere Löschen der Daten nach Beendigung des Vertrags. Es gibt auch die Variante, die Kapazität günstig anzubieten aber den Upload pro Monat zu beschränken. Service und Support schlägt in den meisten Fällen ebenfalls extra zu buche.

Sind zu Anfang sehr große Datenmengen zum Provider zu übertragen, kann eine mit der Post versandte Festplatte die günstigere und vor allem schnellere Alternative für die Erstbeschickung sein. Nicht alle Provider bieten diesen Weg an und nicht alle verschlüsseln die Daten auf der Festplatte automatisch für den Versand. Noch wichtiger ist diese Wahlmöglichkeit bei der Wiederherstellung von großen Datenmengen. Selbst wenn der Datenträger einen Tag unterwegs ist, schlägt er den Download möglicherweise um Längen.

Einfach muss es sein

Der Hauptgrund für die vielen Probleme beim Backup sind Benutzerfehler. Sobald menschliche Interaktion für die Ausführung notwendig ist, können Fehler passieren. Um Benutzer und Administratoren zu entlasten, muss der Online-Backup Provider eine Software anbieten die sich zum einen schnell und nahtlos in die zu sichernden Systeme integrieren lässt und zum anderen so viel manuelle Bedienung erlaubt,

wie nötig. Während die Backups in der Regel automatisch erfolgen sollen, muss auch die Möglichkeit bestehen, eine Sicherung per Mausklick auszulösen. Die unterstützten Betriebssysteme spielen ebenfalls eine große Rolle. Viele Anbieter beschränken sich auf Windows, gerade im KMU-Umfeld sind aber auch Macs weit verbreitet. Die Server-Varianten der Betriebssysteme müssen unter Umständen ebenfalls berücksichtigt werden. Für die Wiederherstellung ist auch ein betriebssystemunabhängiger Web-Zugang sinnvoll.

Möglichst einfach sollte die Auswahl der zu sichernden Daten sein. Üblich ist ein Verzeichnisbaum im Explorer-Stil, in dem der Anwender einen Haken bei den gewünschten Ordnern macht. Nicht jede Datei eignet sich allerdings für die Online-Sicherung. So können offene Dateien nur dann korrekt gesichert werden, wenn Sicherungssoftware mit Microsofts VSS (Volume Shadow Copy Service) unterstützt. Wenn selbst geschriebene oder Custom-Applikationen geschützt werden sollen, ist vorher die Rücksprache mit Programmierer oder Hersteller ratsam. Gute Datensicherungs-Tools verfügen zudem über einen Dateifilter, um temporäre Files auszuschließen. Sonst produziert die Software unnötigen Datenverkehr für Dateien, die ohnehin wieder gelöscht werden. Beinahe selbstverständlich ist, dass neben dem anfänglichen Vollbackup auch inkrementelle Backups möglich sind.

Gerade wenn Word- oder Excel-Dateien in der Online-Vault liegen, ist eine Versionshistorie sinnvoll. So können auf einfache Weise frühere Stände von gesicherten Dateien zurückgeholt werden. Unbedingt notwendig sind regelmäßige Reports über Erfolg oder Misserfolg der Sicherungsvorgänge. Interessenten sollten darauf achten, dass die Häufigkeit der Meldungen ebenso konfigurierbar ist, wie die Zieladressen. Manchmal soll der Benutzer selbst sehen, was von seinem

Computer gesichert wurde, manchmal ist der Administrator zentraler Ansprechpartner für alle Reports. Übrigens ist das Ziel des Backups zwar immer ein Online-Datenspeicher, doch einige Anbieter erlauben es, zusätzliche Speicherorte zu benennen. Andere PCs im lokalen Netz sind ebenso möglich wie ein gemeinsames Netzlaufwerk.

Sicherung der Sicherung

Es liegt in der Natur der Dinge, dass bei einem extern gelagerten Backup Informationen die Firmengrenzen verlassen, die niemand sonst sehen darf. Daher stehen die Sicherheitsvorkehrungen bei der Auswahl des richtigen Anbieters ganz weit oben. Jeder Provider offeriert mindestens zwei Sicherheitsvorkehrungen: Verschlüsselung für die Daten in Transit und ein Passwort, das den Zugriff auf die abgelegten Dateien schützt. Diese Art des Schutzes lässt dem Provider meist ebenfalls Zugriff auf die Datensätze. Das kann erwünscht sein, weil dann noch ein Hintertürchen offen ist, falls man die eigenen Zugangsdaten verliert.

Doch vielen Firmen wird bei dem Gedanken nicht ganz wohl sein, dass auch der Provider theoretisch sehen kann, was im Archiv liegt. Daher sollten potenzielle Kunden darauf achten, dass es eine zweite Sicherheitsstufe im Angebot gibt, die zur Grundverschlüsselung noch ein weiteres privates Passwort hinzufügt. Das zweite Passwort kennt nur der Kunde. Auf diese Weise gesicherte Backups können nur mit beiden geheimen Passwörtern gelesen und wieder hergestellt werden. Allerdings kann der Service Provider auch im Notfall kein verlorenes Passwort zur Verfügung stellen. Ist das Passwort weg, werden die bis dahin abgelegten Daten unbrauchbar.

Das stellt aber nur dann ein Problem dar, wenn gerade ein Datenverlust aufgetreten ist und der Kunde das Backup zurückspielen möchte. Ansonsten wählt man einen neuen

Schlüssel und stößt das Backup mit den aktualisierten Keys erneut an. Verloren sind in dem Fall nur die alten Versionen der Dateien.

Beim niederländischen Anbieter Crashplan Pro gibt es sogar noch eine dritte Sicherheitsstufe. Dabei erzeugt der Nutzer selbst einen privaten Schlüssel mit 448-Bit Länge und verschlüsselt seine Daten damit. Der Schlüssel verlässt niemals den Rechner des Anwenders, bei einer Änderung muss sich der Administrator selbst um das Synchronisieren aller Schlüssel auf allen Computern kümmern. Auf dem Backup-Server wird das Archiv der Festplatte als große verschlüsselte Datei gespeichert.

Der lange Arm des Gesetzes

Sehr selten bieten die Provider eine zusätzliche VPN-Verbindung zwischen eigenem Netz und Backup-Server. Dieses VPN verhindert außerdem Brute Force-Attacken über das Internet auf den Backup-Server. Solche Maßnahmen sind für Anwender mit extrem hohen Sicherheitsanforderungen gedacht. Allerdings stellt sich bei diesem Kundenkreis die Frage, ob ein extern gehostetes Backup generell das richtige ist. Für alle Kunden interessant ist hingegen die Frage nach dem physikalischen Standort der Daten. Jedes Land hat seine eigenen Datenschutzgesetze, Deutschland gehört zu den strengsten Datenwächtern weltweit. Insbesondere bei sehr sicherheitsrelevanten Daten kann die Verpflichtung eines Backup-Partners sinnvoll sein, der über Rechenzentren in Deutschland verfügt und zusichert, die Backups nur dort zu lagern. Übrigens: Wird der Vertrag mit dem Provider beendet, sollte man neben der Bestätigung für die fristgemäße Kündigung auch einen Nachweis über die Löschung der Daten nach Vertragsende einfordern.

Dank Online-Backup sind die Firmendaten nun sicher, aber wie sieht

es mit dem Provider selbst aus? Eine massive abgesicherte und verschlüsselte Verbindung ist ja schön und gut, aber was hilft sie, wenn das Rechenzentrum des Hosting-Partners kein modernes Sicherheitskonzept verfolgt. Die meisten Provider bieten eine Basissicherung nach marktüblichen Standards an. Wer mehr will, zum Beispiel zertifizierte IT-Sicherheit nach ISO-27001/2, muss extra in die Tasche greifen. Dabei gilt es, eines zu bedenken: Die gesicherten Informationen sind das Kapital der Firma, ihre Wiederherstellung ist meist kostenintensiv wenn nicht gar unmöglich. Durch eine zuverlässige Sicherung per Online-Backup stehen selbst nach katastrophalen Systemausfällen alle Informationen praktisch ohne Zeitverzögerung zur Wiederherstellung zur Verfügung. Das sollte auch kleinen und mittelständischen Firmen den Aufpreis für das Rundum-Sorglos-Paket wert sein. ■

(1) http://www.acronis.de/enterprise/download/docs/whitepaper/?f=WP_AcronisStudie_DSR-in-Unternehmen.pdf