Mit Speicherdiensten sorgfältig umgehen

Stiftung Warentest hat Cloud-Speicherdienste getestet – und empfiehlt Unternehmen, auf europäische Anbieter zu setzen statt auf SkyDrive, Google Drive und DropBox.

VON THOMAS ALTHAMMER

Foto: Sonnek Schmidtmann

Burgwedel // Festplatten im Netz sind populär, verbinden sie doch Synchronisation, Datensicherung und vereinfachten Zugriff von einer Vielzahl von Endgeräten. Das geschieht alles automatisch und zu günstigen Konditionen, teils sogar kostenfrei. Doch warum kann für Pflegeeinrichtungen der Einsatz von Online-Speicherdiensten problematisch sein?

1. Sensible Informationen oder gar personenbezogene Daten verlassen über DropBox & Co. unbemerkt die Einrichtung, wenn Mitarbeiter derartige Lösungen auf ihren Computern installieren. So können Unterlagen in fremde Hände gelangen oder haftungsrechtliche Konsequenzen entstehen. Die Verantwortung bei Verstößen liegt fast immer bei der Geschäftsleitung.
2. DropBox und vergleichbare Angebote sind bequem und erhöhen insofern die Datensicherheit, dass die dort gespeicherten Dateien auf verschiedenen Systemen synchron gehalten werden. Das versehentliche Löschen kann rückgängig gemacht werden, manche Dienste bieten sogar die Möglichkeit, vorherige Versionen einer Datei wiederherzustellen. Doch hier kann eine trügerische Sicherheit entstehen: Speicherdienste können Teil eines zentralen Backup-Konzepts sein, dürfen dieses aber nicht ersetzen oder unterlaufen, beispielsweise dadurch, dass Dateien nur noch auf lokalen Workstations gespeichert werden und nicht mehr in die zentrale Datensicherung aufgenommen werden. Ohne regelmäßige Audits und Richtlinien bekommen Unternehmen hiervon häufig nichts mit.
3. Viele Dienste bieten in der Standardausführung öffentliche Ordner an, die zum einfachen Teilen von Dateien genutzt werden können. Unbedacht gespeicherte Fotos und Dokumente sorgen dafür, dass Daten unter Umständen öffentlich zugänglich sind und per Google-Suche gefunden werden können. Einrichtungen sollten über die Einstellungen dafür sorgen, dass nur sie auf private Daten zugreifen können.
4. Cloud-basierte Speicherdienste verteilen Dateien automatisch. Bei Diebstahl oder Verlust eines Geräts hat der Finder damit dann auch Zugriff auf diese Daten. Speicherdienste verleiten dazu, stets alles Wichtige dabei zu haben. Mangelnde Verschlüsselung verursacht so unliebsame Zugriffe, auch auf sensible Bankunterlagen, das Passwortverzeichnis oder Unternehmensinterna.
5. Im Kleingedruckten der Nutzungsbedingungen finden sich häufig Passagen, die das Ablegen unangemessener Inhalte verbieten. Insbesondere die amerikanischen Anbieter setzen automatisierte Verfahren ein, um die Konten der Nutzer zu durchsuchen und problematische Daten zu finden. Auf diese Art wurden bereits Konten bei SkyDrive gesperrt und alle Daten automatisch gelöscht, weil Fotografen ihre Bilder hier gesichert haben. Mit dabei waren auch harmlose Aktaufnahmen, die den Filtersystemen von Microsoft offenbar nicht passten. Die Fotodokumentation eines Dekubitus könnte so für medizinische Einrichtungen oder Pflegeanbieter zu einer vollständigen Kontensperrung beim Cloud-Anbieter führen.

Es empfiehlt sich daher, sich mit dem Thema auseinanderzusetzen. Dienste wie BoxCryptor helfen, bei Cloud-Speicherdiensten abgelegte Dateien vollständig zu verschlüsseln. Oder greifen Sie auf Alternativen wie TeamDrive zurück, die per se alle Daten nur verschlüsselt ablegen, ohne dabei – nach eigenem Bekunden – Zugriff auf die Daten ihrer Kunden zu haben.

Grundsätzlich sind Speicherdienste für Unternehmen eine feine Sache. Art und Umfang der Nutzung sollten jedoch wohl überlegt sein.

■ **Der Autor ist Inhaber der Althammer IT-Beratung in Burgwedel, www.althammer-it.de;**

www.test.de/Daten-in-der-Cloud-Online-Speicherdienste-im-Test-4579657-0