

7 typische Fehler bei der Entscheidung für das Online Backup

23.11.2009, 16:26 | IT, New Media & Software

Pressemitteilung von: *Continum AG*

Presseagentur: *Agentur Denkfabrik*

(Freiburg, 23.11.2009) Nach einer kürzlich durchgeführten Erhebung des Freiburger Hosting-Anbieters Continum AG neigen immer mehr Mittelstands- und Großunternehmen dazu, ihre Sicherungsdaten in die Obhut eines Providers zu geben. Sie verfolgen damit insbesondere wirtschaftliche Motive und eine Entlastung der internen Ressourcen. Die Berater von Continum haben jedoch festgestellt, dass Unternehmen bei ihren Auswahlprozessen der Backup-Services oftmals ein zu unklares Anforderungsprofil entwickeln. Zu den typischen Fehlern mit teilweise weitreichenden Folgen gehören aus Praxissicht der Consultants insbesondere:

1. Datenübertragung ohne VPN: Zugriffe auf den Online Backup-Server und das Kunden-Webinterface müssen auf einen geschlossenen Benutzerkreis beschränkt werden, was die Verwendung von VPN (Virtual Private Network) notwendig macht. Dies verhindert Denial-of-Service-Attacken oder unautorisierte Login-Versuche über das öffentliche Internet auf den Backup-Server. Ohne VPN ist zwar die Übertragung der Daten auch verschlüsselt, aber der Online Backup-Server selbst ist dennoch für die ganze Welt sichtbar. Dies stellt für den Anwender ein entscheidendes Sicherheitsloch dar.
2. Es wird nicht auf vollautomatisierte Datensicherungsprozesse geachtet: Ein Online Backup ist unter Effizienzaspekten nur sinnvoll, wenn der Benutzer einerseits zu frei wählbaren Zeiten die Datensicherung auf den Systemen des Hosting-Partners vornehmen kann, es sich dabei aber gleichzeitig auch um einen vollautomatischen Service handelt. Dies gilt sowohl für Backup über den Client des Benutzers als auch für den Zugriff auf die gespeicherten Daten im Falle einer erforderlichen Wiederherstellung von Daten.
3. Erst- und Rücksicherung nur online möglich: Bei geringen Datenmengen erfolgen die Erstsicherung bei Vertragsbeginn oder Rücksicherungen während der Vertragslaufzeit sinnvollerweise immer online. Bei großer Datenmenge muss der Anwender die Flexibilität haben, die Erstsicherung der Daten auf ein Offsite Medium (z.B. verschlüsselt auf USB Platte) durchzuführen und dem Hosting-Partner zum Übertragen auf die Sicherungsserver einsenden zu können. Noch wichtiger ist diese Wahlmöglichkeit beim Restore von großen Datenmengen im Desasterfall. Der Anwender muß sicherstellen, daß der Hosting-Partner ihn nicht auf die „Online Rücksicherung“ beschränkt.
4. Schwieriges Handling für die Benutzer: Sind spezielle Administratorenkenntnisse erforderlich, könnte ein Backup-Outsourcing nur begrenzten Nutzen bieten. Deshalb muss es sich durch leicht verständliche Funktionen kennzeichnen, die auch von Mitarbeitern in den Fachbereichen der Unternehmen zu bedienen sind, die typischerweise über keine speziellen IT-Kenntnisse verfügen. Dem Benutzer sollte auch bei jedem Backup automatisch ein Report per E-Mail zugeleitet werden, damit er im Falle eines nicht erfolgreichen Backups eine erneute Speicherung vornehmen kann.
5. Unklare Sicherheitsverhältnisse des Provider-Rechenzentrums: Es gibt dem Kunden nur eine Scheinsicherheit, wenn zwar hochsichere Datenverbindungen bestehen, aber das Rechenzentrum des Hosting-Partners kein modernes Sicherheitskonzept verfolgt. Zu dessen elementaren Anforderungen gehört, dass die Kundendaten auf zwei räumlich getrennten Sicherungsservern redundant vorgehalten werden. Zudem muss das Rechenzentrum mit Zugangskontrolle, Alarmanlage, Videoüberwachung, USV und Dieselaggregat, Klimatisierung sowie Feuerlöschanlage ausgestattet sein. Darüber hinaus sollte ein zentrales Überwachungssystem die Erreichbarkeit und Funktion der Services auf den Servern permanent überprüfen.
6. Support erzeugt Extrakosten: Gerade die preislichen Lockangebote beinhalten im Regelfall nur geringe Services und damit auch keine oder lediglich minimale und zeitlich eingeschränkte Support-Dienste. Stattdessen müssen sie im Bedarfsfall zusätzlich bezahlt werden, wodurch sich die Gesamtrechnung für das Backup-Outsourcing ganz erheblich negativ verändern kann. Insofern gilt es, darauf zu achten, dass die Leistungen hochwertige Support-Services rund um

die Uhr enthalten.

7. Eingeschränkter Datenschutz bei Speicherung im Ausland: Der deutsche Datenschutz nach deutschem Recht ist anspruchsvoller als in vielen anderen Ländern. Aus diesem Grund empfiehlt es sich insbesondere bei sehr sicherheitsrelevanten Daten, einen Backup-Partner in Anspruch zu nehmen, dessen Rechenzentrum in Deutschland beheimatet ist.

Portrait

Über Continuum:

Die Continuum AG betreibt in Freiburg i. Br. eines der modernsten Internet-Rechenzentren in Deutschland. Die Kernkompetenz ist der sichere und hochverfügbare Betrieb und die individuelle Betreuung von Internet-Systemen und Anwendungen. Seit der Gründung 1996 ist das Unternehmen mit dieser Kompetenz für gewerbliche Kunden in Deutschland, der Schweiz und Frankreich erfolgreich tätig.

www.continum.net

News-ID: 373624 • Views: 154 (Stand: 14.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/373624/7-typische-Fehler-bei-der-Entscheidung-fuer-das-Online-Backup.html>