ARTIKEL IT-Sicherheit in Unternehmen

Vorsorge ist besser als Datenrettung

Von Cloud-Security bis Disaster Recovery: Für Firmen mit viel IT sind ausgeklügelte Sicherheitsstrategien unverzichtbar.

VON TOBIAS LEMSER

Ob Steuerberatungskanzleien, Krankenkassen oder Maschinenbauunternehmen: Keins dieser Unternehmen kann heutzutage noch auf Informationstechnik verzichten. Damit sie die Betriebsabläufe jederzeit aufrechterhalten können, ist es unerlässlich, die in die IT getätigten hohen Investitionen durch facettenreiche Security-Maßnahmen abzusichern. Und dabei sollte das Spektrum weit über Antivirensoftware und Firewalls hinausgehen.

Redundantes Speichern sichert ab

Ein grundlegender präventiver Beitrag zum Schutz aller Daten liegt vor allem in der redundanten (Echtzeit-) Datensicherung. Zudem sollten Back-up-Medien nicht nur physisch getrennt aufbewahrt werden, auch empfiehlt es sich, das gesamte System regelmäßig zu sichern. Fällt die Festplatte in Gänze aus, besteht so immer die Option, diese durch eine neue zu ersetzen und das System-Back-up binnen kürzester Zeit wieder einzuspielen.

Als strategisch ebenso sinnvoll kann sich die Online-Speicherung auf externen Servern erweisen. Cloud Computing bietet sich insbesondere dann an, wenn Unternehmen kein eigenes Rechenzentrum besitzen und große Datenmengen verwalten müssen. So entfallen nicht nur kostenintensive Investitionen, auch verfügt die Cloud bei schwankendem Bedarf über ausreichend Speicherkapazitäten. Nicht zuletzt ermöglicht sie eine verbrauchsabhängige Bezahlung und ist zudem vor Havarien im Unternehmen sicher.

Rechtlich abgesichert in die Wolke

Um in der Cloud auf Nummer sicher zu gehen, gilt es, datenschutzrechtliche Gesichtspunkte ins Visier zu nehmen. So ist es ratsam, einen Cloud-Anbieter mit einer Auftragsdatenverarbeitung in der Europäischen Union oder auch in der Europäischen Wirtschaftszone zu beauftragen. Darüber hinaus sollten Unternehmen vor Abschluss eines Vertrages mit einem Cloud-Anbieter einen Blick auf transparente Vereinbarungen und eindeutige Garantien haben. Weiterhin gilt es zu klären, ob ein Notfallplan für größere Havarien besteht, wer auf die Daten zugreifen kann und ob seitens des Dienstleisters unabhängige Zertifikate oder Siegel vorliegen. Für Sicherheit stehen ebenso neuartige Verschlüsselungskonzepte, bei denen die Daten auf dem Weg in die Wolke einen sogenannten Cloud-Connector durchlaufen. Erst bei einem erneuten Zugriff werden sie im eigenen Netzwerk wieder entschlüsselt.

Trend zu Mobile-Device-Management

Um der stetig ansteigenden Gerätevielfalt und den damit verbundenen Sicherheitsbedenken Rechnung zu tragen, setzen Unternehmen zunehmend auf ein Mobile-Device-Management (MDM). Vorteil: Mittels zentraler Lösungen lassen sich die unterschiedlichen, teils privaten Endgeräte intelligent in die Firmenabläufe integrieren und verwalten. Auch sind die Firmen dank MDM imstande, enthaltene Daten zu sichern, Sicherheitslücken zu schließen sowie Software-Updates zu zentralisieren und drahtlos aufzuspielen.

Damit Hackern und Wirtschaftsspionen jederzeit der Zugang ins Unternehmen verwehrt bleibt, ist es unerlässlich, die mobilen Endgeräte aufzurüsten: „Zum einen sollte der Einsatz von Schutzsoftware oberste Priorität haben, zum anderen sollten Nutzer jedoch auch ihr neues Gerät detailliert kennen und darauf verzichten, unsichere Apps herunterzuladen“, rät Oliver M. Achten vom Institut für Internet-Sicherheit an der Westfälischen Hochschule. Ferner macht es sich bezahlt, Daten stets verschlüsselt auf dem mobilen IT-System abzulegen und den Zugriff auf das Unternehmensnetzwerk ausschließlich per VPN erfolgen zu lassen.

Von größter Relevanz ist ebenso der Hardwareschutz: Brand, Blitz und Bruch sind die größten Risiken für IT-Hardware. Schützen Überspannungsschutzgeräte vor Blitzeinschlag, schirmen Server-Safes die IT-Hardware vor Wasser und Brand ab. Viele dieser Datensicherungsschränke beinhalten feuer-, gas- und wasserdichte Kabeldurchführungen. Zudem bietet ein Safe Schutz vor Rauchgasen, Staub und Fremdzugriff.

Wie Firmen Stromausfälle abfedern

Bereits eine Unterbrechung der Stromversorgung von nur zehn Millisekunden kann dazu führen, dass wichtige Daten auf Servern oder Computern fehlerhaft verarbeitet werden oder sogar verloren gehen. Gerade deshalb ist es für Firmen oder auch Krankenhäuser, die immense Datenvolumina verarbeiten und auf hoch sensible Technik angewiesen sind, erforderlich, ein Kontinuitätsmanagement durchzuführen.

Geradezu prädestiniert dafür, Stromunterbrechungen zu überbrücken, ist die sogenannte USV-Technik. Sie besteht aus Akkumulatoren, Stromrichtern und elektronischen Regelungen und ist in der Lage, bei einem Stromausfall die Stromversorgung solange aufrechtzuerhalten, bis ein geordnetes Herunterfahren der angeschlossenen Rechner möglich ist. USV-Geräte filtern ebenfalls Störungen wie etwa Spannungs- und Frequenzschwankungen heraus und stellen so eine fehlerfreie Stromversorgung sicher. Rechenzentren großer Unternehmen greifen zudem bei Bedarf auch auf Notstromgeneratoren zurück. Größere, zumeist mit Diesel angetriebene Geräte lösen nach kurzer Anlaufzeit die Akkumulatoren ab, um die Stromlücke fortdauernd zu schließen.

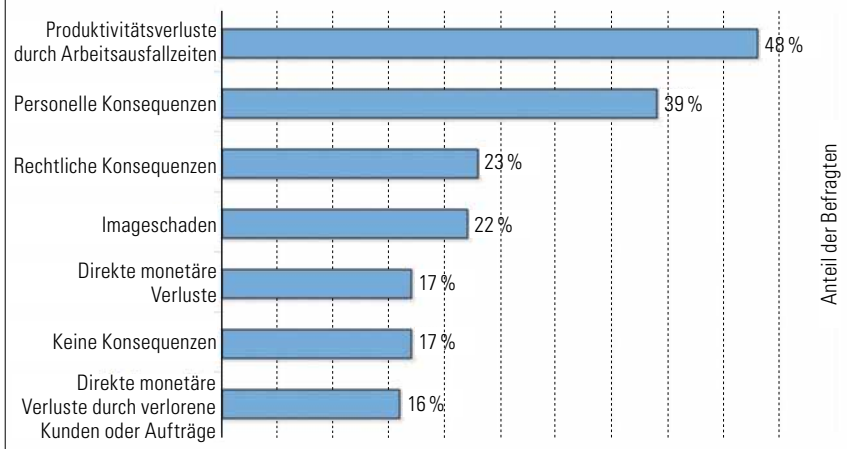
Disaster Recovery bringt Daten zurück

Trotz zahlreicher Vorsorgemaßnahmen empfiehlt Professor Dr. Hartmut Pohl von der Gesellschaft für Informatik Unternehmen ein minutiös geplantes Disaster Recovery: „Es ermöglicht nach einem unvorhergesehenen Ausfall den Wiederanlauf der gesamten IT eines Unternehmens und damit die zeitnahe Wiederaufnahme der Geschäftsfähigkeit eines Unternehmens.“ Dabei sollte eine Analyse der Netzwerke, Systeme und Geschäftsprozesse ganz oben auf der Agenda stehen. Sind gespeicherte Daten auf einem Datenträger abhanden gekommen, so können auf Disaster Recovery spezialisierte Unternehmen – sofern die betroffenen Platten-Sektoren nicht mehrfach überschrieben wurden – diese mittels spezieller Software mit einer hohen Erfolgsquote rekonstruieren.

Ist der Aufwand für Unternehmen zu groß, selbst umfassende Sicherheitsmaßnahmen durchzuführen, besteht die Möglichkeit, sogenannte Managed Security zu betreiben. Dabei kann zwischen Auftraggeber und Outsourcing-Dienstleister individuell festgelegt werden, welche Leistungen dem Bedarf des jeweiligen Unternehmens am ehesten entsprechen. Auch bietet sich die Option, alle Sicherheitsdienstleistungen im Gesamtpaket vom Anbieter übernehmen zu lassen.

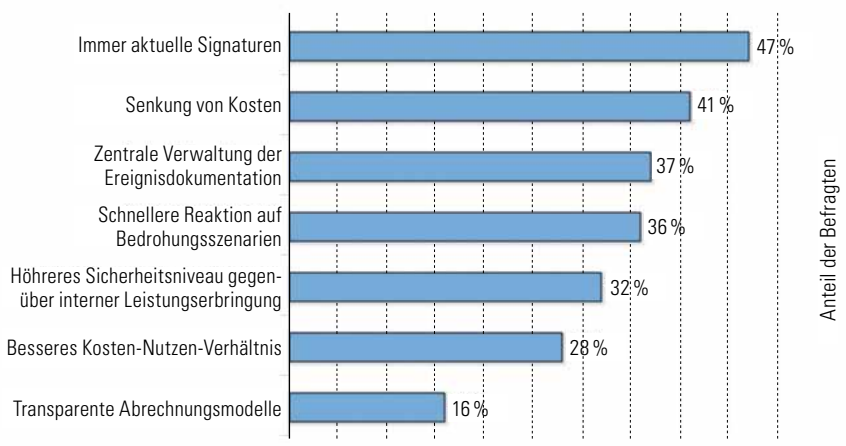
Fakt ist: „Investieren Unternehmen in geeignete Back-up-Strategien können sie Datenverlust nicht nur vorbeugen, sondern praktisch völlig ausschließen“, so Pohl. Sparen sie dagegen an der falschen Stelle und verlieren brisante Daten, drohen Produktivitäts- und Umsatzausfälle, die schlimmstenfalls – gerade für kleinere Betriebe – sogar das Aus bedeuten können. ■

Welche Folgen ergaben sich aus Angriffen auf die IT-Sicherheit in Ihrem Unternehmen?



Deutsche Unternehmen mit mehr als 100 Mitarbeitern; 146 Befragte; Quelle: IDC; © Statista

Welche Argumente sprechen für Coud basierte Security Services?



Deutschland; IT-Verantwortliche in Firmen mit mehr als 100 Mitarbeitern; 202 Befragte; 2011; Quelle: IDC; © Statista