

### DATENSICHERHEIT

# Standard-Methoden der Datensicherung

**Das Thema Datensicherheit wird bei vielen Unternehmen noch nicht so groß geschrieben, wie dies zu wünschen wäre. Dabei ist Datensicherheit ein hohes Gut. Welches Vorgehen sich zur Sicherung der Unternehmensdaten anbietet und welche strategischen Aspekte zu beachten sind, lesen Sie im nachfolgenden Beitrag.**

**IM GLEICHEN MASSE** wie die Menge der digitalen Daten in einem Unternehmen von Jahr zu Jahr wächst, steigt auch die Notwendigkeit, den Mitarbeitern einen unterbrechungsfreien und lückenlosen Datenzugriff zu ermöglichen. Um Datenverluste nachhaltig auszuschließen, muss deshalb in jedem Unternehmen ein Konzept etabliert werden, das für Datensicherung und Ausfallsicherheit sorgt. Leider gibt es aber in der Praxis gravierende Mängel.

Dies bestätigt eine Umfrage des Netzwerks Elektronischer Geschäftsverkehr (NEG), die im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ in den Jahren 2007 bis 2009 durchgeführt wurde. Gerade im Bereich des Backups wurden teilweise erschreckende Zustände aufgezeigt:<sup>1</sup>

- Nur 47 Prozent der Unternehmen haben ihre Backup-Strategie schriftlich fixiert.

<sup>1</sup> Die vollständige Auswertung der Sicherheitsbefragung des – durch das BMWi geförderten – Begleitvorhabens „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr kann unter der Adresse <http://www.ec-net.de/sicherheit> abgerufen werden. Eine Aktualisierung der Befragung wird im Jahr 2010 durchgeführt.

- Weiterhin gaben 16 Prozent der Befragten an, ihre Speichermedien nicht an einem angemessenen Ort aufzubewahren.
- Knapp 17 Prozent sichern lediglich auf CDs/DVDs oder USB-Sticks.
- Nur jedes zweite Unternehmen testet die Sicherungskopien.
- Mehr als 40 Prozent der Befragten gaben an, die eigene IT ohne einen entsprechenden Notfallplan zu betreiben.

Derartig gravierende Zustände zeigen, dass die Sensibilisierung der Geschäftsleitung für Datensicherung nicht vorhanden ist. Dabei sollten gerade die Geschäftsführer die große Bedeutung sehen. Denn nicht nur die gesetzlich angemahnte Sorgfaltspflicht zwingt die Entscheidungsträger dazu, für das jeweilige Unternehmen angemessene Schutzmaßnahmen zu ergreifen und deren Umsetzung regelmäßig zu kontrollieren. Es ist darüber hinaus die häufig durch einen Störfall ausgelöste existenzielle Bedrohung des eigenen Unternehmens, die das Management aufrütteln und zur Bewilligung von Investitionen für die Datensicherung führen sollte

Die regelmäßige und vollständige Sicherung der Daten (= Backup) ist der grundlegendste Aspekt einer jeden Sicherheitsstrategie. Nur wenn nach einem Störfall auf die betrieblichen Daten zurückgegriffen werden kann, sind weiterführende Maßnahmen, etwa die

Bekämpfung eines Computerschädlings, überhaupt möglich. Doch das bloße Erstellen eines Backups sichert noch nicht einen störungsfreien Betrieb des Tagesgeschäfts. Sofern gewährleistet sein muss, dass selbst bei Ausfall zentraler Basis-komponenten wie einem Fileserver alle Angestellten weiterarbeiten können, so müssen diese redundant betrieben und die Daten permanent gespiegelt werden. Erst dann ist ein Ausfall reibungslos zu überwinden und tatsächlich eine hohe Ausfallsicherheit gegeben.

Natürlich sind derartige Anforderungen mit relativ hohen Investitionen bei Hardware (Server) und Infrastruktur (Netzwerk) verbunden. Diese stehen jedoch in keinem Verhältnis zu den durch einen Ausfall verursachten materiellen und immateriellen Kosten: Wenn Angestellte nicht produktiv arbeiten können oder es sogar zu Produktionsausfällen kommt, sind die Schäden erheblichen Ausmaßes. Um die eigenen Daten angemessen sichern zu können, ist eine stufenweise Vorgehensweise notwendig.

### Stufe 1: Sicherung der Daten auf dem Client-PC

In einer unternehmensweiten Backup-Strategie können nur die Daten berücksichtigt werden, die auf einem zentralen Speichermedium vorgehalten werden. Diese Vorgabe bringt es mit sich, dass dezentral erstellte Dateien (zum Beispiel auf einem Laptop)

mit einer Zentrale (in der Regel dem Fileserver) synchronisiert werden müssen. Für diesen Abgleich gibt es auf dem Markt zahlreiche Softwarelösungen – teilweise aus dem Open-Source-Bereich. Durch eine tägliche Synchronisation wird sichergestellt, dass beim Auftreten eines Störfalls der Datenverlust auf maximal 24 Stunden beschränkt werden kann. Nach einem Basisabgleich, bei dem die gesamten „eigenen Dateien“ auf den Server kopiert werden, erfolgt bei der täglichen Synchronisation lediglich der Austausch der Dateien, die sich seit dem Vortag verändert haben. Dies führt dazu, dass die Datenmenge und der damit verbundene Zeitaufwand für den Austausch auf einem erträglichen Niveau bleiben. Die Zeitintervalle zwischen den Datenabgleichen müssen je nach Situation gegebenenfalls verkürzt werden. Durch eine derartige Maßnahme verschiebt sich das Verlustrisiko von den Client-Rechnern hin zur Zentrale – dem Fileserver.

## Stufe 2: Unverzögliche Sicherung der Daten des Fileservers

Das Speichervolumen eines zentralen Fileservers liegt, in Abhängigkeit von der Branche, schon bei kleinen Unternehmen im TByte-Bereich. Um den Umgang mit einem derartigen Datenvolumen überhaupt handhabbar zu gestalten, muss eine Infrastruktur geschaffen werden, die in der Lage ist, dieses Datenvolumen zu speichern und über ein Netzwerk zu übertragen.

Es empfiehlt sich, die gleiche Hardware redundant vorzuhalten und die Inhalte nach dem Aufspielen beziehungsweise Ändern unverzüglich zu spiegeln – sprich eins zu eins zu kopieren. Dadurch kann ein sehr hohes Maß an Sicherheit gewährleistet werden. Die Grundlage dafür bilden ein ausgebautes Netzwerk sowie zwei Serverräume, die mit Netzanbindung, Stromversorgung, Klimaregelung und entsprechenden Zutrittskontrollen ausgestattet sind. Diese Form des Backups bietet auch ein hohes Maß an Ausfallsicherheit! Doch eine zusätzliche Sicherung der Daten darf auch bei dieser Vorgehensweise nicht fehlen.

## Stufe 3: Zusätzliche Sicherung der Daten des Fileservers

Die Fileserver eines Unternehmens müssen zusätzlich auf einem weiteren Speichermedium gesichert werden, um diese nachhaltig vor Ausfällen oder ungewollten Manipulationen zu schützen. In Abhängigkeit von der jeweiligen Branche müssen die Entscheidungsträger festlegen, welche Reaktionszeiten sie im Störfall vorhalten müssen, um einen etwaigen Produktionsausfall abfedern zu können. Hierzu kann entweder ein weiterer Server (so genannter Backup-Server) oder externe Speichermedien (zum Beispiel eine externe USB-Festplatte) dienen. Der Einsatz von USB-Sticks zur Speicherung wird hier vernachlässigt, da eine sichere und praktikable Umsetzung mit diesem Medium nicht gewährleistet werden kann.

Die unterschiedlichen Möglichkeiten werden im Folgenden kurz vorgestellt:

### • Sicherung auf einen weiteren Rechner

Neben der bereits beschriebenen Spiegelung (siehe Stufe 2) erfolgt eine Datensicherung auf einen weiteren – autarken – Server, der nicht ins Tagesgeschäft eingebunden ist. Diese Datensicherung geschieht nach einem zuvor festgelegten Zeitintervall, zum Beispiel alle vier Zeitstunden. Dies führt dazu, dass bei einem Totalausfall des Systems ein maximaler Datenverlust von exakt der gewählten Zeitspanne entsteht. Die Entscheidung, welche Zeitspanne gewählt wird, muss von der Geschäftsleitung auf Basis einer Risikoanalyse erfolgen. Bei der Erstellung dieses Systems ist es von entscheidender Bedeutung, dass der Backup-Server logisch und physisch getrennt vom Tagesgeschäft betrieben wird. Denn nur so kann sichergestellt werden, dass etwaige Störfälle keinen direkten Einfluss auf die Sicherung haben.

### • Sicherung auf externe Speichermedien

Sollte der Betrieb der genannten Infrastruktur als zu aufwendig eingestuft werden, muss eine Speicherung auf einem externen Speichermedium

durchgeführt werden. Dabei kann es sich entweder um Bänder, externe Festplatten oder optische Speichermedien (CD, DVD usw.) handeln. Da die Haltbarkeit von optischen Speichermedien als eher gering eingeschätzt wird, sind diese nur bedingt zu nutzen. Eine kurzfristige Verwendung wäre zwar möglich, von einer mittelfristigen Sicherung kann aber nur abgeraten werden. Gerade bei großen Datenmengen empfiehlt sich die Verwendung von Bändern. Diese haben eine hohe Lebensdauer, sind robust gegenüber externen Einflüssen und ermöglichen die Sicherung von großen Datenmengen auf nur einem Speichermedium. Sofern sich die Verantwortlichen für den Einsatz von Bändern entschließen, sollten aber zwei Bandlaufwerke angeschafft werden, weil ein Störfall im Serverraum Schaden an der Basis-Hardware erzeugen kann und dadurch ein schnelles Zurückspielen der Daten unmöglich wird.

### • Kombination der beschriebenen Vorgehensweisen

Es hat sich in der Praxis häufig gezeigt, dass eine Kombination der beschriebenen Verfahren zu einem hohen Sicherheitsniveau führt. Die Existenz eines zweiten Fileservers, auf dem die Daten gespiegelt vorgehalten werden, ermöglicht ein nahezu unterbrechungsfreies Weiterarbeiten. Die Sicherung auf einen eigenen Sicherungsserver stellt sicher, dass verlorene Daten rasch und ohne technische Modifikationen zurückgespielt werden können. Eine zusätzliche Sicherung auf ein externes Speichermedium garantiert eine mittel- bis langfristige Verfügbarkeit des Datenbestands und ermöglicht nach einem Schadensfall eine umfassende Rekonstruktion der Daten.

Es wurde bis jetzt ausschließlich auf die technische Umsetzung des Backups eingegangen. Von Bedeutung ist aber auch die Art der Sicherung. Es existieren vier grundsätzliche Möglichkeiten, die Daten zwischen Quelle- und Zielort zu transferieren:

- **Kopie:** Die zu sichernden Daten werden vom Original kopiert und auf dem Backup-Medium gesichert.
- **Normal:** Die zu sichernden Daten werden vom Original kopiert und auf dem Backup-Medium gesichert. Die gesicherten Daten werden entsprechend markiert.
- **Inkrementell:** Sichert die ausgewählten Dateien nur, wenn sie seit der letzten Sicherung erstellt oder geändert wurden.
- **Differenziell:** Sichert die ausgewählten Daten nur, wenn sie seit der letzten Sicherung erstellt oder geändert wurden. Die Dateien werden nicht als gesichert markiert.

Ein reines Kopieren der Daten ist sicherlich die einfachste Art und Weise – verbraucht aber auf den Sicherungsmedien ein hohes Speichervolumen. Die Durchführung eines inkrementellen oder differenziellen Backups reduziert die täglich zu sichernde Datenmenge erheblich, kann aber den Prozess des Rückspiels signifikant verlängern.

Bei der Auswahl der für ein Unternehmen geeigneten Vorgehensweise muss im Vorfeld gewissenhaft geprüft werden, welche Rahmenbedingungen vorherrschen und welche Prioritäten die Verantwortlichen setzen. In einer Zeit, in der die Preise für Hardware nahezu täglich sinken, sollte eine Investition in Speicherplatz nicht mehr ins Gewicht fallen.

## Strategische Aspekte der Datensicherung

Die folgenden Aspekte müssen bei einer nachhaltigen Backup-Strategie in jeden Fall Berücksichtigung finden:

- Die beiden Serverräume müssen räumlich voneinander getrennt sein, um sicherzustellen, dass die gleiche Ausfallursache nicht zeitgleich direkten Einfluss auf beide Fileserver ausübt.
- Die Backup-Medien müssen an einem sicheren Ort aufbewahrt werden. Dieser muss von der Datenquelle räumlich getrennt sein und vor direkter Feuer- und Wassereinwirkung ausreichend geschützt werden. Ebenso muss ein Diebstahl der Speichermedien in jedem Fall ausgeschlossen werden.

- Die erfolgreiche Abwicklung der Sicherungen muss regelmäßig durch punktuelle Rücksicherung der Backups geprobt und dadurch nachgewiesen werden. So spielen sich bei den Verantwortlichen die notwendigen Handgriffe ein. Zeitgleich wird die Qualität der Backups getestet.
- Zumindest eine Monatsspeicherung sollte außerhalb der Firma, zum Beispiel in einem Bankschließfach, aufbewahrt werden.
- Die erfolgreiche Durchführung der Datensicherung muss dokumentiert werden.
- Eine Verschlüsselung der Speichermedien – gerade wenn sie außerhalb des Unternehmens gelagert werden – ist eine angemessene Methode, diese vor unberechtigtem Zugriff zu schützen.
- Die Verantwortlichkeiten für die Durchführung der Datensicherung im Unternehmen müssen – zum Beispiel in Stellenbeschreibungen – dokumentiert werden. Daraus ergibt sich für die Umsetzer die Verpflichtung, für entsprechende Vertreterregelungen zu sorgen.

## Vertrauen ist gut, Kontrolle besser

Ein Datensicherungskonzept, das die hier beschriebenen Vorgaben einhält, bietet ein hohes Maß an Sicherheit. Ein hundertprozentiger Schutz kann aber nicht erreicht werden, so dass sich die Verantwortlichen immer mit einem gewissen Restrisiko konfrontiert sehen, dem nur mit einem unverhältnismäßig hohen Aufwand begegnet werden könnte.

Es gibt noch zahlreiche Möglichkeiten, die Durchführung des Backups zu verfeinern. So kann zum Beispiel durch die Verwendung eines RAID-Systems der Ausfall einer Festplatte problemlos verkraftet werden. Inwieweit die Nutzung derartiger Systeme notwendig ist, lässt sich mit der bereits angesprochenen Risikoanalyse ermitteln. Sinnvoll ist es auch, wenn das eigene Konzept von einem Dritten auf dessen Tauglichkeit hin überprüft wird. Denn nur so kann eine betriebsblinde Vorgehensweise ausgeschlossen werden.

**Kennziffer: DBM21058**

## Die Autoren



**ANDREAS GABRIEL**

arbeitet seit Juli 2000 als Forschungsassistent am Lehrstuhl für Betriebswirtschafts-

lehre und Wirtschaftsinformatik von Prof. Dr. Rainer Thome an der Julius-Maximilians-Universität Würzburg. Im Rahmen seiner Tätigkeit war er mehrere Jahre als Netzwerk- und Serveradministrator tätig und konnte bereits in dieser Zeit umfangreiche Erfahrungen im Bereich der Informationssicherheit sammeln. Seit 2003 ist er für das Mainfränkische Electronic Commerce Kompetenzzentrum (MECK) aktiv und kooperiert intensiv mit mittelständischen Unternehmen.

Seinen aktuellen Schwerpunkt bildet die Tätigkeit im Rahmen des Begleitprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG).

Im Mai 2006 absolvierte er erfolgreich die Ausbildung zum Certified Lead Auditor für die Norm ISO:IEC 27001:2005 beim Bundesamt für Sicherheit in der Informationstechnik (BSI), seit 2009 ist er betrieblicher Datenschutzbeauftragter.



**LUDWIG HABERSETZER**

ist seit 2009 wissenschaftlicher Mitarbeiter am Lehrstuhl für Betriebswirtschafts-

lehre und Wirtschaftsinformatik von Prof. Dr. R. Thome an der Julius-Maximilians-Universität Würzburg. Seine Schwerpunkte liegen in den Bereichen Geschäftsprozessmodellierung, E-Business und E-Government. In allen Bereichen war er bereits in Industrie- und Forschungsprojekten tätig. Neben seiner Forschungstätigkeit ist er an der Universität auch als Dozent in die Lehre eingebunden.

Seit 2009 ist er für das Mainfränkische Electronic Commerce Kompetenzzentrum (MECK) aktiv und berät insbesondere kleine und mittlere Unternehmen in Fragen von Online-Marketing, IT-Sicherheit und ERP-Software.