



# Feuer, Blitzschlag oder ein Einbruch: So schützen Sie Ihre Daten!

Kundendaten, Produktionsdaten oder auch die gesamte Buchhaltung stellen einen nicht zu unterschätzenden Wert für das Unternehmen dar. Jeder Unternehmer sollte sich fragen, ob und wie das Unternehmen weitergeführt werden kann, wenn zentrale Datenspeicher ausfallen. Um einen solchen Notfall zu vermeiden, sollte ein Sicherheitskonzept erstellt werden, das die Methode und den zeitlichen Rhythmus der Datensicherungen (oder auch Back-ups genannt) umfasst.

Bei einer Datensicherung werden Daten auf einen externen Datenträger kopiert, der nicht dauerhaft mit dem zu sichernden System verbunden ist. Je kritischer die zu sichernden Daten sind, desto sorgfältiger sollte auch das Sicherungsmedium gewählt werden. Für Privatanwender ist im Normalfall die Sicherung auf einem externen Festplattenlaufwerk ausreichend. Nutzer, wie Unternehmen oder Behörden, deren Daten elementar für die Aufrechterhaltung des Betriebs sind, verwenden üblicherweise RAID-Systeme (Systeme aus mehreren Speicherplatten, die die Daten redundant, d. h. mehrfach speichern) oder Bandlaufwerke zur Sicherung, da diese höhere Ausfallsicherheit beziehungsweise Langlebigkeit besitzen.

## Welche Sicherungsart ist die Richtige?

Es gibt verschiedene Konzepte zur Erstellung einer Datensicherung, die sich in der Menge der zu sichernden Daten und der Häufigkeit der Durchführung unterscheiden.

Bei einer Vollsicherung werden alle Daten eines Systems oder Datenträgers kopiert und gespeichert. Diese Sicherungsart verbraucht am meisten Systemressourcen, da die zu sichernde Datenmenge hier meist mehrere Gigabyte umfasst. Vollsicherungen werden meist in regelmäßigen Abständen (wöchentlich/monatlich) erstellt. Zur Reduzierung der zu sichernden Datenmenge, kann die Vollsicherung mit anderen Sicherungsarten kombiniert werden.

## Differenzielle Sicherung

Aufbauend auf einer vorher erstellten Vollsicherung kann die differenzielle Sicherung verwendet werden, um die Menge der zu sichernden Daten zu verringern. Dies geschieht, indem nur die hinzugekommenen und geänderten Daten seit der letzten Vollsicherung gespeichert werden. Meist wird beim Erstellen einer differenziellen Sicherung der vorhergehende Sicherungssatz verworfen, da die neue Sicherung auch dessen Daten enthält. Üblicherweise werden differenzielle Sicherungen genutzt, um die Änderungen zwischen zwei Vollsicherungen zu speichern. Bei Durchführung der nächsten Vollsicherung werden die differenziellen Sicherungssätze, die sich auf die vorhergehende Vollsicherung beziehen üblicherweise verworfen. ►



## ► Inkrementelle Sicherung

Wie die differenzielle Sicherung benötigt auch die inkrementelle Sicherung als Grundlage eine zuvor erstellte Vollsicherung. Aufbauend auf dieser speichert die inkrementelle Sicherung die geänderten oder hinzugekommenen Daten seit der letzten Vollsicherung oder der letzten inkrementellen Sicherung. Dies verringert die Menge der zu sichernden Daten, im Vergleich mit der differenziellen Sicherung, da nur noch die Änderungen zwischen zwei inkrementellen Sicherungen gespeichert werden müssen. Allerdings bedeutet dies auch, dass zur Datenwiederherstellung sowohl der Sicherungssatz aus der Vollsicherung als auch alle Datensätze aus den inkrementellen Sicherungen notwendig sind. Ebenso wie bei differenziellen Sicherungen werden die inkrementellen Sicherungssätze beim Erstellen der nächsten Vollsicherung meist verworfen.

Falls möglich, werden Systemsicherungen (Betriebssysteme und installierte Programme) und Datensicherungen (Verzeichnisse, Dateien, Datenbanken) getrennt voneinander durchgeführt. Dies erleichtert im Schadensfall die Wiederherstellung.

### Wichtige Pflicht: Die Dokumentation

Damit die Datenwiederherstellung korrekt durchgeführt werden kann, ist es notwendig den Sicherungsvorgang zu dokumentieren. Wichtige Punkte sind hierbei die Sicherungsart, das Speichermedium und der Speicherort, das Ablaufdatum der Sicherung, die verwendeten Sicherungsarten, zusammen mit der Reihenfolge, in der die Sicherungen erfolgt sind.

*Der eBusiness-Lotse Schwaben unterstützt kleine und mittlere Unternehmen (KMU) bei der Nutzung moderner moderner Informations- und Kommunikationstechnologien (IKT) und der Digitalisierung ihrer Geschäftsprozesse. Er ist Teil des Förderschwerpunkts Mittelstand-Digital, der vom Bundesministerium für Wirtschaft und Energie (BMWi) initiiert wurde, um die Entwicklung und breitenwirksame Nutzung von IKT-Anwendungen in KMU und Handwerk voranzutreiben.*

### Autor Sebastian Krämer:

Sebastian Kraemer hat 2011 seinen Master der Informatik an der Hochschule Augsburg absolviert und ist Mitarbeiter der HSASec, der Forschungsgruppe IT-Security und Forensik der Hochschule Augsburg. Seine Schwerpunkte liegen auf der Absicherung von Web-Applikationen sowie der Entwicklung sicherer Software auf Microsoft Betriebssystemen.

Im Rahmen seiner Tätigkeiten überprüft er Online-Systeme auf deren Sicherheit, hält Schulungen und Vorträge, führt Pen-Testing/Security Audits durch und bearbeitet verschiedene Projekte mit unmittelbarem Sicherheitsbezug.

In Zusammenarbeit mit:



**Hochschule Augsburg** University of Applied Sciences

### Impressum

#### Herausgeber:

eBusiness-Lotse Schwaben  
Geschäftsstelle im aiti-Park  
IT-Gründerzentrum GmbH  
Werner-von-Siemens-Str. 6  
86159 Augsburg

#### Redaktion:

eBusiness-Lotse Schwaben  
Andrea Henkel  
Werner-von-Siemens-Str. 6  
86159 Augsburg  
eMail: Team@eBusinessLotse-Schwaben.de  
Tel.: +49 (0) 821 450433-106  
www.eBusinessLotse-Schwaben.de

#### Gestaltung und Produktion:

Technik & Grafik  
Kerstin Meister  
eMail: kerstin.meister@technikundgrafik.de  
Tel.: +49 (0) 8238 958338