



**10) Wann haben Sie zuletzt eine komplette Datenrück-  
sicherung durchgeführt? Ist es gelungen, ein komplet-  
tes System von Null weg auf neuer Hardware wieder-  
herzustellen?**

Bedenken Sie: im Desasterfall verlieren Sie eventuell auch die bestehende Hardware (z.B. bei Brand). Daher sollten Rücksicherungstests am Besten gleich auf anderer Hardware erfolgen. Die für solche Tests benötigten zusätzlichen Systeme können im Normalbetrieb zum Testen von Systempatches verwendet werden und im Katastrophenfall als Ersatzhardware dienen.

Eine Wiederherstellung muss innerhalb eines festgelegten Zeitraums durchgeführt werden können. Kontrollieren Sie die rückgesicherten Daten auf Richtigkeit. Dokumentieren Sie die Vorgehensweise ausreichend. Dies kann auch schon einen Mehrwert bei der regelmäßigen Finanz/Wirtschaftsprüfung darstellen.

Sollten Sie auch nur eine der 10 Fragen mit NEIN beantworten: tun Sie etwas!

**Reden Sie mit einem Sicherheitsexperten  
Ihres Vertrauens!**

**Daten sind das Herzstück in jedem Unternehmen, die IT ist die Lebensader für das operative Geschäft des Betriebs.**

Die Verfügbarkeit Ihrer Informationen ist durch Schadprogramme, aber auch durch einfache technische Gebrechen wie Hardwareausfälle oder Wasserschäden jederzeit gefährdet.

Manche Verluste kann man verschmerzen, im Allgemeinen zeigt sich aber, dass die Betriebsbereitschaft eines Unternehmens durch einen Ausfall der IT, der länger als einen Tag dauert, gefährdet ist. Der Verlust von Daten kann damit existenzbedrohend sein.

Die folgenden Tipps der Experts Group IT-Security des Fachverbandes Unternehmensberatung und IT zeigen Ihnen, wie Sie Ihre Informationen erfolgreich sichern und für die Zukunft nachhaltig vorsorgen können.

Ihr Alfred Harl, MBA CMC  
Obmann des Fachverbandes Unternehmensberatung und IT



**10 Fragen zur Datensicherung.**

**So verhindern Sie Datenverlust.**

**Sicher gut  
beraten.**



**IT-Security Experts**  
[www.itsecurityexperts.at](http://www.itsecurityexperts.at)



**IT-Security Experts**  
[www.itsecurityexperts.at](http://www.itsecurityexperts.at)

**Impressum**

Fachverband Unternehmensberatung und Informationstechnologie  
1045 Wien | Wiedner Hauptstraße 63  
<http://www.itsecurityexperts.at>  
e-Mail: [office@itsecurityexperts.at](mailto:office@itsecurityexperts.at)  
Tel: 05 90900-3540  
Fotos: Martin Prager

Jede Änderung Ihrer Systemlandschaft (WLAN, Notebooks, etc...) birgt neue Sicherheitsrisiken in sich.  
**Fragen Sie Ihren Sicherheitsexperten!**

## 10 Fragen an die Geschäftsleitung zur Datensicherung

### 1) Haben Sie einen präzisen Überblick darüber, welche Daten wo gespeichert sind und werden alle, z.B. auch die Daten Ihrer „Office-Anwendung“, ausreichend gesichert?

Unterschiedliche Datenklassen erfordern unterschiedliche Strategien. Wichtige Daten sollen häufiger gesichert werden als weniger wichtige. Bitte beachten Sie, dass unternehmensbezogene Daten auf einem zentralen Dateiserver liegen müssen, damit diese Dateien in die Sicherungsroutinen dieses Servers eingebunden werden können. Berücksichtigen Sie auch, Ihre E-Mail Daten und Archive entsprechend zu sichern.

### 2) Haben Sie eine klar definierte und dokumentierte Auslagerungsstrategie für die Datensicherung, um zu verhindern, dass bei einem Vorfall im Serverraum auch die Sicherungen vernichtet werden?

Die Sicherungsmedien müssen ausreichend weit entfernt von einander aufbewahrt werden, aber im Bedarfsfall schnell genug greifbar sein. Bei der Aufbewahrung ist der physische Schutz der Medien zu berücksichtigen. Bedenken Sie den Eintritt von eventuellen Naturkatastrophen, Diebstahl oder unberechtigtem Zugriff. Die Verschlüsselung von Datensicherungsmedien sollte auf jeden Fall in Erwägung gezogen werden (auch bei Entsorgung und Austausch der Medien relevant).

### 3) Haben Sie berücksichtigt, wie schnell sich die jeweiligen Daten verändern?

Manche Daten müssen häufiger gesichert werden als andere. Was sich öfters ändert, muss häufiger gesichert werden. Bedenken Sie auch, dass sich eventuell nicht alle Daten per Hand rekonstruieren lassen. Ein regelmäßiges

und kritisches Hinterfragen der eingesetzten Sicherungsstrategie und Sicherungslösung sollte zumindest jährlich erfolgen. Wichtig ist, dass diese mit den sich ständig veränderten Businessanforderungen Hand in Hand gehen.

### 4) Kennen Sie die Aufbewahrungsfristen und die Löschungsverpflichtungen und wie Sie diese einhalten?

Eine Datensicherung ersetzt nicht unbedingt eine Archivierung Ihrer Daten und umgekehrt.

### 5) Nutzen Sie die Vorteile einer separaten Archivierung?

Zur Nachvollziehbarkeit und langfristigen Aufbewahrung eignet sich eine elektronische Archivlösung besser als die herkömmliche Archivierung in Papierform. Die elektronische Archivlösung kann mitunter auch Betriebskosten reduzieren. Bedenken Sie auch die Sicherung der Daten im Archiv.

### 6) Gibt es klare Anweisungen zur Durchführung von Datensicherungen und sind Ihre MitarbeiterInnen entsprechend geschult?

Ohne Sicherstellung der organisatorischen Rahmenbedingungen sowie Durchführung klarer Vorgaben und die entsprechenden Kenntnisse der MitarbeiterInnen ist die Datensicherung nicht sichergestellt. Auf das fachliche Know-how zu dem Thema sollte ein Augenmerk gelegt werden.

### 7) Wissen Sie, dass hochverfügbare Systeme und RAID keine Datensicherung(en) ersetzen?

Ein Datenarchiv, eine Plattenspiegelung oder parallel betriebene Datenbanken ersetzen nicht eine regelmäßige Datensicherung, da durch den Abgleich mehrerer Platten auch potentielle Fehler abgeglichen werden. Ebenso werden Anwenderfehler und logische Fehler dadurch nicht berücksichtigt.

### 8) Entsprechen die für Backup und Archivierung verwendeten Systeme im Hinblick auf Software, Hardware und Medien allen Anforderungen Ihres Unternehmens?

Die Software für Backup und Archivierung muss die notwendige Funktionalität aufweisen (z.B. Zeitsteuerung, Verifikation, Logging, Fehlerhinweise). Die Hardware ist den Bedürfnissen entsprechend auszuwählen (u.a. Speichertyp, Kapazität, Verfügbarkeit). Die Medien (CD-ROM, DVD, Wechseldatenplatte, DATBandkassette) müssen den Anforderungen im Hinblick auf Datensicherheit und Langzeitstabilität entsprechen und regelmäßig erneuert werden.

Ebenso gibt es Möglichkeiten, die Datensicherung auszulagern (z.B. Cloud). Bei der Auslagerung an externe Provider gilt es auch, die rechtlichen Aspekte und Security-Themen zu berücksichtigen.

### 9) Wissen Sie, wie Sie Ihre Daten zeitsparend sichern und rüchsichern können?

Wissen Sie, dass Datenbanken spezielle Programme benötigen, um gesichert werden zu können?

Datensicherungen werden üblicherweise unterteilt in vollständige, differenzielle und inkrementelle Sicherungen. Sicherungspläne wenden einen Mix der Methoden zur effizienten Nutzung von Zeit und Speichermedien an.

Bewährt hat sich ein Backupkonzept über mehrere Generationen, wobei die Backupdaten zyklisch überschrieben werden. Das Generationenprinzip, auch Großvater-Vater-Sohn-Prinzip genannt, stellt sicher, dass immer mehrere Sicherungen in verschiedenen zeitlichen Abstufungen (Großvater, Vater, Sohn) vorhanden sind, um verschiedene Versionen für eine mögliche Wiederherstellung zur Verfügung zu stellen.