

Daten? Aber sicher!

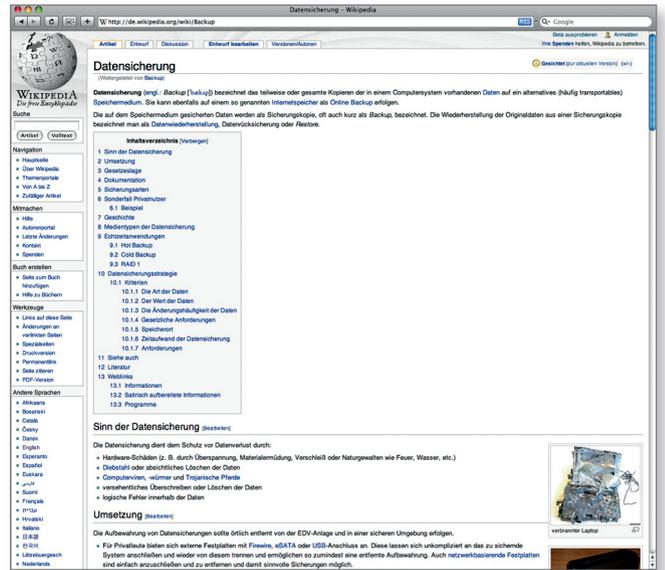
Datensicherung als Aufgabe und Herausforderung

Kaum jemand hätte sich vor wenigen Jahren vorstellen können wieviel Daten beinahe jeder heute verwaltet. Patientendaten, Korrespondenz, Dokumente, Bilder, Musik, Filme, alles liegt heute als Daten vor. Und dabei ist nur eines sicher: es wird immer mehr.

Oft gerät dabei aus dem Blickfeld, dass wir zunehmend von diesen Daten abhängig sind. Gehen sie verloren, dann kann das nicht nur unsere Arbeit beeinträchtigen, es kann auch sehr teuer werden.

Daher möchte ich im Folgenden eine Einführung zur Datensicherung geben. Ausdrücklich ist diese auch als Anregung und Erinnerung gemeint, die eigene (Datensicherungs-)Praxis zu überprüfen und zu aktualisieren.

Lesenswerte Grundlagen zur Datensicherung finden sich in der Wikipedia <http://de.wikipedia.org/wiki/Backup>



Grundregeln der Datensicherung

1. Automatisierung

Nur eine regelmäßige Sicherung ist eine gute Sicherung. Um sich diese Aufgabe zu erleichtern lohnt es sich, eine Automatisierung einzurichten. Eine Frage ist dabei zu klären:

Wieviel Datenverlust (in Stunden oder Tagen) können Sie im Notfall verschmerzen? Können Sie beispielsweise die Daten eines Tages verschmerzen, so ist eine tägliche Sicherung ausreichend. Diese kann automatisch nachts laufen, um den Arbeitsablauf nicht zu stören.

2. Mehrstufige Sicherung

Verschiedene Faktoren und Angreifer bedrohen Ihre Daten. Ihre Einwirkung kann manchmal erst nach einiger Zeit erkannt werden. Daher ist es wichtig sowohl aktuelle Sicherungen zum Beispiel von gestern und vorgestern als auch eine Sicherung von letzter und vorletzter Woche zu haben.

3. Restore testen

Alle seriösen Backup-Software-Hersteller empfehlen den Test des Restore-Prozesses ausdrücklich. Dass sich darin alle einig sind, hängt damit zusammen, dass sie gerne zufriedene Kunden hätten. Oft wird nämlich nach Kauf und Einrichtung blind auf die Sicherung ver-

traut. Erst im Notfall zeigt sich dann, ob, wie und was gesichert wurde und ob Ihre Vorstellung einer Datenwiederherstellung realistisch war. Testen Sie den Restore-Vorgang und simulieren Sie den Notfall. Nur so können Sie erkennen, ob Sie im Falle eines Falles tatsächlich gewappnet sind.

4. Vollständigkeit für Einsatz-Zweck prüfen

Welche Daten eine Arbeitsumgebung ausmachen ist höchst unterschiedlich. Daher können hier nur Hinweise gegeben werden. Oft wird vergessen für die Arbeitsumgebung nötige Datenbereiche einzubeziehen. Ein Beispiel hierfür sind Konfigurations- oder Voreinstellungsdateien. Sie bilden manchmal die Grundlage für einen ganzen Arbeitsablauf. Erstellen Sie eine Liste mit Verzeichnissen und Dateien, die gesichert werden müssen. Denken Sie an E-Mail und Bilddaten, Buchhaltung, Adressen. Beobachten Sie Ihr Nutzungsverhalten und notieren Sie eine Zeit lang mit, welche Datei-Kategorien Sie benutzen und wo diese abgelegt ist. Es sind mehr als sie denken!

5. Ausfall und Fehlbedienung einkalkulieren

Menschen machen Fehler. Maschinen können versagen. Auch Infrastruktur wie Strom und Internet(!) unterliegt diesen Gesetzen. Mobile Geräte wie Laptops können gestohlen werden oder verloren gehen. Daher ist es wichtig, Toleranzen einzuplanen. Besonders die mehrstufige Sicherung (siehe unter 2.) kann hier die Rettung bedeuten, wenn durch Fehlbedienung oder technischen Ausfall eine Sicherung zerstört wird. Egal worauf Sie sichern, sorgen Sie für eine Rotation der Sicherungsmedien.

6. Auslagern von Sicherungen

Daten können auch bei ganz banalen Missgeschicken wie Wasserschaden, Einbruch, Diebstahl, Blitzschlag, Überspannung usw. verloren gehen. Befindet sich die Sicherung und die Originaldaten im gleichen Raum, so sind dann meist beide in Mitleidenschaft gezogen. Schlimmstenfalls sind alle Daten verloren. Sorgen Sie für eine regelmäßige Auslagerung Ihrer Sicherung. Am einfachsten nimmt man ein Sicherungsmedium mit nach Hause und tauscht

BSI: B 1 Inhaltsverzeichnis Schicht 1 – IT-Grundschutz-Kataloge – 10. EL Stand 2008

https://www.bsi.bund.de/cln_136/ContentBSI/grundschutz/kataloge/baust/b01/b01004.html

das BSI | Themen | Aktuelles | Presse | Publikationen

IT-Grundschutz-Kataloge

Startseite IT-Grundschutz
Inhalt
Allgemeines
Übersichtliche Aspekte
Infrastruktur
IT-Systeme
Netze
Anwendungen
Gefährdungskataloge
Maßnahmenkataloge
Richtlinien
Glossar
Index A-Z
Hilfsmittel
Servicequellen
FAQ
Registrierung / Newsletter
Download
Kontakt

Suche Suchbegriff eingeben

Stichtage | Themen | IT-Grundschutz-Kataloge | Inhalt | Bausteine | Überordnete Aspekte | B 1.4 Datensicherungskonzept

B 1.4 Datensicherungskonzept

Beschreibung

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

Die Konzeption einer angemessenen und funktionsstüchtigen Datensicherung bedarf allerdings aufgrund der Komplexität einer geordneten Vorgehensweise. In diesem Baustein wird ein Weg beschrieben, wie für ein IT-System ein Datensicherungskonzept erstellt werden kann.

Gefährdungslage

Für die mittels eines Datensicherungskonzepts zu schützenden Daten wird für den IT-Grundschutz folgende typische Gefährdung angenommen:

Technisches Versagen:

-	M 6.13	Verlust gespeicherter Daten
---	--------	-----------------------------

Maßnahmenempfehlungen

Um den betrachteten IT-Verband abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um eine effektive Datensicherung einzurichten, sind eine Reihe von Schritten zu durchlaufen. Diese sind in der Maßnahme **M 6.33 Entwicklung eines Datensicherungskonzepts** beschrieben und werden durch die dort aufgeführten Maßnahmen erläutert. Dabei sollte mit der Umsetzung der Maßnahme **M 6.33** begonnen werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Datensicherungskonzept" vorgestellt, das vor allem für größere IT-Systeme oder IT-Systeme mit großem Datenvolumen sinnvoll ist. Die Bearbeitung der Maßnahmen sollte in der angegebenen Reihenfolge geschehen, um systematisch ein Datensicherungskonzept zu erarbeiten.

Planung und Konzeption

-	M 6.33	(B)	Entwicklung eines Datensicherungskonzepts
-	M 6.34	(B)	Erhebung der Einflussfaktoren der Datensicherung
-	M 6.35	(B)	Festlegung der Verfahrensweise für die Datensicherung
-	M 6.36	(A)	Festlegung des Minimaldatensicherungskonzepts

Beschaffung

-	M 2.132	(A)	Beschaffung eines geeigneten Datensicherungssystems
---	---------	-----	---

Umsetzung

-	M 2.41	(A)	Verpflichtung der Mitarbeiter zur Datensicherung
-	M 6.21	(C)	Sicherungskopie der eingesetzten Software
-	M 6.32	(A)	Dokumentation der Datensicherung

Richtlinien zur Datensicherung und Datensicherheit bietet das zuständige Bundesamt: [www.bsi.bund.de](http://www.bsi.bund.de/www.bsi.bund.de/cln_136/ContentBSI/grundschutz/kataloge/baust/b01/b01004.html)

es regelmäßig aus. Je nach Datenmenge und Anforderung eignen sich dafür sowohl Bandkassetten wie auch externe Festplatten.

7. Bestimmen Sie den Wert Ihrer Daten

Da Datensicherung Geld kostet, ist es sinnvoll sich über den Wert der damit gesicherten Daten Gedanken zu machen. Folgende Fragen geben Ihnen einen Anhalt, um die nötige Investition richtig einzuschätzen.

Was kostet die Wiederherstellung Ihrer Daten?

Was kostet eine Stunde/ein Tag, in dem Ihre Daten nicht zur Verfügung stehen?

Wieviel Mehraufwand entsteht durch Ausfall?

Wie lange dauert der (geplante und getestete) Wiederherstellungsprozess?

8. Nutzen Sie professionelle Software

Selbstverständlich sollte es sein, seine Daten entsprechend ihrem Wert nur einer professionellen Sicherungssoftware anzuvertrauen. Software, die als kostenlose Dreingabe beispielsweise mit Festplatten mitgeliefert wird, ist dafür kaum geeignet.

Dabei noch eine Richtschnur zum Schluss: Richten Sie alle Abläufe so einfach ein, dass Sie sie auch tatsächlich einhalten und Ihre Daten sichern!

Hinweis:

In den vergangenen beiden Folgen wurde auf die mediengerechte und effektive Nutzung von Informationen hingewiesen. Das lässt sich auch auf diese Kolumne anwenden, die sowohl gedruckt als auch als PDF-Dokument erscheint. Nutzen Sie die Papierversion als Anregung und surfen Sie die Links aus dem PDF-Dokument an, wo sie eingebettet sind und somit auf Klick zur Verfügung stehen.

Dr. Marc M. Batschkus, Arzt, Medizinische Informatik, Spezialist für eHealth, eLearning & Mac OS X, Steinstraße 40, 81667 München, E-Mail: mail@batschkus.de

Wer es genau wissen will, kann sich bei der Sicherung an Unternehmensstrategien orientieren: www.tecchannel.de/storage/backup/2020371/ratgeber_backup_restore_disaster_recovery/index3.html

Ratgeber: Backup und Restore – Disaster Recovery in Unternehmen für ein Backup- und Restore-System | TecChannel.de

Monstag, 07.09.2009

Suchbegriff hier eingeben

TECCHANNEL IT EXPERTS INSIDE

HOME | SICHERHEIT | NETZWERK | SERVERS | STORAGE | PC-MOBIL | KOMMUNIKATION | WERTTECHNIK | KARRIERE | TECCOMMUNITY

Übersicht | News | Komponenten | NAS | SAN | Backup | Management | Tools | Extra | 2,5-Zoll-Festplatten | SSD | Forum

STORAGE / BACKUP > weitere Artikel anzeigen

Vom 03.08.2009

Disaster Recovery in Unternehmen

Ratgeber: Backup und Restore

Gründe und Lösungen für ein Backup- und Restore-System

Bevor man sich mit der Implementation eines Backup- und Restore-Systems auseinandersetzt, muss man sich über die Gründe und Ziele einer solchen Lösung Gedanken machen. Möchte man Daten im Sinne von „kurzfristiger“ Absicherung gegen Datenverlust sichern oder ist man zum Beispiel durch gesetzliche Vorgaben aufgefordert, Daten, die kaum noch in Benutzung sind, über einen längeren Zeitraum vorzuhalten? Oftmals wird auch „nur“ über das Verschieben von Daten auf kostengünstigere Medien nachgedacht. Handelt es sich im ersten Fall klar um eine „konventionelle“ Backup- und Restore-Lösung, zielt das Aufbewahren von Daten über einen längeren Zeitraum auf eine Archivierung ab.

Im Unterschied zum herkömmlichen Backup werden bei einer Archivierung Daten, die nicht oder kaum noch im Online-Zugriff benötigt werden, auf dem Quellsystem gelöscht. Zum einen werden so die gesetzlichen Vorgaben erfüllt, zum anderen lassen sich Kosten einsparen, da sich die Daten nach der Archivierung auf kostengünstigeren Medien (in der Regel Bänder) befinden. Die archivierten Daten sollten sich, falls es sich bei dem Medium um Tapes handelt, dupliziert auf zwei Bändern befinden (Coppypol), um einen Datenverlust durch Bandfehler auszuschließen.

Auf der nächsten Seite: Integrierte Hierarchische-Storage-Management-Lösung

< Vorangehe Seite Seite 3 von 6 Nächste Seite >

Inhalt dieses Artikels

- > Ratgeber: Backup und Restore
- > Grundlegende Backup- und Restore-Aspekte
- > Gründe und Lösungen für ein Backup- und Restore-System
- > Integrierte Hierarchische-Storage-Management-Lösung
- > Rechenzentrum oder verteilte Lokationen?
- > Tape-Lösung – die bessere Alternative
- > Backup und Restore in der Praxis
- > Wege zum erfolgreichen Backup- und Recovery-Management

Mehr zum Thema: Storage, Backup, Restore, Disaster Recovery

Live-Berater: TecChannel Experten-Netzwerk

Links zum Artikel

AUTOR

Stephan Schorn
Der Autor Stephan Schorn ist Teamleiter in der IBM Deutschland GmbH und innerhalb des European Storage Competence and Briefing Center (ESCC) verantwortlich für Backup und Restore Lösungen für Outsourcing Kunden in Deutschland.

ARTIKEL-RANKING

★★★★★ Gelesene Seiten.
★★★★★ Dieser Artikel wurde 11 mal bewertet. Zum Bewerten über die Sterne fahren.

ARTIKEL-PDF / IT-EBOOK

- > Diesen Artikel als PDF-Datei
- > IT-eBook zusammenstellen
- Aktueller Inhalt: 0 Artikel 0 News
- > Diesen Artikel hinzufügen
- > IT-eBook öffnen

STELLENANGEBOTE IM BEREICH STORAGE

- > IT-Spezialisten (m/w) Engineering-Release-Testinformatik
FERCHAU Engineering GmbH, München
- > Senior Windows Expert (m/w) - Ihre berufliche Zukunft bei einem expandierenden IT-Beratungsbüro
personal total Heilbronn - DK, Personalmanagement GmbH, Metzingen Rhein-Neckar
- > Key Account Manager Lösungsvertrieb (w/m)
Claranet GmbH, München

Weitere Stellenangebote: [Nur Bereich Storage](#)

Suchbegriff Ort/PLZ Umkreis Suchen

WHITEPAPER

- > Netzwerksicherheit: Outsourcing von IT-Sicherheitsdienstleistungen
- > ROI steigern: Modernisierung von IT Systemen mit automatisierten Tools
- > Datenmanagement: Data Services steigern den Return on