

Führungs-Akademie

Datensicherungskonzept

Stand: Juli 2013

	Erstellt	Geprüft und Freigegeben
am:		
von:		
Unterschrift		

Inhaltsverzeichnis

A) Grundlagen

1 Einleitung

Die Informationstechnologie ist für die heutigen Arbeits- und Geschäftsprozesse – unabhängig ob es sich dabei um Unternehmen, Firmen, Verwaltungen oder (Sport-)Organisationen handelt –mittlerweile unverzichtbar geworden. Die Entwicklung der zugrunde liegenden Technologien schreitet mit rasantem Tempo voran. In vielen Organisationen muss sich die IT-Infrastruktur flexibel und spontan an sich ständig ändernde Anforderungen der Geschäftsprozesse anpassen und den notwendigen Rahmenbedingungen schaffen.

Bei diesem ständigen Wachstum werden Sicherheitsaspekte oftmals vernachlässigt. Hinzu kommt, dass der „IT-Fuhrpark" trotz größter Standardisierungsbestrebungen immer umfangreicher und vielfältiger wird.

Für Unternehmen ebenso wie für Organisationen ist es dennoch von hoher Priorität, die ausgezeichneten Chancen der Informations- und Kommunikationstechnologie zu nutzen und ihre Risiken so gering wie möglich zu halten. Chancen zu erkennen, zu nutzen und dabei auch Risiken einzugehen, ist der Kern unternehmerischen Handelns überhaupt. Spektakuläre Unternehmenskrisen zu Beginn der Neunzigerjahre haben jedoch dazu geführt, dass die Betrachtung der Risiken wieder stärker in den Vordergrund gerückt ist. Begriffe wie „Corporate Governance", „IT-Sicherheitsmanagement" und „Risiko-Controlling" sind dabei in aller Munde.

In diesem Zusammenhang ist auch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) zu sehen, das in Deutschland am 1. Mai 1998 in Kraft getreten ist. Das KonTraG fordert unter anderem in einem neu formulierten § 91 Abs. 2 AktG die Einrichtung eines Risikomanagements. Wörtlich spricht der Gesetzgeber dabei von einem so genannten „Überwachungssystem", das dazu beitragen soll, „den Fortbestand der Gesellschaft gefährdenden Entwicklungen" frühzeitig aufzuzeigen. Ein Teilaspekt, der dabei zutage tritt, ist , dass der geschäftliche oder gesellschaftliche Erfolg eines Unternehmens bzw. einer Organisation in zunehmendem Maße von einer einwandfrei funktionierenden IT–Infrastruktur abhängt – zumal diese durch die starke Penetration der IT in den Geschäftsprozessen den Fortbestand eines Unternehmens beeinflusst.

Dabei spielt ein entsprechend etabliertes Datensicherungskonzept eine erhebliche Rolle, zumal Informationen und Daten einen unabdingbaren Produktionsfaktor jedes Unternehmens darstellen.

Wichtig zu beachten ist dabei, dass ein Datensicherungskonzept lediglich einen Teilbereich des Themas „IT-Sicherheit" darstellt. Notwendigerweise ist IT-Sicherheit ganzheitlich zu betrachten. Dabei bezeichnet IT-Sicherheit einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Gefährdungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind. IT-Sicherheit ist also der Zustand, in dem die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

2 Gefährdungslage

Der Verlust von Daten kann erhebliche Auswirkungen auf die Geschäftstätigkeit haben. Sind Anwendungsdaten oder Kundenstammdaten verloren oder verfälscht, kann dies die Existenz eines Organisation bedrohen.

Darüber hinaus existieren gesetzlich verpflichtende Regelungen (Handels- und Steuerrecht etc.), die einzuhalten sind. So schreiben z. B. die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) Datensicherungsmaßnahmen vor, „die Risiken für die gesicherten Programme / Datenbestände hinsichtlich Unauffindbarkeit, Vernichtung und Diebstahl" vermeiden.

Dabei können die Gründe für den Verlust gespeicherter Daten vielfältiger Art sein, wie z. B.

- Zerstörung von Datenträgern durch höhere Gewalt wie z. B. Feuer,
- versehentliches Löschen oder Überschreiben von Dateien,
- vorsätzliches oder versehentliches Setzen von Löschmarkierungen in Archivsystemen,
- fehlerhafte Datenträger,
- unkontrollierte Veränderungen gespeicherter Daten,
- Datenzerstörung durch Computerviren.

2.1 Zielsetzung

Ein kompletter Ausschluss der Risiken ist nahezu unmöglich, sodass Maßnahmen ergriffen werden müssen, die die Folgen eines Datenverlusts mindern. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wieder aufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

Von der Datensicherung zu unterscheiden ist die Archivierung von Daten. Darüber hinaus sollte ein Notfallvorsorgekonzept existieren, in dem Verhaltensregeln für den Notfall zusammengestellt sind.

2.2 Definitionen - Daten

Nachfolgend werden die verschiedenen Datenarten kurz dargestellt, die von Relevanz sind.

Anwendungsdaten

Anwendungsdaten sind Dateien mit geschäftsbezogenen Inhalten. Dazu gehören u.a. Textdateien, E-Mails, Datenbanken etc.

Systemdaten

Systemdaten sind Dateien, die vom Betriebssystem oder Anwendungsprogrammen aus technischen Gründen verwaltet werden.

Protokolldaten

Aktionen von IT-Benutzern oder IT-Systemen werden teilweise zur besseren Nachvollziehbarkeit protokolliert. Daten aus der Protokollierung der Netz- und Zugriffsaktivitäten sind in der Regel auf den Servern hinterlegt.

Software

Hierbei handelt es sich neben System- und systemnaher Software auch um Anwendungssoftware.

2.3 Datensicherungsarten

Die Wahl der Datensicherungsart ist abhängig von verschiedenen Einflussfaktoren.

Datenspiegelung

Die Daten werden redundant und zeitgleich auf verschiedenen Datenträgern gespeichert.

BITTE BEACHTEN: Diese Art der Datensicherung ist nur für die Systeme zu wählen, bei denen der Speicherausfall ohne Zeitverlust kompensiert werden soll, da durch die doppelte Auslegung der Datenträger (z. B. Festplatten) und durch die notwendige Steuerungssoftware hohe Kosten entstehen.

Zu beachten gilt, dass dies keine vollwertige Datensicherung darstellt, sondern lediglich einen Schutz gegen den Datenverlust durch Hardwaredefekte. Dem Datenverlust z. B. durch versehentliches Löschen oder dem Integritätsverlust durch unkontrollierte Datenänderungen kann dadurch nicht begegnet werden, da der Schaden auf beiden Speichermedien gleichermaßen auftritt.

Volldatensicherung

Bei der Volldatensicherung werden sämtliche zu sichernden Dateien zu einem bestimmten Zeitpunkt auf zusätzlichen Datenträgern gespeichert.

Der Zeitraum zwischen zwei Sicherungen sollte nicht zu lang gewählt werden. Eine Volldatensicherung hat zwar einen hohen Speicherbedarf, ermöglicht aber ein schnelles und einfaches Wiedereinspielen (Rekonstruktion) der Dateien.

Inkrementelle Datensicherung

Im Gegensatz zur Volldatensicherung werden hierbei nur die Dateien gesichert, die sich gegenüber der letzten Datensicherung geändert haben – entweder seit der letzten inkrementellen oder der letzten Volldatensicherung. Da die inkrementelle Datensicherung auf einer Volldatensicherung basiert, muss in periodischen Abständen dennoch eine Vollsicherung erstellt werden.

Die inkrementelle Datensicherung spart Speicherplatz und läuft vom zeitlichen Faktor wesentlich schneller als eine Volldatensicherung. Für die Rekonstruierung der Daten ergibt sich aber ein höherer Zeitbedarf, da die Dateien aus Datensicherungen verschiedener Zeitpunkte extrahiert werden müssen. Bei der Rekonstruierung wird die letzte Volldatensicherung als Grundlage genommen, die um die in der Zwischenzeit geänderten Dateien aus den inkrementellen Sicherungen ergänzt wird.

Differenzielle Datensicherung

Anders als bei der inkrementellen Datensicherung werden alle Dateien gesichert, die sich gegenüber der letzten Volldatensicherung geändert haben.

Eine Differenzielle Datensicherung benötigt im Vergleich zur inkrementellen mehr Speicherplatz und dauert aufgrund des höheren Datenvolumens länger. Die Dateien lassen sich jedoch einfacher und schneller rekonstruieren. Für die Rekonstruierung der Daten reichen die letzte Volldatensicherung sowie die aktuellste differenzielle Sicherung.

2.4 Datensicherungsmedium

Auch die Wahl des Datensicherungsmediums ist abhängig von verschiedenen Einflussfaktoren. Hierbei ist insbesondere das zu erwartende Datenvolumen von Bedeutung. Nachfolgend werden die gängigsten Datenträger aufgezeigt.

Wechseldatenträger

Optische Datenträger

Hierunter fallen CD- und DVD-Medien. Die DVD unterscheidet sich von der CD im wesentlich nur im erheblich größeren Speichervolumen.

Diese eignen sich insbesondere für die Sicherung ganzer Festplatteninhalte, wenngleich selbst bei Datenkompression mehrere Datenträger zur Sicherung einer Festplatte notwendig sein können. Des Weiteren eignet sich dieses Medium zur Sicherung von Software. Vorteilhaft sind die geringen Kosten des Mediums und der geringe Platzbedarf zur Lagerung.

Bänder/Streamer Tapes

Vorteilhaft an Magnetbändern/Streamer Tapes ist die höhere Speicherkapazität gegenüber CD oder DVD bei gleichzeitig geringeren Kosten gegenüber Festplatten. Nachteilig sind die geringe Datensicherungsgeschwindigkeit und der nicht wahlfreie Zugriff auf die Daten. Magnetbänder/Streamer Tapes haben eine sehr hohe Lebensdauer. Daher sollen Streamer Tapes insbesondere bei der Speicherung großer Datenvolumen und bei der Speicherung von Daten über einen langen Zeitraum eingesetzt werden.

Festplatte

Festplatten haben eine hohe Datenkapazität. Nachteilig ist die Gefahr eines Hardware-/Festplattendefekts und die vergleichsweise geringe Lebensdauer. Die Festplattensicherung ist für die Datenspiegelung notwendig. Festplatten eignen sich für Sicherungen mit großen Datenvolumen und sind bei der Notwendigkeit einer schnellen Datenrekonstruierung zu nutzen.

2.5 Verfahrensweise für die Datensicherung

Im nachfolgenden Teil B des Dokuments (Dokumentierte Verfahrensweise für die Datensicherung (je Server-System) stellen wir Ihnen insgesamt 6 Tabellen zur Verfügung, mit denen Sie die Verfahren zur Datensicherung und die Verantwortlichkeiten dokumentieren können.

Auch wenn jede Organisation ihr eigenes IT-System mit einer unterschiedlichen Anzahl von Servern so sind die zu beschreibenden Verfahren doch (weitgehend) identisch. Zur Kennzeichnung der Einzelheiten der Server haben wir vor jeder Tabelle zwei Textfelder angelegt.

Sollten Sie mehr als 6 Server im Einsatz haben, können Sie die Liste durch Copy & Paste Ihren Bedingungen anpassen.

Dokumentierte Verfahrensweise für die Datensicherung (je Server-System)

1 Server 1 / Mailserver

IT-System: Klicken Sie hier, um Text einzugeben.

Aufgabe	Beschreibung Verfahrensweise
Verantwortlicher für die Datensicherung	
Art der Datensicherung	
Umfang der Datensicherung	
Datensicherungs-Hardware	
Datensicherungs-Software (inkl. Version und Build)	
Datensicherungs-Benutzer	
Ist das Kennwort für Datensicherungs-Benutzer dokumentiert?	
Häufigkeit und Zeitpunkte der Sicherung	
Anzahl der Generationen	
Vorgehensweise und Speichermedium	
Aufbewahrungsort	
Transportmodalitäten	
Regelmäßige Kontrolle der Datensicherung	
Notfallpläne zur System-/ Datenrekonstruktion	
Regelmäßige Wartungsarbeiten / Reinigung	
Service Level Agreement für Datensicherungs-Software	
Service Level Agreement für Datensicherungs-Hardware	
Dokumentation der Back-up-Software-Einrichtung?	
frei für ergänzenden Eintrag	

	Erstellt	Geprüft und Freigegeben
am:		
von:		
Unterschrift		

2 Server x 2 **Klicken Sie hier, um Text einzugeben.**

IT-System: Klicken Sie hier, um Text einzugeben.

Aufgabe	Beschreibung Verfahrensweise
Verantwortlicher für die Datensicherung	
Art der Datensicherung	
Umfang der Datensicherung	
Datensicherungs-Hardware	
Datensicherungs-Software (inkl. Version und Build)	
Datensicherungs-Benutzer	
Ist das Kennwort für Datensicherungs-Benutzer dokumentiert?	
Häufigkeit und Zeitpunkte der Sicherung	
Anzahl der Generationen	
Vorgehensweise und Speichermedium	
Aufbewahrungsort	
Transportmodalitäten	
Regelmäßige Kontrolle der Datensicherung	
Notfallpläne zur System-/ Datenrekonstruktion	
Regelmäßige Wartungsarbeiten / Reinigung	
Service Level Agreement für Datensicherungs-Software	
Service Level Agreement für Datensicherungs-Hardware	
Dokumentation der Back-up-Software-Einrichtung?	
frei für ergänzenden Eintrag	

	Erstellt	Geprüft und Freigegeben
am:		
von:		
Unterschrift		

3 Server x 3 **Klicken Sie hier, um Text einzugeben.**

IT-System: Klicken Sie hier, um Text einzugeben.

Aufgabe	Beschreibung Verfahrensweise
Verantwortlicher für die Datensicherung	
Art der Datensicherung	
Umfang der Datensicherung	
Datensicherungs-Hardware	
Datensicherungs-Software (inkl. Version und Build)	
Datensicherungs-Benutzer	
Ist das Kennwort für Datensicherungs-Benutzer dokumentiert?	
Häufigkeit und Zeitpunkte der Sicherung	
Anzahl der Generationen	
Vorgehensweise und Speichermedium	
Aufbewahrungsort	
Transportmodalitäten	
Regelmäßige Kontrolle der Datensicherung	
Notfallpläne zur System-/ Datenrekonstruktion	
Regelmäßige Wartungsarbeiten / Reinigung	
Service Level Agreement für Datensicherungs-Software	
Service Level Agreement für Datensicherungs-Hardware	
Dokumentation der Back-up-Software-Einrichtung?	
frei für ergänzenden Eintrag	

	Erstellt	Geprüft und Freigegeben
am:		
von:		
Unterschrift		

4 Server x 4 **Klicken Sie hier, um Text einzugeben.**

IT-System: Klicken Sie hier, um Text einzugeben.

Aufgabe	Beschreibung Verfahrensweise
Verantwortlicher für die Datensicherung	
Art der Datensicherung	
Umfang der Datensicherung	
Datensicherungs-Hardware	
Datensicherungs-Software (inkl. Version und Build)	
Datensicherungs-Benutzer	
Ist das Kennwort für Datensicherungs-Benutzer dokumentiert?	
Häufigkeit und Zeitpunkte der Sicherung	
Anzahl der Generationen	
Vorgehensweise und Speichermedium	
Aufbewahrungsort	
Transportmodalitäten	
Regelmäßige Kontrolle der Datensicherung	
Notfallpläne zur System-/ Datenrekonstruktion	
Regelmäßige Wartungsarbeiten / Reinigung	
Service Level Agreement für Datensicherungs-Software	
Service Level Agreement für Datensicherungs-Hardware	
Dokumentation der Back-up-Software-Einrichtung?	
frei für ergänzenden Eintrag	

	Erstellt	Geprüft und Freigegeben
am:		
von:		
Unterschrift		

5 Server x 5 **Klicken Sie hier, um Text einzugeben.**

IT-System: Klicken Sie hier, um Text einzugeben.

Aufgabe	Beschreibung Verfahrensweise
Verantwortlicher für die Datensicherung	
Art der Datensicherung	
Umfang der Datensicherung	
Datensicherungs-Hardware	
Datensicherungs-Software (inkl. Version und Build)	
Datensicherungs-Benutzer	
Ist das Kennwort für Datensicherungs-Benutzer dokumentiert?	
Häufigkeit und Zeitpunkte der Sicherung	
Anzahl der Generationen	
Vorgehensweise und Speichermedium	
Aufbewahrungsort	
Transportmodalitäten	
Regelmäßige Kontrolle der Datensicherung	
Notfallpläne zur System-/ Datenrekonstruktion	
Regelmäßige Wartungsarbeiten / Reinigung	
Service Level Agreement für Datensicherungs-Software	
Service Level Agreement für Datensicherungs-Hardware	
Dokumentation der Back-up-Software-Einrichtung?	
frei für ergänzenden Eintrag	

	Erstellt	Geprüft und Freigegeben
am:		
von:		
Unterschrift		

6 Server x 6 **Klicken Sie hier, um Text einzugeben.**

IT-System: Klicken Sie hier, um Text einzugeben.

Aufgabe	Beschreibung Verfahrensweise
Verantwortlicher für die Datensicherung	
Art der Datensicherung	
Umfang der Datensicherung	
Datensicherungs-Hardware	
Datensicherungs-Software (inkl. Version und Build)	
Datensicherungs-Benutzer	
Ist das Kennwort für Datensicherungs-Benutzer dokumentiert?	
Häufigkeit und Zeitpunkte der Sicherung	
Anzahl der Generationen	
Vorgehensweise und Speichermedium	
Aufbewahrungsort	
Transportmodalitäten	
Regelmäßige Kontrolle der Datensicherung	
Notfallpläne zur System-/ Datenrekonstruktion	
Regelmäßige Wartungsarbeiten / Reinigung	
Service Level Agreement für Datensicherungs-Software	
Service Level Agreement für Datensicherungs-Hardware	
Dokumentation der Back-up-Software-Einrichtung?	
frei für ergänzenden Eintrag	

	Erstellt	Geprüft und Freigegeben
am:		
von:		
Unterschrift		

C) Randbedingungen für das Datensicherungskonzept

1 Verpflichtung der Mitarbeiter zur Datensicherung

Alle Mitarbeiter(innen) sind zur Einhaltung des Datensicherungskonzepts verpflichtet und sind stets aufgefordert, an seiner stetigen Verbesserung mitzuarbeiten. Anfragen und Verbesserungsvorschläge sind jeweils über den Bereichsleiter an die Abteilung EDV zu richten.

Mitarbeiter(innen), die mit der Datensicherung beauftragt sind, haben diese Aufgaben mit besonderer Sorgfalt durchzuführen und müssen andere Vorgesetzte bzw. den EDV-Verantwortlichen unverzüglich informieren, wenn Probleme aufgetreten sind oder Gefahr im Verzug ist.

Jede(r) Mitarbeiter(in) ist angehalten, nicht mehr benötigte Dateien und E-Mails regelmäßig zu löschen und damit beizutragen, dass die Datenbestände und deren Strukturen überschaubar bleiben und die Kosten der Datenhaltung und Datensicherung in vertretbaren Grenzen bleiben. Dazu gehört auch, dass die Mitarbeiter regelmäßig die EDV-Verantwortlichen informieren, welche Datenbestände auf externe Medien (CD-ROM, DVD usw.) ausgelagert werden können.

Ferner sind im Zusammenhang der Datenspeicherung und –sicherung den Arbeitsanweisungen (AA-IT-Nutzer-?) (Grundeinweisung der Mitarbeiter zur individuellen Laufwerksnutzung), (AA-Admin-? -Beschreibung der Aufgaben der Arbeitsgruppenadministratoren) und (AA-Admin-? - Übersicht Arbeitsgruppenverzeichnisse) Folge zu leisten.

Daten sind vorzugsweise auf den jeweiligen Netzwerklaufwerken zu speichern. Lokal auf dem PC oder Notebook gespeicherte Daten können von der zentralen Server-Datensicherung nicht berücksichtigt werden. Die Verantwortung für lokal gespeicherte Daten liegt allein beim Benutzer, ein eventueller Datenverlust (durch einen Schaden an der PC-Hardware) kann nicht ausgeschlossen werden.

In den Arbeitsanweisungen AA-IT-Nutzer-? (Grundeinweisung der Mitarbeiter(innen) zur individuellen Laufwerksnutzung), AA-Admin-? (Beschreibung der Aufgaben der Arbeitsgruppenadministrator(inn)–en) und AA-Admin-? (Übersicht Arbeitsgruppenverzeichnisse) sind Regeln zur Dateiablage festgelegt.

2 Regelung der Verantwortlichkeiten

In den Arbeitsanweisungen AA-IT-Nutzer-? (Grundeinweisung der Mitarbeiter(innen) zur individuellen Laufwerksnutzung), AA-Admin-? (Beschreibung der Aufgaben der Arbeitsgruppenadministrator(inn)en) und AA-Admin-? (Übersicht Arbeitsgruppenverzeichnisse) sind Regeln zur Dateiablage festgelegt.

Prinzipiell ist jede(r) Benutzer(in) für die sinnvolle Speicherung einer Datei selbst verantwortlich (siehe: Abschnitt „Verpflichtung der Mitarbeiter zur Datensicherung"). Ferner muss entschieden und schriftlich fixiert werden, wer für die Datensicherung der einzelnen Bereiche verantwortlich ist. Es existieren folgende Verantwortlichkeitsgruppen:

- jeder IT-Benutzer bzw. Informationseigentümer selbst,
- der Administrator/Systemverwalter oder
- ggfs. ein für die Datensicherung speziell ausgebildeter Mitarbeiter.

Darüber hinaus sind die Entscheidungsträger zu benennen, die eine Datenrekonstruierung veranlassen können. Auch ist festzulegen, wer berechtigt ist, eine Datenrekonstruierung des Gesamtdatenbestandes oder ausgewählter, einzelner Dateien operativ durchzuführen.

Es ist klar festzulegen und in einem geeigneten Verzeichnis zu dokumentieren, wer auf den/die Datensicherungsträger zugriffsberechtigt ist. Es muss sichergestellt sein, dass nur Berechtigte Zugriff auf die Datensicherungen erhalten (siehe Punkt 6 – Datenträgerverwaltung).

Bei der Festlegung der Verantwortlichkeit ist insbesondere der Vertraulichkeits- und Integritätsbedarf der Daten sowie die Vertrauenswürdigkeit der zuständigen Mitarbeiter(innen) zu betrachten. Es muss sichergestellt werden, dass der/die Verantwortliche erreichbar ist und ein(e) Vertreter(in) benannt und eingearbeitet ist. Darüber hinaus ist ein(e) Verantwortliche(r) für die Datenrekonstruktionsübung festzulegen. Dies ist mit einem Notfallvorsorgekonzept abzustimmen.

Aus folgender Matrix können die Verantwortlichkeiten zur Datensicherung der serverseitigen IT-Systeme entnommen werden:

Aufgabe	Mitarbeiter (in)	1. Vertretung	2. Vertretung
Datensicherung / -rücksicherung AS 400	Name	Name	Name
Datensicherung / -rücksicherung Mailserver	Name	Name	Name
Datensicherung / -rücksicherung Server X	Name	Name	Name
Datensicherung / -rücksicherung Server X	Name	Name	Name
Datensicherung / -rücksicherung Server X	Name	Name	Name
Datensicherung / -rücksicherung Server X	Name	Name	Name
Datensicherung / -rücksicherung Server X	Name	Name	Name
Datensicherung / -rücksicherung Server X	Name	Name	Name
Datensicherung / -rücksicherung Server X	Name	Name	Name

3 Überprüfung auf Wiederherstellbarkeit von Daten

Die interne Arbeitsanweisung AA-? (Datensicherung allgemein) erwähnt – neben allgemeinen Informationen zur Datensicherung – einen monatlichen Funktionstest der durchgeführten Sicherungsvorgänge.

Allerdings gibt es für diese Vorgehensweisen noch keine konkreten Arbeitsanweisungen, so sind auch keine Verantwortlichkeiten für die Durchführung dieser Tätigkeiten benannt und schriftlich festgelegt.

Für eine hohe Qualität der Datensicherung und vor dem Hintergrund einer Anforderung zur Rücksicherung im Katastrophenfall ist zwingend erforderlich, dass die Sicherungsmedien auf die Widerherstellbarkeit von Daten sporadisch bzw. regelmäßig kontrolliert werden. In diesem Zuge sind Verantwortlichkeiten für diese Tätigkeit zu definieren und schriftlich zu fixieren.

Darüber hinaus sind die Ergebnisse der Überprüfung der Sicherungsmedien auf die Wiederherstellbarkeit von Daten in einem Verzeichnis detailliert zu protokollieren und durch den entsprechenden Mitarbeiter abzuzeichnen.

Für die Rekonstruktion eines Datenbestandes muss im Überprüfungsfall getestet werden, ob mit den vorhandenen Sicherungskopien der Daten ein solches Vorhaben durchgeführt werden kann. Technische Defekte, falsche Parametrisierung, unzureichende Dokumentation, eine unzureichende Datenträgerverwaltung o. ä. können eine Rekonstruktion von gesicherten Daten unmöglich machen.

Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen muss – mindestens – nach jeder Änderung des Datensicherungsverfahrens getestet werden. Hierbei ist sicherzustellen, dass eine vollständige Datenrekonstruktion möglich ist. Auf diese Weise wird zuverlässig ermittelt, ob

- die Datenrekonstruktion überhaupt möglich ist,
- die Verfahrensweise der Datensicherung praktikabel ist,
- eine ausreichende Dokumentation der Datensicherung vorliegt, damit ggf. auch ein Vertreter die Datenrekonstruktion vornehmen kann und
- die erforderliche Zeit zur Datenrekonstruktion den Anforderungen an die Verfügbarkeit entspricht.

Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden, dass

- die Daten testweise auf einem Ausweich-IT-System installiert werden müssen,
- für die Datensicherung und Datenrekonstruktion unterschiedliche Schreib- und Lesegeräte benutzt werden.

Die Tätigkeiten sind sinnvollerweise mit den Notfallübungen (Übungen im Rahmen der Notfallvorsorge) abzustimmen.

4 Dokumentation

Für die Vorgehensweise zur Sicherung von Daten bzw. deren Wiederherstellung gibt es für folgende IT-Systeme entsprechende Arbeitsanweisungen:

Arbeits-anweisung Nr. / vom	IT-System	To Do / Hinweise
AA-Nr.-Datum ?	Datensicherung Mail-Server	
AA-Nr.-Datum ?	Datensicherung Server x	
AA-Nr.-Datum ?	Datensicherung Server x	
AA-Nr.-Datum ?	Datensicherung Server x	
AA-Nr.-Datum ?	Datensicherung Server x	
AA-Nr.-Datum ?	Datensicherung Server x	
AA-Nr.-Datum ?	Datensicherung Server x	
AA-Nr.-Datum ?	Datensicherung Server x	
AA-Nr.-Datum ?	Datensicherung Server x	

Eine Dokumentation ist bereits mit den wichtigsten Aspekten zum Bereich Datensicherung im Kapitel B. („Dokumentierte Verfahrensweise für die Datensicherung (je Server-System)“) erstellt worden. Werden Änderungen an der Datensicherung vorgenommen, bedarf es der Anpassung und Aktualisierung der Dokumentationen bzw. Arbeitsanweisungen, ggfs. sind Mitarbeiter aktiv darüber in Kenntnis zu setzen, dass sich Datensicherungsmodalitäten geändert haben.

Ferner ist ein Bestandsverzeichnis notwendig, um einen schnellen und zielgerichteten Zugriff auf benötigte Datensicherungsmedien zu ermöglichen. Dabei muss deutlich erkennbar sein:

- der Aufbewahrungsort,
- die Aufbewahrungsdauer,
- die berechtigten Personen.

Die äußerliche Kennzeichnung von Datenträgern ermöglicht deren schnelle Identifizierung. Hierbei ist eine festgelegte und in den Arbeitsanweisungen dokumentierte Struktur von Kennzeichnungsmerkmalen zu nutzen. Dies erleichtert die Zuordnung in den Bestandsverzeichnissen.

5 Änderungen der gesetzlichen Bestimmungen

Geänderte Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen

Veränderungen im Bereich der IT-Infrastruktur

Da ein Datensicherungskonzept kein statisches Gebilde ist, sondern eher als Prozess verstanden werden muss, ist dieses Konzept entsprechend an sich ändernde Bedingungen bzw. neue Herausforderungen anzupassen. Sinnvoll ist von daher ein regelmäßiger Review, zum Beispiel alle 6 Monate.

6 Datenträgerverwaltung

Aufgrund der Konzentration von Daten auf Datensicherungsmedien besitzen diese einen mindestens ebenso hohen Schutzbedarf bezüglich Vertraulichkeit und Integrität wie die gesicherten Daten selbst. Bei der Aufbewahrung in einem zentralen Datensicherungsarchiv sind daher entsprechend wirksame IT-Sicherheitsmaßnahmen wie z. B. Zutrittskontrollen notwendig.

Aufgabe der Datenträgerverwaltung als Teil der Betriebsmittelverwaltung ist es, den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht. Weiterhin ist im Rahmen der Datenträgerverwaltung die sachgerechte Behandlung und Aufbewahrung der Datenträger, deren ordnungsgemäßer Einsatz und Transport und schließlich auch noch die Löschung bzw. Vernichtung der Datenträger zu gewährleisten. Dies ist durch entsprechende Regelungen bezüglich der Verantwortlichkeiten bzw. mittels entsprechender Arbeitsanweisungen zu definieren.

Bestandsverzeichnisse ermöglichen einen schnellen und zielgerichteten Zugriff auf Datenträger. Bestandsverzeichnisse geben Auskunft über: Aufbewahrungsort, Aufbewahrungsdauer, berechtigte Empfänger.

Die äußere **Kennzeichnung** von Datenträgern ermöglicht deren schnelle Identifizierung. Die Kennzeichnung sollte jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben, um einen Missbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.

Für eine **sachgerechte Behandlung** von Datenträgern sind die Herstellerangaben, die üblicherweise auf der Verpackung zu finden sind, heranzuziehen. Hinsichtlich der **Aufbewahrung** von Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.

Für die unternehmensinterne Weitergabe von Datenträger können Regelungen getroffen werden wie Quittungsverfahren, Abhol-/Mitnahmeberechtigungen sowie das Führen von Bestandsverzeichnissen über den Verbleib der Datenträger.

Für den Fall, dass **von Dritten erhaltene Datenträger** eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Werden zum Beispiel Daten für PCs übermittelt, sollte generell ein Viren-Check des Datenträgers erfolgen. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von Datenträgern diese auf Computer-Viren zu überprüfen.

Eine geregelte Vorgehensweise für die **Löschung oder Vernichtung** von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Vor der Wiederverwendung von Datenträgern muss die Löschung der gespeicherten Daten vorgenommen werden, hier wird im folgenden Abschnitt im Detail eingegangen.

Es ist über eine entsprechende Arbeitsanweisung festzulegen, wer für den Austausch der zu nutzenden Datensicherungsmedien (nach der Durchführung einer Datensicherung) jeweils zuständig ist.

Ferner muss geregelt sein, welche Nutzungsdauer für jeden einzelnen Medientyp veranlagt wird. Hierbei ist dem Verschleiß und der Alterung der verschiedenen Datensicherungsmedien Rechnung zu tragen. So sind wiederbeschreibbare Datenträger regelmäßig zu entsorgen und durch neue zu ersetzen. Dabei sind die entsprechenden Herstellerangaben zu beachten.

Darüber hinaus muss geregelt und schriftlich fixiert sein, wer für die Kontrolle, den Austausch und die anschließende Löschung und Entsorgung der nicht mehr benötigten Sicherungsmedien zuständig ist.

Es ist stets eine ausreichende Menge an Datensicherungsmedien vorzuhalten. Diese sind für die verantwortlichen Personen zugänglich zu lagern.

7 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln

Eine geregelte Vorgehensweise für die Löschung oder Vernichtung von Datenträgern verhindert einen Missbrauch der gespeicherten Daten. Bevor Datenträger wieder verwendet werden, müssen die gespeicherten Daten vollständig gelöscht werden, z. B. durch vollständiges Überschreiben oder Formatieren. Dies ist insbesondere wichtig, wenn Datenträger an Dritte weitergegeben werden sollen. Auch der Empfänger des Datenträgers muss nach dem Empfang prüfen, ob der Schutzwert der Daten ein sofortiges Löschen des Datenträgers erfordert, nachdem die Daten auf ein anderes IT-System übertragen wurden.

Es gibt verschiedene Methoden um Informationen auf Datenträgern zu löschen, z. B. über Löschkommandos, durch Formatieren, durch Überschreiben oder durch Zerstörung des Datenträgers. Welche Methode gewählt werden sollte, hängt hierbei auch vom Schutzbedarf der zu löschenden Daten ab, der Schutz gegen die Restaurierung von Restdaten steigt in der genannten Reihenfolge – hier soll daher nur auf letztere Möglichkeit im Detail eingegangen werden.

- Vernichtung der Sicherungsdatenträger
  - Eine einfache Möglichkeit, Datenträger zu vernichten, besteht darin, dass Disketten und Magnetbänder zerschnitten und Festplatten mechanisch zerstört werden. Dies ist allerdings sehr umständlich bei größeren Mengen zu vernichtender Datenträger und auch nicht ausreichend bei höherem Schutzbedarf.
  - Geeignete Vernichtungsgeräte für Magnetbänder, Disketten und CD-ROMs müssen der Norm DIN 32757 entsprechen. Bei diesen Vernichtungsgeräten werden die Datenträger entweder zerkleinert oder eingeschmolzen. Magnetbänder und Disketten, die vertrauliche oder personenbezogene Daten enthalten, müssen – sofern die Daten nicht mehr benötigt werden – entweder physikalisch gelöscht oder der gesamte Datenträger vernichtet werden.
- Löschen von Datenträgern
  - Der Löschvorgang kann entweder durch das Neutralisieren auf einem speziellen Gerät, oder durch das Überschreiben des Datenträgers mit einer anderen Information durchgeführt werden.

    Wichtiger Hinweis: Wird die zu löschende Information nicht vollständig überschrieben, so ist der Rest der Information noch auf dem Datenträger vorhanden und damit für Personen mit dem entsprechenden Fachwissen lesbar. Darauf ist besonders zu achten, wenn Datenträger dieser Art zum Informationsaustausch an andere, auch externe Stellen, verwendet werden. Hierzu sind nur vollständig gelöschte, z.B. neutralisierte, Datenträger zu verwenden.
- Entsorgung von Sicherungsdatenträger

  Neutralisierte oder vollständig überschriebene Magnetbänder können über den dafür vorgesehenen normalen Entsorgungsweg entsorgt werden.
  - Vernichtung:

    Entweder steht eine eigene Anlage zur Vernichtung zur Verfügung, oder diese Datenträger werden zentral gesammelt und durch eine externe Firma im Auftrag vernichtet. Die mit einem schriftlichen Vertrag beauftragte externe Entsorgungsfirma muss als Auftragsdatenverarbeitung bei der Datenschutzaufsichtsbehörde gemeldet sein.

    Wird sich für die Fremdentsorgung der Datenträger entschieden, die personenbezogene Daten enthalten, so kommt der vom Gesetzgeber geforderten sorgfältigen Auswahl des Auftragnehmers (§ 11, Abs. 2 BDSG) eine besondere Bedeutung zu. Wichtige Gesichtspunkte sind hierbei:
    - Sind technisch organisatorische Maßnahmen getroffen, die die geforderte Sicherheit garantieren?
    - Ist ein betrieblicher Datenschutzbeauftragter gemäß § 36 BDSG bestellt?
    - Sind die Mitarbeiter auf das Datengeheimnis gemäß § 5 BDSG verpflichtet?
    - Ist der Entsorger der Datenschutzaufsichtsbehörde gemeldet (§ 32 BDSG)?
    - Schaltet der Entsorger Dritte zur Vernichtung der Datenträger ein?
    - Auch bei positiver Beantwortung sollte auf eigene Eindrücke bei einer Besichtigung des Entsorgers nicht verzichtet werden. Gegebenenfalls sind auch entsprechende Referenzen einzuholen. Ähnlich sollte verfahren werden, wenn Datenträger mit anderen schutzbedürftigen Daten extern entsorgt werden. Auch hier sollte die Entsorgung in einem schriftlichen Vertrag geregelt werden.

Wird mit einem Entsorger eine Zusammenarbeit angestrebt, so ist **in jedem Fall ein Rahmenvertrag abzuschließen**. Innerhalb des Vertrags/Rahmenvertrages sollten folgende Punkte geregelt sein:

- Art der Übergabe der Datenträger (gegebenenfalls mit Festlegung der Sicherheitsstufe, gem. DIN 32757),
- Vernichtung der Datenträger noch am gleichen Tag,
- Ausstellung eines Übernahmeprotokolls,
- Haftung des Auftragnehmers für den gesicherten Transport und die ordnungsgemäße,
- Vernichtung nach Übergabe des Materials und Ausstellung eines Vernichtungszertifikats,
- Recht des Auftraggebers zur Kontrolle der Einhaltung der Weisungen und Vertragsbestimmungen,
- Verpflichtung der bei der Vertragserfüllung beteiligten Personen gem. Bundesdatenschutzgesetz,
- Haftung des Auftragnehmers für materielle und immaterielle Schäden, die durch missbräuchliche Verwendung des Materials nach Übergabe entstehen,
- Möglichkeiten der außerordentlichen Kündigung bei Vertragswidrigkeiten.