Bundesamt
für Sicherheit in der
Informationstechnik

Datensicherungskonzept

- Beispiel -

Stand: Dezember 2008

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

INHALTSVERZEICHNIS

A. Sensibilisierung

1 Einleitung

Hinweis:

Bemerkungen und Hinweise, an welchen Stellen sich eine individuelle Anpassung oder Ergänzung des Musterkonzeptes besonders empfiehlt, sowie Kommentare sind gelb hinterlegt.

1.1 Gefährdungslage

Der Verlust von Daten kann erhebliche Auswirkungen auf die Geschäftstätigkeit haben. Sind Anwendungsdaten oder Kundenstammdaten verloren oder verfälscht, kann dies für ein Unternehmen Existenz bedrohend sein.

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 Computer-Viren

1.2 Zielsetzung

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

Von der Datensicherung zu unterscheiden ist die Archivierung von Daten. Richtlinien für die Archivierung sind in einem separaten Archivierungskonzept beschrieben. Darüber hinaus gilt das Notfallvorsorgekonzept, in dem Verhaltensregeln für den Notfall zusammengestellt sind. M 2.243 M 6.32

1.3 Begriffliche Definitionen

1.3.1 Daten

Nachfolgend werden die verschiedenen Datenarten kurz dargestellt, die zu sichern sind.

Anwendungsdaten

Anwendungsdaten sind Dateien mit geschäftsbezogenen Inhalten (Textdateien, E-Mails, Datenbanken etc.).

Systemdaten

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

A. Sensibilisierung

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.

1.3.2 Datensicherungsarten

Die Wahl der Datensicherungsart ist abhängig von verschiedenen in Kapitel 2 dargestellten Einflussfaktoren. M 6.35

Datenspiegelung

Die Daten werden redundant und zeitgleich auf verschiedenen Datenträgern gespeichert.

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 inkementellen oder Volldatensicherung geändert haben. Da die inkrementelle Datensicherung auf einer Volldatensicherung basiert, muss in periodischen Abständen dennoch eine Vollsicherungen erstellt werden.

Die inkrementelle Datensicherung spart Speicherplatz und geht 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.

Differentielle Datensicherung

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

A. Sensibilisierung	

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

1.3.3 Datensicherungsmedium

Auch die Wahl des Datensicherungsmediums ist abhängig von verschiedenen in Kapitel 2 dargestellten Einflussfaktoren. Hierbei ist insbesondere das zu erwartende Datenvolumen von Bedeutung. Nachfolgend werden die geläufigsten Datenträger aufgezeigt. M 6.35

Wechseldatenträger

Optische Datenträger

Hierunter fallen CD und DVD. 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 ist 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 Einflussfaktoren

Zur Festlegung der Verfahrensweise zur Datensicherung ist eine Übersicht zu erstellen, in der nachfolgende Angaben aufgeführt werden. Anhand dieser sind für die einzelnen IT-Systeme Datensicherungspläne zu erstellen. Es sind die entsprechenden Verantwortlichen für die IT-Systeme und die darauf betriebenen Anwendungen einzubeziehen. M 6.34

(a) Spezifikation der zu sichernden Daten

Es ist eine Übersicht der in Kapitel 1.3.1 aufgeführten Daten, die zu sichern sind, zu erstellen. Hierzu gehören Anwendungs- und Betriebssoftware, Systemdaten, Anwendungsdaten und Protokolldaten.

(b) *Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten*

Für die unter (a) ermittelten Daten, die gesichert werden sollen, sind die Verfügbarkeitsanforderungen festzulegen. Dabei muss berücksichtigt werden, M 6.1

A. Sensibilisierung

wie lange die Fachaufgabe ohne diese Daten weitergeführt werden kann, ohne dass auf Datensicherungsbestände zurückgegriffen werden muss.

(c) *Rekonstruktionsaufwand der Daten ohne Datensicherung*

Zur wirtschaftlichen Betrachtung der Datensicherung ist zu prüfen, ob und mit welchem Aufwand zerstörte Datenbestände rekonstruiert werden könnten, wenn eine Datensicherung nicht zur Verfügung steht.

(d) *Datenvolumen*

Das Datenvolumen ist wesentlicher Faktor bei der Wahl der in Kapitel 1.3.3 aufgeführten Medien.

(e) *Änderungsvolumen*

Das Änderungsvolumen ist sehr entscheidend für die Wahl des Datensicherungsverfahrens und der Datensicherungshäufigkeit. Daher ist zu prüfen, in welchem Umfang die verschiedenen Daten sich innerhalb eines festgelegten Zeitraums ändern. Notwendig sind Angaben, ob bestehende Dateien inhaltlich geändert oder ob neue Dateien erzeugt werden.

(f) *Änderungszeitpunkte der Daten*

Es sind Sicherungszeitpunkte für die verschiedenen Daten festzulegen. Hierzu sollen regelmäßige Zeitpunkte festgelegt werden, die sich an den Besonderheiten der Daten orientieren. Hierbei können Intervalle oder anlassbezogene Datensicherungszeitpunkte gewählt werden.

(g) *Fristen*

Es sind gesetzliche Aufbewahrungs- und Löschfristen zu beachten.

(h) *Vertraulichkeitsbedarf der Daten*

Zur Festlegung der Sicherheitsmaßnahmen für die Datensicherungskopien ist die Vertraulichkeit der jeweiligen Daten festzulegen. Zu beachten ist, dass durch Zusammenführen verschiedener Daten mit gleicher Vertraulichkeitsstufe auf einem Sicherungsmedium (durch Kumulation) eine höhere Schutzbedarfsstufe für das Sicherungsmedium erreicht werden kann.

(i) *Integritätsbedarf der Daten*

Die Daten sind entsprechend ihres Integritätsbedarfs abzuspeichern und aufzubewahren. Dabei muss sichergestellt sein, dass die Daten während der Aufbewahrungszeit nicht verändert werden.

Dies ist insbesondere bei Datenbanken und anderen in Verbindung stehenden Daten zu berücksichtigen.

(j) *Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer*

Sofern es die Kenntnisse und Fähigkeiten der einzelnen IT-Benutzer zulassen, können bestimmte Datensicherungen an die Benutzer delegiert werden.

B. Allgemeine Regelungen

3 Verpflichtung der Benutzer auf Datensicherung

Alle Mitarbeiter sind zur Einhaltung des Datensicherungskonzepts verpflichtet und aufgefordert, an seiner stetigen Verbesserung mitzuarbeiten. M 2.41

4 Regelung der Verantwortlichkeiten

Alle Informationseigentümer bzw. Vorgesetzte oder Projektleiter entscheiden für ihren Verantwortungsbereich über Regeln zur Dateiablage und legen in Zusammenarbeit mit den Administratoren die Modalitäten der Datensicherung fest. Alle Regelungen werden in einem Datensicherungsplan festgehalten (Details zum Datensicherungsplan sind in Kapitel 11 beschrieben).

Es ist zu entscheiden und schriftlich zu fixieren, wer für die Durchführung der Datensicherung verantwortlich ist. Es gibt folgende Verantwortlichkeitsgruppen:

1. IT-Benutzer bzw. Informationseigentümer selbst,
2. Administrator/Systemverwalter oder
3. für die Datensicherung speziell ausgebildete 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. M 6.59

Es ist klar festzulegen und in dem in Kapitel 10.2 dargestellten Verzeichnis zu dokumentieren, wer auf den/die Datensicherungsträger zugriffsberechtigt ist. Es muss sichergestellt sein, dass nur Berechtigte Zugriff auf die Datensicherungen erhalten. M 2.8

Bei der Festlegung der Verantwortlichkeit ist insbesondere der Vertraulichkeits-, Integritätsbedarf der Daten und die Vertrauenswürdigkeit der zuständigen Mitarbeiter zu betrachten. Es muss sichergestellt werden, dass der Verantwortliche erreichbar ist und ein Vertreter benannt und eingearbeitet wird.

Darüber hinaus ist ein Verantwortlicher für die Datenrekonstruktionsübung festzulegen. Dies ist mit dem Notfallvorsorgekonzept abzustimmen. M 6.3

5 Allgemeine Grundsätze

Es ist eine zentrale Datenhaltung anzustreben, so dass Daten automatisch über das Netz gesichert werden können. Ausnahmen für mobil eingesetzte IT-Systeme oder IT-Systeme, mit denen geheime Daten verarbeitet werden, sind zugelassen.

Komplexe Systeme sind nur durch entsprechend kompetente Mitarbeiter zu sichern. IT-Benutzer sollten die Daten nur selbst sichern, wenn die Sicherung durch einen ausgebildeten Administrator nicht möglich oder nicht sinnvoll ist (z. B. bei Tele(heim)arbeit, mobiler Nutzung des IT-Systems). M 2.41

Die Pflicht zur Datensicherung darf aber nur auf die IT-Benutzer übertragen werden, wenn diese ausreichend qualifiziert und der Aufgabe gewachsen sind!

Datensicherungen sollten möglichst automatisiert ablaufen, um Fehler zu vermeiden. Wenn IT-Benutzer mit der Datensicherung betraut wurden, sind ihnen entsprechende IT-Anwendungen zur Verfügung zu stellen und Aufbewahrungsorte für die Verwahrung der Datensicherungen bereitzustellen (ab-

schließbarer Schrank, Tresor, Büroräume etc.).

Wird die Datensicherung nicht von den IT-Benutzern selbst durchgeführt, sind die Verantwortlichen zur Verschwiegenheit bezüglich der Dateninhalte verpflichtet. In Einzelfällen ist eine Verschlüsselung in Betracht zu ziehen. M 6.35

Bei der Rekonstruktion von Daten ist größte Vorsicht geboten, um nicht versehentlich Daten zu überschreiben oder Abläufe zu stören.

6 Kontrolle der Datensicherung

Der Verantwortliche für die Datensicherung muss regelmäßig überprüfen, ob die Datensicherung tatsächlich korrekt durchgeführt wurde. Besonders bei automatischen Prozeduren ist diese Prüfung notwendig. Prüfpunkte können dabei die Auswertung von Log-Dateien und Fehlerprotokollen, das Datum der Sicherungsdatei, die Stichprobenprüfung der Dateiinhalte, die Plausibilität der Dateigröße etc sein. In Einzelfällen, z. B. wenn kryptographische Verfahren eingesetzt werden, kann ein Dateivergleich notwendig sein.

7 Schulung und Information der Mitarbeiter

Die Mitarbeiter sind hinsichtlich der Bedeutung der Datensicherung zu sensibilisieren. M 2.198

Alle IT-Benutzer müssen über sie betreffende Regelungen informiert werden, insbesondere darüber, welche Daten bzw. Verzeichnisse regelmäßig automatisch gesichert werden und welche nicht. Auch die Aufbewahrungszeit der Datensicherungen muss bekannt gegeben werden.

Vor der ersten Durchführung einer Datensicherung sind betroffene Mitarbeiter in der Durchführung der notwendigen Maßnahmen zu schulen. Hierunter fällt:

- korrekte Wahl und Nutzung der Datensicherungs-Datenträger
- Zugriffsberechtigungen auf Datensicherung bei Datensicherung und Datenrekonstruktion M 2.8
- korrekte Nutzung der Programme zur Datensicherung M 2.12, M 3.4
- korrekte Aufbewahrung und Dokumentation der Datenträger zur Datensicherung.

8 Übungen zur Datenrekonstruktion

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

Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen muss auf jedenfall nach jeder Änderung des Datensicherungsverfahrens, ansonsten in regelmäßigen Abständen, getestet werden. Hierbei ist sicherzustellen, dass eine vollständige Datenrekonstruktion möglich ist.

Auf diese Weise muss zuverlässig ermittelt werden, 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

B. Allgemeine Regelungen

die Verfügbarkeit entspricht.

Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden, dass M 6.41

- die Daten vielleicht auf einem Ausweich-IT-System installiert werden müssen, M 6.6
- für die Datensicherung und Datenrekonstruktion unterschiedliche Schreib-/Lesegeräte benutzt werden.

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

9 Revision

Die Erkenntnisse aus den Übungen sollten dazu verwendet werden, das Datensicherungskonzept zu verbessern. Dabei ist auf eine Abstimmung mit dem Notfallvorsorgekonzept zu achten.

Darüber hinaus ist regelmäßig zu überprüfen, ob die Datensicherungen durchgeführt wurden. Dies betrifft insbesondere die dezentrale Datensicherung durch die Benutzer selbst.

C. Detailregelungen

10 Durchführung von Datensicherungen

10.1 Transportmodalitäten

Bei der Durchführung einer Datensicherung werden Daten über ein Netz oder eine Leitung übertragen oder Datenträger zum Datenträgerarchiv transportiert. M 6.74

Bei der Auswahl des Datenübertragungsmediums bzw. des Datenträger-Transportweges sind die Verfügbarkeitsanforderungen zu berücksichtigen. Wenn zur Datenrekonstruierung die Daten über ein Netz übertragen werden, muss bei der Auswahl der Übertragungskapazität des Netzes das Datenvolumen beachtet werden. Es ist zum Zeitpunkt der Datensicherung eine ausreichende Datenübertragungskapazität sicherzustellen. M 5.23

Es ist zu verhindern, dass die Daten während der Übertragung bzw. auf dem Transport unbefugt gelesen, kopiert oder manipuliert werden. In Abhängigkeit vom Schutzbedarf sind Verschlüsselung bzw. sichere Transportbehältnisse und Wege zu benutzen. Der Versand oder Transport von Datenträgern muss in der Weise erfolgen, dass eine Beschädigung der Datenträger möglichst ausgeschlossen werden kann (z. B. luftgepolsterte Umschläge). M 5.23

Es ist für die einzelnen Anwendungsdaten festzulegen, wie schnell diese rekonstruiert zur Verfügung stehen müssen. Die Zeit für die Rekonstruierung soll kleiner als die maximal tolerierbare Ausfallzeit sein.

10.2 Datensicherungsarchiv

Der Zugriff auf Datensicherungsdatenträger ist im erforderlichen Umfang und in angemessener Zeit zu gewährleisten. Auch nach einem Katastrophen-Fall müssen die Datensicherungen verfügbar bzw. zugänglich sein. Dies erfordert eine geregelte Verwaltung der Datensicherungsdatenträger. M 2.3

Es ist für die Backup-/Datensicherungsdatenträger ein Datensicherungsarchiv festzulegen. M 6.74

Keinesfalls darf der Datensicherungsbestand aus der gleichen Schadensursache heraus untergehen wie die Produktionsdaten. Daher sind die Backup-Datenträger zumindest in einem anderen Brandabschnitt als der Originaldatenträger aufzubewahren. Sicherer ist die Lagerung in einem anderen Gebäude oder außerhalb des Betriebsgeländes. Bei der Wahl des Ortes gilt zu beachten, dass bei zunehmender Entfernung die Transportzeit und somit die Gesamtrekonstruierungszeit steigt.

Backup-Datenträger, die im Rahmen der Tele(heim)arbeit oder der mobilen Nutzung eines IT-Systems angefertigt werden, müssen auch im häuslichen Bereich verschlossen aufbewahrt werden. Es ist sicherzustellen, dass nur der Benutzer selber (bzw. sein Vertreter) darauf Zugriff hat. M 6.71

Die Aufbewahrung erfordert angemessene Sicherheitsmaßnahmen. Diese haben sicherzustellen, dass niemand unbefugt auf die Datenträger zugreifen kann. Der Schutzbedarf der Schränke und Räume kann variieren und richtet sich nach dem Schutzbedarf der gelagerten Daten. Es sind folgende Maßnahmen zu ergreifen:

- Es ist ein Bestandsverzeichnis zum schnellen und zielgerichteten Zugriff auf Datenträger zu führen.
- Es ist zur schnellen Identifizierung von Datenträgern eine eindeutige Kennzeichnung vorzunehmen.

C. Detailregelungen

- Es ist durch entsprechende Maßnahmen die sachgemäße Lagerung sicherzustellen. Darunter fällt u. a. die magnetfeld-/staubgeschützte und klimagerechte Aufbewahrung der Datenträger. Hierzu sind die Angaben der Hersteller zu beachten. — M 6.20
- Es sind Maßnahmen zur Verhinderung des unbefugten Zutritts und Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.
- Eine geregelte Vorgehensweise für die Löschung oder Vernichtung von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Sind Löschungsfristen einzuhalten, muss das Datensicherungsarchiv dem angepasst sein. — M 2.167

Im Falle der Auslagerung des Datensicherungsarchivs an einen externen Anbieter sind Verfügbarkeits-, Integritäts- und Vertraulichkeitsvereinbarungen dem Vertrag zu Grunde zu legen. Es sind Kontrollrechte einzuräumen.

Im Vertrag ist speziell für Datensicherungsarchive schriftlich zu vereinbaren: — M 2.253

- Verfügbarkeits-, Integritäts- und Vertraulichkeitsanforderungen an Datensicherung — M 6.1
- Weisungsgebundenheit des Outsourcing-Dienstleisters
- Zutrittsregelungen für die eigenen und fremden Mitarbeiter
- Einhaltung der geltenden einschlägigen Gesetze (insb. Datenschutz), Vorschriften und internen Regelungen — M 3.2, M 2.226
- Stillschweigen über alle bekannt werdenden Informationen — M 3.6
- Zu treffende technische und organisatorische Maßnahmen durch den Outsourcing-Dienstleister und dessen Kontrolle — M 2.254, M 2.250, M 2.251
- Notfallvorsorgemaßnahmen — M 6.3
- Rechte und Pflichten des externen Personals — M 2.4, M 2.226
- Regelungen zur Haftung

Zu den gesetzlich oder organisatorisch vorgegebenen Löschungszeitpunkten ist im Datensicherungsarchiv die Löschung zu initiieren bzw. durchzuführen. Ist eine Löschung technisch nicht möglich, so ist durch organisatorische Maßnahmen eine Wiederverwendung zu löschender Daten zu verhindern.

Sofern Datenträger erneut genutzt werden sollen, ist sicherzustellen, dass keine Restinformationen mehr enthalten sind. — M 2.167

10.3 Anforderungen an Datensicherungsmedien

Es sind ausreichende Datensicherungsmedien vorzuhalten. Diese sind für die verantwortlichen Personen (siehe 4) zugänglich zu lagern. — M 6.35

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.

Die Entsorgung ist sicher zu gestalten, so dass eine Rekonstruktion durch einen unbefugten Dritten nicht möglich ist.

Für die Sicherstellung von etwaigen Aufbewahrungsfristen ist das Archivierungskonzept zu beachten. — M 2.243

11 Datensicherungspläne

Datensicherungspläne sollten so formuliert sein, dass ein sachverständiger Dritter in der Lage ist, sämtliche für den Wiederanlauf einer IT-Anwendung erforderliche Software (Betriebssystemsoftware, Anwendungssoftware) und deren Daten in angemessener Zeit beschaffen und installieren zu können.

C. Detailregelungen

Hierbei wird eine Unterscheidung zwischen den einzelnen Datenarten vorgenommen, da diese unterschiedlichen Vertraulichkeits-, Verfügbarkeits- und Integritätsanforderungen unterliegen.

Folgende Punkte sollten in einem Datensicherungsplan aufgeführt werden: M 6.13

- Art der Daten
- zuständig für Sicherung bzw. Rekonstruktion
- Art der Datensicherung (z. B. inkrementell, voll, komprimiert, verschlüsselt)
- Hinweise zur Rekonstruktion
- Häufigkeit und Zeitpunkt der Datensicherung
- Datensicherungsmedium
- Aufbewahrungszeit bzw. Anzahl der Generationen

Es sind für die verschiedenen Datenarten entsprechende Datensicherungspläne zu erstellen. Zunächst werden die allgemein gültigen Verfahrensanweisungen aufgezeigt. M 6.13

Der Rest von Kapitel 11 ist aus didaktischen Gründen sehr ausführlich gestaltet. In einem "realen" Datensicherungskonzept kann hier natürlich stark gekürzt werden!

11.1 Allgemeine Datensicherungspläne

Anzahl der Generationen

Inkrementelle Datensicherungen sind bis zur nächsten Vollsicherung aufzubewahren.

Es haben mindestens 3 Generationen (eine Generation ist eine Datenvollsicherung) der wöchentlichen Datenvollsicherungen zu existieren.

Es sind so viele Generationen aufzubewahren, dass auch bei einem verzögerten Bemerken eines Integritäts- oder Verfügbarkeitsverlusts die Daten noch rekonstruiert werden können. Daher ist im Einzelfall nach Abhängigkeit der Bedeutung der Daten eine höhere Generationsanzahl zu wählen.

Mindestens eine Generation, der in der Tele(heim)arbeit und der mobilen Nutzung entstehenden Backup-Datenträger ist in der Institution aufzubewahren, damit im Notfall der Vertreter auf die Backup-Datenträger zugreifen kann.

Die Aufbewahrung und eine über die 3 Generationen hinausgehende Aufbewahrung von Generationen ist innerhalb eines Archivierungskonzepts zu regeln. M 2.243

Häufigkeit und Zeitpunkt der Datensicherung

Häufigkeit und Zeitpunkte der Datensicherungen sind geeignet zu wählen.

Je weniger zeitlicher Abstand zwischen den einzelnen Datensicherungen liegt, desto geringer ist im Allgemeinen auch der für eine Rekonstruierung und Nacherfassung erforderliche Zeitaufwand. Der Intervall der Datensicherungen ist also so zu wählen, dass die Zeit für die Rekonstruierung der in diesem Zeitraum geänderten Daten kleiner als die maximal tolerierbare Ausfallzeit ist.

Gleichzeitig muss beachtet werden, dass der Zeitpunkt der Datensicherung

C. Detailregelungen

nicht nur periodisch gewählt werden kann. Gibt es Zeitpunkte, zu denen sich die Daten in großem Umfang ändern oder zu denen der Komplettdatenbestand vorliegen muss, so bietet es sich an, unmittelbar danach eine Volldatensicherung durchzuführen.

Datensicherungsmedium

Die Auswahl des Datensicherungsmediums hat sich am Volumen/Änderungsvolumen zu orientieren. Sowohl für die inkrementelle als auch die Vollsicherung eignen sich CD oder DVD. Zum schnellen Wiederanlauf kann die neueste Generation auch auf einem zweitem Server (Datensicherungs-/Backupserver) bzw. einer zweiten Festplatte gesichert werden.

Um das Datenvolumen auf dem Speichermedium zu minimieren, können zusätzlich Datenkompressionsalgorithmen angewandt werden. Es ist bei Anwendung der Kompression sicherzustellen, dass die gewählten Parameter und Algorithmen im Rahmen der Datensicherung dokumentiert und für die Datenrekonstruierung (Dekompression) vorgehalten werden.

Sowohl für die inkrementelle als auch die Vollsicherung sind Wechseldatenträger zu nutzen. Bei der inkrementellen Datensicherung auf nicht vernetzten Rechnern kann unter Umständen auf andere Wechseldatenträger wie Disketten oder USB-Sticks zurückgegriffen werden, sofern die benötigten Speicherressourcen mit einer geringer Anzahl an Datenträgern realisiert werden können.

Zum schnellen Wiederanlauf ist zu prüfen, inwiefern Vollsicherungen oder auch inkrementelle Datensicherungen neben Wechseldatenträgern die neueste Generation der Anwendungsdaten auch auf einem zweitem Server (Datensicherungs-/Backupserver) bzw. einer zweiten Festplatte gesichert werden.

11.2 Sicherung von Anwendungsdaten

Anwendungsdaten können stark unterschiedlichen Verfügbarkeits-, Integritäts- und Vertraulichkeitsanforderungen unterliegen, daher sind die Schutzanforderungen individuell festzulegen.

Anwendungsdateien sind, sofern möglich nur auf den entsprechenden Servern zu speichern. Bei Laptops oder nicht vernetzten Rechnern sind lokal Datensicherungen vorzunehmen.

Art der Datensicherung

Es muss erreicht werden, dass alle Anwendungsdaten der Server-Festplatte, die z. B. nicht älter als ein Tag sind, rekonstruiert werden können. Als Datensicherungsverfahren ist bei Anwendungsdaten, die auf den Servern gespeichert sind, eine Kombination aus inkrementeller und aus Volldatensicherung zu wählen. M 6.35

Bei Daten mit sehr hohen Verfügbarkeitsanforderungen (z. B. geschäftskritische Kundendatenbank) kann es erforderlich sein, dass die Daten gespiegelt auf einer zweiten Festplatte gesichert werden.

Alternativ können Datensicherungen automatisiert durch spezielle Programme erstellt werden.

Darüber hinaus können die von Anwendungsprogrammen angebotenen automatischen Datensicherungsmöglichkeiten genutzt werden (z. B. das von Textverarbeitungsprogrammen angebotene automatische Erstellen einer Sicherheitskopie).

C. Detailregelungen

Häufigkeit und Zeitpunkt der Datensicherung

Die Anwendungsdaten sind einer täglichen inkrementellen Sicherung und einer wöchentlichen Vollsicherung zu unterziehen.

Sofern es möglich ist, IT-Systeme im mobilen Einsatz (z. B. Laptops) regelmäßig an ein Netz anzuschließen, hat die Sicherung der lokalen Daten über eine Netzanbindung zu erfolgen. Dies sollte mindestens wöchentlich durchgeführt werden. Alternativ sind zur Sicherung externe Datensicherungsmedien wie CDs zu nutzen. Gleiches gilt für die PCs, die in Tele(heim)arbeit eingesetzt werden oder nicht vernetzt sind. Die Datensicherung ist zu kontrollieren.

Die Volldatensicherung hat sich an den arbeitsüblichen Begebenheiten zu orientieren: Sie sollte für gewöhnlich am Ende (Freitagnachmittag oder vor Beginn einer Arbeitswoche (Montag früh) stattfinden. Für einzelne Bereiche hat sich der Termin der Datensicherung am Rechnungslauf zu orientieren (z. B. für die Gehaltsabrechnung am Monatsende).

Datensicherungsmedium

Sowohl für die inkrementelle als auch die Vollsicherung sind Wechseldatenträger zu nutzen. Bei der inkrementellen Datensicherung auf nicht vernetzten Rechnern kann unter Umständen auf andere Wechseldatenträger (Disketten oder USB-Sticks) zurückgegriffen werden, sofern die benötigten Speicherressourcen mit einer geringer Anzahl an Datenträgern realisiert werden können.

Zum schnellen Wiederanlauf ist zu prüfen, inwiefern Vollsicherungen oder auch inkrementelle Datensicherungen neben Wechseldatenträgern die neueste Generation der Anwendungsdaten auch auf einem zweitem Server (Datensicherungs-/Backupserver) bzw. einer zweiten Festplatte gesichert werden.

11.3 Sicherung von Systemdaten

Unter Systemdaten sind systeminterne Einstellungen zu verstehen, die sowohl auf den Servern als auch lokal auf den Endgeräten existieren. Auf den Servern sind z. B. die Rechtestruktur oder Passwörter hinterlegt, auf den Endgeräten zumeist Initialisierungsdateien von Textverarbeitungs- oder Datenbank-Software (*.INI und *.BNK), Makrodefinitionen sowie Textbausteine etc.

Diese Dateien haben unterschiedliche Verfügbarkeits-, Integritäts- und Vertraulichkeitsanforderungen. Systemdaten auf den Servern weisen höhere Anforderungen als angeschlossene (vernetzte) Endgeräte auf.

Es sind so wenige Systemdaten auf den Endgeräten zu speichern wie möglich.

Art der Datensicherung

Aufgrund des relativ geringen Daten- und Änderungsvolumens ist als Datensicherungsverfahren die Volldatensicherung zu wählen. M 6.35

Alternativ können Datensicherungen automatisiert durch spezielle Programme erstellt werden.

Häufigkeit und Zeitpunkt der Datensicherung

Die Systemdaten der Server und der Endgeräte sind anlassbezogen zu sichern, wie bei der Umstrukturierung der Rechte oder anderen Änderungen. Gleiches gilt für IT-Systeme im mobilen Einsatz.

Datensicherungsmedium

Es sind Wechseldatenträger zu empfehlen. Sofern die benötigten Speicherres-

C. Detailregelungen

sourcen mit einem anderen Wechseldatenträger wie Disketten oder USB-Stick realisiert werden können, können bei der Datensicherung auf diese Datenträger zurückgegriffen werden.

Sofern ein zweiter Server (Backup- oder Datenspiegelungsserver) genutzt wird, sollen die Systemdaten auch hier gesichert werden.

11.4 Sicherung von Protokolldaten

Protokolldaten (Login-Protokolle, Protokolle von Sicherheitsverletzungen, Datenübertragungsprotokolle etc.) liegen in der Regel auf dem Server vor.

Protokolldaten haben hohe Vertraulichkeits- und auch Integritätsanforderungen, was bei der Datensicherung zu berücksichtigen ist.

Art der Datensicherung

Protokolldaten sind mittels einer Vollsicherung zu sichern. Hierbei sind betriebliche Notwendigkeiten zu berücksichtigen (wie Speicherkapazitäten). M 6.35

Häufigkeit und Zeitpunkt der Datensicherung

Die Protokolldaten sind mindestens monatlich zu sichern. Die Datensicherung ist so zu gestalten, dass Löschfristen einhaltbar sind.

Datensicherungsmedium

Es sind je nach Platzbedarf Wechseldatenträger wie CD, DVD oder Bänder/Streamer zu nutzen.

11.5 Sicherung von Software

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

Je nach Bedeutung der einzelnen Software für den Geschäftsablauf liegen entsprechend unterschiedliche Verfügbarkeits-, Integritäts- und Vertraulichkeitsanforderungen vor.

Urheberrecht und Copyright-Vereinbarungen sind zu beachten.

Art der Datensicherung

Es ist von den Originaldatenträgern gekaufter Software sowie von Eigenentwicklungen eine Sicherungskopie zu erstellen. M 6.21

Häufigkeit und Zeitpunkt der Datensicherung

Die Software ist dann zu sichern, wenn diese erworben bzw. eingespielt wurde. Darüber hinaus ist insbesondere bei komplexerer Anwendungssoftware eine Datensicherung nach der Parametrisierung durchzuführen.

Eine regelmäßige Sicherung ist nicht erforderlich, jedoch sollte eine regelmäßige Überprüfung stattfinden, ob Sicherheitskopien erstellt wurden.

Anzahl der Generationen

Es ist ausreichend, wenn eine Sicherheitskopie der aktuellsten Version von der genutzten Software vorhanden ist.

Datensicherungsmedium

Es ist aufgrund des Platzbedarfs empfehlenswert, mindestens die CD als Datensicherungsmedium zu nutzen. Es ist darauf zu achten, dass der physikalische Schreibschutz des Datenträgers ein versehentliches Löschen oder Überschreiben der Daten verhindert.

C. Detailregelungen

Sofern ein zweiter Server (Backup- oder Datenspiegelungsserver) genutzt wird, soll die Software auch hier gesichert werden. M 6.6

12 Dokumentation

Eine erfolgte Datensicherung ist unbedingt zu dokumentieren. Dabei ist bei der Erstellung der Datensicherung zu dokumentieren: M 6.37

- Datum der Datensicherung,
- Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert),
- Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind,
- Datenträger, auf dem die Daten gesichert wurden,
- Für Datensicherung eingesetzte Hard- und Software (mit Versionsnummer)
- Bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.).

Darüber hinaus bedarf es einer Beschreibung der Vorgehensweise für die Wiederherstellung eines Datensicherungsbestandes (z. B. erforderliche Hard- und Software, benötigte Parameter). Auch die Reihenfolge der Datensicherungen zu dokumentieren, um ein ordnungsgemäßes Wiederherstellen sicherzustellen.

Des Weiteren ist ein Bestandsverzeichnis zu erstellen. Dies ermöglicht einen schnellen und zielgerichteten Zugriff auf die Datensicherungsdatenträger. Im Bestandsverzeichnis sind folgenden Angaben zu machen: M 2.2

- Aufbewahrungsort
- Aufbewahrungsdauer
- berechtigte Empfänger

Die äußerliche Kennzeichnung von Datenträgern ermöglicht deren schnelle Identifizierung. Hierbei ist eine festlegte Struktur von Kennzeichnungsmerkmalen zu nutzen. Hierbei soll eine (möglichst sprechende) Bezeichnung gewählt werden sowie das Datum der Datensicherung und die Art der Sicherung (inkrementell/komplett) notiert werden. Dies erleichtert die Zuordnung in den Bestandsverzeichnissen. M 2.43

D. Rekonstruktion

13 Regelungen zur Rekonstruktion

Es ist eine Rekonstruktionsreihenfolge für den Schadensfall festzulegen.

Dies hat sich zum einen an der Art des Datenverlusts zu orientieren. Ein Komplettdatenverlust aufgrund einer defekten Festplatte hat andere Anforderungen als ein Verlust von Teilen der Anwendungsdaten.

Zum anderen hat sich die Reihenfolge an der Bedeutung der Daten für die geschäftskritischen Prozesse zu orientieren. Archivdaten können eine geringere Bedeutung als eine Kundendatenbank haben. Dies ist mit dem Notfallvorsorgekonzept abzustimmen.

Technische Erforderlichkeiten sind ebenfalls zu berücksichtigen. Hard- und Software muss auch für veraltete Formate stehen.

Es muss zuerst die Volldatensicherung und danach in richtiger Reihenfolge jede angelegte inkrementelle Datensicherung zurückgesichert werden, um den aktuellen Datenbestand wiederherzustellen. M 6.22

Um ein vollständig zerstörtes IT-System zurückzusichern, müssen unter Umständen alle Datensicherungen in der Reihenfolge ihres Entstehens zurückgespielt werden. Die Reihenfolge kann der Datensicherungsdokumentation entnommen werden (siehe Kapitel 12).