



Parasol Island

Datensicherungs-Richtlinie

Dateiname:	02_09_PSL_ISMS_Datensicherung_v01.00_jH
Dokumentenebene:	02_Richtlinie
Erstellt von:	Philip Hansen
Version:	01.00
Status:	Freigegeben
Letzte Aktualisierung am/von:	07.11.2017 Justus Heinser
Exportiert am:	07.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	07.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	-

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	15.09.2017	Justus Heinser	Ergänzung
01.00	07.11.2017	Justus Heinser	Finalisierung



Parasol Island

Inhaltsverzeichnis

1. Einleitung	4
Gefährdungslage	4
Zielsetzung	4
Begriffliche Definitionen	4
Anwendungsdaten	4
Systemdaten	4
Protokolldaten	5
Software	5
Datensicherungsarten	5
Datenspiegelung	5
Volldatensicherung	5
Inkrementelle Datensicherung	5
Differentielle Datensicherung	5
Datensicherungsmedium	6
Optische Datenträger	6
Bänder/Streamer Tapes	6
Festplatte	6
2. Einflussfaktoren	6
a) Spezifikation der zu sichernden Daten	6
b) Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten	7
c) Rekonstruktionsaufwand der Daten ohne Datensicherung	7
d) Datenvolumen	7
e) Änderungsvolumen	7
f) Änderungszeitpunkte der Daten	7
g) Fristen	7
h) Vertraulichkeitsbedarf der Daten	7
i) Integritätsbedarf der Daten	7
j) Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer	8
3. Verpflichtung der Benutzer auf Datensicherung	8
4. Regelung der Verantwortlichkeiten	8
5. Allgemeine Grundsätze	9
6. Kontrolle der Datensicherung	9
7. Schulung und Information der Mitarbeiter	9



Parasol Island

8. Übungen zur Datenrekonstruktion	10
Auf diese Weise muss zuverlässig ermittelt werden, ob	10
Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden:	10
9. Revision	10
10. Durchführung von Datensicherungen	11
Transportmodalitäten	11
Datensicherungsarchiv	11
Anforderungen an Datensicherungsmedien	12
11. Datensicherungspläne	12
Allgemeine Datensicherungspläne	13
Anzahl der Generationen	13
Häufigkeit und Zeitpunkt der Datensicherung	13
Sicherung von Anwendungsdaten	13
Sicherung von Systemdaten	14
Sicherung von Protokolldaten	14
Sicherung von Software	14
12. Dokumentation	15
13. Regelungen zur Rekonstruktion	15



Parasol Island

1. Einleitung

Gefährdungslage

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

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 gilt „Handlungsanweisung für ausgewählte Schadensfälle“, in dem Verhaltensregeln für den Notfall zusammengestellt sind.

Begriffliche Definitionen

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.



Parasol Island

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.

Datensicherungsarten

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

Differentielle Datensicherung

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

Eine differentielle Datensicherung benötigt im Vergleich zur inkrementellen Datensicherung mehr Speicherplatz und dauert aufgrund des höheren Datenvolumens länger. Die Dateien lassen sich jedoch



Parasol Island

einfacher und schneller rekonstruieren. Für die Rekonstruktion der Daten reicht die letzte Volldatensicherung sowie die aktuellste differentielle Sicherung.

Datensicherungsmedium

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

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 Datenrekonstruktion zu nutzen.

2. Einflussfaktoren

Zur Festlegung der Verfahrensweise zur Datensicherung ist eine Übersicht zu erstellen, in den nachfolgenden 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.

a) Spezifikation der zu sichernden Daten

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



Parasol Island

b) Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten

Für die unter 0 ermittelten Daten, die gesichert werden sollen, sind die Verfügbarkeitsanforderungen festzulegen. Dabei muss berücksichtigt werden, 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 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.



Parasol Island

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.

3. Verpflichtung der Benutzer auf Datensicherung

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

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.

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 Datenrekonstruktion veranlassen können. Auch ist festzulegen, wer berechtigt ist, eine Datenrekonstruktion des Gesamtdatenbestandes oder ausgewählter, einzelner Dateien operativ durchzuführen.

Es ist klar festzulegen und in dem in Kapitel 0 dargestellten Verzeichnis zu dokumentieren, wer auf den/die Datensicherungsträger zugriffsberechtigt ist. Es muss sichergestellt sein, dass nur Berechtigte Zugriff auf die Datensicherungen erhalten.

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.

5. Allgemeine Grundsätze

Es ist eine zentrale Datenhaltung anzustreben, sodass 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.



Parasol Island

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). 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 (abschließbarer 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.

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.

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 Datensicherungsdatenträger
- Zugriffsberechtigungen auf Datensicherung bei Datensicherung und Datenrekonstruktion
- korrekte Nutzung der Programme zur Datensicherung
- 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 jeden Fall 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 die Verfügbarkeit entspricht.

Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden,

- dass die Daten vielleicht auf einem Ausweich-IT-System installiert werden müssen,
- dass 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.



10. Durchführung von Datensicherungen

Transportmodalitäten

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

Bei der Auswahl des Datenübertragungsmediums bzw. des Datenträger-Transportweges sind die Verfügbarkeitsanforderungen zu berücksichtigen. Wenn zur Datenrekonstruktion 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.

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).

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

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

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.

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

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 Gesamtrekonstruktionszeit 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 selbst (bzw. sein Vertreter) darauf Zugriff hat.

Die Aufbewahrung erfordert angemessene Sicherheitsmaßnahmen. Diese haben sicherzustellen, dass niemand unbefugt auf die Datenträger zugreifen kann. Der Schutzbedarf der Schränke und Räume



Parasol Island

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.
- 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.
- Es sind Maßnahmen zur Verhinderung des unbefugten Zutritts und Zugriffs (geeignete Behälter, 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.

Zu den gesetzlich oder organisatorisch vorgegebenen Lösungszeitpunkten 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.

Anforderungen an Datensicherungsmedien

Es sind ausreichende Datensicherungsmedien vorzuhalten. Diese sind für die verantwortlichen Personen zugänglich zu lagern. 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, sodass eine Rekonstruktion durch einen unbefugten Dritten nicht möglich ist.

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

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. 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:

- Art der Daten
- zuständig für Sicherung bzw. Rekonstruktion
- Art der Datensicherung (z. B. inkrementell, voll, komprimiert, verschlüsselt)



Parasol Island

- 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.

Allgemeine Datensicherungspläne

Anzahl der Generationen^^

Es sind so viele Generationen aufzubewahren, dass auch bei einem verzögerten Bemerkens 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. Die Aufbewahrung und eine über die 3 Generationen hinausgehende Aufbewahrung von Generationen ist innerhalb eines Archivierungskonzepts zu regeln.

Häufigkeit und Zeitpunkt der Datensicherung

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

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.

Es muss erreicht werden, dass alle Anwendungsdaten der Server-Festplatte, rekonstruiert werden können. Als Datensicherungsverfahren ist bei Anwendungsdaten, die auf den Servern gespeichert sind, eine Kombination aus inkrementeller und aus Volldatensicherung zu wählen.

Alternativ können Datensicherungen automatisiert durch spezielle Programme erstellt werden.

Sofern es möglich ist müssen IT-Systeme im mobilen Einsatz (z. B. Laptops) regelmäßig an ein Netz angeschlossen werden, um die Sicherung der lokalen Daten über eine Netzanbindung durchzuführen. Die Datensicherung ist zu kontrollieren.



Parasol Island

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.

Aufgrund des relativ geringen Daten- und Änderungsvolumens ist als Datensicherungsverfahren die Volldatensicherung zu wählen. Alternativ können Datensicherungen automatisiert durch spezielle Programme erstellt werden.

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.

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.

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.

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

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

12. Dokumentation

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

- Datum der Datensicherung
- Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert)



Parasol Island

- 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.

Die äußerliche Kennzeichnung von Datenträgern ermöglicht deren schnelle Identifizierung. Hierbei ist eine festgelegte 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.

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 Erfordernisse 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.

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.