Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein CON.3 Datensicherungskonzept

1. Einleitung

Institutionen speichern immer mehr Daten und sind gleichzeitig immer stärker auf sie angewiesen. Gehen Daten verloren, z. B. durch defekte Hardware, Malware oder versehentliches Löschen, können gravierende Schäden entstehen. Dies kann klassische IT-Systeme, wie Server oder Clients, betreffen. Aber auch Router, Switches oder IoT-Geräte können schützenswerte Informationen, wie Konfigurationen, speichern. Deswegen umfasst der Begriff IT-System in diesem Umsetzungshinweis alle Formen von IT-Komponenten, die schützenswerte Informationen speichern.

Durch regelmäßige Datensicherungen lassen sich Auswirkungen von Datenverlusten minimieren. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der Betrieb der Informationstechnik kurzfristig wiederaufgenommen werden kann, wenn Teile des aktiv genutzten Datenbestandes oder der gesamte Datenbestand verloren gehen. Das Datensicherungskonzept nimmt somit auch eine zentrale Rolle in der Notfallplanung ein. Die wesentlichen Anforderungen der Notfallplanung, wie der maximal zulässige Datenverlust (Recovery Point Objective, RPO), sollten in dem Datensicherungskonzept berücksichtigt werden.

Zu einem vollständigen Datensicherungskonzept gehört nicht nur der Aspekt, wie Datensicherungen präventiv erstellt werden (Backup), sondern auch, wie angefertigte Datensicherungen auf dem Ursprungssystem wiederhergestellt werden (Restore). Für eine Datensicherung können die unterschiedlichsten Lösungen eingesetzt werden, wie beispielweise:

- Storage-Systeme,

- Bandlaufwerke,
- mobile Wechseldatenträger (USB-Sticks oder externe Festplatten),
- optische Datenträger sowie
- Online-Lösungen.

Diese Lösungen werden im Folgenden als Speichermedien für die Datensicherung zusammengefasst. Dem gegenüber werden Datenspiegelungen über RAID-Systeme nicht als Datensicherung verstanden, da die gespiegelten Daten simultan verändert werden. Das bedeutet, dass eine Datenspiegelung über ein RAID-System zwar einem Ausfall durch einen Hardwaredefekt einzelner Datenträger vorbeugen kann, sie kann jedoch nicht vor einem unbeabsichtigten Überschreiben oder einer Infektion mit Schadsoftware schützen.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins CON.3 *Datensicherungskonzept* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein CON.3 Datensicherungskonzept

CON.3.M1 Erhebung der Einflussfaktoren für Datensicherungen (B)

Für jedes IT-System, eventuell sogar für einzelne IT-Anwendungen mit besonderer Bedeutung, müssen die nachfolgenden Einflussfaktoren ermittelt werden. Dazu können die Systemadministratoren und die Zuständigen für die einzelnen IT-Anwendungen befragt werden. Die Ergebnisse sind nachvollziehbar zu dokumentieren. Im Einzelnen muss ermittelt werden:

- Spezifikation der zu sichernden Daten: Es sollte der Datenbestand des IT-Systems (der IT-Anwendung) ermittelt werden, der für die Fachaufgaben erforderlich ist. Dazu gehören die Anwendungs- und Betriebssoftware, die Systemdaten (z. B. Initialisierungsdateien, Makrodefinitionen, Konfigurationsdaten, Textbausteine, Passwortdateien, Zugriffsrechtedateien), die Anwendungsdaten selbst und Protokolldaten (z. B. Login-Protokollierung, Protokolle über Sicherheitsverletzungen, Datenübertragungsprotokolle).
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten: Für die im ersten Schritt spezifizierten Daten müssen nun die Verfügbarkeitsanforderungen festgelegt werden. Ein erprobtes Maß dazu ist die Angabe der maximal tolerierbaren Ausfallzeit. Sie gibt an, über welchen Zeitraum der Geschäftsprozess bzw. die Fachaufgabe ohne diese Daten weitergeführt werden kann, ohne dass auf Datensicherungsbestände zurückgegriffen werden muss.
- Rekonstruktionsaufwand der Daten ohne Datensicherung: Um ein unter wirtschaftlichen Gesichtspunkten angemessenes Datensicherungskonzept zu entwickeln (siehe CON.3.M6 *Entwicklung eines Datensicherungskonzepts*), ist es notwendig zu wissen, ob und mit welchem Aufwand zerstörte Datenbestände rekonstruiert werden können, wenn eine Datensicherung nicht verfügbar ist. Untersucht werden sollte, aus welchen Quellen die Daten rekonstruiert werden können und wie lange das dauern würde. Beispiele hierfür sind die Aktenlage, Ausdrucke, Befragungen und Erhebungen.
- Speichervolumen: Für die Auswahl des Speichermediums ist ein entscheidender Faktor das gespeicherte und zu sichernde Datenvolumen.
- Änderungsvolumen: Um die Häufigkeit der Datensicherung und das adäquate Sicherungsverfahren bestimmen zu können, muss bekannt sein, wie viele Daten sich in einem

bestimmten Zeitabschnitt ändern. Notwendig sind Angaben, ob bestehende Dateien inhaltlich geändert oder ob neue Dateien erzeugt werden.

- Änderungszeitpunkte der Daten: Es gibt IT-Anwendungen, bei denen sich Daten nur zu bestimmten Terminen ändern, wie zum Beispiel der Abrechnungslauf zur Lohnbuchhaltung zum Monatsende. In solchen Fällen ist eine Datensicherung unverzüglich nach einem solchen Termin sinnvoll. Daher sollte für die zu sichernden Daten angegeben werden, ob sie sich täglich, wöchentlich oder zu bestimmten Terminen ändern.
- Fristen (rechtliche Anforderungen): Für die Daten ist zu klären, ob bestimmte Fristen einzuhalten sind. Hierbei kann es sich um Aufbewahrungsfristen oder auch um Löschfristen im Zusammenhang mit personenbezogenen Daten handeln. Diese Fristen sind bei der Datensicherung zu berücksichtigen.
- Vertraulichkeitsbedarf der Daten: Der Vertraulichkeitsbedarf einer Datei überträgt sich bei einer Datensicherung auf die Sicherungskopie.
- Integritätsbedarf der Daten: Für Datensicherungen muss sichergestellt sein, dass die Daten integer gespeichert werden und während der Aufbewahrungszeit nicht verändert werden. Das ist umso wichtiger, je höher der Integritätsbedarf der Nutzdaten ist. Daher ist für die Datensicherungen anzugeben, wie hoch der Integritätsbedarf ist.
- Kenntnisse und Fähigkeiten der Benutzer: Um entscheiden zu können, wer die Datensicherung durchführt, der Benutzer selbst oder speziell beauftragte Mitarbeiter bzw. die Systemadministratoren, ist ausschlaggebend, über welche Kenntnisse und Fähigkeiten der Benutzer verfügt und welche Werkzeuge ihm zur Verfügung gestellt werden können. Falls die zeitliche Belastung bei der Durchführung einer Datensicherung für Benutzer zu hoch ist, sollte dies angegeben werden.

CON.3.M2 Festlegung der Verfahrensweise für die Datensicherung (B)

Wie eine Datensicherung durchzuführen ist, wird hauptsächlich von den in CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung* erhobenen Einflussfaktoren bestimmt. Für jedes IT-System muss die Verfahrensweise der Datensicherung festgelegt werden. Bei Bedarf sollte die Datensicherung sogar für einzelne IT-Anwendungen des jeweiligen IT-Systems differenziert werden.

Folgende Punkte sollten bei der Festlegung einer Verfahrensweise für die Datensicherung betrachtet werden:

- Art der Datensicherung,
- Häufigkeit und Zeitpunkt der Datensicherung,
- Anzahl der Generationen,
- Vorgehensweise und Speichermedium,
- Zuständigkeit für die Datensicherung,
- Aufbewahrungsort,
- Anforderungen an das Datensicherungsarchiv,
- Transportmodalitäten und
- Aufbewahrungsmodalität.

In der nachfolgenden Tabelle werden die Abhängigkeiten zwischen den genannten Punkten und den Einflussfaktoren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) dargestellt und anschließend erläutert:

	Art der Datensicherung	Häufigkeit und Zeitpunkte der Datensicherung	Anzahl der Generationen	Vorgehensweise und Speichermedium	Zuständigkeit für Datensicherung	Aufbewahrungsort	Anforderungen an DS-Archiv	Transportmodalitäten	Aufbewahrungsmodalität
Verfügbarkeitsanforderungen	X	(X)	X	X	X	X	X	X	
Rekonstruktionsaufwand ohne Datensicherung		(X)	X						
Speichervolumen	X		X	X		X	X	X	
Änderungsvolumen	X	X	X	X					
Änderungszeitpunkte der Daten	(X)	X						(X)	
Fristen				X			X		X
Vertraulichkeitsbedarf der Daten				(X)	X		X	X	X
Integritätsbedarf der Daten			(X)	(X)	X		X	X	X
Kenntnisse der Benutzer	X			X	X				

x = direkte Abhängigkeit, (x) = indirekte Abhängigkeit

Art der Datensicherung

Folgende Datensicherungsarten gibt es:

- **Volldatensicherung**: Bei der Volldatensicherung werden sämtliche zu sichernden Dateien zu einem bestimmten Zeitpunkt auf einen separaten Datenträger gespeichert. Es wird dabei nicht berücksichtigt, ob die Dateien sich seit der letzten Datensicherung geändert haben oder nicht. Daher benötigt eine Volldatensicherung viel Speicher. Der Vorteil ist, dass die Daten vollständig für den Sicherungszeitpunkt vorliegen und die Restaurierung von Dateien einfach und schnell möglich ist, da nur die betroffenen Dateien aus der letzten Volldatensicherung extrahiert werden müssen. Werden Volldatensicherungen selten durchgeführt, so kann sich durch umfangreiche nachträgliche Änderungen innerhalb einer Datei ein hoher Nacherfassungsaufwand ergeben.
- **Inkrementelle Datensicherung**: Bei der inkrementellen Datensicherung werden im Gegensatz zur Volldatensicherung nur die Dateien gesichert, die sich gegenüber der letzten Datensicherung (Volldatensicherung oder inkrementelle Sicherung) geändert haben. Das spart Speicherplatz und verkürzt die erforderliche Zeit für die Datensicherung. Die inkrementelle Datensicherung basiert immer auf einer Volldatensicherung. In periodischen Zeitabständen werden Volldatensicherungen erzeugt, in der Zeit dazwischen werden eine oder mehrere

inkrementelle Datensicherungen vollzogen. Bei der Restaurierung wird die letzte Volldatensicherung als Grundlage genommen, die um die in der Zwischenzeit geänderten Dateien aus den inkrementellen Sicherungen ergänzt wird.

- **Differenzielle Datensicherung**: Bei der differenziellen Datensicherung werden jedes Mal die Dateien gesichert, die sich gegenüber der letzten Volldatensicherung geändert haben. Eine differenzielle Datensicherung benötigt mehr Speicherplatz als eine inkrementelle, Dateien lassen sich aber einfacher und schneller restaurieren. Für die Restaurierung der Daten reicht die letzte Volldatensicherung sowie die aktuellste differenzielle, nicht wie bei der inkrementellen, wo unter Umständen mehrere Datensicherungen nacheinander eingelesen werden müssen.
- **Image-Datensicherung**: Hier werden nicht die einzelnen Dateien eines Festplattenstapels gesichert, sondern die physikalischen Sektoren der Festplatte. Es handelt sich dabei um eine Vollsicherung, die sehr schnell auf eine gleichartige Festplatte restauriert werden kann.
- **Hierarchische Speicher-Management (HSM)**. Hierbei geht es in erster Linie darum, vorhandenen Speicher möglichst wirtschaftlich zu nutzen. Dateien werden abhängig von der Häufigkeit, mit der auf sie zugegriffen wird, auf schnellen Online-Speichern (Festplatten) gehalten, auf Nearline-Speicher (automatische Datenträger-Wechselsysteme) ausgelagert oder auf Offline-Speichern (Magnetbänder) archiviert. Gleichzeitig bieten diese HSM-Systeme auch automatische Datensicherungsroutinen kombiniert aus inkrementeller Datensicherung und Volldatensicherung.

Manchmal werden in der Praxis fälschlicherweise Datenspiegelungen auch als Datensicherung verstanden. Hierbei wird permanent eine exakte Kopie der Daten in einem anderen Verzeichnis oder Medium erstellt. Dies geschieht in der Regel transparent für den Benutzer, beispielsweise durch ein RAID-System. Eine Spiegelung alleine ersetzt jedoch keine Datensicherung, da Inkonsistenzen, Dateifehler oder Löschungen von Dateien sich sofort auf die gespiegelte Version auswirken. Werden beispielsweise die originalen Datenbestände durch Ransomware verschlüsselt, wirkt sich dies direkt auf die gespiegelte Kopie aus.

Eine redundante Datenspeicherung bieten RAID-Systeme an (Redundant Array of Inexpensive Disks). Das RAID-Konzept beschreibt die Verbindung von mehreren Festplatten. Dies kann über einen proprietären Hardware-Controller oder über eine Softwarelösung geschehen. Es gibt verschiedene RAID-Level, wovon RAID-Level 1 die Datenspiegelung beschreibt. RAID-Systeme ersetzen jedoch keine Datensicherung! Sie helfen nicht bei Diebstahl, Ransomware oder Brand, daher müssen auch die auf RAID-Systemen gespeicherten Daten auf zusätzliche Medien gesichert werden und diese Medien auch in anderen Brandabschnitten untergebracht werden.

Für die Entscheidung, welche Datensicherungsstrategie angewendet werden soll, sind die folgenden Einflussfaktoren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) zu berücksichtigen, um eine für die Anforderungen geeignete und gleichzeitig wirtschaftliche Form zu finden:

- Verfügbarkeitsanforderungen: Sind die Verfügbarkeitsanforderungen sehr hoch, so ist eine Datenspiegelung in Erwägung zu ziehen. Sind die Verfügbarkeitsanforderungen hoch, so sollte einer Volldatensicherung statt einer inkrementellen Datensicherung durchgeführt werden.
- Datenvolumen und Änderungsvolumen: Entspricht das Änderungsvolumen annähernd dem Datenvolumen (z. B. bei der Nutzung einer Datenbank), so verringert sich die Speicherplatzersparnis der inkrementellen Datensicherung so stark, dass eine Vollsicherung erwogen werden kann. Ist jedoch das Änderungsvolumen erheblich kleiner als das Datenvolumen, so spart die inkrementelle Datensicherung Speicherplatz.
- Änderungszeitpunkte der Daten: Einen Einfluss auf die Datensicherungsstrategie können die Änderungszeitpunkte der Daten haben. Gibt es Zeitpunkte, an denen anwendungsbezogen der Komplettdatenbestand gesichert werden muss (z. B. nach buchhalterischen Wochen-, Monats- oder Jahresabschlüsse), so kommt zu diesen Zeitpunkten nur eine Vollsicherung infrage.

- Kenntnisse der Benutzer: Eine Datenspiegelung setzt entsprechende Kenntnisse des Systemadministrators voraus, erfordert jedoch vom Benutzer keinerlei Kenntnisse. Eine Volldatensicherung lässt sich auch von einem Benutzer mit geringen Systemkenntnissen durchführen. Demgegenüber erfordert eine inkrementelle Datensicherung schon mehr Systemkenntnisse und Erfahrungen im Umgang mit Datensicherungen.

Häufigkeit und Zeitpunkte der Datensicherung

Tritt ein Datenverlust ein, sind alle Daten bis zur letzten Sicherung verloren. Je aktueller die letzte Datensicherung ist, desto weniger Datenverlust muss die Institution verkraften. Gleichzeitig muss beachtet werden, dass der Zeitpunkt der Datensicherung nicht nur periodisch (z. B. täglich, wöchentlich, werktags) gewählt werden kann, sondern dass auch ereignisabhängige Datensicherungen (z. B. nach x Transaktionen, nach Ausführung eines bestimmten Programms, nach Systemänderungen) notwendig sein können.

Bei der Auswahl der Häufigkeit und der Zeitpunkte der Datensicherung sind folgende Einflussfaktoren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) zu beachten:

- Verfügbarkeitsanforderungen, Wiederherstellungsaufwand ohne Datensicherung und Änderungsvolumen: Der zeitliche Abstand der Datensicherungen ist so zu wählen, dass die Restaurierungs- und Nacherfassungszeit (Rekonstruktionsaufwand der geänderten Daten, für die keine Datensicherung vorhanden ist) der in diesem Zeitraum geänderten Daten (Änderungsvolumen) kleiner als die maximal tolerierbare Ausfallzeit ist.
- Änderungszeitpunkte der Daten: Gibt es Zeitpunkte, an denen sich die Daten in großem Umfang ändern (z. B. Programmlauf für Gehaltszahlung oder Versionswechsel der Software) oder an denen der Komplettdatenbestand vorliegen muss, so bietet es sich an, unmittelbar danach eine Volldatensicherung durchzuführen. Dazu sind neben den periodischen die ereignisabhängigen Datensicherungszeitpunkte festzulegen.

Anzahl der Generationen

Einerseits werden Datensicherungen in kurzen Zeitabständen wiederholt, um eine Kopie eines möglichst aktuellen Datenbestandes verfügbar zu haben, andererseits muss die Datensicherung gewährleisten, dass gesicherte Daten möglichst lange aufbewahrt werden. Eine Volldatensicherung wird als Generation bezeichnet. Die Anzahl der aufzubewahrenden Generationen und der zeitliche Abstand, der zwischen den Generationen liegen muss, sollten festgelegt werden. Diese Anforderungen lassen sich an folgenden Beispielen erläutern:

- Wird eine Datei absichtlich oder unabsichtlich gelöscht, so ist diese Datei in allen späteren Datensicherungen nicht mehr verfügbar. Stellt sich heraus, dass diese gelöschte Datei dennoch benötigt wird, so muss zur Wiederherstellung auf eine ältere Datensicherung zurückgegriffen werden, die zeitlich vor dem Löschen erstellt wurde. Ist eine solche Generation nicht mehr vorhanden, so muss die Datei neu erfasst werden.
- Tritt ein Integritätsverlust in einer Datei auf, z. B. durch Malware, ist es wahrscheinlich, dass dies nicht direkt, sondern erst zeitlich versetzt bemerkt wird. Um die Integrität der Datei wiederherstellen zu können, muss dann auf eine Generation zurückgegriffen werden, die vor dem Integritätsverlust erstellt wurde.
- Es kann nicht ausgeschlossen werden, dass eine Datensicherung fehlerhaft oder unvollständig erstellt wurde. Deswegen ist es oft hilfreich, wenn auf eine weitere Generation zurückgegriffen werden kann.

Um diese Vorteile des Generationenprinzips aufrechterhalten zu können, muss jedoch eine Randbedingung eingehalten werden: der zeitliche Abstand der Generationen darf ein Mindestmaß nicht unterschreiten. Beispiel: In einem automatisierten Datensicherungsverfahren kommt es zu wiederholten Abbrüchen des Datensicherungslaufs. Hierdurch würden nacheinander sämtliche Generationen überschrieben werden. Verhindert werden kann dies, indem vor Überschreiben einer

Generation das Mindestalter überprüft und nur dann überschrieben wird, wenn dieses Alter überschritten ist.

Charakterisieren lässt sich ein Generationsprinzip durch zwei Größen: das Mindestalter der ältesten Generation und die Anzahl der verfügbaren Generationen. Dabei gilt:

- je höher das Mindestalter der ältesten Generation ist, je größer ist die Wahrscheinlichkeit, dass zu einer Datei mit Integritätsverlust (eine gelöschte Datei, die im Nachhinein als notwendig erkannt wird, ist ebenfalls darunter zu fassen) noch eine Vorläuferversion vorhanden ist,
- je größer die Anzahl der verfügbaren Generationen ist, umso aktueller ist die angeforderte Vorläuferversion.

Die Anzahl der Generationen hängt jedoch direkt mit den Kosten der Datensicherung zusammen, weil Datenträger in ausreichender Zahl vorhanden sein müssen. Daher muss die Anzahl der Generationen auf ein wirtschaftlich sinnvolles Maß beschränkt werden.

Für die Wahl der Parameter des Generationsprinzips ergeben sich folgende Einflüsse (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*):

- Verfügbarkeitsanforderungen und Integritätsbedarf der Daten: Je höher die Verfügbarkeitsanforderungen oder der Integritätsbedarf der Daten ist, umso mehr Generationen müssen vorhanden sein, um im Fall des Integritätsverlustes die Wiederherstellungszeit zu minimieren.
- Wenn der Verlust einer Datei oder eine Integritätsverletzung möglicherweise erst sehr spät bemerkt werden kann, sind zusätzliche Quartals- oder Jahressicherungsdatenbestände empfehlenswert.
- Wiederherstellungsaufwand ohne Datensicherung: Sind die Daten zwar umfangreich, aber auch ohne Datensicherung rekonstruierbar, so kann das als eine weitere Pseudo-Generation ins Kalkül gezogen werden.
- Datenvolumen: Je höher das Datenvolumen ist, desto mehr Speicherplatz wird gebraucht und desto höher sind auch die Kosten einer Generation. Ein hohes Datenvolumen kann deshalb die Anzahl der Generationen aus wirtschaftlichen Gründen beschränken.
- Änderungsvolumen: Je höher das Änderungsvolumen ist, umso kürzer sollten die Zeitabstände zwischen den Generationen sein, um eine möglichst zeitnahe Version der betreffenden Datei zu haben und den Wiederherstellungsaufwand gering zu halten.

Vorgehensweise und Speichermedium

Nachdem die Art der Datensicherung, die Häufigkeit und das Generationenprinzip festgelegt wurden, ist nun die Vorgehensweise und das angemessene Speichermedium auszuwählen.

Um das Datenvolumen auf dem Speichermedium zu minimieren, können Datenkompressionsalgorithmen angewandt werden. Teilweise kann das Datenvolumen damit sehr stark reduziert werden. Es ist dabei jedoch sicherzustellen, dass die gewählten Parameter und Algorithmen dokumentiert und für die Wiederherstellung der Daten (Dekompression) vorgehalten werden.

Für die **Vorgehensweise** gibt es zwei Parameter, die festgelegt werden müssen: den Automatisierungsgrad und die Zentralisierung (Speicherort).

Es ist zwischen einem manuellen und automatischen Automatisierungsgrad zu unterscheiden:

- Manuelle Datensicherung bedeutet, dass die Datensicherung händisch angestoßen wird. Vorteilhaft kann sein, dass die ausführende Person individuell den Termin der Datensicherung dem Arbeitsablauf anpassen kann. Nachteil ist, dass die Datensicherung von der Motivation und Disziplin des Mitarbeiters abhängt. Durch Krankheit oder sonstige Abwesenheitsgründe können so eventuell Datensicherungen ausfallen.

- Automatische Datensicherungen werden programmgesteuert zu bestimmten Terminen angestoßen. Vorteilhaft ist, dass die Datensicherung zuverlässig durchgeführt wird, sofern der Terminplan vollständig und aktuell ist. Nachteilig kann sein, dass der Terminplan aktuellen Änderungen angepasst werden muss oder wichtige Änderungen nicht unmittelbar gesichert werden.

Bezüglich der Zentralisierung sind zentral und dezentral durchgeführte Datensicherungen zu unterscheiden:

- Zentrale Datensicherungen zeichnen sich dadurch aus, dass der Speicherort und die Datensicherung am zentralen IT-System durchgeführt werden. Diese Verfahrensweise hat den Vorteil, dass nur ein Mitarbeiter intensiv geschult werden muss und die Benutzer von dieser Arbeit entlastet werden. Vorteilhaft ist weiterhin, dass durch das höhere zentrale Datenaufkommen kostengünstigere Speichermedien verwendet werden können. Nachteilig ist, dass eventuell vertrauliche Daten übertragen und von nicht Befugten eingesehen werden könnten.
- Dezentrale Datensicherungen werden von den Benutzern selbst durchgeführt, ohne dass die Daten auf ein zentrales IT-System übertragen werden müssen. Vorteilhaft ist, dass der Benutzer die Kontrolle über die Daten und die Backup-Datenträger behält, insbesondere wenn es sich um vertrauliche Daten handelt. Nachteilig ist, dass die konsequente Datensicherung damit von der Zuverlässigkeit der Benutzer abhängt und dass dezentrale Lösungen den Benutzern Zeitaufwand abfordern.

Nach der Entscheidung, ob die Datensicherung manuell oder automatisch, zentral oder dezentral durchgeführt wird, muss nun der geeignete Datenträger bzw. das geeignete Speichermedium für die Datensicherung gefunden werden. Dazu können folgende Parameter betrachtet werden:

- Datenträger-Anforderungszeit: Wie lang darf es dauern, bis ein Backup-Datenträger für eine Wiederherstellung bereitstehen muss? Speicher auf Netzlaufwerken können dies innerhalb von Sekunden, Roboter-Systeme können das innerhalb von Minuten, ausgelagerte Bänder müssen unter Umständen erst aufwendig transportiert und aufgelegt werden.
- Zugriffszeit, Transferrate: Wie lang eine Datensicherung dauert und wie schnell sich Daten wiederherstellen lassen, hängt von der mittleren Zugriffszeit des Datenträgers und von der Transferrate ab. Festplatten erlauben einen Zugriff auf bestimmte Dateien im Millisekunden-Bereich, ein Magnetband muss erst zur entsprechenden Stelle gespult werden und bei einem Cloud-Speicher hängt die Transferrate direkt von der Internet-Anbindung ab.
- Speicherkapazität: Das Speichermedium muss über ausreichende Speicherkapazitäten verfügen. Dabei müssen auch zukünftige Datenmengen mit eingeplant werden.
- Kosten: Die Kosten für die Datensicherung müssen in einem angemessenen Verhältnis zum Sicherungszweck stehen. Hierbei ist auch die Lebensdauer der Datenträger zu berücksichtigen.

Die folgenden Einflussgrößen (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) müssen dabei beachtet werden:

- Verfügbarkeitsanforderungen: Je höher die Verfügbarkeitsanforderungen sind, desto schneller muss auf die Datenträger als Speichermedium der Datensicherung zugegriffen werden können und desto schneller müssen die benötigten Daten vom Datenträger wieder einspielbar sein.
- Es muss sichergestellt sein, dass die Speichermedien auch bei Ausfall eines Lesegerätes zur Wiederherstellung genutzt werden können. Die Kompatibilität und Funktion eines Ersatzgerätes sind zu gewährleisten.
- Daten- und Änderungsvolumen: Mit zunehmenden Datenvolumen werden oft preisgünstige Speichermedien benutzt.
- Fristen: Müssen Löschfristen eingehalten werden (z. B. bei personenbezogenen Daten), muss das ausgewählte Speichermedium die Löschung ermöglichen. Speichermedien, die nicht oder

nur mit großem Aufwand löschbar sind (z.B. WORM = Write Once Read Many), sollten in diesem Fall vermieden werden.

- Vertraulichkeitsbedarf und Integritätsbedarf der Daten: Ist der Vertraulichkeits- oder Integritätsbedarf der zu sichernden Daten hoch, so überträgt sich dieser Schutzbedarf auch auf die zur Datensicherung eingesetzten Datenträger. Ist eine Verschlüsselung der Datensicherung nicht möglich, kann über die Auswahl von Datenträgern nachgedacht werden, die aufgrund ihrer kompakten Bauart in Datensicherungsschränken oder Tresoren untergebracht werden können.
- Kenntnisse der Benutzer: Die Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der Benutzer entscheiden darüber, ob eine Verfahrensweise gewählt werden kann, in der der Benutzer selbst manuell für die Datensicherung tätig wird, ob andere ausgebildete Personen die Datensicherung dezentral durchführen oder ob eine automatisierte Datensicherung praktikabler ist.

Zuständigkeit für die Datensicherung

Für die Entscheidung, wer für die Datensicherung zuständig ist, kommen drei Personengruppen infrage: Zunächst kann es der Benutzer selbst sein (typischerweise bei dezentralen und nicht vernetzten IT-Systemen), der allgemeine IT-Betrieb oder ein für die Datensicherung speziell ausgebildeter Administrator. Wird die Datensicherung nicht vom Benutzer durchgeführt, sind die Zuständigen auf Verschwiegenheit bezüglich der Dateninhalte zu verpflichten. Eventuell sollten die Daten auch verschlüsselt werden.

Darüber hinaus sind die Entscheidungsträger zu benennen, die eine Wiederherstellung veranlassen können. Zu klären ist weiterhin, wer berechtigt ist, auf Datensicherungsträger zuzugreifen, insbesondere, wenn sie in Datensicherungsarchiven ausgelagert sind. Es muss sichergestellt sein, dass nur Berechtigte Zutritt erhalten. Abschließend ist zu definieren, wer berechtigt ist, eine Wiederherstellung des Gesamtdatenbestandes oder ausgewählter, einzelner Dateien operativ durchzuführen.

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

Als Einflussfaktor (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) ist zu beachten:

- Kenntnisse der Benutzer: Die Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der Benutzer entscheiden darüber, ob die Datensicherung eigenverantwortlich je Benutzer durchgeführt werden sollte. Sind die Kenntnisse der Benutzer nicht ausreichend, ist die Verantwortung dem Systemadministrator oder einer speziell ausgebildeten Person zu übertragen.

Aufbewahrungsort

Grundsätzlich sollten Datensicherungsmedien und Originaldatenträger in unterschiedlichen Brandabschnitten aufbewahrt werden (siehe CON.3.M12 *Geeignete Aufbewahrung der Backup-Datenträger*). Je weiter entfernt jedoch die Datenträger lagern, desto länger können die Transportwege und damit die Transportzeiten sein, und desto länger dauert die Wiederherstellung. Als Einflussfaktoren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) sind daher zu betrachten:

- Verfügbarkeitsanforderungen: Je höher die Verfügbarkeitsanforderungen sind, umso schneller müssen die Datenträger der Datensicherung verfügbar sein. Werden die Datenträger extern ausgelagert, so ist bei sehr hohen Verfügbarkeitsanforderungen zu erwägen, Kopien der Datensicherung zusätzlich in unmittelbarer Nähe vorzuhalten.
- Vertraulichkeits- und Integritätsbedarf der Daten: Je höher dieser Bedarf ist, umso besser muss verhindert werden, dass an den Datenträgern manipuliert werden kann. Die notwendige

Zutrittskontrolle lässt sich durch entsprechende infrastrukturelle und organisatorische Maßnahmen erreichen.

- Datenvolumen: Mit steigendem Datenvolumen ist die Sicherheit des Aufbewahrungsortes zunehmend wichtig.

Anforderungen an das Datensicherungsarchiv

Datensicherungen besitzen 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 Sicherheitsmaßnahmen notwendig, z. B. eine Zutrittskontrolle.

Zusätzlich muss durch organisatorische und personelle Maßnahmen (Datenträgerverwaltung) sichergestellt werden, dass der schnelle und gezielte Zugriff auf benötigte Datenträger möglich ist. Hierzu ist der Baustein OPS.1.2.2 *Archivierung* zu beachten.

Folgende Einflussfaktoren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*) müssen beachtet werden:

- Verfügbarkeitsanforderungen: Je höher die Verfügbarkeitsanforderungen sind, umso schneller muss der gezielte Zugriff auf benötigte Datenträger möglich sein. Wenn eine manuelle Bestandsführung den Verfügbarkeitsanforderungen nicht genügt, können automatisierte Zugriffsverfahren eingesetzt werden.
- Datenvolumen: Das Datenvolumen bestimmt letztendlich die Art und die Anzahl der aufzubewahrenden Datenträger bzw. die Größe des Online-Speichers. Für entsprechend große Datenvolumen ist eine ausreichende Aufbewahrungskapazität im Datenträgerarchiv vorzusehen.
- Fristen: Sind Löschungsfristen einzuhalten, muss die Organisation des Datensicherungsarchivs sicherstellen, dass die Daten zu den vorgegebenen Zeitpunkten gelöscht werden. Der Vorgang ist zu dokumentieren.
- Vertraulichkeits- und Integritätsbedarf der Daten: Je höher dieser Bedarf ist, umso sorgfältiger muss verhindert werden, dass an den Datenträgern manipuliert werden kann. Die notwendige Zutrittskontrolle lässt sich durch entsprechende infrastrukturelle und organisatorische Maßnahmen erreichen.

Transportmodalitäten

Während einer Datensicherung werden Daten transportiert. Sei es, dass sie über ein Netz übertragen werden, sei es, dass Datenträger zum Datenträgerarchiv transportiert werden. Dabei gilt es folgendes zu beachten:

- Verfügbarkeitsanforderungen: Je höher die Verfügbarkeitsanforderungen sind, desto schneller müssen die Daten zur Wiederherstellung verfügbar sein. Das ist bei der Auswahl des Datenübertragungsmediums bzw. bei Auswahl des Datenträger-Transportweges zu berücksichtigen.
- Datenvolumen: Wenn zur Wiederherstellung die Daten über ein Netz übertragen werden, muss die Übertragungskapazität des Netzes beachtet werden. Es muss gewährleistet sein, dass das Datenvolumen innerhalb der erforderlichen Zeit (Verfügbarkeitsanforderung) übertragen werden kann.
- Änderungszeitpunkte der Daten: Werden Datensicherungen über ein Netz durchgeführt (insbesondere zu ausgewählten Terminen), kann aufgrund des zu übertragenden Datenvolumens ein Kapazitätsengpass entstehen. Daher ist zum Zeitpunkt der Datensicherung eine ausreichende Datenübertragungskapazität sicherzustellen.
- Vertraulichkeits- und Integritätsbedarf der Daten: Je höher dieser Bedarf ist, umso sorgfältiger muss verhindert werden, dass die Daten auf dem Transport abgehört, unbefugt kopiert oder

manipuliert werden. Bei Datenübertragungen ist schließlich eine Verschlüsselung oder ein kryptografischer Manipulationsschutz zu bedenken. Beim physischen Transport sind sichere Behältnisse und Wege zu benutzen und eventuell auch Nutzen und Aufwand einer Verschlüsselung abzuwägen.

Aufbewahrungsmodalität

Im Rahmen des Datensicherungskonzeptes (siehe CON.3.M6 *Entwicklung eines Datensicherungskonzepts*) sollte mit betrachtet werden, ob für bestimmte Daten Aufbewahrungs- oder Löschfristen einzuhalten sind.

- Fristen: Falls Aufbewahrungsfristen einzuhalten sind, sollten die Daten archiviert werden (siehe OPS.1.2.2 *Archivierung*). Falls Löschfristen einzuhalten sind, müssen der organisatorische Ablauf festgelegt und die technischen Voraussetzungen geschaffen werden, damit die Daten zu den vorgegebenen Zeitpunkten gelöscht werden können.

CON.3.M3 ENTFALLEN (B)

Die zugehörige Anforderung ist entfallen.

CON.3.M4 Erstellung von Datensicherungsplänen (B)

Der IT-Betrieb muss Datensicherungspläne je IT-System oder Gruppe von IT-Systemen auf Basis der festgelegten Verfahrensweise für die Datensicherung erstellen. Diese müssen festlegen, welche Anforderungen für die Datensicherung mindestens einzuhalten sind. Die Datensicherungpläne müssen mindestens eine kurze Beschreibung dazu enthalten:

- welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,
- in welcher Reihenfolge IT-Systeme und Anwendungen wiederhergestellt werden,
- wie die Datensicherungen erstellt und wiederhergestellt werden können,
- wie lange Datensicherungen aufbewahrt werden,
- wie die Datensicherungen vor unbefugtem Zugriff und Veränderungen gesichert werden,
- welche Parameter zu wählen sind sowie
- welche Hard- und Software eingesetzt wird.

CON.3.M5 Regelmäßige Datensicherung (B)

Nach den Vorarbeiten und der Grundkonzeption müssen mit der gewählten Vorgehensweise regelmäßige Datensicherungen durchgeführt werden.

Es müssen mindestens regelmäßig Datensicherungen anhand der Datensicherungspläne durchgeführt werden. Empfehlenswert ist die Erstellung eines Datensicherungskonzepts (siehe CON.3.M6 *Entwicklung eines Datensicherungskonzepts*).

Abhängig von der Menge und Wichtigkeit der laufend neu gespeicherten Daten und vom möglichen Schaden bei Verlust dieser Daten ist Folgendes festzulegen:

- Zeitintervall
    - Beispiel: täglich, wöchentlich, monatlich
- Zeitpunkt
    - Beispiel: nachts, freitags abends
- Anzahl der aufzubewahrenden Generationen
    - Beispiel: Bei täglicher Komplettsicherung werden die letzten sieben Sicherungen aufbewahrt, außerdem die Freitag-Abend-Sicherungen der letzten zwei Monate.

- Umfang der zu sichernden Daten
    - Am einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden. Eine geeignete Differenzierung kann die Übersichtlichkeit vergrößern sowie helfen, Aufwand und Kosten zu sparen.
    - Beispiel: selbst erstellte Dateien und individuelle Konfigurationsdateien
- Speichermedien (abhängig von der Datenmenge)
    - Beispiel: DVDs, USB-Speicher oder Festplatten
- Vorherige Löschung der Datenträger vor Wiederverwendung
    - Beispiel: bei Festplatten, bei mobilen Datenträgern
- Zuständigkeit für die Durchführung
    - Beispiel: Administrator, Benutzer
- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung
    - Beispiel: Fehlermeldungen, verbleibender Platz auf den Speichermedien
- Dokumentation der erstellten Sicherungen
    - Beispiel: Datum, Art der Durchführung der Sicherung sowie gewählte Parameter, Beschriftung der Datenträger

Wegen des großen Aufwands können Komplettsicherungen in der Regel höchstens einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wieder eingespielt werden. Daher und zur Senkung der Kosten sollten zwischen den Komplettsicherungen regelmäßig differenzielle oder inkrementelle Sicherungen durchgeführt werden. Hinweise zu den verschiedenen Arten von Datensicherungen finden sich in CON.3.M2 *Festlegung der Verfahrensweise für die Datensicherung*.

Eine differenzielle oder inkrementelle Sicherung kann häufiger erfolgen, zum Beispiel sofort nach Erstellung wichtiger Dateien oder mehrmals täglich. Die Vereinbarkeit mit dem laufenden Betrieb ist sicherzustellen.

Für eingesetzte Software ist separat zu entscheiden, ob sie von der regelmäßigen Datensicherung erfasst werden muss. Dies hängt beispielsweise davon ab, wie aufwändig eine Neuinstallation und das Einspielen von Patches und Updates ist. Unter Umständen ist es ausreichend, Sicherungskopien von den Originaldatenträgern anzufertigen (siehe CON.3.M11 *Sicherungskopie der eingesetzten Software*).

Alle betroffenen Benutzer sollten über die Regelungen zur Datensicherung informiert sein (siehe CON.3.M10 *Verpflichtung der Mitarbeiter zur Datensicherung*).

Falls bei vernetzten IT-Systemen nur die Datenträger der Server gesichert werden, ist sicherzustellen, dass die zu sichernden Daten regelmäßig von den Benutzern oder automatisch dorthin überspielt werden. Bei größeren Änderungen an IT-Systemen oder im Informationsverbund muss der Datensicherungsprozess entsprechend angepasst werden.

Vertrauliche Daten sollten vor der Sicherung möglichst verschlüsselt werden, wobei darauf zu achten ist, dass eine Entschlüsselung auch nach einem längeren Zeitraum möglich sein muss (siehe CON.3.M13 *Einsatz kryptografischer Verfahren bei der Datensicherung*).

Der Ausdruck von Daten auf Papier ist keine angemessene Art der Datensicherung.

CON.3.M6 Entwicklung eines Datensicherungskonzepts (S)

Die Verfahrensweise der Datensicherung wird von einer großen Zahl von Einflussfaktoren bestimmt: Das IT-System, das Datenvolumen, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Im Datensicherungskonzept gilt es, eine

Lösung zu finden, die diese Faktoren berücksichtigt und gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist.

Die technischen Möglichkeiten, Datensicherungen durchzuführen, sind vielfältig. Jedoch wird die Auswahl immer von den genannten Faktoren bestimmt. Daher gilt es zunächst, die Einflussgrößen der IT-Systeme und der damit realisierten IT-Anwendungen zu bestimmen und nachvollziehbar zu dokumentieren (siehe CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung)*. Anschließend muss die geeignete Verfahrensweise entwickelt und dokumentiert werden (siehe CON.3.M2 *Festlegung der Verfahrensweise für die Datensicherung*). Zum Abschluss muss durch die Institutionsleitung die Durchführung angeordnet werden. Auch muss das Datensicherungskonzept regelmäßige Funktionstest für Datensicherung vorsehen (siehe CON.3.M9 *Funktionstests und Überprüfung der Wiederherstellbarkeit*)

Die Ergebnisse sollten aktualisierbar und erweiterbar in einem Datensicherungskonzept niedergelegt werden. Ein möglicher Aufbau eines Datensicherungskonzepts ist im nachfolgenden Inhaltsverzeichnis beispielhaft aufgezeigt:

Inhaltsverzeichnis Datensicherungskonzept

1. Definitionen

- Anwendungsdaten, Systemdaten, Software, Protokolldaten
- Vollsicherung, inkrementelle Datensicherung

2. Gefährdungslage (zur Motivation)

- Abhängigkeit der Institution vom Datenbestand
- Typische Gefährdungen wie ungeschulte Benutzer, gemeinsam genutzte Datenbestände, Schadsoftware, Angreifer, Stromausfall, Festplattenfehler
- Institutionsrelevante Schadensursachen
- Schadensfälle im eigenen Haus

3. Einflussfaktoren je IT-System

- Spezifikation der zu sichernden Daten
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen
- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der Benutzer

4. Datensicherungsplan je IT-System (Alternativ kann ein Datensicherungsplan auch je Prozess bzw. Fachverfahren oder Anwendung erstellt werden)

- Art der Datensicherung (inklusive zu sichernde Daten)
    - Datenart
    - Verzeichnisse
    - Dateieigenschaften

- Häufigkeit und Zeitpunkt der Datensicherung
- Anzahl der Generationen
- Datensicherungsmedium
- Zuständigkeit für die Datensicherung
- Aufbewahrungsort der Backup-Datenträger
- Anforderungen an das Datensicherungsarchiv
- Transportmodalitäten
- Wiederherstellungszeiten bei vorhandener Datensicherung
- Randbedingungen für das Datensicherungsarchiv
- Vertragsgestaltung (bei externen Archiven)
- Refresh-Zyklen der Datensicherung
- Bestandsverzeichnis
- Löschen von Datensicherungen
- Vernichtung von unbrauchbaren Datenträgern
- Vorhalten von arbeitsfähigen Lesegeräten

5. Verpflichtung der Mitarbeiter zur Datensicherung

6. Sporadische Restaurierungsübungen

Einzelne Punkte dieses Datensicherungskonzepts werden in den Maßnahmen CON.3.M1 *Erhebung der Einflussfaktoren der Datensicherung*, CON.3.M2 *Festlegung der Verfahrensweise für die Datensicherung*, CON.3.M8 *Funktionstests und Überprüfung der Wiederherstellbarkeit* und CON.3.M10 *Verpflichtung der Mitarbeiter zur Datensicherung* näher ausgeführt.

7. relevante Ergebnisse des Notfallmanagements/BCM, insbesondere die Recovery Point Objective (RPO) je IT-System oder Gruppe von IT-Systemen

Wurde im Rahmen des BCM bereits eine Business-Impact-Analyse durchgeführt, dann wurde bereits für alle zeitkritischen Geschäftsprozesse analysiert, welche Ressourcen für einen Notfall benötigt werden und wie alt die Daten zum Weiterarbeiten maximal sein dürfen, beziehungsweise was für ein Datenverlust maximal erlaubt wird. Diese Information wird auch als RPO (Recovery Point Objective) bezeichnet und wird für jede IT-Ressource und für allgemeine Informationen (auch in analoger Form) der zeitkritischen Geschäftsprozesse erhoben.

Die RPO kann dabei als direkte Anforderung für das Datensicherungskonzept gesehen werden und hieraus können unmittelbar die Intervalle der Datensicherung abgeleitet werden.

CON.3.M7 Beschaffung eines geeigneten Datensicherungssystems (S)

Bei der Beschaffung eines Datensicherungssystems sollte nicht allein auf seine Leistungsfähigkeit geachtet werden, sondern auch auf die Bedienbarkeit und insbesondere auf seine Toleranz gegenüber Benutzerfehlern.

Die Sicherungssoftware sollte folgende Anforderungen erfüllen:

- Die Datensicherungssoftware sollte ein falsches oder ein beschädigtes Medium im Sicherungslaufwerk erkennen können.
- Sie sollte mit der vorhandenen Hardware problemlos zusammenarbeiten.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.

- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren. Die Durchführung von Datensicherungen inklusive des Sicherungsergebnisses und möglicher Fehlermeldungen sollten in einer Protokolldatei abgespeichert werden.
- Die Sicherungssoftware sollte die Sicherung des Backup-Mediums durch ein Passwort oder noch besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.
- Es sollte möglich sein, die zu sichernden Daten abhängig vom Erstellungsdatum bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte logische und physische Vollkopien sowie inkrementelle Kopien (Änderungssicherungen) erzeugen können.
- Die zu sichernden Daten sollten auch auf Netzlaufwerken oder in Online-Datenspeichern abgespeichert werden können.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.
- Bei der Wiederherstellung von Dateien sollte es möglich sein auszuwählen, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, dass Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte man wählen können, ob diese Datei immer, nie oder nur in dem Fall, dass sie älter als die zu rekonstruierende Datei ist, überschrieben wird, oder dass in diesem Fall eine explizite Anfrage erfolgt.

Falls mit dem eingesetzten Programm die Datensicherung durch Passwort geschützt werden kann, sollte diese Option genutzt werden. Das Passwort ist dann gesichert zu hinterlegen.

Bei den meisten Betriebssystemen werden Programme für Datensicherungen mitgeliefert. Diese bieten häufig den Vorteil, dass sie komfortabel in das System integriert sind und auf Software-Ebene selten Inkompatibilitäten auftreten.

Unabhängig davon, ob in Betriebssystemen integrierte Datensicherungssysteme eingesetzt werden oder Lösungen von Drittherstellern, sollte die eingesetzte Lösung die Anforderungen erfüllen. Der Baustein APP.6 *Allgemeine Software* beschreibt für Softwarelösungen entsprechende Anforderungen von der Anforderungsanalyse bis hin zu Außerbetriebnahme und muss daher für diese Lösungen zusätzlich betrachtet werden.

CON.3.M8 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

CON.3.M9 Voraussetzungen für die Online-Datensicherung (S)

Diese Maßnahme und die damit verbundene Anforderung aus dem Baustein beziehen sich auf Online-Datensicherungen, die in einer Cloud-Konstellation eingesetzt werden, in der die Online-Lösung durch einen Dritten betrieben wird. Daher sollte in diesem Fall auch immer der Baustein OPS.2.2 *Cloud-Nutzung* berücksichtigt werden.

Die Erstellung einer Datensicherung mithilfe eines Online-Speicher-Dienstes wird in der Regel über eine entsprechende Anwendung auf dem Client eines Benutzers oder auf einem Server der Institution

initiiert. Auch möglich ist z. B. ein hybrides Modell durch eine Appliance: Hier werden die Daten lokal auf der Appliance und zusätzlich in einem Online-Speicher-Dienst vorgehalten. In allen Fällen werden die zu sichernden Daten über das Internet von einem IT-System innerhalb der Institution auf einen Server des Online-Speicher-Anbieters übertragen.

Je nach Anbieter kann der Umgang mit den übertragenen Daten dabei variieren. Ein Großteil der Anbieter unterstützt beispielsweise die Speicherung und Wiederherstellung unterschiedlicher Versionen einer zu übertragenden Datei. Bietet der Online-Speicher-Anbieter hingegen keine Versionierung von Dateien an, wird die ältere Datei ohne zusätzliche Rückfrage überschrieben und ist damit nicht mehr für eine Rücksicherung verfügbar. In diesem Fall erfüllt der Online-Speicher jedoch nicht die Anforderungen, die an eine Datensicherung im Unternehmens- oder Behördenumfeld gestellt werden. Institutionen sollten daher insbesondere auf die vorhandene Versionierung der Daten achten, um dem unerwünschten Löschen älterer Datenversionen vorzubeugen.

Grundsätzlich sollten immer die Fragen im Vordergrund stehen, welchen Schutzbedarf die gesicherten Daten haben, welchen gesetzlichen Verpflichtungen hinsichtlich der geschäftsrelevanten Daten eine Institution unterliegt und wie es sich auswirkt, wenn Daten verloren gehen oder durch Unbefugte verändert werden.

Viele Anbieter von Online-Speicher-Diensten sind sich durchaus bewusst, dass Institutionen großen Wert auf die Verfügbarkeit ihrer Daten legen und halten die Daten ihrer Kunden redundant vor. Institutionen sollten darauf achten, dass der Anbieter die Daten an unterschiedlichen Standorten bzw. in räumlich voneinander getrennten Rechenzentren speichert. Kommt es zu Problemen in einem Rechenzentrum, stehen die Daten in diesem Fall dennoch weiterhin in einem anderen Rechenzentrum zur Verfügung.

Unternehmen und Behörden sollten nicht nur Wert auf die sichere Speicherung ihrer Daten legen, sondern darüber hinaus auch die Umsetzung der Zugriffsmöglichkeiten auf die angelegten Benutzerkonten hinterfragen. Im Unternehmens- und Behördenumfeld sind gezielte Angriffe vorstellbar, deren Absicht darin liegt, dass die entsprechenden Benutzerkonten gesperrt werden. Auf diesem Weg wird der Zugriff auf das Backup der Daten verhindert.

Nicht nur Vollständigkeit und Verfügbarkeit ihrer gesicherten Daten interessieren Institutionen, vielmehr legen sie, unter anderem zur Vermeidung rechtlicher Konsequenzen oder eines Imageverlustes, auch großen Wert auf deren Vertraulichkeit und Integrität. Institutionen sollten daher Verschlüsselungsverfahren einsetzen, um das Sicherheitsniveau bei der Übermittlung und der Datenspeicherung bei externen Dienstleistern zu erhöhen.

Viele Anbieter von Online-Speicher-Lösungen werben mit der erhöhten Sicherheit durch Verschlüsselung. Hier muss jedoch genauer analysiert werden, wie die Verschlüsselung konkret umgesetzt ist. In der Regel erfolgt nämlich lediglich die eigentliche Übertragung der Daten verschlüsselt, etwa über den Aufbau einer https-Verbindung (Hyper Text Transfer Protocol Secure). Vor und nach dem Transport liegen die Daten jedoch unverschlüsselt im Klartext vor. Einige Anbieter stellen ihren Kunden, unabhängig vom Transportweg der Daten, zusätzliche Verschlüsselungsmethoden zur Verfügung. Allerdings kann die Institution dabei oft nicht ausschließen, dass sich ein Innentäter, also ein Mitarbeiter des Online-Speicher-Anbieters, die entsprechenden Schlüssel verschafft und damit auch auf die verschlüsselten Informationen zugreifen, diese verfälschen oder veröffentlichen kann. Erlangt ein Angreifer Zugriff auf die Daten, indem er die Authentisierung kompromittiert, dann ist die Verschlüsselung beim Anbieter ebenfalls wirkungslos.

Sehen Institutionen ihre Daten also als besonders schützenswert an, sollten sie diese bereits auf ihren eigenen Systemen und damit vor dem eigentlichen Datentransfer verschlüsseln.

Das Bedürfnis nach einer sicheren Methode zur Nutzung von Online-Speicher-Lösungen, gerade im Behörden- oder Unternehmensumfeld, wird vom Markt jedoch zunehmend aufgegriffen. So hat sich mittlerweile eine Reihe von Verschlüsselungslösungen etabliert, die größtenteils speziell auf die Zusammenarbeit mit Online-Speicher-Diensten abgestimmt sind. Die Programme überprüfen bereits bei der Installation, ob ein passender Ordner eines Online-Speichers existiert, und erzeugen anschließend einen entsprechenden Unterordner, in dem die verschlüsselten Dateien abgelegt werden.

Institutionen, die zusätzliche Verschlüsselungssoftware einsetzen, sollten darauf achten, dass für die Anwendung ein ausreichend starkes Passwort oder anderer Zugriffsschutz gewählt wird. Zudem sollten eine Kopie der eingesetzten Softwarelösung und der zugehörigen kryptografischen Schlüssel an einem sicheren Ort hinterlegt werden, um im Falle eines vollständigen Datenverlustes innerhalb der Institution noch auf die verschlüsselten Datensicherungen des Online-Speichers zugreifen zu können. Zu diesem Zweck kann die Verschlüsselungssoftware unverschlüsselt beim Online-Speicher-Dienst gesichert werden, der Schlüssel muss selbstverständlich anders gesichert werden. Auf diesem Weg ist die Institution unabhängig davon, ob die Verschlüsselungssoftware auch nach einem längeren Zeitraum noch in einer kompatiblen Version zur Verfügung steht.

Institutionen sollten sich zudem davon überzeugen, dass die Wiederherstellung der gespeicherten Daten vom Online-Speicher fehlerfrei funktioniert, und sollten dies darüber hinaus regelmäßig testen (siehe CON.3.A8 *Funktionstests und Überprüfung der Wiederherstellbarkeit*).

CON.3.M10 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

CON.3.M11 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

CON.3.M12 Sichere Aufbewahrung der Speichermedien für die Datensicherungen (B)

Speichermedien für die Datensicherungen unterliegen besonderen Anforderungen hinsichtlich ihrer Aufbewahrung:

- Der Zugriff auf diese Speichermedien darf nur befugten Personen möglich sein.
- Ein ausreichend schneller Zugriff muss im Bedarfsfall gewährleistet sein.
- Der Aufbewahrungsort muss auch die klimatischen Bedingungen für eine längerfristige Aufbewahrung von Speichermedien gewährleisten.
- Die Speichermedien müssen räumlich getrennt vom gesicherten IT-System aufbewahrt werden, wenn möglich in einem anderen Brandabschnitt.

CON.3.M13 Einsatz kryptografischer Verfahren bei der Datensicherung (H)

Der Vertraulichkeitsbedarf der gesicherten Daten innerhalb einer Datensicherung sollte stets berücksichtigt werden. Hierbei sollte beachtet werden, dass durch die Aggregation der vielen gesicherten Daten in einer Datensicherung bzw. auf einem Datenträger der Schutzbedarf der Datensicherung sogar über den einzelnen Schutzbedarfen der gesicherten Daten liegen kann. Andererseits, wird je nach technischer Implementation der Datensicherung, die Datensicherung über verschiedene Datenträger verteilt, sodass ein Verteilungseffekt auftreten kann.

Daher sollte bei einem erhöhten Schutzbedarf der Daten die Datensicherung verschlüsselt werden. Für die Datensicherungen müssen geeignete Verschlüsselungsverfahren ausgewählt werden. Das entscheidende Merkmal eines Verschlüsselungsverfahrens ist die Güte des Algorithmus sowie der Schlüsselauswahl. Da die Sicherheitseignung der Verschlüsselungsverfahren durch die technische Entwicklung von Hard- und Software sowie Fortschritte in der Kryptografie beschränkt wird, müssen sie regelmäßig nach dem Stand der Technik aktualisiert werden.

Auch muss sichergestellt sein, dass die Schlüssel geeignet verwaltet werden.

Weitere Hinweise zu kryptografischen Verfahren finden sich im Baustein CON.1 *Kryptokonzept*.

CON.3.M14 Schutz von Datensicherungen (B)

Die erstellten Datensicherungen können für die Institution eine überlebenswichtige Ressource darstellen, wenn die Ursprungssysteme ausfallen und von einem Datenverlust betroffen sind. Hierbei ist es unerheblich, ob ein solcher Datenverlust durch einen technischen Defekt, einen menschlichen

Fehler oder einen Angriff ausgelöst wurde. Daher müssen die Speichermedien für die Datensicherung in geeigneter Weise vor unbefugtem Zugriff geschützt werden. Hierbei muss insbesondere sichergestellt werden, dass Datensicherungen nicht absichtlich oder unbeabsichtigt überschrieben werden können. Die kann grundsätzlich über zwei Wege umgesetzt werden:

1. IT-Systeme, die für die Datensicherung eingesetzt werden, sollten einen schreibenden Zugriff auf die Speichermedien für die Datensicherung nur für autorisierte Datensicherungen oder autorisierte Administrationstätigkeiten gestatten. Diese Möglichkeit bietet sich in Netzspeichern oder komplexeren vernetzten Datensicherungsystemen an. Hierbei ist entscheidend, dass tatsächlich kein unbeabsichtiges Überschreiben oder Löschen der Speichermedien für die Datensicherung möglich ist.
2. Alternativ sollten die Speichermedien für die Datensicherung nur für autorisierte Datensicherungen oder autorisierte Administrationstätigkeiten mit den entsprechenden IT-Systemen verbunden werden. Dies bietet sich insbesondere bei kleineren Datensicherungslösungen an, wo die Datensicherung z. B. auf ein externes Laufwerk oder einen optischen Datenträger gesichert werden.

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

Für den Umsetzungshinweis CON.3 *Datensicherungskonzept* sind keine Quellenverweise vorhanden.