CON: Konzepte und Vorgehensweisen

CON.3: Datensicherungskonzept

1 Beschreibung

1.1 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 sowohl 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 im Rahmen dieses Bausteins alle möglichen Arten und Formen von IT-Komponenten, die schützenswerte Informationen speichern.

Durch regelmäßige Datensicherungen lassen sich Auswirkungen von Datenverlusten jedoch minimieren. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der Betrieb der Informationstechnik kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

1.2 Zielsetzung

Dieser Baustein zeigt auf, wie Institutionen ein Datensicherungskonzept erstellen können und welche Anforderungen dabei zu beachten sind.

1.3 Abgrenzung und Modellierung

Der Baustein CON.3 *Datensicherungskonzept* ist auf den Informationsverbund einmal anzuwenden.

Der Baustein beschreibt grundsätzliche Anforderungen, die zu einem angemessenen Datensicherungskonzept beitragen. Nicht behandelt werden Anforderungen an die Aufbewahrung und Erhaltung von elektronischen Dokumenten für die Langzeitspeicherung. Diese finden sich im Baustein OPS.1.2.2 *Archivierung*.

Dieser Baustein behandelt auch keine systemspezifischen und anwendungsspezifischen Eigenschaften von Datensicherungen. Die systemspezifischen und anwendungsspezifischen Anforderungen an das Datensicherungskonzept werden in den entsprechenden Bausteinen der Schichten NET *Netze und Kommunikation*, SYS *IT-Systeme* und APP *Anwendungen* ergänzt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein CON.3 *Datensicherungskonzept* von besonderer Bedeutung:

2.1 Fehlende Datensicherung

Wenn Daten verloren gehen und sie nicht vorher gesichert wurden, kann das existenzbedrohende Folgen für die Institution haben. Daten können z. B. durch Malware, technische Fehlfunktionen oder einen Brand verloren gehen, aber auch, wenn Mitarbeiter Daten absichtlich oder unabsichtlich löschen. Wenn zum Beispiel die Daten eines E-Mail-Servers nicht gesichert wurden, kann der Geschäftsbetrieb nach Verlust dieser Daten nicht mehr effektiv und nur mit großen Einschränkungen wieder aufgenommen werden.

2.2 Fehlende Wiederherstellungstests

Eine regelmäßige Sicherung von Daten gewährleistet nicht automatisch, dass diese Daten auch wiederhergestellt werden können. Wenn nicht regelmäßig getestet wird, ob sich Daten wiederherstellen lassen, kann es sein, dass die gesicherten Daten im Fall einer notwendigen Wiederherstellung nicht nutzbar sind.

2.3 Ungeeignete Aufbewahrung der Datenträger von Datensicherungen

Auf Datenträgern mit Datensicherungen befinden sich zahlreiche schützenswerte Informationen der Institution. Sind die Datenträger an einem unsicheren Ort aufbewahrt, kann ein Angreifer (z. B. ein Innentäter), eventuell darauf zugreifen und schützenswerte Informationen stehlen oder manipulieren. Ebenso können Datenträger mit Datensicherungen durch ungünstige Lagerung oder klimatische Raumbedingungen unbrauchbar werden. Dann sind die auf ihnen abgespeicherten Informationen nicht mehr verfügbar, wenn sie benötigt werden.

2.4 Fehlende oder unzureichende Dokumentation

Werden Datensicherungsmaßnahmen nicht oder nur mangelhaft dokumentiert, kann es länger als geplant dauern, sie wiederherzustellen. Dadurch können sich wichtige Prozesse verzögern, z. B. in der Produktion. Auch ist es möglich, dass sich eine Datensicherung gar nicht mehr einspielen lässt und die Daten damit verloren sind.

2.5 Missachtung gesetzlicher Vorschriften

Wenn bei der Datensicherung gesetzliche Vorgaben, wie Datenschutzgesetze, nicht beachtet werden, können gegen die Institution Bußgelder verhängt oder Schadenersatzansprüche geltend gemacht werden.

2.6 Unsichere Cloud-Anbieter für Online-Datensicherungen

Lagern Institutionen ihre Datensicherung online zu einem Cloud-Anbieter aus, können Angriffe auf den Cloud-Anbieter auch die Datensicherung der Institution betreffen. In der Folge kann dies dazu führen, dass schützenswerte Daten abfließen.

Des Weiteren besteht die Gefahr, dass die Datensicherung nicht mehr kurzfristig verfügbar ist. Im Notfall kann die Wiederherstellung dann nicht in der festgelegten Zeit durchgeführt werden.

2.7 Ungenügende Speicherkapazitäten

Die Menge an verarbeiteten und damit auch gespeicherten Daten nimmt stetig zu. Verfügen die Datenträger für Datensicherungen nicht über genügend freien Speicher, werden aktuellere Daten eventuell nicht mehr gesichert. Auch kann es sein, dass die eingesetzte Datensicherungssoftware automatisch alte und möglicherweise noch benötigte Datensicherungen überschreibt. Werden die Verantwortlichen darüber nicht informiert, weil z. B. das Monitoring unzureichend ist, gehen Daten eventuell ganz verloren. Es könnte auch sein, dass im Notfall nur die falschen Versionen verfügbar sind.

2.8 Unzureichendes Datensicherungskonzept

Wird für Datensicherungsmaßnahmen kein angemessenes Datensicherungskonzept erstellt und

befolgt, könnten gesicherte Daten bei Bedarf nicht wiederhergestellt werden. Wird beispielsweise die Datensicherung verschlüsselt und ist bei einem Datenverlust auch der Schlüssel zum Entschlüsseln der Datensicherung betroffen, können die Daten nicht wieder hergestellt werden. Das könnte dann der Fall sein, wenn nicht daran gedacht wurde, den Schlüssel getrennt aufzubewahren.

3 Anforderungen

Im Folgenden sind die spezifische Anforderungen des Bausteins CON.3 *Datensicherungskonzept* aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	Informationssicherheitsbeauftragter (ISB)
Weitere Zuständigkeiten	Fachverantwortliche, IT-Betrieb

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein CON.3 *Datensicherungskonzept* vorrangig erfüllt werden:

CON.3.A1 Erhebung der Einflussfaktoren für Datensicherungen [Fachverantwortliche, IT-Betrieb] (B)

Der IT-Betrieb MUSS für jedes IT-System und darauf ausgeführten Anwendungen die Rahmenbedingungen für die Datensicherung erheben. Dazu MUSS der IT-Betrieb die Fachverantwortlichen für die Anwendungen und die Zuständigen für die jeweiligen IT-Systeme befragen. Der IT-Betrieb MUSS mindestens die nachfolgenden Rahmenbedingungen berücksichtigen:

- Speichervolumen,
- Änderungsvolumen,
- Änderungszeitpunkte,
- Verfügbarkeitsanforderungen,
- Integritätsbedarf sowie
- rechtliche Anforderungen.

Die Ergebnisse MÜSSEN nachvollziehbar und auf geeignete Weise festgehalten werden. Neue Anforderungen MÜSSEN zeitnah berücksichtigt werden.

CON.3.A2 Festlegung der Verfahrensweise für die Datensicherung [Fachverantwortliche, IT-Betrieb] (B)

Der IT-Betrieb MUSS für jedes IT-System ein Verfahren festlegen, das definiert, welche Daten des IT-Systems wie gesichert werden. In virtuellen Umgebungen SOLLTE geprüft werden, ob das System durch Snapshot-Mechanismen der Virtualisierungsumgebung gesichert werden kann.

Für die Datensicherungsverfahren MÜSSEN Art, Häufigkeit und Zeitpunkte der Datensicherungen bestimmt werden. Dies MUSS wiederum auf Basis der erhobenen Einflussfaktoren und in Abstimmung mit den jeweiligen Fachverantwortlichen der Anwendungen geschehen. Auch MUSS definiert sein, welche Speichermedien benutzt werden und wie die Transport- und Aufbewahrungsmodalitäten ausgestaltet sein müssen.

CON.3.A3 ENTFALLEN (B)
Diese Anforderung ist entfallen.

CON.3.A4 Erstellung eines Minimaldatensicherungskonzeptes [IT-Betrieb] (B)
Der IT-Betrieb MUSS ein Minimaldatensicherungskonzept auf Basis der festgelegten Verfahrensweise für die Datensicherung erstellen. Dieses MUSS festlegen, welche Anforderungen für die Datensicherung mindestens vom IT-Betrieb einzuhalten sind. Das Minimaldatensicherungskonzept MUSS mindestens eine kurze Beschreibung dazu enthalten,

- welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,
- wie die Datensicherungen erstellt und wiederhergestellt werden können,
- welche Parameter zu wählen sind, sowie
- welche Hard- und Software eingesetzt wird.

CON.3.A5 Regelmäßige Datensicherung [IT-Betrieb] (B)
Der IT-Betrieb MUSS regelmäßige Datensicherungen gemäß dem (Minimal-)Datensicherungskonzept erstellen. Die erstellten Datensicherungen MÜSSEN in geeigneter Weise vor dem Zugriff Dritter geschützt werden. Es MUSS regelmäßig getestet werden, ob die Datensicherungen wie gewünscht funktionieren, vor allem, ob gesicherte Daten problemlos und in angemessener Zeit zurückgespielt werden können.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein CON.3 *Datensicherungskonzept*. Sie SOLLTEN grundsätzlich erfüllt werden.

CON.3.A6 Entwicklung eines Datensicherungskonzepts [Fachverantwortliche, IT-Betrieb] (S)
Der IT-Betrieb SOLLTE ein Datensicherungskonzept auf Basis des Minimaldatensicherungskonzepts erstellen. Dieses SOLLTE mindestens die nachfolgenden Punkte umfassen:

- Definitionen zu wesentlichen Aspekten der Datensicherung (z. B. zu differenzierende Datenarten),
- Gefährdungslage,
- Einflussfaktoren je IT-Systeme,
- Datensicherungsplan je IT-Systeme sowie
- relevante Ergebnisse des Notfallmanagements/BCM, insbesondere die Recovery Point Objective (RPO) je IT-System.

Der IT-Betrieb SOLLTE das Datensicherungskonzept mit den jeweiligen Fachverantwortlichen der betreffenden Anwendungen abstimmen.

Die Mitarbeiter SOLLTEN über den Teil des Datensicherungskonzepts unterrichtet werden, der sie betrifft. Regelmäßig SOLLTE kontrolliert werden, ob das Datensicherungskonzept korrekt umgesetzt wird.

CON.3.A7 Beschaffung eines geeigneten Datensicherungssystems [IT-Betrieb] (S)
Bevor ein Datensicherungssystem beschafft wird, SOLLTE der IT-Betrieb eine Anforderungsliste erstellen, nach der die am Markt erhältlichen Produkte bewertet werden. Die angeschafften Datensicherungssysteme SOLLTEN die Anforderungen des Datensicherungskonzepts und der gesamten Sicherheitskonzeption der Institution erfüllen.

CON.3.A8 ENTFALLEN (S)
Diese Anforderung ist entfallen.

CON.3.A9 Voraussetzungen für die Online-Datensicherung [IT-Betrieb] (S)

Wenn für die Datensicherung ein Online-Speicher genutzt werden soll, SOLLTEN mindestens folgende Punkte geregelt werden:

- Gestaltung des Vertrages,
- Ort der Datenspeicherung,
- Vereinbarungen zur Dienstgüte (SLA), insbesondere in Hinsicht auf die Verfügbarkeit,
- geeignete Authentisierungsmethoden,
- Verschlüsselung der Daten auf dem Online-Speicher sowie
- Verschlüsselung auf dem Transportweg.

CON.3.A10 Verpflichtung der Mitarbeiter zur Datensicherung (S)

Alle Mitarbeiter SOLLTEN über die Regelungen zur Datensicherung informiert sein. Auch SOLLTEN sie darüber informiert werden, welche Aufgaben sie bei der Erstellung von Datensicherungen haben. Die Mitarbeiter SOLLTEN dazu verpflichtet werden, Datensicherungen durchzuführen.

CON.3.A11 Sicherungskopie der eingesetzten Software [IT-Betrieb] (S)

Der IT-Betrieb SOLLTE Sicherungskopien von eingesetzten Softwareprogrammen anfertigen, sofern das rechtlich erlaubt und technisch möglich ist. Dabei SOLLTEN alle notwendigen Pakete und Informationen vorhanden sein, um die Software im Notfall wieder installieren zu können. Auch SOLLTEN die originalen Installationsquellen sowie die Lizenznummern an einem geeigneten Ort sicher aufbewahrt werden.

CON.3.A12 Geeignete Aufbewahrung der Datenträger von Datensicherungen [IT-Betrieb] (S)

Der IT-Betrieb SOLLTE die Datenträger von Datensicherungen geeignet aufbewahren, sodass diese vor unbefugtem Zugriff geschützt werden. Sie SOLLTEN räumlich getrennt von den gesicherten IT-Systemen aufbewahrt werden. Der Aufbewahrungsort SOLLTE so klimatisiert sein, dass die Datenträger entsprechend der zeitlichen Vorgaben des Datensicherungskonzepts aufbewahrt werden können.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein CON.3 *Datensicherungskonzept* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

CON.3.A13 Einsatz kryptografischer Verfahren bei der Datensicherung [IT-Betrieb] (H)

Um die Vertraulichkeit und Integrität der gesicherten Daten zu gewährleisten, SOLLTE der IT-Betrieb alle Datensicherungen verschlüsseln. Es SOLLTE sichergestellt werden, dass sich die verschlüsselten Daten auch nach längerer Zeit wieder einspielen lassen. Verwendete kryptografische Schlüssel SOLLTEN mit einer getrennten Datensicherung geschützt werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Die International Organization for Standardization (ISO) nennt in der Norm ISO/IEC 27002:2013 unter „12.3 Backup“ Anforderungen an ein Datensicherungskonzept.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) hat eine Anleitung zur Durchführung von Datensicherungen in seiner Publikation „Leitfaden Backup / Recovery / Disaster Recovery“ erstellt.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel „SY2.3 Backup“ Vorgaben für Datensicherungen.

Das National Institute of Standards and Technology stellt Anforderungen an Backups in der „CP-9 Information System Backup“ der Veröffentlichung „NIST Special Publication 800-53“ zur Verfügung.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein CON.3 *Datensicherungskonzept* von Bedeutung.

G 0.1	Feuer
G 0.2	Ungünstige klimatische Bedingungen
G 0.18	Fehlplanung oder fehlende Anpassung
G 0.19	Offenlegung schützenswerter Informationen
G 0.22	Manipulation von Informationen
G 0.29	Verstoß gegen Gesetze oder Regelungen
G 0.45	Datenverlust
G 0.46	Integritätsverlust schützenswerter Informationen