Bundesamt
für Sicherheit in der
Informationstechnik

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 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 Baustein 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 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 beispielsweise:

- 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.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, aufzuzeigen, wie Institutionen ein Datensicherungskonzept erstellen können und wie sie anhand dessen ihre Daten angemessen gegen einen Datenverlust absichern können.

1.3. Abgrenzung und Modellierung

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

Für das Löschen und Vernichten von Datensicherungen muss der Baustein CON.6 *Löschen und Vernichten* berücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen 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 eine Institution haben. Daten können z. B. durch Malware, technische Fehlfunktionen oder einen Brand verloren gehen, aber auch, wenn Mitarbeitende Daten absichtlich oder unabsichtlich löschen.

2.2. Fehlende Wiederherstellungstests

Werden Daten regelmäßig gesichert, gewährleistet dies nicht automatisch, dass diese auch problemlos wiederhergestellt werden können. Wenn nicht regelmäßig getestet wird, ob sich Daten wiederherstellen lassen, kann es sein, dass die gesicherten Daten nicht wiederhergestellt werden können.

2.3. Ungeeignete Aufbewahrung der Speichermedien für die Datensicherungen

Auf den Speichermedien für die Datensicherungen befinden sich zahlreiche schützenswerte Informationen der Institution, egal ob es sich um klassische Bänder oder moderne Storage-Systeme handelt. Werden die Speichermedien für die Datensicherungen an einem unsicheren Ort aufbewahrt, kann bei einem Angriff eventuell darauf zugegriffen und schützenswerte Informationen gestohlen oder manipuliert werden. Ebenso können Speichermedien für die Datensicherungen durch ungünstige

Lagerung oder klimatische Raumbedingungen unbrauchbar werden. Dann sind die auf ihnen abgespeicherten Informationen nicht mehr verfügbar.

2.4. Fehlende oder unzureichende Dokumentation

Wenn Datensicherungsmaßnahmen und besonders die Maßnahmen zur Wiederherstellung nicht oder nur mangelhaft dokumentiert sind, kann dies die Wiederherstellung erheblich verzögern. Dadurch können sich in der Folge auch wichtige Prozesse verzögern, z. B. in der Produktion. Zudem ist es möglich, dass sich eine Datensicherung gar nicht mehr einspielen lässt und die Daten damit verloren sind.

Wenn die Information zur Wiederherstellung nur digital vorliegt, besteht die Gefahr, dass diese bei Großschäden (wie Ransomware) ebenfalls verloren geht, und die Wiederherstellung dann gefährdet ist.

2.5. Missachtung gesetzlicher Vorschriften

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

2.6. Unsichere Anbieter für Online-Datensicherungen

Lagern Institutionen ihre Datensicherung online zu einer fremden Institution aus, können Angriffe auf diese auch die Daten der eigenen Institution betreffen. In der Folge kann dies dazu führen, dass schützenswerte Daten abfließen.

Des Weiteren besteht die Gefahr, dass ungünstige vertragliche Konditionen dazu führen, dass Datensicherungen nicht kurzfristig verfügbar sind. Im Notfall können sie nicht in einer definierten Zeitspanne wiederhergestellt werden.

2.7. Ungenügende Speicherkapazitäten

Verfügen Speichermedien für die Datensicherung nicht über genügend freie Kapazität, werden aktuellere Daten eventuell nicht mehr gesichert. Auch kann es sein, dass die eingesetzte Software zur Datensicherung automatisch alte und möglicherweise noch benötigte Datensicherungen überschreibt. Werden die Zuständigen darüber nicht informiert, weil z. B. das Monitoring unzureichend ist, können Daten eventuell ganz verlorengehen. Es wäre zudem möglich, dass im Notfall lediglich veraltete Versionen verfügbar sind.

2.8. Unzureichendes Datensicherungskonzept

Wenn für Datensicherungsmaßnahmen kein angemessenes Konzept erstellt wird, könnten die fachlichen Anforderungen an die betroffenen Geschäftsprozesse unberücksichtigt bleiben. Werden beispielsweise die Wiederherstellungszeit oder die Datensicherungsintervalle nicht beachtet, könnte dies dazu führen, dass die Datensicherungen bei einem Datenverlust nicht dazu geeignet sind, die verlorenen Daten in angemessener Weise wiederherzustellen.

Zudem kann ein Speichermedium für eine Datensicherung selbst zu einem bevorzugten Angriffsziel werden, wenn konzentriert wertvolle Daten aus allen Geschäftsprozessen der Institution darauf gespeichert werden.

Darüber hinaus können organisatorische Mängel dazu führen, dass die Datensicherung unbrauchbar wird. Wird diese beispielsweise verschlüsselt, und ist bei einem Datenverlust auch der Schlüssel zum Entschlüsseln der Datensicherung betroffen, können die Daten nicht wiederhergestellt werden. Das könnte dann der Fall sein, wenn nicht daran gedacht wurde, den Schlüssel getrennt aufzubewahren.

2.9. Ungenügende Datensicherungsgeschwindigkeit

Neben dem benötigten Speicherplatz für die Datensicherung steigt auch die Zeit, die benötigt wird, um eine Datensicherung durchzuführen. Dies kann im ungünstigsten Fall dazu führen, dass eine Datensicherung noch nicht beendet ist, wenn eine neue Datensicherung beginnt. Hieraus können wiederum unterschiedliche Probleme folgen. Unter Umständen wird die noch nicht abgeschlossene Datensicherung beendet. Somit würden fortan keine vollständigen Datensicherungen mehr angefertigt. Alternativ könnte die Datensicherungslösung versuchen, parallel die neue Datensicherung zusammen mit der alten durchzuführen. In der Folge könnte dies dazu führen, dass das Datensicherungssystem am Ende unter der zunehmenden Last ausfällt.

2.10. Ransomware

Eine spezielle Form von Schadprogrammen ist Ransomware, bei der Daten auf den infizierten IT-Systemen verschlüsselt werden. Nach der Verschlüsselung wird ein Lösegeld gefordert, damit das Opfer die Daten wieder entschlüsseln kann. Ohne Datensicherungen sind die verschlüsselten Daten in vielen Fällen verloren oder können nur durch das geforderte Lösegeld freigekauft werden. Es ist jedoch auch nach der Zahlung eines Lösegelds nicht gewährleistet, dass die Daten wiederhergestellt werden können.

Viele Ausprägungen von Ransomware suchen nach Netzlaufwerken mit Schreibzugriff, auf denen alle Daten ebenfalls verschlüsselt werden. Damit können alle verschlüsselten Informationen seit der letzten Datensicherung verloren sein, auch wenn ein Lösegeld gezahlt wurde. Nicht nur das ursprünglich infizierte IT-System wäre hiervon betroffen, sondern auch zentral abgelegte Informationen, auf die viele IT-Systeme zugreifen dürfen.

Sind die Speichermedien für die Datensicherung nicht hinreichend abgesichert, dann besteht die zusätzliche Gefahr, dass sie selbst von einem Ransomware-Angriff betroffen sind und die auf ihnen gespeicherten Informationen (Datensicherungen) selbst verschlüsselt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.3 *Datensicherungskonzept* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

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

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

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

Der IT-Betrieb MUSS für jedes IT-System und darauf ausgeführten Anwendungen die Rahmenbedingungen für die Datensicherung erheben. Dazu MÜSSEN die Fachverantwortlichen für die Anwendungen ihre Anforderungen an die Datensicherung definieren. Der IT-Betrieb MUSS mindestens die nachfolgenden Rahmenbedingungen mit den Fachverantwortlichen abstimmen:

- zu sichernde Daten,
- Speichervolumen,
- Änderungsvolumen,
- Änderungszeitpunkte,
- Verfügbarkeitsanforderungen,
- Vertraulichkeitsanforderungen,
- Integritätsbedarf,
- rechtliche Anforderungen,
- Anforderungen an das Löschen und Vernichten der Daten sowie
- Zuständigkeiten für die Datensicherung.

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

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

Der IT-Betrieb MUSS Verfahren festlegen, wie die Daten gesichert werden.

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 geschehen. Auch MUSS definiert sein, welche Speichermedien benutzt werden und wie die Transport- und Aufbewahrungsmodalitäten ausgestaltet sein müssen. Datensicherungen MÜSSEN immer auf separaten Speichermedien für die Datensicherung gespeichert werden. Besonders schützenswerte Speichermedien für die Datensicherung SOLLTEN nur während der Datensicherung und Datenwiederherstellung mit dem Netz der Institution oder dem Ursprungssystem verbunden werden.

In virtuellen Umgebungen sowie für Storage-Systeme SOLLTE geprüft werden, ob das IT-System ergänzend durch Snapshot-Mechanismen gesichert werden kann, um hierdurch mehrere schnell wiederherstellbare Zwischenversionen zwischen den vollständigen Datensicherungen zu erstellen.

CON.3.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

CON.3.A4 Erstellung von Datensicherungsplänen (B) [IT-Betrieb]

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 Datensicherungspläne MÜSSEN mindestens eine kurze Beschreibung dazu enthalten:

- welche IT-Systeme und welche darauf befindlichen Daten durch welche Datensicherung gesichert werden,
- in welcher Reihenfolge IT-System und Anwendungen wiederhergestellt werden,

- wie die Datensicherungen erstellt und wiederhergestellt werden können,
- wie lange Datensicherungen aufbewahrt werden,
- wie die Datensicherungen vor unbefugtem Zugriff und Überschreiben gesichert werden,
- welche Parameter zu wählen sind sowie
- welche Hard- und Software eingesetzt wird.

CON.3.A5 Regelmäßige Datensicherung (B) [IT-Betrieb, Mitarbeitende]

Regelmäßige Datensicherungen MÜSSEN gemäß den Datensicherungsplänen erstellt werden. Alle Mitarbeitenden MÜSSEN über die Regelungen zur Datensicherung informiert sein. Auch MÜSSEN sie darüber informiert werden, welche Aufgaben sie bei der Erstellung von Datensicherungen haben.

CON.3.A12 Sichere Aufbewahrung der Speichermedien für die Datensicherungen (B) [IT-Betrieb]

Die Speichermedien für die Datensicherung MÜSSEN räumlich getrennt von den gesicherten IT-Systemen aufbewahrt werden. Sie SOLLTEN in einem anderen Brandabschnitt aufbewahrt werden. Der Aufbewahrungsort SOLLTE so klimatisiert sein, dass die Datenträger entsprechend der zeitlichen Vorgaben des Datensicherungskonzepts aufbewahrt werden können.

CON.3.A14 Schutz von Datensicherungen (B) [IT-Betrieb]

Die erstellten Datensicherungen MÜSSEN in geeigneter Weise vor unbefugtem Zugriff geschützt werden. Hierbei MUSS insbesondere sichergestellt werden, dass Datensicherungen nicht absichtlich oder unbeabsichtigt überschrieben werden können. 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. Alternativ SOLLTEN die Speichermedien für die Datensicherung nur für autorisierte Datensicherungen oder autorisierte Administrationstätigkeiten mit den entsprechenden IT-Systemen verbunden werden.

CON.3.A15 Regelmäßiges Testen der Datensicherungen (B) [IT-Betrieb]

Es MUSS regelmäßig getestet werden, ob die Datensicherungen wie gewünscht funktionieren, vor allem, ob gesicherte Daten einwandfrei 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 diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

CON.3.A6 Entwicklung eines Datensicherungskonzepts (S) [Fachverantwortliche, IT-Betrieb]

Die Institution SOLLTE ein Datensicherungskonzept erstellen, dass mindestens die nachfolgenden Punkte umfasst:

- Definitionen zu wesentlichen Aspekten der Datensicherung (z. B. unterschiedliche Verfahrensweisen zur Datensicherung),
- Gefährdungslage,
- Einflussfaktoren je IT-System oder Gruppe von IT-Systemen,
- Datensicherungspläne je IT-System oder Gruppe von IT-Systemen sowie
- relevante Ergebnisse des Notfallmanagements/BCM, insbesondere die Recovery Point Objective (RPO) je IT-System oder Gruppe von IT-Systemen.

Der IT-Betrieb SOLLTE das Datensicherungskonzept mit den jeweiligen Fachverantwortlichen der betreffenden Anwendungen abstimmen. Wird ein zentrales Datensicherungssystem für die Sicherung der Daten eingesetzt, SOLLTE beachtet werden, dass sich aufgrund der Konzentration der Daten ein höherer Schutzbedarf ergeben kann. Datensicherungen SOLLTEN regelmäßig gemäß dem Datensicherungskonzept durchgeführt werden.

Das Datensicherungskonzept selbst SOLLTE auch in einer Datensicherung enthalten sein. Die im Datensicherungskonzept enthaltenen technischen Informationen, um Systeme und Datensicherungen wiederherzustellen (Datensicherungspläne), SOLLTEN in der Art gesichert werden, dass sie auch verfügbar sind, wenn die Datensicherungssysteme selbst ausfallen.

Die Mitarbeitenden 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 (S) [IT-Betrieb]

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 der Institution erfüllen.

CON.3.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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

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

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

Zudem SOLLTEN Sicherungssystem und Netzanbindung so beschaffen sein, dass die zulässigen Sicherungs- bzw. Wiederherstellungszeiten nicht überschritten werden.

CON.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.3.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

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

Um die Vertraulichkeit 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.