Bundesamt
für Sicherheit in der
Informationstechnik

CON: Konzepte und Vorgehensweisen

CON.6: Löschen und Vernichten

1 Beschreibung

1.1 Einleitung

Damit Informationen nicht in falsche Hände geraten, ist eine geregelte Vorgehensweise erforderlich, um Daten und Datenträger vollständig und zuverlässig zu löschen oder zu vernichten. Dabei müssen schutzbedürftige Informationen, die auf analogen und digitalen Datenträgern gespeichert sind, berücksichtigt werden.

Wenn nicht oder nur unzureichend gelöschte Datenträger weitergegeben, verkauft oder ausgesondert werden, können dadurch unbeabsichtigt schützenswerte Informationen in falsche Hände gelangen. Dadurch können erhebliche Schäden entstehen. Jede Institution muss deshalb eine Vorgehensweise zum sicheren Löschen und Vernichten von Informationen etablieren.

1.2 Zielsetzung

In diesem Baustein wird beschrieben, wie Informationen in Institutionen sicher gelöscht und vernichtet werden können und wie ein entsprechendes Konzept dazu erstellt wird.

1.3 Abgrenzung und Modellierung

Der Baustein CON.6*Löschen und Vernichten*ist für den gesamten Informationsverbund einmal anzuwenden. Der Baustein beinhaltet nur die allgemeinen prozessualen, technischen und organisatorischen Anforderungen an das Löschen und Vernichten.

Spezifische Anforderungen zum Löschen und Vernichten von Informationen finden sich hierüber hinaus in den einzelnen Bausteinen der Schichten CON *Konzepte und Vorgehensweisen*, ISMS *Sicherheitsmanagement*, ORP *Organisation und Personal*, OPS *Betrieb*, DER *Detektion und Reaktion*, IND *Industrielle IT*, APP *Anwendungen*, SYS *IT-Systeme*, NET *Netze und Kommunikation* und INF *Infrastruktur*. Vor allem die Bausteine CON.3 *Datensicherungskonzept*, OPS 1.2.2 *Archivierung* und CON.9 *Informationsaustausch* sind zusätzlich zu berücksichtigen, da diese Themen immer in Verbindung mit dem Löschen und Vernichten zu behandeln sind.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein CON.6 *Löschen und Vernichten* von besonderer Bedeutung:

2.1 Fehlende oder unzureichend dokumentierte Regelungen beim Löschen und Vernichten

Wenn es keine sicheren Prozesse und Verfahrensweisen für das Löschen und Vernichten von Informationen und Datenträgern gibt oder diese nicht korrekt angewendet werden, können vertrauliche Informationen in die falschen Hände geraten. Diese Gefahr ist bei Datenträgern und IT-Systemen, die ausgesondert werden sollen, besonders hoch, da nicht immer sofort ersichtlich ist, welche (Rest-) Informationen sich auf diesen befinden. Diese Informationen könnten durch unbefugte Dritte ausgelesen oder entwendet werden. Wenn darunter institutionskritische Informationen sind, wäre die gesamte Institution gefährdet.

2.2 Vertraulichkeitsverlust durch Restinformationen auf Datenträgern

Bei den meisten Dateisystemen werden Dateien, die gelöscht werden, nicht wirklich vernichtet. Es werden lediglich die Verweise auf die Datei aus den Verwaltungsinformationen des Dateisystems entfernt und die zu der Datei gehörenden Blöcke als frei markiert. Der tatsächliche Inhalt der Blöcke auf dem Datenträger bleibt jedoch erhalten und kann mit entsprechenden Werkzeugen rekonstruiert werden. Dadurch können Angreifer auf die Datei zugreifen, z. B. wenn solche Datenträger an Dritte weitergegeben oder ungeeignet entsorgt werden. So könnten vertrauliche Informationen nach außen gelangen.

2.3 Unstrukturierte Datenhaltung

Durch unzureichende Vorgaben sowie fehlende Schulung der Mitarbeiter können Informationen unübersichtlich auf Datenträgern gespeichert werden. Das kann dazu führen, dass Informationen nicht vollständig gelöscht werden können, da kein Zuständiger mehr weiß, was in welchen Dateien gespeichert ist. Auch können Angreifer eventuell unbemerkt auf Informationen zugreifen, wenn viele Kopien einer Datei existieren und diese in verschiedenen Verzeichnissen mit unterschiedlichen Schutzfunktionen vorliegen. Kopien werden oft nicht nur in verschiedenen Verzeichnissen eines Datenträgers abgelegt. Viel kritischer ist es, wenn mehrere Kopien auf unterschiedlichen Datenträgern abgelegt werden und nicht mehr ersichtlich ist, wo was wann abgelegt wurde. Das Risiko wird noch größer, wenn die Datenträger dezentral beschafft und nicht kontrolliert werden.

Eine unstrukturierte Datenhaltung gefährdet somit die Verfügbarkeit, Integrität und Verfügbarkeit der Daten.

2.4 Verlust der Vertraulichkeit durch Auslagerungs- und temporäre Dateien

In Auslagerungsdateien oder Auslagerungspartitionen befinden sich mitunter vertrauliche Daten, z. B. Passwörter oder kryptografische Schlüssel. Die Auslagerungsdateien und deren Inhalte sind jedoch nicht geschützt. Sie können z. B. ausgelesen werden, wenn die Festplatte ausgebaut und in einem anderen IT-System wieder eingebaut wird.

Auch fallen im laufenden Betrieb vieler Anwendungen Dateien an, die nicht für den produktiven Betrieb benötigt werden, z. B. die Browser-Historie. Auch diese Dateien können sicherheitsrelevante Informationen enthalten. Werden Auslagerungsdateien oder temporäre Dateien nicht sicher gelöscht, können schützenswerte Informationen, Passwörter und Schlüssel von Unbefugten missbraucht werden, um sich einen Zugang zu weiteren IT-Systemen und Daten zu verschaffen, Wettbewerbsvorteile auf dem Markt zu erlangen oder gezielt Benutzerverhalten auszuspionieren.

2.5 Ungeeignete Entsorgung der Datenträger und Dokumente

Wenn Datenträger oder Dokumente nicht geeignet entsorgt werden, können daraus eventuell Informationen extrahiert werden, die Dritten nicht in die Hände fallen sollten. So können Angreifer z. B. Datenträger aus unzureichend gesicherten Entsorgungseinrichtungen stehlen. Auch wenn beauftragte Entsorgungsdienstleister ungenügend kontrolliert werden, kann die Vertraulichkeit nicht ausreichend sichergestellt werden.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.6 *Löschen und Vernichten* 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.

Grundsätzlich zuständig	Informationssicherheitsbeauftragter (ISB)
Weitere Zuständigkeiten	Mitarbeiter, Fachverantwortliche, Datenschutzbeauftragter, Beschaffungsstelle, IT-Betrieb, Leiter Haustechnik, Leiter IT, Leiter Organisation

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein CON.6 *Löschen und Vernichten* vorrangig umgesetzt werden:

CON.6.A1Regelung der Vorgehensweise für die Löschung und Vernichtung von Informationen [Leiter IT, Leiter Organisation] (B)

Die Institution MUSS das Löschen und Vernichten von Informationen und ihrer Träger regeln. Dabei MUSS je nach Organisationseinheit geregelt werden, welche Informationen und Betriebsmittel unter welchen Voraussetzungen gelöscht und entsorgt werden dürfen. Ebenso MUSS festgelegt werden, in welchen räumlichen Bereichen Entsorgungs- und Vernichtungseinrichtungen aufgebaut werden sollen.

Außerdem MUSS schon in der Planungsphase festgelegt sein, wer für das Löschen und Vernichten von Informationen und Betriebsmitteln zuständig ist. Es MUSS geklärt sein, welche Schnittstellen es zwischen den Organisationseinheiten gibt. Ebenso MUSS der Informationsfluss intern und zwischen den Zuständigen der Institution mit möglichen Outsourcing-Dienstleistern geregelt werden.

CON.6.A2Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln und Informationen [Mitarbeiter, Leiter Haustechnik, Leiter IT] (B)

Alle schutzbedürftigen Informationen und Betriebsmittel MÜSSEN sicher entsorgt werden. Zu diesem Zweck MÜSSEN abgesicherte und geeignete Entsorgungseinrichtungen auf dem Gelände der Institution verfügbar sein. Dabei MUSS auch berücksichtigt werden, dass Informationen und Betriebsmittel eventuell erst gesammelt und dann später entsorgt werden. Eine solche zentrale Sammelstelle MUSS vor unbefugten Zugriffen abgesichert werden.

Wenn externe Dienstleister beauftragt werden, MUSS der Entsorgungsvorgang ausreichend sicher und nachvollziehbar sein. Die mit der Entsorgung beauftragten Unternehmen SOLLTEN regelmäßig daraufhin überprüft werden, ob der Entsorgungsvorgang noch korrekt abläuft.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein CON.6 *Löschen und Vernichten*. Sie SOLLTEN grundsätzlich umgesetzt werden.

CON.6.A3Löschen der Datenträger vor und nach dem Austausch [IT-Betrieb, Mitarbeiter] (S)

Bevor bereits benutzte Datenträger weitergegeben oder noch einmal eingesetzt werden, SOLLTEN alle Daten darauf sicher gelöscht werden. Dazu SOLLTEN den Mitarbeitern geeignete Verfahren zur

Verfügung stehen.

CON.6.A4Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern [Leiter IT, Leiter Organisation] (S)

Für das Löschen und Vernichten SOLLTEN geeignete Verfahren ausgewählt werden. Für alle eingesetzten Datenträgerarten SOLLTE es geeignete Geräte und Werkzeuge geben, mit denen der verantwortliche Mitarbeiter die gespeicherten Informationen löschen oder vernichten kann. Die ausgewählten Verfahrensweisen SOLLTEN allen Mitarbeitern bekannt sein. Es SOLLTE regelmäßig kontrolliert werden, ob die gewählten Verfahren noch dem Stand der Technik entsprechen und für die Institution noch ausreichend sicher sind.

CON.6.A5Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern [IT-Betrieb, Mitarbeiter, Fachverantwortliche, Leiter IT] (S)

Es SOLLTE geregelt und dokumentiert werden, wie IT-Systeme und Datenträger außer Betrieb zu nehmen sind. Dabei SOLLTE sichergestellt sein, dass vor der Aussonderung alle auf einem IT-System oder Datenträger gespeicherten Informationen sicher gelöscht sind. Bei der Aussonderung SOLLTEN neben „klassischen" IT-Systemen auch alle IT-Systeme berücksichtigt werden, die nichtflüchtige Speicherelemente enthalten.

CON.6.A6Einweisung aller Mitarbeiter in die Methoden zur Löschung oder Vernichtung von Informationen [Leiter IT] (S)

Alle Mitarbeiter SOLLTEN in die Methoden und Verfahrensweisen zum Löschen und Vernichten von Informationen eingewiesen werden.

CON.6.A7Beseitigung von Restinformationen [IT-Betrieb, Mitarbeiter] (S)

Wenn Datenträger und Dateien weitergegeben werden, SOLLTE sichergestellt sein, dass sie keine Restinformationen enthalten. Dazu SOLLTE ein Prozess in der Institution etabliert und dokumentiert werden. Die Mitarbeiter SOLLTEN über die Gefahren von Rest- und Zusatzinformationen in Dateien informiert werden. Es SOLLTE stichprobenartig überprüft werden, ob die in Dateien enthaltenen Restinformationen auch wirklich gelöscht werden.

CON.6.A8Erstellung einer Richtlinie für die Löschung und Vernichtung von Informationen [Mitarbeiter, Leiter IT, Datenschutzbeauftragter] (S)

Die Regelungen der Institution zum Löschen und Vernichten SOLLTEN in einer Richtlinie dokumentiert werden. Die Richtlinie SOLLTE allen relevanten Verantwortlichen und Mitarbeitern der Institution bekannt sein und die Grundlage für ihre Arbeit und ihr Handeln bilden. Inhaltlich SOLLTE die Richtlinie alle eingesetzten Datenträger, Anwendungen, IT-Systeme und sonstigen Betriebsmittel und Informationen enthalten, die vom Löschen und Vernichten betroffen sind. Es SOLLTE regelmäßig und stichprobenartig überprüft werden, ob die Mitarbeiter sich an die Richtlinie halten. Die Richtlinie SOLLTE regelmäßig aktualisiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein CON.6 *Löschen und Vernichten* 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. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

CON.6.A9Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern bei erhöhtem Schutzbedarf [Leiter IT, Leiter Organisation] (H)

Für das Löschen und Vernichten SOLLTEN Verfahren ausgewählt werden, die dem erhöhten Schutzbedarf der Informationen und Betriebsmittel gerecht werden.

CON.6.A10 Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten [Leiter IT, Beschaffungsstelle, Leiter Organisation] (H)

Bevor Geräte zur Löschung oder Vernichtung von Daten beschafft werden, SOLLTE eine Anforderungsdokumentation erstellt werden, anhand derer die auf dem Markt verfügbaren Werkzeuge miteinander verglichen werden können.

CON.6.A11 Vernichtung von Datenträgern durch externe Dienstleister [Leiter Organisation, Datenschutzbeauftragter] (H)

Auf dem Gelände der Institution SOLLTEN alle zu vernichtenden Datenträger bis zur Abholung durch den externen Dienstleister sicher vor unbefugten Zugriffen aufbewahrt werden. Der Abtransport SOLLTE ebenfalls dem Schutzbedarf entsprechend abgesichert sein. Die Institution SOLLTE den Entsorgungsprozess regelmäßig durch eingewiesene Personen kontrollieren lassen.

4 Weiterführende Informationen

4.1 Wissenswertes

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27001:2013 im Annex A „A.8.3 Media handling" Vorgaben für die Behandlung von Medien und Informationen, die auch das Löschen und Vernichten umfassen.

Das Deutsche Institut für Normung hat mit der Normenreihe DIN 66399-1:2012-10 „Büro- und Datentechnik - Vernichtung von Datenträgern":

- Teil 1: Grundlagen und Begriffe
- Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern
- Teil 3: Prozess der Datenträgervernichtung

Publikationen zum Vernichten von Datenträgern veröffentlicht.

Das National Institute of Standards and Technology stellt Richtlinien zum Löschen und Vernichten in der NIST Special Publication 800-88 „Guidelines for Media Sanitization" 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.6 *Löschen und Vernichten* von Bedeutung.

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

Elementare Gefährdungen Anforderungen	CIA	G 0.16	G 0.18	G 0.19	G 0.24	G 0.31
CON.6.A1			X	X	X	
CON.6.A2		X		X		
CON.6.A3				X		X
CON.6.A4			X	X	X	
CON.6.A5			X	X		
CON.6.A6						X
CON.6.A7				X		X
CON.6.A8			X	X		
CON.6.A9	CIA		X	X	X	
CON.6.A10	CIA		X	X		
CON.6.A11	CIA	X		X		