Bundesamt
für Sicherheit in der
Informationstechnik

CON.6 Löschen und Vernichten

1. Beschreibung

1.1. Einleitung

Das Löschen und Vernichten stellt einen essentiellen Bestandteil im Lebenszyklus von Informationen auf Datenträgern dar. Unter dem Begriff Datenträger werden in diesem Baustein analoge Datenträger wie Papier oder Filme, sowie digitale Datenträger wie Festplatten, SSDs oder CDs zusammengefasst.

Werden Datenträger ausgesondert, könnten die darauf enthaltenen Informationen offengelegt werden, wenn die Datenträger zuvor nicht sicher gelöscht bzw. vollständig vernichtet worden sind. Dies kann neben Clients und Server alle IT-Systeme, wie IoT-Geräte (z. B. Smart-TVs) betreffen, auf denen vermeintlich nur unbedeutende Informationen abgespeichert sind. IoT-Geräte sind jedoch häufig über ein WLAN verbunden und speichern die hierfür erforderlichen Zugangsdaten. Diese Zugangsdaten können wiederum selbst eine schützenswerte Information sein und dürfen nicht an Unbefugte gelangen.

Gewöhnliche Löschvorgänge über die Funktionen des Betriebssystems bewirken in der Regel kein sicheres Löschen der Informationen, das verhindert, dass die Daten wieder rekonstruiert werden können. Um Informationen sicher zu löschen, bedarf es daher spezieller Verfahren. Datenträger können jedoch nur effektiv in ihrer Gesamtheit sicher gelöscht werden und dies ist bei einzelnen Dateien meist nur mit Einschränkungen möglich.

Zusätzlich existieren gesetzlichen Bestimmungen, wie das Handelsgesetzbuch oder Datenschutzgesetze, die weitreichende Konsequenzen für das Löschen und Vernichten von Dokumenten nach sich ziehen. Einerseits ergeben sich hieraus Aufbewahrungsfristen für beispielsweise Geschäftsabschlüsse, Bilanzen oder Verträge, die ein frühzeitiges Löschen verbieten. Andererseits leiten sich aus diesen gesetzlichen Bestimmungen Rechtsansprüche auf das sichere und zeitnahe Löschen von Daten ab, wenn z. B. personenbezogene Daten betroffen sind.

1.2. Zielsetzung

In diesem Baustein wird beschrieben, wie Informationen in Institutionen sicher gelöscht und vernichtet werden und wie ein entsprechendes, ganzheitliches 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 allgemeine prozessuale, technische und organisatorische

Anforderungen an das Löschen und Vernichten. Der Baustein behandelt nur das sichere Löschen und Vernichten vollständiger Datenträger, da das sichere Löschen einzelner Dateien in den meisten Fällen nur eingeschränkt möglich ist.

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.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, ist nicht sichergestellt, dass vertrauliche Informationen sicher gelöscht bzw. vernichtet werden. Damit ist nicht absehbar, wo diese Informationen verbleiben und ob diese für Dritte zugänglich sind. Diese Gefahr ist bei digitalen 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 werden. Handelt es sich hierbei um besonders schützenswerte Informationen, wie z. B. schützenswerte personenbezogene Daten nach Artikel 9 DSGVO oder Geschäftsgeheimnisse, kann dies hohe Geldstrafen nach sich ziehen.

2.2. Vertraulichkeitsverlust durch Restinformationen auf Datenträgern

Die meisten Anwendungen und Betriebssysteme löschen Dateien standardmäßig nicht sicher und vollständig irreversibel. Es werden lediglich die Verweise auf die Dateien aus den Verwaltungsinformationen des Dateisystems entfernt und die zu den Dateien gehörenden Blöcke als frei markiert. Der tatsächliche Inhalt der Blöcke auf den Datenträgern bleibt jedoch erhalten und kann mit entsprechenden Werkzeugen rekonstruiert werden. Dadurch kann weiterhin auf die Dateien zugegriffen werden, z. B. wenn diese Datenträger an Dritte weitergegeben oder ungeeignet entsorgt werden. So könnten vertrauliche Informationen an Unberechtigte gelangen.

Auch in Auslagerungsdateien, Auslagerungspartitionen oder „Hibernatefiles“ (Dateien für den Ruhezustand) befinden sich mitunter vertrauliche Daten, wie Passwörter oder kryptografische Schlüssel. Diese Daten und deren Inhalte sind jedoch oft nicht geschützt. Sie können z. B. ausgelesen werden, wenn die Datenträger ausgebaut und in einem anderen IT-Systemen wieder eingebaut werden.

Auch fallen im laufenden Betrieb vieler Anwendungen Dateien an, die nicht für den produktiven Betrieb benötigt werden, wie 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 Benutzendenverhalten auszuspionieren.

2.3. Ungeeignete Einbindung externer Dienstleistende in das Löschen und Vernichten

Wenn Datenträger durch externe Dienstleistende gelöscht oder vernichtet werden, könnten die darauf befindlichen Informationen offengelegt werden, wenn nicht hinreicht geregelt ist, wie die externen Dienstleistenden in den Prozess des Löschens und Vernichtens eingebunden wird.

So können Angreifende z. B. Datenträger aus unzureichend gesicherten Sammelstellen stehlen oder an Restinformationen gelangen, wenn Dienstleistende Datenträger nicht hinreichend sicher löschen bzw. vernichten.

2.4. Ungeeigneter Umgang mit defekten Datenträgern oder IT-Geräten

Tritt ein Defekt bei Datenträgern auf, bedeutet dies nicht unbedingt, dass die darauf befindlichen Daten irreversibel beschädigt sind. In vielen Fällen können die Daten, oder zumindest Teile davon, mit Spezialwerkzeugen wiederhergestellt werden. Werden nun defekte Datenträger oder IT-Geräte einfach entsorgt, ohne dass die darauf befindlichen Daten gelöscht bzw. vernichtet worden sind, könnten die Daten bei dem Entsorgungsvorgang offengelegt werden.

Auch in Garantie- bzw. Gewährleistungsfällen oder bei Reparaturaufträgen könnten die Daten von den defekten Datenträgern offengelegt werden. So kann z. B. eine defekte Festplatte zum herstellenden Unternehmen als Garantiefall übersendet werden. Dieses stellt einen Defekt des Controllers fest und ersetzt dem Kunden oder der Kundin das defekte Modell durch ein Neues. Gleichzeitig wird der defekte Controller durch einen Neuen ersetzt und die ursprünglich defekte Festplatte nur schnell und somit unsicher gelöscht. Anschließend gelangt die Festplatte wieder in den Handel. Hierbei können über den gesamten Prozess schützenswerte Informationen offengelegt werden, da sich diese nach wie vor auf der Festplatte befinden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.6 *Löschen und Vernichten* 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 oder die 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	Mitarbeitende, Fachverantwortliche, Datenschutzbeauftragte, Zentrale Verwaltung, IT-Betrieb

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.6.A1 Regelung für die Löschung und Vernichtung von Informationen (B) [Zentrale Verwaltung, Fachverantwortliche, Datenschutzbeauftragte, IT-Betrieb]

Die Institution MUSS das Löschen und Vernichten von Informationen regeln. Dabei MÜSSEN die Fachverantwortlichen für jedes Fachverfahren bzw. Geschäftsprozess regeln, welche Informationen unter welchen Voraussetzungen gelöscht und entsorgt werden müssen.

Hierbei MÜSSEN die gesetzlichen Bestimmungen beachtet werden,

- die einerseits minimale Aufbewahrungsfristen bestimmen sowie
- anderseits maximale Aufbewahrungszeiten und ein Anrecht auf das sichere Löschen von personenbezogenen Daten garantieren.

Sind personenbezogene Daten betroffen, dann MÜSSEN die Regelungen zum Löschen und Vernichten mit Bezug zu personenbezogenen Daten mit dem oder der Datenschutzbeauftragten abgestimmt werden.

Das Löschen und Vernichten von Informationen MUSS dabei für Fachverfahren, Geschäftsprozesse und IT-Systeme geregelt werden, bevor diese produktiv eingeführt worden sind.

CON.6.A2 Ordnungsgemäßes Löschen und Vernichten von schützenswerten Betriebsmitteln und Informationen (B)

Bevor schutzbedürftigen Informationen und Datenträger entsorgt werden, MÜSSEN sie sicher gelöscht oder vernichtet werden. Zu diesem Zweck MUSS der Prozess klar geregelt werden. Einzelne Mitarbeitende MÜSSEN darüber informiert werden, welche Aufgaben sie zum sicheren Löschen und Vernichten erfüllen müssen. Der Prozess zum Löschen und Vernichten von Datenträgern MUSS auch Datensicherungen, wenn erforderlich, berücksichtigen.

Der Standort von Vernichtungseinrichtungen auf dem Gelände der Institution MUSS klar geregelt sein. Dabei MUSS auch berücksichtigt werden, dass Informationen und Betriebsmittel eventuell erst gesammelt und erst später gelöscht oder vernichtet werden. Eine solche zentrale Sammelstelle MUSS vor unbefugten Zugriffen abgesichert werden.

CON.6.A11 Löschung und Vernichtung von Datenträgern durch externe Dienstleistende (B)

Wenn externe Dienstleistende beauftragt werden, MUSS der Prozess zum Löschen und Vernichten ausreichend sicher und nachvollziehbar sein. Die von externen Dienstleistenden eingesetzten Verfahrensweisen zum sicheren Löschen und Vernichten MÜSSEN mindestens die institutionsinternen Anforderungen an die Verfahrensweisen zur Löschung und Vernichtung erfüllen.

Die mit der Löschung und Vernichtung beauftragten Unternehmen SOLLTEN regelmäßig daraufhin überprüft werden, ob der Lösch- bzw. Vernichtungsvorgang noch korrekt abläuft.

CON.6.A12 Mindestanforderungen an Verfahren zur Löschung und Vernichtung (B)

Die Institution MUSS mindestens die nachfolgenden Verfahren zum Löschen und Vernichten von schützenswerten Datenträgern einsetzen. Diese Verfahren SOLLTEN in Abhängigkeit des Schutzbedarfs der verarbeiteten Daten überprüft und, falls erforderlich, angepasst werden:

- Digitale wiederbeschreibbare Datenträger MÜSSEN vollständig mit einem Datenstrom aus Zufallswerten (z. B. PRNG Stream) überschrieben werden, wenn sie nicht verschlüsselt eingesetzt werden.
- Wenn digitale Datenträger verschlüsselt eingesetzt werden, MÜSSEN sie durch ein sicheres Löschen des Schlüssels unter Beachtung des Kryptokonzepts gelöscht werden.

- Optische Datenträger MÜSSEN mindestens nach Sicherheitsstufe O-3 entsprechend der ISO/IEC 21964-2 vernichtet werden.
- Smartphones oder sonstige Smart Devices SOLLTEN entsprechend des Kryptokonzepts verschlüsselt werden. Smartphones oder sonstige Smart Devices MÜSSEN auf die Werkseinstellung (Factory Reset) zurückgesetzt werden. Anschließend SOLLTE der Einrichtungsvorgang zum Abschluss des Löschvorgangs durchgeführt werden.
- IoT Geräte MÜSSEN auf den Werkszustand zurückgesetzt werden. Anschließend MÜSSEN alle in den IoT-Geräten hinterlegten Zugangsdaten geändert werden.
- Papier MUSS mindestens nach Sicherheitsstufe P-3 entsprechend der ISO/IEC 21964-2 vernichtet werden.
- In sonstigen Geräten integrierte Datenträger MÜSSEN über die integrierten Funktionen sicher gelöscht werden. Ist das nicht möglich, MÜSSEN die Massenspeicher ausgebaut und entweder wie herkömmliche digitale Datenträger von einem separatem IT-System aus sicher gelöscht werden oder mindestens nach Sicherheitsstufe E-3 bzw. H-3 entsprechend der ISO/IEC 21964-2 vernichtet werden.

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.6.A3 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.6.A4 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern (S)

Die Institution SOLLTE überprüfen, ob die Mindestanforderungen an die Verfahrensweisen zur Löschung und Vernichtung (siehe dazu CON.6.A12 *Mindestanforderungen an Verfahren zur Löschung und Vernichtung*) für die tatsächlich eingesetzten Datenträger und darauf befindlichen Informationen ausreichend sicher sind. Auf diesem Ergebnis aufbauend SOLLTE die Institution geeignete Verfahren zur Löschung und Vernichtung je Datenträger bestimmen.

Für alle eingesetzten Datenträgerarten, die von der Institution selbst vernichtet bzw. gelöscht werden, SOLLTE es geeignete Geräte und Werkzeuge geben, mit denen die zuständigen Mitarbeitenden die gespeicherten Informationen löschen oder vernichten können. Die ausgewählten Verfahrensweisen SOLLTEN allen verantwortlichen Mitarbeitenden bekannt sein.

Die Institution SOLLTE regelmäßig kontrollieren, ob die gewählten Verfahren noch dem Stand der Technik entsprechen und für die Institution noch ausreichend sicher sind.

CON.6.A5 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.6.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.6.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.6.A8 Erstellung einer Richtlinie für die Löschung und Vernichtung von Informationen (S) [Mitarbeitende, IT-Betrieb, Datenschutzbeauftragte]

Die Regelungen der Institution zum Löschen und Vernichten SOLLTEN in einer Richtlinie dokumentiert werden. Die Richtlinie SOLLTE allen relevanten Mitarbeitenden 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 Mitarbeitenden sich an die Richtlinie halten. Die Richtlinie SOLLTE regelmäßig aktualisiert werden.

CON.6.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.6.A13 Vernichtung defekter digitaler Datenträger (S)

Können digitale Datenträger mit schützenswerten Informationen aufgrund eines Defekts nicht sicher entsprechend der Verfahren zur Löschung von Datenträgern gelöscht werden, dann SOLLTEN diese mindestens entsprechend der Sicherheitsstufe 3 nach ISO/IEC 21964-2 vernichtet werden.

Alternativ SOLLTE für den Fall, dass defekte Datenträger ausgetauscht oder repariert werden, vertraglich mit den hierzu beauftragten Dienstleistenden vereinbart werden, dass diese Datenträger durch die Dienstleistenden sicher vernichtet oder gelöscht werden. Die Verfahrensweisen der Dienstleistenden SOLLTEN hierbei mindestens die institutionsinternen Anforderungen an die Verfahrensweisen zur Löschung und Vernichtung erfüllen.

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.6.A10 ENTFALLEN (H)

Diese Anforderung ist entfallen.

CON.6.A14 Vernichten von Datenträgern auf erhöhter Sicherheitsstufe (H)

Die Institution SOLLTE die erforderliche Sicherheitsstufe zur Vernichtung von Datenträgern entsprechend der ISO/IEC 21964-1 anhand des Schutzbedarf der zu vernichtenden Datenträger bestimmen. Die Datenträger SOLLTEN entsprechend der zugewiesenen Sicherheitsstufe nach ISO/IEC 21964-2 vernichtet werden.

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.

Die International Organisation for Standardization (ISO) hat mit der Normenreihe ISO/IEC 21964 „Information technology - Destruction of data carriers“, die auf der DIN Normenreihe DIN 66399 „Büro- und Datentechnik - Vernichtung von Datenträgern“ aufbaut, Publikationen zum Vernichten von Datenträgern veröffentlicht:

- Part 1: Principles and definitions
- Part 2: Requirements for equipment for destruction of data carriers
- Part 3: Process of destruction of data carriers

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.