Bundesamt
für Sicherheit in der
Informationstechnik

CON.1 Kryptokonzept

1. Beschreibung

1.1. Einleitung

Kryptografie ist ein weit verbreitetes Mittel, um Informationssicherheit in den Schutzzielen Vertraulichkeit, Integrität und Authentizität zu gewährleisten. Damit ist es beispielsweise möglich, Informationen so zu verschlüsseln, dass deren Inhalt ohne den zugehörigen Schlüssel nicht lesbar ist. Bei symmetrischen Verfahren wird derselbe Schlüssel zum Ver- und Entschlüsseln verwendet, bei asymmetrischen Verfahren ein Schlüssel zum Verschlüsseln und ein anderer zum Entschlüsseln.

In den unterschiedlichsten IT-Umgebungen, wie beispielsweise Client-Server-Umgebungen, können lokal gespeicherte Informationen und auch die zu übertragenden Informationen zwischen Kommunikationspartnern und -partnerinnen wirkungsvoll durch kryptografische Verfahren geschützt werden. Kryptografische Verfahren können dabei in Hard- oder Software-Komponenten implementiert sein (im Folgenden als Hard- oder Software mit kryptografischen Funktionen zusammengefasst).

Der alleinige technische Einsatz von kryptografischen Verfahren genügt nicht, um die Vertraulichkeit, Integrität und Authentizität der Informationen zu gewährleisten. Darüber hinaus werden organisatorische Maßnahmen benötigt. Um Informationen effektiv zu schützen, ist es erforderlich, das Thema Kryptografie ganzheitlich im Rahmen eines Kryptokonzepts zu behandeln.

1.2. Zielsetzung

Dieser Baustein beschreibt, wie ein Kryptokonzept erstellt werden sollte und wie damit Informationen in Institutionen kryptografisch abgesichert werden können.

1.3. Abgrenzung und Modellierung

Der Baustein CON.1 *Kryptokonzept* ist einmal auf den Informationsverbund anzuwenden. In diesem Baustein werden organisatorische und technische Anforderungen für Hard- oder Software mit kryptografischen Funktionen sowie kryptografische Verfahren behandelt. Die mit dem Betrieb von Hard- oder Software mit kryptografischen Funktionen zusammenhängenden Kern-IT-Aufgaben werden nicht thematisiert. Dafür müssen die Anforderungen der Bausteine aus der Schicht OPS.1.1 *Kern-IT-Betrieb* erfüllt werden.

Wie Anwendungen (z. B. Ende-zu-Ende-Verschlüsselung bei E-Mails), einzelne IT-Systeme (z. B. Laptops) oder Kommunikationsverbindungen kryptografisch abgesichert werden können, ist ebenfalls

nicht Gegenstand dieses Bausteins. Diese Themen werden in den entsprechenden Bausteinen der Schichten APP *Anwendungen*, SYS *IT-Systeme* und NET *Netze und Kommunikation* behandelt.

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.1 *Kryptokonzept* von besonderer Bedeutung.

2.1. Unzureichendes Schlüsselmanagement bei Verschlüsselung

Durch ein unzureichendes Schlüsselmanagement könnten bei Angriffen unverschlüsselte Informationen offengelegt werden. So kann es beispielsweise sein, dass sich aufgrund fehlender Regelungen verschlüsselte Informationen mit den dazugehörigen Schlüsseln auf demselben Datenträger befinden oder über denselben Kommunikationskanal unverschlüsselt übertragen werden. In diesen Fällen kann bei symmetrischen Verfahren jede Person, die auf den Datenträger oder den Kommunikationskanal zugreifen kann, die Informationen entschlüsseln.

Ein unzureichendes oder fehlendes Schlüsselmanagement kann auch die Verfügbarkeit von Anwendungen bedrohen, wenn zum Beispiel kryptographische Funktionen nicht mehr benutzbar sind, nachdem die Gültigkeitsdauer von Schlüsseln oder Zertifikaten abgelaufen ist.

2.2. Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Hard- oder Software mit kryptografischen Funktionen

Wenn Institutionen Hard- oder Software mit kryptografischen Funktionen einsetzen, müssen sie diverse gesetzliche Rahmenbedingungen beachten. In einigen Ländern dürfen beispielsweise kryptografische Verfahren nur mit staatlicher Genehmigung eingesetzt werden, sodass der Einsatz von Hard- oder Software mit starken kryptografischen Funktionen erheblich eingeschränkt ist. Das kann dazu führen, dass Empfänger oder Empfängerinnen in solchen Ländern verschlüsselte Datensätze nicht lesen können, da sie die benötigte Hard- oder Software mit kryptografischen Funktionen nicht einsetzen dürfen. Im ungünstigsten Fall würden Empfänger oder Empfängerinnen sich sogar strafbar machen, wenn sie die benötigte Hard- oder Software mit kryptografischen Funktionen ungenehmigt einsetzen würden. Oder diese Situation verleitet die an der Kommunikation beteiligten Personen dazu, die Informationen unverschlüsselt auszutauschen, was wiederum zu einer Vielzahl von Gefährdungen der Vertraulichkeit, Integrität und Authentizität der ausgetauschten Informationen führen kann.

Es kann sogar die Situation auftreten, dass die rechtlichen Bestimmungen eines Landes festlegen, dass angemessene Kryptografie einzusetzen ist, während die Bestimmungen eines anderen Landes dies genau verbieten oder eine staatliche Möglichkeit zur Entschlüsselung vorsehen. So können beispielsweise europäische Datenschutzbestimmungen vorschreiben, dass angemessene kryptografische Verfahren eingesetzt werden müssen, um personenbezogene Daten zu schützen. Soll nun aus einem entsprechenden europäischen Land in ein anderes Land kommuniziert werden, in dem der Einsatz von Kryptografie stark reglementiert ist und in dem konkreten Fall nicht genehmigt ist, dann ist eine legale Kommunikation zwischen zwei Personen aus den jeweiligen Ländern nicht möglich.

2.3. Vertraulichkeits- oder Integritätsverlust von Informationen durch Fehlverhalten

Werden kryptographische Funktionen nicht oder nicht richtig verwendet, so können sie den damit beabsichtigten Schutz von Informationen nicht gewährleisten. Setzt eine Institution beispielsweise Hard- oder Software mit kryptografischen Funktionen ein, die sehr kompliziert zu bedienen ist,

könnten die Benutzenden auf Verschlüsselung der Information verzichten und sie stattdessen im Klartext übertragen. Dadurch können die übertragenen Informationen bei einem Angriff mitgelesen werden.

Wird Hard- oder Software mit kryptografischen Funktionen falsch bedient, kann dies auch dazu führen, dass vertrauliche Informationen bei Angriffen abgegriffen werden, etwa, wenn diese im Klartext übertragen werden, weil versehentlich der Klartext-Modus aktiviert wurde.

2.4. Schwachstellen oder Fehler in Hard- oder Software mit kryptografischen Funktionen

Schwachstellen oder Fehler in Hard- oder Software mit kryptografischen Funktionen beeinträchtigen die Sicherheit der eingesetzten kryptografischen Verfahren. Sie können etwa dazu führen, dass die damit geschützten Informationen mitgelesen werden.

So setzt eine Vielzahl von kryptografischen Verfahren auf Zufallsgeneratoren, um sichere Schlüssel z. B. für eine Kommunikationsverbindung zu generieren. Auch wenn ein solches Verfahren als prinzipiell und konzeptionell sicher gilt, kann ein Fehler in der Hard- oder Software-Implementierung dazu führen, dass z. B. vorhersagbare Zufallszahlen generiert werden und somit auch die damit verbundenen kryptografischen Schlüssel rekonstruiert werden können. Dadurch können verschlüsselte Informationen ausgespäht werden, was wiederum weitreichende Folgen nach sich ziehen kann.

2.5. Ausfall von Hardware mit kryptografischen Funktionen

Hardware mit kryptografischen Funktionen (z. B. Chipkarten zur Laufwerksverschlüsselung) kann durch technische Defekte, Stromausfälle oder absichtliche Zerstörung ausfallen. Dadurch könnten bereits verschlüsselte Informationen nicht mehr entschlüsselt werden, solange die erforderliche Hardware nicht verfügbar ist. Als Folge können ganze Prozessketten stillstehen, z. B. wenn weitere Anwendungen auf die Informationen angewiesen sind.

2.6. Unsichere kryptografische Algorithmen

Unsichere oder veraltete kryptografische Algorithmen lassen sich bei einem Angriff mit geringem Aufwand brechen. Bei Verschlüsselungsalgorithmen bedeutet dies, dass es gelingt, aus dem verschlüsselten Text den ursprünglichen Klartext zu ermitteln, ohne dass bei dem Angriff zusätzliche Informationen zur Verfügung stehen, wie z. B. den verwendeten kryptografischen Schlüssel. Werden unsichere kryptografische Algorithmen eingesetzt, können Angreifende den kryptografischen Schutz unterlaufen und somit auf schützenswerte Informationen der Institution zugreifen. Selbst wenn in einer Institution ausschließlich sichere (z. B. zertifizierte) Hard- oder Software mit kryptografischen Funktionen eingesetzt wird, kann die Kommunikation trotzdem unsicher werden. Das ist beispielsweise der Fall, wenn der Kommunikationspartner oder die Kommunikationspartnerin kryptografische Verfahren einsetzt, die nicht dem Stand der Technik entsprechen.

2.7. Fehler in verschlüsselten Informationen oder kryptografischen Schlüsseln

Werden Informationen verschlüsselt und die Chiffrate im Anschluss verändert, lassen sich die verschlüsselten Informationen eventuell nicht mehr korrekt entschlüsseln. Je nach Betriebsart der Verschlüsselungsroutinen kann dies bedeuten, dass nur wenige Bytes oder sämtliche Informationen verloren sind. Ist keine Datensicherung vorhanden, sind solche Informationen verloren. Dieser Umstand kann auch bei Angriffen ausgenutzt werden, indem nur ein minimaler Anteil der Chiffrate verändert wird und dadurch die verschlüsselten Informationen vollständig verloren gehen.

Noch kritischer kann sich ein Fehler in den verwendeten kryptografischen Schlüsseln auswirken. Schon die Änderung eines einzigen Bits eines kryptografischen Schlüssels führt dazu, dass sämtliche damit verschlüsselten Informationen nicht mehr entschlüsselt werden können.

2.8. Kompromittierung kryptografischer Schlüssel

Die Sicherheit kryptografischer Verfahren hängt entscheidend davon ab, wie vertraulich die verwendeten kryptografischen Schlüssel bleiben. Daher wird bei einem Angriff in der Regel versucht, die verwendeten Schlüssel zu erlangen oder zu ermitteln. Das könnte z. B. gelingen, indem flüchtige Speicher ausgelesen oder ungeschützte Schlüssel gefunden werden, die beispielsweise in einer Datensicherung oder einer Konfigurationsdatei hinterlegt sind. Sind die verwendeten Schlüssel und das eingesetzte Kryptoverfahren bekannt, dann können die Informationen relativ leicht entschlüsselt werden.

2.9. Gefälschte Zertifikate

Zertifikate dienen dazu, einen öffentlichen kryptografischen Schlüssel an eine Person, ein IT-System oder eine Institution zu binden. Diese Bindung des Schlüssels wird wiederum kryptografisch mittels einer digitalen Signatur häufig von einer vertrauenswürdigen dritten Stelle abgesichert.

Die Zertifikate werden von Dritten benutzt, um digitale Signaturen der im Zertifikat ausgewiesenen Person, des IT-Systems oder der Institution zu prüfen. Alternativ kann der im Zertifikat hinterlegte Schlüssel für ein asymmetrisches Verschlüsselungsverfahren benutzt werden, um die Informationen für den Zertifikatsinhaber oder die Zertifikatsinhaberin zu verschlüsseln.

Ist ein solches Zertifikat gefälscht, dann werden digitale Signaturen fälschlicherweise als korrekt geprüft und der Person, dem IT-System oder der Institution im Zertifikat zugeordnet. Oder es werden Informationen mit einem möglicherweise unsicheren Schlüssel verschlüsselt und versandt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.1 *Kryptokonzept* 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	Fachverantwortliche, IT-Betrieb, Benutzende

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.1.A1 Auswahl geeigneter kryptografischer Verfahren (B) [Fachverantwortliche]

Es MÜSSEN geeignete kryptografische Verfahren ausgewählt werden. Dabei MUSS sichergestellt sein, dass etablierte Algorithmen verwendet werden, die von der Fachwelt intensiv untersucht wurden und von denen keine Sicherheitslücken bekannt sind. Ebenso MÜSSEN aktuell empfohlene Schlüssellängen verwendet werden. Um eine geeignete Schlüssellänge auszuwählen, SOLLTE berücksichtigt werden, wie lange das kryptografische Verfahren eingesetzt werden soll. Bei einer längeren Einsatzdauer SOLLTEN entsprechend längere Schlüssellängen eingesetzt werden.

CON.1.A2 Datensicherung beim Einsatz kryptografischer Verfahren (B) [IT-Betrieb]

In Datensicherungen MÜSSEN kryptografische Schlüssel vom IT-Betrieb derart gespeichert oder aufbewahrt werden, dass Unbefugte nicht darauf zugreifen können. Langlebige kryptografische Schlüssel MÜSSEN offline, außerhalb der eingesetzten IT-Systeme, aufbewahrt werden.

Bei einer Langzeitspeicherung verschlüsselter Informationen SOLLTE regelmäßig geprüft werden, ob die verwendeten kryptografischen Algorithmen und die Schlüssellängen noch für die jeweiligen Informationen geeignet sind. Der IT-Betrieb MUSS sicherstellen, dass auf verschlüsselt gespeicherte Informationen auch nach längeren Zeiträumen noch zugegriffen werden kann. Verwendete Hard- oder Software mit kryptografischen Funktionen SOLLTE archiviert werden.

CON.1.A4 Geeignetes Schlüsselmanagement (B)

In einem geeigneten Schlüsselmanagement für kryptografische Hard oder Software MUSS festgelegt werden, wie Schlüssel und Zertifikate erzeugt, gespeichert, ausgetauscht und wieder gelöscht oder vernichtet werden. Es MUSS ferner festgelegt werden, wie die Integrität und Authentizität der Schlüssel sichergestellt wird.

Kryptografische Schlüssel SOLLTEN immer mit geeigneten Schlüsselgeneratoren und in einer sicheren Umgebung erzeugt werden. In Hard- oder Software mit kryptografischen Funktionen SOLLTEN voreingestellte Schlüssel (ausgenommen öffentliche Zertifikate) ersetzt werden. Ein Schlüssel SOLLTE möglichst nur einem Einsatzzweck dienen. Insbesondere SOLLTEN für die Verschlüsselung und Signaturbildung unterschiedliche Schlüssel benutzt werden. Kryptografische Schlüssel SOLLTEN mit sicher geltenden Verfahren ausgetauscht werden.

Wenn öffentliche Schlüssel von Dritten verwendet werden, MUSS sichergestellt sein, dass die Schlüssel authentisch sind und die Integrität der Schlüsseldaten gewährleistet ist.

Geheime Schlüssel MÜSSEN sicher gespeichert und vor unbefugtem Zugriff geschützt werden. Alle kryptografischen Schlüssel SOLLTEN hinreichend häufig gewechselt werden. Grundsätzlich SOLLTE geregelt werden, wie mit abgelaufenen Schlüsseln und damit verbundenen Signaturen verfahren wird. Falls die Gültigkeit von Schlüsseln oder Zertifikaten zeitlich eingeschränkt wird, dann MUSS durch die Institution sichergestellt werden, dass die zeitlich eingeschränkten Zertifikate oder Schlüssel rechtzeitig erneuert werden.

Eine Vorgehensweise SOLLTE für den Fall festgelegt werden, dass ein privater Schlüssel offengelegt wird. Alle erzeugten kryptografischen Schlüssel SOLLTEN sicher aufbewahrt und verwaltet 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.1.A3 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.1.A5 Sicheres Löschen und Vernichten von kryptografischen Schlüsseln (S) [IT-Betrieb, Benutzende]

Nicht mehr benötigte private Schlüssel SOLLTEN sicher gelöscht oder vernichtet werden. Die Vorgehensweisen und eingesetzten Methoden, um nicht mehr benötigte private Schlüssel zu löschen oder zu vernichten, SOLLTEN im Kryptokonzept dokumentiert werden.

CON.1.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.1.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.1.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.1.A9 Festlegung von Kriterien für die Auswahl von Hard- oder Software mit kryptografischen Funktionen (S) [Fachverantwortliche]

Im Kryptokonzept SOLLTE festgelegt werden, anhand welcher Kriterien und Anforderungen Hard- oder Software mit kryptografischen Funktionen ausgesucht wird. Hierbei SOLLTEN Aspekte wie

- Funktionsumfang,
- Interoperabilität,
- Wirtschaftlichkeit,
- Fehlbedienungs- und Fehlfunktionssicherheit,
- technische Aspekte,
- personelle und organisatorische Aspekte,
- Lebensdauer von kryptografischen Verfahren und der eingesetzten Schlüssellängen sowie
- gesetzliche Rahmenbedingungen
- internationale rechtliche Aspekte wie Export- und Importbeschränkungen für Hard- oder Software mit kryptografischen Funktionen, wenn die kryptografischen Verfahren auch im Ausland eingesetzt werden
- Datenschutz

berücksichtigt und im Kryptokonzept dokumentiert werden. Dabei SOLLTE grundsätzlich zertifizierte Hard- oder Software mit kryptografischen Funktionen, deren Zertifizierung die jeweils relevanten Aspekte der Kryptografie umfasst, bevorzugt ausgewählt werden.

CON.1.A10 Erstellung eines Kryptokonzepts (S)

Ausgehend von dem allgemeinen Sicherheitskonzept der Institution SOLLTE ein Kryptokonzept für Hard- oder Software mit kryptografischen Funktionen erstellt werden. Im Kryptokonzept SOLLTE beschrieben werden,

- wie die Datensicherungen von kryptografischen Schlüsseln durchgeführt werden,
- wie das Schlüsselmanagement von kryptografischen Schlüsseln ausgestaltet ist sowie
- wie das Krypto-Kastaster erhoben wird.

Weiterhin SOLLTE im Kryptokonzept beschrieben werden, wie sichergestellt wird, dass kryptografische Funktionen von Hard- oder Software sicher konfiguriert und korrekt eingesetzt werden. Im Kryptokonzept SOLLTEN alle technischen Vorgaben für Hard- und Software mit

kryptografischen Funktionen beschrieben werden (z. B. Anforderungen, Konfiguration oder Parameter). Um geeignete kryptografische Verfahren auszuwählen, SOLLTE die BSI TR 02102 berücksichtigt werden.

Wird das Kryptokonzept verändert oder von ihm abgewichen, SOLLTE dies mit dem oder der ISB abgestimmt und dokumentiert werden. Das Kryptokonzept SOLLTE allen bekannt sein, die kryptografische Verfahren einsetzen. Außerdem SOLLTE es bindend für ihre Arbeit sein. Insbesondere der IT-Betrieb SOLLTE die kryptografischen Vorgaben des Kryptokonzepts umsetzen.

CON.1.A15 Reaktion auf praktische Schwächung eines Kryptoverfahrens (S)

Die Institution SOLLTE mindestens jährlich anhand des Krypto-Katasters überprüfen, ob die eingesetzten kryptografischen Verfahren und die zugehörigen Parameter noch ausreichend sicher sind und keine bekannten Schwachstellen aufweisen.

Im Kryptokonzept SOLLTE ein Prozess für den Fall definiert und dokumentiert werden, dass Schwachstellen in kryptografischen Verfahren auftreten. Dabei SOLLTE sichergestellt werden, dass das geschwächte kryptografische Verfahren entweder abgesichert oder durch eine geeignete Alternative abgelöst wird, sodass hieraus kein Sicherheitsrisiko entsteht.

CON.1.A19 Erstellung eines Krypto-Katasters (S) [IT-Betrieb]

Für jede Gruppe von IT-Systemen SOLLTEN folgende Informationen im Krypto-Kataster festgehalten werden:

- Einsatzzweck (z. B. Festplattenverschlüsselung oder Verschlüsselung einer Kommunikationsverbindung)
- Zuständige
- eingesetztes kryptografische Verfahren
- eingesetzte Hard- oder Software mit kryptografischen Funktionen
- eingesetzte sicherheitsrelevante Parameter (z. B. Schlüssellängen)

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.1.A11 Test von Hardware mit kryptografischen Funktionen (H) [IT-Betrieb]

Im Kryptokonzept SOLLTEN Testverfahren für Hardware mit kryptografischen Funktionen festgelegt werden. Bevor Hardware mit kryptografischen Funktionen eingesetzt wird, sollte getestet werden, ob die kryptografischen Funktionen korrekt funktionieren.

Wenn ein IT-System geändert wird, SOLLTE getestet werden, ob die eingesetzte kryptografische Hardware noch ordnungsgemäß funktioniert. Die Konfiguration der kryptografischen Hardware SOLLTE regelmäßig überprüft werden.

CON.1.A12 ENTFALLEN (H)

Diese Anforderung ist entfallen.

CON.1.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

CON.1.A14 ENTFALLEN (H)

Diese Anforderung ist entfallen.

CON.1.A16 Physische Absicherung von Hardware mit kryptografischen Funktionen (H) [IT-Betrieb]

Im Kryptokonzept SOLLTE festgelegt werden, wie der IT-Betrieb sicherstellt, dass nicht unautorisiert physisch auf Hardware mit kryptografischen Funktionen zugegriffen werden kann.

CON.1.A17 Abstrahlsicherheit (H) [IT-Betrieb]

Es SOLLTE geprüft werden, ob zusätzliche Maßnahmen hinsichtlich der Abstrahlsicherheit notwendig sind. Dies SOLLTE insbesondere dann geschehen, wenn staatliche Verschlusssachen (VS) der Geheimhaltungsgrade VS-VERTRAULICH und höher verarbeitet werden. Getroffene Maßnahmen hinsichtlich der Abstrahlsicherheit SOLLTEN im Kryptokonzept dokumentiert werden.

CON.1.A18 Kryptografische Ersatzhardware (H) [IT-Betrieb]

Hardware mit kryptografischen Funktionen (z. B. Hardware-Token für Zwei-Faktor-Authentifizierung) SOLLTE vorrätig sein. Im Kryptokonzept SOLLTE dokumentiert werden, für welche Hardware mit kryptografischen Funktionen Ersatzhardware zur Verfügung steht und wie diese ausgetauscht werden kann.

CON.1.A20 Manipulationserkennung für Hard- oder Software mit kryptografischen Funktionen (H)

Hard- und Software mit kryptografischen Funktionen SOLLTE auf Manipulationsversuche hin überwacht werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) behandelt das Thema Kryptografie in der Norm ISO/IEC 27001:2013 im Annex A.10 anhand von zwei Richtlinien.

Für die Auswahl von Verschlüsselungsverfahren und Schlüssellängen sollte die technische Richtlinie „BSI-TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI beachtet werden.

Das Information Security Forum (ISF) hat in seinem Standard „The Standard of Good Practice for Information Security“ in der „Area TS2 Cryptography“ Anforderungen an Kryptokonzepte erarbeitet.

Bundesamt
für Sicherheit in der
Informationstechnik

CON.2 Datenschutz

1. Beschreibung

1.1. Einleitung

Im Gegensatz zur Informationssicherheit, die primär dem Schutz der datenverarbeitenden Institution dient, ist es Aufgabe des Datenschutzes, natürliche Personen davor zu schützen, dass Institutionen oder Stellen mit ihren Verarbeitungstätigkeiten zu intensiv in die Grundrechte und Grundfreiheiten der Personen eingreifen. Das Grundgesetz für die Bundesrepublik Deutschland gewährleistet das Recht von Bürgerinnen und Bürgern, grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten zu bestimmen. Die Datenschutzgesetze des Bundes und der Bundesländer nehmen darauf Bezug, wenn sie den Schutz des Rechts auf informationelle Selbstbestimmung hervorheben. Die EU-Grundrechtecharta formuliert in Artikel 8 unmittelbar das Recht auf den Schutz personenbezogener Daten (Absatz 1), hebt die Notwendigkeit einer Rechtsgrundlage zur Datenverarbeitung hervor (Absatz 2) und schreibt die Überwachung der Einhaltung von Datenschutzvorschriften durch eine unabhängige Stelle vor (Absatz 3). Die Datenschutz-Grundverordnung (DSGVO) führt diese Anforderungen der Grundrechtecharta näher aus. Von zentraler Bedeutung ist dabei der Artikel 5 DSGVO, der die Grundsätze für die Verarbeitung personenbezogener Daten auflistet, die teilweise auch als Schutzziele verstanden werden können. Neben der DSGVO sind das Bundesdatenschutzgesetz (BDSG) und die Datenschutzgesetze der Bundesländer sowie weitere bereichsspezifische Regelungen wie beispielsweise das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) zu berücksichtigen.

Zugespitzt sind im Rahmen des operativen Datenschutzes vier Typen von Risiken, die mit unterschiedlichen Ausprägungen von Schutzmaßnahmen zu verringern sind, zu unterscheiden:

- Risikotyp A: Der Grundrechtseingriff bei natürlichen Personen durch die Verarbeitung ist nicht hinreichend milde gestaltet.
- Risikotyp B: Die Maßnahmen zur Verringerung der Eingriffsintensität einer Verarbeitung sind, in Bezug auf die Gewährleistungsziele, nicht vollständig oder werden nicht hinreichend wirksam betrieben oder nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp C: Die Maßnahmen, die nach der Informationssicherheit geboten sind (vgl. z. B. IT-Grundschutz nach BSI), sind nicht vollständig oder werden nicht hinreichend wirksam betrieben oder werden nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp D: Die Maßnahme der Informationssicherheit werden nicht ausreichend datenschutzgerecht, im Sinne des Risikotyp A und Risikotyp B, betrieben.

Die Prüfung der Verhältnismäßigkeit des Grundrechtseingriffs einer Verarbeitung ist nicht vom SDM umfasst. Diese rechtliche Prüfung sowie die Prüfung der Rechtsgrundlage (vergleiche insbesondere Art. 6 und 9 DS-GVO) und des Verarbeitungszwecks müssen vor der Anwendung des SDM erfolgen. Somit ist die Behandlung des zuvor genannten Risikotyps A nicht unmittelbar Gegenstand der Anwendung des SDM. Wird ein oder werden mehrere Risikotypen nicht betrachtet oder nicht hinreichend zwischen den Risiko-Typen differenziert, dann besteht die Gefahr, dass das informationelle Selbstbestimmungsrecht der betroffenen Person nicht gesetzeskonform gewährleistet werden kann.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (kurz: Datenschutzkonferenz, DSK) hat mit dem Standard-Datenschutzmodell (SDM) eine Methode entwickelt, welche die in den deutschen und europäischen Rechtsvorschriften genannten technischen und organisatorischen Maßnahmen auf der Basis von sieben Schutz- beziehungsweise Gewährleistungszielen systematisiert. Damit dient das Modell den für die Datenverarbeitung verantwortlichen und als Auftragsverarbeiter beteiligten Stellen, erforderliche Maßnahmen systematisch zu planen sowie umzusetzen. Es fördert somit die datenschutzgerechte Ausgestaltung und Organisation von informationstechnischen Verfahren, Anwendungen und Infrastrukturen. Andererseits bietet das Modell den Datenschutzaufsichtsbehörden eine Möglichkeit, mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren und belastbaren Gesamturteil über eine Verarbeitung zu gelangen. Das SDM ist als Methode geeignet, die Wirksamkeit der technischen und organisatorischen Maßnahmen einer Datenverarbeitung auf der Grundlage und nach den Kriterien der DSGVO regelmäßig zu überprüfen und fachgerecht zu bewerten.

Das SDM nimmt bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen die Perspektive der Betroffenen und deren Grundrechtsausübung ein und unterscheidet sich daher grundlegend von der Sicht des IT-Grundschutzes. Dieser legt den Schwerpunkt vorrangig auf die Informationssicherheit und soll die datenverarbeitenden Institutionen schützen. Für die Risikobeurteilung und die anschließende Auswahl von Maßnahmen nach dem SDM ist hingegen die Beeinträchtigung maßgeblich, die Betroffene durch die Datenverarbeitung der Institution hinnehmen müssen.

Vor diesem Hintergrund ist zwischen der Auswahl von Maßnahmen zur Gewährleistung der Informationssicherheit für Institutionen und der Auswahl von Maßnahmen zur Gewährleistung des Datenschutzes zu unterscheiden: Die IT-Grundschutz-Methodik dient vorrangig der Informationssicherheit, das Standard-Datenschutzmodell dient der Umsetzung der datenschutzrechtlichen Anforderungen (insbesondere der Grundsätze aus Artikel 5 DSGVO und der Betroffenenrechte aus Kapitel III DSGVO). Das SDM hat daher die folgenden Ansprüche:

- Es überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen.
- Es gliedert die betrachteten Verfahren in die Komponenten Daten, Systeme und Dienste (inkl. Schnittstellen) sowie Prozesse.
- Es berücksichtigt die Einordnung von Verarbeitungstätigkeiten basierend auf den Risikostufen "kein oder gering", "normal" und "hoch" gemäß DSGVO in die Schutzbedarfsstufen „normal“ und „hoch“, insbesondere mit Auswirkungen auf der Ebene der Sachbearbeitung mit ihren Fachverfahren, die von Anwendungen und IT-Infrastruktur unterstützt werden.
- Es bietet einen Katalog mit standardisierten Schutzmaßnahmen.

Der Referenzmaßnahmen-Katalog des SDM umfasst Maßnahmen, die auf Informationsverbünde oder Verfahren (Verarbeitungen) sowie auf die gesamte Institution im Rahmen eines Datenschutzmanagementprozesses anzuwenden sind.

Die Prüfung der Verhältnismäßigkeit des Grundrechtseingriffs einer Verarbeitung ist nicht vom SDM umfasst. Diese rechtliche Prüfung sowie die Prüfung der Rechtsgrundlage nach Artikel 6 und gegebenenfalls des Artikels 9 DSGVO müssen erfolgen, bevor das SDM angewendet wird. Somit wird der Risikotyp A nicht im Rahmen des SDM selbst behandelt.

1.2. Zielsetzung

Ziel des Bausteins ist es, die Verbindung der Anforderungen des Datenschutzes, die durch das Standard-Datenschutzmodell operationalisiert werden, zum IT-Grundschutz darzustellen.

1.3. Abgrenzung und Modellierung

Der Baustein CON.2 *Datenschutz* ist für den Informationsverbund einmal anzuwenden, wenn personenbezogene Daten unter deutschem oder europäischem Recht verarbeitet werden. Der Baustein CON.2 *Datenschutz* und insbesondere die umfangreichen Erläuterungen in der Einleitung unterstützen somit Anwendende in Deutschland und Europa bei der Orientierung, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert werden, bei denen personenbezogene oder -beziehbare Daten verarbeitet oder sonstig genutzt werden. Dabei sollte dann geprüft werden, ob der Baustein nicht nur auf einzelne Informationsverbünde oder Verfahren, sondern auf die gesamte Institution anzuwenden 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.2 *Datenschutz* von besonderer Bedeutung.

2.1. Missachtung von Datenschutzgesetzen oder Nutzung eines unvollständigen Risikomodells

Nach der DSGVO ist die Verarbeitung personenbezogener Daten grundsätzlich verboten. Die Verarbeitung dieser Daten ist nur dann rechtmäßig, wenn die Voraussetzungen des Artikels 6 DSGVO erfüllt sind, also beispielsweise eine Einwilligung der betroffenen Person vorliegt oder eine Rechtsvorschrift die Datenverarbeitung erlaubt. Nicht rechtskonform ist eine Verarbeitung z. B. auch dann, wenn eine Institution eine Datenverarbeitung nicht hinreichend zweckbestimmt, den Zweck überdehnt oder gänzlich zweckungebunden durchführt. Dasselbe gilt, wenn die entsprechende Institution die personenbezogenen Daten intransparent oder ohne integritätssichernde Maßnahmen und ohne Eingriffsmöglichkeiten durch Betroffene verarbeitet.

Aus der Sicht des Datenschutzes ist eine Institution, die personenbezogene Daten verarbeitet (beispielsweise erhebt, speichert, übermittelt oder löscht), grundsätzlich ein Risiko für die davon betroffenen Personen. Dieses Risiko besteht auch dann, wenn die Datenverarbeitung einer Institution rechtskonform ausgestaltet ist.

Ein in der Praxis häufig auftretendes Risiko ist der Zugriff auf Daten, die nicht dem Zweck der ursprünglichen Datenverarbeitung dienen. Dabei kann es sich typischerweise um Zugriffe von ausländischen Konzernmüttern, Sicherheitsbehörden, Banken und Versicherungen, öffentlichen Leistungsverwaltungen, IT-Herstellenden und IT-Dienstleistenden oder Forschungsinstitutionen handeln. Oftmals wird in diesen Kontexten nicht geprüft, ob der Zugriff befugt ist, weil beispielsweise eine langjährig eingefahrene Praxis fortgesetzt wird. Eine andere Möglichkeit ist, dass nachrangige Mitarbeitende das persönliche Risiko scheuen, zu hinterfragen, ob eine hinreichende Rechtsgrundlage vorliegt. Ferner werden aus (teilweise) negativen Prüfergebnissen durch eine Rechtsabteilung oder eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten oft seitens der Verantwortlichen keine Konsequenzen gezogen. Ignorieren Verantwortliche Prüf- oder Beratungsergebnisse, so können sich dadurch Fragen zur Haftung ergeben.

Ein weiteres Risiko sowohl für Personen als auch für verantwortliche Institutionen besteht, wenn für rechtmäßig erfolgte Zugriffe auf IT-Dienste oder die Übermittlung von Datenbeständen durch Dritte

keine Standardprozesse vorgesehen sind. Dasselbe gilt, wenn keine Nachweise über die Ordnungsmäßigkeit in Form von Protokollen und Dokumentationen erbracht werden können.

Eine große Gefahr für Personen oder Beschäftigte ist auch eine mangelhafte Datensicherheit. Erwägungsgrund 75 der DSGVO beschreibt die mit der Verarbeitung personenbezogener Daten einhergehenden Risiken und damit die Gefährdungslage durch unbefugten Zugriff wie folgt: „Die Risiken für die Rechte und Freiheiten natürlicher Personen, mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere, können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft."

2.2. Festlegung eines zu niedrigen Schutzbedarfs

Eine weitere Gefahr für Personen bzw. Beschäftigte ist ein falsch angesetzter Schutzbedarf ihrer personenbezogenen Daten. Dieser Schutzbedarf, der typischerweise durch die Institution, die verantwortlich personenbezogene Daten verarbeitet, selbst festgelegt wird, kann aus verschiedenen Gründen falsch oder zu niedrig angesetzt sein:

- Die Institution hat den gegenüber der Informationssicherheit erweiterten Schutzzielkatalog des Datenschutzes nicht berücksichtigt.
- Die Institution hat bei der Schutzbedarfsermittlung nicht zwischen den Risiken für die Umsetzung der Grundrechte der Betroffenen und den Risiken für die Institution unterschieden.
- Die Institution hat zwar die beiden Schutzinteressen unterschieden, aber die Funktionen des Verfahrens und der Schutzmaßnahmen zugunsten der Institution bzw. zu Ungunsten betroffener Personen gestaltet.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.2 *Datenschutz* aufgeführt. Die Institutionsleitung ist dafür verantwortlich, dass die datenschutzrechtlichen Bestimmungen eingehalten werden. Die Umsetzung der zur Sicherstellung des Datenschutzes erforderlichen Maßnahmen kann sie an eine Organisationseinheit delegieren. Hiervon abzugrenzen ist die Rolle der oder des Datenschutzbeauftragten. Zu ihren Aufgaben gemäß Artikel 39 DSGVO gehört es, die Verantwortlichen, die Auftragsverarbeiter und deren jeweilige Mitarbeitende über ihre datenschutzrechtlichen Pflichten zu unterrichten und zu beraten. Ferner gehört es zu ihren Aufgaben, zu überwachen, ob die datenschutzrechtlichen Bestimmungen eingehalten werden. Die Verantwortung für die Wahrung des Datenschutzes verbleibt hingegen bei den Verantwortlichen bzw.

den Auftragsverarbeitern. Der oder die Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der oder die ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden.

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

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Institutionsleitung
Weitere Zuständigkeiten	Datenschutzbeauftragte

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.2.A1 Umsetzung Standard-Datenschutzmodell (B)

Die gesetzlichen Bestimmungen zum Datenschutz (DSGVO, BDSG, die Datenschutzgesetze der Bundesländer und gegebenenfalls einschlägige bereichsspezifische Datenschutzregelungen) MÜSSEN eingehalten werden. Wird die SDM-Methodik nicht berücksichtigt, die Maßnahmen also nicht auf der Basis der Gewährleistungsziele systematisiert und mit dem Referenzmaßnahmen-Katalog des SDM abgeglichen, SOLLTE dies begründet und dokumentiert werden.

3.2. Standard-Anforderungen

Für diesen Baustein sind keine Standard-Anforderungen definiert.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Die EU-Datenschutz-Grundverordnung: „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)" (DSGVO) stellt grundlegende, europaweite gesetzliche Anforderungen an die Einhaltung des Datenschutzes.

Das Standard-Datenschutzmodell (SDM) - „Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele" des Arbeitskreises „Technik" der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bietet eine Methode, um gesetzliche Datenschutzvorschriften umzusetzen.

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.

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.

Bundesamt
für Sicherheit in der
Informationstechnik

CON.7 Informationssicherheit auf Auslandsreisen

1. Beschreibung

1.1. Einleitung

Berufsbedingte Reisen gehören mittlerweile zum Alltag in vielen Institutionen. Um auch außerhalb des regulären Arbeitsumfeldes arbeiten zu können, ist es dabei nötig, neben Unterlagen in Papierform auch Informationstechnik mitzuführen, wie beispielsweise Notebooks, Smartphones, Tablets, Wechselfestplatten oder USB-Sticks. Bei Geschäftsreisen, vor allem ins Ausland, gibt es jedoch eine Vielzahl an Bedrohungen und Risiken für die Informationssicherheit, die im normalen Geschäftsbetrieb nicht existieren.

Jede Reise ist individuell zu bewerten, da sich aufgrund der Kombination aus Reisezweck (geschäftliche Besprechung, Tagung, Kongress etc.), Reisedauer und Reiseziel jeweils eine neue Bedrohungslage ergibt, auch in Bezug auf den Schutz geschäftskritischer Informationen.

Die Bedrohungslage ist auf Reisen besonders erhöht. Dies ergibt sich z. B. aus der Kommunikation über öffentliche Netze, die nicht unter der Kontrolle der eigenen Institution stehen. Dadurch werden etwa Gefahren erneut relevant, gegen die sich die Institution vielleicht schon abgesichert hat. Hinzu kommt, dass das Risiko auf Auslandsreisen abhängig vom Zielland oftmals deutlich höher ist als bei Reisen im Inland.

Der Schutz betrieblicher und dienstlicher Informationen ist aufgrund ständig wechselnder Reiseziele, sowie regulatorischer und gesetzlicher Anforderungen, nicht immer einfach zu realisieren. So können z. B. gesetzliche Anforderungen die Einreisekontrolle verschärfen und somit den Schutz der Vertraulichkeit von Daten beeinflussen. Damit ergeben sich abhängig von Art und Dauer der Reise, sowie dem Reiseziel, individuelle Anforderungen an die Informationssicherheit. Politische, gesellschaftliche, religiöse, geografische, klimatische, gesetzliche und regulatorische Besonderheiten einzelner Reiseziele spielen hier eine maßgebliche Rolle.

1.2. Zielsetzung

Dieser Baustein beschreibt den Schutz aller Informationen, die auf Auslandsreisen sowohl in elektronischer als auch in physischer Form mitgeführt werden, in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit. Vertrauliche Informationen, die reisende Mitarbeitende im Kopf mitführen, sind ebenfalls Gegenstand dieses Bausteines. Es werden angemessene Regelungen und Maßnahmen für den Umgang mit schützenswerten Informationen und Daten auf Auslandsreisen aufgezeigt. Zu

berücksichtigen sind dabei grundsätzliche Rahmenbedingungen, etwa aus den Bereichen IT, Datenschutz und Recht.

In diesem Baustein werden Gefährdungen und Anforderungen spezifischer Szenarien herausgestellt, die in direktem Zusammenhang mit dem sicheren Einsatz von Informationstechnik, den Informationen und den eingesetzten Geräten auf Auslandsreisen stehen.

Dieser Baustein dient den Verantwortlichen einer Institution als Orientierungshilfe, um angemessene Sicherheitsmaßnahmen im Rahmen der Informationssicherheit auf Auslandsreisen zu etablieren. Dabei werden die wesentlichen Grundsätze aufgezeigt, die in diesem Zusammenhang zu berücksichtigen sind. Viele der genannten Gefährdungen gelten auch bei Reisen im Inland oder grundsätzlich bei der Verarbeitung von Informationen in Umgebungen, die nicht unter Kontrolle der eigenen Institution stehen.

1.3. Abgrenzung und Modellierung

Der Baustein CON.7 *Informationssicherheit auf Auslandsreisen* ist für den Informationsverbund anzuwenden, wenn Mitarbeitende ins Ausland reisen oder zeitweise im Ausland tätig sind und dabei besonders schutzbedürftige Informationen mitgeführt oder verarbeitet werden.

Der Baustein umfasst grundsätzlich die Anforderungen, die zu einem angemessenen Schutz von Informationen auf Auslandsreisen beitragen. Dabei hat der Schutz der Vertraulichkeit und der Integrität von schützenswerten Informationen auf Reisen den gleichen Stellenwert wie am Sitz der Institution.

Gefährdungen und Anforderungen, die den lokalen Informationsverbund betreffen, werden hier nicht betrachtet.

Da im Baustein CON.7 *Informationssicherheit auf Auslandsreisen* speziell die prozessualen, technischen und organisatorischen Anforderungen betrachtet werden, die spezifisch für die geschäftliche Arbeit auf Reisen sind, werden Anforderungen der Schichten NET *Netze und Kommunikation*, SYS *IT-Systeme* und APP *Anwendungen* nicht betrachtet. Alle notwendigen Bausteine, vor allem SYS.2.1 *Allgemeiner Client*, NET.3.3 *VPN* und SYS.3.2.2 *Mobile Device Management (MDM)*, müssen gesondert berücksichtigt werden.

Zudem sind die Anforderungen aus den thematisch ähnlichen Bausteinen INF.9 *Mobiler Arbeitsplatz* und OPS.1.2.4 *Telearbeit* zu beachten und umzusetzen.

Innerhalb dieses Bausteins kommt es außerdem zu Überschneidungen mit weiteren Bausteinen und Themenfeldern, die hier nicht betrachtet werden:

- Erfüllung der Datenschutzanforderungen,
- Präventive Maßnahmen zum Schutz von Informationen (auch technische Anforderungen, die an tragbare IT-Systeme gestellt werden, z. B. Abstrahl- oder Abhörschutz) sowie
- Personelle Sicherheit.

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.7 *Informationssicherheit auf Auslandsreisen* von besonderer Bedeutung.

2.1. Abhören und Ausspähen von Informationen/Wirtschaftsspionage

Mit Spionage werden Angriffe bezeichnet, die das Ziel haben, Informationen über Institutionen, Personen, Produkte oder andere Zielobjekte zu sammeln, auszuwerten und aufzubereiten. Insbesondere bei Reisen ins Ausland gibt es unbekannte Gefahrenquellen, auf die das Informationssicherheitsmanagement der eigenen Institution keinen Einfluss hat. Grundsätzlich bestehen in fremden Räumen und fremden IT-Umgebungen viele Gefahren durch das gezielte Abhören von Unterhaltungen, Leitungen, Telefongesprächen oder Datenübertragungen. Dies kann vor allem im Ausland durch entsprechende rechtliche Möglichkeiten problematisch und für die Reisenden nur schwer einschätzbar sein.

Die Gefährdungen können öffentliche Plätze und Räume betreffen, Gegebenheiten in anderen Institutionen, aber auch institutionseigene Repräsentanzen im Ausland. Auch Geräte, wie z. B. Mobiltelefone, können dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören. Zudem sind viele IT-Systeme standardmäßig mit Mikrofon und Kameras ausgestattet, die angegriffen und dann ausgenutzt werden können.

Darüber hinaus kann es bei bestimmten Ländern Restriktionen bei der Ein- und Ausreise geben, die regulatorische Vorgaben des Herkunftslandes und Anforderungen der Institution an die Sicherheit außer Kraft setzen bzw. diesen widersprechen. Zum Beispiel kann Einsicht in Daten verlangt werden, die auf Notebooks und anderen tragbaren IT-Systemen gespeichert sind. Hierbei können zum Teil vertrauliche und personenbezogene Daten nicht nur eingesehen, sondern auch kopiert und gespeichert werden. Da es sich bei diesen Informationen z. B. auch um Strategiepapiere oder streng vertrauliche Entwürfe einer Institution handeln könnte, muss bei einer Einsichtnahme immer mit einem potenziellen Missbrauch gerechnet werden (Wirtschaftsspionage).

Auf Auslandsreisen besteht nicht nur die Gefahr, dass Informationen auf technisch komplexem Weg abgehört werden können. Oft können schützenswerte Daten auf optischem, akustischem oder elektronischem Weg einfacher ausgespäht werden, da im Ausland häufig nicht die gewohnten Ansprüche an informationssicherheitstechnische Bestimmungen gestellt werden können. Dies betrifft z. B. das allgemeine Sicherheitslevel eines Landes sowie die Gegebenheiten vor Ort, die Reisende zwangsläufig nutzen müssen.

2.2. Offenlegung und Missbrauch schützenswerter Informationen (elektronisch und physisch)

Beim Austausch von Informationen kann es vorkommen, dass neben den gewünschten Informationen auch ungewollt schutzbedürftige Informationen übermittelt werden. Das kann sowohl beim elektronischen Versenden von Informationen als auch während eines Telefonats oder bei der persönlichen Übergabe von Datenträgern geschehen. Auf Auslandsreisen wird der sichere Informationsaustausch aufgrund von technisch unsicheren Gegebenheiten zum Teil noch weiter erschwert. Zudem kann es vorkommen, dass Geschäftsreisende vertrauliche Dokumente sowohl physischer als auch elektronischer Art in öffentlichen Räumen oder im Hotelzimmer aus Unachtsamkeit offen einsehbar liegen lassen.

Die Kommunikation mit unbekannten IT-Systemen und Netzen birgt immer ein Gefährdungspotenzial für das eigene Endgerät. So können z. B. auch vertrauliche Informationen kopiert werden.

Auf der anderen Seite können fremde Datenträger auch Schadprogramme enthalten. Hier besteht die Gefahr, dass wichtige Daten gestohlen, manipuliert, verschlüsselt oder vernichtet werden. Ebenso können aber auch Integrität und Verfügbarkeit von IT-Systemen beeinträchtigt werden. Dieser Aspekt wird durch die Tatsache begünstigt, dass ein Datenaustausch im Ausland häufig über unsichere Medien stattfindet. Dieser wichtige Aspekt ist den Mitarbeitenden jedoch nicht immer bewusst.

2.3. Vortäuschen einer falschen Identität

Im Rahmen von Kommunikation auf Reisen besteht eine erhöhte Gefahr, dass bei Angriffen sowohl persönlich als auch elektronisch versucht wird, eine falsche Identität vorzutäuschen oder eine autorisierte Identität zu übernehmen, z. B. durch Maskerade, Spoofing-Arten, Hijacking oder Man-in-the-Middle-Angriffe. Hierbei können Benutzende über die Identität ihres Kommunikationspartners oder ihrer Kommunikationspartnerin so getäuscht werden, dass sie schützenswerte Informationen preisgeben. Eine falsche digitale Identität erlangt die angreifende Person z. B. durch das Ausspähen von Benutzenden-ID und Passwort, die Manipulation des Absenderfeldes einer Nachricht oder durch die Manipulation einer Adresse im Netz.

Mitarbeitende kennen bei ausländischen Geschäftsbeziehungen ihre Kontaktpersonen nicht immer persönlich. Daher kann es passieren, dass sich fremde Personen mit dem Namen der Kontaktpersonen vorstellen und die Mitarbeitenden ihnen vertrauen und wertvolle Informationen weitergeben.

Die Sicherheitsanforderungen an Vertraulichkeit und Integrität können in institutionsfremden, vor allem ausländischen Gebäuden und Räumen, nie vollständig erfüllt werden. Daher besteht immer ein Restrisiko, dass auch Geräte manipuliert sein könnten, die normalerweise als sicher eingestuft würden. Dazu gehört etwa die Rufnummernanzeige am Telefon oder die Faxkennung eines Faxabsenders, durch die eine falsche Identität vorgetäuscht und Informationen erlangt werden können.

2.4. Fehlendes Sicherheitsbewusstsein und Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass es in Institutionen zwar organisatorische Regelungen und technische Sicherheitsverfahren für tragbare IT-Systeme und mobile Datenträger gibt, diese jedoch von den Beschäftigten nicht ausreichend beachtet und umgesetzt werden. Zum Beispiel lassen Mitarbeitende mobile Datenträger oft unbeaufsichtigt im Besprechungsraum oder auch im Zugabteil zurück.

Darüber hinaus werden Geschenke in Form von Datenträgern, wie etwa USB-Sticks, von Mitarbeitenden angenommen und unüberlegt an das eigene Notebook angeschlossen. Hier besteht dann die Gefahr, dass das Notebook mit Schadsoftware infiziert wird und dadurch schützenswerte Daten gestohlen, manipuliert oder verschlüsselt werden.

In öffentlichen Verkehrsmitteln oder auch während Geschäftsessen ist zudem immer wieder zu beobachten, dass Menschen offene Gespräche über geschäftskritische Informationen führen. Diese können dann von Außenstehenden leicht mitgehört und möglicherweise zum schwerwiegenden Nachteil der Mitarbeitenden oder ihrer Institution verwendet werden.

2.5. Verstoß gegen lokale Gesetze oder Regelungen

Bei Reisen ins Ausland sind insbesondere abweichende Gesetze und Regularien der Zieldestination zu berücksichtigen, da sich diese massiv von der nationalen Rechtslage unterscheiden können. Einschlägige Gesetze und Verordnungen des Ziellandes, z. B. zu Datenschutz, Informationspflichten, Haftung oder Informationszugriffe für Dritte, sind Reisenden häufig unbekannt oder werden falsch eingeschätzt. Dadurch kann nicht nur im Ausland, sondern auch im Inland gegen eine Vielzahl von Gesetzen verstoßen werden, beispielsweise wenn im Ausland personenbezogene Daten inländischer Kundschaft bei einer Auslandsdienstreise ungeschützt über öffentliche Netze übertragen werden.

2.6. Nötigung, Erpressung, Entführung und Korruption

Im Ausland gelten oft andere Sicherheitsrisiken aufgrund politischer und gesellschaftlicher Umstände. Die Sicherheit von Informationen, aber auch die Sicherheit der Reisenden selbst, könnte bei Auslandsreisen etwa durch Nötigung, Erpressung oder Entführung gefährdet werden. Mitarbeitende könnte zum Beispiel Gewalt angedroht werden, um sie zur Herausgabe von schützenswerten Daten zu

zwingen. Dabei werden sie dann genötigt, Sicherheitsrichtlinien und -maßnahmen zu umgehen bzw. zu missachten. Im Fokus stehen hierbei oftmals hochrangige Führungskräfte oder Mitarbeitende, die eine besondere Vertrauensstellung genießen.

Angriffe verfolgen vor allem das Ziel, schützenswerte Informationen zu stehlen oder zu manipulieren, um den Ablauf der Geschäftsprozesse zu beeinträchtigen oder sich und andere zu bereichern. Hier spielen vor allem politische, ideologische und wirtschaftliche Ziele der Angreifenden eine Rolle.

Neben der Androhung von Gewalt besteht auch die Möglichkeit der Bestechung oder Korruption. Reisenden werden etwa gezielt Geld oder andere Vorteile angeboten, um sie zur Herausgabe von vertraulichen Informationen an Unbefugte bzw. zu Sicherheitsverletzungen zu bewegen.

Generell werden durch Nötigung, Erpressung, Entführung und Korruption die Regelungen zur Informationssicherheit gestört bzw. ausgehebelt.

2.7. Informationen aus unzuverlässiger Quelle

Im Rahmen einer Auslandstätigkeit können den Reisenden absichtlich falsche oder irreführende Informationen zugespielt werden, um sie zu täuschen. In Folge dieser Täuschung könnten falsche Aussagen in geschäftskritische Berichte einfließen. Dies kann unter anderem dazu führen, dass geschäftsrelevante Informationen auf einer falschen Datenbasis beruhen, Berechnungen falsche Ergebnisse liefern und darauf basierend falsche Entscheidungen getroffen werden.

2.8. Diebstahl oder Verlust von Geräten, Datenträgern und Dokumenten

Insbesondere auf Reisen im Ausland ist damit zu rechnen, dass mobile Endgeräte leicht verloren gehen oder gestohlen werden. Je kleiner und begehrter diese Geräte sind, desto höher ist dieses Risiko. Neben dem rein materiellen Schaden durch den unmittelbaren Verlust des mobilen Gerätes kann durch die Offenlegung schützenswerter Daten, z. B. E-Mails, Notizen von Besprechungen oder Adressen, weiterer finanzieller Schaden entstehen. Außerdem kann der Ruf der Institution geschädigt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.7 *Informationssicherheit auf Auslandsreisen* 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	Benutzende, IT-Betrieb, Personalabteilung

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-Anforderung

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.7.A1 Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen (B)

Alle für die Informationssicherheit relevanten Aspekte, die in Verbindung mit den Tätigkeiten im Ausland stehen, MÜSSEN betrachtet und geregelt werden. Die Sicherheitsmaßnahmen, die in diesem Zusammenhang ergriffen werden, MÜSSEN in einer Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen dokumentiert werden. Diese Sicherheitsrichtlinie oder ein entsprechendes Merkblatt mit zu beachtenden Sicherheitsmaßnahmen MÜSSEN transnational agierenden Mitarbeitenden ausgehändigt werden.

Erweiternd MUSS ein Sicherheitskonzept zum Umgang mit tragbaren IT-Systemen auf Auslandsreisen erstellt werden, das alle Sicherheitsanforderungen und -maßnahmen angemessen detailliert beschreibt. Die Umsetzung des Sicherheitskonzeptes MUSS regelmäßig überprüft werden.

CON.7.A2 Sensibilisierung der Mitarbeitenden zur Informationssicherheit auf Auslandsreisen (B)

Benutzende MÜSSEN im verantwortungsvollen Umgang mit Informationstechnik bzw. tragbaren IT-Systemen auf Auslandsreisen sensibilisiert und geschult werden. Benutzende MÜSSEN die Gefahren kennen, die durch den unangemessenen Umgang mit Informationen, die unsachgemäße Vernichtung von Daten und Datenträgern oder durch Schadsoftware und den unsicheren Datenaustausch entstehen können. Außerdem MÜSSEN die Grenzen der eingesetzten Sicherheitsmaßnahmen aufgezeigt werden. Die Benutzenden MÜSSEN dazu befähigt und darin bestärkt werden, einem Verlust oder Diebstahl vorzubeugen bzw. bei Ungereimtheiten fachliche Beratung einzuholen. Außerdem SOLLTEN Mitarbeitende auf gesetzliche Anforderungen einzelner Reiseziele in Bezug auf die Reisesicherheit hingewiesen werden. Hierzu MUSS sich der oder die Informationssicherheitsbeauftragte über die gesetzlichen Anforderungen im Rahmen der Informationssicherheit (z. B. Datenschutz, IT-Sicherheitsgesetz) informieren und die Mitarbeitenden sensibilisieren.

CON.7.A3 Identifikation länderspezifischer Regelungen, Reise- und Umgebungsbedingungen (B) [Personalabteilung]

Vor Reiseantritt MÜSSEN die jeweils geltenden Regelungen der einzelnen Länder durch das Informationssicherheitsmanagement bzw. die Personalabteilung geprüft und an die entsprechenden Mitarbeitenden kommuniziert werden.

Die Institution MUSS geeignete Regelungen und Maßnahmen erstellen, umsetzen und kommunizieren, die den angemessenen Schutz interner Daten ermöglichen. Dabei MÜSSEN die individuellen Reise- und Umgebungsbedingungen berücksichtigt werden.

Außerdem MÜSSEN sich Mitarbeitende vor Reiseantritt mit den klimatischen Bedingungen des Reiseziels auseinandersetzen und abklären, welche Schutzmaßnahmen er für sich benötigt, z. B. Impfungen, und welche Schutzmaßnahmen für die mitgeführte Informationstechnik nötig sind.

CON.7.A4 Verwendung von Sichtschutz-Folien (B) [Benutzende]

Benutzende MÜSSEN insbesondere im Ausland darauf achten, dass bei der Arbeit mit mobilen IT-Geräten keine schützenswerten Informationen ausgespäht werden können. Dazu MUSS ein angemessener Sichtschutz verwendet werden, der den gesamten Bildschirm des jeweiligen Gerätes umfasst und ein Ausspähen von Informationen erschwert.

CON.7.A5 Verwendung der Bildschirm-/Code-Sperre (B) [Benutzende]

Eine Bildschirm- bzw. Code-Sperre, die verhindert, dass Dritte auf die Daten mobiler Endgeräte zugreifen können, MUSS verwendet werden. Die Benutzenden MÜSSEN dazu einen angemessenen Code bzw. ein sicheres Gerätepasswort verwenden. Die Bildschirmsperre MUSS sich nach einer kurzen Zeit der Inaktivität automatisch aktivieren.

CON.7.A6 Zeitnahe Verlustmeldung (B) [Benutzende]

Mitarbeitende MÜSSEN ihrer Institution umgehend melden, wenn Informationen, IT-Systeme oder Datenträger verloren gegangen sind oder gestohlen wurden. Hierfür MUSS es klare Meldewege und Kontaktpersonen innerhalb der Institution geben. Die Institution MUSS die möglichen Auswirkungen des Verlustes bewerten und geeignete Gegenmaßnahmen ergreifen.

CON.7.A7 Sicherer Remote-Zugriff auf das Netz der Institution (B) [IT-Betrieb, Benutzende]

Um Beschäftigten auf Auslandsreisen einen sicheren Fernzugriff auf das Netz der Institution zu ermöglichen, MUSS zuvor vom IT-Betrieb ein sicherer Remote-Zugang eingerichtet worden sein, z. B. ein Virtual Private Network (VPN). Der VPN-Zugang MUSS kryptografisch abgesichert sein. Außerdem MÜSSEN Benutzende über angemessen sichere Zugangsdaten verfügen, um sich gegenüber dem Endgerät und dem Netz der Institution erfolgreich zu authentisieren. Mitarbeitende MÜSSEN den sicheren Remote-Zugriff für jegliche darüber mögliche Kommunikation nutzen. Es MUSS sichergestellt werden, dass nur autorisierte Personen auf IT-Systeme zugreifen dürfen, die über einen Fernzugriff verfügen. Mobile IT-Systeme MÜSSEN im Rahmen der Möglichkeiten vor dem direkten Anschluss an das Internet durch eine restriktiv konfigurierte Personal Firewall geschützt werden.

CON.7.A8 Sichere Nutzung von öffentlichen WLANs (B) [Benutzende]

Grundsätzlich MUSS geregelt werden, ob mobile IT-Systeme direkt auf das Internet zugreifen dürfen.

Für den Zugriff auf das Netz der Institution über öffentlich zugängliche WLANs MÜSSEN Benutzende ein VPN oder vergleichbare Sicherheitsmechanismen verwenden (siehe CON.7.A7 *Sicherer Remote-Zugriff* und NET.2.2 *WLAN-Nutzung*). Bei der Benutzung von WLAN-Hotspots MÜSSEN ebenfalls Sicherheitsmaßnahmen getroffen werden, siehe auch INF.9 *Mobiler Arbeitsplatz*.

CON.7.A9 Sicherer Umgang mit mobilen Datenträgern (B) [Benutzende]

Werden mobile Datenträger verwendet, MÜSSEN Benutzende vorab gewährleisten, dass diese nicht mit Schadsoftware infiziert sind. Vor der Weitergabe mobiler Datenträger MÜSSEN Benutzende außerdem sicherstellen, dass keine schützenswerten Informationen darauf enthalten sind. Wird er nicht mehr genutzt, MUSS der Datenträger sicher gelöscht werden, insbesondere wenn er an andere Personen weitergegeben wird. Dazu MUSS der Datenträger mit einem in der Institution festgelegten, ausreichend sicheren Verfahren überschrieben werden.

CON.7.A10 Verschlüsselung tragbarer IT-Systeme und Datenträger (B) [Benutzende, IT-Betrieb]

Damit schützenswerte Informationen nicht durch unberechtigte Dritte eingesehen werden können, MÜSSEN Mitarbeitende vor Reiseantritt sicherstellen, dass alle schützenswerten Informationen entsprechend den internen Richtlinien abgesichert sind. Mobile Datenträger und IT-Systeme SOLLTEN dabei vor Reiseantritt durch Benutzende oder den IT-Betrieb verschlüsselt werden. Die kryptografischen Schlüssel MÜSSEN getrennt vom verschlüsselten Gerät aufbewahrt werden. Bei der Verschlüsselung von Daten SOLLTEN die gesetzlichen Regelungen des Ziellandes beachtet werden. Insbesondere landesspezifische Gesetze zur Herausgabe von Passwörtern und zur Entschlüsselung von Daten SOLLTEN berücksichtigt werden.

CON.7.A12 Sicheres Vernichten von schutzbedürftigen Materialien und Dokumenten (B) [Benutzende]

Die Institution MUSS den Beschäftigten Möglichkeiten aufzeigen, schutzbedürftige Dokumente angemessen und sicher zu vernichten. Benutzende MÜSSEN diese Regelungen einhalten. Sie DÜRFEN interne Unterlagen der Institution NICHT entsorgen, bevor diese sicher vernichtet worden sind. Ist dies vor Ort nicht möglich oder handelt es sich um Dokumente bzw. Datenträger mit besonders schützenswerten Informationen, MÜSSEN diese bis zur Rückkehr behalten und anschließend angemessen 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.7.A11 Einsatz von Diebstahl-Sicherungen (S) [Benutzende]

Zum Schutz der mobilen IT-Systeme außerhalb der Institution SOLLTEN Benutzende Diebstahl-Sicherungen einsetzen, vor allem dort, wo ein erhöhter Publikumsverkehr herrscht oder die Fluktuation von Benutzenden sehr hoch ist. Die Beschaffungs- und Einsatzkriterien für Diebstahl-Sicherungen SOLLTEN an die Prozesse der Institution angepasst und dokumentiert werden.

CON.7.A13 Mitnahme notwendiger Daten und Datenträger (S) [Benutzende]

Vor Reiseantritt SOLLTEN Benutzende prüfen, welche Daten während der Reise nicht unbedingt auf den IT-Systemen gebraucht werden. Ist es nicht notwendig, diese Daten auf den Geräten zu lassen, SOLLTEN diese sicher gelöscht werden. Ist es nötig, schützenswerte Daten mit auf Reisen zu nehmen, SOLLTE dies nur in verschlüsselter Form erfolgen. Darüber hinaus SOLLTE schriftlich geregelt sein, welche mobilen Datenträger auf Auslandsreisen mitgenommen werden dürfen und welche Sicherheitsmaßnahmen dabei zu berücksichtigen sind (z. B. Schutz vor Schadsoftware, Verschlüsselung geschäftskritischer Daten, Aufbewahrung mobiler Datenträger). Die Mitarbeitenden SOLLTEN diese Regelungen vor Reiseantritt kennen und beachten.

Diese sicherheitstechnischen Anforderungen SOLLTEN sich nach dem Schutzbedarf der zu bearbeitenden Daten im Ausland und der Daten, auf die zugegriffen werden soll, richten.

CON.7.A14 Kryptografisch abgesicherte E-Mail-Kommunikation (S) [Benutzende, IT-Betrieb]

Die E-Mail-basierte Kommunikation SOLLTEN Benutzende entsprechend den internen Vorgaben der Institution kryptografisch absichern. Die E-Mails SOLLTEN ebenfalls geeignet verschlüsselt bzw. digital signiert werden. Öffentliche IT-Systeme, etwa in Hotels oder Internetcafés, SOLLTEN NICHT für den Zugriff auf E-Mails genutzt werden.

Bei der Kommunikation über E-Mail-Dienste, z. B. Webmail, SOLLTE durch den IT-Betrieb vorab geklärt werden, welche Sicherheitsmechanismen beim Provider umgesetzt werden und ob damit die internen Sicherheitsanforderungen erfüllt werden. Hierzu SOLLTE z. B. der sichere Betrieb der Server, der Aufbau einer verschlüsselten Verbindung und die Dauer der Datenspeicherung zählen.

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.7.A15 Abstrahlsicherheit tragbarer IT-Systeme (H)

Es SOLLTE vor Beginn der Reise festgelegt werden, welchen Schutzbedarf die einzelnen Informationen haben, die auf dem mobilen Datenträger bzw. Client der Mitarbeitenden im Ausland verarbeitet werden. Die Institution SOLLTE prüfen, ob die mitgeführten Informationen einen besonderen Schutzbedarf haben, und entsprechend abstrahlarme bzw. -sichere Datenträger und Clients einsetzen.

CON.7.A16 Integritätsschutz durch Check-Summen oder digitale Signaturen (H) [Benutzende]

Benutzende SOLLTEN Check-Summen im Rahmen der Datenübertragung und Datensicherung verwenden, um die Integrität der Daten überprüfen zu können. Besser noch SOLLTEN digitale Signaturen verwendet werden, um die Integrität von schützenswerten Informationen zu bewahren.

CON.7.A17 Verwendung vorkonfigurierter Reise-Hardware (H) [IT-Betrieb]

Damit schützenswerte Informationen der Institution auf Auslandsreisen nicht von Dritten abgegriffen werden können, SOLLTE der IT-Betrieb den Mitarbeitenden vorkonfigurierte Reise-Hardware zur Verfügung stellen. Diese Reise-Hardware SOLLTE auf Basis des Minimalprinzips nur die Funktionen und Informationen bereitstellen, die zur Durchführung der Geschäftstätigkeit unbedingt erforderlich sind.

CON.7.A18 Eingeschränkte Berechtigungen auf Auslandsreisen (H) [IT-Betrieb]

Vor Reiseantritt SOLLTE geprüft werden, welche Berechtigungen Mitarbeitende wirklich brauchen, um ihrem Alltagsgeschäft im Ausland nachgehen zu können. Dabei SOLLTE geprüft werden, ob Zugriffsrechte für die Reisedauer der Benutzenden durch den IT-Betrieb entzogen werden können, um einen unbefugten Zugriff auf Informationen der Institution zu verhindern.

4. Weiterführende Informationen

4.1. Wissenswertes

Die „Initiative Wirtschaftsschutz“ gibt auf ihrer Website unter https://www.wirtschaftsschutz.info weiterführende Informationen zur Sicherheit auf Geschäftsreisen.

Bundesamt
für Sicherheit in der
Informationstechnik

CON.8 Software-Entwicklung

1. Beschreibung

1.1. Einleitung

Viele Institutionen stehen vor Herausforderungen, die sie nicht mehr hinreichend mit einem fertigen, unangepassten Softwareprodukt lösen können. Sie benötigen hierzu Software-Lösungen, die auf ihre individuellen Anforderungen hin angepasst sind. Beispiele hierfür sind hochspezifische Software-Lösungen für branchenspezialisierte (wie zur Steuerung von Produktionsanlagen) oder an die eigenen Geschäftsprozesse angepasste IT-Anwendungen (wie Content-Management-Systeme oder Identity-Management-Systeme). Aber auch Altsysteme, die nicht mehr vom ursprünglichen herstellendem Unternehmen weitergepflegt werden, können individuell weiterentwickelt werden.

Hierbei kann (Individual-) Software durch die Institution selbst oder von einem Dritten entwickelt werden. Die Software-Entwicklung nimmt dabei eine zentrale Rolle ein, wenn aus den Anforderungen der Institution ein Programm-Code entwickelt bzw. angepasst wird. Hierbei ist es von essentieller Bedeutung, dass die Informationssicherheit über den gesamten Software-Entwicklungsprozess hinweg berücksichtigt wird und nicht erst in einer späteren Phase. Nur auf diese Weise kann die Informationssicherheit der zu entwickelnden Software-Lösung nachhaltig gewährleistet werden.

Software kann dabei im Rahmen von klassischen, in sich abgeschlossenen Projekten entwickelt werden, oder aber als kontinuierliche Tätigkeit ohne festes Ende. In beiden Fällen werden in der Praxis sehr häufig Werkzeuge aus dem Projektmanagement benutzt, um die Software-Entwicklung zu koordinieren und zu steuern. Deswegen wird in diesem Baustein der Begriff Projekt vermehrt verwendet und auch nicht durchgehend zwischen einer projektbasierten und kontinuierlichen Entwicklung unterschieden, da sich die damit verbundenen Vorgehensweisen und Werkzeuge ähneln.

1.2. Zielsetzung

Der Baustein beschäftigt sich mit allen relevanten Sicherheitsaspekten, die von Institutionen bei der Eigenentwicklung von Software zu beachten sind. Hierzu wird betrachtet, wie eine Institution die Software-Entwicklung vorbereiten und durchführen kann. Es werden entsprechende Gefährdungen identifiziert und Anforderungen formuliert.

1.3. Abgrenzung und Modellierung

Der Baustein CON.8 *Software-Entwicklung* ist für jedes Entwicklungsvorhaben im Informationsverbund anzuwenden, wenn Software entwickelt werden soll.

Wird Software entwickelt, liegt sehr häufig ein auftraggebendes und auftragnehmendes Verhältnis vor. Im IT-Grundschutz spiegelt sich dieser Sachverhalt wider, indem der Baustein APP.7 *Entwicklung von Individualsoftware* die auftraggebende Seite und der Baustein CON.8 *Software-Entwicklung* die auftragnehmende Seite umfassen. Die Anforderungen dieses Bausteins sind somit von Auftragnehmenden zu erfüllen. Die für die Software-Entwicklung relevanten Anforderungen (funktionale und nicht-funktionale Anforderungen, Anforderungen an die sichere Vorgehensweise sowie das Sicherheitsprofil) werden vom Auftraggebenden im Rahmen des Bausteins APP.7 *Entwicklung von Individualsoftware* erhoben.

Der Baustein stellt keine vollständige Anleitung oder generelle Vorgehensweise für die Entwicklung von Software dar, sondern er konzentriert sich auf die relevanten Aspekte der Informationssicherheit bei der Software-Entwicklung. Der Baustein umfasst ferner keine Aspekte zum Patch- und Änderungsmanagement. Hierzu ist der Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* anzuwenden.

Die Abnahme und hiermit verbundenen Tests von eigenentwickelter bzw. beauftragter Software werden in dem Baustein OPS.1.1.6 *Software-Tests und Freigaben* geregelt. Darüber hinaus gehende Aspekte zu Tests im Rahmen der Software-Entwicklung werden in diesem Baustein CON.8 *Software-Entwicklung* behandelt.

Der Baustein ORP.5 *Compliance Management (Anforderungsmanagement)* muss mit betrachtet werden, da über diesen Baustein geregelt wird, wie die gesetzlichen und institutsinterne Vorgaben, sowie Anforderungen der Kundschaft berücksichtigt werden.

Umfasst die Software-Entwicklung kryptographische Aspekte, dann sind die relevanten Anforderungen aus dem Baustein CON.1 *Kryptokonzept* zu berücksichtigen.

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.8 *Software-Entwicklung* von besonderer Bedeutung.

2.1. Auswahl eines ungeeigneten Vorgehensmodells

Vorgehensmodelle strukturieren und planen den Ablauf der Software-Entwicklung, indem bestimmte Handlungsschritte und deren Abfolge vorgegeben werden. Wird ein ungeeignetes Vorgehensmodell bei der Software-Entwicklung ausgewählt, kann der Verlauf der Entwicklung und das damit verbundene Entwicklungsprojekt erheblich gestört werden. Je nachdem, wie das gewählte Modell ausgeprägt und wie umfangreich das Entwicklungsvorhaben ist, könnten entweder wichtige Aspekte vernachlässigt oder irrelevante Aspekte übermäßig fokussiert werden. Beide genannten Probleme erhöhen den Arbeitsaufwand im Projektmanagement und schränken die produktive Arbeit ein.

Wird gar kein Vorgehensmodell verwendet, erhöht sich die Gefahr, dass relevante Aspekte, die insbesondere die Informationssicherheit betreffen, in der Software-Entwicklung nicht in geeigneter Art und Weise berücksichtigt werden. Dies kann dazu führen, dass relevante Sicherheitsfunktionen überhaupt nicht implementiert oder getestet werden, sodass die entwickelte Software nicht den Sicherheitsanforderungen entspricht.

2.2. Auswahl einer ungeeigneten Entwicklungsumgebung

Wird eine Entwicklungsumgebung ungeeignet oder von den Mitarbeitenden individuell ausgewählt, können dringend benötigte Funktionen fehlen oder nicht in ausreichender Form implementiert sein. Weiterhin kann eine ungeeignete Entwicklungsumgebung auch Fehler oder Schwachstellen aufweisen, die erhebliche Störungen im Verlauf der Software-Entwicklung verursachen können.

Wenn keine bestimmte Entwicklungsumgebung ausgewählt und vorgegeben wird, arbeiten verschiedene Entwickelnde möglicherweise mit unterschiedlichen, selbst gewählten Werkzeugen an der Software und können dadurch Kompatibilitätsprobleme verursachen. Beispielweise können unterschiedliche Compiler solche Kompatibilitätsprobleme auslösen.

2.3. Fehlende oder unzureichende Qualitätssicherung des Entwicklungsprozesses

Durch eine fehlende oder unzureichende Qualitätssicherung während der Software-Entwicklung kann sich das Entwicklungsvorhaben verzögern oder sogar gänzlich scheitern. Wenn nicht geprüft wird, ob die eigenentwickelte Software sicher implementiert wird, drohen Schwachstellen in der ausgelieferten Software.

Ist die Qualitätssicherung nicht fest im Entwicklungsprozess verankert, können Fehler und Manipulationen in der Konzeption oder Implementierung unter Umständen nicht erkannt werden. Dabei sollte die Aufmerksamkeit nicht nur selbst entwickelten Bestandteilen, sondern gerade auch externen Beiträgen und übernommenen Bestandteilen gelten.

2.4. Fehlende oder unzureichende Dokumentation

Wird die Software in der Konzeptions- oder Entwicklungsphase nicht oder nur unzureichend dokumentiert, kann dies dazu führen, dass eventuelle Fehler nur verzögert oder gar nicht diagnostiziert und behoben werden können. Wird die Entwicklung ungeeignet dokumentiert, kann die Software außerdem später nur mit hohem Aufwand aktualisiert, angepasst oder erweitert werden.

Bei unzureichender Administrations- oder Benutzendendokumentation könnte die Software im produktiven Betrieb fehlerhaft verwaltet oder bedient werden. Dies kann beispielsweise den IT-Betrieb stören, falsche Arbeitsergebnisse verursachen oder den Arbeitsablauf verzögern.

2.5. Unzureichend gesicherter Einsatz von Entwicklungsumgebungen

Wenn die Entwicklungsumgebung unzureichend gesichert wird, kann die zu produzierende Software möglicherweise manipuliert werden. Solche Manipulationen können dadurch nachträglich nur schwer erkannt werden.

Wenn nicht bekannt ist, welche Benutzenden zu welchem Zeitpunkt auf die Entwicklungsumgebung zugreifen können und konnten, kann die Software anonym manipuliert werden. Sofern die manipulierten Teile der Software entdeckt werden, kann dann unter Umständen nicht nachvollzogen werden, welche Benutzenden sie manipuliert haben.

Bei einer fehlenden oder unzureichenden Versionsverwaltung des Quellcodes ist es nicht möglich, Änderungen zuverlässig nachzuvollziehen sowie vorherige und bereits funktionierende Versionen der Software wiederherzustellen.

Wenn Quellcodes unzureichend vor versehentlichen oder absichtlichen Änderungen geschützt werden, können Teile eines Quellcodes oder sogar der gesamte Quellcode beschädigt werden und die bereits eingebrachte Arbeitsleistung verloren gehen.

Wird der Quellcode bzw. die Versionsverwaltung nicht hinreichend vor einem Datenverlust geschützt, folgen daraus verschiedene Gefährdungen, unabhängig davon, ob der Datenverlust z. B. durch einen technischen Defekt oder durch menschliches Versagen ausgelöst wird. Möglicherweise kann die Software überhaupt nicht mehr weiterentwickelt werden, da der Datenbestand gänzlich fehlt, oder es ist nur ein veralteter und möglicherweise fehlerhafter Zwischenstand verfügbar, der nur mit sehr hohen Aufwänden verwendet werden kann.

2.6. Software-Konzeptionsfehler

Je umfangreicher eine Software vom Funktionsumfang wird, umso umfangreicher wird häufig auch ihr Programm-Code. Wenn der Programm-Code nicht durch geeignete Maßnahmen strukturiert wird und wenn er nicht auf einer angemessenen Software-Architektur basiert, dann kann er zumeist nur sehr schwer gewartet werden. So können Sicherheitslücken nur schwer geschlossen oder veraltete Programm-Teile nur mit sehr hohen Aufwand ausgetauscht werden, wenn sich z. B. der Schutzbedarf der verarbeiteten Daten ändert und somit auch die Sicherheitsanforderungen an die Software.

Software-Konzeptionsfehler erschweren hierbei nicht nur die Wartung der Software, sondern sie können selbst zu Sicherheitslücken und Gefährdungen führen. Ist der Programm-Code nicht sinnvoll strukturiert und die Software-Architektur nicht nachvollziehbar dokumentiert, dann können konzeptionelle Fehler in Software-Tests nur sehr schwer identifiziert werden. In Folge dessen können auf den unterschiedlichsten Ebenen der Software Sicherheitslücken bestehen.

Software-Konzeptionsfehler sind in der Praxis häufig historisch bedingt, indem z. B. Altsysteme für Aufgaben und Umgebungen eingesetzt werden, für diese sie zuerst gar nicht konzeptioniert worden sind. Auch wurden bei der Software-Entwicklung von sehr alten Anwendungen Aspekte wie Wartbarkeit und Modifizierbarkeit nicht in dem erforderlichen Maße berücksichtigt, wie es heute dem Stand der Technik entspricht.

2.7. Fehlendes oder unzureichendes Test- und Freigabeverfahren

Wird neue Software nicht ausreichend getestet und freigegeben, können Fehler in der Software nicht erkannt werden. Solche Fehler gefährden nicht nur den produktiven Einsatz und die Informationssicherheit der neuen Software selbst, sondern unter Umständen auch andere Anwendungen und IT-Systeme in der Produktivumgebung.

Werden Sicherheitsfunktionen bzw. die grundlegenden Sicherheitsanforderungen nicht getestet, ist nicht sichergestellt, dass die entwickelte Software den Sicherheitsanforderungen der einsetzenden Institution genügt. In Folge dessen könnten schützenswerte Informationen offengelegt, manipuliert oder zerstört werden, indem z. B. unbefugte Dritte aufgrund mangelhafter Authentifizierungsfunktionen auf die Software zugreifen.

2.8. Software-Tests mit Produktivdaten

Wenn neue Software mit Produktivdaten getestet wird, könnten eventuell nicht befugte Personen hierbei vertrauliche Informationen einsehen, wie besonders schützenswerte personenbezogene Daten.

Wird nicht mit Kopien der Produktivdaten getestet, sondern mit den Originalen (z. B. bei Datenbanksystemen) entstehen noch umfangreichere Gefährdungen:

- Fehlfunktionen von Software während des Testens können dazu führen, dass neben der Vertraulichkeit der Produktivdaten auch deren Integrität oder Verfügbarkeit beeinträchtigt wird.
- Ungewollte Veränderungen an Produktivdaten können auch dadurch entstehen, dass die Software fehlerhaft getestet oder bedient wird. Möglicherweise wird diese Veränderung nicht zeitnah festgestellt. Solche Fehler können sich auch auf andere IT-Anwendungen auswirken, die auf die gleichen Datenbestände zugreifen.

Diese Umstände werden sehr häufig dadurch verschärft, dass während die Software getestet wird, nicht der Schutz der Testdaten im Vordergrund steht, sondern, ob die Software sich wie gewünscht, bzw. durch die Anforderungen definiert, verhält.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.8 *Software-Entwicklung* 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	Fachverantwortliche
Weitere Zuständigkeiten	Testende, Zentrale Verwaltung, IT-Betrieb, Entwickelnde

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.8.A2 Auswahl eines Vorgehensmodells (B)

Ein geeignetes Vorgehensmodell zur Software-Entwicklung MUSS festgelegt werden. Anhand des gewählten Vorgehensmodells MUSS ein Ablaufplan für die Software-Entwicklung erstellt werden. Die Sicherheitsanforderungen der Auftraggebenden an die Vorgehensweise MÜSSEN im Vorgehensmodell integriert werden.

Das ausgewählte Vorgehensmodell, einschließlich der festgelegten Sicherheitsanforderungen, MUSS eingehalten werden.

Das Personal SOLLTE in der Methodik des gewählten Vorgehensmodells geschult sein.

CON.8.A3 Auswahl einer Entwicklungsumgebung (B)

Eine Liste der erforderlichen und optionalen Auswahlkriterien für eine Entwicklungsumgebung MUSS von Fachverantwortlichen für die Software-Entwicklung erstellt werden. Die Entwicklungsumgebung MUSS anhand der vorgegebenen Kriterien ausgewählt werden.

CON.8.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

CON.8.A5 Sicheres Systemdesign (B)

Folgende Grundregeln des sicheren Systemdesigns MÜSSEN in der zu entwickelnden Software berücksichtigt werden:

- Grundsätzlich MÜSSEN alle Eingabedaten vor der Weiterverarbeitung geprüft und validiert werden.
- Bei Client-Server-Anwendungen MÜSSEN die Daten grundsätzlich auf dem Server validiert werden.
- Die Standardeinstellungen der Software MÜSSEN derart voreingestellt sein, dass ein sicherer Betrieb der Software ermöglicht wird.
- Bei Fehlern oder Ausfällen von Komponenten des Systems DÜRFEN NICHT schützenswerte Informationen preisgegeben werden.

- Die Software MUSS mit möglichst geringen Privilegien ausgeführt werden können.
- Schützenswerte Daten MÜSSEN entsprechend der Vorgaben des Kryptokonzepts verschlüsselt übertragen und gespeichert werden.
- Zur Benutzenden-Authentisierung und Authentifizierung MÜSSEN vertrauenswürdige Mechanismen verwendet werden, die den Sicherheitsanforderungen an die Anwendung entsprechen.
- Falls zur Authentifizierung Passwörter gespeichert werden, MÜSSEN diese mit einem sicheren Hashverfahren gespeichert werden.
- Sicherheitsrelevante Ereignisse MÜSSEN in der Art protokolliert werden, dass sie im Nachgang ausgewertet werden können.
- Informationen, die für den Produktivbetrieb nicht relevant sind (z. B. Kommentare mit Zugangsdaten für die Entwicklungsumgebung), SOLLTEN in ausgeliefertem Programmcode und ausgelieferten Konfigurationsdateien entfernt werden.

Das Systemdesign MUSS dokumentiert werden. Es MUSS überprüft werden, ob alle Sicherheitsanforderungen an das Systemdesign erfüllt wurden.

CON.8.A6 Verwendung von externen Bibliotheken aus vertrauenswürdigen Quellen (B)

Wird im Rahmen des Entwicklungs- und Implementierungsprozesses auf externe Bibliotheken zurückgegriffen, MÜSSEN diese aus vertrauenswürdigen Quellen bezogen werden. Bevor externe Bibliotheken verwendet werden, MUSS deren Integrität sichergestellt werden.

CON.8.A7 Durchführung von entwicklungsbegleitenden Software-Tests (B) [Testende, Entwickelnde]

Schon bevor die Software im Freigabeprozess getestet und freigegeben wird, MÜSSEN entwicklungsbegleitende Software-Tests durchgeführt und der Quellcode auf Fehler gesichtet werden. Hierbei SOLLTEN bereits die Fachverantwortlichen des Auftraggebenden oder der beauftragenden Fachabteilung beteiligt werden.

Die entwicklungsbegleitenden Tests MÜSSEN die funktionalen und nichtfunktionalen Anforderungen der Software umfassen. Die Software-Tests MÜSSEN dabei auch Negativtests abdecken. Zusätzlich MÜSSEN auch alle kritischen Grenzwerte der Eingabe sowie der Datentypen überprüft werden.

Testdaten SOLLTEN dafür sorgfältig ausgewählt und geschützt werden. Darüber hinaus SOLLTE eine automatische statische Code-Analyse durchgeführt werden.

Die Software MUSS in einer Test- und Entwicklungsumgebung getestet werden, die getrennt von der Produktionsumgebung ist. Außerdem MUSS getestet werden, ob die Systemvoraussetzungen für die vorgesehene Software ausreichend dimensioniert sind.

CON.8.A8 Bereitstellung von Patches, Updates und Änderungen (B) [Entwickelnde]

Es MUSS sichergestellt sein, dass sicherheitskritische Patches und Updates für die entwickelte Software zeitnah durch die Entwickelnden bereitgestellt werden. Werden für verwendete externe Bibliotheken sicherheitskritische Updates bereitgestellt, dann MÜSSEN die Entwickelnden ihre Software hierauf anpassen und ihrerseits entsprechende Patches und Updates zur Verfügung stellen.

Für die Installations-, Update- oder Patchdateien MÜSSEN vom Entwickelnden Checksummen oder digitale Signaturen bereitgestellt werden.

CON.8.A9 ENTFALLEN (B)

Diese Anforderung ist entfallen.

CON.8.A10 Versionsverwaltung des Quellcodes (B) [Entwickelnde]

Der Quellcode des Entwicklungsprojekts MUSS über eine geeignete Versionsverwaltung verwaltet werden. Die Institution MUSS den Zugriff auf die Versionsverwaltung regeln und festlegen, wann Änderungen am Quellcode durch die Entwickelnden als eigene Version in der Versionsverwaltung gespeichert werden sollen. Es MUSS sichergestellt sein, dass durch die Versionsverwaltung alle Änderungen am Quellcode nachvollzogen und rückgängig gemacht werden können.

Die Versionsverwaltung MUSS in dem Datensicherungskonzept berücksichtigt werden. Die Versionsverwaltung DARF NICHT ohne Datensicherung erfolgen.

CON.8.A20 Überprüfung von externen Komponenten (B)

Unbekannte externe Komponenten (bzw. Programm-Bibliotheken), deren Sicherheit nicht durch etablierte und anerkannte Peer-Reviews oder vergleichbares sichergestellt werden kann, MÜSSEN auf Schwachstellen überprüft werden. Alle externen Komponenten MÜSSEN auf potentielle Konflikte überprüft werden.

Die Integrität von externen Komponenten MUSS durch Prüfsummen oder kryptographische Zertifikate überprüft werden.

Darüber hinaus SOLLTEN keine veralteten Versionen von externen Komponenten in aktuellen Entwicklungsprojekten verwendet 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.8.A1 Definition von Rollen und Zuständigkeiten (S) [Zentrale Verwaltung]

Für den Software-Entwicklungsprozess SOLLTE eine gesamtzuständige Person ein benannt werden. Außerdem SOLLTEN die Rollen und Zuständigkeiten für alle Aktivitäten im Rahmen der Software-Entwicklung festgelegt werden. Die Rollen SOLLTEN dabei fachlich die nachfolgenden Themen abdecken:

- Requirements-Engineering (Anforderungsmanagement) und Änderungsmanagement,
- Software-Entwurf und -Architektur,
- Informationssicherheit in der Software-Entwicklung,
- Software-Implementierung in dem für das Entwicklungsvorhaben relevanten Bereichen, sowie
- Software-Tests.

Für jedes Entwicklungsvorhaben SOLLTE eine zuständige Person für die Informationssicherheit benannt werden.

CON.8.A11 Erstellung einer Richtlinie für die Software-Entwicklung (S)

Es SOLLTE eine Richtlinie für die Software-Entwicklung erstellt und aktuell gehalten werden. Die Richtlinie SOLLTE neben Namenskonventionen auch Vorgaben zu Elementen beinhalten, die verwendet bzw. nicht verwendet werden dürfen. Die relevanten Anforderungen aus diesem Baustein SOLLTEN in die Richtlinie aufgenommen werden. Die Richtlinie SOLLTE für die Entwickelnden verbindlich sein.

CON.8.A12 Ausführliche Dokumentation (S)

Es SOLLTEN ausreichende Projekt-, Funktions- und Schnittstellendokumentationen erstellt und aktuell gehalten werden. Die Betriebsdokumentation SOLLTE konkrete Sicherheitshinweise für die Installation und Konfiguration für Administration, sowie für die Benutzung des Produktes beinhalten.

Die Software-Entwicklung SOLLTE so dokumentiert sein, dass Fachleute mithilfe der Dokumentation den Programm-Code nachvollziehen und weiterentwickeln können. Die Dokumentation SOLLTE dabei auch die Software-Architektur und Bedrohungsmodellierung umfassen.

Die Aspekte zur Dokumentation SOLLTEN im Vorgehensmodell zur Software-Entwicklung berücksichtigt werden.

CON.8.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.8.A14 Schulung des Entwicklungsteams zur Informationssicherheit (S)

Die Entwickelnden und die übrigen Mitglieder des Entwicklungsteams SOLLTEN zu generellen Informationssicherheitsaspekten und zu den jeweils speziell für sie relevanten Aspekten geschult sein:

- Anforderungsanalyse,
- Projektmanagement allgemein sowie speziell bei der Software-Entwicklung,
- Risikomanagement bzw. Bedrohungsmodellierung in der Software-Entwicklung,
- Qualitätsmanagement und Qualitätssicherung,
- Modelle und Methoden für die Software-Entwicklung,
- Software-Architektur,
- Software-Tests,
- Änderungsmanagement sowie
- Informationssicherheit, Sicherheitsvorgaben in der Institution und Sicherheitsaspekte in speziellen Bereichen.

CON.8.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

CON.8.A16 Geeignete Steuerung der Software-Entwicklung (S)

Bei einer Software-Entwicklung SOLLTE ein geeignetes Steuerungs- bzw. Projektmanagementmodell auf Basis des ausgewählten Vorgehensmodells verwendet werden. Das Steuerungs- bzw. Projektmanagementmodell SOLLTE in die Richtlinie zur Software Entwicklung integriert werden. Dabei SOLLTEN insbesondere die benötigten Qualifikationen beim Personal und die Abdeckung aller relevanten Phasen während des Lebenszyklus der Software berücksichtigt werden. Für das Vorgehensmodell SOLLTE ein geeignetes Risikomanagement festgelegt werden. Außerdem SOLLTEN geeignete Qualitätsziele für das Entwicklungsprojekt definiert werden.

CON.8.A21 Bedrohungsmodellierung (S)

In der Entwurfsphase der Software-Entwicklung SOLLTE eine Bedrohungsmodellierung durchgeführt werden. Hierzu SOLLTEN auf Basis des Sicherheitsprofils, des Anforderungskatalogs und der geplanten Einsatzumgebung bzw. Einsatzszenarios potentielle Bedrohungen identifiziert werden. Die Bedrohungen SOLLTEN hinsichtlich ihrer Eintrittswahrscheinlichkeit und Auswirkung bewertet werden.

CON.8.A22 Sicherer Software-Entwurf (S)

Der Software-Entwurf SOLLTE den Anforderungskatalog, das Sicherheitsprofil und die Ergebnisse der Bedrohungsmodellierung berücksichtigen. Im Rahmen des sicheren Software-Entwurfs SOLLTE eine sichere Software-Architektur entwickelt werden, auf deren Grundlage der Quellcode der Anwendung zu entwickeln ist. Hierbei SOLLTEN möglichst zukünftige Standards und Angriffstechniken berücksichtigt werden, damit die zu entwickelnde Software auch zukünftig leicht gewartet werden kann.

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.8.A17 Auswahl vertrauenswürdiger Entwicklungswerkzeuge (H)

Zur Entwicklung der Software SOLLTEN nur Werkzeuge mit nachgewiesenen Sicherheitseigenschaften verwendet werden. An die herstellenden Unternehmen von Hardware oder Software SOLLTEN hinreichende Anforderungen zur Sicherheit ihrer Werkzeuge gestellt werden.

CON.8.A18 Regelmäßige Sicherheitsaudits für die Entwicklungsumgebung (H)

Es SOLLTEN regelmäßige Sicherheitsaudits der Software-Entwicklungsumgebung und der Software-Testumgebung durchgeführt werden.

CON.8.A19 Regelmäßige Integritätsprüfung der Entwicklungsumgebung (H) [IT-Betrieb]

Die Integrität der Entwicklungsumgebung SOLLTE regelmäßig mit kryptographischen Mechanismen entsprechend dem Stand der Technik geprüft werden. Die Prüfsummendateien und das Prüfprogramm selbst SOLLTEN ausreichend vor Manipulationen geschützt sein. Wichtige Hinweise auf einen Integritätsverlust SOLLTEN nicht in einer Fülle irrelevanter Warnmeldungen (false positives) untergehen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) stellt Anforderungen zur Software-Entwicklung unter anderem in diesen Normen:

- ISO/IEC 27001:2013 Apendix A.14.2 „Security in development and support processes“ - Anforderungen an die Sicherheit in Entwicklungs- und Unterstützungsprozessen,
- ISO/IEC 25000:2014 „Systems and software Quality Requirements and Evaluation - Guide to SQuaRE“ - ein genereller Überlick über die SQuaRE-Normen-Reihe,
- ISO/IEC 25001:2014 „Planning and management“ - Anforderungen an die Planung und das Management" sowie
- ISO/IEC 25010:2011 „System and software quality models“ - Anforderungen an ein Qualitätsmodell und Leitlinien.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel „SD System Development“ Vorgaben an die sichere Software-Entwicklung.

Das National Institute of Standards and Technologie gibt in seiner Special Publication 800-160 „Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems“ Anforderungen an ein sicheres Systemdesign.

Die Fachgruppe „Vorgehensmodelle für die betriebliche Anwendungsentwicklung“ der Gesellschaft für Informatik gibt in ihren Publikationen einen Überblick über aktuelle Informationen zur Anwendungsentwicklung.

Weiterführende Informationen zur Bedrohungsmodellierung können dem wissenschaftlichen Artikel „Bedrohungsmodellierung (Threat Modeling) in der Softwareentwicklung“ entnommen werden. Der

Artikel wurde zu der Konferenz „Sicherheit 2010: Sicherheit, Schutz und Zuverlässigkeit)“ der Gesellschaft für Information veröffentlicht.

Bundesamt
für Sicherheit in der
Informationstechnik

CON.9 Informationsaustausch

1. Beschreibung

1.1. Einleitung

Informationen werden zwischen Sendenden und Empfangenden über unterschiedliche Kommunikationswege übertragen, wie z. B. persönliche Gespräche, Telefonate, Briefpost, Wechseldatenträger oder Datennetze. Regeln zum Informationsaustausch stellen sicher, dass vertrauliche Informationen nur an berechtigte Personen weitergegeben werden. Solche Regelungen sind besonders dann notwendig, wenn Informationen über externe Datennetze übermittelt werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, den Informationsaustausch zwischen verschiedenen Kommunikationspartnern abzusichern. Mithilfe dieses Bausteins lässt sich ein Konzept zum sicheren Informationsaustausch erstellen.

1.3. Abgrenzung und Modellierung

Der Baustein CON.9 *Informationsaustausch* ist einmal auf den gesamten Informationsverbund anzuwenden, wenn Informationen mit Kommunikationspartnern, die nicht dem Informationsverbund angehören, ausgetauscht werden sollen.

Die Absicherung von Netzverbindungen wird in anderen Bausteinen des IT-Grundschutz-Kompendiums behandelt, siehe Schicht NET *Netze und Kommunikation.* Anforderungen an Wechseldatenträger (siehe Baustein SYS.4.5 *Wechseldatenträger*) und die Weiterverarbeitung in IT-Systemen außerhalb des Informationsverbunds werden ebenfalls nicht in diesem Baustein berücksichtigt.

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.9 *Informationsaustausch* von besonderer Bedeutung.

2.1. Nicht fristgerecht verfügbare Informationen

Der Informationsaustausch kann gestört, verzögert oder unterbrochen werden.

Informationen treffen verzögert oder nicht vollständig ein oder werden zu langsam verarbeitet, wenn die eingesetzte Technik Übertragungsfehler erzeugt. Unter Umständen endet der Austausch von Informationen vollständig, weil Schnittstellen oder Betriebsmittel nicht leistungsfähig genug sind oder ausfallen.

Geschäftsprozesse können erheblich beeinträchtigt werden, wenn erforderliche Fristen zur Lieferung von Informationen nicht eingehalten werden. Im Extremfall werden vertraglich vereinbarte Fristen gebrochen, weil eine Datenübertragung durch technisches oder menschliches Versagen scheitert.

2.2. Ungeregelte Weitergabe von Informationen

Schutzbedürftige Informationen können in die Hände unbefugter Personen gelangen.

Es kann nicht beeinflusst werden, wer eine Information erhält und nutzt, wenn z. B. im Vorfeld eines Informationsaustauschs versäumt wurde, eine Vertraulichkeitsvereinbarung abzuschließen. Das Risiko des Datenmissbrauchs erhöht sich ebenfalls, wenn die Vertraulichkeitsvereinbarung unpräzise oder lückenhaft formuliert wurde.

2.3. Weitergabe falscher oder interner Informationen

Schutzbedürftige Informationen können an unbefugte Empfangende versendet werden.

Schutzbedürftige Informationen können versehentlich in falsche Hände gelangen, falls das Personal nicht ausreichend sensibilisiert und geschult wird. So werden können z. B. Datenträger weitergegeben werden, auf denen sich Restinformationen wie unzureichend gelöschte Alt-Daten befinden. Andere Restinformationen sind ungelöschte interne Kommentare, die versehentlich in einem elektronischen Dokument, z. B. als E-Mail-Anhang, übermittelt werden. In weiteren Fällen werden z. B. vertrauliche Unterlagen versehentlich an die falsche Person verschickt, weil klare Handlungsvorgaben für den Umgang mit vertraulichen Unterlagen fehlen.

2.4. Unberechtigtes Kopieren oder Verändern von Informationen

Informationen und Daten können unbemerkt durch Angriffe abgegriffen oder beeinflusst werden.

Bei Angriffen können Informationen vorsätzlich gestohlen werden, wenn sie nicht ausreichend geschützt werden. So kann bei einem Angriff z. B. ein Datenträger auf dem Postweg abfangen oder unbemerkt der Inhalt einer ungeschützt versendeter E-Mails gelesen werden. Außerdem können bei Angriffen ungeschützte Informationen verändert werden, während sie übertragen werden und so beispielsweise Schadsoftware in Dateien eingespielt werden.

2.5. Unzulängliche Anwendung von Verschlüsselungsverfahren

Der Schutz von Informationen während der Übertragung mithilfe kryptographischer Verfahren kann durch Angriffe unterlaufen werden.

Falls das kryptographische Verfahren bei einem Angriff bekannt ist, können die verschlüsselten Daten und der zugehörige Schlüssel abfangen werden, wenn die Verschlüsselungsverfahren nicht sachgerecht anwendet werden. Mitarbeitende, die nicht ausreichend geschult wurden, könnten z. B. den Schlüssel gemeinsam mit den Daten auf demselben Datenträger verschicken. Darüber hinaus werden beispielsweise oft Schlüssel verwendet, die zu leicht zu erraten sind.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.9 *Informationsaustausch* 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	Fachverantwortliche, Benutzende, Zentrale Verwaltung

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.9.A1 Festlegung zulässiger Empfangender (B) [Zentrale Verwaltung]

Die zentrale Verwaltungsstelle MUSS sicherstellen, dass durch die Weitergabe von Informationen nicht gegen rechtliche Rahmenbedingungen verstoßen wird.

Die zentrale Verwaltungsstelle MUSS festlegen, wer welche Informationen erhalten und weitergeben darf. Es MUSS festgelegt werden, auf welchen Wegen die jeweiligen Informationen ausgetauscht werden dürfen. Alle Beteiligten MÜSSEN vor dem Austausch von Informationen sicherstellen, dass die empfangende Stelle die notwendigen Berechtigungen für den Erhalt und die Weiterverarbeitung der Informationen besitzt.

CON.9.A2 Regelung des Informationsaustausches (B)

Bevor Informationen ausgetauscht werden, MUSS die Institution festlegen, wie schutzbedürftig die Informationen sind. Sie MUSS festlegen, wie die Informationen bei der Übertragung zu schützen sind.

Falls schutzbedürftige Daten übermittelt werden, MUSS die Institution die Empfangenden darüber informieren, wie schutzbedürftig die Informationen sind. Falls die Informationen schutzbedürftig sind, MUSS die Institution die Empfangenden darauf hingewiesen werden, dass diese die Daten ausschließlich zu dem Zweck nutzen dürfen, zu dem sie übermittelt wurden.

CON.9.A3 Unterweisung des Personals zum Informationsaustausch (B) [Fachverantwortliche]

Fachverantwortliche MÜSSEN die Mitarbeitenden über die Rahmenbedingungen jedes Informationsaustauschs informieren. Die Fachverantwortlichen MÜSSEN sicherstellen, dass die Mitarbeitenden wissen, welche Informationen sie wann, wo und wie weitergeben dürfen.

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.9.A4 Vereinbarungen zum Informationsaustausch mit Externen (S) [Zentrale Verwaltung]

Bei einem regelmäßigen Informationsaustausch mit anderen Institutionen SOLLTE die Institution die Rahmenbedingungen für den Informationsaustausch formal vereinbaren. Die Vereinbarung für den Informationsaustausch SOLLTE Angaben zum Schutz aller vertraulichen Informationen enthalten.

CON.9.A5 Beseitigung von Restinformationen vor Weitergabe (S) [Benutzende]

Zusätzlich zu den allgemeinen Schulungsmaßnahmen SOLLTE die Institution über die Gefahren von Rest- und Zusatzinformationen in Dokumenten und Dateien informieren. Es SOLLTE vermittelt werden, wie sie Rest- und Zusatzinformationen in Dokumenten und Dateien vermeiden werden können.

Die Institution SOLLTE Anleitungen bereitstellen, die vorgeben wie unerwünschte Restinformationen vom Austausch auszuschließen sind.

Jede Datei und jedes Dokument SOLLTE vor der Weitergabe auf unerwünschte Restinformationen überprüft werden. Unerwünschte Restinformationen SOLLTEN vor der Weitergabe aus Dokumenten und Dateien entfernt werden.

CON.9.A6 Kompatibilitätsprüfung des Sende- und Empfangssystems (S)

Vor einem Informationsaustausch SOLLTE überprüfen werden, ob die eingesetzten IT-Systeme und Produkte kompatibel sind.

CON.9.A7 Sicherungskopie der übermittelten Daten (S)

Die Institution SOLLTE eine Sicherungskopie der übermittelten Informationen anfertigen, falls die Informationen nicht aus anderen Quellen wiederhergestellt werden können.

CON.9.A8 Verschlüsselung und digitale Signatur (S)

Die Institution SOLLTE prüfen, ob Informationen während des Austausches kryptografisch gesichert werden können. Falls die Informationen kryptografisch gesichert werden, SOLLTEN dafür ausreichend sichere Verfahren eingesetzt werden.

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.9.A9 Vertraulichkeitsvereinbarungen (H) [Zentrale Verwaltung]

Bevor vertrauliche Informationen an andere Institutionen weitergeben werden, SOLLTE die zentrale Verwaltung informiert werden. Die zentrale Verwaltung SOLLTE eine Vertraulichkeitsvereinbarung mit der empfangenden Institution abschließen. Die Vertraulichkeitsvereinbarung SOLLTE regeln, wie die Informationen durch die empfangende Institution aufbewahrt werden dürfen. In der Vertraulichkeitsvereinbarung SOLLTE festgelegt werden, wer bei der empfangenden Institution Zugriff auf welche übermittelten Informationen haben darf.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) beschreibt in ihrem Standard *ISO/IEC 27001:2013*, Kap. 13.2 Anforderungen an den Austausch von Informationen.

Bundesamt
für Sicherheit in der
Informationstechnik

CON.10 Entwicklung von Webanwendungen

1. Beschreibung

1.1. Einleitung

Webanwendungen bieten bestimmte Funktionen und dynamische (sich verändernde) Inhalte. Dazu stellen Webanwendungen auf einem Server Dokumente und Bedienoberflächen, z. B. in Form von Eingabemasken, bereit und liefern diese auf Anfrage an entsprechende Programme auf den Clients aus, z. B. an Webbrowser. Webanwendungen werden gewöhnlich auf der Grundlage von Frameworks (Rahmenstrukturen) entwickelt. Frameworks sind wiederverwendbare Programmschablonen für häufig wiederkehrende Aufgaben. Auch für Sicherheitskomponenten gibt es Frameworks.

Webanwendungen müssen Sicherheitsmechanismen umsetzen, die den Schutz der verarbeiteten Informationen gewährleisten und deren Missbrauch verhindern. Typische Sicherheitskomponenten bzw. -mechanismen sind Authentisierung, Autorisierung, Eingabevalidierung, Ausgabekodierung, Session-Management, Fehlerbehandlung und Protokollierung.

Die Entwickelnden müssen mit den relevanten Sicherheitsmechanismen einer Webanwendung vertraut sein. Aus diesem Grund hat der Entwicklungsprozess einen entscheidenden Einfluss auf die Sicherheit der späteren Software.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, sichere Webanwendungen zu entwickeln sowie Informationen zu schützen, die durch eine Webanwendung verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein ist auf jedes Entwicklungsvorhaben im Informationsverbund anzuwenden, bei dem Webanwendungen entwickelt werden.

In diesem Baustein werden die spezifischen Gefährdungen und Anforderungen betrachtet, die bei der Entwicklung von Webanwendungen relevant sind. Anforderungen an den sicheren Einsatz von Webanwendungen werden nicht in diesem Baustein betrachtet. Sie sind im Baustein APP.3.1 *Webanwendungen und Webservices* zu finden. Ebenso werden allgemeine Anforderungen an die sichere

Entwicklung von Software an anderer Stelle behandelt. Sie werden im Baustein CON.8 *Software-Entwicklung* behandelt.

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.10 *Entwicklung von Webanwendungen* von besonderer Bedeutung.

2.1. Umgehung der Autorisierung bei Webanwendungen

Bei einem Angriff wird häufig versucht, auf Funktionen oder Daten von Webanwendungen zuzugreifen, die nur mit bestimmten Zugriffsrechten verfügbar sind. Ist die Autorisierung fehlerhaft umgesetzt, können unter Umständen die Berechtigungen eines anderen Kontos mit umfangreicheren Rechten erlangt werden und somit auf geschützte Bereiche und Daten zugegriffen werden. Dies geschieht beispielsweise, indem Eingaben gezielt manipuliert werden.

2.2. Unzureichende Eingabevalidierung und Ausgabekodierung

Verarbeitet eine Webanwendung ungeprüfte Eingabedaten, können möglicherweise Schutzmechanismen umgangen werden. Dieses Risiko erhöht sich, wenn gleichzeitig die Ausgabedaten der Webanwendung ohne ausreichende Kodierung direkt an den Webbrowser, die aufrufende Anwendung oder an nachgelagerte IT-Systeme übermittelt werden. Solche Ausgabedaten können Schadcode enthalten, der auf den Zielsystemen interpretiert oder ausgeführt wird. Beispielsweise kann bei einem Angriff Javascript Code in Formulardaten eingeben werden. Dieser Schadcode wird dann ungewollt vom IT-System ausgeführt, das die Webanwendung mit den Daten verarbeitet.

2.3. Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen

Wenn während des Betriebs einer Webanwendung Fehler auftreten, die nicht korrekt behandelt werden, können sowohl der Betrieb einer Webanwendung als auch der Schutz ihrer Funktionen und Daten beeinträchtigt werden. Beispielsweise kann ein Fehler dazu führen, dass die Webanwendung nicht mehr korrekt ausgeführt wird und für Clients nicht mehr erreichbar ist. Außerdem werden unter Umständen Aktionen nur noch unvollständig durchgeführt, zwischengespeicherte Aktionen und Daten gehen verloren oder Sicherheitsmechanismen fallen aus.

2.4. Unzureichende Protokollierung von sicherheitsrelevanten Ereignissen

Wenn sicherheitsrelevante Ereignisse von der Webanwendung unzureichend protokolliert werden, können Sicherheitsvorfälle zu einem späteren Zeitpunkt nur schwer nachvollzogen werden. Die Ursachen für einen Vorfall sind dann möglicherweise nicht mehr ermittelbar. Beispielsweise können Konfigurationsfehler übersehen werden, wenn sie nicht zu Fehlermeldungen in den Log-Dateien führen. Auch Schwachstellen sind bei unzureichender Protokollierung schwer oder gar nicht zu erkennen und zu beheben.

2.5. Offenlegung sicherheitsrelevanter Informationen durch Webanwendungen

Webseiten und Daten, die von einer Webanwendung generiert und ausgeliefert werden, können Informationen zu den Hintergrundsystemen enthalten, z. B. Angaben zu Datenbanken oder Versionsständen von Frameworks. Diese Informationen können es erleichtern, gezielte Angriffe auf die Webanwendung durchzuführen.

2.6. Missbrauch einer Webanwendung durch automatisierte Nutzung

Wenn Funktionen einer Webanwendung automatisiert benutzt werden, können zahlreiche Vorgänge in kurzer Zeit ausgeführt werden. Mithilfe eines wiederholt durchgeführten Login-Prozesses kann bei einem Angriff z. B. versucht werden, gültige Kombinationen von Konten und Passwörtern zu erraten (Brute-Force). Außerdem können Listen mit gültigen Konten erzeugt werden (Enumeration), falls die Webanwendung Informationen über vorhandene Konten zurückgibt. Darüber hinaus können wiederholte Aufrufe von ressourcenintensiven Funktionen wie z. B. komplexen Datenbankabfragen für Denial-of-Service-Angriffe auf Anwendungsebene missbraucht werden.

2.7. Unzureichendes Session-Management von Webanwendungen

Unzureichendes Session-Management kann es ohne spezielle Zugriffsrechte ermöglichen, die Session-ID von Konten mit umfangreichen Zugriffsrechten zu ermitteln. Anschließend kann bei einem Angriff mit dieser ID auf geschützte Funktionen und Ressourcen der Webanwendung zugegriffen werden, z. B. in Form eines Session-Fixation-Angriffs. Hier wird zunächst eine Session-ID mit eingeschränkten Rechten von der Webanwendung beschafft. Diese ID wird, z. B. über einen Link in einer E-Mail, an höher legitimierte Personen übermittelt. Falls die höher legitimierten Personen diesem Link folgen und sich gegenüber der Webanwendung unter der Session-ID authentisieren, können Angreifende die Anwendung anschließend mit den vollen Zugriffsrechten der legitimen Konten verwenden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.10 *Entwicklung von Webanwendungen* 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	Entwickelnde
Weitere Zuständigkeiten	Keine

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.10.A1 Authentisierung bei Webanwendungen (B)

Die Entwickelnden MÜSSEN sicherstellen, dass sich die Benutzenden gegenüber der Webanwendung sicher und angemessen authentisieren, bevor diese auf geschützte Funktionen oder Inhalte zugreifen können. Es MUSS eine angemessene Authentisierungsmethode ausgewählt werden. Der Auswahlprozess MUSS dokumentiert werden.

Eine zentrale Authentisierungskomponente MUSS verwendet werden. Die zentrale Authentisierungskomponente SOLLTE mit etablierten Standardkomponenten (z. B. aus Frameworks oder Programmbibliotheken) umgesetzt werden. Falls eine Webanwendung Authentisierungsdaten auf einem Client speichert, MUSS explizit auf die Risiken der Funktion hingewiesen werden und zustimmen („Opt-In“).

Die Webanwendung MUSS die Möglichkeit bieten, Grenzwerte für fehlgeschlagene Anmeldeversuche festzulegen. Die Webanwendung MUSS Benutzende sofort informieren, wenn deren Passwort zurückgesetzt wurde.

CON.10.A2 Zugriffskontrolle bei Webanwendungen (B)

Die Entwickelnden MÜSSEN mittels einer Autorisierungskomponente sicherstellen, dass die Benutzenden ausschließlich solche Aktionen durchführen können, zu denen sie berechtigt sind. Jeder Zugriff auf geschützte Inhalte und Funktionen MUSS kontrolliert werden, bevor er ausgeführt wird.

Die Autorisierungskomponente MUSS sämtliche Ressourcen und Inhalte berücksichtigen, die von der Webanwendung verwaltet werden. Ist die Zugriffskontrolle fehlerhaft, MÜSSEN Zugriffe abgelehnt werden. Es MUSS eine Zugriffskontrolle bei URL-Aufrufen und Objekt-Referenzen geben.

CON.10.A3 Sicheres Session-Management (B)

Session-IDs MÜSSEN geeignet geschützt werden. Session-IDs MÜSSEN zufällig und mit ausreichender Entropie erzeugt werden. Falls das Framework der Webanwendung sichere Session-IDs generieren kann, MUSS diese Funktion des Frameworks verwendet werden. Sicherheitsrelevante Konfigurationsmöglichkeiten des Frameworks MÜSSEN berücksichtigt werden. Wenn Session-IDs übertragen und von den Clients gespeichert werden, MÜSSEN sie ausreichend geschützt übertragen werden.

Eine Webanwendung MUSS die Möglichkeit bieten, eine bestehende Sitzung explizit zu beenden. Nachdem ein Konto angemeldet wurde, MUSS eine bereits bestehende Session-ID durch eine neue ersetzt werden. Sitzungen MÜSSEN eine maximale Gültigkeitsdauer besitzen (Timeout). Inaktive Sitzungen MÜSSEN automatisch nach einer bestimmten Zeit ungültig werden. Nachdem die Sitzung ungültig ist, MÜSSEN alle Sitzungsdaten ungültig und gelöscht sein.

CON.10.A4 Kontrolliertes Einbinden von Inhalten bei Webanwendungen (B)

Es MUSS sichergestellt werden, dass eine Webanwendung ausschließlich vorgesehene Daten und Inhalte einbindet ausliefert.

Die Ziele der Weiterleitungsfunktion einer Webanwendung MÜSSEN ausreichend eingeschränkt werden, sodass ausschließlich auf vertrauenswürdige Webseiten weitergeleitet wird. Falls die Vertrauensdomäne verlassen wird, MUSS ihn die Webanwendung darüber informieren.

CON.10.A5 Upload-Funktionen (B)

Die Entwickelnden MÜSSEN sicherstellen, dass die Benutzenden Dateien nur im vorgegebenen Pfad speichern können. Die Entwickelnden MÜSSEN sicherstellen, dass die Benutzenden den Ablageort der Uploads nicht beeinflussen kann. Die Entwickelnden MÜSSEN Funktionen in die Webanwendung integrieren, mit denen die Uploads während des Betriebs der Webanwendung konfiguriert werden können.

CON.10.A6 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen (B)

Die Entwickelnden MÜSSEN Sicherheitsmechanismen implementieren, die die Webanwendung vor automatisierten Zugriffen schützen. Bei der Implementierung der Sicherheitsmechanismen MUSS berücksichtigt werden, wie sich diese auf die Nutzungsmöglichkeiten der berechtigten Konten auswirken.

CON.10.A7 Schutz vertraulicher Daten (B)

Die Entwickelnden MÜSSEN sicherstellen, dass vertrauliche Daten von den Clients zu den Servern nur mit der HTTP-Post-Methode übertragen werden.

Entwickelnde MÜSSEN durch Direktiven in der Webanwendung gewährleisten, dass clientseitig keine schützenswerten Daten zwischengespeichert werden. Entwickelnde MÜSSEN sicherstellen, dass in Formularen keine vertraulichen Formulardaten im Klartext angezeigt werden. Die Webanwendung SOLLTE verhindern, dass vertrauliche Daten vom Webbrowser unerwartet gespeichert werden. Sämtliche Zugangsdaten der Webanwendung MÜSSEN serverseitig mithilfe von sicheren kryptografischen Algorithmen vor unbefugtem Zugriff geschützt werden (Salted Hash). Die Dateien mit den Quelltexten der Webanwendung MÜSSEN vor unerlaubten Abrufen geschützt werden.

CON.10.A8 Umfassende Eingabevalidierung und Ausgabekodierung (B)

Die Entwickelnden MÜSSEN sämtliche an eine Webanwendung übergebenen Daten als potenziell gefährlich behandeln und geeignet filtern. Sämtliche Eingabedaten sowie Datenströme und Sekundärdaten, wie z. B. Session-IDs, MÜSSEN serverseitig validiert werden.

Fehleingaben SOLLTEN möglichst nicht automatisch behandelt werden (Sanitizing). Lässt es sich jedoch nicht vermeiden, MUSS Sanitizing sicher umgesetzt werden.

Ausgabedaten MÜSSEN so kodiert werden, dass schadhafter Code auf dem Zielsystem nicht interpretiert oder ausgeführt wird.

CON.10.A9 Schutz vor SQL-Injection (B)

Falls Daten an ein Datenbankmanagementsystem (DBMS) weitergeleitet werden, MÜSSEN Stored Procedures bzw. Prepared SQL Statements eingesetzt werden. Falls Daten an ein DBMS weitergeleitet werden und weder Stored Procedures noch Prepared SQL Statements von der Einsatzumgebung unterstützt werden, MÜSSEN die SQL-Queries separat abgesichert werden.

CON.10.A10 Restriktive Herausgabe sicherheitsrelevanter Informationen (B)

Die Entwickelnden MÜSSEN sicherstellen, dass Webseiten, Rückantworten und Fehlermeldungen von Webanwendungen keine Informationen enthalten, die Angreifenden Hinweise darauf geben, wie er Sicherheitsmechanismen umgehen kann.

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.10.A11 Softwarearchitektur einer Webanwendung (S)

Die Entwickelnden SOLLTEN die Softwarearchitektur der Webanwendung mit allen Bestandteilen und Abhängigkeiten dokumentieren. Die Dokumentation SOLLTE bereits während des Entwicklungsverlaufs aktualisiert und angepasst werden. Die Dokumentation SOLLTE so gestaltet sein, dass sie schon in der Entwicklungsphase benutzt werden kann und Entscheidungen nachvollziehbar sind. In der Dokumentation SOLLTEN alle für den Betrieb notwendigen Komponenten gekennzeichnet werden, die nicht Bestandteil der Webanwendung sind. In der Dokumentation SOLLTE beschrieben sein, welche Komponenten welche Sicherheitsmechanismen umsetzen, wie die

Webanwendung in eine bestehende Infrastruktur integriert wird und welche kryptografischen Funktionen und Verfahren eingesetzt werden.

CON.10.A12 Verifikation essenzieller Änderungen (S)

Falls wichtige Einstellungen mit der Anwendung geändert werden sollen, dann SOLLTEN die Entwickelnden sicherstellen, dass die Änderungen durch die Eingabe eines Passworts erneut verifiziert werden. Falls dies nicht möglich ist, dann SOLLTE die Webanwendung auf andere geeignete Weise sicherstellen, dass sich die Benutzenden authentisieren. Die Benutzenden SOLLTEN über Änderungen mithilfe von Kommunikationswegen außerhalb der Webanwendung informiert werden.

CON.10.A13 Fehlerbehandlung (S)

Treten während der Laufzeit einer Webanwendung Fehler auf, SOLLTEN diese so behandelt werden, dass die Webanwendung weiter in einem konsistenten Zustand bleibt.

Die Webanwendung SOLLTE Fehlermeldungen protokollieren. Falls eine veranlasste Aktion einen Fehler verursacht, SOLLTE die Webanwendung diese Aktion abbrechen. Die Webanwendung SOLLTE im Fehlerfall den Zugriff auf eine angeforderte Ressource oder Funktion verweigern.

Zuvor reservierte Ressourcen SOLLTEN im Rahmen der Fehlerbehandlung wieder freigegeben werden. Der Fehler SOLLTE möglichst von der Webanwendung selbst behandelt werden.

CON.10.A14 Sichere HTTP-Konfiguration bei Webanwendungen (S)

Zum Schutz vor Clickjacking, Cross-Site-Scripting und anderen Angriffen SOLLTEN geeignete HTTP-Response-Header gesetzt werden. Es SOLLTEN mindestens die folgenden HTTP-Header verwendet werden: Content-Security-Policy, Strict-Transport-Security, Content-Type, X-Content-Type-Options sowie Cache-Control. Die verwendeten HTTP-Header SOLLTEN auf die Webanwendung abgestimmt werden. Die verwendeten HTTP-Header SOLLTEN so restriktiv wie möglich sein.

Cookies SOLLTEN grundsätzlich mit den Attributen *secure*, *SameSite* und *httponly* gesetzt werden.

CON.10.A15 Verhinderung von Cross-Site-Request-Forgery (S)

Die Entwickelnden SOLLTEN die Webanwendung mit solchen Sicherheitsmechanismen ausstatten, die eine Unterscheidung zwischen beabsichtigten Seitenaufrufen und unbeabsichtigt weitergeleiteten Befehlen Dritter ermöglichen. Dabei SOLLTE mindestens geprüft werden, ob neben der Session-ID ein geheimes Token für den Zugriff auf geschützte Ressourcen und Funktionen benötigt wird.

CON.10.A16 Mehr-Faktor-Authentisierung (S)

Es SOLLTE eine Mehr-Faktor-Authentisierung implementiert werden.

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.10.A17 Verhinderung der Blockade von Ressourcen (H)

Zum Schutz vor Denial-of-Service (DoS)-Angriffen SOLLTEN ressourcenintensive Operationen vermieden werden. Falls ressourcenintensive Operationen notwendig sind, dann SOLLTEN diese besonders abgesichert werden. Bei Webanwendungen SOLLTE ein möglicher Überlauf von Protokollierungsdaten überwacht und verhindert werden.

CON.10.A18 Kryptografische Absicherung vertraulicher Daten (H)

Vertrauliche Daten einer Webanwendung SOLLTEN durch sichere, kryptografische Algorithmen abgesichert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Open Web Application Security Projekt stellt auf seiner Webseite Hinweise zur Absicherung von Webanwendungen zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Kryptographische Verfahren: Empfehlungen und Schlüssellängen: BSI TR-02102“ Hinweise zur Anwendung kryptografischer Verfahren zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Entwicklung sicherer Webanwendungen“ Hinweise zur Entwicklung sicherer Webanwendungen zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Leitfaden zur Entwicklung sicherer Webanwendungen“ Hinweise zur Entwicklung sicherer Webanwendungen durch Unternehmen zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

1. Beschreibung

1.1. Einleitung

Der staatliche Geheimschutz umfasst alle Maßnahmen zur Geheimhaltung von Informationen, die durch eine staatliche Stelle oder auf deren Veranlassung als Verschlusssachen (VS) eingestuft worden sind. VS sind im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes, geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform.

Der staatliche Geheimschutz wird durch Vorschriften des Bundes- und des Landesrechts geregelt. Rechtliche Grundlage für den staatlichen Geheimschutz des Bundes ist das Sicherheitsüberprüfungsgesetz (SÜG). Für den materiellen Geheimschutz des Bundes ist die Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung, VSA) maßgeblich. Diese richtet sich an Bundesbehörden oder bundesunmittelbare öffentlich-rechtliche Einrichtungen (Dienststellen), die mit VS arbeiten.

Wird Informationstechnik zur Handhabung von VS (VS-IT) eingesetzt, dann sind die Anforderungen der VSA zu beachten. Voraussetzung für den Einsatz von VS-IT ist ein Informationssicherheitskonzept nach den BSI-Standards des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung. Hinzu kommen die in diesem Baustein beschriebenen Anforderungen des Geheimschutzes, die über den IT-Grundschutz hinausgehen.

Unter Zusammenschaltung von VS-IT wird die direkte oder kaskadierte Verbindung von zwei oder mehr VS-IT-Systemen für die gemeinsame Nutzung von Daten und anderen Informationsressourcen (beispielsweise Kommunikation) bezeichnet.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, dass die Anforderungen des Geheimschutzes frühzeitig in den Informationssicherheitskonzepten berücksichtigt werden (Security-by-Design). Dieser Baustein soll die Geheimschutzbeauftragten dabei unterstützen, die Anforderungen der VSA für die elektronische Verarbeitung von VS bis zum Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

festzulegen und gemeinsam mit den Informationssicherheitsbeauftragten in das Informationssicherheitskonzept zu integrieren.

1.3. Abgrenzung und Modellierung

Der Baustein CON.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* ist einmal auf den gesamten Informationsverbund der VS-IT anzuwenden, falls VS des Geheimhaltungsgrades VS-NfD verarbeitet werden oder werden sollen. Dieser Baustein richtet sich an Bundesbehörden oder bundesunmittelbare öffentlich-rechtliche Einrichtungen, die der VSA unterliegen.

Falls der Baustein angewendet werden soll, dann ist zu beachten, dass dieser Baustein kein eigenständiges Regelwerk darstellt, sondern lediglich unterstützen soll, die VSA umzusetzen. Grundsätzlich ist zwischen Anforderungen zur Gewährleistung der Informationssicherheit und des Geheimschutzes zu unterscheiden. Der IT-Grundschutz dient der Umsetzung der Informationssicherheit und die VSA der Umsetzung des Geheimschutzes. Aus diesem Grund ersetzt eine ISO27001-Zertifizierung auf Basis von IT-Grundschutz nicht die Freigaben nach VSA. Um einen durchgehenden Geheimschutz umzusetzen, müssen die Anforderungen der VSA beachtet werden.

Die Anforderungen dieses Bausteins sind aus der VSA abgeleitet und behandeln folgende Aspekte:

- allgemeine Grundsätze der VSA,
- Zugang von Personen zu VS,
- VS-IT-Dokumentation,
- Handhabung elektronischer VS,
- Einsatz von VS-IT sowie
- Wartung und Instandhaltung von VS-IT.

Dabei bauen die Anforderungen dieses Bausteins auf den Anforderungen der Informationssicherheit auf und erweitern diese um die Anforderungen des Geheimschutzes. Um den betrachteten Informationsverbund mit VS-IT abzusichern und zu gewährleisten, dass die Informationssicherheit umgesetzt ist, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. Neben den relevanten System-Bausteinen wird unter anderem die Umsetzung der folgenden Prozess-Bausteine durch diesen Baustein vorausgesetzt, da diese um die Anforderungen des Geheimschutzes erweitert werden:

- ORP.1 *Organisation*,
- ORP.2 *Personal*,
- CON.6 *Löschen und Vernichten* sowie
- OPS.1.2.5 *Fernwartung*.

Dieser Baustein behandelt nicht:

- die Anforderungen der VSA, um VS-IT abzusichern, die für die Verarbeitung von VS der Geheimhaltungsgrade VS-VERTRAULICH oder höher eingesetzt werden sollen,
- die bauliche und technische Absicherung von Gebäuden und Räumen, in denen VS des Geheimhaltungsgrades VS-NfD verarbeitet werden, diese werden in den entsprechenden Bausteinen der Schicht INF *Infrastruktur* behandelt,
- die allgemeinen Anforderungen der VSA, die keinen unmittelbaren Bezug zu VS-IT haben sowie
- den Freigabeprozess für VS-IT.

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.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* von besonderer Bedeutung.

2.1. Unbefugte Kenntnisnahme

Eine wesentliche Gefährdung des Geheimschutzes stellt die Kenntnisnahme von VS durch unbefugte Personen dar. Diese kann sich ergeben, wenn die Vorgaben der VSA nicht beachtet werden.

Beispiele:

- Die Einstufung und Kennzeichnung von VS unterbleibt, erfolgt falsch oder unvollständig.
- VS werden durch IT-Produkte gelöscht, die keine Zulassungsaussage besitzen.
- Die VS-IT-Dokumentation fehlt oder wird nur mangelhaft gepflegt.

Werden die Vorgaben der VSA nicht beachtet, kann dies dazu führen, dass

- bei einer fehlerhaften Handhabung von VS einige Geheimschutzmaßnahmen fälschlicherweise als nicht notwendig erachtet werden, wodurch diese nicht oder nicht im notwendigen Maße umgesetzt werden,
- VS so gelöscht werden, dass der Inhalt der VS wiederherstellbar ist,
- aufgrund einer fehlenden oder mangelhaften VS-IT-Dokumentation nicht nachvollzogen werden kann, ob ein erforderliches Geheimschutzniveau erreicht wird, in der Vergangenheit schon notwendige Maßnahmen zum Schutz der VS-IT getroffen wurden oder aktuell geplante Maßnahmen zu bereits umgesetzten Maßnahmen passen,
- VS mit einer IT verarbeitet werden, die keine ausreichenden Schutzmaßnahmen bietet.

Durch Anwendungen können Daten unbemerkt gespeichert oder vervielfältigt werden.

Beispiele:

- In Auslagerungsdateien oder Auslagerungspartitionen befinden sich mitunter schützenswerte Daten, z. B. Passwörter oder kryptografische Schlüssel.
- Bei der Verarbeitung von VS mit einem Textverarbeitungsprogramm können temporäre Arbeitskopien erzeugt werden, die unter bestimmten Umständen, beispielsweise nach einem Absturz des Programms, nicht gelöscht wurden.
- Auch fallen im laufenden Betrieb vieler Anwendungen Dateien an, die nicht für den produktiven Betrieb benötigt werden (z. B. Browserhistorie). Diese Dateien können sicherheitsrelevante Informationen enthalten.

Als Folge können solche Dateien ausgelesen werden, wenn die Datenträger ausgebaut und in ein anderes IT-System eingebaut werden. Wurden die Auslagerungs- oder Anwendungsdateien oder temporäre Dateien nicht sicher gelöscht, können Unbefugte Kenntnis von VS erlangen. Passwörter und Schlüssel können missbraucht werden, um unberechtigt auf VS-IT oder VS zuzugreifen.

Die Auswirkungen einer unbefugten Kenntnisnahme von VS des Geheimhaltungsgrad VS-NfD können für die Bundesrepublik Deutschland oder eines ihrer Länder von Nachteil sein. Diese können je nach Art der als VS eingestuften Informationen unterschiedlich ausfallen. Wenn beispielsweise eingestufte Netzpläne oder Informationssicherheitskonzepte offengelegt werden, dann können diese Informationen genutzt werden, um in IT-Systeme einzudringen. Erhalten Unbefugte beispielsweise Kenntnis von diplomatischen Informationen über ein anderes Land, dann kann dies die diplomatischen Beziehungen zwischen Deutschland und diesem Land belasten.

2.2. Konspirative Angriffe

Als konspirativer Angriff wird eine Form der Spionage bezeichnet, bei der Informationen verdeckt von nicht öffentlich zugänglichen Informationen durch ausländische Nachrichtendienste gewonnen werden. Bei konspirativen Angriffen möchten Nachrichtendienste möglichst unbemerkt an für sie interessante Informationen, wie z. B. VS, gelangen.

Bei konspirativen Beschaffungsaktivitäten verschleiern die Nachrichtendienste ihre wahren Absichten. Die Informationen werden über den Einsatz menschlicher Quellen (z. B. Social Engineering), durch technische Mittel (z. B. Abhörmaßnahmen oder Cyber-Angriffe, bei denen Hintertüren ausgenutzt oder Schadsoftware eingesetzt wird) oder durch eine Kombination beider Möglichkeiten beschafft.

In der Folge können ausländische Nachrichtendienste auf VS zugreifen und sich einen strategischen Vorteil gegenüber der Bundesrepublik Deutschland oder eines ihrer Länder verschaffen. Beispielsweise könnten andere Staaten diese Informationen nutzen, um ihre Verhandlungsposition gegenüber der Bundesrepublik Deutschland zu stärken. Auch andere Gruppierungen, wie beispielsweise terroristische Organisationen oder die organisierte Kriminalität, können mit den aus konspirativen Angriffen erlangten Informationen mögliche Aktivitäten effektiver planen und durchführen.

2.3. Angriffe durch Innentäter und -täterinnen

Bei einem Angriff durch sogenannte Innentäter und -täterinnen werden interne Informationen, wie z. B. VS, durch interne oder externe Mitarbeitende bewusst entwendet und gegebenenfalls an Dritte verkauft oder veröffentlicht. Innentäter und -täterinnen verfügen über ein breites Wissen über interne Prozesse und Arbeitsabläufe ihrer Institutionen. Darüber hinaus verfügen sie über Zutritts-, Zugangs- und Zugriffsrechte, über die Außenstehende nicht verfügen. Dieses Wissen und die ihnen für ihre dienstlichen Aufgaben erteilten Rechte können sie einsetzen, um die Erfolgswahrscheinlichkeit eines Angriffs zu erhöhen. Weiterhin können sie den Zeitpunkt des Angriffs so steuern, dass dieser durchgeführt wird, wenn dieser nur schwer erkannt werden kann, beispielsweise in Wartungsfenstern.

Die Ursachen, warum sich Mitarbeitende dazu entschließen Informationen zu entwenden, sind individuell unterschiedlich.

Beispiele:

- Die Innentäter und -täterinnen fühlen sich moralisch dazu verpflichtet, Informationen, die als VS eingestuft sind, zu veröffentlichen, um damit beispielsweise Missstände aufzudecken.
- Die Innentäter und -täterinnen wurden von einem Nachrichtendienst angeworben.
- Die Innentäter und -täterinnen möchten sich mit dem Verkauf von Informationen bereichern.

In der Folge können Dritte unberechtigt Zugang zu VS erlangen. Dies kann für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein. Die Voraussetzungen, unter denen Innentäter und -täterinnen agieren, erschweren den Schutz vor einem solchen Angriff. Viele der zum Schutz vor Angriffen eingesetzten Maßnahmen sind gegen den Angriff durch Innentäter und -täterinnen nicht wirksam.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* aufgeführt. Die Gesamtverantwortung für den Geheimschutz trägt die jeweilige Dienststellenleitung. Die damit verbundenen Aufgaben nimmt, sofern bestellt, der oder die jeweilige Geheimschutzbeauftragte war. Dieser oder diese ist für die Umsetzung der VSA zuständig. Wurde kein oder keine Geheimschutzbeauftragte bestellt, nimmt die Dienststellenleitung diese Aufgaben wahr. Der oder die Informationssicherheitsbeauftragte (diese Rolle entspricht der in der VSA und im UP Bund definierten Rolle der IT-Sicherheitsbeauftragten) unterstützt und berät den oder die Geheimschutzbeauftragte in allen Fragen zum Einsatz von VS-IT.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Geheimschutzbeauftragte
Weitere Zuständigkeiten	Keine

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.
Hinweis: Bei der Anwendung dieses Bausteins sind folgende Regelungen zu beachten:

- Dieser Baustein hat **keinerlei** Regelungscharakter. Es handelt sich **nicht** um ein eigenständiges Regelwerk, sondern die Anforderungen ergeben sich aus der VSA.
- Allgemeine Regelungen der VSA, die keine spezifischen Vorgaben zu VS-IT enthalten, sind **nicht** Bestandteil dieses Bausteins. Diese Regelungen sind der VSA zu entnehmen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.11.1.A1 Einhaltung der Grundsätze zur VS-Verarbeitung mit IT nach § 3, 4 und 6 und Nr. 1 Anlage V zur VSA (B)

VS des Geheimhaltungsgrades VS-NfD DÜRFEN NUR mit VS-IT verarbeitet, die hierfür freigegeben ist. Private IT DARF NICHT für die Verarbeitung von Verschlusssachen eingesetzt werden. Bei der Verarbeitung von VS mit VS-IT MUSS der Grundsatz "Kenntnis nur, wenn nötig" eingehalten werden. Es DÜRFEN NUR Personen Kenntnis von einer VS erhalten, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis erhalten müssen. Personen DÜRFEN NICHT umfassender oder eher über eine VS unterrichtet werden, als dies aus Gründen der Aufgabenerfüllung notwendig ist.

Die Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig“ SOLLTE, insbesondere falls die VS-IT durch mehrere Benutzende verwendet wird, primär über technische Maßnahmen sichergestellt werden.

Nach dem Grundsatz der mehrschichtigen Sicherheit MÜSSEN personelle, organisatorische, materielle und technische Maßnahmen getroffen werden, die in ihrem Zusammenwirken

- Risiken eines Angriffs reduzieren (Prävention),
- Angriffe erkennbar machen (Detektion) und
- im Falle eines erfolgreichen Angriffs die negativen Folgen begrenzen (Reaktion).

Bei der Erfüllung der Anforderungen des vorliegenden Bausteins MÜSSEN die relevanten Technischen Leitlinien des BSI (BSI TL) beachtet werden. Falls von den BSI TL abgewichen werden soll, dann DARF dies NUR in Ausnahmefällen und im Einvernehmen mit dem BSI erfolgen.

CON.11.1.A2 Erstellung und Fortschreibung der VS-IT-Dokumentation nach § 12 und Nr. 2.2 Anlage II zur VSA (B)

Jede Dienststelle, die VS-IT einsetzt, MUSS als Teil der Geheimschutzdokumentation eine VS-IT-Dokumentation erstellen. Die VS-IT-Dokumentation MUSS alle Dokumente beinhalten, welche in Nr. 2.2 Anlage II zur VSA aufgeführt sind.

Die VS-IT-Dokumentation MUSS bei allen geheimschutzrelevanten Änderungen aktualisiert werden. Sie MUSS zudem mindestens alle drei Jahre auf Aktualität, Vollständigkeit und Erforderlichkeit bestehender und noch zu treffender Geheimschutzmaßnahmen überprüft werden.

CON.11.1.A3 Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA (B)

Auf Basis der im VS-Produktkatalog für einzelne Produkttypen vom BSI festgelegten Zulassungsrelevanz und insbesondere basierend auf den Ergebnissen der Strukturanalyse MÜSSEN alle für die geplante VS-IT relevanten IT-Sicherheitsfunktionen identifiziert werden. Diese lassen sich den folgenden Kategorien gemäß § 52 VSA zuordnen:

- Zugangs- und Zugriffskontrolle,
- Identifikation und Authentisierung,
- kryptographische Unterstützung,
- Sicherheitsmanagement,
- Informationsflusskontrolle,
- interner Schutz der Benutzerdaten,
- Selbstschutz der Sicherheitsfunktionen und ihrer Daten,
- Netztrennung,
- Schutz der Unversehrtheit,
- Verfügbarkeitsüberwachung oder
- Sicherheitsprotokollierung und Nachweisführung.

Anschließend MÜSSEN die identifizierten IT-Sicherheitsfunktionen den jeweiligen Teilkomponenten der VS-IT unter Berücksichtigung des VS-Produktkataloges des BSI zugeordnet werden. Jede identifizierte und für den Schutz von VS wesentlich verantwortliche Teilkomponente MUSS als IT-Sicherheitsprodukt gemäß VSA festgelegt und behandelt werden

Sofern das identifizierte IT-Sicherheitsprodukt einem Produkttyp angehört für das eine Zulassungsaussage gemäß BSI TL - IT 01 erforderlich ist, MUSS ein entsprechendes Produkt gemäß BSI Schrift 7164 (Liste der zugelassenen Produkte) verwendet werden. Sofern dort keine IT-Sicherheitsprodukte gelistet sind, MUSS Kontakt mit der Zulassungsstelle des BSI aufgenommen werden. Bei der Verwendung von IT-Sicherheitsprodukten mit Zulassungsaussage MÜSSEN zusätzlich die Bestimmungen des BSI für den Einsatz und Betrieb (SecOPs) des jeweiligen Produktes eingehalten werden.

CON.11.1.A4 Beschaffung von VS-IT nach § 49 VSA (B)

Bevor VS-IT beschafft wird, MUSS sichergestellt werden, dass deren Sicherheit während des gesamten Lebenszyklus ab dem Zeitpunkt, zu dem fest steht, dass die IT zur VS-Verarbeitung eingesetzt werden soll, bis zur Aussonderung kontinuierlich gewährleistet wird. Um einen durchgehenden Geheimschutz sicherzustellen, MÜSSEN die Vergabeunterlagen so formuliert werden, dass die Anforderungen der VSA vollständig erfüllt werden können.

Bei Beschaffungsaufträgen für VS-IT MÜSSEN die notwendigen IT-Sicherheitsfunktionen der jeweiligen IT-Produkte vorab festgelegt werden. Bei der Formulierung der Vergabeunterlagen MÜSSEN insbesondere die

- Aufbewahrung,
- Archivierung und
- Löschung von elektronischer VS sowie
- Aussonderung,
- Wartung und Instandsetzung von VS-IT

berücksichtigt werden. Sofern einem zu beschaffenden IT-Produkt eine IT-Sicherheitsfunktion zugeordnet ist, SOLLTE ein IT-Produkt aus der Liste der zugelassenen IT-Sicherheitsprodukte beschafft

werden. Wird stattdessen ein Produkt ohne Zulassungsaussage ausgewählt, dann SOLLTE im Vorhinein mit dem BSI abgeklärt werden, ob es zugelassen werden kann. Zusätzlich SOLLTE in der Ausschreibung aufgenommen werden, dass der Hersteller an einem Zulassungsverfahren mitwirken muss (siehe BSI TL - IT 01). Verträge MÜSSEN derart gestaltet werden, dass bei einer Rückgabe von defekten oder geleasten IT-Produkten deren Datenträger oder sonstige Komponenten, auf denen VS gespeichert sein könnten, im Besitz der Dienststelle verbleiben.

CON.11.1.A5 Verpflichtung bei Zugang zu VS nach § 4 VSA und Anlage V zur VSA (B)

Bevor eine Person Zugang zu VS des Geheimhaltungsgrades VS-NfD erhält, MUSS sie auf Anlage V verpflichtet werden. Ein Exemplar der Anlage V zur VSA MUSS jeder Person gegen Empfangsbestätigung zugänglich gemacht werden.

Wird Personal von nichtöffentlichen Stellen Zugang zu VS gewährt, so MUSS Nr. 6.6 Anlage V zur VSA beachtet werden. Von der Verpflichtung einer Person DARF NUR abgesehen werden, falls an VS-IT nur kurzzeitig gearbeitet und währenddessen ein Zugriff auf VS ausgeschlossen werden kann.

CON.11.1.A6 Beaufsichtigung und Begleitung von Fremdpersonal für VS-IT nach §§ 3, 4 VSA (B)

Nicht verpflichtetes Fremdpersonal, das an VS-IT arbeitet, MUSS während der gesamten Zeit begleitet und beaufsichtigt werden. Die begleitenden Personen MÜSSEN über die notwendigen Fachkenntnisse verfügen, um die Tätigkeiten kontrollieren zu können.

CON.11.1.A7 Kennzeichnung von elektronischen VS und Datenträgern nach §§ 20, 54 und Anlage III, V und VIII zur VSA (B)

Elektronische VS MÜSSEN nach den Vorgaben der VSA gekennzeichnet werden. Die Kennzeichnung MUSS bei der Verarbeitung von VS mit VS-IT während der gesamten Dauer ihrer Einstufung jederzeit erkennbar sein. Die Kennzeichnung MUSS auch bei kopierten, elektronisch versendeten oder ausgedruckten VS erhalten bleiben. Falls die Beschaffenheit elektronischer VS eine Kennzeichnung nach VSA nicht zulässt, dann MÜSSEN VS sinngemäß gekennzeichnet werden.

Der Dateiname einer elektronischen VS SOLLTE eine Kennzeichnung enthalten, die den VS-Charakter des Inhalts erkennen lässt, ohne die VS öffnen zu müssen. E-Mails MÜSSEN entsprechend des Musters 11 der Anlage VIII zur VSA gekennzeichnet werden.

Falls eine elektronische Kennzeichnung von VS (im Sinne von Metadaten) verwendet werden soll, dann MUSS geprüft werden, ob diese IT-Sicherheitsfunktionen übernimmt (siehe CON.11.1.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA)*.

Datenträger, auf denen elektronische VS des Geheimhaltungsgrades VS-NfD durch Produkte ohne Zulassungsaussage verschlüsselt gespeichert sind, MÜSSEN mit dem Geheimhaltungsgrad der darauf gespeicherten VS gekennzeichnet werden. Falls sich durch die Zusammenstellung der VS auf dem Datenträger ein Datenbestand ergibt, welcher eine höhere Einstufung erforderlich macht, dann MUSS der Datenträger selbst als VS des Geheimhaltungsgrades VS-VERTRAULICH behandelt und gekennzeichnet werden.

CON.11.1.A8 Verwaltung und Nachweis von elektronischen VS nach § 21 VSA (B)

Für die Verwaltung von elektronischen VS MÜSSEN die Grundsätze ordnungsgemäßer Aktenführung (gemäß Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien) und die Vorgaben der VSA zur Verwaltung und Nachweisführung von VS eingehalten werden (keine Nachweisführung für VS des Geheimhaltungsgrades VS-NfD erforderlich). Elektronische VS, die als VS-NfD eingestuft sind, DÜRFEN NUR unter Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig“ in offenen (elektronischen) Registraturen verwaltet werden.

CON.11.1.A9 Speicherung elektronischer VS nach § 23 und Nr. 5 Anlage V zur VSA (B)

Elektronische VS MÜSSEN mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt gespeichert oder entsprechend den Vorgaben der VSA materiell gesichert werden (siehe CON.11.1.A15 *Handhabung von Datenträgern und IT-Produkten nach § 54 und Anlage V zur VSA*).

CON.11.1.A10 Elektronische Übertragung von VS nach §§ 24, 53, 55 und Nr. 6.2 Anlage V zur VSA (B)

Falls VS elektronisch übertragen werden sollen, MÜSSEN die Regelungen der VSA zur Weitergabe von VS (§ 24 VSA) eingehalten werden. Für die Weitergabe an Parlamente, Landesbehörden und nicht öffentliche Stellen MÜSSEN zusätzlich die besonderen Regelungen nach §§ 25 und 26 VSA beachtet werden.

Die VS-IT aller Kommunikationspartner MUSS für die Verarbeitung von VS des Geheimhaltungsgrads VS-NfD freigegeben sein. Werden VS elektronisch übertragen, MÜSSEN sie grundsätzlich durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt werden. Auf eine Verschlüsselung DARF NUR verzichtet werden, falls:

- VS ausschließlich leitungsgebunden übertragen werden und die Übertragungseinrichtungen, einschließlich Kabel und Verteiler, gegen unbefugten Zugriff geschützt sind, oder
- neben den Hausnetzen zusätzlich das Transportnetz für die Verarbeitung von VS freigegeben ist.

Es DARF NUR innerhalb von Räumen und Bereichen, die gegen unkontrollierten Zutritt geschützt sind, von einem Zugriffsschutz ausgegangen werden.

VS DÜRFEN NUR in Ausnahmefällen nach § 55 Abs. 2-4 VSA unter Einhaltung der dort genannten Anforderungen und Vorsichtsmaßnahmen auf anderem Wege elektronisch übertragen werden. Falls im Vorhinein zu erwarten ist, dass VS elektronisch übertragen werden könnten, DARF die Ausnahmeregelung nach § 55 VSA NICHT angewendet werden.

CON.11.1.A11 Mitnahme elektronischer VS nach § 28 VSA und Nr. 7 Anlage V zur VSA (B)

Elektronische VS DÜRFEN NUR auf Dienstreisen und zu Dienstbesprechungen mitgenommen werden, soweit dies dienstlich notwendig ist und sie angemessen gegen unbefugte Kenntnisnahme gesichert werden. Werden diese persönlich mitgenommen, MÜSSEN diese folgendermaßen gespeichert werden:

- auf hierfür freigegebener VS-IT,
- auf einem Datenträger, der in einem verschlossenen Umschlag transportiert wird,
- auf einem Datenträger, der mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurde, oder
- durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt, falls der Datenträger selbst nicht durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurde.

Falls VS des Geheimhaltungsgrades VS-NfD in Privatwohnungen verarbeitet werden sollen, dann DÜRFEN diese NUR elektronisch mit hierfür freigegebener VS-IT verarbeitet werden.

CON.11.1.A12 Archivierung elektronischer VS nach §§ 30, 31 VSA (B)

VS MÜSSEN entsprechend dem Bundesarchivgesetz wie nicht eingestufte Informationen ausgesondert werden. Schon bei Einführung von Systemen zur elektronischen Schriftgutverwaltung und Vorgangsbearbeitung MÜSSEN die technischen Verfahren zur Aussonderung frühzeitig mit dem zuständigen Archiv abgesprochen werden. Falls das zuständige Archiv VS nicht übernehmen möchte, MÜSSEN VS gemäß CON.11.1.A13 *Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 VSA* sicher gelöscht bzw. vernichtet werden.

CON.11.1.A13 Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 und Nr. 8 Anlage V zur VSA (B)

Um VS oder Datenträger zu löschen, die mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurden, MUSS der Schlüssel unter Beachtung der SecOPs gelöscht werden.

Sollen elektronische VS gelöscht werden, die nicht durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurden, dann MUSS der gesamte Datenträger oder das IT-Produkt, auf dem VS gespeichert sind, mittels eines IT-Sicherheitsprodukts mit Zulassungsaussage gelöscht werden.

Die Datenträger oder IT-Produkte MÜSSEN gelöscht werden, bevor sie die gesicherte Einsatzumgebung dauerhaft verlassen. Sie MÜSSEN physisch vernichtet werden, falls sie nicht gelöscht werden können. Für die Vernichtung MÜSSEN Produkte oder Verfahren eingesetzt oder Dienstleister beauftragt werden, die die Anforderungen der BSI TL - M 50 erfüllen.

Die zuvor beschriebenen Teilanforderungen MÜSSEN auch bei defekten Datenträgern und IT-Produkten eingehalten werden.

CON.11.1.A14 Zugangs- und Zugriffsschutz nach § 3 VSA (B)

VS-IT, die für VS-NfD eingestufte VS eingesetzt wird, MUSS so geschützt werden, dass ein Zugang zur VS-IT und ein Zugriff auf VS nur für verpflichtete Personen (siehe CON.11.1.A5 *Verpflichtung bei Zugang zu VS nach § 4 und Anlage V zur VSA*) möglich ist. Der Schutz der VS MUSS sichergestellt werden über:

- IT-Sicherheitsprodukte mit Zulassungsaussage,
- materielle,
- organisatorische oder
- personelle Maßnahmen.

Für den Zugangs- und Zugriffsschutz SOLLTE eine Mehr-Faktor-Authentisierung genutzt werden.

CON.11.1.A15 Handhabung von Datenträgern und IT-Produkten nach § 54 und Anlage V zur VSA (B)

Datenträger und IT-Produkte MÜSSEN bei Nichtgebrauch in verschlossenen Behältern oder Räumen aufbewahrt werden, falls:

- der Datenträger bzw. das IT-Produkt selbst als VS-NfD eingestuft ist,
- auf dem Datenträger bzw. IT-Produkt unverschlüsselte VS des Geheimhaltungsgrades VS-NfD gespeichert sind oder
- auf dem Datenträger bzw. IT-Produkt VS des Geheimhaltungsgrades VS-NfD durch ein Produkt ohne Zulassungsaussage verschlüsselt gespeichert sind.

CON.11.1.A16 Zusammenschaltung von VS-IT nach § 58 VSA (B)

Bevor VS-IT mit anderer VS-IT zusammengeschaltet werden darf, MUSS geprüft werden, ob und inwieweit Informationen zwischen der zusammengeschalteten VS-IT ausgetauscht werden dürfen. Bei der Prüfung MUSS das jeweilige Schutzniveau und der Grundsatz „Kenntnis nur, wenn nötig“ berücksichtigt werden.

Abhängig vom Ergebnis der Prüfung MÜSSEN IT-Sicherheitsfunktionen zum Schutz der Systemübergänge implementiert werden (siehe CON.11.1.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA*). Vor der Zusammenschaltung der VS-IT MUSS bewertet und dokumentiert werden, ob diese für das angestrebte Szenario zwingend erforderlich ist und ob durch die Zusammenschaltung eine besondere Gefährdung der einzelnen Teilsysteme entsteht. Es MUSS geprüft werden, ob der durch

die Zusammenschaltung von VS-IT entstandene Gesamtbestand der Daten höher einzustufen ist und weitere Geheimschutzmaßnahmen notwendig werden.

Wird VS-IT für die Verarbeitung von VS des Geheimhaltungsgrads VS-NfD direkt oder kaskadiert mit VS-IT für die Verarbeitung von VS des Geheimhaltungsgrades STRENG GEHEIM gekoppelt, dann MUSS sichergestellt werden, dass keine Verbindungen zu ungeschützten oder öffentlichen Netzen hergestellt werden.

CON.11.1.A17 Wartungs- und Instandsetzungsarbeiten von VS-IT nach § 3 Abs. 3 VSA (B)

Wartungs- und Instandsetzungsarbeiten an Komponenten der VS-IT SOLLTEN innerhalb der eigenen Dienstliegenschaft durchgeführt werden. Ist dies nicht möglich, MUSS sichergestellt werden, dass die Anforderungen der VSA sowohl während des Transports als auch bei den Wartungs- und Instandsetzungsarbeiten erfüllt werden.

Während der Wartungs- und Instandsetzungsarbeiten SOLLTE die Verarbeitung von VS in dem von der Wartung betroffenen Bereich der VS-IT eingestellt werden. Ist dies nicht möglich, MUSS während des Zeitraums der Wartungs- und Instandsetzungsarbeiten lückenlos sichergestellt werden, dass keine VS abfließen können.

Nach Abschluss der Wartungs- und Instandsetzungsarbeiten MUSS der oder die Geheimschutzbeauftragte bewerten, ob sich geheimschutzrelevante Änderungen an der VS-IT ergeben haben.

CON.11.1.A18 Fernwartung von VS-IT nach § 3 Abs. 3 VSA (B)

Wird VS-IT ferngewartet, dann MUSS die Fernwartungsverbindung verschlüsselt sein. Für die Verschlüsselung MÜSSEN IT-Sicherheitsprodukte mit Zulassungsaussage eingesetzt werden.

Die IT, mit der die Fernwartung durchgeführt wird, sowie die Übertragungsstrecken MÜSSEN als VS-IT behandelt und als Schutzobjekte definiert werden.

Die Fernwartungsverbindung MUSS durch die Dienststelle auf- und abgebaut werden. Die Dienststelle MUSS in der Lage sein, die Verbindung bei Auffälligkeiten auch während der Wartung zu unterbrechen.

Für die Fernwartung von VS-IT MUSS ein Informationssicherheitskonzept erstellt werden, das alle Komponenten, die an der Fernwartung beteiligt sind, berücksichtigt. Hierbei MÜSSEN insbesondere die Netzübergänge und die VS-IT, aus dem die Fernwartung gesteuert wird, betrachtet werden.

3.2. Standard-Anforderungen

Für diesen Baustein sind keine Standard-Anforderungen definiert.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Gesetzliche Grundlage für den Geheimschutz bildet das „Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz - SÜG).

Die auf der Grundlage des SÜG erlassene „Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA)“ enthält die Vorgaben für den materiellen Geheimschutz in der Bundesverwaltung.

Das BMWK veröffentlicht für den nichtöffentlichen Bereich das Geheimschutzhandbuch der Wirtschaft (GHB).

Das BSI gibt zur Umsetzung der VSA Technische Leitlinien heraus.

Das BSI gibt mit der „BSI-Schrift 7164“ eine Liste heraus, die alle IT-Sicherheitsprodukte mit gültiger Zulassungsaussage auflistet.

Weitergehende Informationen zur Zulassung von IT-Sicherheitsprodukten und einer genaueren Beschreibung der einzelnen IT-Sicherheitsfunktionen bietet das Dokument „VS-Produktkatalog des BSI“.

Die Grundsätze ordnungsgemäßer Aktenführung sind in der „Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien“, die vom BMI herausgegeben wird, festgelegt.