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.