Bundesamt
für Sicherheit in der
Informationstechnik

CON: Konzepte und Vorgehensweisen

CON.1: Kryptokonzept

1 Beschreibung

1.1 Einleitung

Kryptografie ist ein weit verbreitetes Mittel, um die Informationssicherheit in den Schutzzielen Vertraulichkeit, Integrität und Authentizität zu gewährleisten. Mit Hilfe von kryptografischen Verfahren werden Informationen verschlüsselt, sodass deren Inhalt ohne den zugehörigen Schlüssel nicht lesbar ist. Dabei können symmetrische Verfahren, d.h. es wird der selbe Schlüssel zum Verschlüsseln und Entschlüsseln verwendet, sowie asymmetrische Verfahren, d.h. es wird ein Schlüssel zum Verschlüsseln und ein anderer Schlüssel zum Entschlüsseln verwendet, eingesetzt werden.

In einer heterogenen Umgebung können dabei lokal gespeicherte Daten und auch die zu übertragenden Daten einer Institution wirkungsvoll durch kryptografische Verfahren und Techniken geschützt werden.

Darüber hinaus werden weitergehende Maßnahmen auf organisatorischer und prozessualer Ebene benötigt. Der alleinige technische Einsatz von kryptografischen Verfahren genügt nicht, um die Vertraulichkeit, Integrität und Authentizität der verschlüsselten Informationen zu gewährleisten.

Die Gesamtheit der eingesetzten kryptografischen Verfahren und damit verbundenen Maßnahmen wird im Rahmen eines Kryptokonzeptes gebündelt betrachtet. Nur durch eine ganzheitliche Betrachtung der Thematik wird ein effektiver Schutz durch Kryptografie ermöglicht.

Eine Besonderheit stellen Kryptomodule dar, die für kryptografische Verfahren bei erhöhtem Schutzbedarf eingesetzt werden können. Mit einem Kryptomodul ist ein Produkt gemeint, das die im Kryptokonzept dargelegte Sicherheitsfunktion bietet. Ein solches Produkt kann dabei aus Hardware, Software, Firmware oder aus einer Kombination daraus bestehen. Hinzu kommen noch notwendige Bauteile wie Speicher, Prozessoren, Busse und die Stromversorgung, um die Kryptoprozesse umzusetzen. Ein Kryptomodul kann in unterschiedlichen IT- oder Telekommunikationssystemen verwendet werden, um sensible Daten bzw. Informationen zu schützen.

1.2 Zielsetzung

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

1.3 Abgrenzung und Modellierung

Der Baustein CON.1 *Kryptokonzept* ist für den Informationsverbund einmal anzuwenden. In diesem Baustein werden allgemeine Anforderungen, organisatorische Rahmenbedingungen und prozessuale Abläufe für kryptografische Produkte und Verfahren behandelt. Die mit dem Betrieb von

Kryptomodulen zusammenhängenden Kern-IT-Aufgaben werden hier nicht thematisiert. Dafür müssen die Anforderungen der Bausteine aus der Schicht OPS.1.1 *Kern-IT-Betrieb* erfüllt werden.

Wie auf Anwendungsebene (z. B. Verschlüsselung oder Hashen von Passwörtern in einer Datenbank), 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

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein CON.1 *Kryptokonzept* von besonderer Bedeutung.

2.1 Unzureichendes Schlüsselmanagement bei Verschlüsselung

Durch ein unzureichendes Schlüsselmanagement könnten Angreifer auf verschlüsselte Daten zugreifen. So kann es beispielsweise sein, dass sich aufgrund fehlender Regelungen verschlüsselte Informationen mitsamt den dazugehörigen Schlüsseln auf demselben Datenträger befinden oder über den selben Kommunikationskanal (unverschlüsselt) übertragen werden. Dadurch kann bei symmetrischen Verfahren jeder, der auf den Datenträger oder den Kommunikationskanal zugreifen kann, die Informationen entschlüsseln, wenn das eingesetzte Verschlüsselungsverfahren bekannt ist.

2.2 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptografischen Verfahren

Wenn Institutionen kryptografische Verfahren und Produkte einsetzen, müssen sie dabei diverse gesetzliche Rahmenbedingungen beachten. In einigen Ländern dürfen beispielsweise kryptografische Verfahren nicht ohne staatliche Genehmigung eingesetzt werden. Das kann dazu führen, dass Empfänger im Ausland verschlüsselte Datensätze nicht lesen können, da sie die benötigten kryptografischen Produkte nicht einsetzen dürfen und sich dabei vielleicht sogar strafbar machen.

Außerdem ist in vielen Ländern auch der Einsatz von Produkten mit starker Kryptografie erheblich eingeschränkt. Das kann dazu verleiten, schützenswerte Daten unverschlüsselt zu lassen oder mit unsicheren Verfahren zu schützen. Dadurch sind einerseits leicht Angriffe möglich, andererseits kann auch gegen nationales Recht verstoßen werden. So können beispielsweise Datenschutzgesetze vorschreiben, dass adäquate kryptografische Verfahren eingesetzt werden müssen, um personenbezogene Daten zu schützen.

2.3 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten

Setzt eine Institution beispielsweise Kryptomodule ein, die zu kompliziert zu bedienen sind, könnten die Benutzer aus Bequemlichkeit oder aus pragmatischen Gründen darauf verzichten und stattdessen die Informationen im Klartext übertragen. Dadurch können die übertragenen Informationen von Angreifern abgehört werden.

Auch kann eine Fehlbedienung von Kryptomodulen dazu führen, dass vertrauliche Informationen von Angreifern abgegriffen werden, etwa wenn diese im Klartext übertragen werden, weil versehentlich der Klartext-Modus aktiviert wurde.

2.4 Software-Schwachstellen oder -Fehler in Kryptomodulen

Software-Schwachstellen oder -Fehler in Kryptomodulen beeinträchtigen die Sicherheit der eingesetzten kryptografischen Verfahren. Sie können etwa dazu führen, dass die damit geschützten Informationen mitgelesen werden. Darüber hinaus ist es möglich, dass Angreifer die Kryptomodule manipulieren, z. B. über Schadsoftware. So können institutionskritische Daten abfließen oder auch ganze Produktionsprozesse stillstehen, weil sich Daten nicht mehr entschlüsseln lassen.

2.5 Ausfall eines Kryptomoduls

Kryptomodule können durch technische Defekte, Stromausfälle oder absichtliche Zerstörung ausfallen. Dadurch könnten bereits verschlüsselte Daten nicht mehr entschlüsselt werden, solange das erforderliche Kryptomodul nicht mehr verfügbar ist. So können ganze Prozessketten stillstehen, z. B. wenn weitere IT-Anwendungen auf die Daten angewiesen sind.

2.6 Unsichere kryptografische Algorithmen oder Produkte

Unsichere oder veraltete kryptografische Algorithmen lassen sich von einem Angreifer mit vertretbaren Ressourcen brechen. Bei Verschlüsselungsalgorithmen bedeutet dies, dass es ihm gelingt, aus dem verschlüsselten Text den ursprünglichen Klartext zu ermitteln, ohne dass er zusätzliche Informationen hat, wie z. B. den verwendeten kryptografischen Schlüssel. Werden unsichere kryptografische Algorithmen eingesetzt, können Angreifer den kryptografischen Schutz unterlaufen und somit auf schützenswerte Informationen der Institution zugreifen. Selbst wenn in einer Institution ausschließlich sichere (z. B. zertifizierte) Produkte eingesetzt werden, kann die Kommunikation trotzdem unsicher werden. Das ist etwa dann der Fall, wenn der Kommunikationspartner kryptografische Verfahren benutzt, die nicht dem Stand der Technik entsprechen.

2.7 Fehler in verschlüsselten Daten 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 auch sämtliche Daten falsch entschlüsselt werden. Ist keine Datensicherung vorhanden, sind solche Daten verloren.

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 Daten nicht mehr entschlüsselt werden können.

2.8 Unautorisierte Nutzung eines Kryptomoduls

Gelingt es einem Angreifer, ein Kryptomodul unautorisiert zu benutzen, kann er kritische Sicherheitsparameter manipulieren. Somit bieten die kryptografischen Verfahren keine ausreichende Sicherheit mehr. Weiterhin kann ein Angreifer das Kryptomodul so manipulieren, dass es zwar auf den ersten Blick korrekt arbeitet, sich jedoch tatsächlich in einem unsicheren Zustand befindet. Dadurch bleibt der Angreifer längere Zeit unentdeckt und kann auf zahlreiche institutionskritische Informationen zugreifen.

2.9 Kompromittierung kryptografischer Schlüssel

Die Sicherheit kryptografischer Verfahren hängt entscheidend davon ab, wie vertraulich die verwendeten kryptografischen Schlüssel bleiben. Daher wird ein potenzieller Angreifer in der Regel versuchen, die verwendeten Schlüssel zu ermitteln. Das könnte ihm z. B. gelingen, indem er flüchtige Speicher ausliest oder ungeschützte Schlüssel findet, die beispielsweise in einer Datensicherung hinterlegt sind. Kennt er den verwendeten Schlüssel und das eingesetzte Kryptoverfahren, kann er die Daten relativ leicht entschlüsseln.

2.10 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.

Diese Zertifikate werden dann 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 Kommunikation mit dem Zertifikatsinhaber 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 Daten mit einem möglicherweise unsicheren Schlüssel verschlüsselt und versandt.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.1 *Kryptokonzept* aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	Informationssicherheitsbeauftragter (ISB)
Weitere Zuständigkeiten	Fachverantwortliche, IT-Betrieb, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein CON.1 *Kryptokonzept* vorrangig erfüllt werden:

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

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.

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

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

Bei einer Langzeitspeicherung verschlüsselter Daten SOLLTE regelmäßig geprüft werden, ob die verwendeten kryptografischen Algorithmen und die Schlüssellängen noch dem Stand der Technik entsprechen. Der IT-Betrieb MUSS sicherstellen, dass auf verschlüsselt gespeicherte Daten auch nach längeren Zeiträumen noch zugegriffen werden kann. Verwendete Kryptoprodukte SOLLTEN archiviert werden. Die Konfigurationsdaten von Kryptoprodukten SOLLTEN gesichert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein CON.1 *Kryptokonzept*. Sie SOLLTEN grundsätzlich erfüllt werden.

CON.1.A3 Verschlüsselung der Kommunikationsverbindungen (S)

Es SOLLTE geprüft werden, ob mit vertretbarem Aufwand eine Verschlüsselung der Kommunikationsverbindungen möglich und praktikabel ist. Ist dies der Fall, SOLLTEN Kommunikationsverbindungen geeignet verschlüsselt werden.

CON.1.A4 Geeignetes Schlüsselmanagement (S)

Kryptografische Schlüssel SOLLTEN immer mit geeigneten Schlüsselgeneratoren und in einer sicheren Umgebung erzeugt werden. Ein Schlüssel SOLLTE möglichst nur einem Einsatzzweck dienen.

Insbesondere SOLLTEN für die Verschlüsselung und Signaturbildung unterschiedliche Schlüssel benutzt werden. Der Austausch von kyptografischen Schlüsseln SOLLTE mit einem als sicher geltenden Verfahren durchgeführt werden.

Wenn Schlüssel verwendet werden, SOLLTE die authentische Herkunft und die Integrität der Schlüsseldaten überprüft werden.

Alle kryptografischen Schlüssel SOLLTEN hinreichend häufig gewechselt werden. Es SOLLTE eine festgelegte Vorgehensweise für den Fall geben, dass ein Schlüssel offengelegt wurde. Alle erzeugten kryptografischen Schlüssel SOLLTEN sicher aufbewahrt und verwaltet werden.

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

Nicht mehr benötigte Schlüssel und Zertifikate SOLLTEN sicher gelöscht bzw. vernichtet werden.

CON.1.A6 Bedarfserhebung für kryptografische Verfahren und Produkte [IT-Betrieb, Fachverantwortliche] (S)

Es SOLLTE festgelegt werden, für welche Geschäftsprozesse oder Fachverfahren kryptografische Verfahren eingesetzt werden sollen. Danach SOLLTEN die Anwendungen, IT-Systeme und Kommunikationsverbindungen identifiziert werden, die notwendig sind, um die Aufgaben zu erfüllen. Diese SOLLTEN durch den IT-Betrieb geeignet kryptografisch abgesichert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein CON.1 *Kryptokonzept* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

CON.1.A7 Erstellung einer Sicherheitsrichtlinie für den Einsatz kryptografischer Verfahren und Produkte (H)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTE eine spezifische Richtlinie für den Einsatz von Kryptoprodukten erstellt werden. In der Sicherheitsrichtlinie SOLLTE geregelt werden, wer für den sicheren Betrieb der kryptografischen Produkte zuständig ist. Für die benutzten Kryptoprodukte SOLLTE es Vertretungsregelungen geben.

Auch SOLLTEN notwendige Schulungs- und Sensibilisierungsmaßnahmen für Benutzer sowie Verhaltensregeln und Meldewege bei Problemen oder Sicherheitsvorfällen festgelegt werden. Weiter SOLLTE die Richtlinie definieren, wie sichergestellt wird, dass Kryptomodule sicher konfiguriert, korrekt eingesetzt und regelmäßig gewartet werden.

Die Richtlinie SOLLTE allen relevanten Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von ihr abgewichen, SOLLTE dies mit dem ISB abgestimmt und dokumentiert werden. Es SOLLTE regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt wird. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

CON.1.A8 Erhebung der Einflussfaktoren für kryptografische Verfahren und Produkte (H)

Bevor entschieden werden kann, welche kryptografischen Verfahren und Produkte bei erhöhtem Schutzbedarf eingesetzt werden, SOLLTEN unter anderem folgende Einflussfaktoren ermittelt werden:

- Sicherheitsaspekte (siehe CON.1.A6 Bedarfserhebung für kryptografische Verfahren und Produkte),
- technische Aspekte,
- personelle und organisatorische Aspekte,
- wirtschaftliche Aspekte,

- Lebensdauer von kryptografischen Verfahren und der eingesetzten Schlüssellängen,
- Zulassung von kryptografischen Produkten sowie
- gesetzliche Rahmenbedingungen.

CON.1.A9 Auswahl eines geeigneten kryptografischen Produkts [IT-Betrieb, Fachverantwortliche] (H)

Bevor ein kryptografisches Produkt ausgewählt wird, SOLLTE die Institution festlegen, welche Anforderungen das Produkt erfüllen muss. Dabei SOLLTEN Aspekte wie Funktionsumfang, Interoperabilität, Wirtschaftlichkeit sowie Fehlbedienungs- und Fehlfunktionssicherheit betrachtet werden. Es SOLLTE geprüft werden, ob zertifizierte Produkte vorrangig eingesetzt werden sollen. Auch die zukünftigen Einsatzorte SOLLTEN bei der Auswahl beachtet werden, da es z. B. Export- und Importbeschränkungen für kryptografische Produkte gibt.

Auf Produkte mit unkontrollierbarer Schlüsselablage SOLLTE generell verzichtet werden.

CON.1.A10 Entwicklung eines Kryptokonzepts (H)

Es SOLLTE ein Kryptokonzept entwickelt werden, das in das Sicherheitskonzept der Institution integriert wird. Im Konzept SOLLTEN alle technischen und organisatorischen Vorgaben für die eingesetzten kryptografischen Produkte beschrieben werden. Auch SOLLTEN alle relevanten Anwendungen, IT-Systeme und Kommunikationsverbindungen aufgeführt sein. Das erstellte Kryptokonzept SOLLTE regelmäßig aktualisiert werden.

CON.1.A11 Sichere Konfiguration der Kryptomodule [IT-Betrieb] (H)

Kryptomodule SOLLTEN sicher installiert und konfiguriert werden. Alle voreingestellten Schlüssel SOLLTEN geändert werden. Anschließend SOLLTE getestet werden, ob die Kryptomodule korrekt funktionieren und vom Benutzer auch bedient werden können.

Weiterhin SOLLTEN die Anforderungen an die Einsatzumgebung festgelegt werden. Wenn ein IT-System geändert wird, SOLLTE getestet werden, ob die eingesetzten kryptografischen Verfahren noch greifen. Die Konfiguration der Kryptomodule SOLLTE dokumentiert und regelmäßig überprüft werden.

CON.1.A12 Sichere Rollenteilung beim Einsatz von Kryptomodulen [IT-Betrieb] (H)

Bei der Konfiguration eines Kryptomoduls SOLLTEN Benutzerrollen festgelegt werden. Es SOLLTE mit Zugriffskontroll- und Authentisierungsmechanismen verifiziert werden, ob ein Mitarbeiter den gewünschten Dienst auch tatsächlich benutzen darf. Das Kryptomodul SOLLTE so konfiguriert sein, dass bei jedem Rollenwechsel oder bei Inaktivität nach einer bestimmten Zeitdauer die Authentisierungsinformationen erneut eingegeben werden müssen.

CON.1.A13 Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen (H)

Das Zusammenwirken von Betriebssystem und Kryptomodulen SOLLTE gewährleisten, dass

- die installierten Kryptomodule nicht unbemerkt abgeschaltet oder umgangen werden können,
- die angewendeten oder gespeicherten Schlüssel nicht kompromittiert werden können,
- die zu schützenden Daten nur mit Wissen und unter Kontrolle des Benutzers auch unverschlüsselt auf Datenträgern abgespeichert werden bzw. das informationsverarbeitende System verlassen können sowie
- Manipulationsversuche am Kryptomodul erkannt werden.

CON.1.A14 Schulung von Benutzern und Administratoren [Vorgesetzte, Fachverantwortliche, IT-Betrieb] (H)

Es SOLLTE Schulungen geben, in denen Benutzern und Administratoren der Umgang mit den für sie relevanten Kryptomodulen vermittelt wird. Den Benutzern SOLLTE genau erläutert werden, was die spezifischen Sicherheitseinstellungen von Kryptomodulen bedeuten und warum sie wichtig sind. Außerdem SOLLTEN sie auf die Gefahren hingewiesen werden, die drohen, wenn diese

Sicherheitseinstellungen aus Bequemlichkeit umgangen oder deaktiviert werden. Die Schulungsinhalte SOLLTEN immer den jeweiligen Einsatzszenarien entsprechend angepasst werden.

Die Administratoren SOLLTEN zudem gezielt dazu geschult werden, wie die Kryptomodule zu administrieren sind. Auch SOLLTEN sie einen Überblick über kryptografische Grundbegriffe erhalten.

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

Es SOLLTE ein Prozess etabliert werden, der im Falle eines geschwächten kryptografischen Verfahrens herangezogen werden kann. Dabei SOLLTE sichergestellt werden, dass das geschwächte kryptografische Verfahren abgesichert werden kann oder durch eine geeignete Alternative abgelöst wird.

CON.1.A16 Physische Absicherung von Kryptomodulen [IT-Betrieb] (H)

Der IT-Betrieb SOLLTE sicherstellen, dass nicht unautorisiert physisch auf Modulinhalte des Kryptomoduls zugegriffen wird. Hard- und Softwareprodukte, die als Kryptomodule eingesetzt werden, SOLLTEN einen Selbsttest durchführen können.

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

Es SOLLTE untersucht 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.

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

Es SOLLTEN Ersatzkryptomodule vorrätig sein.

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.

Das BSI hat die Arbeitshilfen „Leitfaden Erstellung von Kryptokonzepten“ und ein „Musterkryptokonzept“erstellt, die Institutionen bei der Erstellung eigener Kryptokonzepte unterstützen können.

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.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein CON.1 *Kryptokonzept* von Bedeutung.

G 0.13 Abfangen kompromittierender Strahlung

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen