DER: Detektion und Reaktion

DER.1: Detektion von sicherheitsrelevanten Ereignissen

1 Beschreibung

1.1 Einleitung

Um IT-Systeme schützen zu können, müssen sicherheitsrelevante Ereignisse rechtzeitig erkannt und behandelt werden. Dazu ist es notwendig, dass Institutionen im Vorfeld geeignete organisatorische, personelle und technische Maßnahmen planen, implementieren und regelmäßig üben. Denn wenn auf ein vorgegebenes und erprobtes Verfahren aufgesetzt werden kann, lassen sich Reaktionszeiten verkürzen und vorhandene Prozesse optimieren.

Als sicherheitsrelevantes Ereignis wird ein Ereignis bezeichnet, das sich auf die Informationssicherheit auswirkt und die Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen kann. Typische Folgen solcher Ereignisse sind ausgespähte, manipulierte oder zerstörte Informationen. Die Ursachen dafür sind dabei vielfältig. So spielen unter anderem Malware, veraltete IT-Systeminfrastrukturen oder Innentäter eine Rolle. Angreifer nutzen aber auch oft Zero-Day-Exploits aus, also Sicherheitslücken in Programmen, bevor es für diese einen Patch gibt. Eine weitere ernstzunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APT). Dabei handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen Zugriff in der Folge auf weitere IT-Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus und sind oft schwer zu detektieren.

1.2 Zielsetzung

Dieser Baustein zeigt einen systematischen Weg auf, wie Informationen gesammelt, korreliert und ausgewertet werden können, um sicherheitsrelevante Ereignisse möglichst vollständig und zeitnah zu detektieren. Die aus der Detektion gewonnenen Erkenntnisse sollen die Fähigkeit von Institutionen verbessern, sicherheitsrelevante Ereignisse zu erkennen und angemessen darauf zu reagieren.

1.3 Abgrenzung und Modellierung

Der Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* ist auf den Informationsverbund einmal anzuwenden.

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn sicherheitsrelevante Ereignisse detektiert werden sollen. Voraussetzung hierfür ist jedoch, dass umfassend protokolliert wird. Die dafür notwendigen Anforderungen werden nicht im vorliegenden

Baustein beschrieben, sondern sind im Baustein OPS.1.1.5 *Protokollierung* enthalten.

Im Vorfeld der Detektion von sicherheitsrelevanten Ereignissen ist es wichtig, dass Zuständigkeiten und Kompetenzen klar definiert und zugewiesen werden. Es sollte insbesondere auf den Grundsatz der Funktionstrennung geachtet werden. Dieses Thema ist nicht Bestandteil dieses Bausteins, sondern wird im Baustein ORP. 1 *Organisation* behandelt.

Außerdem beschreibt der Baustein nicht, wie mit sicherheitsrelevanten Ereignissen umzugehen ist, nachdem sie detektiert worden sind. Empfehlungen dazu werden in den Bausteinen DER.2.1 *Behandlung von Sicherheitsvorfällen* und DER.2.2 *Vorsorge für die IT-Forensik* aufgeführt. Ebenso wird nicht auf das Thema Datenschutz eingegangen, dieses wird im Baustein CON.2 *Datenschutz* behandelt.

Um sicherheitsrelevante Ereignisse zu erkennen, sind oft zusätzliche Programme erforderlich, z. B. Antivirenprogramme, Firewalls oder Intrusion Detection /Intrusion Prevention Systeme (IDS/IPS). Sicherheitsaspekte dieser Systeme sind ebenfalls nicht Gegenstand des vorliegenden Bausteins. Sie werden z. B. in den Bausteinen OPS.1.1.4 *Schutz vor Schadprogrammen* bzw. NET.3.2 *Firewall* thematisiert.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* von besonderer Bedeutung.

2.1 Missachtung von gesetzlichen Vorschriften und betrieblichen Mitbestimmungsrechten

Programme, die sicherheitsrelevante Ereignisse detektieren und Protokolldaten auswerten, sammeln oft viele Informationen über die Netzstruktur und die internen Abläufe einer Institution. Darin können schützenswerte Informationen wie personenbezogene Daten, vertrauliche Daten oder Arbeitsabläufe von Mitarbeitern enthalten sein. Dadurch, dass solche Daten gespeichert werden, können jedoch Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeiter verletzt werden. Auch verstößt die Institution unter bestimmten Voraussetzungen eventuell gegen die jeweiligen Datenschutzgesetze.

2.2 Unzureichende Qualifikation der Mitarbeiter

Im täglichen IT-Betrieb einer Institution können viele Störungen und Fehler auftreten, z. B. könnten ankommende Protokolldaten plötzlich stark zunehmen. Sind die zuständigen Mitarbeiter nicht ausreichend sensibilisiert und geschult, kann es passieren, dass sie sicherheitsrelevante Ereignisse nicht als solche identifizieren und so Angriffe unerkannt bleiben. Und auch wenn die Mitarbeiter ausreichend für die Belange der Informationssicherheit sensibilisiert bzw. geschult sind, kann trotzdem nicht ausgeschlossen werden, dass sie Sicherheitsvorfälle nicht erkennen. Beispiele dafür sind:

- Ein Benutzer, der seit längerer Zeit nicht im lokalen Netz seiner Institution angemeldet war, stuft es als normal ein, dass sein Notebook seit einer Woche während des Internetzugangs deutlich langsamer ist. Er bemerkt nicht, dass ein Schadprogramm im Hintergrund aktiv ist. Er wurde nicht oder nur unzureichend geschult, bei verdächtigen Auffälligkeiten den Informationssicherheitsbeauftragten zu informieren.
- Ein Produktionsleiter bemerkt nicht, dass die Daten in den Produktionssystemen und auch die Steuerungsanzeigesysteme heimlich verändert wurden. Er schöpft keinen Verdacht, als die SCADA-Steuerung der Produktionsanlage seltsame Werte anzeigt, da dies nur kurzzeitig erfolgte. Der Vorfall wird nicht gemeldet, da alle Werte wieder den erwarteten Anzeigewerten entsprechen. Dass eine Schadsoftware die Anzeigewerte manipuliert hat, fällt somit niemandem auf.

2.3 Fehlerhafte Administration der eingesetzten Detektionssysteme

Fehlerhafte Konfigurationen können dazu führen, dass eingesetzte Detektionssysteme nicht ordnungsgemäß funktionieren. Ist beispielsweise die Alarmierung falsch eingestellt, können vermehrt

Fehlalarme auftreten. Die zuständigen Mitarbeiter können dann eventuell nicht mehr zwischen einem Fehlalarm und einem sicherheitsrelevanten Ereignis unterscheiden. Auch nehmen sie die Meldungen möglicherweise nicht schnell genug wahr, da zu viele Alarme generiert werden. Dadurch bleiben möglicherweise Angriffe unerkannt. Ebenso steigt der Aufwand stark an, um die Menge der Meldungen auszuwerten.

2.4 Fehlende Informationen über den zu schützenden Informationsverbund

Sind keine oder nur ungenügende Informationen über den zu schützenden Informationsverbund vorhanden, kann es passieren, dass wesentliche Bereiche des Informationsverbunds nicht ausreichend durch Detektionssysteme abgesichert werden. Dadurch können Angreifer leicht in das Netz der Institution eindringen und z. B. schützenswerte Informationen abgreifen. Auch ist es ihnen so möglich, lange unbemerkt im System zu bleiben und dauerhaft auf das Netz zuzugreifen.

2.5 Unzureichende Nutzung von Detektionssystemen

Wenn keine Detektionssysteme eingesetzt werden und auch die in IT-Systemen und Anwendungen vorhandenen Funktionen zur Detektion von sicherheitsrelevanten Ereignissen nicht benutzt werden, können Angreifer leichter unbemerkt in das Netz der Institution eindringen. Dort könnten sie unbefugt auf sensible Informationen zugreifen. Besonders kritisch ist es, wenn die Übergänge zwischen Netzgrenzen nur unzureichend überwacht werden.

2.6 Unzureichende personelle Ressourcen

Ist nicht genügend Personal vorhanden, um Protokolldaten auszuwerten, können sicherheitsrelevante Ereignisse nicht vollständig detektiert werden. So bleiben Angriffe eventuell lange verborgen oder werden erst entdeckt, nachdem z. B. schon sehr viele schützenswerte Informationen abgeflossen sind. Auch wenn durch zu wenig Personal keine externen Informationsquellen ausgewertet werden, bleiben Sicherheitslücken eventuell zu lange offen. Dann können sie von Angreifern ausgenutzt werden, um unerlaubt in die IT-Systeme der Institution einzudringen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.1 *Detektion von sicherheitsrelevanten Ereignissen* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der 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 Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Mitarbeiter, Fachverantwortliche, Benutzer, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* vorrangig erfüllt werden:

DER.1.A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen erstellt werden. In der spezifischen Sicherheitsrichtlinie MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben werden, wie die Detektion von sicherheitsrelevanten Ereignissen geplant, aufgebaut und sicher betrieben werden kann. Die spezifische Sicherheitsrichtlinie MUSS allen im Bereich Detektion zuständigen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Falls die spezifische Sicherheitsrichtlinie verändert wird oder von den Anforderungen abgewichen wird, dann MUSS dies mit dem verantwortlichen ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist. Die Ergebnisse der Überprüfung MÜSSEN sinnvoll dokumentiert werden.

DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokollierungsdaten (B)

Wenn Protokollierungsdaten ausgewertet werden, dann MÜSSEN dabei die Bestimmungen aus den aktuellen Gesetzen zum Bundes- und Landesdatenschutz eingehalten werden. Wenn Detektionssysteme eingesetzt werden, dann MÜSSEN die Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitervertretungen gewahrt werden. Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden, z. B. das Telemediengesetz (TMG), das Betriebsverfassungsgesetz und das Telekommunikationsgesetz.

DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse (B)

Für sicherheitsrelevante Ereignisse MÜSSEN geeignete Melde- und Alarmierungswege festgelegt und dokumentiert werden. Es MUSS bestimmt werden, welche Stellen wann zu informieren sind. Es MUSS aufgeführt sein, wie die jeweiligen Personen erreicht werden können. Je nach Dringlichkeit MUSS ein sicherheitsrelevantes Ereignis über verschiedene Kommunikationswege gemeldet werden.

Alle Personen, die für die Meldung bzw. Alarmierung relevant sind, MÜSSEN über ihre Aufgaben informiert sein. Alle Schritte des Melde- und Alarmierungsprozesses MÜSSEN ausführlich beschrieben sein. Die eingerichteten Melde- und Alarmierungswege SOLLTEN regelmäßig geprüft, erprobt und aktualisiert werden, falls erforderlich.

DER.1.A4 Sensibilisierung der Mitarbeiter [Vorgesetzte, Benutzer, Mitarbeiter] (B)

Jeder Benutzer MUSS dahingehend sensibilisiert werden, dass er Ereignismeldungen seines Clients nicht einfach ignoriert oder schließt. Jeder Benutzer MUSS die Meldungen entsprechend der Alarmierungswege an das verantwortliche Incident Management weitergeben (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

Jeder Mitarbeiter MUSS einen von ihm erkannten Sicherheitsvorfall unverzüglich dem Incident Management melden.

DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion [Fachverantwortliche] (B)

Falls eingesetzte IT-Systeme oder Anwendungen über Funktionen verfügen, mit denen sich sicherheitsrelevante Ereignisse detektieren lassen, dann MÜSSEN diese aktiviert und benutzt werden. Falls ein sicherheitsrelevanter Vorfall vorliegt, dann MÜSSEN die Meldungen der betroffenen IT-Systeme ausgewertet werden. Zusätzlich MÜSSEN die protokollierten Ereignisse anderer IT-Systeme überprüft werden. Auch SOLLTEN die gesammelten Meldungen in verbindlich festgelegten Zeiträumen stichpunktartig kontrolliert werden.

Es MUSS geprüft werden, ob zusätzliche Schadcodescanner auf zentralen IT-Systemen installiert werden sollen. Falls zusätzliche Schadcodescanner eingesetzt werden, dann MÜSSEN diese es über einen zentralen Zugriff ermöglichen, ihre Meldungen und Protokolle auszuwerten. Es MUSS sichergestellt sein, dass die Schadcodescanner sicherheitsrelevante Ereignisse automatisch an die

Zuständigen melden. Die Zuständigen MÜSSEN die Meldungen auswerten und untersuchen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen*. Sie SOLLTEN grundsätzlich erfüllt werden.

DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten (S)

Alle Protokollierungsdaten SOLLTEN möglichst permanent aktiv überwacht und ausgewertet werden. Es SOLLTEN Mitarbeiter benannt werden, die dafür zuständig sind.

Falls die zuständigen Mitarbeiter aktiv nach sicherheitsrelevanten Ereignissen suchen müssen, z. B. wenn sie IT-Systeme kontrollieren oder testen, dann SOLLTEN solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein.

Für die Detektion von sicherheitsrelevanten Ereignissen SOLLTEN genügend personelle Ressourcen bereitgestellt werden.

DER.1.A7 Schulung von Zuständigen [Vorgesetzte] (S)

Alle Zuständigen, die Ereignismeldungen kontrollieren, SOLLTEN weiterführende Schulungen und Qualifikationen erhalten. Wenn neue IT-Komponenten beschafft werden, SOLLTE ein Budget für Schulungen eingeplant werden. Bevor die zuständigen Mitarbeiter Schulungen für neue IT-Komponenten bekommen, SOLLTE ein Schulungskonzept erstellt werden.

DER.1.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

DER.1.A9 Einsatz zusätzlicher Detektionssysteme [Fachverantwortliche] (S)

Anhand des Netzplans SOLLTE festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen. Der Informationsverbund SOLLTE um zusätzliche Detektionssysteme und Sensoren ergänzt werden. Schadcodedetektionssysteme SOLLTEN eingesetzt und zentral verwaltet werden. Auch die im Netzplan definierten Übergange zwischen internen und externen Netzen SOLLTEN um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.

DER.1.A10 Einsatz von TLS-/SSH-Proxies [Fachverantwortliche] (S)

An den Übergängen zu externen Netzen SOLLTEN TLS-/SSH-Proxies eingesetzt werden, welche die verschlüsselte Verbindung unterbrechen und es so ermöglichen, die übertragenen Daten auf Malware zu prüfen. Alle TLS-/SSH-Proxies SOLLTEN vor unbefugten Zugriffen geschützt werden. Auf den TLS-/SSH-Proxies SOLLTEN sicherheitsrelevante Ereignisse automatisch detektiert werden. Es SOLLTE eine organisatorische Regelung erstellt werden, unter welchen datenschutzrechtlichen Voraussetzungen die Logdaten manuell ausgewertet werden dürfen.

DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse [Fachverantwortliche] (S)

Die auf einer zentralen Protokollinfrastruktur gespeicherten Ereignismeldungen der IT-Systeme und Anwendungen (siehe OPS.1.1.5 *Protokollierung*) SOLLTEN mithilfe eines Tools abgerufen werden können. Mit dem auswählten Tool SOLLTEN die Meldungen ausgewertet werden können. Die gesammelten Ereignismeldungen SOLLTEN regelmäßig auf Auffälligkeiten kontrolliert werden. Die Signaturen der Detektionssysteme SOLLTEN immer aktuell und auf dem gleichen Stand sein, damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können.

DER.1.A12 Auswertung von Informationen aus externen Quellen [Fachverantwortliche] (S)

Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, SOLLTEN externe Quellen herangezogen werden. Meldungen über unterschiedliche Kanäle

SOLLTEN von den Mitarbeitern auch als relevant erkannt und an die richtige Stelle weitergeleitet werden. Informationen aus zuverlässigen Quellen SOLLTEN grundsätzlich ausgewertet werden. Alle gelieferten Informationen SOLLTEN danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind. Ist dies der Fall, SOLLTEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.

DER.1.A13 Regelmäßige Audits der Detektionssysteme (S)

Die vorhandenen Detektionssysteme und getroffenen Maßnahmen SOLLTEN in regelmäßigen Audits daraufhin überprüft werden, ob sie noch aktuell und wirksam sind. Es SOLLTEN die Messgrößen ausgewertet werden, die beispielsweise anfallen, wenn sicherheitsrelevante Ereignisse aufgenommen, gemeldet und eskaliert werden. Die Ergebnisse der Audits SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* 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.

DER.1.A14 Auswertung der Protokollierungsdaten durch spezialisiertes Personal (H)

Es SOLLTEN Mitarbeiter speziell damit beauftragt werden, alle Protokollierungsdaten zu überwachen. Die Überwachung der Protokollierungsdaten SOLLTE die überwiegende Aufgabe der beauftragten Mitarbeiter sein. Die beauftragten Mitarbeiter SOLLTEN spezialisierte weiterführende Schulungen und Qualifikationen erhalten. Ein Personenkreis SOLLTE benannt werden, der ausschließlich für das Thema Auswertung von Protokollierungsdaten verantwortlich ist.

DER.1.A15 Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen (H)

Zentrale Komponenten SOLLTEN eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. Zentrale, automatisierte Analysen mit Softwaremitteln SOLLTEN eingesetzt werden. Mit diesen zentralen, automatisierten Analysen mit Softwaremitteln SOLLTEN alle in der Systemumgebung anfallenden Ereignisse aufgezeichnet und in Bezug zueinander gesetzt werden. Die sicherheitsrelevanten Vorgänge SOLLTEN sichtbar gemacht werden. Alle eingelieferten Daten SOLLTEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein. Die Daten SOLLTEN möglichst permanent ausgewertet werden. Werden definierte Schwellwerte überschritten, SOLLTE automatisch alarmiert werden. Das Personal SOLLTE sicherstellen, dass bei einem Alarm unverzüglich eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. In diesem Zusammenhang SOLLTE auch der betroffene Mitarbeiter sofort informiert werden.

Die Systemverantwortlichen SOLLTEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist. Zusätzlich SOLLTEN bereits überprüfte Daten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.

DER.1.A16 Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen (H)

Anwendungen mit erhöhtem Schutzbedarf SOLLTEN durch zusätzliche Detektionsmaßnahmen geschützt werden. Dafür SOLLTEN z. B. solche Detektionssysteme eingesetzt werden, mit denen sich der erhöhte Schutzbedarf technisch auch sicherstellen lässt.

DER.1.A17 Automatische Reaktion auf sicherheitsrelevante Ereignisse (H)

Bei einem sicherheitsrelevanten Ereignis SOLLTEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und mit geeigneten Schutzmaßnahmen reagieren. Hierbei SOLLTEN Verfahren eingesetzt werden, die automatisch mögliche Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen erkennen. Es SOLLTE möglich sein, automatisch in den Datenstrom

einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden.

DER.1.A18 Durchführung regelmäßiger Integritätskontrollen (H)

Alle Detektionssysteme SOLLTEN regelmäßig daraufhin überprüft werden, ob sie noch integer sind. Auch SOLLTEN die Benutzerrechte kontrolliert werden. Zusätzlich SOLLTEN die Sensoren eine Integritätskontrolle von Dateien durchführen. Bei sich ändernden Werten SOLLTE eine automatische Alarmierung ausgelöst werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) regelt in seinem Mindeststandard „Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen“ die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen (SRE).

Das BSI hat das weiterführende Dokument „BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen, Version 1.0“ zum Themenfeld Intrusion Detection veröffentlicht.

Das Infomation Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel TS1.5 Intrusion Detection Vorgaben für den Einsatz von Intrusion Detection Systemen.

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 DER.1 *Detektion von sicherheitsrelevanten Ereignissen* von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

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 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.46 Integritätsverlust schützenswerter Informationen