Systeme zur Angriffserkennung – Kriterienkatalog und Vorgehensweise zur Prüfung und Nachweisführung

datenschutz cert GmbH
Version 1.4

datenschutz cert

Inhaltsverzeichnis

Historie

Version	Datum	Geänderte Kapitel	Grund der Änderung	Geändert durch
1.0	11.11.2022		Erstellung	Dr. Sönke Maseberg
1.1	14.11.2022	4.3	Ergänzung zum Erreichungsgrad	Dr. Sönke Maseberg
1.2	15.11.2022		Editorielle Korrekturen	Dr. Sönke Maseberg
1.3	22.02.2023		Editorielle Korrekturen	Dr. Sönke Maseberg
1.4	20.03.2023		##SzA-15 gelöscht	Dr. Sönke Maseberg

1. Einleitung

Der Gesetzgeber verpflichtet Betreiber Kritischer Infrastrukturen sowie Netz- und Kraftwerksbetreiber sogenannte „Systeme zur Angriffserkennung“ einzuführen. Diese Systeme zur Angriffserkennung (SzA) müssen dabei „geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen“ (§8a Abs. 1a BSIG).

Diese gesetzliche Verpflichtung betrifft nicht nur KRITIS-Unternehmen gem. §8a BSIG, die die KRITIS-Schwellwerte überschreiten, sondern über §11 Abs. 1d EnWG auch alle Strom- und Gasnetzbetreiber sowie alle Kraftwerksbetreiber, die unter die KRITIS-VO fallen.

Neben der Einführung von Systemen zur Angriffserkennung ist eine Prüfung mit Nachweis der Umsetzung durch unabhängige Stellen gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgesehen.

Vom Gesetzgeber sind ferner Fristen festgelegt worden:

- Einführung von Systemen zur Angriffserkennung: bis 01.05.2023
- Nachweis der Umsetzung ggü. dem BSI:
  - Netzbetreiber: erstmals am 01.05.2023, danach alle zwei Jahre
  - Kraftwerksbetreiber, die unter KRITIS fallen: erstmals am 01.05.2023, danach alle zwei Jahre
  - Betreiber Kritischer Infrastrukturen, die unter KRITIS fallen: reguläre §8a-Nachweispflichten

Das BSI hat in der „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ [OH-SzA] weitere Vorgaben normiert.

Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle (DAkkS) als Zertifizierungsstelle akkreditiert und beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als IT-Sicherheitsdienstleister zertifiziert, und verfügt über Prüfer mit §8a-Prüfverfahrenskompetenz; damit kann die datenschutz cert GmbH die Prüfungen zu Systemen zur Angriffserkennung durchführen und Nachweise gegenüber dem BSI erbringen.

Das vorliegende Dokument enthält die Anforderungen an Systeme zur Angriffserkennung (Kriterienkatalog) sowie Informationen zur Prüfung und Nachweisführung.

2. Systeme zur Angriffserkennung und gesetzliche Vorgaben

Zwei Gesetze sind relevant: Das BSI-Gesetz (BSIG) mit den Schwellwerten der KRITIS-Verordnung (KRITIS-VO) sowie das Energiewirtschaftsgesetz (EnWG).

§ 8a Abs. 1 BSIG normiert zentral Vorkehrungen zur Informationssicherheit bei Betreibern von Kritischen Infrastrukturen:

> § 8a Abs. 1 BSIG: „Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht."

§ 8a Abs. 1a BSIG ergänzt diese Vorgaben um Systeme zur Angriffserkennung:

> § 8a Abs. 1a BSIG: „Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend."

Systeme zur Angriffserkennung werden in §2 Abs. 9b BSIG definiert:

> §2 Abs. 9b BSIG: „Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten."

In § 8a Abs. 3 BSIG finden sich die Vorgaben zur Nachweispflicht gegenüber dem BSI:

> § 8a Abs. 3 BSIG: „Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre dem Bundesamt nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten

Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen."

Strom- und Gasnetz- sowie Kraftwerksbetreiber – exakt Betreiber von Energieversorgungsnetzen und Energieanlagen – werden über §11 Abs. 1d EnWG einbezogen:

§11 Abs. 1d EnWG: Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben spätestens ab dem 1. Mai 2023 in ihren informationstechnischen Systemen, Komponenten oder Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen Energieversorgungsnetze oder Energieanlagen maßgeblich sind, in angemessener Weise Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Dabei soll der Stand der Technik eingehalten werden. Der Einsatz von Systemen zur Angriffserkennung ist angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen eines Ausfalls oder einer Beeinträchtigung des betroffenen Energieversorgungsnetzes oder der betroffenen Energieanlage steht."

Die Nachweisfristen werden in §11 Abs. 1e EnWG definiert:

§11 Abs. 1e EnWG: „Betreiber von Energieversorgungsnetzen und Energieanlagen, die nach der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur gelten, haben dem Bundesamt für Sicherheit in der Informationstechnik erstmalig am 1. Mai 2023 und danach alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1d nachzuweisen. Das Bundesamt für Sicherheit in der Informationstechnik hat die hierfür eingereichten Nachweisdokumente unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Das Bundesamt für Sicherheit in der Informationstechnik kann bei Mängeln in der Umsetzung der Anforderungen nach Absatz 1d oder in den Nachweisdokumenten nach Satz 1 im Einvernehmen mit der Bundesnetzagentur die Beseitigung der Mängel verlangen."

In §11 Abs. 1g EnWG wird bereits eine Konkretisierung zum 22.05.2023 angekündigt:

§11 Abs. 1g EnWG: Die Bundesnetzagentur legt bis zum 22. Mai 2023 im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Allgemeinverfügung im Wege einer Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheits-

anforderungen für das Betreiben von Energieversorgungsnetzen und Energieanlagen fest,

1. welche Komponenten kritische Komponenten im Sinne des § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe a des BSI-Gesetzes sind oder

2. welche Funktionen kritisch bestimmte Funktionen im Sinne des § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b des BSI-Gesetzes sind.

Die Betreiber von Energieversorgungsnetzen und Energieanlagen, die durch Rechtsverordnung gemäß § 10 Absatz 1 Satz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben die Vorgaben des Katalogs spätestens sechs Monate nach dessen Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden. Der Katalog wird mit den Katalogen der Sicherheitsanforderungen nach § 11 Absatz 1a und 1b verbunden.

In der Orientierungshilfe [OH-SzA] werden Systeme zur Angriffserkennung näher erläutert:

[OH-SzA]: Zum einen müssen die Systeme durch fortlaufende Auswertung der gesammelten Informationen (Protokollierung) sicherheitsrelevante Ereignisse erkennen (Detektion). Dies kann beispielsweise durch Missbrauchserkennung oder Anomalie-Erkennung erfolgen.

Zum anderen sollten Systeme zur Angriffserkennung Maßnahmen implementieren, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren (Reaktion). Dies kann sowohl durch technische als auch durch organisatorische Maßnahmen umgesetzt werden.

Der Einsatz von SzA muss die informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, abdecken. Dies bezieht sowohl IT als auch OT sowie Rechenzentren oder Embedded Systems und schließt weitere Bereiche mit ein.

Ferner finden sich in der Orientierungshilfe konkrete Anforderungen, die im Nachfolgenden dargestellt werden.

3. Kriterienkatalog

Ausgehend von den oben skizzierten Vorgaben hat die datenschutz cert GmbH für ihre Prüfungen von Systemen zur Angriffserkennung den vorliegenden Kriterienkatalog erstellt. Vorgaben der Orientierungshilfe [OH-SzA] wurden dabei wortwörtlich übernommen.

Der Kriterienkatalog enthält konkrete Anforderungselemente zu den drei Phasen

- Protokollierung,
- Detektion und
- Reaktion.

Zur besseren Orientierung sind die Anforderungselemente mit „##SzA“ gekennzeichnet.

3.1. Protokollierung

Planung der Protokollierung

3.1.1. ##SzA-01: Risikoanalyse

In der Planungsphase SOLLTE, basierend auf den Ergebnissen der Risikoanalyse und in Anbetracht der kritischen Prozesse des Betreibers, eine schrittweise Vorgehensweise für die Umsetzung der Protokollierung geplant werden. Die Schritte MÜSSEN dabei so gewählt werden, dass eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt wird.

3.1.2. ##SzA-02: Protokoll- und Protokollierungsdaten

Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (siehe Glossar gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können. Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann. Die zur Speicherung notwendigen Systeme und deren IT-Sicherheitsvorkehrungen MÜSSEN schon in der Planung bedacht werden. Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.

3.1.3. ##SzA-03: Relevante Systeme

Im Rahmen der Planung MÜSSEN alle Systeme identifiziert werden, die zur Aufrechterhaltung der kritischen Dienstleistung maßgeblich sind, damit deren Protokoll- und Protokollierungsdaten später erfasst werden können.

3.1.4. ##SzA-04: Modernisierungsaufforderung

Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.

3.1.5. ##SzA-05: Kapazitätsabschätzung

Das anfallende Protokoll- und Protokollierungsdatenaufkommen KANN (und wird dringend empfohlen) anhand eines repräsentativen Systems pro Systemgruppe bestimmt werden.

3.1.6. ##SzA-06: Dokumentation der Planung

Die Ergebnisse der Planungsphase MÜSSEN in einer geeigneten Form dokumentiert werden. Die Dokumentation MUSS alle Netzbereiche, die Protokoll- und Protokollierungsdatenquellen, deren Beziehungen untereinander und den Datenfluss der Protokoll- und Protokollierungsdaten im Anwendungsbereich umfassen. Hierbei ist ein angemessener Abstraktions- und Detailgrad zu wählen, sodass der effektive Einsatz von SzA bewertet werden kann. Um dies zu unterstützen, SOLLTE insbesondere eine Gruppierung gleicher Systemgruppen innerhalb der Dokumentation erfolgen. Gleiche bzw. sehr ähnliche Netze (beispielsweise verschiedene Standorte mit gleichem Netzaufbau) können zusammengefasst werden. Darüber hinaus MUSS für jedes System bzw. für jede Systemgruppe dokumentiert werden, welche Ereignisse dieses bzw. diese protokolliert.

3.1.7. ##SzA-07: Change Prozess

Es MUSS ein Prozess eingerichtet werden, der sicherstellt, dass die Protokollierung bei Veränderungen im Anwendungsbereich (Changes) entsprechend angepasst wird.

Umsetzung der Protokollierung

3.1.8. ##SzA-08: OPS.1.1.5.A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für die Protokollierung erstellt werden. In dieser Sicherheitsrichtlinie MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie die Protokollierung zu planen, aufzubauen und sicher zu betreiben ist. In der spezifischen Sicherheitsrichtlinie MUSS geregelt werden, wie, wo und was zu protokollieren ist. Dabei SOLLTEN sich Art und Umfang der Protokollierung am Schutzbedarf der Informationen orientieren.

Die spezifische Sicherheitsrichtlinie MUSS vom ISB gemeinsam mit den Fachverantwortlichen erstellt werden. Sie MUSS allen für die Protokollierung zuständigen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die spezifische Sicherheitsrichtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit

dem ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist. Die Ergebnisse der Überprüfung MÜSSEN dokumentiert werden.

3.1.9. ##SzA-09: OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene

Alle sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen MÜSSEN protokolliert werden. Sofern die in der Protokollierungsrichtlinie als relevant definierten IT-Systeme und Anwendungen über eine Protokollierungsfunktion verfügen, MUSS diese benutzt werden. Wenn die Protokollierung eingerichtet wird, MÜSSEN dabei die Herstellervorgaben für die jeweiligen IT-Systeme oder Anwendungen beachtet werden.

In angemessenen Intervallen MUSS stichpunktartig überprüft werden, ob die Protokollierung noch korrekt funktioniert.

Die Prüfintervalle MÜSSEN in der Protokollierungsrichtlinie definiert werden.

Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.

3.1.10. ##SzA-10: OPS.1.1.5.A4 Zeitsynchronisation der IT-Systeme

Die Systemzeit aller protokollierenden IT-Systeme und Anwendungen MUSS immer synchron sein. Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist.

3.1.11. ##SzA-11: OPS.1.1.5.A5 Einhaltung rechtlicher Rahmenbedingungen

Bei der Protokollierung MÜSSEN die Bestimmungen aus den aktuellen Gesetzen zum Bundes- sowie Landesdatenschutz eingehalten werden (siehe CON.2 Datenschutz).

Darüber hinaus MÜSSEN eventuelle Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitervertretungen gewahrt werden.

Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden. Protokollierungsdaten MÜSSEN nach einem festgelegten Prozess gelöscht werden. Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.

3.1.12. ##SzA-12: Aufbau einer zentralen Protokollierungsinfrastruktur

Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden. Die Zahl an zentralen Stellen zur Speicherung SOLLTE möglichst geringgehalten werden und sich mindestens an funktionalen Einheiten orientieren, sodass der Zugriff auf die gespeicherten Daten einfach erfolgen kann.

Die Protokollierungsinfrastruktur MUSS dazu ausreichend dimensioniert sein. Dafür MÜSSEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein.

3.1.13. ##SzA-13: Bereitstellung von Protokollierungsdaten für die Auswertung

Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.

Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen.

3.1.14. ##SzA-14: Priorisierung der Protokollierungsdatenquellen

Für die Erzielung einer angemessenen Sichtbarkeit von Angriffen SOLLTEN die Protokollierungsdatenquellen auf Netzebene von außen (Netzgrenzen) nach innen (Netzbereiche) erschlossen werden.

Die Systemebene (kritische Anwendungen und Applikationen) SOLLTE ausgehend von den zentralen, kritischen Systemen, wie z. B. Prozessleit- und Automatisierungstechnik und Leitsystemen, erschlossen werden. Die Priorisierung zur Auswahl der Protokollierungsdatenquellen SOLLTE ausgehend von der Kritikalität der Systeme abgeleitet werden.

3.1.15. ##SzA-15

(gelöscht)

3.1.16. ##SzA-16: Check Umsetzung vs. Planung

Nach erfolgreicher Umsetzung der Protokollierung MUSS geprüft werden, ob alle geplanten Protokollierungsdatenquellen gemäß der Planung umgesetzt wurden.

3.1.17. ##SzA-17: Branchenspezifische Anforderungen

Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen an die Protokollierung bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden.

3.2. Detektion

Planung der Detektion

3.2.1. ##SzA-18: Abdeckung der Bedrohungslandschaft

Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden. Dazu MÜSSEN die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens in der Planung einbezogen werden. Zur Bestimmung der Abdeckung KANN (und es wird empfohlen) eine standardisierte Methode angewendet werden (z. B. MITRE ATT&CK bzw. ATT&CK for ICS 6). In Abhängigkeit der Unternehmensgröße und der Bedrohungslandschaft KANN eine separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung erforderlich sein.

Umsetzung der Detektion

3.2.2. ##SzA-19: DER.1.A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen

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.

3.2.3. ##SzA-20: DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokollierungsdaten

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.

3.2.4. ##SzA-21: DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse

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.

3.2.5. ##SzA-22: DER.1.A4 Sensibilisierung der Mitarbeiter

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.

3.2.6. ##SzA-23: DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion

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.

3.2.7. ##SzA-24: Kontinuierliche Überwachung und Auswertung von Protokoll- und Protokollierungsdaten

Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden. Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist. Die Prüfung des Ereignisses und ggf. die Reaktion MUSS innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgt. Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern benannt werden, die dafür zuständig sind.

Müssen die verantwortlichen Mitarbeitenden aktiv nach sicherheitsrelevanten Ereignissen suchen, z. B. wenn sie IT-Systeme kontrollieren oder testen, MÜSSEN solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein.

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

3.2.8. ##SzA-25: Einsatz zusätzlicher Detektionssysteme

Es MÜSSEN Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden. Anhand des Netzplans MUSS festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen. Auch die im Netzplan definierten Übergänge zwischen internen und externen Netzen MÜSSEN um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.

3.2.9. ##SzA-26: Infrastruktur zur Auswertung von Protokoll- und Protokollierungsdaten und Prüfung sicherheitsrelevanter Ereignisse

Damit die Protokoll- und Protokollierungsdaten korreliert und abgeglichen werden können, SOLLTEN sie alle zeitlich synchronisiert werden. Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden. Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, MÜSSEN die Signaturen der Detektionssysteme immer auf aktuellstem Stand gehalten werden.

3.2.10. ##SzA-27: Auswertung von Informationen aus externen Quellen

Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden. Da Meldungen über unterschiedliche Kanäle in eine Institution gelangen, MUSS sichergestellt sein, dass diese Meldungen von den Mitarbeitenden auch als relevant erkannt und an die richtige Stelle weitergeleitet werden. Informationen aus zuverlässigen Quellen MÜSSEN grundsätzlich ausgewertet werden. Alle gelieferten Informationen MÜSSEN danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind. Ist dies der Fall, MÜSSEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.

3.2.11. ##SzA-28: Auswertung der Protokoll- und Protokollierungsdaten durch spezialisiertes Personal

Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten auszuwerten. Die Auswertung der Protokoll- und Protokollierungsdaten SOLLTE bei diesen höher priorisiert sein, als ihre übrigen Aufgaben. Daher empfiehlt es sich, dass dies ihre überwiegende Aufgabe ist. Dieses Personal SOLLTE spezialisierte weiterführende Schulungen und Qualifikationen erhalten. Ein Personenkreis MUSS benannt werden, der für das Thema Auswertung von Protokoll- und Protokollierungsdaten verantwortlich ist

3.2.12. ##SzA-29: Zentrale Detektion und Echtzeitüberprüfungen von Ereignismeldungen

Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. Zentrale automatisierte Analysen mit Softwaremitteln MÜSSEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen. Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein. Die Daten MÜSSEN kontinuierlich ausgewertet werden.

Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden. Das zuständige Personal MUSS sicherstellen, dass bei einem Alarm nach fachlicher Bewertung und innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist. Zusätzlich MÜSSEN bereits überprüfte

Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.

3.2.13. ##SzA-30: Stand der Technik

Als eine zentrale Grundvoraussetzung für die effektive Detektion MÜSSEN zudem Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden. Dazu MÜSSEN fortlaufend Meldungen der Hersteller (Hard- und Software), von Behörden, den Medien und weiterer relevanter Stellen geprüft werden und in dokumentierte Prozesse des Schwachstellenmanagements einfließen.

3.2.14. ##SzA-31: Kalibrierung

Bei der Umsetzung von Detektionsmechanismen SOLLTE initial eine Kalibrierung durchgeführt werden, um festzustellen, welche sicherheitsrelevanten Ereignisse (SRE) im Normalzustand auftreten (Baselining). Dazu SOLLTE bewertet werden, ob dieser Normalzustand in Hinblick auf die Zahl der falsch positiven Meldungen hingenommen werden kann oder ob Änderungen vorzunehmen sind. Die Kalibrierung SOLLTE bei Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage erneut durchgeführt werden.

3.2.15. ##SzA-32: Bewertung

Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten. Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen. Nur qualifizierte SRE SOLLTEN den Prozess der Reaktion auslösen. Die Qualifizierung SOLLTE in automatisiert nicht eindeutig zuordenbaren Fällen manuell durch festgelegte Verantwortliche vorgenommen werden. Basierend auf den gewonnenen Erkenntnissen der Qualifizierung MÜSSEN die Detektionsmechanismen nachjustiert werden.

3.2.16. ##SzA-33: Branchenspezifische Anforderungen

Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden.

3.3. Reaktion

3.3.1. ##SzA-34: DER.2.1.A1 Definition eines Sicherheitsvorfalls

In einer Institution MUSS klar definiert sein, was ein Sicherheitsvorfall ist. Ein Sicherheitsvorfall MUSS so weit wie möglich von Störungen im Tagesbetrieb abgegrenzt sein. Alle an der Behandlung von Sicherheitsvorfällen beteiligten Mitarbeiter MÜSSEN die Definition eines Sicherheitsvorfalls kennen. Die Definition und die Eintrittsschwellen eines solchen Vorfalls SOLLTEN sich nach dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Systeme bzw. Anwendungen richten.

3.3.2. ##SzA-35: DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen

Eine Richtlinie zur Behandlung von Sicherheitsvorfällen MUSS erstellt werden. Darin MÜSSEN Zweck und Ziel der Richtlinie definiert sowie alle Aspekte der Behandlung von Sicherheitsvorfällen geregelt werden. So MÜSSEN Verhaltensregeln für die verschiedenen Arten von Sicherheitsvorfällen beschrieben sein. Zusätzlich MUSS es für alle Mitarbeiter zielgruppenorientierte und praktisch anwendbare Handlungsanweisungen geben. Weiterhin SOLLTEN die Schnittstellen zu anderen Managementbereichen berücksichtigt werden, z. B. zum Notfallmanagement.

Die Richtlinie MUSS allen Mitarbeitern bekannt sein. Sie MUSS mit dem IT-Betrieb abgestimmt und durch die Institutionsleitung verabschiedet sein. Die Richtlinie MUSS regelmäßig geprüft und aktualisiert werden.

3.3.3. ##SzA-36: DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen

Es MUSS geregelt werden, wer bei Sicherheitsvorfällen wofür verantwortlich ist. Für alle Mitarbeiter MÜSSEN die Aufgaben und Kompetenzen bei Sicherheitsvorfällen festgelegt werden. Insbesondere Mitarbeiter, die Sicherheitsvorfälle bearbeiten sollen, MÜSSEN über ihre Aufgaben und Kompetenzen unterrichtet werden. Dabei MUSS auch geregelt sein, wer die mögliche Entscheidung für eine forensische Untersuchung trifft, nach welchen Kriterien diese vorgenommen wird und wann sie erfolgen soll.

Die Ansprechpartner für alle Arten von Sicherheitsvorfällen MÜSSEN den Mitarbeitern bekannt sein. Kontaktinformationen MÜSSEN immer aktuell und leicht zugänglich sein.

3.3.4. ##SzA-37: DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen

Von einem Sicherheitsvorfall MÜSSEN alle betroffenen internen und externen Stellen zeitnah informiert werden.

Dabei MUSS geprüft werden, ob der Datenschutzbeauftragte, der Betriebs- und Personalrat sowie Mitarbeiter aus der Rechtsabteilung einbezogen werden müssen. Ebenso MÜSSEN die Meldepflichten für Behörden und regulierte Branchen berücksichtigt werden. Außerdem MUSS gewährleistet sein, dass betroffene Stellen über die erforderlichen Maßnahmen informiert werden.

3.3.5. ##SzA-38: DER.2.1.A5 Behebung von Sicherheitsvorfällen

Damit ein Sicherheitsvorfall erfolgreich behoben werden kann, MUSS der Zuständige zunächst das Problem eingrenzen und die Ursache finden. Danach MUSS er die erforderlichen Maßnahmen auswählen, um das Problem zu beheben. Der Leiter des IT-Betriebs MUSS seine Freigabe erteilen, bevor die Maßnahmen umgesetzt werden. Anschließend MUSS die Ursache beseitigt und ein sicherer Zustand hergestellt werden.

Eine aktuelle Liste von internen und externen Sicherheitsexperten MUSS vorhanden sein, die bei Sicherheitsvorfällen für Fragen aus den erforderlichen Themenbereichen

hinzugezogen werden können. Es MÜSSEN sichere Kommunikationsverfahren mit diesen internen und externen Stellen etabliert werden.

3.3.6. ##SzA-39: DER.2.1.A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen

Nach einem Sicherheitsvorfall MÜSSEN die betroffenen Komponenten vom Netz genommen werden. Zudem MÜSSEN alle erforderlichen Daten gesichert werden, die Aufschluss über die Art und Ursache des Problems geben könnten.

Auf allen betroffenen Komponenten MÜSSEN das Betriebssystem und alle Applikationen auf Veränderungen untersucht werden.

Die Originaldaten MÜSSEN von schreibgeschützten Datenträgern wieder eingespielt werden. Dabei MÜSSEN alle sicherheitsrelevanten Konfigurationen und Patches mit aufgespielt werden. Wenn Daten aus Datensicherungen wieder eingespielt werden, MUSS sichergestellt sein, dass diese vom Sicherheitsvorfall nicht betroffen waren. Nach einem Angriff MÜSSEN alle Zugangsdaten auf den betroffenen Komponenten geändert werden, bevor sie wieder in Betrieb genommen werden. Die betroffenen Komponenten SOLLTEN einem Penetrationstest unterzogen werden, bevor sie wieder eingesetzt werden.

Bei der Wiederherstellung der sicheren Betriebsumgebung MÜSSEN die Benutzer in die Anwendungsfunktionstests einbezogen werden. Nachdem alles wiederhergestellt wurde, MÜSSEN die Komponenten inklusive der Netzübergänge gezielt überwacht werden.

3.3.7. ##SzA-40: DER.2.1.A7 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen

Es SOLLTE eine geeignete Vorgehensweise zur Behandlung von Sicherheitsvorfällen definiert werden. Die Abläufe, Prozesse und Vorgaben für die verschiedenen Sicherheitsvorfälle SOLLTEN dabei eindeutig geregelt und geeignet dokumentiert werden. Die Institutionsleitung SOLLTE die festgelegte Vorgehensweise in Kraft setzen und allen Beteiligten zugänglich machen. Es SOLLTE regelmäßig überprüft werden, ob die Vorgehensweise noch aktuell und wirksam ist. Bei Bedarf SOLLTE die Vorgehensweise angepasst werden.

3.3.8. ##SzA-41: DER.2.1.A8 Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen

Für den Umgang mit Sicherheitsvorfällen SOLLTEN geeignete Organisationsstrukturen festgelegt werden. Es SOLLTE ein Sicherheitsvorfall-Team aufgebaut werden, dessen Mitglieder je nach Art des Vorfalls einberufen werden können. Auch wenn das Sicherheitsvorfall-Team nur für einen konkreten Fall zusammentritt, SOLLTEN bereits im Vorfeld geeignete Mitglieder benannt und in ihre Aufgaben eingewiesen sein. Es SOLLTE regelmäßig geprüft werden, ob die Zusammensetzung des Sicherheitsvorfall-Teams noch angemessen ist. Gegebenenfalls SOLLTE das Sicherheitsvorfall-Team neu zusammengestellt werden.

3.3.9. ##SzA-42: DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle

Für die verschiedenen Arten von Sicherheitsvorfällen SOLLTEN die jeweils passenden Meldewege aufgebaut sein.

Es SOLLTE dabei sichergestellt sein, dass Mitarbeiter Sicherheitsvorfälle über verlässliche und vertrauenswürdige Kanäle schnell und einfach melden können.

Wird eine zentrale Anlaufstelle für die Meldung von Störungen oder Sicherheitsvorfällen eingerichtet, SOLLTE dies an alle Mitarbeiter kommuniziert werden.

Eine Kommunikations- und Kontaktstrategie SOLLTE vorliegen. Darin SOLLTE geregelt sein, wer grundsätzlich informiert werden muss und wer informiert werden darf, durch wen dies in welcher Reihenfolge erfolgt und in welcher Tiefe informiert wird. Es SOLLTE definiert sein, wer Informationen über Sicherheitsvorfälle an Dritte weitergibt.

Ebenso SOLLTE sichergestellt sein, dass keine unautorisierten Personen Informationen über den Sicherheitsvorfall weitergeben.

3.3.10. ##SzA-43: DER.2.1.A10 Eindämmen der Auswirkung von Sicherheitsvorfällen

Parallel zur Ursachenanalyse eines Sicherheitsvorfalls SOLLTE entschieden werden, ob es wichtiger ist, den entstandenen Schaden einzudämmen oder den Vorfall aufzuklären. Um die Auswirkung eines Sicherheitsvorfalls abschätzen zu können, SOLLTEN ausreichend Informationen vorliegen. Für ausgewählte Sicherheitsvorfallsszenarien SOLLTEN bereits im Vorfeld Worst-Case-Betrachtungen durchgeführt werden.

3.3.11. ##SzA-44: DER.2.1.A11 Einstufung von Sicherheitsvorfällen

Ein einheitliches Verfahren SOLLTE festgelegt werden, um Sicherheitsvorfälle und Störungen einzustufen. Das Einstufungsverfahren für Sicherheitsvorfälle SOLLTE zwischen Sicherheitsmanagement und der Störungs- und Fehlerbehebung (Incident Management) abgestimmt sein.

3.3.12. ##SzA-45: DER.2.1.A12 Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung

Die Schnittstellen zwischen Störungs- und Fehlerbehebung, Notfallmanagement und Sicherheitsmanagement SOLLTEN analysiert werden. Dabei SOLLTEN auch eventuell gemeinsam benutzbare Ressourcen identifiziert werden.

Die bei der Störungs- und Fehlerbehebung beteiligten Mitarbeiter SOLLTEN für die Behandlung von Sicherheitsvorfällen sowie für das Notfallmanagement sensibilisiert werden. Das Sicherheitsmanagement SOLLTE lesenden Zugriff auf eingesetzte Incident-Management-Werkzeuge haben.

3.3.13. ##SzA-46: DER.2.1.A13 Einbindung in das Sicherheits- und Notfallmanagement

Die Behandlung von Sicherheitsvorfällen SOLLTE mit dem Notfallmanagement abgestimmt sein. Falls es in der Institution eine spezielle Rolle für Störungs- und Fehlerbehebung gibt, SOLLTE auch diese mit einbezogen werden.

3.3.14. ##SzA-47: DER.2.1.A14 Eskalationsstrategie für Sicherheitsvorfälle

Über die Kommunikations- und Kontaktstrategie hinaus SOLLTE eine Eskalationsstrategie formuliert werden. Diese SOLLTE zwischen den Verantwortlichen für Störungs- und Fehlerbehebung und dem Informationssicherheitsmanagement abgestimmt werden.

Die Eskalationsstrategie SOLLTE eindeutige Handlungsanweisungen enthalten, wer auf welchem Weg bei welcher Art von erkennbaren oder vermuteten Sicherheitsstörungen wann einzubeziehen ist. Es SOLLTE geregelt sein, zu welchen Maßnahmen eine Eskalation führt und wie reagiert werden soll.

Für die festgelegte Eskalationsstrategie SOLLTEN geeignete Werkzeuge wie z. B. Ticket-Systeme ausgewählt werden.

Diese SOLLTEN sich auch dafür eignen, vertrauliche Informationen zu verarbeiten. Es SOLLTE sichergestellt sein, dass die Werkzeuge auch während eines Sicherheitsvorfalls bzw. Notfalls verfügbar sind.

Die Eskalationsstrategie SOLLTE regelmäßig überprüft und gegebenenfalls aktualisiert werden. Die Checklisten (Matching Szenarios) für Störungs- und Fehlerbehebung SOLLTEN regelmäßig um sicherheitsrelevante Themen ergänzt bzw. aktualisiert werden. Die festgelegten Eskalationswege SOLLTEN in Übungen erprobt werden.

3.3.15. ##SzA-48: DER.2.1.A15 Schulung der Mitarbeiter des Service Desk

Den Mitarbeitern des Service Desk SOLLTEN geeignete Hilfsmittel zur Verfügung stehen, damit sie Sicherheitsvorfälle erkennen können. Sie SOLLTEN ausreichend geschult sein, um die Hilfsmittel selbst anwenden zu können. Die Mitarbeiter des Service Desk SOLLTEN den Schutzbedarf der betroffenen IT-Systeme kennen.

3.3.16. ##SzA-49: DER.2.1.A16 Dokumentation der Behebung von Sicherheitsvorfällen

Die Behebung von Sicherheitsvorfällen SOLLTE nach einem standardisierten Verfahren dokumentiert werden. Es SOLLTEN alle durchgeführten Aktionen inklusive der Zeitpunkte sowie die Protokolldaten der betroffenen Komponenten dokumentiert werden. Dabei SOLLTE die Vertraulichkeit bei der Dokumentation und Archivierung der Berichte gewährleistet sein.

Die benötigten Informationen SOLLTEN in die jeweiligen Dokumentationssysteme eingepflegt werden, bevor die Störung als beendet und als abgeschlossen markiert wird. Im Vorfeld SOLLTEN mit dem ISB die dafür erforderlichen Anforderungen an die Qualitätssicherung definiert werden.

3.3.17. ##SzA-50: DER.2.1.A17 Nachbereitung von Sicherheitsvorfällen

Sicherheitsvorfälle SOLLTEN standardisiert nachbereitet werden. Dabei SOLLTE untersucht werden, wie schnell die Sicherheitsvorfälle erkannt und behoben wurden. Weiterhin SOLLTE untersucht werden, ob die Meldewege funktionierten, ausreichend Informationen für die Bewertung verfügbar und ob die Detektionsmaßnahmen wirksam waren.

Ebenso SOLLTE geprüft werden, ob die ergriffenen Maßnahmen und Aktivitäten wirksam und effizient waren.

Die Erfahrungen aus vergangenen Sicherheitsvorfällen SOLLTEN genutzt werden, um daraus Handlungsanweisungen für vergleichbare Sicherheitsvorfälle zu erstellen. Diese Handlungsanweisungen SOLLTEN den relevanten Personengruppen bekanntgegeben und auf Basis neuer Erkenntnisse regelmäßig aktualisiert werden.

Die Institutionsleitung SOLLTE jährlich über die Sicherheitsvorfälle unterrichtet werden. Besteht sofortiger Handlungsbedarf, MUSS die Institutionsleitung umgehend informiert werden.

3.3.18. ##SzA-51: DER.2.1.A18 Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen

Nachdem ein Sicherheitsvorfall analysiert wurde, SOLLTE untersucht werden, ob die Prozesse und Abläufe im Rahmen der Behandlung von Sicherheitsvorfällen geändert oder weiterentwickelt werden müssen. Dabei SOLLTEN alle Personen, die an dem Vorfall beteiligt waren, über ihre jeweiligen Erfahrungen berichten.

Es SOLLTE geprüft werden, ob es neue Entwicklungen im Bereich Incident Management und in der Forensik gibt und ob diese in die jeweiligen Dokumente und Abläufe eingebracht werden können.

Werden Hilfsmittel und Checklisten eingesetzt, z. B. für Service-Desk-Mitarbeiter, SOLLTE geprüft werden, ob diese um relevante Fragen und Informationen zu erweitern sind.

3.3.19. ##SzA-52: Automatische Reaktion auf sicherheitsrelevante Ereignisse

Bei einem sicherheitsrelevanten Ereignis MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren. In Netzen, wo die kritische Dienstleistung durch die Umsetzung nicht gefährdet wird, MUSS es möglich sein, automatisch in den Datenstrom einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden. Sollte eine automatische Reaktion nicht möglich sein, MUSS über manuelle Prozesse sichergestellt werden, dass der mögliche Sicherheitsvorfall unterbunden wird.

Der Ausschluss von Netzen oder Netzsegmenten von einer automatischen Reaktion, bzw. dem Eingriff in den Datenstrom MUSS schlüssig begründet sein.

3.3.20. ##SzA-53: Behandlung

Festgestellte Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen MÜSSEN behandelt werden.

3.3.21. ##SzA-54: Meldepflichten

Bei Störungen und Sicherheitsvorfällen insbesondere im vermeintlichen Zusammenhang mit Angriffen MUSS überprüft werden, ob diese den Kriterien der Meldepflicht nach § 8b Absatz 3 BSIG bzw. §11 Absatz 1c EnWG entsprechen und eine Meldung an das BSI notwendig ist.

3.3.22. ##SzA-55: Automatisierte Maßnahmen

Die zur Angriffserkennung eingesetzten Systeme SOLLTEN automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen ergreifen können, sofern das zu Grunde liegende SRE eindeutig qualifizierbar ist. Dabei MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.

3.3.23. ##SzA-56: Manuelle Maßnahmen

Die eingesetzten SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.

4. Vorgehensweise zur Prüfung und Nachweisführung

Die Prüfung wird in Form eines Audits sowie einer technischen Prüfung durchgeführt. Die Prüfung spaltet sich auf in

- Vorbereitung
- Dokumentenprüfung
- Site Visit
- Nachbereitung inkl. BSI-Nachweis

4.1. Vorbereitung

Im Rahmen der Vorbereitung stellen Sie dem Prüfteam die benötigten Referenzdokumente zur Verfügung – dies umfasst

- eine Darstellung des Geltungsbereiches mit Detailinformationen zu Netzstruktur und IT-Systemen, insb. Netzstrukturplan
- die Umsetzungsdokumentation zu allen Anforderungselementen des Kriterienkatalogs
- alle relevanten Richtlinien und Prozessbeschreibungen

4.2. Dokumentenprüfung

Die Dokumentenprüfung besteht aus einer Sichtung der Referenzdokumente.

Ziel ist es, den Geltungsbereich und den Umfang der IT-Infrastruktur kennenzulernen und Ihre Umsetzung der normativen Vorgaben einzuschätzen. Dazu werden stichpunktartig Aspekte des Kriterienkatalogs geprüft.

4.3. Site Visit

Das Ziel des Site Visits ist es, die Umsetzung einschließlich der Wirksamkeit Ihrer Systeme zur Angriffserkennung hinsichtlich der Vorgaben zu beurteilen.

Dazu prüft das Prüfteam zu jedem Anforderungselement des Kriterienkatalogs

- Ihre Umsetzungsbeschreibung sowie
- die Wirksamkeit der beschriebenen Maßnahmen in der Realität,

und dokumentiert die Ergebnisse der Prüfung in einem Report.

Im Ergebnis sieht die Orientierungshilfe [OH-SzA] eine Bewertung nach folgendem Reifegradmodell vor:

0. Es sind bisher keine Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Anforderungen.
1. Es bestehen Planungen zur Umsetzung von Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen.
2. In allen Bereichen wurde mit der Umsetzung von Anforderungen begonnen. Es sind noch nicht alle MUSS-Anforderungen umgesetzt worden.

3. Alle MUSS-Anforderungen wurden für alle Bereiche umgesetzt. Idealerweise wurden SOLLTE-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
4. Alle MUSS-Anforderungen wurden für alle Bereiche umgesetzt. Alle SOLLTE-Anforderungen wurden umgesetzt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
5. Alle MUSS-Anforderungen wurden für alle Bereiche umgesetzt. Alle SOLLTE-Anforderungen und KANN-Anforderungen wurden für alle Bereiche umgesetzt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse / Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

Im Ergebnis ist lt. [OH-SzA] der folgende Erreichungsgrad vorgesehen:

- Grundsätzlich sollte ein **Umsetzungsgrad der Stufe 4** erreicht werden, um die Anforderungen nach § 8a Absatz 1a BSIG bzw. § 11 Absatz 1e EnWG zu erfüllen. Abweichungen nach unten sind nur unter der Angabe von Gründen zulässig.
- In Anerkennung der Tatsache, dass die Einführung von Systemen zur Angriffserkennung ein längerfristig angelegter Prozess ist, wird im **ersten Nachweiszyklus ein Umsetzungsgrad der Stufe 3 zur Erfüllung** der Anforderungen nach § 8a Absatz 1a BSIG bzw. § 11 Absatz 1e EnWG durch das BSI als ausreichend akzeptiert, wobei Abweichungen nach unten begründet werden müssen und nur im Ausnahmefall vertretbar sind.

4.4. Nachbereitung

Das Ergebnis der Prüfung wird dokumentiert.

Zudem erhalten Sie den geforderten BSI-Nachweis, den Sie dann beim BSI einreichen.

4.5. Kontinuität und Laufzeit

Informationssicherheit nach Stand der Technik setzt insbesondere ein Informationssicherheits-Managementsystem (ISMS) voraus.

Aus diesem Grund setzt das Modell der datenschutz cert GmbH zur Prüfung von Systemen zur Angriffserkennung auf kontinuierliche Prüfungen:

- es finden jährliche Prüfungen statt
- BSI-Nachweise werden gem. gesetzlichen Vorgaben erstellt: initial und sodann alle zwei Jahre

Hintergrund ist, dass die zweijährigen BSI-Nachweise eine Bewertung der Systeme nach Stand der Technik über die vergangenen zwei Jahre umfasst.

4.6. Zertifizierungen gem. IT-Sicherheitskatalog

Netz- und Kraftwerksbetreiber müssen sich zertifizieren lassen:

- Strom- und Gasnetzbetreiber gem. IT-Sicherheitskatalog gem. §11 Abs. 1a EnWG

- Energieanlagenbetreiber gem. IT-Sicherheitskatalog gem. §11 Abs. 1b EnWG, sofern sie unter die KRITIS-VO fallen

Diese Zertifizierungen setzen ein Informationssicherheits-Managementsystem (ISMS) gem. ISO/IEC 27001 voraus, weshalb Synergien zu den Anforderungen des vorliegenden Kriterienkatalogs vorliegen. Aus diesem Grund strebt die datenschutz cert GmbH an, Audits gem. IT-Sicherheitskatalog mit Prüfungen gem. SzA zu kombinieren.

5. datenschutz cert GmbH

5.1. Was wir tun

Die datenschutz cert GmbH bietet Konformitätsbewertungen auf dem Gebiet des Datenschutzes und der Informationssicherheit an. Diese Konformitätsbewertungen schließen sowohl Prüfaktivitäten als auch Zertifizierungstätigkeiten ein – einerseits für IT-Systeme und -Produkte und andererseits für Verfahren und Managementprozesse.

Die datenschutz cert GmbH ist ein Unternehmen der DSN GROUP. Sitz der Gesellschaft ist Bremen. Geschäftsführer ist Dr. Sönke Maseberg. Die Unternehmen der DSN GROUP sind inhabergeführt.

5.2. Unsere Anerkennungen und Akkreditierungen

Die datenschutz cert GmbH ist eine bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) gemäß ISO/IEC 27006 akkreditierte Zertifizierungsstelle und darf danach international gültige Zertifikate für ISO/IEC 27001-konforme Informationssicherheits-Managementsysteme (ISMS) erteilen. Die Akkreditierung der DAkkS umfasst auch das Regelwerk „IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG“.

Die datenschutz cert GmbH ist als Prüfstelle für IT-Sicherheit und IT-Sicherheitsdienstleister beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt.

Aufgrund der Akkreditierung bei der DAkkS und der Anerkennung beim BSI darf die datenschutz cert GmbH im Kontext von §8a-Verfahren die Rolle der „prüfenden Stelle“ einnehmen. Ferner sind die Auditoren der datenschutz cert GmbH beim BSI als Prüfer für § 8a BSIG anerkannt.

Ferner ist die datenschutz cert GmbH bei der DAkkS für Produkte und Dienstleistungen gemäß ISO/IEC 17065 akkreditiert und darf danach als Konformitätsbewertungsstelle Vertrauensdienste gemäß eIDAS prüfen und bewerten.

Auditoren der datenschutz cert GmbH sind beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Auditoren für die TR-03109-6 (Smart Meter Gateway Administratoren) sowie BSI TR-03145 (Secure CA Operation) zertifiziert.

Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschutz-Auditoren und IS-Revisoren. Die datenschutz cert GmbH stellt eines der beiden GS-Zertlabs, die für das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Prüfbegleitung in den IT-Grundschutz-Verfahren durchführen.

Die datenschutz cert GmbH ist eine bei der Bundesnetzagentur anerkannte Zertifizierungsstelle nach eIDAS gem. Vertrauensdienstegesetz (VDG) sowie Konformitätsbewertungsstelle nach eIDAS.

6. Referenzen

[OH-SzA] Bundesamt für Sicherheit in der Informationstechnik, „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“, Version 1.0, 26.09.2022.

datenschutz cert

datenschutz cert GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88a
28217 Bremen
Tel.: +49 421 69 66 32-550

Standort Offenbach
Mainstraße 143
63065 Offenbach am Main
Tel.: +49 69 870 07 83-580

office@datenschutz-cert.de
www.datenschutz-cert.de