Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

Version 1.0

Vom 26.09.2022

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6166
E-Mail: kritische.infrastrukturen@bsi.bund.de
Internet: www.bsi.bund.de

Inhalt

1 Überblick

Die Betreiber Kritischer Infrastrukturen sowie Betreiber von Energieversorgungsnetzen sind in Deutschland dazu verpflichtet, Angriffserkennung zu leisten, um ihre Informationssysteme zu schützen. Nach einer Neuerung im BSIG und im EnWG müssen Systeme zur Angriffserkennung (SzA) Bestandteil der Nachweise gegenüber dem BSI sein. Das vorliegende Dokument bietet eine Orientierung für Betreiber Kritischer Infrastrukturen sowie prüfenden Stellen zu SzA und den Anforderungen bei deren Umsetzung. Ein Umsetzungsgradmodell zur Bewertung der ergriffenen Maßnahmen und die Nachweiserbringung gegenüber dem BSI werden ebenfalls vorgestellt. Das Dokument eignet sich zudem als Grundlage für die Fortentwicklung der Branchenspezifischen Sicherheitsstandards (B3S) im Zuge der Integration der SzA.

Zielsetzung und Adressatenkreis der Orientierungshilfe

Betreiber Kritischer Infrastrukturen haben die Verpflichtung, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Das BSIG benennt nach Umsetzung des 2. IT-Sicherheitsgesetzes im neuen § 8a Absatz 1a BSIG nun auch ausdrücklich den Einsatz von Systemen zur Angriffserkennung (SzA). Derartige Systeme stellen eine effektive Maßnahme zur (frühzeitigen) Erkennung von Cyber-Angriffen dar und unterstützen insbesondere die Schadensreduktion und Schadensvermeidung.

Ziel der vorliegenden Orientierungshilfe SzA ist es, den Betreibern Kritischer Infrastrukturen sowie den prüfenden Stellen einen Anhaltspunkt für die individuelle Umsetzung und Prüfung der Vorkehrungen zu geben.

Zusätzlich soll eine einheitliche Nachweiserbringung gewährleistet werden, indem eine systematische Bewertung der getroffenen Maßnahmen unter Verwendung eines Umsetzungsgradmodells eingeführt wird. Als Bewertungsgrundlage werden die jeweiligen Anforderungen an SzA bzw. deren Umsetzungsgrad verwendet.

Die von Betreibern gemäß § 8a Absatz 1a BSIG bzw. § 11 Absatz 1e EnWG geforderten Sicherheitsvorkehrungen lassen in ihrer konkreten Umsetzung Freiheiten zu, so stellt diese Orientierungshilfe keine verbindliche Vorgabe dar. Vielmehr gibt sie, wie auch die Orientierungshilfe zu Branchenspezifischen Sicherheitsstandards, einen qualitativen Rahmen, innerhalb dessen gleichwertige und individuelle Alternativen, unter Berücksichtigung ihrer Angemessenheit, möglich sind.

Die Formulierungen in der Orientierungshilfe und dem Umsetzungsgradmodell sind an den IT-Grundschutz angelehnt, da dieser die durch das BSI verwendete Beschreibung des Stands der Technik ist. Zusätzlich eignet sich der IT-Grundschutz gerade bei Neueinführung von Schutzmaßnahmen besonders, da durch die Bausteine konkrete Anforderungen an die Informationssicherheit gegeben werden. Sollten bereits Systeme zur Angriffserkennung eingeführt worden sein oder werden andere Standards verwendet, so können diese weiterhin genutzt werden, so lange sie ein mit der Orientierungshilfe vergleichbares Sicherheitsniveau bieten.

Die Orientierungshilfe beschreibt die Vorstellung des BSI, welche Anforderungen Betreiber Kritischer Infrastrukturen und Betreiber von Energieversorgungsnetzen für SzA erfüllen sollen. Dabei wird davon ausgegangen, dass unabhängig von der Art und Ausrichtung einer Institution überall versorgungsrelevante Informationen sicher verarbeitet werden müssen, gängige IT-Systeme eingesetzt werden und ähnliche Umfelder existieren. Damit liegen meistens ebenso vergleichbare Bedrohungen vor. Die Anforderungen der Geschäftsprozesse und Fachanwendungen sind zwar individuell und können unterschiedlich sein, in der Praxis führen sie jedoch meist zu ähnlichen Anforderungen an die einzusetzenden Systeme zur Angriffserkennung.

Aufbau der Orientierungshilfe

Nach diesem einleitenden Abschnitt gibt Kapitel 2 eine Einführung in die Grundlagen zum Thema „Systeme zur Angriffserkennung“. Dazu wird zunächst der gesetzliche Hintergrund erläutert, darauf aufbauend die Systeme zur Angriffserkennung definiert und diese anschließend im Hinblick auf ihren branchenspezifischen Einsatz eingeordnet.

Kapitel 3 beschreibt Anforderungen an Systeme zur Angriffserkennung, welche auch in der späteren Bewertung durch das Umsetzungsgradmodell berücksichtigt werden.

In Kapitel 4 erfolgt die Vorstellung des Umsetzungsgradmodells zur Bewertung von Systemen zur Angriffserkennung. Abschließend wird die Anwendung des Umsetzungsgradmodells im Zuge der Nachweiserbringung behandelt.

Weiterführende Informationen

Weitere Orientierung zum Thema Angriffserkennung bietet der IT-Grundschutz des BSI, dort unter anderem die Bausteine (www.bsi.bund.de/dok/531534)

- OPS.1.1.4 Schutz vor Schadprogrammen,
- OPS.1.1.5 Protokollierung
- NET.1.2 Netzmanagement
- NET.3.2 Firewall
- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.2.1: Behandlung von Sicherheitsvorfällen

Der Mindeststandard zur Protokollierung und Detektion von Cyber-Angriffen macht verbindliche Vorgaben für die Bundesverwaltung. (www.bsi.bund.de/dok/886714)

In der ISO/IEC 2700x-Reihe und der Norm IEC 62443 werden ebenfalls Anforderungen an Detektion und Reaktion formuliert.

Auch der „The Standard of Good Practice for Information Security“ des Information Security Forum (ISF) sowie die Special Publication 800-61 Revision 2 und 800-83 Revision 1 des National Institute of Standards and Technology (NIST) enthalten Empfehlungen zu Detektion und Reaktion.

Diese Orientierungshilfe gibt keinen allgemeinen Überblick über das IT-Sicherheitsgesetz bzw. die Rechte und Pflichten der Betreiber Kritischer Infrastrukturen.

Die hier aufgeführten Informationen zur weiteren Lektüre erheben keinen Anspruch auf Vollständigkeit.

2 Grundlagen

In diesem Kapitel wird der gesetzliche Hintergrund für Systeme zur Angriffserkennung im Kontext Kritischer Infrastrukturen und Energieversorgungsnetze erläutert. Neben einer Begriffsbestimmung werden Hinweise zur branchenspezifischen Konkretisierung der Orientierungshilfe gegeben.

Gesetzlicher Hintergrund

Am 28. Mai 2021 sind mit dem zweiten IT-Sicherheitsgesetz zahlreiche Änderungen im BSIG in Kraft getreten. Der Begriff „Systeme zur Angriffserkennung“ wurde in § 8a Absatz 1a BSIG mit der Pflicht zum ordnungsgemäßen Einsatz dieser in das Gesetz eingefügt, sowie in § 2 Absatz 9b Satz 1 BSIG legal definiert und in Satz 2 technisch weiter erläutert (siehe z. B. www.gesetze-im-internet.de/bsig_2009/):

> *„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“*
> (§ 2 Absatz 9b BSIG)

Gemäß § 8a Absatz 1a BSIG sind Betreiber Kritischer Infrastrukturen *ab dem 1. Mai 2023 verpflichtet,* solche Systeme zur Angriffserkennung als Teil der angemessenen Vorkehrungen nach Absatz 1 einzusetzen, um Störungen der von ihnen betriebenen Kritischen Infrastruktur zu vermeiden. Dabei soll der Stand der Technik eingehalten und der ordnungsgemäße Einsatz der Angriffserkennungssysteme mit dem Nachweis nach § 8a Absatz 3 BSIG ebenfalls nachgewiesen werden.

> *„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“*
> (§ 8a Absatz 1a Satz 1, 2 BSIG, Unterstreichungen für diese OH vorgenommen).

> *„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“*
> (§ 8a Absatz 3 Satz 1 BSIG, Unterstreichungen für diese OH vorgenommen).

Für Betreiber von Energieversorgungsnetzen und Energieanlagen, die nach § 8d BSIG von der KRITIS-Regulierung gemäß BSIG ausgenommen sind, gelten die Neuerungen für „Systeme zur Angriffserkennung“ parallel gemäß § 11 Absatz 1e und 1f EnWG. Der Nachweis des ordnungsgemäßen Einsatzes der Systeme zur Angriffserkennung ist ebenfalls gegenüber dem BSI vorzulegen. Dies umfasst ebenfalls die Übermittlung der Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen der Systeme zur Angriffserkennung einschließlich der dabei aufgedeckten Sicherheitsmängel.

Systeme zur Angriffserkennung und ihr branchenspezifischer Einsatz

Systeme zur Angriffserkennung sind nach der Definition aus § 2 Absatz 9b Satz 1 BSIG Prozesse, die *durch technische Werkzeuge und organisatorische Einbindung unterstützt* werden. Dies bedeutet, dass die Systeme explizit neben technischen Maßnahmen auch organisatorische Maßnahmen erfordern und diese deshalb bei Planung der Ressourcenverteilung ausreichend berücksichtigt werden müssen.

In § 8a Absatz 1a BSIG werden Systeme zur Angriffserkennung in Bezug auf ihre Funktionalität weiter konkretisiert. Sie „müssen *geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten*“ können. Die Auswertung wird in § 2 Absatz 9b BSIG als *„Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten“* spezifiziert. Zusätzlich sollten die Systeme *„dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen“* (§ 8a Absatz 1a Satz 3 BSIG). Während § 2 Absatz 9b Satz 2 und § 8a Absatz 1a Satz 2 BSIG also vor allem die technische Unterstützung weiter erläutern, geht damit § 8a Absatz 1a Satz 3 BSIG auch auf die Funktion der organisatorischen Unterstützung weiter ein.

Daraus ergeben sich für Systeme zur Angriffserkennung im Hinblick auf deren Funktionalität die wesentlichen Aufgabenbereiche der Protokollierung, Detektion und Reaktion.

- 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.

Im Sinne einer branchenübergreifenden Orientierungshilfe wird darauf verzichtet, die konkreten, branchenspezifischen Einsatzbereiche zu betrachten. Stattdessen sollen auf Grundlage der in Kapitel 3 genannten Anforderungen branchenspezifische Sicherheitsstandards unter Berücksichtigung der jeweils branchenüblichen Technik erarbeitet werden. Die beim BSI zur Eignungsfeststellung eingereichten Branchenspezifischen Sicherheitsstandards (B3S) nach § 8a Absatz 2 BSIG müssen deshalb zukünftig Vorgaben für Systeme zur Angriffserkennung abdecken.

3 Anforderungen

Die technische Funktionalität eines Systems zur Angriffserkennung basiert im Wesentlichen auf Abläufen, die sich den Bereichen

- Protokollierung,
- Detektion und
- Reaktion

zuordnen lassen. Um eine effektive Erkennung von Angriffen gewährleisten zu können, sind an die genannten Bereiche Anforderungen zu stellen, die Sie den folgenden Abschnitten entnehmen können. Damit Planung und Umsetzung dieser Anforderungen möglichst effizient gestaltet werden können und die SzA reibungslos und effektiv mit vorhandenen Systemen und Prozessen arbeiten können, empfiehlt es sich für alle Unternehmen, ein (Informations-)Sicherheitsmanagementsystem (ISMS) zu etablieren.[1] Zudem können so auch zukünftige Änderungen effizienter geplant und umgesetzt werden.

Im Sinne einer strukturierten Umsetzung sind in diesem Dokument die Anforderungen an Protokollierung und Detektion in die Prozesse der Planung und der Umsetzung unterteilt.

Die Anforderungen werden mit den in Versalien geschriebenen Modalverben MUSS, SOLLTE und KANN sowie den zugehörigen Verneinungen formuliert, um die jeweiligen Anforderungen in Bezug auf das Umsetzungsgradmodell eindeutig zu kennzeichnen. Die Modalverben werden entsprechend den sprachlichen Erfordernissen konjugiert. Der Ausdruck MUSS bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss, um einen Umsetzungsgrad der Stufe 3 zu erreichen. Der Ausdruck SOLLTE bedeutet, dass etwas normalerweise getan werden sollte, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden, um einen Umsetzungsgrad der Stufe 4 zu erreichen. KANN wird für Anforderungen verwendet, deren Erfüllung nicht zwingend erforderlich, aber eine sinnvolle Ergänzung ist, wenn ein Umsetzungsgrad der Stufe 5 erreicht werden soll.

Grundsätzlich gilt für die Gesamtheit aller Bereiche (Protokollierung, Detektion und Reaktion) und Prozesse zur Angriffserkennung in diesem Dokument, dass

- die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen geschaffen werden MÜSSEN,
- Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden MÜSSEN,
- durchgängig alle zur effektiven Angriffserkennung erforderliche Hard- und Software auf einem aktuellen Stand gehalten werden MUSS,
- die Signaturen von Detektionssystemen immer aktuell sein MÜSSEN,
- alle relevanten Systeme[2] so konfiguriert sein MÜSSEN, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt werden können, sofern keine schwerwiegenden Gründe dagegensprechen[3].

[1] Siehe dazu ISMS.1: *Sicherheitsmanagement:* www.bsi.bund.de/dok/531260
[2] Siehe hierzu Planung der Protokollierung.
[3] Schwerwiegende Gründe liegen beispielsweise vor, wenn die dazu notwendigen Maßnahmen zu einer relevanten Gefährdung bzw. Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.

Protokollierung

Im Folgenden werden die Anforderungen im Bereich der Protokollierung aufgeführt, getrennt nach Planung und Umsetzung.

Planung der Protokollierung

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[4] innerhalb angemessener Zeit erzielt wird.

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.

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.

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.

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

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.

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

Umsetzung der Protokollierung

Als Mindestanforderung für die Protokollierung MÜSSEN alle Basisanforderungen von OPS.1.1.5 *Protokollierung* und die folgenden Anforderungen erfüllt werden:

[4] Vgl. Glossar.

Aufbau zentralisierter Protokollierungsinfrastrukturen:

Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen[5] 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.

Bereitstellung von Protokoll- und 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.

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.

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

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

[5] Zentral im Sinne der Netzarchitektur

Detektion

Im Folgenden werden die Anforderungen im Bereich der Detektion aufgeführt, getrennt nach Planung und Umsetzung.

Planung der Detektion

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

Als Mindestanforderung für die Detektion MÜSSEN alle Basisanforderungen von DER.1 *Detektion von sicherheitsrelevanten Ereignissen* und die folgenden Anforderungen erfüllt werden:

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 erfolgen. 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.

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. Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.

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.

[6] *MITRE ATT&CK* ist eine Informationsdatenbank über mögliche Aktionen böswilliger Cyber-Akteure und definiert eine Taxonomie für den Lebenszyklus von Cyber-Angriffen. *MITRE ATT&CK for ICS* ist eine entsprechende Informationsdatenbank spezialisiert auf Aktionen innerhalb von ICS-Netzwerken.

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.

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.

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[7] 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.

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.

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.

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

[7] Eigenes oder das eines Dienstleisters

manuell durch festgelegte Verantwortliche vorgenommen werden. Basierend auf den gewonnenen Erkenntnissen der Qualifizierung MÜSSEN die Detektionsmechanismen nachjustiert werden.

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

Reaktion

Als Mindestanforderung für die Reaktion MÜSSEN alle Basisanforderungen von DER.2.1 *Behandlung von Sicherheitsvorfällen* erfüllt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.

Es SOLLTEN zudem die Standardanforderungen aus DER.2.1 *Behandlung von Sicherheitsvorfällen* umgesetzt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.

Außerdem MUSS die folgende Anforderung erfüllt werden:

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.

Festgestellte Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen MÜSSEN behandelt werden.

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.

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.

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

4 Nachweis von Systemen zur Angriffserkennung[8]

Um Nachweise nach § 8a Absatz 3 BSIG und § 11 Absatz 1e EnWG einfach zu halten, sollen die umgesetzten Maßnahmen von Systemen zur Angriffserkennung über einen Umsetzungsgrad nachgewiesen werden. Das hierfür nötige Umsetzungsgradmodell wird im folgenden Abschnitt vorgestellt.

Das Umsetzungsgradmodell

Die Qualität der eingesetzten Systeme gemäß § 8a Absatz 1a BSIG bzw. nach § 11 Absatz 1e EnWG lässt sich mit Hilfe eines Umsetzungsgradmodells bewerten. Dieses können Auditoren und Prüfer nutzen, um zu beurteilen, wie weit die organisatorischen und technischen Maßnahmen in der geprüften Kritischen Infrastruktur fortgeschritten sind. Das Modell orientiert sich hierbei an den zuvor formulierten Anforderungen und somit am IT-Grundschutz des BSI. Sollten vom Betreiber andere Standards zur Erfüllung der Anforderungen nach § 8a Absatz 1a BSIG bzw. § 11 Absatz 1e EnWG verwendet werden, kann das Modell von Prüfern sinngemäß verwendet werden, so lange ein vergleichbares Sicherheitsniveau bei der Umsetzung von Maßnahmen zur Erfüllung der Anforderungen gewährleistet ist.

Nachfolgende Liste enthält die Definition der Stufen des Umsetzungsgradmodells zur Umsetzung des § 8a Absatz 1a BSIG bzw. § 11 Absatz 1e EnWG. Hierbei bezieht sich der Begriff Bereiche auf a) Protokollierung, b) Detektion und c) Reaktion mit den jeweils in Kapitel 3 dieses Dokuments formulierten Anforderungen:

0. Es sind bisher keine Maßnahmen zur Erfüllung der Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Maßnahmen.
1. Es bestehen Planungen zur Umsetzung von Maßnahmen zur Erfüllung der Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen.
2. In allen Bereichen wurde mit der Umsetzung von Maßnahmen zur Erfüllung der Anforderungen begonnen. Es sind noch nicht alle MUSS-Anforderungen[9] erfüllt worden.
3. Alle MUSS-Anforderungen[9] wurden für alle Bereiche erfüllt. Idealerweise wurden SOLLTE-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert oder ist in Planung.
4. Alle MUSS- Anforderungen[9] wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen wurden erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
5. Alle MUSS-Anforderungen[9] wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen und KANN-Anforderungen wurden für alle Bereiche erfüllt, 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.

Ziel der Anwendung eines Umsetzungsgradmodells ist es, die Qualität von Systemen zur Angriffserkennung zu erhöhen. Durch regelmäßige Analysen kann überprüft werden, welche Teilbereiche noch unzureichend gesteuert sind. Ein niedriger Umsetzungsgrad begründet einen besonderen Handlungsbedarf. Umsetzungsgradmodelle können folglich dabei unterstützen, Schwerpunkte für die Weiterentwicklung von Systemen zur Angriffserkennung zu setzen.

[8] Dieser Abschnitt wird perspektivisch in die OH Nachweise integriert.
[9] Bei der Wahl geeigneter Maßnahmen zur Erfüllung der Anforderungen ist der Betreiber frei.

Nachweiserbringung

Nach dem BSIG regulierte Betreiber müssen dem BSI alle zwei Jahre ihre Nachweise gemäß § 8a Absatz 3 BSIG einreichen. Nachweise, die dem BSI ab dem 1. Mai 2023 vorgelegt werden, müssen auch Aussagen zur Umsetzung des § 8a Absatz 1a BSIG, also zum Einsatz von Angriffserkennungssystemen, enthalten.

Betreiber von Energieversorgungsnetzen und solchen Energieanlagen, die nach der Rechtsverordnung gemäß § 10 Absatz 1 BSIG als Kritische Infrastruktur gelten, haben gemäß § 11 Absatz 1f EnWG dem Bundesamt für Sicherheit in der Informationstechnik erstmalig am 1. Mai 2023 und danach alle zwei Jahre die Erfüllung der Anforderungen nach § 11 Absatz 1e EnWG nachzuweisen.

Die verschiedenen Rollen und Zuständigkeiten im Rahmen der Nachweiserbringung sind in der *Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG* (www.bsi.bund.de/OHNachweise) beschrieben. Die dort benannten Aufgaben für das Prüfteam und die Prüfende Stelle werden um die Nachweisprüfung der Systeme zur Angriffserkennung erweitert.

Gemäß der in Kapitel 3 dieser Orientierungshilfe benannten Kriterien wird durch die Prüfenden der individuelle Umsetzungsgrad der Systeme zur Angriffserkennung bewertet. Der so bestimmte Umsetzungsgrad ist im Zuge der Nachweiserbringung an das BSI zu übermitteln. 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.

Zur Nachweiserbringung stellt das BSI für KRITIS-Betreiber ein erweitertes Nachweisformular sowie für die Betreiber von Energieversorgungsnetzen und Energieanlagen ein eigenständiges Nachweisformular bereit.

KRITIS-Betreiber müssen gegenüber dem BSI allgemein die Erfüllung der Anforderungen aus § 8a Absatz 1 und Absatz 1a BSIG durch die entsprechenden Nachweise bestätigen. Daher muss ein Nachweis nach §8a Absatz 3 BSIG, um als vollständig zu gelten, ab 1. Mai 2023 auch die Ergebnisse der Prüfung der Systeme zur Angriffserkennung inklusive der aufgedeckten Sicherheitsmängel enthalten.

Analog gilt gemäß § 11 Absatz 1f EnWG ein Nachweis zu Angriffserkennungssystemen als vollständig, wenn die Ergebnisse der Prüfung der Systeme zur Angriffserkennung inklusive der aufgedeckten Sicherheitsmängel enthalten sind.

5 Glossar

Angriff

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Anomaliebasierte Erkennung / Anomalie-Detektion

Anomalie-Detektion beschreibt das Erkennen von Abweichungen von einem vorher definierten störungsfreien Zustand. In einer Lern- und Trainingsphase werden alle Geräte und deren Kommunikationsbeziehungen untereinander einer Allowlisting-Bewertung unterzogen (Baselining/ Kalibrierung). Das hierbei entstehende Regelset definiert den Normalzustand des informationstechnischen Systems. Alle von der Kalibrierung abweichende Ereignisse werden zunächst gemeldet und müssen (meist) individuell bewertet und das Regelset ggf. angepasst werden.

Intrusion-Detection-System (IDS)

Als Intrusion-Detection-System wird ein Werkzeug bezeichnet, welches sicherheitsrelevante Ereignisse system- oder netzwerkbasiert erkennt und deren Auswertung, Eskalation und Dokumentation unterstützt. Die Detektion von sicherheitsrelevanten Ereignissen kann musterbasiert und/ oder anomaliebasiert erfolgen.

Hostbasierte IDS (Host based IDS)

Hostbasierte IDS sind dadurch gekennzeichnet, dass sie auf den zu überwachenden Systemen betrieben werden. Sie werden typischerweise eingesetzt, um sicherheitsrelevante Ereignisse auf Anwendungs- oder Betriebssystemebene zu erkennen. Die verfügbaren Systeme unterscheiden sich stark in Art und Umfang der Auswertung der auf dem System zur Verfügung stehenden Informationen.

IT-Systemgruppe

Gruppenbildung von IT-Systemen (z. B. Arbeitsplatzcomputer (APC), Fileserver, TK-Anlage, DMZ) gemäß der Strukturanalyse, siehe BSI-Standard 200-2, Abschnitt 8.1. Die auf den IT-Systemen laufenden Anwendungen werden miterfasst.

Netzbasierte IDS (Network-based IDS, NIDS)

Netzbasierte IDS überwachen den Netzverkehr eines oder mehrerer Netzsegmente auf sicherheitsrelevante Ereignisse.

An Netzwerkübergängen wird die IDS-Funktionalität meist in Firewalls integriert. Innerhalb einzelner Netzwerksegmente kommen typischerweise IDS-Sensoren zum Einsatz. Diese überwachen den Netzwerkverkehr an zentralen Switchen über Mirror-Ports oder einzelnen Netzwerkverbindungen über Inline-TAPs. Viele Systeme verzichten auf dezidierte Hardware (insbesondere Open-Source-Lösungen und können in virtuellen Umgebungen oder als Docker-Container direkt auf den Netzwerkkomponenten (wie beispielsweise Switch oder EDGE-Router) betrieben werden.

Protokolldaten

Sind gemäß § 2 Nummer 8 BSIG Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes enthalten.

Protokollierungsdaten

Sind gemäß § 2 Nummer 8a BSIG Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme. Sie sind historische Aufzeichnungen über die Art und Weise, wie IT-Systeme genutzt wurden, über technische Ereignisse oder Zustände innerhalb des Systems (z. B. Syslog) und wie diese miteinander kommuniziert haben. Protokollierungsdaten bestehen aus (Protokollierungs-) Ereignissen, welche mit einem Zeitstempel versehen sind. Protokollierungsdaten lassen sich aus verschiedenen Perspektiven betrachten und organisieren. Für den operativen Umgang mit Protokollierungsdaten ist die gesetzliche eine der wichtigsten Perspektiven.

Sicherheitsrelevantes Ereignis (SRE)

Als sicherheitsrelevantes Ereignis (Security Event) wird ein Ereignis bezeichnet, das sich auf die Informationssicherheit auswirkt und die Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit eines Systems beeinträchtigen. Beispiele: Mehrfache fehlgeschlagene Anmeldeversuche eines Benutzers an einem System, Detektion einer Schadsoftware, Missachtung einer Sicherheitsrichtlinie

Sicherheitsvorfall (Qualifiziertes sicherheitsrelevantes Ereignis)

Als Sicherheitsvorfall (Security Incident) wird ein unerwünschtes Ereignis bezeichnet, das Auswirkungen auf die Informationssicherheit hat und in der Folge große Schäden nach sich ziehen kann. Typische Folgen von Sicherheitsvorfällen können die Ausspähung, Manipulation oder Zerstörung von Daten sein. Bei Sicherheitsvorfällen, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur führen oder führen können, handelt es sich um meldepflichtige Sicherheitsvorfälle im Sinne des § 8b Absatz 4 BSIG.

Sichtbarkeit

Die Sichtbarkeit dient als Größe für die Protokollierung und beschreibt die Anzahl der Datenquellen, deren zu protokollierende Ereignisse durch die Einrichtung erhoben werden. Zur genaueren Bestimmung der Protokollierungsgüte kann die Sichtbarkeit in die Quantität und die Qualität unterteilt werden.

Die Quantität der Sichtbarkeit bezeichnet die Anzahl der IT-Systeme und Datenquellen auf Endpunkten und im Netz, deren Daten durch die Einrichtung gesammelt werden.

Die Qualität der Sichtbarkeit bezeichnet die Positionierung der Punkte der Erhebung (wie z. B. Sensoren). Die Qualität wird bestimmt durch

a. die Fähigkeit, ausgewählte Angriffe theoretisch erkennen zu können (z. B. kann Lateral Movement nur eingeschränkt an den Netzgrenzen erkannt werden) und

b. das Vorliegen sämtlicher notwendigen Informationen aus unterschiedlichen Quellen zur Bewertung (z. B. IP-Adresse, pDNS, DHCP Logs, DNS Logs, etc. des betroffenen Endsystems statt nur eine IP-Adresse der Firewall).