Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 29.06.2023

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	15.10.2018	Erstveröffentlichung
1.0a	24.02.2021	Anpassungen von Verlinkungen
2.0	29.06.2023	Major-Release: Integration der PR-B, Entfall des RDSK, Ergänzungen zur Detektion

Tabelle 1: Versionsgeschichte des Mindeststandards zur Protokollierung und Detektion von Cyber-Angriffen. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: https://www.bsi.bund.de/dok/mst-pd-log

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort

Risiken für die Cyber- und Informationssicherheit sind nicht zuletzt aufgrund der zunehmenden Komplexität und Vernetzung von IT-Systemen allgegenwärtig. Dadurch betreffen potenzielle Schwachstellen und Cyber-Angriffe in der Regel nicht nur einzelne Stellen.

Umso wichtiger ist die Vorgabe verbindlicher Sicherheitsanforderungen an die Informationstechnik des Bundes. So kann ein einheitliches Mindestsicherheitsniveau mit effektiven Maßnahmen zur Abwehr von Cyber-Angriffen innerhalb der heterogenen Behördenlandschaft etabliert werden.

Dazu legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Mindeststandards (MST) für die Sicherheit der Informationstechnik des Bundes[1] fest. Dies erfolgt auf der Grundlage des § 8 Absatz 1 BSIG im Benehmen mit den Ressorts. Als gesetzliche Vorgabe definieren Mindeststandards somit ein verbindliches Mindestniveau für die Informationssicherheit.

Bereits 2017 hat das Bundeskabinett mit dem Umsetzungsplan Bund 2017 (UP Bund 2017)[2] eine Leitlinie für Informationssicherheit in der Bundesverwaltung in Kraft gesetzt. Damit wurde die Beachtung der Mindeststandards für den Bereich der Stellen des Bundes verbindlich. Durch das IT-Sicherheitsgesetz 2.0 wurde die Einhaltung der Mindeststandards des BSI auch gesetzlich geregelt. Die Umsetzungspflicht der Mindeststandards ergibt sich aus dem dadurch neu gefassten § 8 BSIG.

Die Mindeststandards richten sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe), Informationssicherheitsbeauftragte (ISB), IT-Betriebspersonal und Beschaffungsstellen. Die Gesamtverantwortung für die Informationssicherheit und damit auch für die Einhaltung der Mindeststandards trägt gemäß UP Bund 2017 die Leitung der jeweiligen Einrichtung[1].

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf dem Mindestsicherheitsniveau sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Einrichtung auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Einrichtungen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Die von den Mindeststandards adressierten Stellen werden in § 8 Absatz 1 BSI-Gesetz (BSIG) definiert (siehe https://www.gesetze-im-internet.de/bsig_2009/__8.html). Zur besseren Lesbarkeit wird im weiteren Verlauf für alle dort genannten Stellen der Begriff „Einrichtung“ verwendet.
[2] Vgl. UP Bund (BMI 2017)
[3] Siehe FAQ zu den MST: https://www.bsi.bund.de/dok/mst-faq, (BSI 2023a)

Inhalt

1 Beschreibung

1.1 Begriffsbestimmung und Abgrenzung

Der Mindeststandard „Protokollierung und Detektion von Cyber-Angriffen“ (MST PD) definiert gemäß § 8 Abs. 1 BSIG das Mindestniveau für die Informationssicherheit des Bundes im Bereich der Protokollierung von Ereignissen und in der Detektion von daraus folgenden sicherheitsrelevanten Ereignissen (SRE), um ein zielgerichtetes und einheitliches Vorgehen zur Erkennung und Abwehr von Cyber-Angriffen auf die Kommunikationstechnik des Bundes (§ 2 Abs. 3 S. 1 BSIG) zu etablieren. Der Mindeststandard beschreibt den dazu notwendigen Rahmen und eine strategische Vorgehensweise, die situationsunabhängig für eine angemessene Protokollierung und Detektion im jeweiligen Kontext angewendet werden muss.

Der Mindeststandard definiert allgemeine Anforderungen (Kapitel 2.1), die eine Voraussetzung für eine wirksame Umsetzung der prozessualen Anforderungen für die Protokollierung[4] (Kapitel 0) und Detektion (Kapitel 2.3) schaffen.

Die Umsetzung dieses Mindeststandards erfüllt nicht die Verpflichtungen für die Bundesverwaltung gemäß der §§ 5 und 5a BSIG.[5] Die Umsetzung der Anforderungen kann jedoch die Grundlage für die Datenzulieferung gemäß § 5 Abs. 1 Satz 4 und § 5a Satz 2 BSIG bilden. Aus diesem Grund sind Abweichungen von diesem Mindeststandard im Hinblick auf die aus den §§ 5 und 5a BSIG bestehenden Verpflichtungen für die Einrichtungen nur im Einvernehmen mit dem BSI zulässig.

Bei der Umsetzung des Mindeststandards sind die im konkreten Einzelfall relevanten gesetzlichen Regelungen, insbesondere der Europäischen Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) sowie ggf. des Fernmeldegeheimnisses (Art. 10 Grundgesetz), zu beachten.

Der Mindeststandard baut auf den IT-Grundschutz-Bausteinen[6] *OPS.1.1.5 Protokollierung* und *DER.1 Detektion von sicherheitsrelevanten Ereignissen* und deren Inhalten auf.[7] Er dient insbesondere den IT-Verantwortlichen und Informationssicherheitsbeauftragten als Grundlage für die Einforderung und Umsetzung von organisatorischen und technischen Maßnahmen. Die erforderlichen personellen Ressourcen sind zu ermitteln und bereitzustellen.

Für eine gemeinsame Basis und Anwendung werden zunächst besonders relevante Begriffe im Kapitel 1.1 festgelegt. Weitere Begriffe, die nicht bereits aus dem IT-Grundschutz hervorgehen, sind im Glossar beschrieben und definiert.

In Kapitel 2 werden die Sicherheitsanforderungen an die konkrete Umsetzung der Protokollierung und Detektion im Informationsverbund der Einrichtung definiert.

[4] Die mit MST Version 1.0(a) veröffentlichte Protokollierungsrichtlinie-Bund (PRB) wurde in diese Version direkt integriert. Weitere Ausführungen zu Protokollierungskonfigurationen finden sich in den systemspezifischen Dokumentations- und Konfigurationsvorgaben des BSI.

[5] Gemäß § 5 Abs. 1 Satz 4 und § 5a Satz 2 BSIG sind Bundesbehörden dazu verpflichtet, das BSI bei Maßnahmen zur Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik zu unterstützen und hierbei den Zugang des BSI zu behördeninternen Protokolldaten und Protokollierungsdaten sowie Schnittstellendaten sicherzustellen.

[6] Vgl. IT-Grundschutz-Kompendium, (BSI 2023b)

[7] Laut Mindeststandard-Anforderung PD.2.1.03 a) sind alle Basis- und Standardanforderungen umzusetzen, und zwar unabhängig davon, ob die einzelnen Anforderungen im übrigen Mindeststandard explizit referenziert werden oder nicht.

1.1.1 Zu protokollierende Ereignisse

Die zu protokollierenden Ereignisse werden zur Abgrenzung zunächst in Protokoll- bzw. Protokollierungsdaten (Kapitel 1.1.1.1) und sicherheitsrelevante Ereignisse (SRE, Kapitel 1.1.1.3) eingeteilt. Abbildung 1 stellt die Aufteilung und Zusammenhänge grafisch dar, die nachfolgend weiter beschrieben werden.[8]

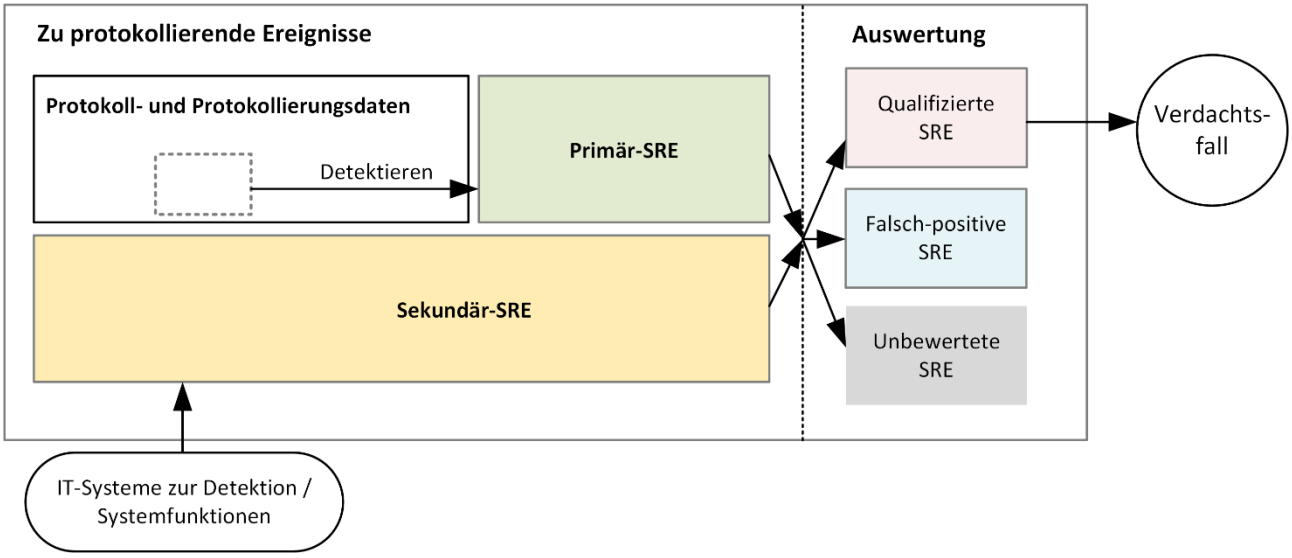

Abbildung 1: Darstellung der verschiedenen Ereignisarten. SRE werden gemäß ihrem Ursprung in primär und sekundär unterteilt. In der Auswertung von SRE findet die Qualifizierung statt und es wird entschieden, ob es sich bei einem SRE um einen Verdachtsfall handelt.

1.1.1.1 Protokoll- und Protokollierungsdaten

Protokoll- und Protokollierungsdaten (gemäß § 2 Abs. 8 und 8a BSIG; siehe Glossar) stellen die Basis zur Detektion fortgeschrittener Angriffe dar. Gleichzeitig bieten sie die Grundlage zur effektiven Auswertung von primären SRE und zur Reaktion auf Sicherheitsvorfälle. Aus einzelnen Protokoll- und Protokollierungsdaten allein lässt sich in den meisten Fällen nicht eindeutig auf das Vorliegen eines Verdachtsfalls schließen. Erst in Korrelation mit anderen Informationen (z. B. anderen Protokoll- und Protokollierungsdaten oder Kontextinformationen) lässt sich erschließen, dass ein Verdachtsfall existieren könnte.

Protokollierungsdaten aus IT-System-Sicht (gemäß § 2 Abs. 8a BSIG)

Auf allen IT-Systemen fallen Protokollierungsdaten aus IT-System-Sicht an. Diese Daten enthalten Informationen über die Interaktion eines Nutzenden mit einem IT-System (z. B. „User X hat sich erfolgreich authentifiziert.“) oder die eines Administrierenden mit einem IT-System (z. B. „User Y hat erfolgreich administrative Rechte erhalten.“). Die Ereignisse können aber auch durch automatisierte Prozesse ausgelöst werden. Ereignisse aus IT-System-Sicht können sowohl auf Clients und Servern als auch auf allen Netzwerkkomponenten, wie beispielsweise Router und Firewalls, auftreten (siehe Abbildung 2). Typische Kategorien, in die sich Protokollierungsdaten einordnen lassen, sind für Microsoft Windows z. B. Warning, Error, Critical oder unter Linux z. B. auth.log, boot.log, secure.log. Daneben können auch Meta-Informationen von Inhaltsdaten auf dem IT-System protokolliert werden, z. B. Hash-Werte (zur Integritätssicherung).

[8] Erläuterungen für die Auswertung der primären und sekundären sicherheitsrelevanten Ereignisse erfolgen im Rahmen der Detektion (Kapitel 1.1.2.2).

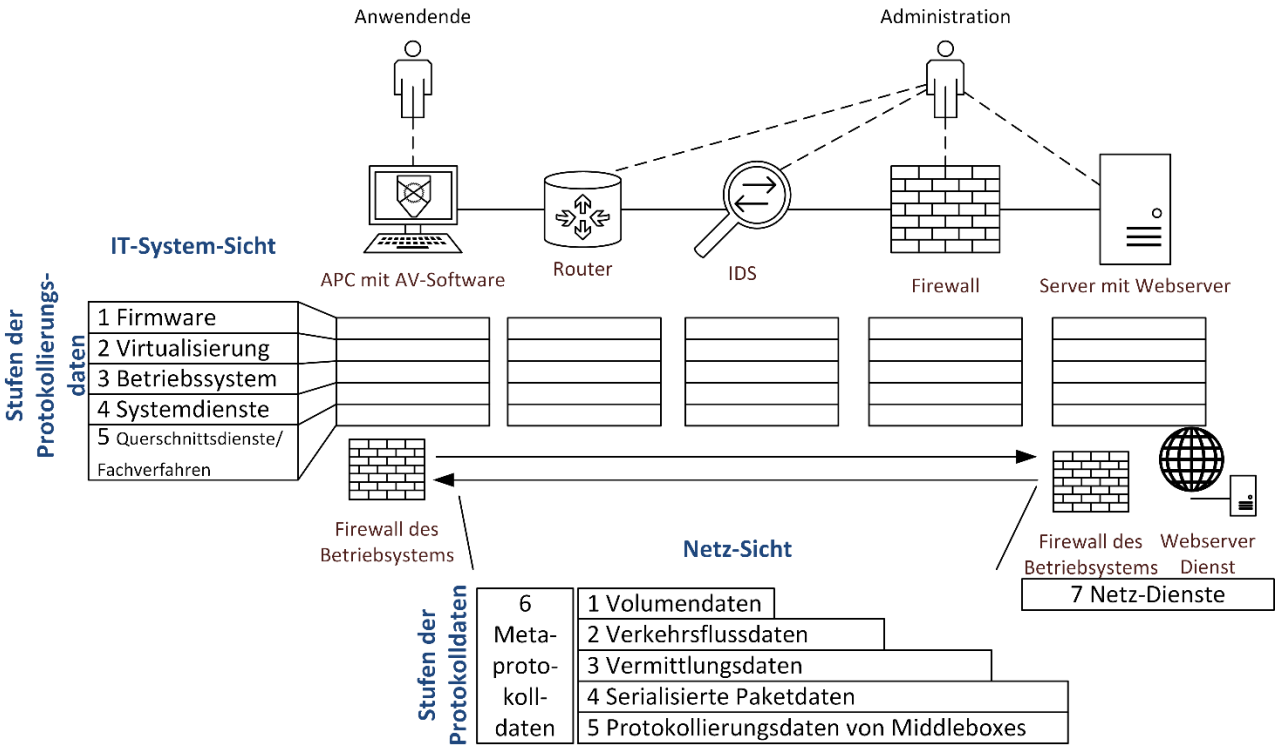

Abbildung 2: Detaillierte Darstellung der Sichten auf Protokoll- und Protokollierungsdaten. Protokoll- und Protokollierungsdaten werden in Stufen unterteilt und zu repräsentativen Beispielkomponenten zugeordnet.

Die in Abbildung 2 dargestellten Stufen der IT-System-Sicht werden im Folgenden detaillierter beschrieben:

1. Firmware: Die auf der Stufe Firmware zu erhebenden Protokollierungsdaten dienen primär dazu, eine Kompromittierung des Hostsystems festzustellen. Die Protokollierungsdaten können sowohl eigenständig als auch im Kontext von Protokollierungsdaten auf höheren Stufen Rückschlüsse auf den Zustand des Gesamtsystems zulassen.
2. Systembasierte Virtualisierung (in Abgrenzung zu prozessbasierter Virtualisierung): Die auf dieser Stufe anfallenden Protokollierungsdaten dienen dazu, eine mögliche Kompromittierung des Host-Systems festzustellen und die Zuverlässigkeit der Protokolldaten aus Netz-Sicht, die in der Virtualisierung erhoben werden, zu bestimmen. Da virtualisierte Systeme in den meisten Einrichtungen zum Einsatz kommen, darf ihre Betrachtung nicht vernachlässigt werden. Eine Kompromittierung des Host-Systems würde gleichzeitig eine Kompromittierung aller darauf ausgeführten Gast-Systeme bedeuten.
3. Betriebssystem: Die Protokollierungsdaten auf dieser Stufe dienen der Detektion von Cyber-Angriffen, welche auf eine oder mehrere Komponenten des Betriebssystems abzielen. Ein typischer Angriff, welcher auf dieser Stufe anzusiedeln ist, ist die Ausnutzung von Schwachstellen in Betriebssystemkomponenten zum Zwecke einer Kompromittierung.
4. Systemdienste: Unter Systemdiensten sind sämtliche Dienste (in Windows-Umgebungen auch als Rollen, Rollendienste und Features bezeichnet) zu verstehen, welche zusätzlich zur Basisfunktionalität eines Betriebssystems zum Einsatz kommen. Die Systemdienste können dabei essentiell für den Betrieb des Behördennetzes oder unterstützender Natur sein. Die Protokollierungsdaten auf dieser Stufe dienen dazu, eine Kompromittierung dieser essentiellen Dienste festzustellen. Beispiele für Systemdienste sind Authentisierungs- und Verzeichnisdienste, Datei- und Speicherdienste oder Druck- und Dokumentendienste.
   Hinweis: Wie zuvor beschrieben gibt es manche Dienste auf den IT-Systemen (z. B. lokale Firewall oder lokale Webserver), welche zusätzlich Protokolldaten aus Netz-Sicht erzeugen.
5. Querschnittsdienste und Fachverfahren: Durch deren Individualität sind Protokollierungsdaten abhängig von den Möglichkeiten der Querschnittsdienste und Fachverfahren zu erheben.

Protokolldaten aus Netz-Sicht (gemäß § 2 Abs. 8 BSIG)

Wenn zwei IT-Systeme miteinander kommunizieren (im Beispiel in Abbildung 2; Kommunikation zwischen APC und Webserver), dann entstehen Protokolldaten. Bei Netzwerkkomponenten (z. B. Switch, Router, Firewall, Load Balancer, Intrusion Detection System/IDS) entsteht dadurch eine Besonderheit. Zum einen erzeugen diese Systeme über sich selbst Protokollierungsdaten aus IT-System-Sicht (siehe Beispiel oben). Zum anderen erzeugen diese IT-Systeme Ereignisse aus Netz-Sicht: Protokolldaten über die Kommunikation zweier anderer IT-Systeme. Diese Besonderheit kann auch für IT-Systeme mit Netzwerkfunktionalitäten gelten (z. B. Web- und Mailserver, Browser und Mail-Client, lokale Firewall, Netzschnittstellenkarte).

Die in Abbildung 2 dargestellten Stufen aus Netz-Sicht werden im Folgenden detaillierter beschrieben:

1. Volumendaten: Protokolldaten dieser Stufe entsprechen den Messdaten zum Betriebsverhalten eines IT-Systems. Aus diesen Daten sind die beteiligten IT-Systeme einer Kommunikation nicht ableitbar, sondern lediglich statistische Werte über die Art und den Umfang der Kommunikation. Beispielsweise: Anzahl übertragener Bytes über Port 80 innerhalb eines Zeitintervalls.
2. Verkehrsflussdaten: Protokolldaten dieser Stufe entstehen, wenn über die erste Stufe hinaus Informationen der IT-Systeme einer Kommunikation gespeichert werden. Um statistische Werte berechnen zu können, werden einzelne Verkehrsflüsse aggregiert. Die Aggregation zeichnet sich dadurch aus, dass meistens das 4-Tupel Quellsystem, Quellport, Zielsystem und Zielport über einen definierten Zeitraum identisch ist. Da Port-Nummern keine eindeutige Identifizierung von Applikationen ermöglichen, können auch weitere Informationen über die Art der Kommunikation zu diesem 4-Tupel hinzugefügt werden. Diese Verkehrsflussdaten können z. B. aus NetFlow- oder IPFIX-Daten generiert werden.
3. Vermittlungsdaten: Protokolldaten dieser Stufe beschreiben die Vermittlung und den Verbindungsaufbau eines Kommunikationsvorgangs. Beispielsweise: Bei dem Aufbau einer TLS-verschlüsselten Verbindung wird ein Zertifikat übertragen, welches zum Teil protokolliert wird. Die Vermittlungsdaten können z. B. an Netzübergängen an TLS-Proxies oder mithilfe von TAPs oder Spiegelports erhoben werden.
4. Serialisierte Paketdaten: Protokolldaten dieser Stufe sind zusammengesetzte Pakete der Layer 4 bis 7 des ISO/OSI-Modells, deren Inhalte so aufbereitet wurden, dass sie analysiert werden können. Diese können durch unterstützende Analysewerkzeuge generiert werden. Die z. B. durch TAPs oder Spiegelports aufgezeichneten Paketdaten werden in serialisierte Paketdaten zusammengesetzt und wesentliche Informationen extrahiert. Serialisierte Paketdaten enthalten keine Inhaltsdaten. In den meisten Fällen dürfen daher ausschließlich die Paket-Header gespeichert werden (Ausnahme z. B. DNS, hier werden die gesamten Anfragen und Antworten gespeichert).
5. Protokolldaten von Middleboxes (z. B. RFC 3234): Serialisierte Paketdaten können nur durch das Mitschneiden des Netzwerkverkehrs erzeugt werden; häufig sind aber bereits schon IT-Systeme im Einsatz, welche den Netzwerkverkehr terminieren und zum eigentlichen Zielsystem neu aufbauen. Hierzu zählen z. B. Web-Proxies, E-Mail-Gateways und sonstige Application Layer Gateways. Derartige Systeme (auch bekannt als Middleboxes) bieten häufig die Möglichkeit, die Kommunikation zweier IT-Systeme zu protokollieren und damit etwas Ähnliches wie serialisierte Paketdaten zu erzeugen. Allerdings hängt die Qualität von den Möglichkeiten der jeweiligen Middlebox ab, sodass häufig nur die Anfrage protokolliert werden kann.
6. Metaprotokolldaten: Protokolldaten dieser Stufe werden von Systemen als Analyse eines Kommunikationsvorgangs erzeugt (z. B. die Spam-Score-Klassifizierung einer E-Mail). Typischerweise sind diese unmittelbar ein Sekundär-SRE. Beispiele sind ein IDS-Alarm zu einem IP-Paket oder die Information, dass eine Verbindung am Paketfilter geblockt wurde.
7. Netz-Dienste auf IT-Systemen: Wie zuvor beschrieben, gibt es Systemdienste, welche der Netz-Sicht zugeordnet werden. Dies ist immer dann der Fall, wenn der Dienst Teil eines Kommunikationsvorgangs

ist, z. B. (Front-End-) Webserverdienste oder die Betriebssystem-Firewall. Protokolldaten können für diese Systeme analog zu den Stufen 5 und 6 erhoben werden.

1.1.1.2 Datenquellen

Datenquellen sind informationstechnische Systeme und Programme in einer Infrastruktur, an denen Protokoll- und Protokollierungsdaten und/oder sekundäre sicherheitsrelevante Ereignisse zum Zwecke der Detektion erhoben werden. Die Anzahl der an die Protokollierung angebundenen Datenquellen ist eine der Größen zur Bestimmung der Sichtbarkeit im Informationsverbund und bietet somit die Grundlage für die Detektion.

1.1.1.3 Sicherheitsrelevante Ereignisse

Sicherheitsrelevante Ereignisse (SRE) sind unter anderem Protokoll- und Protokollierungsdaten, die Auswirkungen auf die Informationssicherheit und ihre Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) haben können.[9] Sie werden in primäre und sekundäre sicherheitsrelevante Ereignisse eingeteilt, wobei diese Einteilung sich auf den Ursprung des SRE und nicht auf dessen Relevanz oder Wichtigkeit bezieht.

Primäre sicherheitsrelevante Ereignisse

Über verschiedene Verfahren zur Detektion werden in Protokoll- und Protokollierungsdaten SRE (z. B. „Nachladen einer schadhaften Datei aus dem Nutzendenkontext“) erkannt. Diese werden als primäre sicherheitsrelevante Ereignisse (Primär-SRE) bezeichnet. Primär-SRE beinhalten damit immer einen direkten Bezug auf einzelne oder mehrere Protokoll- und Protokollierungsdaten.

Sekundäre sicherheitsrelevante Ereignisse

Sekundäre sicherheitsrelevante Ereignisse (Sekundär-SRE) stammen aus IT-Systemen bzw. Software zur Detektion (z. B. Meldungen der Schadsoftware-Erkennung oder eines Intrusion Detection Systems). Ebenso gehören hierzu Protokoll- und Protokollierungsdaten von Systemfunktionen zur Detektion (z. B. die Verletzung der Regeln einer Betriebssystem-Firewall oder einer dedizierten Firewall), die nicht zwangsläufig einer Alarmierung zugeführt werden.

Eine Beziehung zu Protokoll- und Protokollierungsdaten lässt sich bei Sekundär-SRE nicht immer herstellen. Entweder, weil die zugehörigen Protokoll- und Protokollierungsdaten gar nicht dauerhaft erhoben werden (können), oder weil das Wissen darüber in den eingesetzten IT-Systemen bzw. Systemfunktionen und der eingesetzten Software verborgen ist.

1.1.2 Kontinuierlicher Prozess

In Abbildung 3 wird der kontinuierliche Prozess für die Protokollierung und Detektion von SRE mit den Ausgangsgrößen Sichtbarkeit und Abdeckung dargestellt. Die Sichtbarkeit dient als Größe für die Protokollierung und beschreibt die Anzahl der Datenquellen und deren zu protokollierende Ereignisse. Die Abdeckung dient als Größe für die Detektion und bestimmt die Anzahl der Vorgehensweisen von Cyber-Akteuren bzw. Arten von Cyber-Angriffen, die durch die Etablierung von Detektoren oder Detektionssystemen theoretisch erkannt und abgewehrt werden könnten. Dabei sorgt eine höhere Sichtbarkeit (z. B. Anzahl Datenquellen) oder höhere Abdeckung (z. B. Anzahl Detektoren) nicht automatisch für ein gesteigertes Sicherheitsniveau. Vielmehr definiert dieser Mindeststandard eine prozessuale Vorgehensweise zur Bestimmung von Sichtbarkeit und Abdeckung, um ein angemessenes Sicherheitsniveau durch die Protokollierung und Detektion zu erreichen. Die Kontinuität der Prozesse soll dafür sorgen, dass die Vorgehensweise priorisiert erfolgen und sich initial auf die wichtigen Bereiche innerhalb eines jeden Informationsverbundes fokussieren kann. Die Entscheidung zur Erschließung von

[9] Vgl. DER.1 Detektion von sicherheitsrelevanten Ereignissen, (BSI 2023b)

unkritischen Teilen des Informationsverbundes bleibt als Restrisiko im Rahmen des Informationssicherheitsmanagements zu treffen.

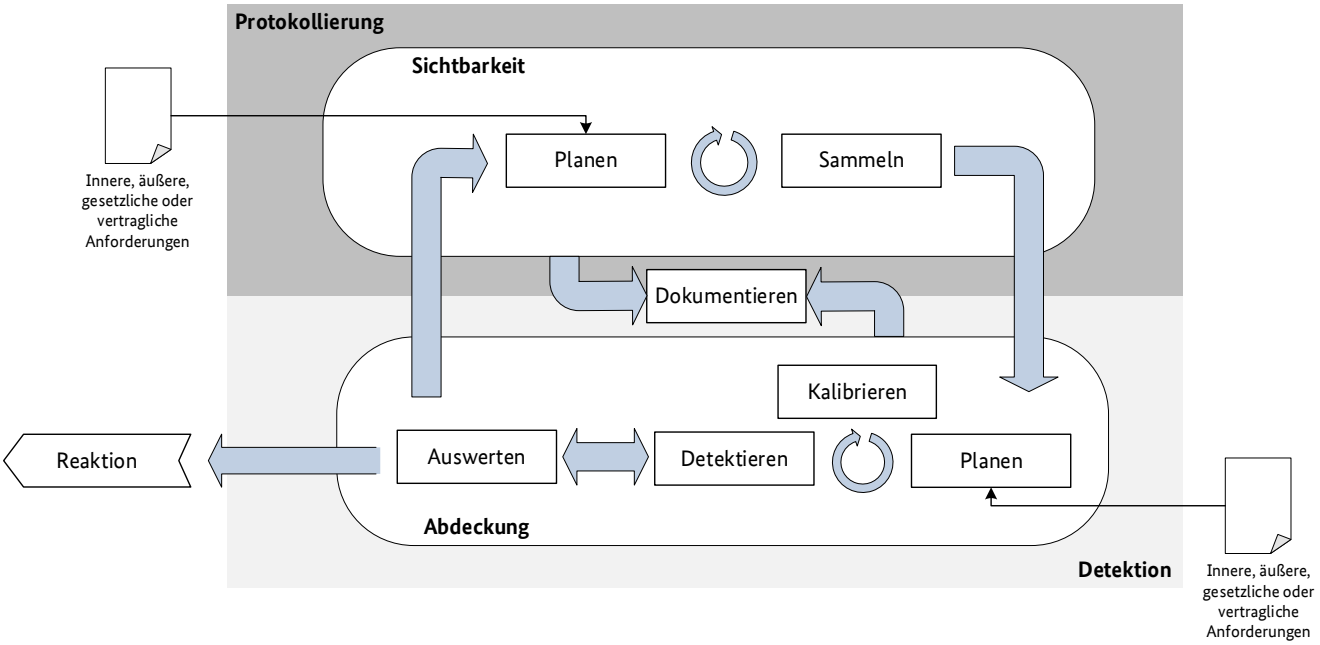

Abbildung 3: Kontinuierliche Prozesse Protokollierung und Detektion. Die Protokollierung (Planen und Sammeln) bildet die Ausgangsgröße Sichtbarkeit, die Detektion (Planen, Kalibrieren, Detektieren und Auswerten) bildet die Ausgangsgröße Abdeckung.

Dazu besteht der Prozess für die Protokollierung aus den Aktivitäten Planen und Sammeln. Die Detektion mit den Aktivitäten Planen, Kalibrieren, Detektieren und Auswerten bildet die Brücke zu dem Prozess der Reaktion und dient als dessen Auslöser. Im Querschnitt dient die Aktivität Dokumentieren dazu einerseits das Protokollierungsvorhaben fortlaufend festzuhalten (vgl. PD.2.2.02.e) und andererseits eine priorisierte Vorgehensweise für die Detektion zu formalisieren (vgl. PD.2.3.02.a). Durch die in diesem Mindeststandard beschriebene Methodik entsteht ein geschlossener Regelkreis zwischen der Protokollierung und Detektion. Dazu gilt es fortlaufend die inneren und äußeren Anforderungen, die einen Einfluss auf die Protokollierung und Detektion haben, zu identifizieren und zu berücksichtigen.

1.1.2.1 Protokollierung

Planen der Protokollierung

Die Aktivität *Planen* dient dazu, alle Datenquellen zu identifizieren, welche sinnvolle Protokoll- bzw. Protokollierungsdaten oder Sekundär-SRE für die Detektion erzeugen. Durch die Planung wird die Sichtbarkeit im Informationsverbund festgelegt. Es ist zu planen, wie die zu protokollierenden Ereignisse in die zentrale Protokollierungsinfrastruktur gelangen und welches Datenaufkommen zu erwarten ist. Weiterhin sind Verantwortlichkeiten verbindlich festzulegen. Hierzu zählt insbesondere die Verantwortlichkeit für die Protokollierung als solche sowie für die betriebenen Datenquellen. Im Zuge der Planung erfolgt auch die Schutzbedarfsfeststellung[10] sowie die Festlegung der konformen Erhebung und Speicherung der Daten, um die Absicherung der zentralen Protokollierungsinfrastruktur angemessen vorzunehmen.

Dokumentieren

Die Ergebnisse der Planungsaktivität werden durch eine angemessene Darstellung dokumentiert (siehe Anforderung PD.2.2.02.e). Die Dokumentation dient als gemeinsame Kommunikationsgrundlage für die

[10] Gem. BSI-Standard 200-2, Kapitel 8.2 Schutzbedarfsfeststellung, (BSI 2017)

Aufgabenbereiche *Operative IT-Sicherheit* (Kapitel 1.1.3.1), *IT-Betrieb* (Kapitel 1.1.3.2) und *User Help Desk* zur Interpretation der Protokoll- und Protokollierungsdaten sowie der SRE.

Sammeln

Im Anschluss an *Planen* und *Dokumentieren* erfolgt die Umsetzung (u. a. durch das *Sammeln* der zu protokollierenden Ereignisse). Diese erfolgt in mehreren Iterationen, da ggf. auch noch Änderungen an den IT-Systemen oder der IT-Infrastruktur erforderlich sind, um gewisse Daten erfassen zu können.

Die Aktivität *Sammeln* beschreibt den Prozess, um die zu protokollierenden Ereignisse automatisiert zur zentralen Protokollierungsinfrastruktur zu übertragen und dort zu speichern. Diese Aktivität beinhaltet auch eine kontinuierliche Überwachung der zentralen Protokollierungsinfrastruktur auf Fehlerzustände. Es kann erforderlich sein, zusätzliche IT-Systeme oder Software einzuführen, damit die bei der Planung als erforderlich identifizierten Datenquellen erfasst werden können. Innerhalb der Aktivität *Sammeln* muss darüber hinaus geprüft werden, ob eine Anreicherung oder Normalisierung der Daten erforderlich ist, um diese für die Detektion vorzubereiten.

Alle Aktivitäten müssen regelmäßig wiederholt werden, um stetige Veränderungen der IT in der Protokollierung und Detektion kontinuierlich zu berücksichtigen.

1.1.2.2 Detektion

Planen der Detektion

Die Aktivität *Planen* dient dazu, auf Basis der Protokollierung diejenigen Detektoren und Detektionssysteme auszuwählen, die zu einer angemessenen Abdeckung im Informationsverbund führen. Um die Abdeckung im Informationsverbund als quantifizierbare Größe darzustellen, ist die Auswahl einer geeigneten Methodik empfehlenswert. Diese Methodik erlaubt es, Detektoren und Detektionssysteme den Vorgehensweisen von Cyber-Akteuren bzw. Arten von Cyber-Angriffen zuzuordnen (z. B. mit Hilfe von Zuordnungsmatrizen zu Taktiken und Techniken von Cyber-Angriffen). Somit kann eine Aussage darüber erzielt werden, welche Arten von Cyber-Angriffen für die sichtbare[11] Infrastruktur mit den Detektoren und Detektionssystemen erkannt werden könnten. Ziel ist es, eine priorisierte Detektionsstrategie festzulegen, wie ein angemessenes Abdeckungsziel im Informationsverbund erreicht wird. Als Eingangsgröße bei der Festlegung der Detektionsstrategie sind innere und äußere Anforderungen (z. B. Schutzbedarfsfeststellungen, gesetzliche und vertraglich Anforderungen) zu berücksichtigen.

In der Planungsphase sollten notwendige Vorarbeiten zur Nutzbarkeit der Detektion durchgeführt werden. Dazu zählt, dass Kontextinformationen identifiziert und dokumentiert werden müssen, die für die Detektion und die spätere Auswertung im Rahmen der Reaktion erforderlich sein könnten (z. B. Namensschema, Rechte- und Rollenkonzepte, IP-Adressräume, Netzübergänge, Alarmierungskontakte). Außerdem sind die technischen und organisatorischen Maßnahmen, die bei der Anwendung von Detektoren und Detektionssysteme und der Reaktion auf resultierende SRE notwendig sind, festzulegen und zu dokumentieren.

Kalibrieren

Ziel des *Kalibrierens* ist es festzustellen, welche Primär-SRE im Normalzustand auftreten (sowohl hinsichtlich des Auftretens, als auch hinsichtlich der Häufigkeit des Auftretens). Dabei ist zu bewerten, ob dieser ermittelte Zustand akzeptabel ist, oder ob die Feststellung des Auftretens dazu genutzt werden sollte, die Detektionsparameter oder das jeweilige IT-System anzupassen. Dies ist insbesondere dann angeraten, wenn das SRE auf eine potentielle Schwachstelle hindeutet. Da sich der Normalzustand mit jeder größeren Organisationsänderung und durch Anpassungen des Informationsverbundes ändern kann, muss die Kalibrierung regelmäßig durchgeführt werden und wird idealerweise an die bestehenden Change-Prozesse

[11] Sichtbarkeit im Sinne der erfassten Datenquellen im Informationsverbund.

gekoppelt. Die Aktivität *Kalibrieren* kann auch für Sekundär-SRE erforderlich sein. Hier sind dann die Anforderungen des jeweils eingesetzten Produktes zu berücksichtigen.

Durch das *Kalibrieren* werden die verwendeten Verfahren zur Detektion (z. B. Detektoren, basierend auf Regeln, statistischen Kenngrößen oder Anomalieerkennung) in den Informationsverbund eingemessen. Unmittelbar nach der Kalibrierung müssen die Detektoren initial justiert werden, um die Anzahl an falsch-positiven SRE zu minimieren. Bei der initialen Justierung ist darauf zu achten, dass unbekannte Cyber-Angriffe nicht als falsch-positive SRE interpretiert werden.

Detektieren

Detektieren ist der automatisierte Prozess zur Analyse und Bewertung der Protokoll- und Protokollierungsdaten auf SRE durch die Detektoren und Detektionssysteme. Die Ausgangsgröße des Detektierens ist die Menge aller identifizierten Primär-SRE. Diese Aktivität beinhaltet auch eine kontinuierliche Überwachung der Detektoren und Detektionssysteme auf Fehlerzustände (z. B. durch unvollständige Daten) oder auf abweichende Detektionsergebnisse (siehe Kalibrieren).

Auswerten

Die Primär- und Sekundär-SRE müssen überprüft und dahingehend bewertet werden, ob sie auf einen Verdachtsfall hindeuten (siehe Abbildung 1). Nach der Auswertung ist nicht mehr zwischen Primär- oder Sekundär-SRE zu unterscheiden. Unter dem Aspekt der Auswertung sind die SRE dann wie folgt einzuteilen:

- qualifizierte SRE: Hinweis auf einen Verdachtsfall,
- falsch-positive SRE: SRE irrtümlich erzeugt; insbesondere bei Primär-SRE zu erwarten, oder
- unbewertete SRE: SRE nicht ausgewertet, da Klärung aus Zeit- oder Kostengründen nicht möglich.

Nur qualifizierte SRE lösen den Prozess der Reaktion[12] aus. Diese Bewertung zu treffen ist wesentlicher Bestandteil des *Auswertens* und bedarf einer sehr guten Kenntnis des jeweiligen Informationsverbundes.

Um diese Bewertung vornehmen zu können, stimmen sich die Aufgabenbereiche *Operative IT-Sicherheit* und *IT-Betrieb* bzw. *User Help Desk* ab. Kommt die *Operative IT-Sicherheit* zu dem Ergebnis, dass ein Verdachtsfall vorliegt, sind diese Erkenntnisse unverzüglich in den Prozess der Reaktion zu geben. Basierend auf den Erkenntnissen der *Operativen IT-Sicherheit* wird zusammen mit dem Informationssicherheitsmanagement die Planung der zu protokollierenden Ereignisse kontinuierlich an die Erfordernisse der Einrichtung angepasst. Dazu zählt auch, dass die Detektoren nachjustiert werden müssen, um die Anzahl an falsch-positiven SRE stetig zu reduzieren.

1.1.3 Aufgabenbereiche

Aus den Prozessen Protokollierung und Detektion ergeben sich die in Abbildung 4 dargestellten Aufgaben.

[12] Außerhalb des Regelungsbereiches dieses Mindeststandards, siehe dazu insbesondere DER.2.1 Behandlung von Sicherheitsvorfällen, (BSI 2023b).

Die Aufgabenbereiche *Operative IT-Sicherheit*, *IT-Betrieb* und *Revision* werden in den folgenden Abschnitten weiter ausgeführt. Dabei werden ausschließlich die Aufgaben betrachtet, die sich aus diesem Mindeststandard ergeben. Sonstige Aufgaben bleiben hiervon unberührt.

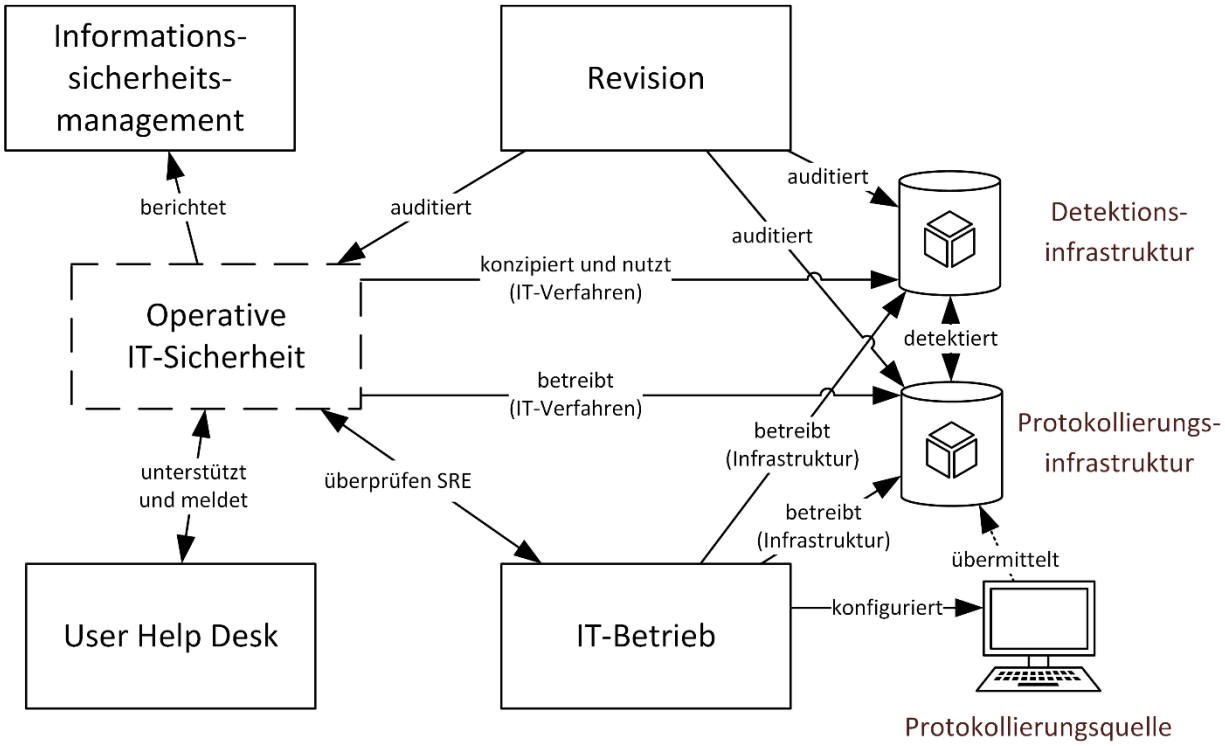

Abbildung 4: Übersicht über die Aufgabenbereiche der Protokollierung und Detektion. Die Operative IT-Sicherheit dient als zentrale Stelle zur Konzeption und dem Betrieb der Protokollierungs- und Detektionsinfrastruktur. Dazu bestehen notwendige Schnittstellen zum IT-Betrieb, dem Informationssicherheitsmanagement, der Revision und dem User Help Desk der Einrichtung.

1.1.3.1 Operative IT-Sicherheit

Die *Operative IT-Sicherheit* nimmt den zentralen Aufgabenbereich ein und kann sowohl vom *Informationssicherheitsmanagement* als auch vom *IT-Betrieb* wahrgenommen werden. Es liegt im Ermessen der jeweiligen Einrichtung, wie in diesem Zusammenhang die Aufgabe der *Operativen IT-Sicherheit* in der Aufbauorganisation zu verankern ist.

Die *Operative IT-Sicherheit* übernimmt neben der Daueraufgabe, SRE auszuwerten, insbesondere die Verantwortung für die Prozesse Protokollierung und Detektion. Hier sind die initiale und stetige Planung der Protokollierung inklusive der Spezifikation der zentralen Protokollierungsinfrastruktur hervorzuheben. Darüber hinaus konzipiert und nutzt die *Operative IT-Sicherheit* die Detektionsinfrastruktur im Rahmen des Prozesses *Detektion*. Die Protokollierungs- und Detektionsinfrastruktur selbst ist auch als IT-Verfahren zu betrachten und benötigt daher eine Verfahrensadministration. Mit Blick auf eine durchgängige Aufgabentrennung sollte die Verfahrensadministration grundsätzlich dem Aufgabenbereich *Operative IT-Sicherheit* zugeordnet sein. Bei der Umsetzung des Mindeststandards sind die im konkreten Einzelfall relevanten gesetzlichen Regelungen, insbesondere der EU-Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) sowie ggf. des Fernmeldegeheimnisses (Art. 10 Grundgesetz), zu beachten.

Um die Prozesse *Protokollierung* und *Detektion* erfolgreich umsetzen zu können, benötigt die *Operative IT-Sicherheit* eine sehr gute Vernetzung zum Aufgabenbereich *IT-Betrieb*, da dieser die Protokollierung einrichten muss und in der Regel die einzige Instanz ist, die Aussagen bezüglich der Kalibrierung treffen kann. Ebenso muss die *Operative IT-Sicherheit* mit dem *IT-Betrieb* Rücksprache halten können, wenn

qualifizierte SRE identifiziert wurden. Neben der informellen Vernetzung muss die *Operative IT-Sicherheit* ebenso wie der *User Help Desk* als Aufgabenbereich formal mit Rechten ausgestattet sein. Beispielsweise muss die *Operative IT-Sicherheit* Prüfungen von SRE durch den *IT-Betrieb* entsprechend der Kritikalität priorisieren oder eskalieren können.

Weiterhin muss die *Operative IT-Sicherheit* Zugriff auf Dokumentationen aus dem *IT-Betrieb* haben. Hierzu zählen u.a. Netzpläne, IP-Adresspläne und insbesondere die Datenbank des Change-, Incident- und Problem-Managements. Dies ist erforderlich, um die Belastung des *IT-Betriebs* mit Rückfragen bzgl. der SRE gering zu halten. Die Dokumentation sollte frühzeitig in der Planungsphase erstellt und kontinuierlich fortgeschrieben werden. Der Aufgabenbereich *Operative IT-Sicherheit* muss weiterhin ein grundlegendes technisches Verständnis der gesamten IT-Infrastruktur besitzen. Anhand der Dokumentation zur Protokollierung und den aufkommenden Daten, muss sie sich orientieren, um die auftretenden SRE einordnen zu können. Neben einer grundlegenden Fachkompetenz hinsichtlich gängiger Angriffsmethoden und einem Verständnis der IT-Infrastruktur, wird auch ein Verständnis von Risiken bezüglich Cyber-Angriffen benötigt, die konkret für die jeweilige Einrichtung bestehen.

Der Aufgabenbereich der *Operativen IT-Sicherheit* berichtet regelmäßig an das Informationssicherheitsmanagement über alle Ergebnisse der Auswertung (auch wenn es zu keinem Verdachtsfall kommt). Diese Informationen können vom Informationssicherheitsmanagement in die Planung und Ausgestaltung zukünftiger präventiver Maßnahmen einfließen.

1.1.3.2 IT-Betrieb

Der Betrieb von IT-Infrastrukturen der zentralen Protokollierungs- und Detektionssysteme sollte durch den *IT-Betrieb* erfolgen, um Synergieeffekte nutzen zu können. Die Operative IT-Sicherheit als Verfahrensadministration sollte bei Produktentscheidung, Planung und Projektierung entscheidend einwirken und bei der Installation und dem späteren Betrieb mitwirken.

Die erforderliche IT-Infrastruktur für die zentrale Protokollierungsinfrastruktur besteht im Regelfall aus verteilten IT-Systemen. Hierzu wird erfahrenes Personal zur Administration benötigt, das sich auf den Betrieb verteilter IT-Systeme spezialisieren kann. Idealerweise kann hier auf vorhandene Betriebskenntnisse in der Einrichtung zurückgegriffen werden, so dass der erforderliche Aufwand minimiert wird. Vor der Umsetzung dieses Mindeststandards sollte geprüft werden, ob zusätzliche Ressourcen für den Betrieb der zentralen Protokollierungs- und Detektionsinfrastruktur notwendig sind. Die zentrale Protokollierungsinfrastruktur sollte ganzheitlich als Protokollierungssystem für alle Bereiche der Einrichtung gedacht werden, d. h. sowohl für die Protokollierung zur Erkennung von Cyber-Angriffen als auch für die Protokollierung aus der Perspektive der Betriebssicherheit. Dies erleichtert die Kommunikation zwischen den beteiligten Aufgabenbereichen *IT-Betrieb* und *Operative IT-Sicherheit*.

Zusätzlich ist der *IT-Betrieb* in die Planung und Konfiguration der zentralen Protokollierung und vor allem der Protokollierungsquellen einzubeziehen. Insbesondere auch, um sicherzustellen, dass durch die Protokollierung kein negativer Einfluss auf die Betriebssicherheit erzeugt wird. Die Aufgabenbereiche *IT-Betrieb* und *User Help Desk* unterstützen die *Operative IT-Sicherheit* bei der regelmäßigen Kalibrierung und der Überprüfung der SRE.

1.1.3.3 Revision

Die regelmäßige Auditierung der zentralen Protokollierungs- und Detektionsinfrastruktur, die ggf. erforderliche De-Pseudonymisierung von Protokoll- und Protokollierungsdaten und die Auditierung der Durchführung der Aufgaben der *Operativen IT-Sicherheit* erfordert Ressourcen, welche hier als *Revision* zusammengefasst werden. Je nachdem, wie dies durch die Einrichtung organisatorisch festgelegt ist, kann die *Revision* zum Beispiel im Auftrag der behördlichen Datenschutzbeauftragten (bDSB) erfolgen, um festzustellen, ob die Protokoll- und Protokollierungsdaten missbräuchlich ausgewertet wurden.

1.2 Modalverben

In Anlehnung an den IT-Grundschutz[13] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[14] und DIN 820-2: 2018[15].

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Die Begründung muss dokumentiert und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Die Begründung muss dokumentiert und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung oder Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

[13] Vgl. BSI-Standard 200-2, (BSI 2017), S. 18
[14] Vgl. Key words for use in RFCs, (IETF 1997)
[15] Vgl. DIN-820-2: Gestaltung von Dokumenten, (DIN 2018)

2 Sicherheitsanforderungen

Nachfolgende allgemeine Anforderungen (Kapitel 2.1) setzen die Grundvoraussetzungen für eine wirksame Umsetzung der prozessualen Anforderungen für die Protokollierung (Kapitel 0) und Detektion (Kapitel 2.3). Die Umsetzung dieser Sicherheitsanforderungen erfüllt nicht die Verpflichtungen für die Bundesverwaltung gemäß der §§ 5 und 5a BSIG.

2.1 Allgemeine Anforderungen

PD.2.1.01: Aufgabenbereiche

a) Zuständigkeit und Verantwortung für die Aufgabenbereiche *Operative IT-Sicherheit*, *IT-Betrieb* und *Revision* MÜSSEN gemäß Kapitel 1.1.3 verbindlich festgelegt werden, zum Beispiel unter Zuhilfenahme des Geschäftsverteilungsplans der Einrichtung.

PD.2.1.02: Sensibilisierung der Mitarbeitenden

a) Es MUSS eine Sensibilisierung der Mitarbeitenden in Bezug auf die Protokollierung und Detektion erfolgen.[16]

PD.2.1.03: Grundlegende Anforderungen

a) Einrichtungen MÜSSEN die Basis- und Standardanforderungen der IT-Grundschutz-Bausteine OPS.1.1.5 *Protokollierung* und DER.1 *Detektion von sicherheitsrelevanten Ereignissen* umsetzen.[17]

b) Darüber hinaus MÜSSEN die folgenden Anforderungen[18] umgesetzt werden:

> *i) Auswertung der Protokoll- und Protokollierungsdaten durch spezialisiertes Personal[19]:*
> Es MUSS Personal speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten zu überwachen. Das beauftragte Personal MUSS die notwendigen Fachkenntnisse für diese Aufgabe erhalten. Ein Personenkreis MUSS benannt werden, der für das Thema Auswertung von Protokoll- und Protokollierungsdaten verantwortlich ist.
>
> *ii) Zentrale Detektion und Überprüfungen von Ereignismeldungen[20]:*
> Komponenten an zentraler Stelle innerhalb der Infrastruktur MÜSSEN eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. Zentrale, automatisierte Analysen mit Softwaremitteln MÜSSEN eingesetzt werden. Mit diesen zentralen, automatisierten Analysen MÜSSEN alle in der Systemumgebung anfallenden Ereignisse ermittelt und ggfs. in Bezug zueinander gesetzt werden. Alle eingelieferten Daten MÜSSEN lückenlos einsehbar und auswertbar sein. Die eingelieferten Daten MÜSSEN permanent ausgewertet werden. Werden definierte Schwellwerte überschritten oder bestätigte Verdachtsfälle erkannt, MUSS automatisch alarmiert werden. Das Personal MUSS sicherstellen, dass bei einem Alarm unverzüglich eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. In diesem Zusammenhang MÜSSEN die Zuständigen und die Beteiligten des Kommunikationsvorgangs sofort informiert werden.
> Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist. Zusätzlich MÜSSEN bereits überprüfte Protokoll- und

[16] Vgl. DER.1.A4 Sensibilisierung der Mitarbeitenden, (BSI 2023b)
[17] Vgl. DER.1 Detektion von sicherheitsrelevanten Ereignissen und OPS.1.1.5 Protokollierung, (BSI 2023b)
[18] Diese Anforderungen stammen ebenfalls aus den genannten IT-Grundschutz-Bausteinen und wurden im vorliegenden Mindeststandard entsprechend verschärft.
[19] Vgl. DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten, DER.1.A7 Schulung von Zuständigen, DER.1.A14 Auswertung der Protokollierungsdaten durch spezialisiertes Personal, (BSI 2023b)
[20] Vgl. DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten, DER.1.A15 Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen, (BSI 2023b)

Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.

c) Die Umsetzung der Detektion KANN ausgelagert werden.[21]

d) IT-Dienstleister und andere Einrichtungen, die über erhöhte Ressourcen für die Detektion verfügen, SOLLTEN eine eigenständige Protokollierungs- und Detektionsinfrastruktur konzipieren und nutzen.[22]

PD.2.1.04: Bestimmung und Einhaltung rechtlicher und vertraglicher Rahmenbedingungen

a) Es MUSS eine Bestimmung der rechtlichen und vertraglichen Rahmenbedingungen im Zusammenhang mit der Protokollierung und Detektion durchgeführt werden.[23]

b) Die Anforderungen aus den Ergebnissen der Bestimmung rechtlicher und vertraglicher Rahmenbedingungen MÜSSEN bei der Festlegung der Sichtbarkeiten zur Auswahl von Datenquellen eingehalten werden. Es DÜRFEN NUR die Daten erhoben werden, für die die Legitimität geprüft worden ist.

c) Aus den geltenden rechtlichen und vertraglichen Rahmenbedingungen MUSS eine konforme Speicherfrist für die Protokollierung identifiziert und angewendet werden. Es MUSS sichergestellt werden, dass die Protokoll- und Protokollierungsdaten sowie Sekundär-SRE nach Ablauf der Speicherfrist gelöscht werden.[24]

PD.2.1.05: Protokollierung und Detektion bei Bezug von IT-Dienstleistungen

a) Einrichtungen, die Teile ihrer IT bei einem Dienstleister ausgelagert haben, MÜSSEN sicherstellen, dass die Anforderungen dieses Mindeststandards auch im Rahmen der Auslagerung berücksichtigt werden.

b) Alle Aspekte der Protokollierung und Detektion, die im Rahmen der Dienstleistungserbringung gemäß dieses Mindeststandards festgelegt werden, MÜSSEN schriftlich zwischen den Parteien geregelt werden.

c) Es SOLLTE sichergestellt werden, dass die Einrichtung Zugriff auf die Protokoll- und Protokollierungsdaten sowie auf die Sekundär-SRE der ausgelagerten Systeme erhält. Dies SOLLTE über eine kontinuierliche Datenübertragung der Protokoll- und Protokollierungsdaten sowie der Sekundär-SRE zu einem zentralen System[25] realisiert werden. Wenn eine Datenübertragung nicht möglich ist, KANN alternativ eine unmittelbare Meldung des Dienstleisters bei sicherheitsrelevanten Ereignissen mit der Möglichkeit zur nachfolgenden Übersendung der Protokoll- und Protokollierungsdaten sowie der Sekundär-SRE etabliert werden.

d) Sollten einer Partei Erkenntnisse über einen Angriff in Bezug auf die ausgelagerten Infrastrukturen vorliegen, MUSS sichergestellt sein, dass die jeweils andere Partei unmittelbar informiert wird, um gemeinsam reaktive Maßnahmen zu etablieren.

[21] Auslagerung bezieht sich hier auf die Leistungserbringung durch andere verantwortliche Organisationen (Dienstleister, andere Einrichtungen etc.).
[22] Die Datenzuleitungen gemäß der §§ 5 und 5a BSIG sind davon ausgenommen.
[23] Vgl. OPS.1.1.5.A5 Einhaltung rechtlicher Rahmenbedingungen bzw. DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokollierungsdaten, (BSI 2023b)
[24] Vgl. OPS.1.1.5.A8 Archivierung von Protokollierungsdaten, (BSI 2023b)
[25] Die Datenzulieferung gemäß der §§ 5 und 5a BSIG fällt nicht unter diesen Anwendungszweck und ist gemäß des im BSIG beschriebenen Rahmens verpflichtend.

2.2 Protokollierung

PD.2.2.01: Organisatorische und personelle Rahmenbedingungen zur Protokollierung

a) Die organisatorischen und personellen Rahmenbedingungen für die effektive Umsetzung des oben definierten Protokollierungsprozesses, der sich daraus ergebenen Aufgaben für Planen, Sammeln und Dokumentieren sowie für die Umsetzung der Anforderungen dieses Mindeststandards MÜSSEN geschaffen werden.[26]

PD.2.2.02: Planungs- und Dokumentationsphase der Protokollierung

a) Die folgenden Kriterien der Planungsphase werden definiert, um eine angemessene Sichtbarkeit durch die Protokollierung zu erzielen:

i) Die Erschließung von Datenquellen SOLLTE auf Basis der Schutzbedarfsfeststellungen[27] im Informationsverbund priorisiert erfolgen.

ii) Sollten für die im Einsatz befindlichen oder geplanten Detektoren und Detektionssysteme zusätzliche Sichtbarkeiten notwendig sein, MÜSSEN diese erschlossen werden.

iii) Es KÖNNEN „Quick-Wins“[28] in der Protokollierung berücksichtigt werden.

b) Es MUSS sichergestellt werden, dass trotz der Protokollierung die Betriebssicherheit gewährleistet bleibt.

c) Das anfallende Protokoll- und Protokollierungsdatenaufkommen SOLLTE anhand eines repräsentativen Systems pro IT-Systemgruppe[29] bestimmt werden.

d) Bei der Erschließung von Datenquellen MUSS geprüft werden, ob sich das Datenformat für die Detektionssysteme eignet. Es MUSS geprüft werden, ob die Daten normalisiert und, falls erforderlich, durch zusätzliche Informationen angereichert werden müssen.[30] Daraus KÖNNEN sich Normalisierungsregeln für Logformate ableiten.

e) Die Ergebnisse der Planungsphase MÜSSEN in einer geeigneten Dokumentation zusammengefasst werden. Eine geeignete Abstraktion SOLLTE sicherstellen, dass die Dokumentation keinen ständigen Änderungen unterliegt. Die Dokumentation MUSS alle Netzbereiche, die Datenquellen, deren Beziehungen untereinander und den Datenfluss der Protokoll- und Protokollierungsdaten sowie der Sekundär-SRE im Informationsverbund umfassen. Darüber hinaus MUSS für jedes System dokumentiert werden, welche Ereignisse dieses protokolliert. Es SOLLTE eine Gruppierung gleicher Systemgruppen innerhalb der Dokumentation erfolgen.

f) Es MUSS ein Prozess eingerichtet werden, der sicherstellt, dass die Planungsphase bei grundlegenden Veränderungen im Informationsverbund, die Auswirkung auf die Protokollierung und Detektion haben, erneut durchlaufen wird.

g) Jede Einrichtung bzw. im Auftrag der jeweilige IT-Dienstleister des Bundes MUSS eine auf den konkreten Informationsverbund abgestimmte spezifische Sicherheitsrichtlinie für die Protokollierung[31] erstellen.

[26] Vgl. ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit, (BSI 2023b)
[27] Vgl. BSI-Standard 200-2, Kapitel 8.2 Schutzbedarfsfeststellungen, (BSI 2017), S. 104ff.
[28] „Quick-Wins“ sind Datenquellen, die aufgrund der Komplexität, Dokumentation und Erfahrungswerte ohne größere Aufwände für die Protokollierung und Detektion nutzbar gemacht werden können. Die Priorisierung anhand des Schutzbedarfs der Systeme ist weiterhin zu beachten.
[29] Vgl. BSI-Standard 200-2, (BSI 2017), S. 78. Mithilfe der repräsentativen Erhebung können Größe und Umfang der Protokoll- und Protokollierungsdaten bzw. Sekundär-SRE ermittelt werden.
[30] Vgl. OPS.1.1.5.A9 Bereitstellung von Protokollierungsdaten für die Auswertung, (BSI 2023b)
[31] Vgl. OPS.1.1.5.A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung, (BSI 2023b)

PD.2.2.03: Umsetzungsphase der Protokollierung

a) Jede Einrichtung MUSS die Protokoll- und Protokollierungsdaten in einer zentralisierten Protokollierungsinfrastruktur speichern.[32] Die Protokollierungsinfrastruktur SOLLTE in einer physikalisch dedizierten Zone ohne Internetverbindung betrieben werden.[33] Der Zugriff auf die Protokollierungsinfrastruktur sowie die Protokoll- und Protokollierungsdaten MUSS restriktiv konfiguriert und überwacht werden.[34] Die Protokollierungsinfrastruktur MUSS derart dimensioniert werden, dass die protokollierten Ereignisse für die doppelte Dauer der identifizierten Speicherfrist (siehe PD.2.1.04) vorgehalten werden könnten.[35] Die verwaltungsinternen Angebote des Bundes zur Protokollierung SOLLTEN genutzt werden.[36]

b) Vorhandene Konfigurationsvorgaben des BSI SOLLTEN als Basiskonfiguration für die Protokollierung auf IT-System- und Netz-Sicht verwendet werden.[37] Sollten betriebliche Aspekte oder die Geschäftstätigkeit der Einrichtung durch diese Vorgaben eingeschränkt werden, KANN eine abweichende Konfiguration vorgenommen werden. Falls keine Konfigurationsvorgaben des BSI existieren oder abweichende Konfigurationen aufgrund der oben genannten Kriterien vorgenommen werden müssen, MÜSSEN die von den Systemen als sicherheitsrelevant ausgegebenen Ereignisse (Protokoll- und Protokollierungsdaten oder Sekundär-SRE) protokolliert werden. Zusätzliche behördenspezifische Einstellungen KÖNNEN ergänzend vorgenommen werden. Diese Einstellungen DÜRFEN NICHT herstellerspezifische oder intern etablierte Vorgaben zur Protokollierung ersetzen, sondern erweitern diese.

c) Nach erfolgreichem Abschluss der Umsetzungsphase MUSS geprüft werden, ob alle geplanten Datenquellen der Planungs- und Dokumentationsphase erschlossen wurden. Die Kompatibilität der Datenformate, der angestrebte Informationsgehalt (vgl. Sichtbarkeit) sowie die Zeitsynchronisation[38] der Daten MUSS überprüft werden. Sofern erforderlich, MUSS eine Aktualisierung der Dokumentation erfolgen.

PD.2.2.04: Protokollierung aus IT-System-Sicht

a) Die Auslegung der Sichtbarkeiten für die Protokollierung aus IT-System-Sicht MUSS quellenspezifisch entschieden werden.[39] Sollten Konfigurationsvorgaben vom BSI existieren, MÜSSEN diese berücksichtigt werden (siehe PD.2.2.03.b). Um ein einheitliches Schutzniveau zu schaffen, SOLLTEN mindestens aus den folgenden Kategorien Ereignisse protokolliert werden:

- Anlegen und Änderungen von Rechten, Benutzenden und Gruppen,
- Änderungen von Zugangsdaten,
- Anmeldeversuche (erfolgreich und fehlgeschlagen), Abmeldungen und Zugriffe auf System-, Programm- und Dateiressourcen,
- Systemstarts, Neustarts und Herunterfahren,
- Ausführungen von Applikationen, Programmen und Skripten,

[32] Vgl. DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse, (BSI 2023b)
[33] Vgl. OPS.1.1.5.A6 Aufbau einer zentralen Protokollierungsinfrastruktur, (BSI 2023b)
[34] Vgl. OPS.1.1.5.A10 Zugriffsschutz für Protokollierungsdaten, (BSI 2023b)
[35] Aufgrund der Komplexität heutiger Informationsverbünde und vielfältiger Angriffsszenarien ist ein stetiger Anstieg des Protokollierungsvolumens zu erwarten. Eine Dimensionierung gemäß der doppelten Dauer soll sicherstellen, dass die Daten bis zum Ende der Speicherfrist vollständig gespeichert werden können. Eine regelmäßige Überwachung der Speicherkapazitäten unterstützt das Abschätzen des Protokollierungsvolumens.
[36] Die zur Umsetzung verpflichteten Stellen können sich für Informationen zu den verwaltungsinternen Detektionsangeboten an das Bundes Security Operations Center (BSOC) des BSI unter bsoc-kontakt@bsi.bund.de wenden.
[37] Die Konfigurationsvorgaben werden im Rahmen der Beratung des BSOC zu den Detektionsangeboten in der Bundesverwaltung den zur Umsetzung verpflichteten Behörden bereitgestellt.
[38] Vgl. OPS.1.1.5.A4 Zeitsynchronisation der IT-Systeme, (BSI 2023b)
[39] Vgl. OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene, (BSI 2023b)

- Installationen und Deinstallationen,
- Konfigurations- und Systemänderungen,
- Prozessinformationen (z. B. Start, Terminierung und Abhängigkeiten),
- System- / Datei-Integrität,
- Sekundäre sicherheitsrelevante Ereignisse.

Je Datensatz SOLLTEN mindestens die folgenden Informationen[40] erhoben werden, sofern dies möglich ist:

- Zeitstempel,
- Quellsystem, ggf. Benutzer,
- Event-IDs,
- Ereignisinformationen.

b) Auf allen in der Planungs- und Dokumentationsphase identifizierten Systemen MUSS die Protokollierung aktiviert werden. Es SOLLTE dabei NICHT zwischen virtuellen und physischen Systemen unterschieden werden.

c) Für Querschnittsdienste und Fachverfahren MUSS systemabhängig definiert werden, welche Ereignisse protokolliert werden und wie diese in die zentralisierte Protokollierung mit einzubinden sind.

d) Die zu protokollierenden Ereignisse SOLLTEN über die Betriebssystemmittel und/oder über Agenten erfasst werden. Ein Einsatz von Agenten SOLLTE vorab geprüft werden, um die Kompatibilität zur Protokollierungs- und Detektionsinfrastruktur[41] zu gewährleisten.

e) Die Zuordenbarkeit der Protokollierungsdaten zu deren Identitäten MUSS über die Gesamtheit der Speicherdauer gewährleistet werden. Auf IT-Systemebene SOLLTE es dazu eine eindeutige Bezeichnung (z. B. Hostname) geben, mit der die protokollierenden Systeme und deren Daten identifiziert werden können.

PD.2.2.05: Protokollierung aus Netz-Sicht

a) Die Auslegung der Sichtbarkeiten für die Protokollierung aus Netz-Sicht MUSS quellenspezifisch entschieden werden.[42] Sollten Konfigurationsvorgaben vom BSI existieren, MÜSSEN diese berücksichtigt werden (siehe PD.2.2.03.b). Um eine umfassende Sichtbarkeit zu schaffen, SOLLTEN mindestens die folgenden Bereiche protokolliert werden:

- Ein- und ausgehende Kommunikationen an allen Netzgrenzen (über entsprechende IT-Systeme, wie z. B., Proxies, Application Layer Gateways, Router; auch virtuelle Netzgrenzen) der relevanten Stufen aus Netz-Sicht,
- Kommunikation innerhalb von Netzen und zwischen IT-Systemen der relevanten Stufen aus Netz-Sicht,
- SRE der Netzwerkinfrastruktur.

Je Datensatz SOLLTEN mindestens die folgenden Informationen[43] erhoben werden, sofern dies möglich ist:

- Zeitstempel,
- Quellsystem,
- Zielsystem,
- Protokollinformationen.

[40] Für Beispiele zu Formatvorgaben und zu erhebende Informationen können die zur Umsetzung verpflichteten Einrichtungen sich an den Konfigurationsvorgaben (siehe PD.2.2.03.b) orientieren.
[41] Hierzu sollten auch etwaige externe Infrastrukturen (z. B. durch IT-Dienstleister) sowie die Datenzulieferung gemäß der §§ 5 und 5a BSIG berücksichtigt werden.
[42] Vgl. OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene, (BSI 2023b)
[43] Für Beispiele zu Formatvorgaben und zu erhebende Informationen können die zur Umsetzung verpflichteten Einrichtungen sich an den Konfigurationsvorgaben (siehe PD.2.2.03.b) orientieren.

b) Es KÖNNEN zusätzlich Sensoriken eingesetzt werden, die zum Beispiel über Spiegelports (TAPs) die relevanten Protokolldaten aus Netz-Sicht protokollieren.

c) Die Zuordenbarkeit der Protokolldaten zu deren Identitäten MUSS über die Gesamtheit der Speicherdauer gewährleistet werden. Falls eine dynamische Zuordnung von IP-Adressen erfolgt, SOLLTEN zusätzliche Protokollierungsquellen (z. B. der DHCP-Server) erschlossen werden, um die Zuordenbarkeit über die Speicherdauer der Protokolldaten zu garantieren.

d) Es SOLLTE mit geeigneten Maßnahmen (z. B. Reverse-DNS-Abfragen) sichergestellt werden, dass die Protokolldaten der Netz-Sicht den Protokollierungsdaten der IT-System-Sicht zuordenbar sind, sofern dies nicht durch die vorhergehende Maßnahme abgebildet werden kann.

2.3 Detektion

PD.2.3.01: Organisatorische und personelle Rahmenbedingungen zur Detektion

a) Die organisatorischen und personellen Rahmenbedingungen[44] für die effektive Umsetzung des Detektionsprozesses[45], der sich daraus ergebenen Aufgaben für Planen, Kalibrieren, Detektieren, Auswerten und Dokumentieren sowie für die Umsetzung der Anforderungen dieses Mindeststandards MÜSSEN geschaffen werden.

PD.2.3.02: Planungs- und Dokumentationsphase der Detektion

a) Die Einrichtung MUSS eine strategische Vorgehensweise für die Detektion festlegen. Folgende Kriterien sind bei der Festlegung der Vorgehensweise zu berücksichtigen:

i) Zur Bestimmung der Abdeckung SOLLTE eine standardisierte Methodik angewendet werden, die es erlaubt Detektoren und Detektionssysteme zu den Vorgehensweisen von Cyber-Akteuren oder Arten von Cyber-Angriffen (z. B. über Matrizen zu Taktiken und Techniken von Cyber-Angriffen) zuzuordnen.

ii) Es MUSS eine angemessene[46] Abdeckung im Informationsverbund erzielt werden, die auf den theoretisch zu erkennenden Vorgehensweisen von Cyber-Akteuren oder Arten von Cyber-Angriffen basiert. Dazu MÜSSEN die Ergebnisse der Schutzbedarfsfeststellungen der Einrichtung in die Planung einbezogen werden. [47]

iii) Bei der Produktauswahl, der Entwicklung oder dem Einsatz von Detektoren oder Detektionssystemen SOLLTE eine größtmögliche Abdeckung der Detektionsfähigkeit in Bezug auf die Bedrohungslandschaft der Einrichtung erzielt werden.[48]

iv) Es MUSS eine auf den konkreten Informationsverbund abgestimmte spezifische Sicherheitsrichtlinie für die Detektion[49] erstellt werden.

b) Die Einrichtung SOLLTE die verwaltungsinternen Detektionsangebote zur automatisierten Analyse der Protokoll- und Protokollierungsdaten auf sicherheitsrelevante Ereignisse nutzen.[50]

[44] Vgl. DER.1.A7 Schulung von Zuständigen, (BSI 2023b)
[45] Vgl. Abbildung 3
[46] Vgl. BSI-Standard 200-2, (BSI 2017), S. 24ff.
[47] Vgl. DER.1.A16 Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen, (BSI 2023b)
[48] Vgl. BSI-Standard 200-2, Kapitel 8.2 Schutzbedarfsfeststellung, (BSI 2017)
[49] Vgl. DER.1.A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen, (BSI 2023b)
[50] Die zur Umsetzung verpflichteten Stellen können sich für Informationen zu den verwaltungsinternen Detektionsangeboten an das Bundes Security Operations Center (BSOC) des BSI unter bsoc-kontakt@bsi.bund.de wenden.

c) Informationen zu aktuellen technischen Schwachstellen und Angriffsmustern MÜSSEN fortlaufend für die im Informationsverbund eingesetzten Systeme eingeholt werden.[51] Dazu MÜSSEN laufend Meldungen[52] der Hersteller (Hard- und Software), Behörden und Medien geprüft werden.

PD.2.3.03: Umsetzungsphase der Detektion

a) Bei der Umsetzung von Maßnahmen zur Detektion SOLLTE initial eine Kalibrierung durchgeführt werden, um festzustellen, welche SRE im Normalzustand auftreten. Dazu SOLLTE bewertet werden, ob dieser Normalzustand hingenommen werden kann oder, ob die Feststellung genutzt werden sollte Änderungen durchzuführen, um das gewünschte Detektionsergebnis zu erzielen. Die Kalibrierung SOLLTE bei Änderungen innerhalb des Informationsverbunds oder der Bedrohungslage erneut durchgeführt werden.

b) Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Verdachtsfall (qualifizierter SRE) hindeuten. Die zur Detektion eingesetzten Systeme SOLLTEN in eindeutig zuordenbaren Fällen eine automatisierte Auswertung der SRE ermöglichen. Nur Verdachtsfälle DÜRFEN den Prozess der Reaktion auslösen. Die Qualifizierung MUSS in automatisiert nicht eindeutig zuordenbaren Fällen manuell durch die Einrichtung vorgenommen werden. Für die Qualifizierung KÖNNEN weitere Erkenntnisse aus Protokoll- und Protokollierungsdaten sowie anderen SRE notwendig sein. Basierend auf den gewonnenen Erkenntnissen der Auswertung MÜSSEN die Detektionsmechanismen nachjustiert werden.

c) Es SOLLTEN geeignete Evaluierungsprozesse definiert werden, um aus erfolgreich detektierten Vorfällen die notwendigen Maßnahmen zur Vorbeugung derartiger Vorfälle abzuleiten. Insbesondere die Aufarbeitung für die Verbesserung der Threat-Intelligence der Organisation SOLLTE berücksichtigt werden.[53]

d) Es SOLLTEN geeignete Evaluierungsprozesse definiert werden, um die Funktionsweisen der Detektoren und Detektionssysteme fortlaufend zu überprüfen.[54]

PD.2.3.04: Einsatz von Systemfunktionen zur Detektion

a) Der Einsatz von mitgelieferten Systemfunktionen zur Detektion[55] MUSS (z. B. bei Schadcodescannern, Paketfiltern oder Firewalls) umgesetzt werden. Insofern ein Sekundär-SRE festgestellt worden ist, MÜSSEN die protokollierten Ereignisse als zusätzliches Hilfsmittel im Rahmen der Auswertung hinzugezogen werden.

PD.2.3.05: Einsatz zusätzlicher Produkte zur Detektion

a) Bei dem Einsatz zusätzlicher Produkte (z. B. Agenten) zur Detektion[56] sind die folgenden Anforderungen bei der Produktauswahl zu berücksichtigen:

i) Es MUSS sichergestellt sein, dass das Produkt kompatibel zur bestehenden Protokollierungs- und Detektionsinfrastruktur[57] ist.

[51] Vgl. DER.1.A12 Auswertung von Informationen aus externen Quellen, (BSI 2023b)
[52] Dazu können z. B. folgende Quellen herangezogen werden: Warn- und Informationsdienst des CERT-Bund (BSI 2023c), Common Vulnerabilities and Exposures (MITRE 2023), Threat-Intelligence Reporte, Fachpublikationen, Herstellerdokumentationen
[53] Vgl. DER.1.A12 Auswertung von Informationen aus externen Quellen, (BSI 2023b); BSI-Standard 200-3, Kapitel 4 Erstellung einer Gefährdungsübersicht, (BSI 2017a), S. 16ff.
[54] Vgl. DER.1.A13 Regelmäßige Audits der Detektionssysteme sowie DER.1.A18 Durchführung regelmäßiger Integritätskontrollen, (BSI 2023b)
[55] Vgl. DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion, (BSI 2023b)
[56] Vgl. DER.1.A9 Einsatz zusätzlicher Detektionssysteme, (BSI 2023b)
[57] Zum Beispiel muss sichergestellt sein, dass das Produkt die Protokoll- und Protokollierungsdaten oder direkt erzeugte SRE in einem kompatiblen Format zuliefert.

ii) Das Produkt MUSS vollständig autonom auf einem IT-System agieren und Sekundär-SRE protokollieren und/oder die Protokoll- und Protokollierungsdaten zu einem zentralisierten IT-System versenden (analog zur zentralen Protokollierungsinfrastruktur) und dort SRE detektieren.

iii) Das Produkt DARF KEINE Verbindung zu externen Netzen außerhalb des Regierungsnetzes, insbesondere dem Internet, benötigen, um Ergebnisse zu SRE zu kommunizieren. Produktaktualisierungen und der Abgleich von Indikatoren oder Klassifikationen DÜRFEN NUR unidirektional heruntergeladen werden. Alternativ KÖNNEN diese auf einem vom Produkt unabhängigen Weg heruntergeladen und von der Einrichtung eingespielt werden.

PD.2.3.06: Festlegung der Meldewege und Reaktion

a) Es MÜSSEN geeignete Melde- und Alarmierungswege für die sicherheitsrelevanten Ereignisse[58] umgesetzt werden.

b) Dazu MUSS ein geeigneter Prozess zur Reaktion auf begründete Verdachtsfälle geschaffen werden. Dieser MUSS erprobt und regelmäßig geprüft werden, insbesondere die Meldewege zwischen der Detektion und der Reaktion.[59]

[58] Vgl. DER.1.A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse, DER.2.1 Behandlung von Sicherheitsvorfällen und DER.4 Notfallmanagement, (BSI 2023b)

[59] Vgl. DER.1.A17 Automatische Reaktion auf sicherheitsrelevante Ereignisse, (BSI 2023b)

Glossar

Abdeckung

Die Abdeckung bezeichnet die Anzahl der Vorgehensweisen von Cyber-Akteuren oder Arten von Cyber-Angriffen, die durch die Einrichtung theoretisch unter Nutzung der aktuell vorhandenen Detektoren und Detektionssysteme erkannt werden könnten.

Angriffsziel

Angriffe können die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit betreffen.

Detektoren

Ein Detektor ist ein IT-gestütztes Verfahren zur Erkennung von sicherheitsrelevanten Ereignissen. Ein Detektor kann sich auf bekanntes Wissen von schadhaftem Verhalten stützen (vgl. Threat-Intelligence) und über definierte Signaturen oder Muster dieses in Protokoll- und Protokollierungsdaten erkennen. Detektoren können darüber hinaus lernbasiert zur Charakterisierung von anomalem gegenüber normalem Verhalten eingesetzt werden.

Es können auch mehrere Detektoren genutzt werden, um ein Detektionsergebnis zu erhalten.

Detektionssystem

Ein Detektionssystem umschreibt die Kumulierung von Detektoren in einer automatisierbaren Lösung zur Detektion und Analyse von sicherheitsrelevanten Ereignissen. Detektionssysteme können einen spezifischen Anwendungszweck abdecken (z. B. Intrusion Detection System) oder organisationsweite Systeme darstellen (z. B. Security-Information-and-Event-Management). Detektionssysteme können Hilfsmittel zur Analyse und Auswertung von sicherheitsrelevanten Ereignissen liefern.

Fachverfahren

Analog zu „Grobkonzept zur IT-Konsolidierung Bund“, Bundeskabinett, 2015 sowie „Architekturrichtlinie für die IT des Bundes“, Bundesministerium des Innern, 2017

Identitäten

Objekte oder Ereignisse enthalten Identifikationen, d.h. Attribute, Merkmale, Kriterien etc. Diese werden genutzt, um eine eindeutige Abgrenzung zu anderen Objekten zu ermöglichen und auf Objekte oder Ereignisse schnell zugreifen zu können, z. B. anhand eines Hashwertes. In der Praxis kann die Identität die IP-Adresse, der Hostname oder eine andere, eindeutige Systembezeichnung darstellen.

Informationsverbund

Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

IT-Dienstleister

Analog zu „Grobkonzept zur IT-Konsolidierung Bund“, Bundeskabinett, 2015 sowie „Architekturrichtlinie für die IT des Bundes“, Bundesministerium des Innern, 2017

IT-Systemgruppe

IT-Systemgruppen sind das Ergebnis der Gruppenbildung von IT-Systemen (z. B. Arbeitsplatzcomputer (APC), Fileserver, TK-Anlage, DMZ) gemäß der Strukturanalyse, siehe BSI-Standard 200-2, Abschnitt 8.1.[60] Die auf den IT-Systemen laufenden Anwendungen werden mit erfasst.

IT-System-Sicht

Die Daten aus der IT-System-Sicht werden in diesem Mindeststandard als Synonym zu Protokollierungsdaten definiert. Auf allen IT-Systemen fallen Protokollierungsdaten an. Protokollierungsdaten aus IT-System-Sicht enthalten Informationen über die Interaktionen eines Nutzenden („Data-in-Use“) oder allgemeine Zustandsdaten („Data-at-Rest“). Die Ereignisse können aber auch durch automatisierte Prozesse ausgelöst werden. Ereignisse aus IT-System-Sicht können sowohl auf APCs und Servern als auch auf allen Netzkomponenten, wie Routern und Firewalls, auftreten.

Middlebox

Eine Middlebox ist ein netzinternes Gerät, das sich auf dem Pfad zwischen zwei miteinander kommunizierenden IT-Systemen befindet und Paketströme während der Ausführung überwachen, filtern oder umwandeln kann.

Netzbereich

Netzbereiche sind entweder durch einen Router oder L3-Switch erzeugte IP-Segmente, die durch VLANs getrennt sein können, oder Bereiche innerhalb eines Netzes, die durch schwach eingeschränkte Schnittstellen, wie Access Control Lists (ACLs), Paketfilter, netzbasierte Intrusion Detection Systeme oder ähnliches, voneinander getrennt werden.

Netzgrenze

Eine Netzgrenze liegt immer dann vor, wenn ein Netz, das außerhalb der Hoheit der betrachteten Einrichtung liegt, mit dem internen Netz verbunden wird. Dabei ist es irrelevant, welche Schutzmaßnahmen an dieser Netzgrenze getroffen werden. Netzgrenzen liegen auch dann vor, wenn an das interne Netz andere Netze angeschlossen werden, die zwar unter der vollständigen Kontrolle der betrachteten Einrichtung liegen, diese Netze aber aus Überlegungen gleich welcher Art physisch vom Netz getrennt werden und nur über definierte, stark eingeschränkte Schnittstellen (z. B. durch Proxies oder Application Layer Gateways (ALGs)) mit dem internen Netz verbunden wurden.

Netz-Sicht

Die Daten aus der Netz-Sicht werden in diesem Mindeststandard als Synonym zu Protokolldaten definiert. Wenn zwei IT-Systeme miteinander kommunizieren („Data-in-Motion“), dann entstehen netzbasierte Protokolldaten. Bei Netzsystemen (z. B. Switch, Router, Firewall, Load Balancer, IDS) entsteht dadurch eine Besonderheit. Zum einen erzeugen diese Systeme über sich selbst Protokollierungsdaten aus IT-System-Sicht. Zum anderen erzeugen diese IT-Systeme Ereignisse aus Netz-Sicht: Protokolldaten über die Kommunikation zweier anderer IT-Systeme.

Normalisierung

Protokoll- und Protokollierungsdaten können an den unterschiedlichsten Stellen und Systemen innerhalb einer IT-Infrastruktur erhoben werden. Die Folge ist, dass diese Daten in variierenden Formatierungen und (Datentypen-)Formaten vorliegen, sodass eine Vereinheitlichung bzw. Homogenisierung der Daten notwendig sein kann, die auch als Normalisierung bezeichnet wird.

[60] Vgl. BSI-Standard 200-2, (BSI 2017), S. 77ff.

Normalzustand

Der Normalzustand des zu überwachenden Netzes wird durch den zeitlichen Vergleich des Auftretens der protokollierten Ereignisse festgestellt. Er beschreibt typische, angenommene gutartige Zustände und Kommunikationen im zu überwachenden Netz. Dies schließt z. B. Zustandsdaten, verwendete Kommunikationsprotokolle, statistische Betrachtungen von Kenngrößen wie Rate und Größe der Pakete, sowie wiederkehrende Abhängigkeiten (Tag-/Nacht, Wochenenden, Wartungsfenster, Ferienzeiten) ein. Die statistischen Kenngrößen der Protokoll- und Protokollierungsdaten können zudem kurzzeitige Spitzenwerte aufweisen, die durch automatisierte Prozesse hervorgerufen werden können. Die wiederkehrenden Abhängigkeiten beziehen sich auf Tag-Nacht-Zyklen, Werktage, Wochenruhetage und jahreszeitliche Abhängigkeiten.

Protokolldaten

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

Protokollierung

Protokollierung ist insbesondere das automatische Speichern von Ereignissen sowie deren Bereitstellung für eine kontinuierliche Auswertung.

Protokollierungsdaten

Protokollierungsdaten sind gemäß § 2 Abs. 8a BSIG Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme.

Querschnittsdienst

Analog zu „Grobkonzept zur IT-Konsolidierung Bund“, Bundeskabinett, 2015 sowie „Architekturrichtlinie für die IT des Bundes“, Bundesministerium des Innern, 2017

Reaktion

Die Reaktion umfasst alle vorgegebenen und erprobten Verfahren zur Behandlung von Sicherheitsvorfällen einschließlich derer Bestätigung.[61] Sie folgt auf die Erkennung (Detektion) von Verdachtsfällen. Darauf aufbauend können IT-Forensik und das Notfallmanagement eingesetzt werden.[62] Die Erkenntnisse aus der Reaktion können wieder in die vorgelagerten Prozesse dieses Mindeststandards mit einfließen, um die gewählten Maßnahmen zu verbessern.

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 Datenquellen auf IT-System- und Netz-Sicht, deren Daten durch die Einrichtung gesammelt werden.

Die Qualität der Sichtbarkeit bezeichnet die Positionierung der Punkte der Erhebung (wie z. B. Sensoren) sowie die Konfiguration der Datenquellen. Die Qualität wird bestimmt durch die Fähigkeit, ausgewählte Angriffe theoretisch erkennen zu können (z. B. kann Lateral Movement nur eingeschränkt an den

[61] Vgl. DER.2.1 Behandlung von Sicherheitsvorfällen, (BSI 2023b)

[62] Vgl. DER.2.2 Vorsorge für die IT-Forensik, DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle, DER.4 Notfallmanagement, (BSI 2023b)

Netzgrenzen erkannt werden), sowie das Vorliegen sämtlicher notwendiger Informationen aus unterschiedlichen Quellen zur Bewertung (z.B. IP-Adresse, pDNS, DHCP-Logs, DNS-Logs des betroffenen Endsystems, statt nur einer IP-Adresse der Firewall).

Threat-Intelligence

Threat-Intelligence umfasst Wissen, Fähigkeiten und erfahrungsbasierte Informationen über das Auftreten und die Bewertung von Cyber-Angriffen. Dies dient dem Verständnis und der Einordnung der häufigsten und schwerwiegendsten Bedrohungen von außen (Zero-Day, APT, Exploits etc.), um geeignete Schutzmaßnahmen ableiten zu können.

Verdachtsfall

Ein Verdachtsfall ist das Ergebnis aus der positiven Qualifizierung von Primär- oder Sekundär-SRE. Bei einem Verdachtsfall liegt eine Bewertung vor, dass in der untersuchten Datenmenge schadhafter Inhalt und / oder anomales Verhalten entdeckt worden ist. Somit ist davon auszugehen, dass es sich um einen Angriff handelt, sodass ein Verdachtsfall ein Initiator für den Reaktionsprozess darstellt.

Virtuelle Netzgrenze

Eine virtuelle Netzgrenze liegt immer dann vor, wenn ein internes Netz (einschließlich der IT-Systeme) auf der gleichen Hardware bereitgestellt wird wie ein anderes Netz, welches nicht in der Hoheit der betrachteten Einrichtung liegt oder aus anderen Überlegungen vom internen Netz getrennt werden soll. Obwohl kein Routing zwischen diesen Netzgrenzen konfiguriert ist, grenzen die Netze über alle IT-Systeme aneinander, welche die Virtualisierung bereitstellen.

Literaturverzeichnis

BMI (2017) Bundesministerium des Innern und für Heimat: Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html

BSI (2017) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0, https://www.bsi.bund.de/dok/10027846

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, https://www.bsi.bund.de/dok/10027822

BSI (2023a) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, https://www.bsi.bund.de/dok/mst-faq

BSI (2023b) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Edition 2023, https://www.bsi.bund.de/gs-kompendium
- OPS.1.1.5 Protokollierung: https://www.bsi.bund.de/dok/1073634
- DER.1 Detektion von sicherheitsrelevanten Ereignissen: https://www.bsi.bund.de/dok/1073616

BSI (2023c) Bundesamt für Sicherheit in der Informationstechnik: Warn- und Informationsdienst von CERT-Bund, https://wid.cert-bund.de

DIN (2018) Deutsches Institut für Normung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://tools.ietf.org/html/rfc2119

MITRE (2023) MITRE Corporation: Common Vulnerabilities and Exposures, https://cve.mitre.org

Abkürzungsverzeichnis

bDSB	behördliche Datenschutzbeauftragte
BDSG	Bundesdatenschutzgesetz
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSOC	Bundes Security Operations Center
DIN	Deutsches Institut für Normung e.V.
DSGVO	(Europäische) Datenschutz-Grundverordnung
FAQ	Frequently Asked Questions
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
ISB	Informationssicherheitsbeauftragte
IT-SiBe	IT-Sicherheitsbeauftragte
MST	Mindeststandard
MST PD	Mindeststandard zur Protokollierung und Detektion von Cyber-Angriffen
RFC	Request for Comments
SRE	Sicherheitsrelevantes Ereignis
UP	Umsetzungsplan