Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0a vom 25.02.2021

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	15.10.2018	Erstveröffentlichung
1.0a	25.02.2021	Anpassungen von Verlinkungen

Tabelle 1: Versionsgeschichte des Mindeststandards zur Protokollierung und Detektion von Cyber-Angriffen

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

Inhaltsverzeichnis

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die nationale Cyber-Sicherheitsbehörde erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[1] und IT-Betriebspersonal.

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 den Mindeststandards 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.[2] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes 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 Stellen des Bundes[3] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Analog „Informationssicherheitsbeauftragte (ISB)“
[2] Zur standardisierten Vorgehensweise siehe BSI (2017a), https://www.bsi.bund.de/mindeststandards
[3] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Behörde“ verwendet.

1 Beschreibung

Dieser Mindeststandard regelt die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen (SRE), um ein zielgerichtetes und gemeinsames Vorgehen zur Erkennung und Abwehr von Cyber-Angriffen auf die Kommunikationstechnik des Bundes (§ 2 Abs. 3 S. 1 BSIG) zu etablieren.[4]

Der Mindeststandard dient insbesondere den IT-Leitern und IT-SiBe als Grundlage für die Einforderung und Umsetzung von organisatorischen und technischen Maßnahmen. Personalverantwortliche ermitteln und stellen hierfür die erforderlichen personellen Ressourcen bereit.

Der Mindeststandard setzt auf die IT-Grundschutz-Methodik des BSI zum Management der Informationssicherheit auf.[5] Er gilt für alle Schutzbedarfskategorien. Sicherheitsanforderungen zur Protokollierung und Detektion ergeben sich daher insbesondere aus dem IT-Grundschutz-Kompendium[6], der Protokollierungsrichtlinie Bund (PR-B)[7] und dem Rahmendatenschutzkonzept (RDSK)[8].
Abbildung 1 stellt die Zusammenhänge grafisch dar.

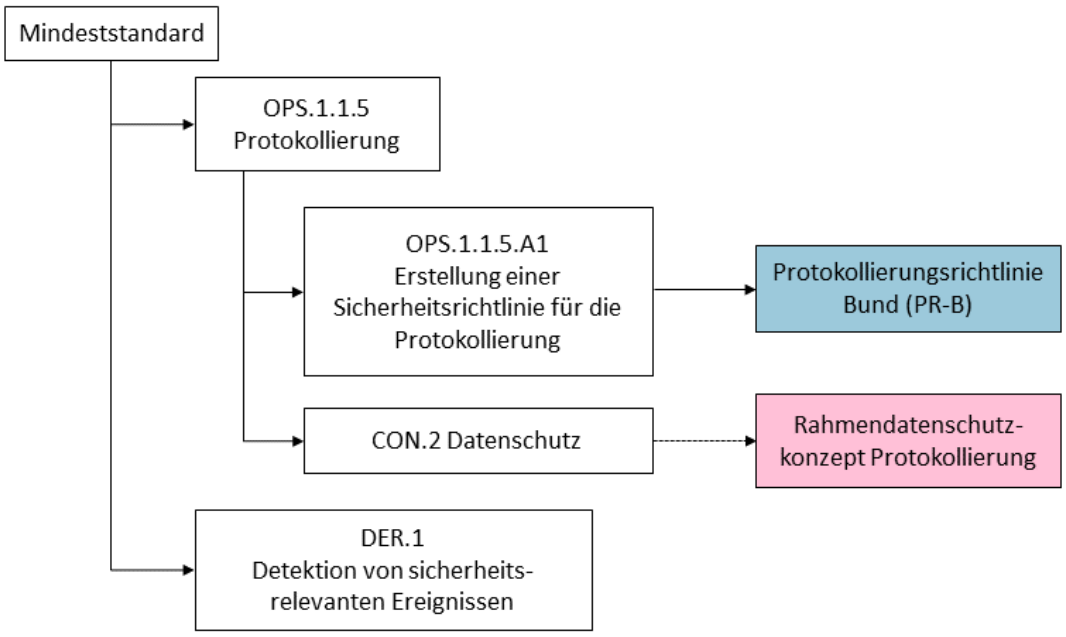

Abbildung 1: Zusammenspiel Mindeststandard und IT-Grundschutz-Bausteine

Für eine gemeinsame Basis und Anwendung werden zunächst besonders relevante Begriffe in den Kapiteln 1.1 bis 1.40 festgelegt. Weitere Begriffe, die nicht bereits aus dem IT-Grundschutz hervorgehen, sind im Glossar beschrieben und definiert.

Kapitel 2 setzt dann Sicherheitsanforderungen an die korrekte Umsetzung der Protokollierung und Detektion in den internen Netzen und den damit verbundenen Demilitarisierten Zonen (DMZ) der Behörden.

[4] Regelungsbereich ist das interne Netz und den damit verbundenen Demilitarisierten Zonen (DMZ) einer Behörde. Übergreifende Netze unterliegen im Regelfall gesonderten Regelungen, die im Einzelnen mit den zuständigen Stellen im BSI abzustimmen sind.
[5] Vgl. BSI (2017b), S. 1f.
[6] Vgl. BSI (2017c), S. 1ff.
[7] Siehe PR-B
[8] Siehe RDSK

1.1 Protokollierungsereignisse

Als Protokollierungsereignis wird jedes Ereignis bezeichnet, dessen Auftreten mit diesem Mindeststandard und der PR-B als verbindlich zur Erhebung definiert wird. Protokollierungsereignisse werden zur Abgrenzung zunächst in Rohereignisse (Kapitel 1.1.1) und sicherheitsrelevante Ereignisse (Kapitel 1.1.2) eingeteilt. Abbildung 2 stellt die Aufteilung und Zusammenhänge grafisch dar, die nachfolgend weiter beschrieben werden.[9]

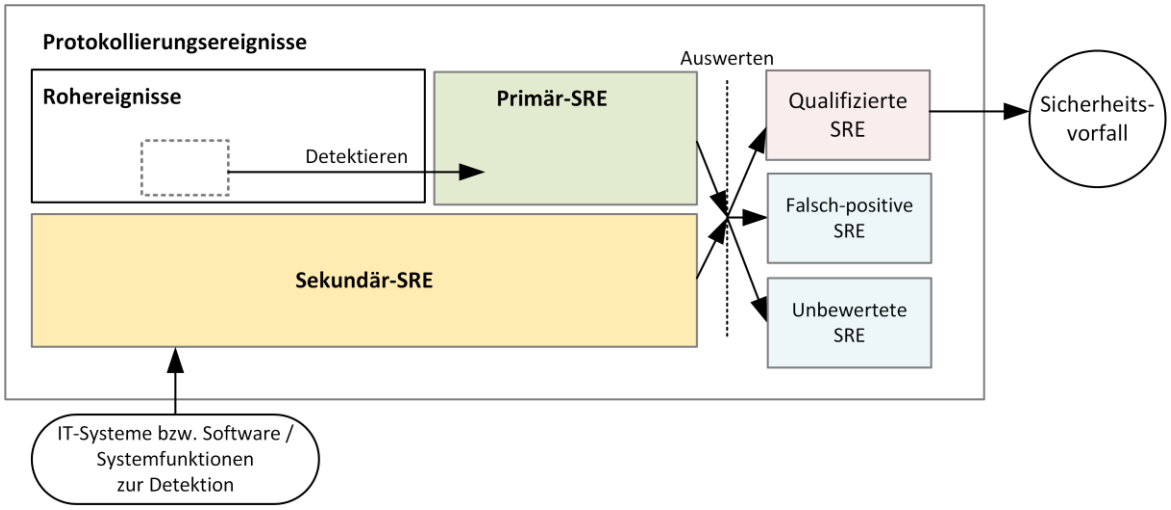

Abbildung 2: Mengendiagramm der verschiedenen Ereignisarten

1.1.1 Rohereignisse

Rohereignisse (engl. log events) sind Protokollierungsereignisse, die aus sich selbst heraus noch keinen Hinweis auf Vorliegen eines Sicherheitsvorfalls ergeben. Erst im Zusammenspiel mit anderen Informationen (z. B. anderen Rohereignissen oder Kontextinformationen) lässt sich erschließen, dass ein Sicherheitsvorfall existieren könnte. Rohereignisse und deren Erhebung werden ausführlich in der PR-B definiert. Sie stellen die Basis zur Detektion fortgeschrittener Angriffe dar. Gleichzeitig bieten sie die Grundlage zur effizienten Auswertung von primären sicherheitsrelevanten Ereignissen und zur Reaktion auf Sicherheitsvorfälle.

1.1.2 Sicherheitsrelevante Ereignisse

Sicherheitsrelevante Ereignisse (engl. security events) sind Protokollierungsereignisse, die Auswirkungen auf die Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) haben können.[10] Sie werden in primäre und sekundäre sicherheitsrelevante Ereignisse eingeteilt, wobei diese Einteilung sich auf den Ursprung des Protokollierungsereignisses und nicht auf dessen Relevanz oder Wichtigkeit bezieht.

Primäre sicherheitsrelevante Ereignisse

Über verschiedene Verfahren zur Detektion werden in Rohereignissen sicherheitsrelevante Ereignisse erkannt. Diese werden als primäre sicherheitsrelevante Ereignisse (Primär-SRE) bezeichnet. Primär-SRE beinhalten damit immer einen direkten Bezug auf einzelne oder mehrere Rohereignisse, welche der Auslöser für das Primär-SRE war.

[9] Erläuterungen für die Auswertung der primären und sekundären sicherheitsrelevanten Ereignisse erfolgen im Rahmen der Detektion (Kapitel 1.3).
[10] BSI (2017c), S. 271ff.

Sekundäre sicherheitsrelevante Ereignisse

Sekundäre sicherheitsrelevante Ereignisse (Sekundär-SRE) sind Protokollierungsereignisse, die aus IT-Systemen bzw. Software zur Detektion stammen (z. B. Protokollierungsereignisse der Schadsoftware-erkennung oder eines Intrusion Detection Systems). Ebenso gehören hierzu Protokollierungsereignisse von Systemfunktionen zur Detektion (z. B. Protokollierungsereignisse über die Verletzung der Regeln einer Betriebssystemfirewall oder einer dedizierten Firewall).

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

1.2 Protokollierung

Abbildung 3 stellt die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen als kontinuierliche Prozesse dar. Dieser besteht für die Protokollierung aus den Aktivitäten *Planen, Dokumentieren und Sammeln*. Die Detektion mit den Aktivitäten *Kalibrieren, Detektieren* und *Auswerten* bildet die Brücke zwischen den Prozessen der Prävention und Reaktion, wodurch ein übergreifender Regelkreis entsteht.

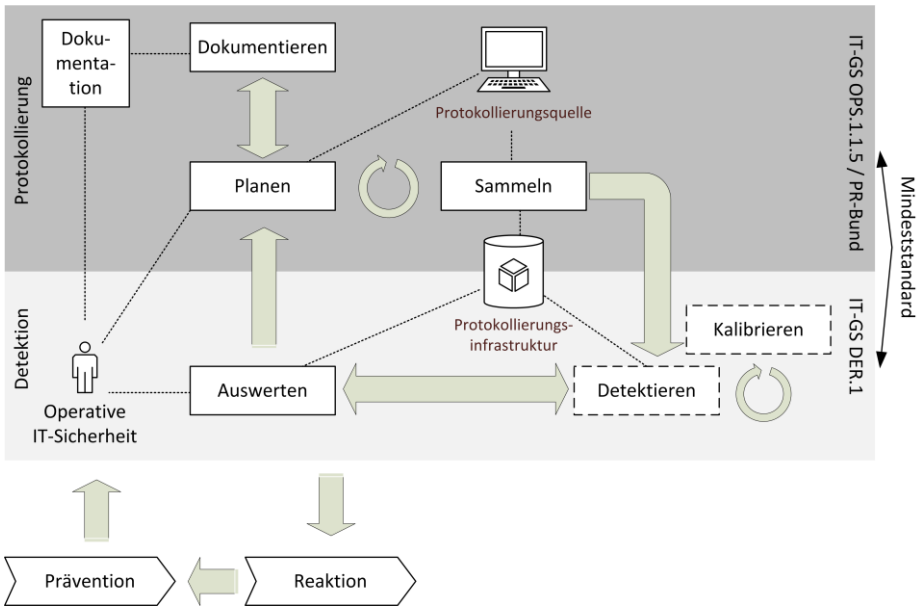

Abbildung 3: Kontinuierliche Prozesse Protokollierung und Detektion

Planen

Die Aktivität *Planen* dient dazu, alle Protokollierungsquellen zu identifizieren, welche Protokollierungsereignisse liefern. Ebenso ist zu planen, wie diese Protokollierungsereignisse 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 solches sowie für die betriebenen Protokollierungsquellen. Im Zuge der Planung erfolgt eine Schutzbedarfsfeststellung[11] der Daten, um die Absicherung der zentralen Protokollierungsinfrastruktur angemessen vorzunehmen. Anhaltspunkte für die Bestimmung des Schutzbedarfes finden sich in der Anforderung PRB.I.7.1.1.6 der PR-B (Anlage 1) und dem Rahmendatenschutzkonzept (Anlage 2).

[11] Gem. BSI (2017b), S. 72f.

Dokumentieren

Die Ergebnisse der Planungsaktivität werden in einer Protokollierungslandkarte dokumentiert.[12] Die Landkarte dient als gemeinsame Kommunikationsgrundlage für die Aufgabenbereiche *Operative IT-Sicherheit* (Kapitel 1.4.1*)*, *IT-Betrieb* (Kapitel 1.4.2) und *User Help Desk* zur Interpretation der Protokollierungsereignisse. Im Anschluss an Planung und Dokumentation erfolgt die Umsetzung (u. a. durch das Sammeln der Protokollierungsereignisse). Diese erfolgt in mehreren Iterationen, da ggf. auch noch Änderungen an den IT-Systemen oder der IT-Infrastruktur erforderlich sind, um gewisse Protokollierungsereignisse erfassen zu können. Diese Aktivitäten müssen regelmäßig wiederholt werden, um sich an Veränderungen der IT anpassen zu können.

Sammeln

Die Aktivität *Sammeln* beschreibt den automatisierten Prozess, um an Protokollierungsquellen erzeugte Protokollierungsereignisse zur zentralen Protokollierungsinfrastruktur zu übertragen und dort zu speichern. Diese Aktivität beinhaltet auch eine kontinuierliche Überwachung der zentralen Protokollierungsinfrastruktur auf Fehlerzustände und wird bereits während der Umsetzung der Planung etabliert. Es kann erforderlich sein, zusätzliche IT-Systeme oder Software einzuführen, damit die bei der Planung als erforderlich identifizierten Protokollierungsereignisse gesammelt bzw. übertragen werden können.

1.3 Detektion

Der vollständige Prozess der Detektion beinhaltet die Aktivitäten *Kalibrieren, Detektieren* und *Auswerten*. Zur besseren Handhabung der Aufwände und der Komplexität wird in der Version 1.0 des Mindeststandards zunächst ein vereinfachter Prozess vorgegeben (siehe gestrichelte Aktivitäten *Kalibrieren* und *Detektieren* in Abbildung 3). Die Sicherheitsanforderungen hierzu sind in Kapitel 2.3 aufgeführt. Gesamtheitlich betrachtet wird der Prozess wie folgt zu gestalten sein:

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 dies hingenommen werden muss oder ob die Feststellung des Auftretens dazu genutzt werden sollte, den Informationsverbund 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 gekoppelt. Die Aktivität Kalibrieren kann auch für Sekundär-SRE erforderlich sein. Hier sind dann die Anforderungen des jeweiligen eingesetzten Produktes zu berücksichtigen.

Detektieren

Durch das Kalibrieren werden die verwendeten Verfahren zu Detektion (Detektoren, basierend auf Regeln oder statistischen Kenngrößen) 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. Während der fortlaufenden Detektion identifizieren die Detektoren aus den gesammelten Rohereignissen Primär-SRE.

Auswerten

Die Primär- und Sekundär-SRE müssen überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (engl. incident) hindeuten (siehe Abbildung 2). Nach der Auswertung ist nicht mehr zwischen Primär- oder Sekundär-SRE zu unterschieden. Unter dem Aspekt der Auswertung sind die SRE dann wie folgt einzuteilen:

[12] Siehe PR-B, Anhang A: Beispiele zur Erstellung einer Protokollierungslandkarte

- Qualifizierte SRE: Hinweis auf einen Sicherheitsvorfall
- Falsch-positive SRE: das SRE wurde irrtümlicherweise erzeugt; dies ist insbesondere bei Primär-SRE sehr häufig der Fall
- Unbewertete SRE: das SRE wurde nicht ausgewertet, da eine Klärung aus zeitlichen oder Kostengründen nicht möglich ist

Nur qualifizierte SRE lösen den Prozess der Reaktion[13] 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* (Kapitel 1.4.1) und *IT-Betrieb* (Kapitel 1.4.2) / *User Help Desk* ab. Kommt die *Operative IT-Sicherheit* zu dem Ergebnis, dass ein Sicherheitsvorfall vorliegt, sind diese Erkenntnisse unverzüglich in den Prozess der Reaktion zu geben. Basierend auf den Erkenntnissen der *Operativen IT-Sicherheit* (Kapitel 1.4.1) wird zusammen mit dem *IT-Sicherheitsmanagement* die Planung der zu protokollierenden Ereignisse kontinuierlich an die Erfordernisse der Behörde angepasst. Basierend auf den gewonnenen Erkenntnissen müssen auch die Detektoren nachjustiert werden, um die Anzahl an falsch-positiven SRE stetig zu reduzieren.

1.4 Aufgabenbereiche

Aus den Prozessen *Protokollierung* (Kapitel 1.2) und *Detektion* (Kapitel 1.3) ergeben sich die in Abbildung 4 dargestellten Aufgaben.

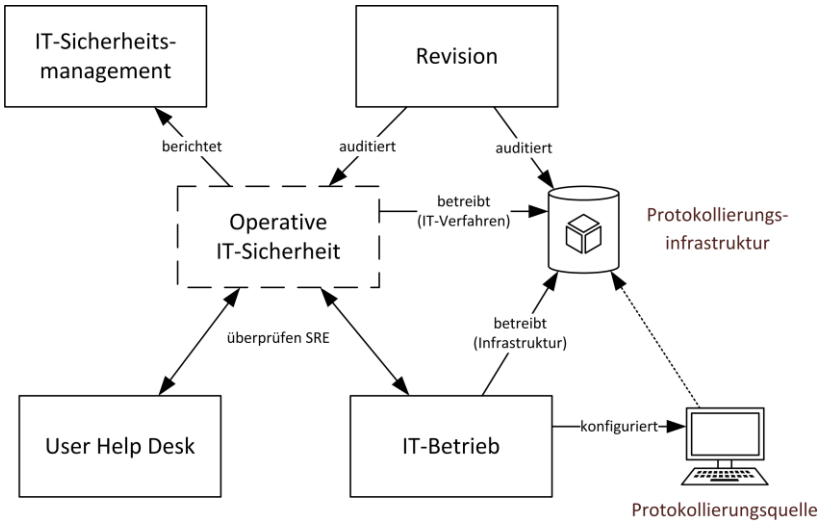

Abbildung 4: Übersicht Aufgabenbereiche

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

1.4.1 Operative IT-Sicherheit

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

[13] Außerhalb des Regelungsbereiches dieses Mindeststandards, siehe dazu insbesondere DER.2.1 *Behandlung von Sicherheitsvorfällen* in BSI (2017c), S. 279ff.

Diese übernimmt neben der Daueraufgabe, SRE auszuwerten, insbesondere die Verantwortung für die Prozesse *Protokollierung* und *Detektion*. Hier sind insbesondere die initiale und stetige Planung der Protokollierung inklusive der Spezifikation der zentralen Protokollierungsinfrastruktur und die Kalibrierung sowie die Justierung der Detektoren hervorzuheben. Die Protokollierungsinfrastruktur selbst ist auch als IT-Verfahren zu betrachten und benötigt daher einen Verfahrensadministrator. Mit Blick auf eine durchgängige Aufgabentrennung sollte der Verfahrensadministrator grundsätzlich dem Aufgabenbereich *Operative IT-Sicherheit* zugeordnet sein. Bei der Wahrnehmung der Aufgaben sind die im konkreten Einzelfall relevanten gesetzlichen Regelungen insbesondere der EU-Datenschutz-Grundverordnung (DSGVO) und des BDSG sowie ggf. des Fernmeldegeheimnisses zu beachten (siehe Anlage 2).

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 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 Protokollierungsereignisse gering zu halten. Der Aufgabenbereich *Operative IT-Sicherheit* muss weiterhin ein grundlegendes technisches Verständnis der gesamten IT-Infrastruktur besitzen. Anhand der Protokollierungslandkarte und den aufkommenden Protokollierungsereignissen muss sie sich orientieren, um die auftretenden Protokollierungsereignisse 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 Behörde bestehen.

Der Aufgabenbereich der *Operativen IT-Sicherheit* berichtet an das *IT-Sicherheitsmanagement* alle Ergebnisse der Auswertung (auch wenn es zu keinem Sicherheitsvorfall kommt). Diese Informationen können vom *IT-Sicherheitsmanagement* in die Planung und Ausgestaltung von zukünftigen präventiven Maßnahmen einfließen.

1.4.2 IT-Betrieb

Der Betrieb der IT-Infrastruktur der zentralen Protokollierungsinfrastruktur sollte durch den *IT-Betrieb* erfolgen, um Synergieeffekte nutzen zu können. Die *Operative IT-Sicherheit* als Verfahrensadministrator sollte bei Planung, Projektierung, Produktentscheidung, Installation und späterem Betrieb mitwirken.

Die erforderliche IT-Infrastruktur für die zentrale Protokollierungsinfrastruktur besteht im Regelfall aus verteilten IT-Systemen. Hierzu bedarf es erfahrener Administratoren, die sich auf den Betrieb verteilter IT-Systeme spezialisieren können. Idealerweise kann hier auf vorhandene Betriebskenntnisse in der Behörde zurückgegriffen werden, so dass der erforderliche Aufwand minimiert wird. Die zentrale Protokollierungsinfrastruktur sollte ganzheitlich als Protokollierungssystem für alle Bereiche der Behörde 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.

1.4.3 Revision

Die regelmäßige Auditierung der zentralen Protokollierungsinfrastruktur, die ggf. erforderliche De-Pseudonymisierung von Protokollierungsereignissen 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 Behörde organisatorisch festgelegt ist, erfolgt die Revision im Auftrag der behördlichen Datenschutzbeauftragten (bDSB) und/oder des Personalrates, um festzustellen, ob die Protokollierungsdaten missbräuchlich ausgewertet wurden.

2 Sicherheitsanforderungen

Abbildung 5 stellt den Rahmen des Mindeststandards grafisch dar. Die Version 1.0 bildet die fachliche Grundlage und legt den Schwerpunkt auf die Anforderungen zur Protokollierung (Kapitel 2.2).

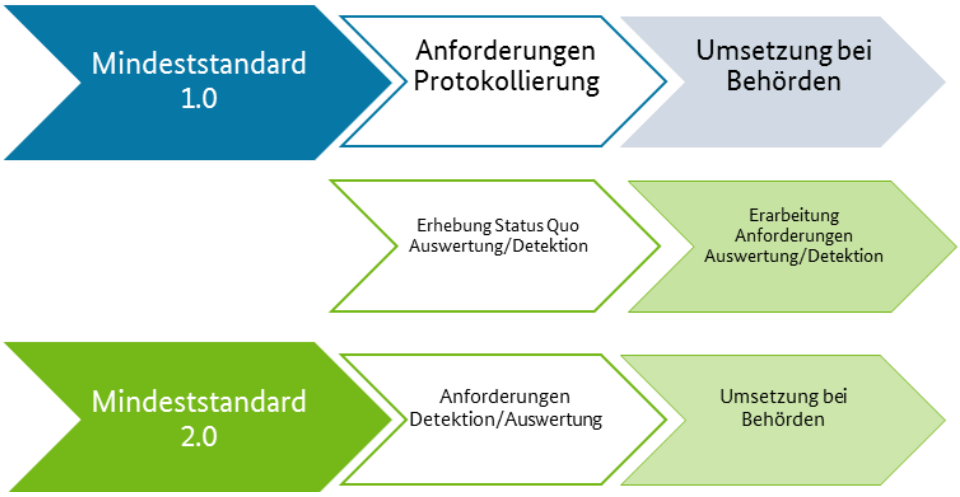

Abbildung 5: Umsetzung der Versionen 1.0 und 2.0

Während der Umsetzung der Version 1.0 durch die Behörden erhebt das BSI den Status Quo in Bezug auf Auswertung und Detektion bei den Behörden. Die daraus resultierenden Anforderungen gehen in den Mindeststandard der künftigen Version 2.0 ein. Dieser wird insbesondere um die detaillierten Anforderungen an die Detektion vervollständigt.

2.1 Allgemeine Anforderungen

Nachfolgende allgemeine Anforderungen setzen die Grundvoraussetzungen für eine wirksame Umsetzung der prozessualen Anforderungen für die Protokollierung (Kapitel 2.2) und Detektion (Kapitel 2.3).

PD.2.1.01: Aufgabenbereiche

Zuständigkeit und Verantwortung für die Aufgabenbereiche *Operative IT-Sicherheit*, *IT-Betrieb* und *Revision* sind im Sinne dieses Mindeststandards verbindlich festzulegen. Hierfür bietet sich der Geschäftsverteilungsplan einer Behörde an.

PD.2.1.02: Einzelbehörden

Einzelbehörden haben die Basis- und Standardanforderungen der IT-Grundschutz-Bausteine OPS.1.1.5 *Protokollierung* und DER.1 *Detektion von sicherheitsrelevanten Ereignissen* umzusetzen.

PD.2.1.03: Behörden mit erhöhten Sicherheitsbedürfnissen und IT-Dienstleister des Bundes

Behörden mit erhöhten Sicherheitsbedürfnissen (BmeS) und IT-Dienstleister des Bundes haben zusätzlich die Anforderungen bei erhöhtem Schutzbedarf der IT-Grundschutz-Bausteine OPS.1.1.5 *Protokollierung* und DER.1 *Detektion von sicherheitsrelevanten Ereignissen* umzusetzen.

Tabelle 1 stellt die mit diesem Mindeststandard geltenden Dokumente dar, welche detailliertere Anforderungen ausführen.

Dokument	Art	Inhalt	Zielgruppe
Protokollierungsrichtlinie Bund, Version 2.0	Richtlinie	Detaillierte technische Anforderungen zur Protokollierung im Sinne der Basisanforderung OPS.1.1.5.A1 *Erstellung einer Sicherheitsrichtlinie für die Protokollierung*. Die Vorgaben sind auf interne Netze und angeschlossene DMZen bis zum Einstufungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH anzuwenden.	IT-Fachkräfte, IT-SiBe
OPS.1.1.5 *Protokollierung*	IT-Grundschutz-Baustein	Standard- und Basisanforderungen	IT-Fachkräfte, IT-SiBe
DER.1 *Detektion von sicherheitsrelevanten Ereignissen*	IT-Grundschutz-Baustein	Standard- und Basisanforderungen	IT-Fachkräfte, IT-SiBe
Rahmendatenschutzkonzept Protokollierung und Detektion von Cyber-Angriffen auf die Bundesverwaltung, Version 1.0	Leitlinie	Mit der BfDI abgestimmtes Konzept aus dem die jeweiligen Datenschutzkonzepte für die Umsetzung der Protokollierung und Detektion abgeleitet werden können.	bDSB

Tabelle 1: Übersicht relevante Dokumente mit Zielgruppen

2.2 Protokollierung

Die Implementierung der zentralen Protokollierung erfolgt in zwei Phasen: Planungs- und Dokumentationsphase und Umsetzungsphase. Diese Phasen können mehrfach durchlaufen werden, bis eine vollständige Protokollierung implementiert ist.

PD.2.2.01: Anforderungen an die Planungs- und Dokumentationsphase

Es werden alle IT-Systemgruppen identifiziert, die Protokollierungsereignisse liefern. Dies umfasst auch die Identifizierung von erforderlichen Anpassungen an der IT-Infrastruktur, damit Protokollierungsereignisse geliefert werden können. Das anfallende Protokollierungsdatenaufkommen wird anhand eines repräsentativen Systems pro IT-Systemgruppe bestimmt. Dabei wird berücksichtigt, dass trotz der Protokollierung die Betriebssicherheit gewährleistet bleibt. Sollten sich bei den repräsentativen Systemen diesbezüglich Auffälligkeiten ergeben, müssen die Protokollierungsanforderungen angepasst werden.

Liegt eine vollständige Risikoanalyse für alle Fachverfahren der Behörde vor und wurden die kritischen Geschäftsprozesse identifiziert, so kann alternativ basierend auf dieser Risikoanalyse die Umsetzung der Anforderungen auf IT-Systemebene schrittweise realisiert werden.

Die Ergebnisse der Planungsphase werden in einer Protokollierungslandkarte[14] zusammengefasst. Eine geeignete Abstraktion stellt sicher, dass die Protokollierungslandkarte keinen ständigen Änderungen unterliegt. Es wird ein Prozess eingerichtet, der sicherstellt, dass die Planungsphase bei Veränderungen im Informationsverbund (Changes) erneut durchlaufen wird.

PD.2.2.02: Anforderungen an die Umsetzungsphase

Begonnen wird mit der Umsetzung der Anforderungen[15] auf Netz-Ebene von Außen (Netzgrenzen) nach Innen (Netzbereiche). Hierdurch ist sichergestellt, dass alle Datenabflüsse und Kommunikationen zwischen kompromittierten IT-Systemen erfasst werden[16].

[14] Beschreibungen und Anforderungen hinsichtlich der Protokollierungslandkarte siehe PR-B, Teil II
[15] Siehe Anforderungen in PR-B, Teil III
[16] Es ist nicht zu empfehlen, in einer Iteration der Umsetzungsphase alle Protokollierungsquellen einzurichten.

Im Anschluss werden die Anforderungen[17] an die IT-Systeme, ausgehend von den zentralen Authentisierungs- und Autorisierungsdiensten über die Clients zu den Servern und den Fachverfahren implementiert.

Nach erfolgreichem Abschluss der Umsetzungsphase wird geprüft, ob alle geplanten Protokollierungsquellen der Protokollierungslandkarte umgesetzt wurden. Sofern erforderlich erfolgt eine Aktualisierung der Protokollierungslandkarte.

PD.2.2.03: Anforderungen an die Implementierung der Protokollierung

Als Mindestanforderungen für die Protokollierung sind die Anforderungen aus der PR-B umzusetzen. Diese konkretisiert insbesondere die Basisanforderung OPS.1.1.5.A1 *Erstellung einer Sicherheitsrichtlinie für die Protokollierung*[18] und regelt in diesem Zusammenhang die folgenden Themenbereiche:

- Grundlegende Protokollierungsanforderungen (z. B. Zeitsynchronisation, rechtliche Rahmenbedingungen, Aufbau einer zentralen Protokollierungsinfrastruktur)
- Planung und Dokumentation
- Konkretisierung der Anforderung OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene*[19]

Aufbauend auf der PR-B erstellt jede Behörde bzw. im Auftrag die jeweiligen IT-Dienstleister des Bundes eine auf den konkreten Informationsverbund abgestimmte spezifische Sicherheitsrichtlinie für die Protokollierung.

2.3 Detektion

Ein zur Erkennung von Cyber-Angriffen genutzter Sensor ist der Mensch. Dieser Sensor funktioniert, sofern er regelmäßig ausreichend sensibilisiert ist, ihm bekannt ist, dass er Auffälligkeiten melden muss und er das Gefühl hat, dass die entgegennehmende Stelle diese Meldungen ernst nimmt.

PD.2.3.01: Festlegung der Meldewege

Aus diesem Grund muss die Basisanforderung DER.1.A3 *Festlegung von Meldewegen für sicherheitsrelevante Ereignisse*[20] umgesetzt werden.

PD.2.3.02: Sensibilisierung der Mitarbeiter

Weiterhin muss DER.1.A4 *Sensibilisierung der Mitarbeiter*[21] im Sinne des obigen Absatzes mit diesem Mindeststandard umgesetzt werden. Den Mitarbeitern muss ihre Rolle als Sensor bewusst sein.

PD.2.3.03: Einsatz von Systemfunktionen zur Detektion

Die in der Basisanforderung DER.1.A.5 *Einsatz von mitgelieferten Systemfunktionen zur Detektion*[22] definierten Anforderungen müssen ebenfalls mit diesem Mindeststandard umgesetzt werden. Danach betrifft dies unter anderem die regelmäßige Auswertung der Protokollierungsdaten der Schadcodescanner, der Protokollierungsereignisse der Paketfilter und der Firewalls.

Zur Erfüllung dieser Anforderungen müssen die Aktivitäten *Kalibrieren* und *Detektieren* auf den Protokollierungsdaten noch nicht erfolgen (siehe gestrichelte Aktivitäten *Kalibrieren* und *Detektieren* in Abbildung 3). Sowohl die Mitarbeiter als auch die Schadcodescanner liefern SRE, welche die *Operative IT-Sicherheit* auswertet. Die zentral protokollierten Ereignisse werden in diesem Fall anlassbezogen als zusätzliches Hilfsmittel im Rahmen der Auswertung hinzugezogen. Basierend auf diesen Erfahrungen können die Aktivitäten Kalibrieren und Detektieren erprobt werden.

[17] Siehe Anforderungen in PR-B, Teil IV
[18] Vgl. BSI (2017c), S. 211
[19] Vgl. BSI (2017c), S. 212
[20] Vgl. BSI (2017c), S. 273
[21] Vgl. BSI (2017c), S. 273f.
[22] Vgl. BSI (2017c), S. 274

Es wird empfohlen, die organisatorischen und personellen Rahmenbedingungen für den vollständigen Detektionsprozess (siehe Kapitel 1.3) bereits nach der Veröffentlichung des Mindeststandards in seiner Version 1.0 zu schaffen.

PD.2.3.04: Einsatz von zusätzlichen Produkten zur Detektion

Zusätzliche Produkte können der Erkennung von Phasen eines Cyber-Angriffs nach erfolgter Erstkompromittierung eines IT-Systems dienen, welche über die Systemfunktionen zur Detektion und Schadsoftwareerkennung hinausgehen. Funktionale Anforderungen an die Detektionsfähigkeiten derartiger Produkte werden mit der Version 2.0 dieses Mindeststandards veröffentlicht.

Erwägt eine Behörde schon jetzt den Einsatz solcher zusätzlichen Produkte, so müssen folgende Anforderungen bei der Produktauswahl mindestens Berücksichtigung finden:

- Das Produkt muss ausschließlich IT-System-basiert sein und darf grundsätzlich nicht in die Netzkommunikation eingreifen.
- Es muss sichergestellt sein, dass das Produkt kompatibel zu bestehenden Produkten zur Detektion ist.
- Das Produkt muss entweder vollständig autonom auf einem IT-System agieren und Sekundär-SRE protokollieren oder die Rohereignisse zu einem zentralisierten IT-System protokollieren (analog zur zentralen Protokollierungsinfrastruktur) und dort SRE detektieren.
- Die Information darüber, ob ein fortgeschrittener Cyber-Angriff in einer Behörde vorliegt, unterliegt dem Geheimschutz. Aus diesem Grund darf das Produkt keine Verbindung zu externen Netzen außerhalb des Regierungsnetzes, insbesondere dem Internet, benötigen. Dies gilt auch für Produktaktualisierungen und den Abgleich von Indikatoren oder Klassifikationen (engl. threat intelligence). Aktualisierungen und Threat Intelligence müssen daher auf einem vom Produkt unabhängigen Weg heruntergeladen und eigenständig von der Behörde eingespielt werden können.
- Das Produkt darf nicht selbstständig den Cyber-Angriff unterbinden und Veränderungen an den betroffenen IT-Systemen vornehmen. Hierdurch können unter Umständen forensische Beweise vernichtet und der Angreifer gewarnt werden, so dass dieser seine Vorgehensweise ändert und weiterhin unentdeckt bleibt.

Glossar

Angriffsziel

Angriffe können Vertraulichkeit, Integrität und Verfügbarkeit betreffen.

Behörde mit erhöhten Sicherheitsbedürfnissen (BmeS)

Grundsätzlich geht dieser Mindeststandard davon aus, dass es sich bei BmeS um Sicherheitsbehörden, IT-Dienstleister des Bundes oder Aufsichtsbehörden für Betreiber kritischer Infrastrukturen handelt. Im Allgemeinen entscheidet der Leiter eines Ressorts/ einer Behörde, ob es sich um eine Behörde mit erhöhten Sicherheitsbedürfnissen handelt.

Einzelbehörde

Als Einzelbehörden werden all jene Behörden bezeichnet, welche nicht durch die Eigenschaften einer BmeS gekennzeichnet sind und keine IT-Verfahren für andere Behörden anbieten.

Fachverfahren

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

Internes Netz

Als internes Netz wird das Netz bezeichnet, welches unter der vollständigen Kontrolle der betrachteten Einrichtung liegt. Alle Netzübergänge müssen logisch und physisch abgesichert sein. Insbesondere darf kein Zugriff von außerhalb erfolgen (ausgenommen zugelassene verschlüsselte Verbindungen).

Inventarisierungssystem

Hiermit werden alle Produkte zusammengefasst, welche unter anderem automatisiert den Informationsverbund bzw. Teile des Informationsverbunds (z. B. installierte Software einschließlich Versionsnummer, Nutzerkonten, IT-Systeme) dokumentieren.

IT-Dienstleister

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

IT-Systemgruppe

Gruppenbildung von IT-Systemen (z. B. Arbeistplatzcomputer (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.

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 Proxys oder Application Layer Gateways/ALGs) mit dem internen Netz verbunden wurden.

Normalzustand

Der Normalzustand des zu überwachenden Netzes wird durch den zeitlichen Vergleich des Auftretens der Protokollierungsereignisse festgestellt. Er beschreibt die typische, angenommen gutartige Kommunikation im zu überwachenden Netz. Dies schließt 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 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.

Schwachstellenerkennungssystem

System zur Erkennung von Schwachstellen, die für mögliche Angriffe ausgenutzt werden können (z.B. OpenVAS).

Protokollierung

Protokollierung ist insbesondere das automatische Speichern von Ereignissen, sowie deren Bereitstellung für eine kontinuierliche Auswertung.[23]

Protokollierungsdaten

Protokollierungsdaten (engl. log files) sind Mengen von Protokollierungsereignissen. Detaillierte Ausführungen dazu siehe PR-B.

Protokollierungslandkarte

Die Protokollierungslandkarte ist eine Darstellung des internen Netzes und der angeschlossenen DMZen. Die Darstellung erfolgt aus Perspektive der Protokollierungsquellen, welche dort jeweils für ein IT-System zusammengefasst werden. Als Ergebnis der Planung wird sie für die Analyse der Protokollierungsereignisse benötigt.

Protokollierungsquelle

Protokollierungsquellen sind Prozesse auf IT-Systemen, welche Protokollierungsereignisse, insbesondere Rohereignisse erzeugen. Beispiele: Syslog, Eventlog, Anwendungslog usw.

Querschnittsdienst

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

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.

[23] Vgl. BSI (2017c), S. 228ff.

Anlagen

1. Protokollierungsrichtlinie Bund (PR-B) – Protokollierung zur Detektion von Cyber-Angriffen auf die Informationstechnik des Bundes, einschließlich der Umsetzungsrichtlinie zu § 5 Abs. 1 Satz 1 Nr. 1 i. V. m. Satz 4 BSIG, Version 2.04
2. Rahmendatenschutzkonzept Protokollierung und Detektion von Cyber-Angriffen auf die Bundesverwaltung (RDSK), Version 1.0

Literaturverzeichnis

BMI (2017) Bundesministerium des Innern: Umsetzungsplan Bund 2017, Leitlinie für Informationssicherheit in der Bundesverwaltung, Berlin 2017

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Frage: "Wie werden Mindeststandards entwickelt?", https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/FAQ_MST/faq_mst_node.html, abgerufen am 25.02.2021

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – *IT-Grundschutz-Methodik*, Version 1.0, Bonn 2017

BSI (2017c) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, 1. Edition 2018, Bonn 2018

Abkürzungsverzeichnis

ACL	Access Control List (engl.)
ALG	Application Layer Gateway (engl.)
APC	Arbeitsplatzcomputer
bDSB	behördliche Datenschutzbeauftragte
BmeS	Behörden mit erhöhten Sicherheitsbedürfnissen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
DMZ	Demilitarisierte Zone
ISB	Informationssicherheitsbeauftragte / Informationssicherheitsbeauftragter
IT-SiBe	IT-Sicherheitsbeauftragte / IT-Sicherheitsbeauftragter
SRE	Sicherheitsrelevante Ereignisse
PR-B	Protokollierungsrichtlinie Bund
RDSK	Rahmendatenschutzkonzept Protokollierung und Detektion von Cyber-Angriffen auf die Bundesverwaltung
VLAN	Virtual Local Area Network (engl.)

Bundesamt
für Sicherheit in der
Informationstechnik

Protokollierungsrichtlinie Bund (PR-B)

Protokollierung zur Detektion von Cyber-Angriffen auf die Informationstechnik des Bundes, einschließlich der Umsetzungsrichtlinie zu § 5 Abs. 1 Satz 1 Nr. 1 und i. V. m. Satz 4 BSIG – Version 2.04

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: protokollierungsrichtlinie@bsi.bund.de
Internet: https://www.bsi.bund.de

Zusammenfassung

Protokollierungsdaten sind historische Aufzeichnungen über die Art und Weise, wie IT-Systeme genutzt wurden und wie diese miteinander kommuniziert haben. Aus diesen Daten gehen nicht nur Erkenntnisse über Fehlerzustände der IT-Systeme oder des Netzes hervor. Basierend auf diesen Daten lassen sich vergangene Cyber-Angriffe rekonstruieren und laufende erkennen, welche alle sonstigen Sicherheitsmaßnahmen umgangen haben. Um die Protokollierungsdaten effektiv zu diesem Zweck zu nutzen, ist eine Planung der zu sammelnden Ereignisse und die Speicherung in einem zentralen System die grundlegende Vorbedingung.

Die Protokollierungsrichtlinie Bund (PR-B) detailliert den Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen [MST-PD], um dadurch konkrete Anforderungen für die Protokollierung sowohl hinsichtlich der Planung und Dokumentation als auch hinsichtlich der Protokollierung für die IT-System- und Netz-Sicht festzulegen. Die PR-B konkretisiert die im Baustein OPS.1.1.5 des IT-Grundschutz-Kompendiums [ITGS-KOMP] enthaltene Basisanforderung OPS.1.1.5.A1 *Erstellung einer Sicherheitsrichtlinie für die Protokollierung*. Teil III der PR-B stellt die Umsetzungsrichtlinie für die Erhebung von behördeninternen Protokolldaten gem. § 5 Abs. 1 Satz 1 Nr. 1 und i. V. m. Satz 4 BSIG dar.

Zusätzlich hat das BSI technische Informationen für gängige Systeme erarbeitet. Diese VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Dokumentations- und Konfigurationsdateien können über den internen Bereich der Webseiten der Informationssicherheitsberatung von Behörden bezogen werden.

Die zu protokollierenden Ereignisse in dieser Version der Richtlinie dienen der Erkennung von Cyber-Angriffen. Für eine vollständige Protokollierung nach dem Baustein OPS.1.1.5 müssen seitens der Behörde auch die Protokollierungszwecke Betriebssicherheit und Datenschutz Berücksichtigung finden. Die Vorgaben dieser Richtlinie sind auf interne Netze und angeschlossene DMZen bis zum Einstufungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH anzuwenden. Darüber hinaus oder für andere Netze müssen diese Anforderungen durch die Behörde ergänzt werden.

Aufbauend auf dieser Richtlinie erstellt jede Behörde der Bundesverwaltung oder im Auftrag die jeweiligen IT-Dienstleister des Bundes eine auf den konkreten Informationsverbund abgestimmte spezifische Sicherheitsrichtlinie für die Protokollierung.

Im Fokus der PR-B steht eine ganzheitliche Protokollierung, unabhängig vom Schutzbedarf einzelner Fachverfahren. Die protokollierten Ereignisse können sowohl zur Reaktion auf, als auch zur Detektion und Verifikation von Cyber-Angriffen verwendet werden. Mit der Umsetzung dieser Richtlinie leistet die Behörde einen wesentlichen Beitrag zur Detektion von Advanced Persistent Threats (APT).

Es werden protokolliert:

- Verkehrsflüsse zwischen den IT-Systemen einer Behörde und externen Netzen
- Interne Verkehrsflüsse zwischen IT-Systemen einer Behörde
- Ereignisse auf IT-Systemen einer Behörde

Inhaltsverzeichnis

Einleitung

1 Aufbau

Die Richtlinie ist in vier Teile gegliedert. An dieser Stelle wird ein kurzer Überblick über alle Teile der Richtlinie gegeben.

Teil I spezifiziert grundlegende Anforderungen an die Protokollierung, wie z. B. die Speicherfrist und die Verwendung eines einheitlichen Zeitservers.

Teil II beschreibt die Planung und standardisierte Dokumentation der Protokollierung. Durch eine sorgfältige Planung wird sichergestellt, dass wichtige Aspekte bei der Protokollierung nicht vergessen werden. Die standardisierte Arbeitsweise soll es zudem erlauben, ein einheitliches Vorgehen im Rahmen der Detektion von Cyber-Angriffen und der Reaktion auf Cyber-Angriffe in der gesamten Bundesverwaltung zu erreichen.

Teil III beschreibt, welche Protokollierungsereignisse aus Netz-Sicht erfasst werden müssen und an welcher Stelle diese erhoben werden können. **Zugleich ist dieser Teil die Umsetzungsrichtlinie für die gesetzliche Verpflichtung der Bundesbehörden, den Zugang des BSI zu behördeninternen Protokolldaten sicherzustellen (§ 5 Abs. 1 Satz 1 Nr. 1 und i. V. m. Satz 4 BSIG).**

Teil IV beschreibt, welche Protokollierungsereignisse aus IT-System-Sicht erhoben werden müssen.

Alle referenzierten Dokumente sind im Kapitel Referenzdokumente

aufgeführt. Begriffe, die nicht aus dem Glossar des IT-Grundschutzes hervorgehen und speziell in dieser Richtlinie definiert wurden, finden sich im Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen [MST-PD] und Rahmendatenschutzkonzept Protokollierung und Detektion von Cyber-Angriffen auf die Bundesverwaltung [RDSK-PD].

2 Anforderungen und verwendete Notationen und Kennzeichnungen

In der gesamten Richtlinie werden Anforderungen eindeutig durch eine Identifikationsnummer am Zeilenanfang kenntlich gemacht. Der Aufbau ist wie folgt:

PRB.{Kürzel des Teils}.{Fortlaufende Nummer} [OPT | EVAL | ALT | BmeS | ITDL]

Anforderungen ohne Ergänzung in eckigen Klammern sind *verbindlich* von allen Behörden einschließlich IT-Dienstleistern des Bundes und Behörden mit erhöhten Sicherheitsbedürfnissen umzusetzen.

Die Ergänzungen bedeuten folgendes:

- **[OPT]:** Diese Anforderung kann optional umgesetzt werden.
- **[ALT]:** Diese Anforderung stellt eine Alternative zu einer anderen Anforderung dar. Das heißt, die Behörde kann zwischen diesen Alternativen wählen. Eine der Alternativen muss umgesetzt werden.
- **[EVAL]:** Diese Anforderung befindet sich noch in der Evaluierung. Dies bedeutet, dass die Anforderung zwar grundsätzlich verbindlich umgesetzt werden muss, allerdings geht das BSI hier von Rückfragen und noch erforderlichen Konkretisierungen bei der Umsetzung aus. Hier ist das BSI auf den Dialog mit den Behörden angewiesen, um die Anforderungen so zu gestalten, dass einerseits das Ziel der Anforderung erreicht wird, anderseits die Umsetzbarkeit durch die Behörden gewahrt bleibt.
- **[BmeS]:** Diese Anforderung ist verpflichtend für IT-Dienstleister des Bundes und Behörden mit erhöhten Sicherheitsbedürfnissen umzusetzen. Sie ist optional für Einzelbehörden.
- **[ITDL]:** Diese Anforderung ist verpflichtend für IT-Dienstleister des Bundes. Sofern anwendbar, kann sie auch von Einzelbehörden oder von Behörden mit erhöhten Sicherheitsbedürfnissen umgesetzt werden.

Verweise auf das IT-Grundschutz-Kompendium, Edition 2018 [ITGS-KOMP] werden durch Angabe des Namens des Bausteins referenziert. „OPS“ steht hierbei für den Betrieb, „SYS“ für IT-Systeme, „DER“ für Detektion und Reaktion und „NET“ für Netze und Kommunikation.

3 Definition und Abgrenzung von Protokollierungsdaten

Protokollierungsdaten 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. Daher erfolgt im [RDSK-PD] eine Herleitung der notwendigen Abgrenzung zwischen Protokollierungsdaten aus der IT-System-Sicht und der Netz-Sicht. Protokollierungsdaten aus der IT-System-Sicht entsprechen hierbei den Zuständen „Data-at-Rest“ und „Data-in-Use“, Protokollierungsdaten aus der Netz-Sicht hingegen dem Zustand „Data-in-Motion“.

Hierbei ist darauf hinzuweisen, dass diese Sichten nicht in allen Aspekten mit der Einteilung des IT-Grundschutzes in SYS (IT-Systeme) und NET (Netze und Kommunikation) übereinstimmen. Abbildung 1 stellt die verschiedenen Sichten im Kontext einer in der Komplexität stark reduzierten Beispiel-IT dar.

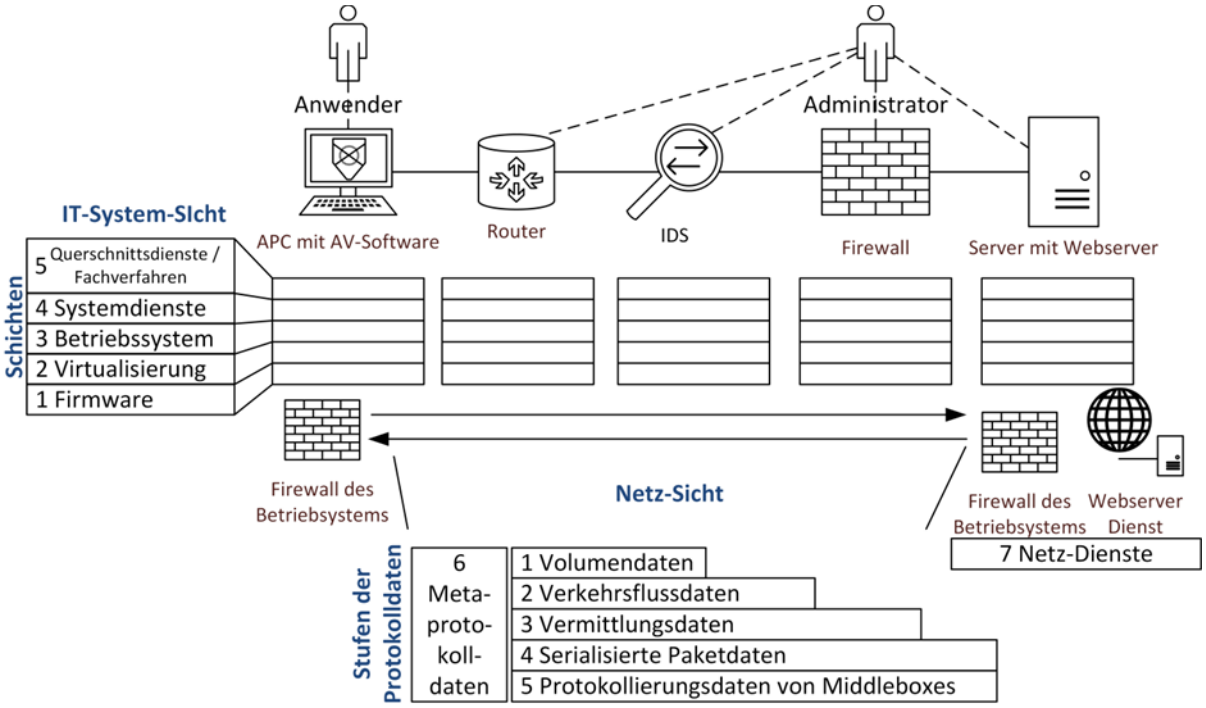

Abbildung 1: Detaillierte Darstellung der Sichten auf Protokollierungsdaten

Protokollierungsdaten aus IT-System-Sicht: Auf allen IT-Systemen fallen Protokollierungsdaten an. Ereignisse aus IT-System-Sicht enthalten Informationen über die Interaktion eines Anwenders mit einem IT-System (z. B. „Nutzer X hat sich erfolgreich authentifiziert.“) oder die eines Administrators mit einem IT-System (z. B. „Nutzer Y hat erfolgreich administrative Rechte erhalten.“). Die Ereignisse können aber auch durch automatisierte Prozesse ausgelöst werden. Ereignisse aus IT-System-Sicht können sowohl auf PCs und Servern als auch auf allen Netzkomponenten wie Routern und Firewalls auftreten (siehe Abbildung 1). Typische Kategorien, in die sich diese Protokollierungsdaten einordnen lassen, sind für Microsoft Windows z. B. Warning, Error, Critical oder unter Linux die Logs in auth.log, boot.log, secure.log. Daneben können auch Meta-Daten über Inhaltsdaten auf dem IT-System protokolliert werden, z. B. Hash-Werte (zur Integritätssicherung).

Die Protokollierungsdaten aus IT-System-Sicht lassen sich in Schichten organisieren (Abbildung 1). Eine Beschreibung dieser Schichten findet sich in Kapitel 3.1. Die Anforderungen an die Protokollierung finden sich nach Schichten organisiert in Teil IV.

Protokollierungsdaten aus Netz-Sicht (Protokolldaten § 2 Abs. 8 BSIG*):* Wenn zwei IT-Systeme miteinander kommunizieren (im Beispiel in Abbildung 1 der APC mit dem Webserver), dann entstehen netzbasierte Protokollierungsdaten bzw. so genannte Protokolldaten. Bei Netzsystemen (z. B. Switch, Router, Firewall, Load Balancer, IDS) entsteht dadurch eine Besonderheit. Zum einen liefern diese Systeme über sich selbst Protokollierungsdaten aus IT-System-Sicht (siehe Beispiel oben). Zum anderen liefern diese IT-Systeme Ereignisse aus Netz-Sicht: Protokolldaten über die Kommunikation zweier anderer IT-Systeme. Diese Besonderheit gilt eingeschränkt auch für die IT-Systeme selbst (z. B. Web- und Mailserver, Browser und Mail-Client, lokale Firewall, Netzschnittstellenkarte).

Die Protokollierungsdaten aus Netz-Sicht werden in dieser Richtlinie in Stufen organisiert. Je höher die Stufe desto mehr Informationen über die Kommunikation sind in den Protokollierungsdaten enthalten (dies ist in Abbildung 1 durch die Länge der Balken angedeutet). Eine Beschreibung der Stufen findet sich in Kapitel 3.2. Die Anforderungen an die Protokollierung aus Netz-Sicht finden sich in Teil III.

3.1 Protokollierungsdaten aus IT-System-Sicht

Die in Abbildung 1 dargestellten Schichten der IT-System-Sicht werden im Folgenden detaillierter beschrieben:

1. *Firmware:* Sämtliche auf der Schicht der Firmware anfallenden Protokollierungsdaten, welche auf eine Kompromittierung des Hostsystems hindeuten. Die erhobenen Protokollierungsdaten können sowohl eigenständig als auch im Kontext von Protokollierungsdaten auf höheren Schichten Rückschlüsse auf den Zustand des Gesamtsystems zulassen.
2. *Systembasierte Virtualisierung (in Abgrenzung zu prozessbasierter Virtualisierung):* Die auf dieser Schicht anfallenden Protokollierungsdaten dienen dazu, eine mögliche Kompromittierung des Host-Systems festzustellen und die Zuverlässigkeit der Protokollierungsdaten aus Netz-Sicht, die in der Virtualisierung erhoben werden, zu bestimmen. Da virtualisierte Systeme in den meisten Bundesbehörden 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 Schicht dienen der Detektion von Cyber-Angriffen, welche auf eine oder mehrere Komponenten des Betriebssystems abzielen. Ein typischer Angriff, welcher auf dieser Schicht anzusiedeln ist, ist die Ausnutzung von Schwachstellen in Betriebssystemkomponenten für eine Kompromittierung. Im Kontext betrachtet können die Protokollierungsdaten für eine Bewertung der Phase des Angriffs herangezogen werden.
4. *Systemdienste*: Unter Systemdiensten sind in dieser Protokollierungsrichtlinie 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 Schicht dienen dazu, eine Kompromittierung dieser essentiellen Dienste festzustellen. Als Beispiele für Systemdienste werden an dieser Stelle Authentisierungs- und Verzeichnisdienste, Datei- und Speicherdienste oder Druck- und Dokumentendienste angeführt.
   Hinweis: Wie zuvor beschrieben gibt es manche Dienste auf den IT-Systemen (z. B. lokale Firewall oder lokale Webserver), welche der Netz-Sicht zuzuordnen sind. Diese werden im Teil III der Protokollierungsrichtlinie behandelt.
5. *Querschnittsdienste und Fachverfahren*: Die Protokollierungsdaten werden abhängig von den vom Fachverfahren angebotenen Möglichkeiten erhoben.

3.2 Protokollierungsdaten aus Netz-Sicht (Protokolldaten)

Die in Abbildung 1 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 Bezeichnungen der IT-Systeme der 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, Zielport über einen definierten Zeitraum identisch sind. Da Port-Nummern keine eindeutige Identifizierung von Applikationen ermöglichen, können auch weitere Informationen über die Art der Kommunikation zu diesem 4-Tupel hinzugefügt werden. In dieser Richtlinie wird der Begriff „Flow“ als Synonym für Verkehrsflussdaten benutzt. Diese Verkehrsflussdaten können z. B. aus NetFlow-Daten generiert

werden. Zur Umsetzung der Anforderungen für Stufe 2 muss auf allen IT-Systemen der Vermittlungsschicht zwischen den identifizierten Netzbereichen die Erzeugung von Netflow der Version 5 oder 9 aktiviert werden. Alternativ dazu kann auch IPFIX verwendet werden.
Die Aktivierung der Konfiguration ist erst dann erforderlich, sobald das BSI die Daten anfordert. Möchte die Behörde die Daten zur Detektion von Cyber-Angriffen selbstständig (d. h. nicht durch das BSI) auswerten, dann wird ein Netflow-Kollektor mit Angriffs-Erkennungsmodul benötigt. Derzeit kann das BSI hierzu keine Empfehlungen aussprechen.

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. Zur Erfüllung der Anforderungen für Stufe 3 ist die Einrichtung von TAPs oder Spiegelports ausreichend. Dem BSI muss auf Nachfrage der Zugang gewährt 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 (z. B. Suricata) generiert werden. Die 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).
Zur Erfüllung der Anforderungen für Daten der Stufe 4 ist die Einrichtung der TAPs oder der Spiegelports ausreichend. Dem BSI muss auf Nachfrage der Zugang gewährt werden.
Möchte die Behörde selbst die TAPs und/oder Spiegelports zur Angriffserkennung verwenden, existieren verschiedene Systeme (angefangen bei klassischen netzbasierten Intrusion Detection Systemen), welche basierend auf diesen Daten eine Angriffserkennung durchführen. Derzeit kann das BSI hierzu keine Empfehlung aussprechen.

5. *Protokollierungsdaten von Middleboxes (z. B. RFC 3234):* Serialisierte Paketdaten können nur durch das Mitschneiden des Verkehrs erzeugt werden; häufig sind bereits aber schon IT-Systeme im Einsatz, welche den Verkehr terminieren und zum eigentlichen Zielsystem neu aufbauen. Hierzu zählen z. B. Web-Proxys, E-Mail-Gateways und sonstige Application Layer Gateways. Bei diesen Systemen spricht man auch von Middleboxes. Derartige Systeme 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 und häufig kann nur die Anfrage protokolliert werden.
Zur Umsetzung der Anforderungen für Stufe 5 muss bei HTTP-verarbeitenden Systemen sichergestellt sein, dass sämtliche HTTP-Header und Post-Requests geloggt werden.

6. *Metaprotokolldaten:* Protokolldaten dieser Stufe werden von Systemen als Analyse eines Kommunikationsvorgangs erzeugt (z. B. die Spam-Score Klassifizierung einer E-Mail). Typischerweise sind dies unmittelbar Sekundär-SRE, wie z. B. ein IDS-Alarm zu einem IP-Paket oder die Information, dass eine Verbindung am Paketfilter geblockt wurde.
Die PR-B sieht derzeit in dieser Stufe die Erhebung aller Sekundär-SRE vor. Welche Ereignisse hier protokolliert werden, ergibt sich aus den bei den Behörden im Einsatz befindlichen Systemen.

7. *Netz-Dienste auf IT-Systemen*: Wie zuvor in Kapitel 3.1 beschrieben, gibt es Systemdienste, welche der Netz-Sicht zugeordnet werden. Dies ist immer dann der Fall, wenn der Dienst Teil eines Kommunikationsvorgangs bildet, z. B. (Front-End-)Webserverdienste oder die Betriebssystem-Firewall. Bezüglich der Protokollierung müssen hier Daten analog zu den Stufen 5 und 6 erhoben werden.

Teil I Grundlegende Protokollierungsanforderungen

1 Prüfung der Vorbedingungen und Erweiterung der Richtlinie

Diese Richtlinie legt die Protokollierungsanforderungen für interne Netze und angeschlossene DMZen bis zur freigegebenen Verarbeitung von VS-NUR FÜR DEN DIENSTGEBRAUCH fest. Zudem wird angenommen, dass die folgenden Vorbedingungen erfüllt sind:

- Die vom BSI formulierten Nutzerpflichten für die Netze des Bundes (NdB) werden umgesetzt.[1]
- Der Mindeststandard des BSI für Schnittstellenkontrollen [MST-SSK] wird umgesetzt.

PRB.I.1.1.1.1 Sind diese Vorbedingungen nicht oder nur zum Teil erfüllt, muss diese Richtlinie durch die jeweilige Behörde um zusätzliche zu protokollierende Ereignisse entsprechend einer Risikoanalyse erweitert werden.

PRB.I.1.1.1.2 Vor Konfiguration der Protokollierungsquellen gem. Teil III und Teil IV dieser Richtlinie muss geprüft werden, ob vom BSI bereits systemspezifische Dokumentations- und Konfigurationsdateien erstellt wurden. Falls diese verfügbar sind, müssen diese als Basiskonfiguration verwendet werden, zusätzliche behördenspezifische Einstellungen können ergänzend vorgenommen werden. Diese VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Dokumentations- und Konfigurationsdateien können von jeder Bundesbehörde über den internen Bereich der Webseiten der Informationssicherheitsberatung von Behörden bezogen werden.

Folgende Werkzeuge und Informationen erleichtern die Umsetzung der Richtlinie:

- Es existiert eine Übersicht, welche Netze Dritter an das interne Netz oder die DMZen angeschlossen sind.
- Es liegt ein aktueller Netzplan des internen Netzes sowie der DMZen vor. Dieser ergibt sich z. B. aus der Strukturanalyse gem. BSI-Standard 200-2 [ITGS200-2].
- Es existiert eine Configuration Management Database (CMDB); alternativ hierzu ist auch ein IP-Adress- und Namenskonzept in maschinenlesbarer Form (z. B. CSV, XML) hilfreich.
- Es findet eine automatisierte Inventarisierung (evtl. einschließlich einer Schwachstellenerkennung) des Netzes und der angeschlossenen IT-Systeme statt.

2 Zeitsynchronisation der IT-Systeme (OPS.1.1.5.A4)

Eine über alle Behörden synchronisierte Zeit ist ausschlaggebend für eine effektive Detektion basierend auf den erhobenen Protokollierungsdaten.

PRB.I.2.1.1.1 Alle Protokollierungsquellen werden auf die gesetzliche Deutsche Zeit synchronisiert (z. B. DCF77, GNSS wie Galileo, Cäsium-Uhr oder NdB-NTP). Der Zeitstempel der Ereignisse ist so konfiguriert, dass er die verwendete Zeitzone protokolliert.

PRB.I.2.1.1.2 [ALT] Alternativ kann die Behörde UTC als Zeitzone für alle Protokollierungsquellen festlegen. Es entfällt dann die Protokollierung der Zeitzone. Diese Festlegung muss in der Protokollierungslandkarte dokumentiert werden.

[1] Gem. UP Bund 2017 werden diese Nutzerpflichten zukünftig als eigenständiger Mindeststandard nach § 8 BSIG veröffentlicht.

3 Aufbau einer zentralen Protokollierungs-infrastruktur (OPS.1.1.5.A6)

PRB.I.3.1.1.1 Jede Behörde errichtet in einer physikalisch dedizierten Zone ohne Internetverbindung eine zentralisierte Protokollierungsinfrastruktur. Diese ist derart ausgelegt, dass die in dieser Richtlinie vorgegebenen Protokollierungsereignisse für die doppelte Dauer der Speicherfrist in diesem Speicher vorgehalten werden können. Konsolidierte Behörden können auf das Angebot zur Protokollierung der IT-Dienstleister des Bundes zurückgreifen (siehe Anforderung PRB.I.3.1.1.2).

PRB.I.3.1.1.2 [ITDL] Die zentralisierte Protokollierungsinfrastruktur der IT-Dienstleister des Bundes ermöglicht den konsolidierten Behörden mandantengetrennt auf ihre Protokollierungsdaten zugreifen zu können. Weiterhin können diese Behörden den Speicher zur Protokollierung der durch sie selbst betriebenen Fachverfahren nutzen.

4 Einhaltung der rechtlichen Rahmenbedingungen (OPS.1.1.5.A5)

Die rechtlichen Rahmenbedingungen im Zusammenhang mit der Protokollierung werden für die Bundesverwaltung insbesondere durch die DSGVO, das BDSG und Artikel 10 GG i. Z. m. § 5 BSIG definiert. Detaillierte Betrachtung finden diese im [RDSK-PD]. An dieser Stelle finden sich die für die Planung und Konzeption wesentlichen Anforderungen.

PRB.I.4.1.1.1 Die Speicherfrist aller Protokollierungsdaten beträgt 90 Tage (siehe [RDSK-PD]). Nach Ablauf der 90 Tage sind die Protokollierungsdaten unwiderruflich zu löschen. Dieser Zeitraum wird spätestens zwei Jahre nach Veröffentlichung der PR-B gemeinsam mit der BfDI evaluiert und ggf. neu festgelegt. Sicherheitsrelevante Ereignisse (sofern keine personenbezogenen Informationen enthalten) und allgemeine Ereignisse, die nachweislich einem Cyber-Angriff zugeordnet wurden, können von dieser Löschung ausgenommen werden. Sollten Gesetze oder Verwaltungsvorschriften im Einzelfall längere Speicherfristen vorsehen (z. B. § 76 BDSG, [VSA]) so haben diese (sofern für die Protokollierungsquelle anwendbar) Vorrang.

PRB.I.4.1.1.2 Die Protokollierungsdaten müssen vor oder bei der Speicherung in der zentralen Protokollierungsinfrastruktur pseudonymisiert werden. Es muss sichergestellt sein, dass eine Rückauflösung der Pseudonyme innerhalb der Speicherfrist möglich ist.

PRB.I.4.1.1.3 [ALT] Die Pseudonymisierung der Protokollierungsdaten kann auf ein Minimum beschränkt werden, wenn System- und Nutzerkennungen keine unmittelbar personenbezogenen Informationen enthalten (Beispiel Systemkennung: „PC024459“ statt „PCMUELLER01“; Beispiel Nutzerkennung: „PK44553“ statt „MuellerRoland“) und die Herstellung des unmittelbaren Personenbezugs einer dritten Quelle bedarf, die nicht für diejenigen im Zugriff ist, welche mit der Auswertung der Protokollierungsdaten betraut sind.
Fachverfahren sollten auf Verzeichnisdienste zurückgreifen (Single Sign-On, siehe IT-Grundschutz M 4.498), um zu vermeiden, dass die Anwender Nutzerkennungen verwenden, welche unmittelbaren Personenbezug enthalten (z. B. Emailadressen).

PRB.I.4.1.1.4 [ALT] Sofern MAC- und IP-Adressen in der Verwaltungshoheit des Bundes für den Zweck der Protokollierung und Detektion begründet nicht pseudonymisiert werden können, kann von der Pseudonymisierung abgesehen werden. In diesem Fall sind organisatorische Maßnahmen zu treffen, sodass eine Zuordnung dieser Adressen zu einer Person für die mit der Protokollierungsdatenauswertung betrauten Personen nicht möglich ist. Die Adressen müssen weiterhin wie personenbezogene Daten behandelt werden. Diese Anforderung wird im [RDSK-PD] weiter detailliert.

PRB.I.4.1.1.5 [ITDL] Bei der Erhebung von Protokollierungsdaten mehrerer verschiedener Behörden müssen diese Daten so gespeichert werden, dass eine angemessene sichere Trennung und Zuordnung zu den jeweiligen Behörden jederzeit gewährleistet ist.

PRB.I.4.1.1.6 Die Protokollierungsdaten in Gänze werden mindestens entsprechend des höchsten VS-Einstufungsgrades eingestuft, für dessen Verarbeitung das interne Netz und die DMZen freigegeben wurden.

5 Konfiguration der Protokollierung für die IT-System- und Netz-Sicht (OPS.1.1.5.A3)

PRB.I.5.1.1.1 Ereignisse, die von IT-Systemen als sicherheitsrelevant ausgegeben werden (Sekundär-SRE), werden protokolliert. Die mindestens erforderliche *darüberhinausgehende* Protokollierung wird durch die PR-B in den folgenden Teilen festgelegt.

PRB.I.5.1.1.2 Die vorliegende Protokollierungsrichtlinie ersetzt nicht herstellerspezifische oder intern etablierte Vorgaben zur Protokollierung, sondern erweitert diese.

PRB.I.5.1.1.3 Die Behörde erarbeitet und etabliert unter Mitwirkung des behördlichen Datenschutzbeauftragten einen Prozess, welcher eine Anpassung der zu protokollierenden Ereignisse ermöglicht. Dieser Prozess erlaubt es, IT-Systeme auf eine automatisierte und flexible Art und Weise derart zu konfigurieren, dass eine unverzügliche Adaption der Protokollierung gewährleistet ist (z. B. im Falle eines Cyber-Angriffs).

Teil II Planung und Dokumentation der Protokollierung

1 Bedeutung der Planung und Dokumentation

Der IT-Grundschutz-Baustein OPS.1.1.5 *Protokollierung* listet acht Gefährdungen auf, die im Bereich der Protokollierung von besonderer Bedeutung sind. Zwei von diesen Gefährdungen kann nur durch eine systematische Planung und Dokumentation entgegengewirkt werden:

- Fehlende oder unzureichende Protokollierung
- Fehlplanung bei der Protokollierung

Dieser Teil der Richtlinie beschreibt ein methodisches Vorgehen, um diesen Gefährdungen zu begegnen.

Darüber hinaus dient die Dokumentation dazu, eine Zusammenarbeit bei der Detektion und Reaktion auf Cyber-Angriffe über Organisationseinheiten innerhalb einer Behörde (z. B. zwischen operativer IT-Sicherheit und IT-Betrieb), aber auch über Behördengrenzen hinweg zu ermöglichen.

2 Aufbau der Protokollierungslandkarte

Als Ergebnis der Planung und Dokumentation entsteht die Protokollierungslandkarte. Sie besteht aus einer grafischen Übersicht, welche alle relevanten Aspekte (siehe Kapitel 3) des internen Netzes und der angeschlossenen DMZen beschreibt. Es ist auch möglich, für das interne Netz und die DMZen getrennte Protokollierungslandkarten zu erstellen. Die grafische Übersicht kann durch weitere Detailübersichten ergänzt werden. Ein Beispiel für die Erstellung einer Protokollierungslandkarte findet sich in Anhang A.

Die Protokollierungslandkarte hat dieselbe Funktion wie eine geografische Landkarte: Sie dient der Orientierung. Werden beispielsweise von einer Protokollierungsquelle sicherheitsrelevante Ereignisse festgestellt, dann ist es wichtig zu wissen, in welchem Netzbereich sich diese Quelle befindet, um darüber ggf. an weitere Ereignisse anderer betroffener IT-Systeme zu gelangen.

Die Protokollierungslandkarte ist kein Netzplan, sondern bildet ausschließlich Protokollierungsquellen und ihre Beziehungen untereinander ab. Für eine Referenz zum Netzplan oder anderen technischen Dokumentationen ist es daher sinnvoll, die Symbole in der Protokollierungslandkarte entsprechend den Bezeichnungen, die der IT-Betrieb hierfür vorsieht, zu wählen (Beispiel: „srvlx<Lfd. Nr.>“ für einen Linux-Server).

Für jeden in der Protokollierungslandkarte dargestellten Objekttyp wird dokumentiert, welche Ereignisse dieses Objekt protokolliert. Ebenso wird der Datenfluss der Protokollierungsereignisse beschrieben. Diese Beschreibung ist insbesondere dann wichtig, wenn Ereignisse nicht unmittelbar von der Protokollierungsquelle zur zentralen Protokollierungsinfrastruktur übertragen werden. Zusätzlich enthält die Protokollierungslandkarte einen Anhang, der beschreibt, an welchen Stellen (z. B. Configuration Management Database (CMDB) oder sonstige Dokumentationssysteme) Detailinformationen zum IP-Adresskonzept, zum Domänenkonzept und zu den eingesetzten Querschnittsdiensten und Fachverfahren zu finden sind.

3 Anforderungen an die Dokumentation

PRB.II.3.1.1.1 Es wird eine Protokollierungslandkarte für das interne Netz und die angeschlossenen DMZen gemäß der Beschreibung in Kapitel 2 erstellt. Anhang A: Beispiele zur Erstellung einer Protokollierungslandkarte

PRB.II.3.1.1.2 [ALT] Liegt bereits ein bereinigter Netzplan vor oder gibt es eine andere geeignete Möglichkeit, auf bestehender Dokumentation aufzubauen, die alle in diesem Kapitel genannten Anforderungen erfüllt, kann auch diese verwendet werden.

PRB.II.3.1.1.3 Es werden alle Netzgrenzen identifiziert und die Systeme, die an diesen Netzgrenzen protokollieren, dokumentiert (siehe Teil III.2).

PRB.II.3.1.1.4 Es werden alle Netzbereiche innerhalb des internen Netzes sowie der DMZen identifiziert. IT-Systeme, welche die Kommunikation zwischen diesen Netzbereichen protokollieren, werden dokumentiert (siehe Teil III.3).

PRB.II.3.1.1.5 Wird bei der Dokumentation der Netzbereiche oder der IT-Systeme festgestellt, dass sich in einem Netzbereich sowohl Client- als auch Server-Systeme befinden, dann werden weitere Netzbereiche eingerichtet, so dass sich Client und Server-Systeme in getrennten Netzbereichen befinden (siehe NET.1.1.A5 *Client-Server-Segmentierung* und NET.1.1.A6 *Endgeräte-Segmentierung im internen Netz*).

PRB.II.3.1.1.6 Wird Netzvirtualisierung eingesetzt, um auf einer physikalischen Netzinfrastruktur mehrere logisch getrennte Netze zu bilden, dann muss aus der Protokollierungslandkarte sowohl ersichtlich sein, welche Netze getrennt sein sollen, als auch, welche gemeinsame Infrastruktur verwendet wird.

PRB.II.3.1.1.7 In die Netzbereiche werden die IT-Systeme eingezeichnet, die sich dort befinden und gemäß Teil IV bis zur Schicht „Systemdienste“ oder bei DMZen gemäß Teil III.5 bis Stufe 7 „Netz-Dienste“ protokollieren. Dabei ist zu beachten, dass für jedes einmalig eingetragene System dieselben Protokollierungseinstellungen gelten müssen (d. h. wenn zwei gleichartige IT-Systeme in der Landkarte aufgeführt sind, bedeutet dies, dass unterschiedliche Protokollierungseinstellungen konfiguriert wurden)[2].

PRB.II.3.1.1.8 Es existiert eine Dokumentation aller eingesetzten Querschnittsdienste und Fachverfahren, die aus der Protokollierungslandkarte referenziert wird. Dort ist dokumentiert, welche Ereignisse diese Dienste und Verfahren protokollieren. Diese Dokumentation muss durch die jeweilige Behörde vorgehalten werden, welche für den Betrieb der Querschnittsdienste und Fachverfahren zuständig ist.

PRB.II.3.1.1.9 Protokollierungslandkarten enthalten schützenswerte Informationen über den Informationsverbund. Wie diese Informationen einzustufen sind, legt die jeweilige Behörde fest. Dabei ist zu beachten, dass Protokollierungslandkarten Arbeitsmittel sind, die im täglichen Zugriff verfügbar sein müssen.

4 Erweiterte Anforderungen an die Dokumentation

PRB.II.4.1.1.1 [BmeS] Dokumentation der in den Querschnittsdiensten und Fachverfahren verarbeiteten Daten und deren Schutzbedarf: Diese Dokumentation muss für die Detektion bereitgestellt werden, da sich hieraus die wahrscheinlichen Angriffsziele auf eine Behörde ableiten lassen.

PRB.II.4.1.1.2 [OPT] Zur Dokumentation der Anforderung PRB.II.4.1.1.1 wird eine CMDB und ggf. ein Inventarisierungssystem verwendet.

PRB.II.4.1.1.3 [BmeS] Dokumentation von IT-Systemen, die nicht regelmäßig aktualisiert oder deren eingeschränkte Konfigurationsmöglichkeiten keine Härtung entsprechend des Schutzbedarfes ermöglichen (z. B. Appliances, Drucker, alte proprietäre Software): Derartige Systeme werden in dieser Richtlinie als „Gefährder“ bezeichnet und müssen in der Protokollierungslandkarte erfasst werden.

[2]Für die Dokumentation der IT-Systeme ist die Strukturanalyse gem. BSI-Standard 200-2 [ITGS200-2] eine sinnvolle Voraussetzung. Die dort durchgeführte Komplexitätsreduktion durch Gruppenbildung (siehe dortiges Kapitel 8.1.1) bildet auch die Grundlage für die Dokumentation in der Protokollierungslandkarte.

PRB.II.4.1.1.4 [OPT] Sowohl zur Erfassung als auch zur Dokumentation der Anforderung PRB.II.4.1.1.3 wird ein Schwachstellenerkennungssystem (wie z. B. OpenVAS) verwendet.

PRB.II.4.1.1.5 [BmeS] Sowohl für IT-Systeme mit einem hohen bis sehr hohen Schutzbedarf als auch für Gefährder wird geprüft, ob über diese Richtlinie hinausgehende Protokollierungsereignisse erfasst werden können oder ob sie in andere Netzbereiche verlagert werden müssen, sodass zumindest die Kommunikation mit diesen IT-Systemen überwacht und protokolliert werden kann.

Teil III Protokollierungsanforderungen für die Netz-Sicht

Dieser Teil ist die Umsetzungsrichtlinie für die gesetzliche Verpflichtung der Bundesbehörden, den Zugang des BSI zu behördeninternen Protokolldaten sicherzustellen (§ 5 Abs. 1 Satz 1 Nr. 1 und i. V. m. Satz 4 BSIG).

Die Umsetzung dieser Protokollierungsanforderungen erfordert eine strikte Aufgabenteilung zwischen Behörde und BSI. Die Behörde muss für das BSI die erforderlichen Schnittstellen und Daten bereitstellen, bspw. durch Installation und Integration von Komponenten oder Anpassung von Konfigurationen. Sämtliche Aufgaben im Kontext der Speicherung und Auswertung werden vom BSI durchgeführt.

1 Anforderungen zur Basisprotokollierung

PRB.III.1.1.1.1 Die Anforderung PRB.I.5.1.1.1 wird für die Netz-Sicht umgesetzt (Stufe 6 und 7). Neben der Protokollierung von IDS-Alarmen werden u. a. auch abgewiesene Netzverbindungen aus dem internen Netz und der DMZen, z. B. Verstöße gegen Access-Control-Listen (Protokollierungsdaten der (Betriebssystem-)Firewall siehe NET.3.2.A9 und SYS.1.1.A10) oder Network-Access-Control-Policies (siehe [MST-SSK]) erfasst.

2 Netzgrenzen

PRB.III.2.1.1.1 An allen Netzgrenzen werden Daten der Stufe 5 protokolliert. Sofern nicht vorhanden, werden hierzu die erforderlichen Proxys oder Application Layer Gateways (ALGs) installiert. Jedes Protokoll, welches über diese Netzgrenze hinweg genutzt wird, wird über einen entsprechend geeigneten Proxy geführt. Sollte kein geeigneter Proxy zur Verfügung stehen, wird dies dem BSI unter protokollierungsrichtlinie@bsi.bund.de angezeigt.

PRB.III.2.1.1.2 [EVAL] Der Proxy wird so installiert, dass es möglich ist, die Kommunikation bis zur Stufe 5 unverschlüsselt zu protokollieren. Findet eine Verschlüsselung auf dem Transport Layer statt, dann wird ein TLS-Proxy eingerichtet, sodass abschnittsweise unverschlüsselte Kommunikation protokolliert werden kann.

PRB.III.2.1.1.3 Wird für die Namensauflösung ein Nameserver außerhalb des Regierungsnetzes genutzt, so muss zwischen dem eigenen Nameserver und dem Uplink zum Netz, dessen Nameserver genutzt wird, ein Test-Access Point (TAP, dedizierte Geräte zum Kopieren des Netzverkehrs) oder Spiegelport („Mirror Port“ für Kopien des Netzverkehrs in Routern oder Switches) installiert werden. Dort werden Daten der Stufe 4 in Bezug auf DNS protokolliert.

PRB.III.2.1.1.4 [BmeS] Am Übergang vom internen Netz zu den Netzgrenzen werden ein oder mehrere Spiegelports oder TAPs eingerichtet, so dass unabhängig von den ALGs und Proxys Protokolldaten der Stufen 3 und 4 erhoben werden.

PRB.III.2.1.1.5 [BmeS]+[ALT] Sofern ein TLS-Proxy verfügbar ist (siehe PRB.III.2.1.1.2), der die Kommunikation unverschlüsselt, aber ansonsten unverändert (z. B. hinsichtlich der Reihenfolge der Header) an einem Spiegelport ausgeben kann, kann dieser statt den Anforderungen PRB.III.2.1.1.3 und PRB.III.2.1.1.4 verwendet werden (siehe auch IT-Grundschutz M 4.223).

PRB.III.2.1.1.6 [ITDL] Die Netzarchitektur wird in der Art eingerichtet, dass die vorhergehenden Anforderungen aus diesem Abschnitt für jede konsolidierte Behörde eingehalten werden. Die Netzgrenzen einzelner Behörden werden dabei nicht aufgelöst.
Hinweis: Diese Anforderung ist nur bei physisch getrennter Bereitstellung der IT-Infrastruktur der einzelnen Behörden vollständig umsetzbar. Sollte dies nicht realisierbar sein, dann ist das der Behörde und dem BSI schriftlich anzuzeigen. Es gelten dann die Anforderungen aus Kapitel 4.

3 Internes Netz

PRB.III.3.1.1.1 Die Router oder L3-Switche werden so konfiguriert, dass Daten der Stufe 2 für die Kommunikation zwischen Netzbereichen protokolliert werden.

PRB.III.3.1.1.2 [ALT] Wenn sich zwischen den Netzbereichen präventive Maßnahmen (z. B. Paketfilter) befinden, können auch diese zur Protokollierung von Daten der Stufe 2 genutzt werden. Weiterhin gilt für diese Systeme die Anforderung PRB.III.1.1.1.1.

PRB.III.3.1.1.3 [BmeS] Behörden mit erhöhten Sicherheitsbedürfnissen müssen an besonders sicherheitsempfindlichen Stellen im Netz weitere Spiegelports oder TAPs einrichten. Hier werden Daten der Stufe 3 und 4 durch das BSI protokolliert (z. B. mittels Suricata).

PRB.III.3.1.1.4 [ITDL] Die Netzarchitektur wird in der Art eingerichtet, dass die vorhergehenden Anforderungen aus diesem Kapitel für jede konsolidierte Behörde eingehalten werden. Dies gilt nicht nur für die Zugangsnetze in den jeweiligen Standorten der Behörden, sondern auch für die Verkehre in den Rechenzentren.

4 Protokollierung beim Einsatz von virtualisierten und hyperkonvergenten Systemen

Die Anforderungen aus den Kapiteln 2 und 3 basieren auf der Annahme, dass physische Schnittstellen existieren. Während diese an den Netzgrenzen des Regierungsnetzes weiterhin existieren, ergibt sich u. a. aus der IT-Konsolidierung und der damit verbundenen Zentralisierung, dass sich die Erhebung behördeninterner Protokolldaten zukünftig ändern wird.

Derzeit liegen hierzu nicht ausreichende Untersuchungen seitens des BSI vor. Bis auf weiteres gelten folgende Übergangsanforderungen. Die Anforderungen sind vornehmlich auf IT-Dienstleister des Bundes ausgerichtet, können aber auch von Behörden mit erhöhten Sicherheitsbedürfnissen übernommen werden.

4.1 Realisierung zu trennender Netze in einer gemeinsamen virtualisierten Umgebung

Für Behörden oder IT-Verfahren, zwischen denen eine Netzgrenze existieren sollte, die aber durch die Zentralisierung nur durch virtuelle Trennung (virtuelle Netzgrenzen) realisierbar ist, gilt:

PRB.III.4.1.1.1 [EVAL] Die Verkehrsflüsse zwischen den virtuellen Netzgrenzen werden so konfiguriert, dass sie über ein IT-System (je nach Schutzbedarf Router, Paketfilter, ALG) geführt werden (Kopplungsstelle), welches außerhalb des Einflussbereiches des Hypervisors der Virtualisierung liegt.

PRB.III.4.1.1.2 [EVAL] An der Kopplungsstelle werden TAPs oder Spiegelports eingerichtet und dort Daten der Stufe 4 protokolliert. Die Kommunikation wird an dieser Stelle unverschlüsselt bereitgestellt (siehe PRB.III.2.1.1.2).

PRB.III.4.1.1.3 [EVAL] Die Netzvirtualisierung wird so konfiguriert, dass Daten der Stufe 2 für alle Verkehre innerhalb eines virtualisierten Netzes protokolliert werden.
Hinweis: Die Umsetzung dieser Anforderung kann die Installation von Agenten auf den Servern oder das Einrichten virtueller Spiegelports mit zusätzlichen virtuellen Maschinen zur Erzeugung der Daten erforderlich machen.

PRB.III.4.1.1.4 [EVAL] Alle Ereignisse, die Indizien für eine versuchte oder erfolgreiche Kompromittierung des Hypervisors liefern können, werden von der Behörde zur Verfügung gestellt und vom BSI protokolliert.

4.2 Dedizierte Bereitstellung von Diensten für mehrere Behörden

Es wird im Zuge der IT-Konsolidierung dazu kommen, dass grundlegende Dienste, die von mehreren Behörden genutzt werden, nur einmalig realisiert werden. Dies wird gegebenenfalls auch dann der Fall sein, wenn aus Sicht der Informationssicherheit eine physisch getrennte Bereitstellung je Behörde erforderlich wäre.

PRB.III.4.2.1.1 [EVAL] Gemeinsam bereitgestellte Dienste werden so erbracht, dass sie innerhalb eines vollständig physisch abgegrenzten Netzes liegen. Es gelten dann für die Protokollierung die Anforderungen aus Kapitel 2 und 3 entsprechend. Sofern zutreffend, gelten auch die Anforderungen aus Kapitel 4.1.

5 Zusätzliche Anforderung Demilitarisierte Zonen (DMZen)

PRB.III.5.1.1.1 Die Anforderungen aus den zutreffenden Bausteinen des IT-Grundschutzes sind vollständig umgesetzt.

PRB.III.5.1.1.2 Fachverfahren, die für andere Behörden oder externe Netze angeboten werden, werden in DMZen betrieben.

PRB.III.5.1.1.3 Es werden die Protokolldaten gemäß Stufe 7 für alle Netz-Dienste in einer DMZ erhoben.

Teil IV Protokollierungsanforderungen für die IT-System-Sicht

Die Richtlinie enthält derzeit ausschließlich Anforderungen für die Schichten Betriebssystem und Systemdienste. Die in den anderen Schichten zu erfassenden Protokollierungsdaten werden in einer zukünftigen Version geregelt. Durch diese mehrstufige, prioritätenorientierte Vorgehensweise wird den Behörden eine schrittweise Anpassung der Protokollierung der IT-Systeme ermöglicht. Die Behörden sind ausdrücklich dazu eingeladen, die Protokollierung der in dieser Version unberücksichtigten Schichten frühestmöglich einzuführen. Bereits bei Behörden umgesetzte Maßnahmen in Bezug auf die Protokollierung werden vom BSI in zukünftigen Versionen der Protokollierungsrichtlinie berücksichtigt.

1 Anforderungen an die zu erhebenden Protokollierungsdaten

1.1 Schichtenübergreifende Anforderungen

Unabhängig von der konkreten Schicht stellen Hersteller, Betreiber und Dienstleister Anforderungen an die Protokollierung. Diese Anforderungen bleiben von den nachstehenden Anforderungen unberührt. Die Protokollierungsrichtlinie ist als Erweiterung bestehender Anforderungen zu sehen (siehe PRB.I.5.1.1.2).

Um die enge Verzahnung mit dem IT-Grundschutz des BSI zu verdeutlichen und eine unmittelbare Abbildbarkeit zu ermöglichen, werden im Folgenden die Anforderungen in „Anforderungen laut IT-Grundschutz“ - mit entsprechendem Verweis - und „Zusätzliche Anforderungen“ aufgeschlüsselt.

1.2 Anforderungen an die Protokollierung für Betriebssysteme

Auf der Betriebssystem-Schicht müssen alle relevanten Vorgänge erfasst werden, welche Rückschlüsse auf eine mögliche Kompromittierung des IT-Systems zulassen. Außerdem dienen die erfassten Ereignisse der Rekonstruktion des Vorgehens eines Angreifers. Diese Schicht umfasst die Protokollierung der Vorgänge auf den lokalen IT-Systemen. Je nach verwendetem Betriebssystem kann es notwendig sein, dass die Behörde die Anforderungen weiter detailliert. Auf die Protokollierung in zentralen Authentisierungs- und Autorisierungsdiensten wird in Kapitel 1.3.1 eingegangen.

Anforderungen laut IT-Grundschutz:

PRB.IV.1.2.1.1 Der Start des IT-Systems wird protokolliert. [SYS.1.1.A10 *Systemstarts und Reboots*]

PRB.IV.1.2.1.2 Ein Neustart des IT-Systems wird protokolliert. [SYS1.1.A10 *Systemstarts und Reboots*] [NET.3.1.A7 *Reboot*]

PRB.IV.1.2.1.3 Das Anlegen neuer Benutzer wird protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.2.1.4 Werden Rechte oder Privilegien von Benutzern geändert, so werden diese Änderungen protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.2.1.5 Werden Zugangsdaten von Benutzern geändert, so wird dies protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.2.1.6 Das Löschen von Benutzern wird protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.2.1.7 Die Erstellung von Gruppen wird protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.2.1.8 Werden Rechte oder Privilegien von Gruppen geändert, so werden diese Änderungen protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.2.1.9 Werden Benutzer in Gruppen aufgenommen, so wird dies protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.2.1.10 Werden Benutzer aus Gruppen entfernt, so wird dies protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.2.1.11 Das Löschen von Gruppen wird protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.2.1.12 Änderungen an der definierten Identitäts- und Berechtigungsrichtlinie werden protokolliert [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.2.1.13 Erfolgreiche Anmeldungen von Benutzern werden protokolliert. [SYS.1.1.A10 *Erfolgreiche und erfolglose Anmeldungen am System*]

PRB.IV.1.2.1.14 Die Protokollierung erfasst fehlgeschlagene Anmeldungen von Benutzern. [SYS.1.1.A10 *Erfolgreiche und erfolglose Anmeldungen am System*] [NET.3.1.A7 Login-Fehler]

PRB.IV.1.2.1.15 Der Versuch eines unberechtigten Zugriffs auf Ressourcen wird protokolliert.[NET.3.2.A9 *Fehlgeschlagene Zugriffe aus System-Ressourcen aufgrund fehlerhafter Authentisierungen, mangelnder Berechtigung oder nicht vorhandener Ressourcen*]

PRB.IV.1.2.1.16 Die Protokollierung erfasst die Installation, die Konfiguration und das Ausführen von Diensten. [NET.3.1.A7*„Konfigurationsänderungen*]

PRB.IV.1.2.1.17 Konfigurationsänderungen an Servern, Routern, Switches, Firewalls und Sicherheitsproxys werden protokolliert. [NET.3.1.A7 *Konfigurationsänderungen*]

Zusätzliche Anforderungen:

PRB.IV.1.2.1.18 Die Abmeldung von Benutzern wird protokolliert.

PRB.IV.1.2.1.19 [EVAL] Die Protokollierung wird auf sämtlichen IT-Systemen aktiviert, die im Teil II identifiziert wurden.

PRB.IV.1.2.1.20 Anhand der Protokollierungsdaten kann das System, von welchem die Protokollierungsdaten stammen identifiziert werden (z. B. Hostnamen „srvlx<Lfd. Nr.>“ für einen Linux-Server).

PRB.IV.1.2.1.21 Betriebssysteme in virtuellen Umgebungen sind in der Protokollierung auf der Betriebssystem-Schicht wie physische Systeme zu behandeln.

PRB.IV.1.2.1.22 Änderungen am Protokollierungs-Level werden protokolliert.

PRB.IV.1.2.1.23 Die Erzeugung von relevanten Prozessen wird protokolliert.

PRB.IV.1.2.1.24 Aus den Protokollierungsdaten geht hervor, durch welchen Benutzer ein Prozess erstellt wurde.

PRB.IV.1.2.1.25 Die Beendigung von relevanten Prozessen wird protokolliert.

PRB.IV.1.2.1.26 [OPT] Ein selektiver Ausschluss von Prozessen, deren Protokollierung mit einer hohen Systemlast verbunden ist, die jedoch keine relevanten Informationen liefert, ist möglich.

PRB.IV.1.2.1.27 Der Zugriff auf Dateien und Verzeichnisse, welche nachweislich und bekanntlich mehrfach im Kontext von Angriffen genutzt wurden, wird protokolliert.

PRB.IV.1.2.1.28 An und in System-Verzeichnissen durchgeführte Änderungen werden protokolliert.

PRB.IV.1.2.1.29 Modifikationen des Zeitstempels des Erstellungszeitpunktes einer Datei werden protokolliert.

PRB.IV.1.2.1.30 Das Ausführen von Befehlen im Adressraum eines anderen Prozesses[3] wird durch die Protokollierung erfasst.

PRB.IV.1.2.1.31 Die Erzeugung und Ausführung automatisierter, wiederkehrender Aufgaben („Scheduled Tasks“/ „Cronjobs“) wird protokolliert.

PRB.IV.1.2.1.32 Die Installation neuer Treiber und Kernel-Module und Änderungen daran werden protokolliert.

PRB.IV.1.2.1.33 Änderungen an den Zugriffsberechtigungen für Ordner, Dateien und Programme werden protokolliert. Ein selektiver Ausschluss der Überwachung von Änderungen, deren Protokollierung mit einer hohen Systemlast verbunden ist, die jedoch keine relevanten Informationen liefert, ist möglich.

1.3 Anforderungen an die Protokollierung für Systemdienste

Derzeit werden nur Dienste zur Authentisierung- und Autorisierung betrachtet. Anforderungen für weitere Systemdienste werden in einer zukünftigen Version geregelt (siehe einleitende Begründung).

1.3.1 Anforderungen an die Protokollierung für Zentrale Authentisierungs- und Autorisierungsdienste

Auf der System-Schicht müssen alle relevanten Vorgänge erfasst werden, welche Rückschlüsse auf eine mögliche Kompromittierung der zentralen Authentisierung- und Autorisierungsdienste zulassen. Außerdem dienen die erfassten Ereignisse der Rekonstruktion des Vorgehens eines Angreifers. Diese Schicht umfasst die Protokollierung der Vorgänge in den zentralen Authentisierungs- und Autorisierungsdiensten. Auf die Protokollierung auf der Betriebssystemschicht wird in Kapitel 1.2 eingegangen.

Anforderungen laut IT-Grundschutz:

PRB.IV.1.3.1.1 Das Anlegen neuer Benutzer im zentralen Authentisierungs- und Autorisierungsdienst wird protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.3.1.2 Werden Rechte oder Privilegien von Benutzern im zentralen Authentisierungs- und Autorisierungsdienst geändert, so werden diese Änderungen protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen]*

PRB.IV.1.3.1.3 Werden Zugangsdaten von Benutzern im zentralen Authentisierungs- und Autorisierungsdienst geändert, so wird dies protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.3.1.4 Erfolgreiche Anmeldungen von Benutzern werden protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.3.1.5 Fehlgeschlagene Anmeldungen von Benutzern im zentralen Authentisierungs- und Autorisierungsdienst werden protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.3.1.6 Das Löschen von Benutzern im zentralen Authentisierungs- und Autorisierungsdienst wird protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

[3]Unter Microsoft Windows z. B. Remote Threads

PRB.IV.1.3.1.7 Die Erstellung von Gruppen im zentralen Authentisierungs- und Autorisierungsdienst wird protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.3.1.8 Werden Rechte oder Privilegien von Gruppen im zentralen Authentisierungs- und Autorisierungsdienst geändert, so werden diese Änderungen protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.3.1.9 Werden Benutzer in Gruppen im zentralen Authentisierungs- und Autorisierungsdienst aufgenommen, so wird dies protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.3.1.10 Werden Benutzer aus Gruppen im zentralen Authentisierungs- und Autorisierungsdienst entfernt, so wird dies protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.3.1.11 Das Löschen von Gruppen im zentralen Authentisierungs- und Autorisierungsdienst wird protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.3.1.12 Änderungen an der definierten Identitäts- und Berechtigungsrichtlinie im zentralen Authentisierungs- und Autorisierungsdienst werden protokolliert. [SYS.1.1.A10 *Einrichtung oder Änderung von Benutzern, Gruppen und Berechtigungen*]

PRB.IV.1.3.1.13 Erfolgreiche Anmeldungen von Benutzern im zentralen Authentisierungs- und Autorisierungsdienst werden protokolliert. [SYS.1.1.A10 *Erfolgreiche und erfolglose Anmeldungen am System*]

PRB.IV.1.3.1.14 Die Protokollierung erfasst fehlgeschlagene Anmeldungen von Benutzern im zentralen Authentisierungs- und Autorisierungsdienst. [SYS.1.1.A10 *Erfolgreiche und erfolglose Anmeldungen am System*] [NET.3.1.A7 *Login-Fehler*]

PRB.IV.1.3.1.15 Der Versuch eines unberechtigten Zugriffs auf Ressourcen im zentralen Authentisierungs- und Autorisierungsdienst wird protokolliert. [NET.3.2.A9 *Fehlgeschlagene Zugriffe aus System-Ressourcen aufgrund fehlerhafter Authentisierungen, mangelnder Berechtigung oder nicht vorhandener Ressourcen*]

Zusätzliche Anforderungen:

PRB.IV.1.3.1.16 Abmeldung von Benutzern im zentralen Authentisierungs- und Autorisierungsdienst wird protokolliert.

1.4 Anforderungen an die Protokollierung für Querschnittsdienste und Fachverfahren

Für Querschnittsdienste und Fachverfahren werden in einer späteren Version grundlegende, allgemeingültige Anforderungen genereller Natur festgelegt. Weitere Anforderungen an die Protokollierung sind von der konkreten Ausprägung der Querschnittsdienste und Fachverfahren abhängig. Ein Vorgehensmodell, welches die Behörden bei der Festlegung der spezifischen Anforderungen unterstützen soll, wird ausgearbeitet und in einer späteren Version in die Protokollierungsrichtlinie aufgenommen.

PRB.IV.1.4.1.1 Die für die Entwicklung und/oder Betrieb verantwortlichen Organisationseinheiten definieren, welche Ereignisse für die jeweiligen Querschnittsdienste und Fachverfahren protokolliert werden, dokumentieren diese und richten die zentralisierte Protokollierung entsprechend ein.

2 Anforderungen an die Erfassung und Übermittlung der Daten an die zentrale Protokollierungsinfrastruktur

PRB.IV.2.1.1.1 [EVAL] Protokollierungsereignisse werden ausschließlich über Betriebssystemmittel und ohne den Einsatz zusätzlicher Agenten erfasst.

PRB.IV.2.1.1.2 Zur Erfüllung der Anforderung PRB.IV.2.1.1.1 können spezielle IT-Systeme eingerichtet werden, die außerhalb der Produktionsinfrastruktur stehen. Diese IT-Systeme können Agenten enthalten, sollten diese zur zentralen Protokollierung erforderlich sein oder diese erleichtern.

Referenzdokumente

Übergeordnete und verbundene Dokumente

[ITGS200-2]	BSI-Standard 200-2
[ITGS-KOMP]	IT-Grundschutz Kompendium (Edition 2018)
[MST-SSK]	Mindeststandard des BSI für Schnittstellenkontrollen
[MST-PD]	Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen
[RDSK-PD]	Rahmendatenschutzkonzept Protokollierung und Detektion von Cyber-Angriffen auf die Bundesverwaltung
[VSA]	Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) vom 31. März 2006

Abkürzungsverzeichnis

APT	Advanced Persistent Threat (engl.)
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CMDB	Configuration Management Database (engl.)
DMZ	Demilitarisierte Zone
IDS	Intrusion Detection System (engl.)
NdB	Netze des Bundes
NTP	Network Time Protocol (engl.)
PITS	Protokollierungsdaten aus IT-System-Sicht
PN	Protokollierungsdaten aus Netz-Sicht
PR-B	Protokollierungsrichtlinie Bund
TAP	Test Access Port (engl.)
UP	Umsetzungsplan
VS	Verschlusssache

Anhang A: Beispiele zur Erstellung einer Protokollierungslandkarte

1 Einleitung

Dieser Anhang illustriert an einem Beispiel, die Erstellung der Protokollierungslandkarte nach Anforderung PRB.II.3.1.1.1. Die vollständige Landkarte, die sich aus diesem Dokument ergibt, ist in Abbildung 2 skizziert.

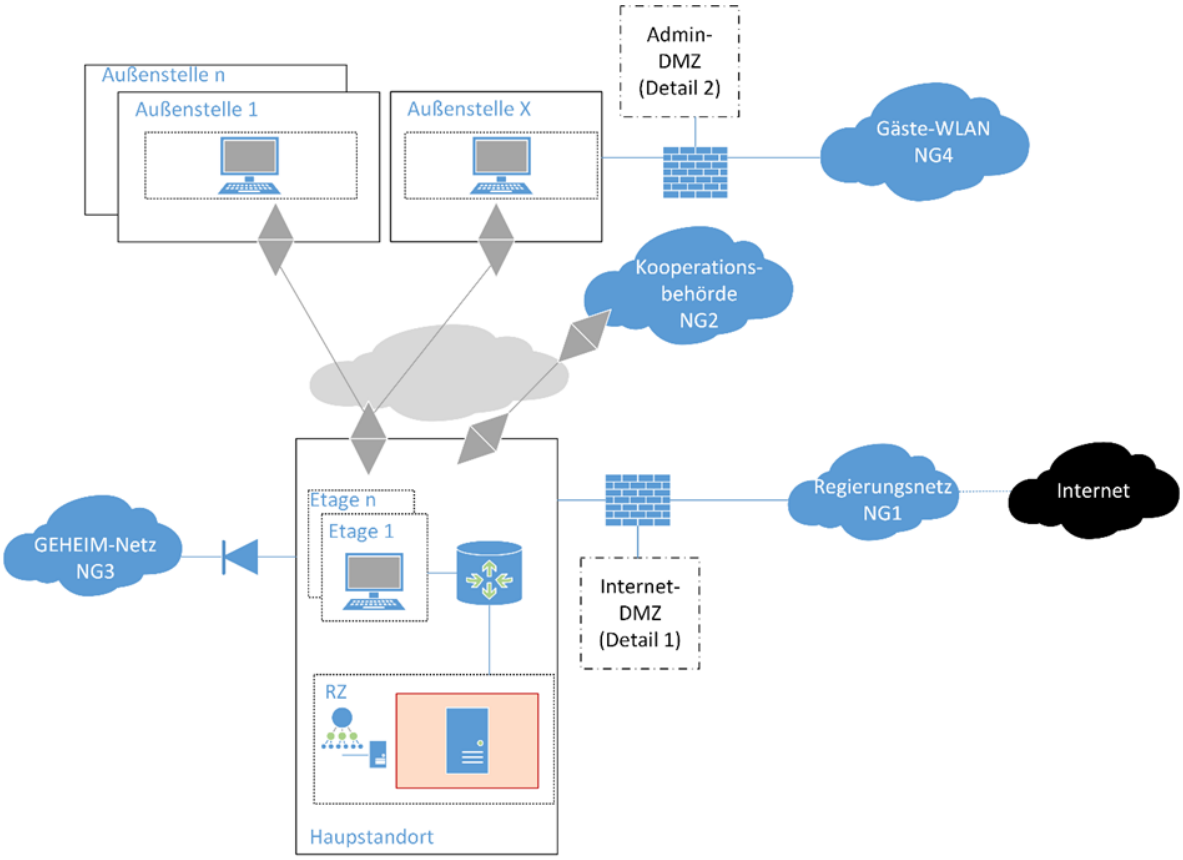

Abbildung 2: Protokollierungslandkarte

In den Kapiteln 2 bis 4 wird erläutert, wie sich diese Landkarte aus einzelnen Schritten zusammensetzt.

Die einzelnen Schritte entsprechen dabei dem folgenden Vorgehen:

1. Protokollierung der Ereignisse aus Netz-Sicht
    a. Zunächst werden alle Netzgrenzen identifiziert und dort die entsprechenden Protokollierungsquellen (Außen) erfasst.
    b. Im nächsten Schritt werden alle Netzbereiche identifiziert und dort die entsprechenden Protokollierungsquellen (Innen) erfasst.
2. Protokollierung der Ereignisse aus IT-System-Sicht
    a. Erfassung der zentralen Authentisierungs- und Autorisierungsdienste.
    b. Im nächsten Schritt wird die Protokollierung auf der Betriebssystemschicht auf den Servern und Clients dokumentiert.
    c. Abschließend wird die Protokollierung auf der Fachverfahrensschicht aufgenommen.

Dieses Vorgehen eignet sich auch zur schrittweisen Einführung einer zentralen Protokollierung und kann daher analog umgesetzt werden. Bei den Schritten 2a und 2b wird von einer gegebenen Gruppierung Gebrauch gemacht, die auch in der Praxis notwendige Voraussetzung für eine effiziente Erstellung einer Protokollierungslandkarte ist. Der Schritt 2c wird in diesem Dokument aufgrund der sehr starken Unterschiede zwischen verschiedenen Behörden nicht betrachtet.

Das Kapitel 5 befasst sich mit fortgeschrittenen Fragestellungen, die sich bei der Erstellung einer Protokollierungslandkarte ergeben können (z. B. Bezeichnungen der Elemente, Datenfluss, Netzvirtualisierung, Sicherheitssystemen in einer DMZ und IT-System-Virtualisierung). Diese Themen sind als bedarfsbezogen zu verstehen.

Die Protokollierungslandkarte kann unter Verwendung einer Visualisierungssoftware erstellt werden (beispielhaft wurde hier Microsoft Visio verwendet).

2 Dokumentation der Protokollierung der Netzgrenzen

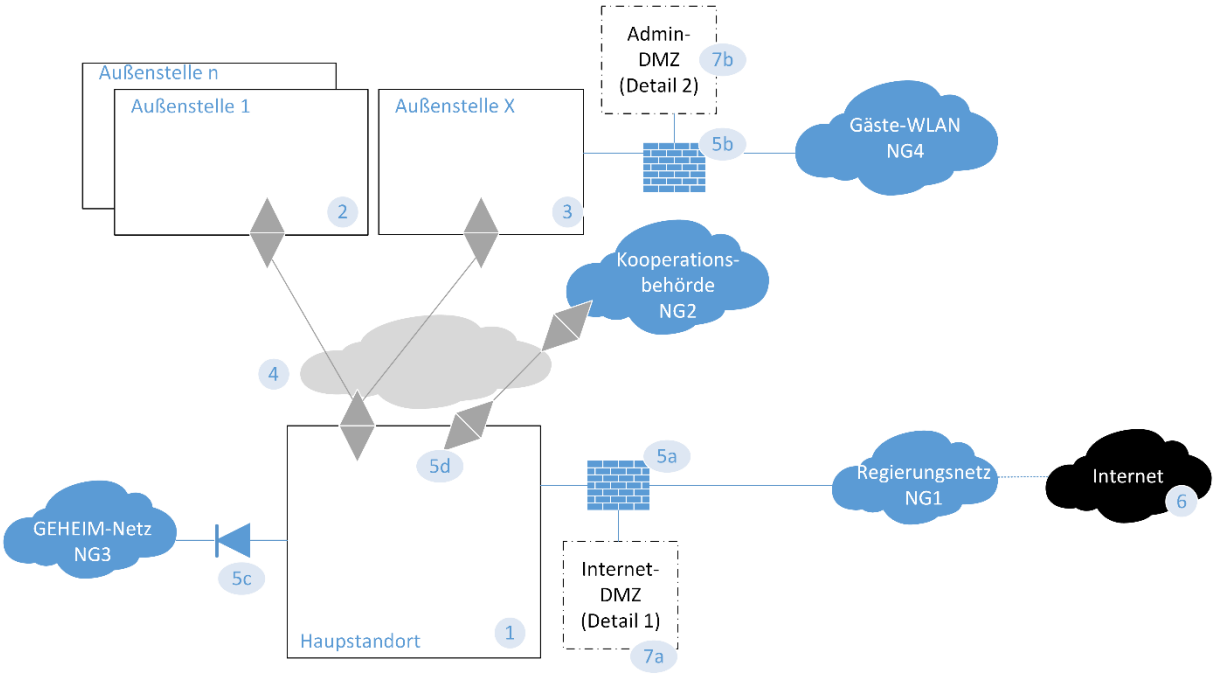

Abbildung 3: Ausschnitt Netzgrenzen

In diesem Beispiel (siehe Abbildung 3) wurden vier Netzgrenzen (NG1 - NG4) identifiziert. Das Internet (Nr. 6) muss immer in die Protokollierungslandkarte eingezeichnet werden, auch wenn es nicht unmittelbar an das Behördennetz grenzt (siehe NG 1). Das interne Netz wird aus dem Hauptstandort (Nr. 1) und den Außenstellen (Nr. 2 und Nr. 3) gebildet. Dabei können ähnliche Netze gruppiert werden, siehe z. B. Außenstellen 1–n. Außenstelle X kann nicht gruppiert werden, da hier das Gäste-WLAN angrenzt (NG 4). Für die Protokollierung transparente Netze und Elemente werden grau eingezeichnet (Nr. 4). In diesem Fall handelt es sich bei den Symbolen um zugelassene Verschlüsselungsgeräte, so dass das darunterliegende Transportnetz keine Netzgrenze bildet. Würden an dieser Stelle nicht zugelassene Verschlüsselungsgeräte verwendet, dann bildet das Transportnetz eine Netzgrenze und muss dementsprechend in die Protokollierung einbezogen werden.

In dieser Abbildung eingezeichnet sind exemplarisch auch die Schutzmaßnahmen an den Netzgrenzen (siehe Nr. 5a - 5d). Nr. 5a, b stellen z. B. Application Layer Gateways dar, Nr. 5c eine Diode und bei Nr. 5d wird gar keine Schutzmaßnahme etabliert.

Nr. 5d würde nicht in der IST-Protokollierungslandkarte auftauchen können, da ohne Anpassungen gar kein System existieren würde, welches diese Netzgrenze protokollieren lassen könnte. In diesem Fall müsste die Netzgrenze als Gefährder markiert werden.

NG 3 und NG 4 bilden (behördeninterne) Netzgrenzen. Durch eine derartige Netzstrukturierung lässt sich die Komplexität der Protokollierung erheblich reduzieren, da so Netz für Netz schrittweise in die Protokollierung aufgenommen werden kann, ohne blinde Flecken in der Protokollierung zu erzeugen. Dabei ist jedoch darauf zu achten, dass hier ausschließlich stark eingeschränkte Schnittstellen verwendet werden.

In Nr. 7a und 7b wurde zusätzlich davon Gebrauch gemacht, Detailbereiche des Netzes abstrahiert darzustellen und auf Detailprotokollierungslandkarten (Detail 1 und Detail 2) zu verweisen. Dies sorgt für mehr Übersichtlichkeit.

3 Dokumentation der Protokollierung der Netzbereiche

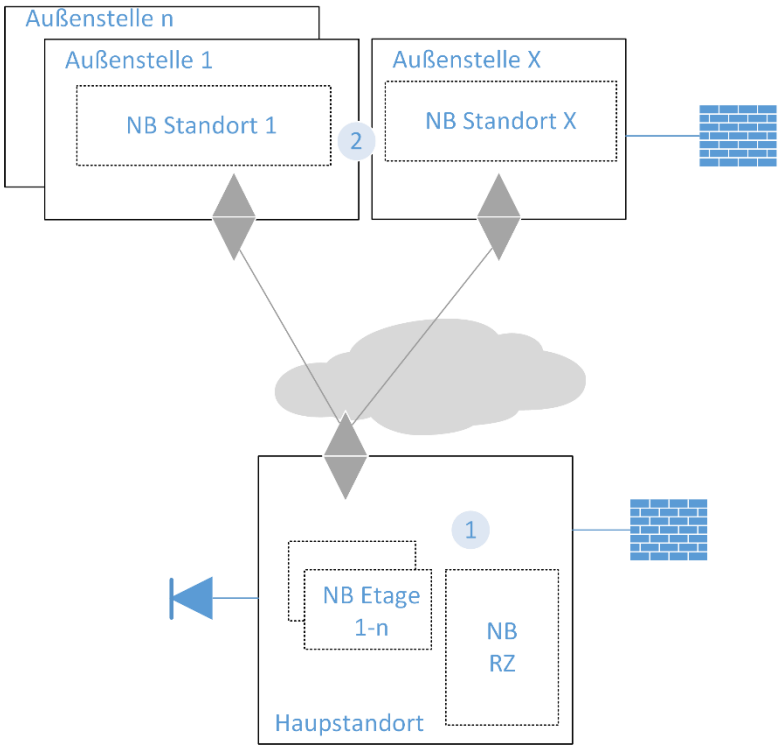

Abbildung 4: Ausschnitt Netzbereiche

Am Hauptstandort findet sich pro Etage je ein Netzbereich und ein Netzbereich für das Rechenzentrum (siehe Nr. 1). Bei den Etagen (NB 1-n) wurde sich der Gruppierung bedient. In den Außenstellen existiert jeweils nur ein Netzbereich (siehe Nr. 2). Auch hier ist zu beachten, dass in der IST-Protokollierungslandkarte ausschließlich die Netzbereiche eingezeichnet werden dürfen, welche auch tatsächlich in der Protokollierung erhoben werden können.

4 Dokumentation der Protokollierung aus IT-System-Sicht

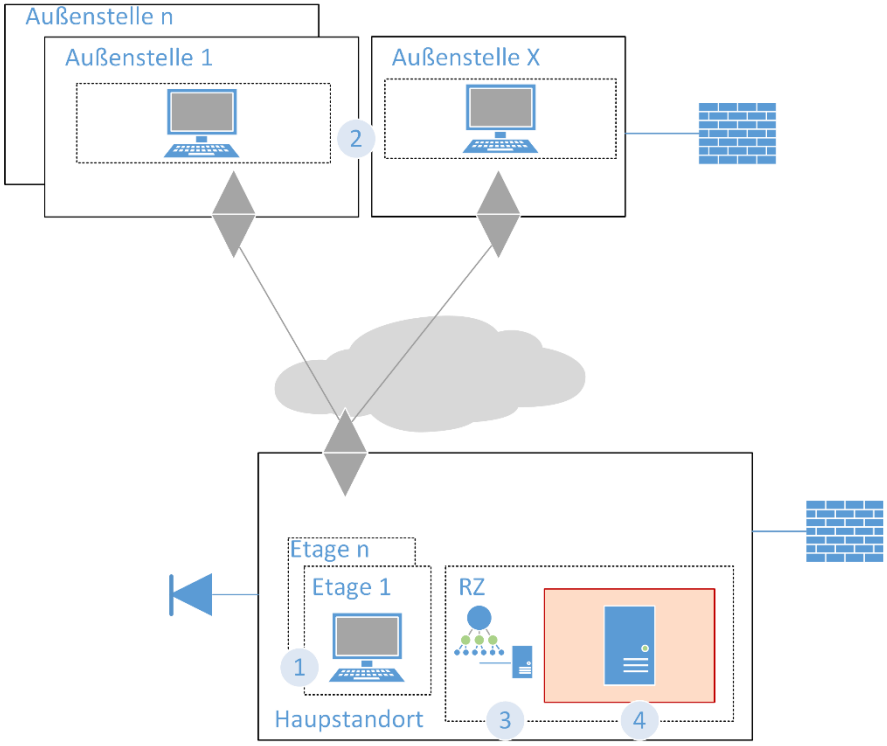

Abbildung 5: Ausschnitt IT-Systeme

Es stellt sich heraus, dass in diesem Szenario (siehe Abbildung 5) nur drei Gruppen von IT-Systemen existieren (Nr. 1 und Nr. 2: APCs; Nr. 3: physische Domain-Controller; sowie Nr. 4: ein Virtualisierungs-Host mit virtuellen Servern). Auch wenn die APCs in allen Netzbereichen identisch sind, müssen sie in jedem Netzbereich erneut eingezeichnet werden, damit ersichtlich wird, dass aus diesem Netzbereich Protokollierungsdaten von APCs erwartet werden. Die Mächtigkeit der Gruppierung bei Endsystemen wird beim Netzbereich RZ deutlich. Auch wenn die Behörde beispielsweise 10 physische Windows Server mit Domain-Controller hätte, die 10 Windows Server aber alle identisch protokollieren und die identische Betriebssystemkonfiguration hätten, müsste an dieser Stelle nur ein Server eingetragen werden. Ähnliches gilt auch für die Virtualisierung. Der Virtualisierungs-Host wird dabei als rote Fläche dargestellt, auf der die virtuellen Server entsprechend der Gruppierung platziert werden können.

5 Fortgeschrittene Aspekte der Dokumentation der Protokollierung

5.1 Dokumentation des Datenflusses der Protokollierungsereignisse

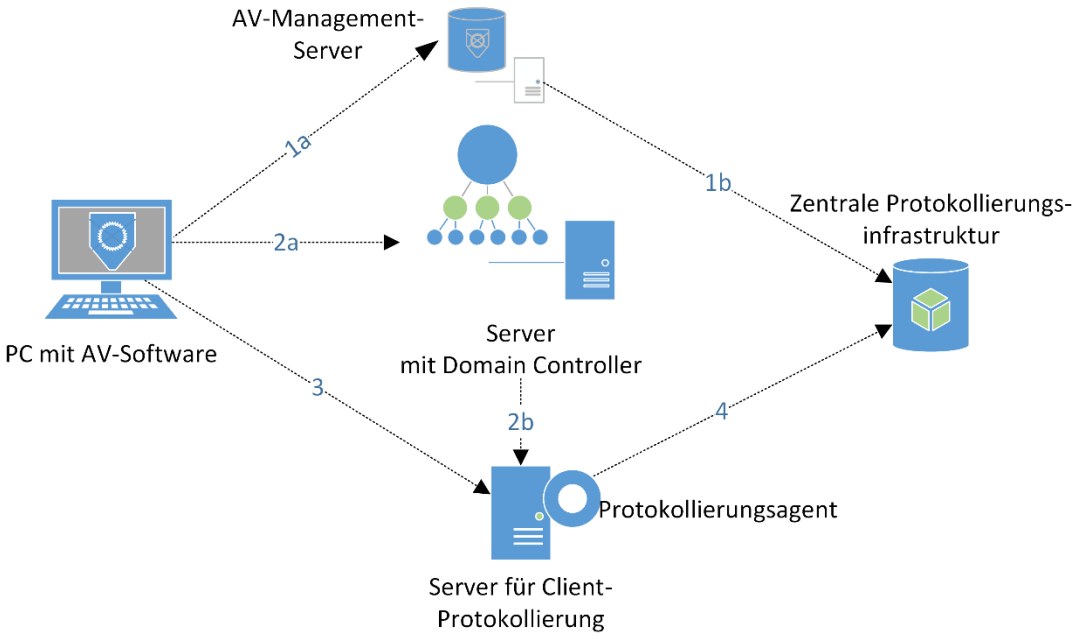

Abbildung 6: Dokumentation des Datenflusses

Der Client (PC mit AV-Software, auch als APC bezeichnet) in Abbildung 6 stellt die Quelle der Protokollierungsereignisse dar. Der installierte Virenscanner liefert Ereignisse an die Virenscanner-Management Software (Nr. 1a), welche die Ereignisse wiederum an die zentrale Protokollierungsinfrastruktur weiterleitet (Nr. 1b). In diesem Beispiel existiert eine zentralisierte Authentifizierung, so dass ein Teil der Authentifizierungsereignisse am IT-System ausschließlich am Domain Controller erfasst werden (Nr. 2a). Die übrigen Protokollierungsereignisse werden in diesem Beispiel zunächst an einen Server für die Client Protokollierung weitergeleitet (Nr. 3). Dasselbe gilt auch für den Domain Controller (Nr. 2b). Dieser Zwischenschritt ist in diesem Beispiel erforderlich, da für die vereinfachte Erfassung der Protokollierungsdaten in der zentralen Protokollierungsinfrastruktur ein Agent erforderlich ist. Über diesen Weg muss dieser nur auf einem System installiert werden (Nr. 4).

Anhand dieses Beispiels kann zudem nachvollzogen werden, warum eine Zeitsynchronisation (siehe Anforderung PRB.I.2.1.1.1) zwingend erforderlich ist. Driften die aus den Protokollierungsdaten hervorgehenden Zeiten der beteiligten Systeme auseinander, so kann dies zur Folge haben, dass die zeitliche Korrelation von Protokollierungsereignissen nicht mehr möglich ist und die Detektion dadurch falsche Erkenntnisse liefert. Eine nicht-synchronisierte Zeit kann ebenso die Unmöglichkeit der Rekonstruktion eines Sicherheitsvorfalles bedingen. Dieses Problem kann unter anderem noch verstärkt werden, wenn die Management-Software oder der Server für die Client-Protokollierung die Ergebnisse zusätzlich verfälschen.

5.2 Dokumentation der IT-Systembezeichnungen

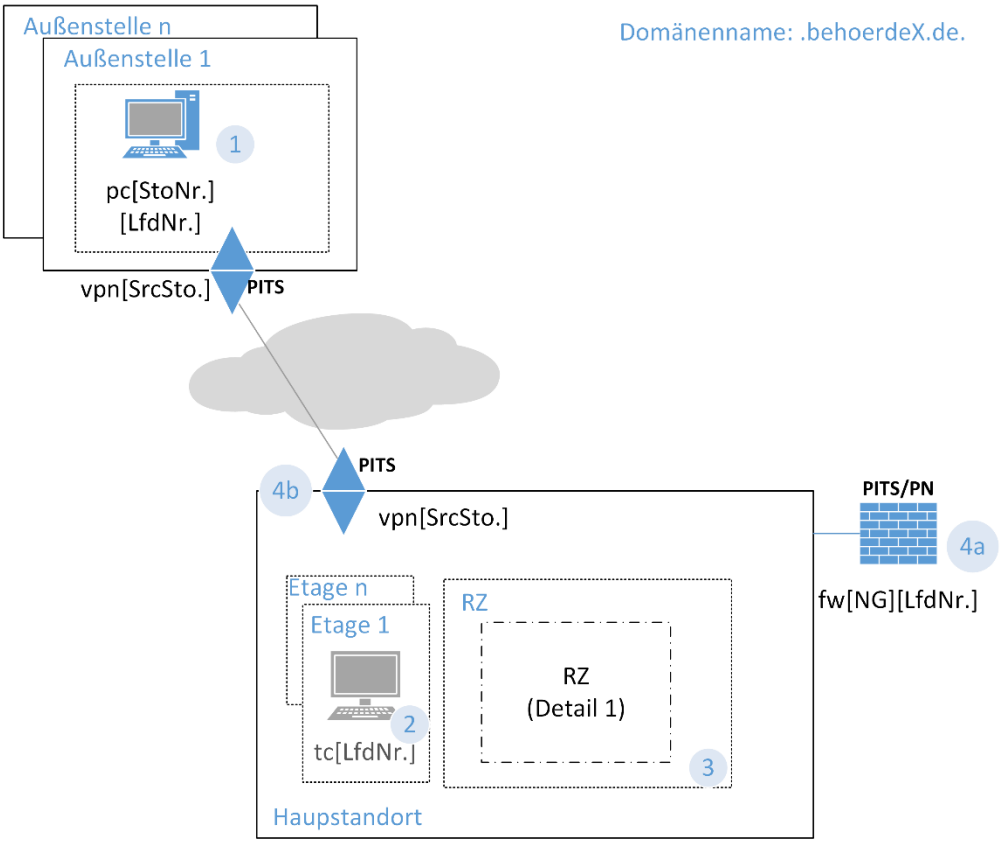

Abbildung 7: Beispiel für IT-Systembezeichnungen (Teil 1)

Um eine Beziehung zwischen der Protokollierungslandkarte und den tatsächlichen Protokollierungsquellen herstellen zu können, ist es erforderlich eine Systematik zu entwickeln, die IT-Systeme in der Protokollierungslandkarte zu bezeichnen.

In Abbildung 7 sind drei verschiedene protokollierende IT-Systemgruppen eingezeichnet. Nr. 1 stellt einen Fat-Client dar, der in den Außenstellen einer Beispielbehörde zum Einsatz kommt. Welche Ereignisse hier protokolliert werden, würde im Anhang zur Protokollierungslandkarte beschrieben werden. Ein Verweis auf die Anlagen der PR-B kann ausreichend sein, wenn darüber hinaus nichts protokolliert werden soll.

Die Bezeichnung „pc[StoNr.][LfdNr.]“ ist das Schema woraus sich der Domänenname des jeweiligen Fat-Client ergibt. Im Hauptstandort werden Thin-Clients eingesetzt, dies ist in Nr. 2 dargestellt. Das Symbol ist grau, da für Thin-Clients derzeit keine Protokollierungsrichtlinie existiert. In dieser Protokollierungslandkarte existieren auch noch zwei Netz-IT-Systeme, welche ausschließlich aus IT-System-Sicht protokollieren (siehe Nr. 4a und Nr. 4b). Bei Netz-IT-Systemen muss zwingend angegeben werden, ob Protokollierungsdaten aus IT-System-Sicht (PITS) und/oder Protokollierungsdaten aus Netz-Sicht (PN) erfasst werden, da die Protokollierungslandkarte sonst nicht semantisch eindeutig ist.

In diesem Fall liefern die Verschlüsselungsgeräte nur PITS und die Firewall sowohl PITS als auch PN. Die Systeme im Rechenzentrum wurden in eine Detaillierung ausgelagert (siehe Nr. 3 und Abbildung 8).

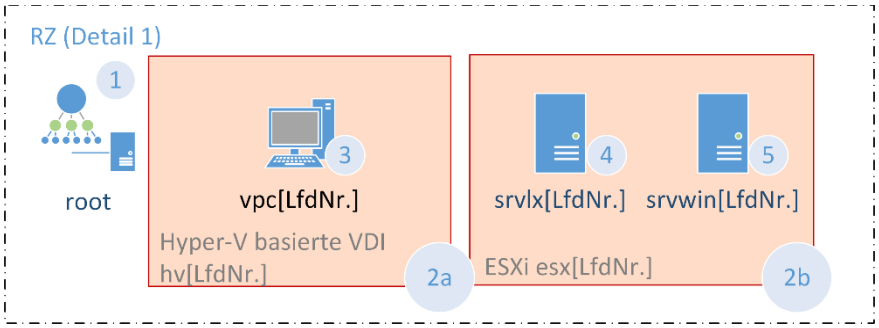

Abbildung 8: Beispiel für IT-Systembezeichnungen (Teil 2)

In der Detaillierung sind drei verschiedene physische Servergruppen eingezeichnet: 1) der oder die Domänen-Root-Server, 2a) Hyper-V Hosts, die zur Virtualisierung der Desktops am Hauptstandort benutzt werden und 2b) ESXi Hosts, die zur Virtualisierung der restlichen Server Infrastruktur benutzt werden. Da auch hier Hyper-V und ESXi grau hinterlegt sind, dient dies nur zur Information, die Systeme selbst protokollieren nicht. Die virtualisierten Desktops protokollieren hingegen schon (siehe Nr. 3). Ebenso protokollieren die virtualisierten Linux- (siehe Nr. 4) und Windows-Server (siehe Nr. 5). Auch hier gilt, dass die umgesetzte operative Protokollierungsrichtlinie im Anhang zur Protokollierungslandkarte dokumentiert sein muss (mindestens durch einen Verweis auf die Anforderungen in der PR-B).

5.3 Dokumentation der Netzgrenzen (Fortgeschritten)

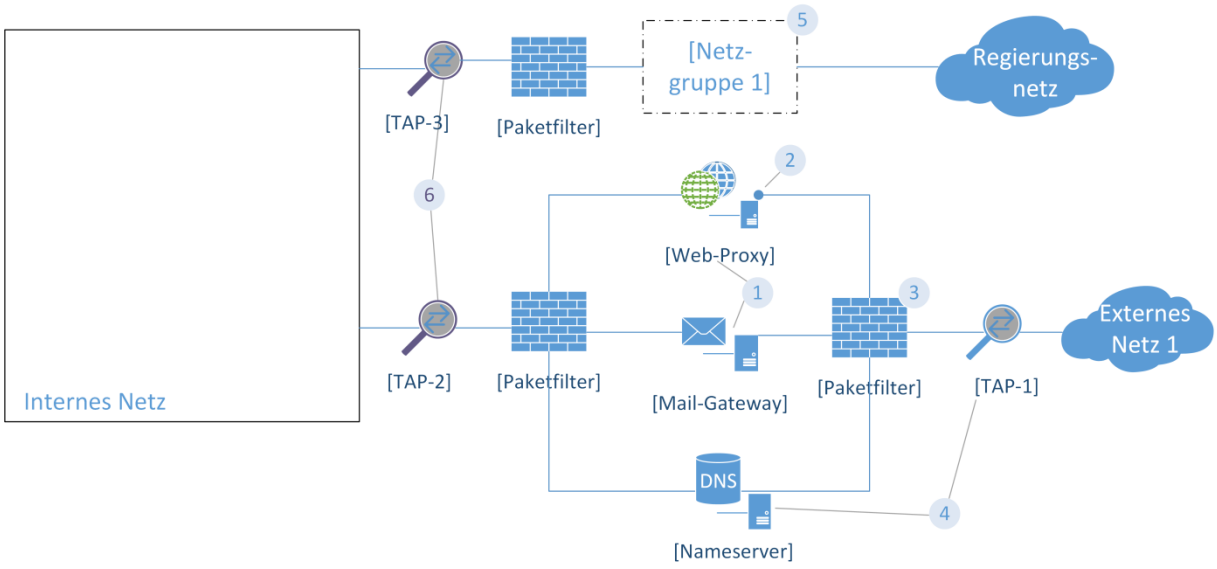

Abbildung 9: Ausschnitt Netzgrenzen (Fortgeschritten)

Bei der Identifizierung der Netzgrenzen wurde im Beispiel in Abbildung 9 zum einen das Regierungsnetz und zum anderen „Externes Netz 1“ identifiziert. Die IT-Systeme zur Absicherung des Übergangs zum Regierungsnetz wurden in dieser Abbildung abstrahiert dargestellt (Nr. 5). Bei der Kommunikation zum „Externen Netz 1“ werden offenbar Web-Protokolle und E-Mail benutzt, da hierfür entsprechende Proxys oder ALGs installiert wurden (siehe Nr. 1). Der Web-Proxy führt NAT durch. Aus diesem Grund sind rechts vom Web-Proxy keine internen IP-Adressen mehr zu erkennen. Da dies für die Protokollierung von hoher Relevanz ist, wird dies in diesem Beispiel durch den Punkt ausgehend vom Web-Proxy illustriert (siehe Nr. 2). Würde das NAT durch den äußeren Paketfilter (siehe Nr. 3) durchgeführt werden, dann wäre dort der Punkt einzuzeichnen. Als zusätzliche präventive Maßnahmen sind in diesem Szenario ausschließlich Paketfilter eingezeichnet. Des Weiteren nutzt die Behörde zur Namensauflösung einen Nameserver im „Externen Netz 1“; hierfür wird ein Nameserver genutzt, der in der Protokollierungslandkarte entsprechend dargestellt wurde. Gemäß den Anforderungen PRB.III.2.1.1.3 und PRB.III.2.1.1.4 hat die Behörde am Uplink

zum „Externen Netz 1“ einen TAP installiert (siehe Nr. 4) Da Behörden mit erhöhten Sicherheitsbedürfnissen an den Netzgrenzen noch weitere TAPs einrichten müssen, finden sich diese bei der Nr. 6.

In Abbildung 9 lassen sich die einzelnen IT-Systeme sehr gut dem jeweiligen Netz zuordnen. Bei der Erstellung der Protokollierungslandkarte ist darauf zu achten, dass die Darstellung eindeutig ist. Ggf. muss mehr beschreibender Text eingefügt werden.

5.4 Dokumentation der Netzbereiche (Fortgeschritten)

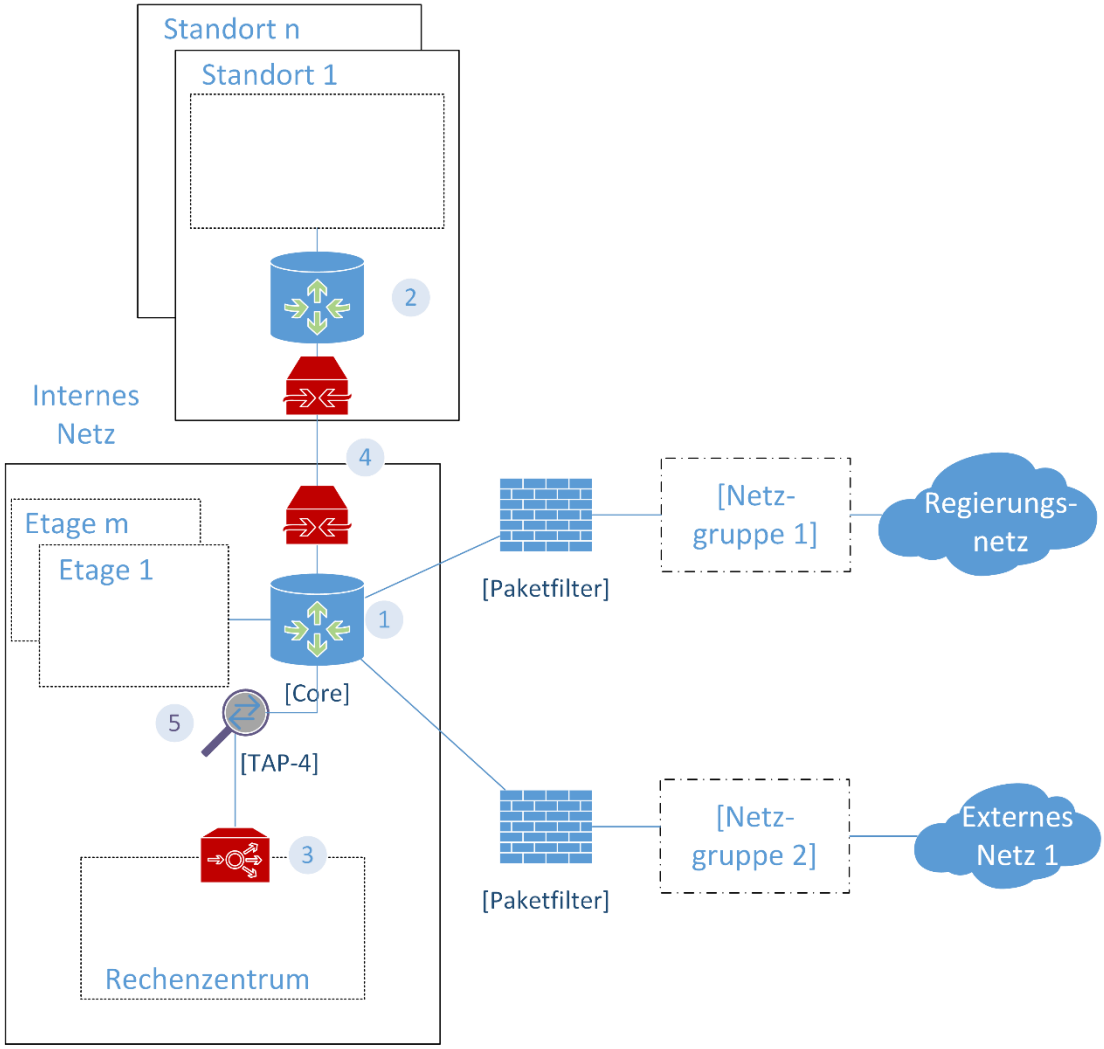

Abbildung 10: Ausschnitt Netzbereiche (Fortgeschritten)

In dem in Abbildung 10 dargestellten Szenario gibt es einen Hauptstandort mit m Etagen und n Nebenstandorten. In jedem Standort befindet sich ein IT-System der Vermittlungsschicht (siehe Nr. 1 und Nr. 2). Aufgrund der Protokolldaten von diesen Systemen wird die Netzkommunikation der einzelnen Netzbereiche untereinander (kurz gestrichelt dargestellt) sichtbar. Es ist zu beachten, dass wenn das IT-System in Nr. 2 nicht vorhanden wäre, eine Kommunikation zwischen den Nebenstandorten nicht sichtbar wäre.

Ohne weitere Ergänzungen würde man nun annehmen, dass jede Kommunikation eines IT-Systems aus einem Netzbereich mit dem eines anderen in den Protokolldaten sichtbar würde. In diesem Szenario ist das jedoch nicht der Fall und auch dies muss in der Dokumentation der Protokollierung festgehalten werden. In Nr. 3 findet sich zum Beispiel ein Load Balancer, welcher adressiert wird. Die Kommunikation der

eigentlichen IT-Systeme im Rechenzentrum kann dadurch z. B. vollständig verdeckt sein. Ähnliches findet sich bei Nr. 4: Die Behörde in diesem Szenario setzt WAN-Beschleuniger ein. Da diese Systeme den Verkehr optimieren und Anfragen cachen, können auch hier Abweichungen zwischen dem protokollierten und tatsächlichen Verkehr entstehen. Derartige Systeme wie in Nr. 3 und Nr. 4 müssen dokumentiert werden, da es ansonsten bei der Auswertung der Protokollierungsereignisse zu Fehlinterpretationen kommen kann.

Da es sich um eine Behörde mit erhöhten Sicherheitsanforderungen handelt, ist bei Nr. 5 ein zusätzliches TAP eingezeichnet. In diesem sehr einfachen Szenario ist das gesamte Rechenzentrum ein besonders schützenswerter Bereich. Je nach Aufbau des Load Balancers könnten eine alternative Unterbringung des TAPs im Rechenzentrum oder die Verwendung von Spiegelports das Mittel der Wahl darstellen. Wichtig bei der Auswahl des Standortes ist, dass die gesamte zu protokollierende Kommunikation auch ausschließlich über die gewählten Stellen fließt und keine Seitenkanäle existieren.

5.5 Dokumentation der Netzvirtualisierung

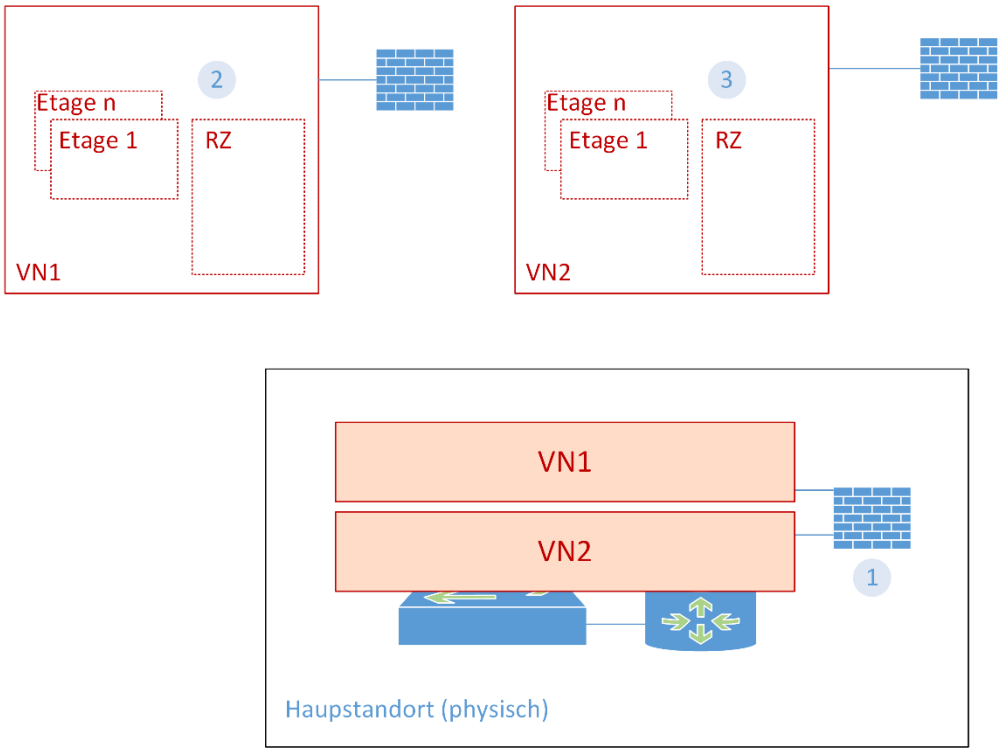

Abbildung 11: Beispiel Netzvirtualisierung

Werden auf einer gemeinsamen physischen Infrastruktur zwei Netze vollständig virtualisiert getrennt bereitgestellt (z. B. mehrere VLANs ohne Inter-VLAN-Routing), dann ist es für die Übersichtlichkeit der Protokollierung empfehlenswert pro virtualisiertes Netz eine Landkarte zu erstellen (siehe Nr. 2 und Nr. 3 in Abbildung 11).

Darüber hinaus wird noch eine weitere Protokollierungslandkarte benötigt, die im unteren Teil der Abbildung sehr abstrakt dargestellt ist. Die beiden virtualisierten Netze werden hier mit „VN1“ und „VN2“ bezeichnet. Sie werden über ein Sicherheitsgateway zusammengeführt (siehe Nr. 1), welches in die Protokollierung aufgenommen werden soll. Die darunterliegenden Komponenten (gruppierte Darstellung: ein Switch, ein Router) würden in diesem Fall ebenfalls in die Protokollierung als IT-System mit aufgenommen werden (sofern gem. PR-B erforderlich).

5.6 Dokumentation der Virtualisierung im Szenario IT-Dienstleister des Bundes

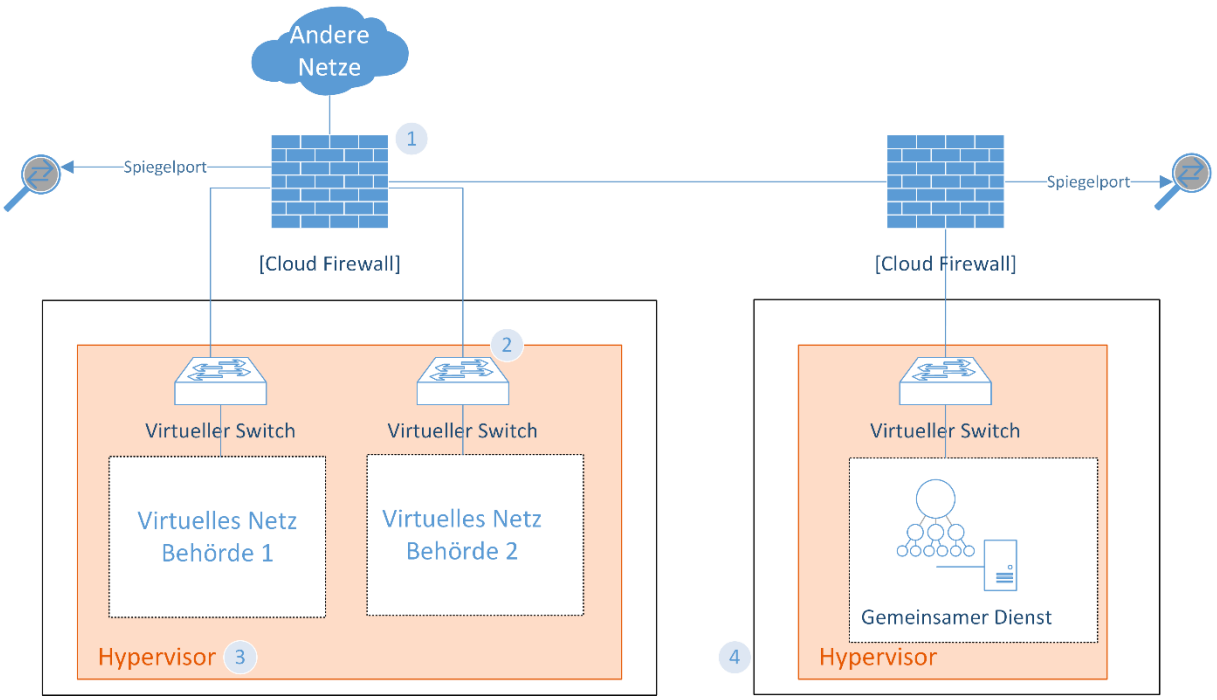

Abbildung 12: Beispiel Virtualisierung IT-Dienstleister des Bundes

In diesem Beispielszenario (siehe Abbildung 12) werden auf einem logischen Hypervisor zwei Behördennetze gemeinsam virtualisiert. Entsprechend den Anforderungen der PR-B ist die Kommunikation so eingeschränkt worden, dass diese Netze ausschließlich über eine „Cloud-Firewall“ untereinander, mit anderen Netzen oder den gemeinsam genutzten Diensten kommunizieren können (siehe Nr. 1). Die Cloud-Firewall bietet die Möglichkeit, Protokolldaten der Stufe 4 über einen Spiegelport zu erheben. In diesem Szenario ist es möglich, dass die virtuellen Switche Protokolldaten der Stufe 2 erzeugen (siehe Nr. 2), so dass keine zusätzlichen virtuellen Maschinen benötigt werden. Im Beispiel wurden noch keine Protokollierungsdaten für den Hypervisor konfiguriert, so dass der gesamte Bereich der Virtualisierung rot eingezeichnet werden muss (siehe Nr. 3). Der gemeinsam genutzte Dienst wird entsprechend den Anforderungen der PR-B in einem physisch abgegrenzten anderen Netz betrieben (siehe Nr. 4). Der Zugriff kann über die zugehörige Firewall protokolliert werden.

Bundesamt
für Sicherheit in der
Informationstechnik

Rahmendatenschutzkonzept Protokollierung und Detektion

von Cyber-Angriffen auf die Bundesverwaltung – Version 1.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: protokollierungsrichtlinie@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Dieses Konzept bildet den Rahmen für alle Datenschutzkonzepte, die im Rahmen von § 5 BSIG oder des Mindeststandards des BSI zur Protokollierung und Detektion von Cyber-Angriffen erstellt werden. Dieses Datenschutzkonzept gibt die Möglichkeiten vor, unter denen gemäß den (gesetzlichen) Erfordernissen der jeweiligen beteiligten Behörden konkrete, für die jeweilige Situation angemessene Datenschutzkonzepte erstellt werden können.

Ziel ist es, dass dieses Rahmendatenschutzkonzept möglichst wenigen Änderungen unterliegt, grundsätzlich abgestimmt werden kann und es dann allen Beteiligten erleichtert, spezifische Datenschutzkonzepte zu erstellen. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ist im Rahmen der Konzepterstellung durch die Möglichkeit zur Stellungnahme beteiligt worden.

1.1 Definition und Abgrenzung von Protokollierungsdaten

Zur Erkennung von IT-Sicherheitsvorfällen werden durch Einzelbehörden, durch die IT-Dienstleister des Bundes und durch das BSI an verschiedenen Stellen in den Netzen der Bundesverwaltung Protokollierungsdaten erhoben. Diese Daten können personenbezogene Daten beinhalten (siehe Kapitel 2.1).

IT-Sicherheitsvorfälle sind Ereignisse, die sich negativ auf die Verfügbarkeit, Integrität oder Vertraulichkeit des Informationsverbundes auswirken, innerhalb dessen die Protokollierungsdaten erhoben werden.

Protokollierungsdaten 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.

Das Ziel der hier beschriebenen Protokollierung ist *nicht* die Nachweisführung über den Zugang von Personen zu Informationen zu betreiben.

Sollen mit dieser Form der Protokollierung auch Innentäter, z. B. der Datenabfluss über lokale Datenträger oder Drucker erkannt werden können, ist das vorliegende Datenschutzkonzept um die Nutzung der Daten zu diesem Zweck zu erweitern.

1.2 Relevante Unterscheidung personenbezogener Daten

Das in diesem Konzept beschriebene Verfahren verarbeitet personenbezogene Daten zweier gänzlich unterschiedlicher Typen. Die beiden Datentypen unterscheiden sich in der gesetzlichen Grundlage auf der sie erhoben werden und damit auch in den Details ihrer Verarbeitung. Personenbezogene Daten von Typ 1 fallen bei der Erledigung von dienstlichen Tätigkeiten innerhalb der Bundesverwaltung an. Personenbezogene Daten von Typ 2 entstehen bei der Kommunikation über die Netzgrenzen der Bundesverwaltung hinaus mit Personen außerhalb der Bundesverwaltung. Sie können daher Informationen über Dritte außerhalb der Bundesverwaltung oder über private Belange von Mitarbeitern der Bundesverwaltung enthalten.

Personenbezogene Daten vom Typ 1 dürfen ausschließlich zum Schutz der Informationstechnik des Bundes verarbeitet werden. Eine andere Verwendung darüber hinaus, wie z. B. für eine Leistungskontrolle von Mitarbeitern, ist unzulässig. Das Erheben von Daten zur Identifikation von Einzelpersonen ist daher eigentlich nicht erforderlich. Technische Daten wie MAC- oder IP-Adressen, die für Analysen notwendig sind, lassen jedoch Rückschlüsse auf die jeweilige Person zu und stellen somit personenbezogene Daten dar.

Da Bundesbehörden teilweise die private Nutzung der Kommunikationstechnik des Bundes erlauben, ist bei personenbezogenen Daten vom Typ 1 nicht zweifelsfrei ausgeschlossen, dass es sich hier auch um private Belange handeln kann.

Für personenbezogene Daten vom Typ 2 gilt, dass diese ausschließlich unter den Randbedingungen von § 5 BSIG verarbeitet werden dürfen und hier somit sehr hohe Anforderungen z. B. an die Pseudonymisierung gestellt werden. Diese Daten sind erforderlich, um einen Täter oder eine Tätergruppe eines Cyber-Angriffes ermitteln zu können und daher besteht hier tatsächlich ein Interesse an der Kenntnis der Person, weswegen in diesem Fall eine wesentlich höhere Anforderung an den Schutz zu stellen ist.

Diese Unterscheidung wird im Beispiel „Pseudonymisierungskonzept“ (siehe Kapitel 5) wieder aufgegriffen.

2 Verfahren zur zentralen Protokollierungsdatenerhebung und -verwendung für die Detektion von Cyber-Angriffen (PDEV-CA)

2.1 Bezeichnung der personenbezogenen Daten und betroffene Rechte

Protokollierungsdaten sind historische Aufzeichnungen über die Art und Weise wie IT-Systeme genutzt wurden und wie diese miteinander kommuniziert haben. Entsprechend lassen sich diese Daten in zwei Sichten einordnen: die IT-System-Sicht und die Netz-Sicht. Diese Systematik ist in Tabelle 1 zusammenfassend dargestellt. Es ist zu berücksichtigen, dass dieses Konzept explizit für die Bundesverwaltung erstellt wird.

Sicht	Betroffene Rechte
Protokollierungsdaten aus IT-System-Sicht (PITS)	Recht auf informationelle Selbstbestimmung (Art 2 Abs. 1, Art. 1 Abs. 1 GG; Art. 8 Abs. 1 GRCh; Art. 8 Abs. 1 EMRK)
Protokollierungsdaten aus Netz-Sicht (PN) (= Protokolldaten i.S.V. § 2 Abs. 8 BSIG)	Recht auf informationelle Selbstbestimmung (Art 2 Abs. 1, Art. 1 Abs. 1 GG; Art. 8 GRCh; Art. 8 EMRK) und Art. 10 GG (Fernmeldegeheimnis)

Tabelle 1: Abgrenzung von Protokollierungsdaten

Bei Protokollierungsdaten der IT-System-Sicht (PITS) werden entweder Informationen über den Zustand des IT-Systems selbst oder Meta-Informationen über die auf dem IT-System verarbeiteten Daten (Data-in-Use) sowie die gespeicherten Inhaltsdaten (Data-at-Rest) dokumentiert. Diese Daten befinden sich vollständig im alleinigen Herrschaftsbereich der jeweiligen Behörde. Über die System- oder Nutzerkennung, welche in den Protokollierungsdaten enthalten ist, lässt sich jedenfalls indirekt ein Personenbezug herstellen. Aus diesem Grund sind die Vorgaben der DSGVO und des BDSG bei der Verarbeitung dieser Daten zu beachten.

Bei Protokollierungsdaten der Netz-Sicht (PN) werden immer Meta-Informationen über einen Datenaustausch/Kommunikationsvorgang (Data-in-Motion) zwischen zwei IT-Systemen dokumentiert. Diese Daten werden gem. § 2 Abs. 8 BSIG als Protokolldaten legal definiert und daher im Folgenden so bezeichnet. Da in Bezug auf diese Daten ein Personenbezug nicht ausgeschlossen werden kann, sind hier ebenfalls die im konkreten Fall relevanten Regelungen der DSGVO und des BDSG zu beachten. Zusätzlich handelt es sich bei den Protokolldaten – anders als bei den PITS – um Kommunikationsdaten, die von dem Schutzbereich des Fernmeldegeheimnisses erfasst werden. Eine Verarbeitung dieser Daten stellt dementsprechend einen Eingriff in Art. 10 GG dar. Eine Erhebung und Auswertung zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes ist bezüglich der Protokolldaten daher nur durch das BSI – auf Grundlage des § 5 BSIG – möglich.

Detaillierte Ausführungen zu den unterschiedlichen Protokollierungsdaten und den verschiedenen Sichten sind in der Protokollierungsrichtlinie Bund (PR-B) aufgeführt.

2.2 Rechtliche Ermächtigung zur Datenverarbeitung

Die Bundesverwaltung ist fortgeschrittenen Angriffen auf die Informations- und Kommunikationstechnik ausgesetzt. Die Wirksamkeit der Präventionsmaßnahmen ist nur durch ein kontinuierliches Monitoring der Protokollierungsdaten überprüfbar. Insbesondere können durch das Monitoring Angriffe festgestellt werden, welche die Präventionsmaßnahmen umgangen haben. Aus diesem Grund legt die Leitlinie für die

Informationssicherheit in der Bundesverwaltung (UP Bund 2017) in Kapitel 9 Maßnahmen für die Detektion und Reaktion fest. Grundlage hierfür sind die Erhebung und Auswertung von Protokollierungsdaten. Die weiteren Anforderungen ergeben sich aus den Bausteinen OPS.1.1.5 *Protokollierung* und DER.1 *Detektion von sicherheitsrelevanten Ereignissen* des IT-Grundschutz-Kompendiums.

Diese Anforderungen sind im Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen sowie der PR-B weiter konkretisiert. Für Protokolldaten stellt § 5 Abs. 1 Satz 1 Nr. 1 BSIG eine Rechtsgrundlage des BSI für die Verarbeitung dar. In § 5 Abs. 1 Satz 4 BSIG wird eine Pflicht für alle Bundesbehörden statuiert, wonach diese das BSI bei Maßnahmen nach § 5 Abs. 1 S. 1 BSIG unterstützen und Zugang zu behördeninternen Protokolldaten gewähren müssen. In Verbindung mit Art. 6 Abs. 1 lit. c) DSGVO stellt § 5 Abs. 1 Satz 1 Nr. 1 BSIG dementsprechend die rechtliche Grundlage für eine rechtmäßige Verarbeitung dar. Des Weiteren stellt Art. 6 Abs. 1 lit. f) DSGVO – unter Berücksichtigung der Wertung aus Erwägungsgrund 49 der DSGVO – bezüglich der Protokollierungsdaten die nicht in den Anwendungsbereich des § 5 BSIG fallen (PITS) eine Grundlage für die Bundesbehörden bei der Verarbeitung personenbezogener Daten dar.

2.3 Speicherfristen

Die Speicherfrist aller Protokollierungsdaten beträgt 90 Tage. Nach Ablauf der 90 Tage sind alle Protokollierungsdaten unwiderruflich zu löschen. Dieser Zeitraum wird gemeinsam mit der BfDI nach 2 Jahren neu evaluiert und ggf. neu festgelegt (vgl. PR-B). Die Speicherfrist für die Protokollierungsdaten des Datenschutzaudits ist vom Auditierungsintervall durch die berechtigten Rollen abhängig.

Die Speicherung aller Protokollierungsdaten für den Zeitraum von 90 Tagen ist für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig. Es besteht zudem ein berechtigtes Interesse der Bundesbehörden widerrechtliche oder mutwillige Eingriffe, die die Verfügbarkeit, Authentizität, Vollständigkeit oder Vertraulichkeit der Informationstechnik des Bundes beeinträchtigen, zu erkennen und zu analysieren (Detektion, Verifikation) um diese abzuwehren (Reaktion).

Für die Protokolldaten ergibt sich die Grundlage für die Speicherfrist unmittelbar aus § 5 BSIG.

Die Speicherfrist der anderen Protokollierungsdaten (PITS) beträgt aus den o.g. Gründen ebenfalls 90 Tagen. Diese 90 Tage sind – wie auch bei den § 5-Daten – erforderlich, um die Netz- und Informationssicherheit der eigenen IT der Bundesbehörden in angemessener Form zu gewährleisten. Bezüglich der personenbezogenen Daten in diesen PITS ist Art. 6 Abs. 1 lit. f) DSGVO – vor der Wertung des Erwägungsgrundes 49 der DSGVO – für die Bundesbehörden die Grundlage für die Speicherung.

2.4 Architektur und Schnittstellen

Die generische Architektur sowie die Prozesse von PDEV-CA sind in Abbildung 1 dargestellt und werden im Folgenden erläutert. Eine Beschreibung der Rollen und Rechte erfolgt in Kapitel 2.6. Detaillierte Erläuterungen zu den technischen Maßnahmen finden sich in Kapitel 4.

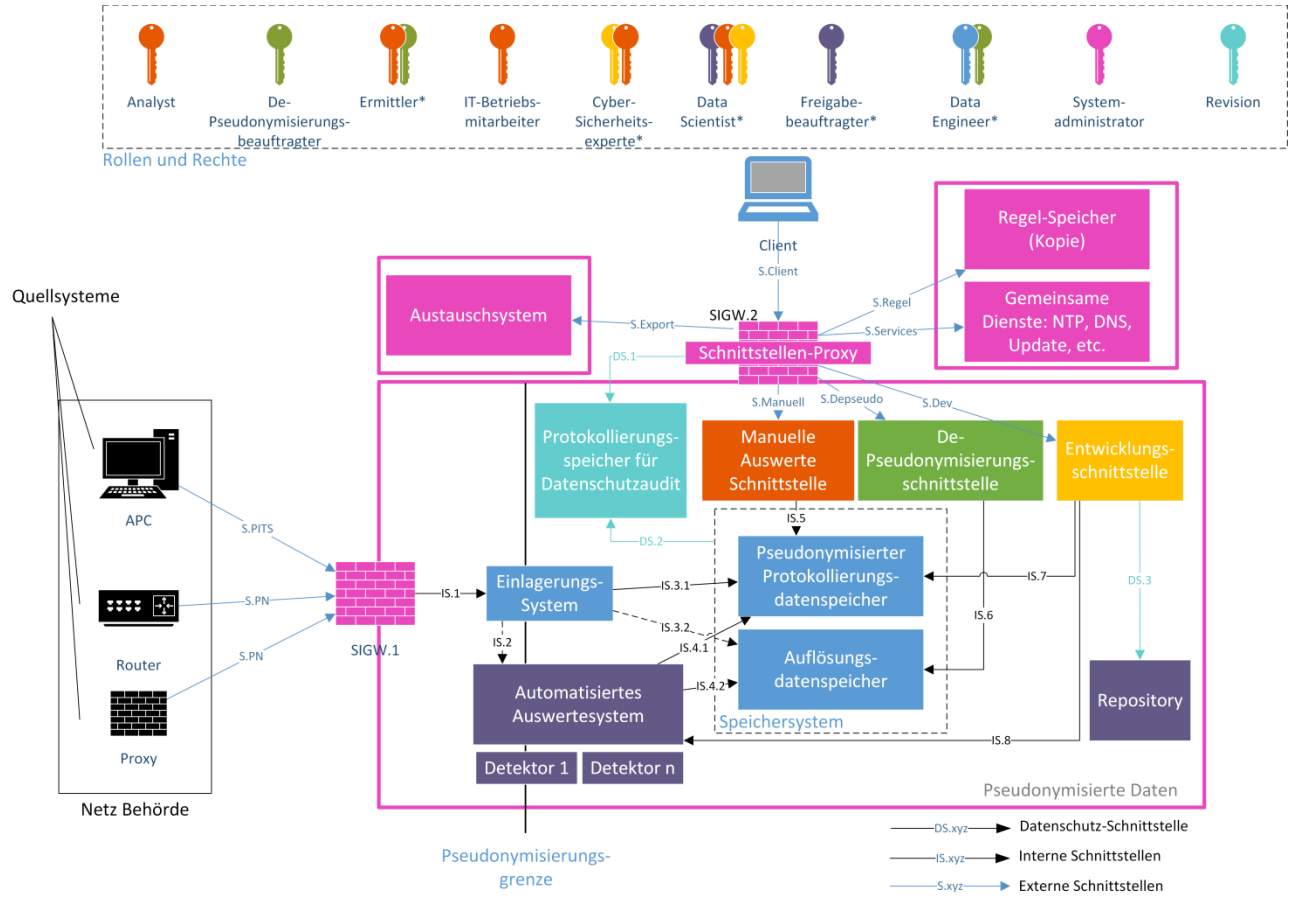

Abbildung 1: Architekturskizze PDEV-CA mit Schnittstellen

Protokollierungsdaten werden auf den Quellsystemen (z. B. Router, Proxies und APCs) erfasst und von dort an das sog. Einlagerungssystem weitergeleitet (S.PITS, S.PN und IS.1)[1]. Die Kommunikation zwischen IT-Systemen und Datenquellen wird durch ein Sicherheitsgateway (SIGW.1) abgesichert.

Die Quellsysteme liegen außerhalb des PDEV-CA und sind daher nicht durch das vorliegende Datenschutzkonzept erfasst. Aus Sicht dieses Konzeptes sollte die Speicherung der Daten auf diesen Systemen so kurz wie möglich erfolgen.

Das Einlagerungssystem bildet die erste Komponente im PDEV-CA und erfüllt hinsichtlich des Datenschutzes die Aufgabe ankommende Protokollierungsdaten zu pseudonymisieren (sofern personenbezogene Daten vorhanden und diese nicht bereits pseudonymisiert erfasst werden, siehe hierzu Kapitel 5). Das Einlagerungssystem legt die pseudonymisierten Protokollierungsdaten im Protokollierungsdatenspeicher ab (IS.3.1) und das Pseudonym mit zugehörigem Klartext im Auflösungsdatenspeicher (IS.3.2). Zusammen bilden der Protokollierungsdatenspeicher und der Auflösungsdatenspeicher das Speichersystem. Dieses bildet die Basis für alle anderen Teil-Systeme und Schnittstellen. Alle Zugriffe auf das Speichersystem werden protokolliert und in dem Protokollierungsspeicher für den Datenschutzaudit abgelegt (DS.2).

Das automatisierte Auswertesystem greift auf das Speichersystem zu (IS.4.1) und analysiert mit sog. Detektoren den Datenbestand, um sicherheitsrelevante Ereignisse zu finden. Ein Detektor kann auch eine Auflösung der Pseudonymisierung vornehmen (IS.4.2). Abhängig von den eingehenden Daten schickt das Einlagerungssystem die Daten ggf. direkt bei der Einlagerung zum automatisierten Auswertesystem (IS.2) und parallel zum Speicher-System. Es gibt verschiedene Arten von Detektoren (siehe Kapitel 2.5.1.1). Eine Art von Detektoren arbeitet regelbasiert. Hierzu ist es erforderlich, regelmäßig neue Regelsätze

[1]Diese Verweise beziehen sich auf Abbildung 1. Sie werden in dieser Form in den übrigen Kapiteln verwendet.

bereitzustellen, die außerhalb von PDEV-CA generiert werden. Das automatisierte Auswertesystem kann zur Aktualisierung auf eine Kopie des Regel-Speichers zugreifen (S.Regel).

Die Ergebnisse der Detektoren werden entweder einzeln oder in Korrelation untereinander in das Speichersystem geschrieben (entweder als einzelnes Datum oder als Anreicherung eines bisher gespeicherten Datensatzes). Die Ergebnisse werden wieder vollständig pseudonymisiert gespeichert, so dass ausschließlich der automatisierte Prozess eine Auflösung der Pseudonymisierung vornimmt.

Der manuelle Zugriff auf PDEV-CA erfolgt ausschließlich über Clients, die mindestens für VS-Nur für den Dienstgebrauch (VS-NfD) zugelassen sind. Zugriffe dürfen ausschließlich (S.Client) über die drei angebotenen Schnittstellen erfolgen:

- Manuelle Auswerte-Schnittstelle (S.Manuell)
- De-Pseudonymisierungsschnittstelle (S.Depseudo)
- Entwicklungsschnittstelle (S.Dev)

Die Kommunikation zwischen Client und den Schnittstellen wird durch ein Sicherheitsgateway (SIGW.2) abgesichert. Dieses protokolliert die Kommunikation und speichert sie im Protokollierungsspeicher für den Datenschutzaudit (DS.1).

Zum Exportieren von Daten aus dem PDEV-CA (für die Notwendigkeit siehe Kapitel 2.5, *UC.007*) ist ein Austauschsystem (S.Export) vorgesehen. Der Datentransfer zum Austauschsystem kann nur aus dem PDEV-CA heraus veranlasst werden, es wird also immer ein authentifizierter Client hierfür benötigt.

2.4.1 Manuelle Auswerte-Schnittstelle

In der manuellen Auswerte-Schnittstelle werden die Ergebnisse der Detektoren als sicherheitsrelevantes Ereignis (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen*) angezeigt. Die berechtigten Rollen können sich hierüber alle pseudonymisierten Protokollierungsdaten, die im Zusammenhang mit diesem sicherheitsrelevanten Ereignis stehen, anzeigen und daraufhin ermitteln, ob es sich tatsächlich um einen Sicherheitsvorfall handelt.

2.4.2 De-Pseudonymisierungsschnittstelle

Die De-Pseudonymisierungsschnittstelle dient dazu Anträge zur De-Pseudonymisierung zu stellen und zu genehmigen. Nach erfolgter Genehmigung wird durch die Pseudonymisierungsschnittstelle der Zugriff des Antragsstellers auf die pseudonymisierten Daten gewährt. Dies ist allerdings nur möglich, sofern die Pseudonymisierung innerhalb von PDEV-CA und nicht schon zuvor erfolgt ist.

Der Antrag kann auf einem Auswerteergebnis beruhen oder zur Qualitätssicherung ein Zufallsereignis eines beantragten Protokollierungsdatentyps darstellen.

2.4.3 Entwicklungsschnittstelle (BSI)

Um neue Detektoren entwickeln zu können, ist die Auswertung der pseudonymisierten Protokollierungsdaten auch ohne vorliegendes sicherheitsrelevantes Ereignis erforderlich (IS.7). Ein Detektor dient gerade dazu dieses erst zu generieren. Für diese andere Art der Auswertung dient die Entwicklungsschnittstelle, welche im Gegensatz zur manuellen Auswerte-Schnittstelle die Möglichkeit zur Programmierung besitzt. Zur Ausführung der in der Entwicklung befindlichen Detektoren wird das automatisierte Auswertesystem verwendet (IS.8). Um auch hier eine Dokumentation zu gewährleisten, werden alle erstellten Programme und Ergebnisse in einem Repository versioniert abgelegt (DS.3).

2.5 Abzubildende Prozesse und Aktivitäten

Das Verfahren PDEV-CA muss die Prozesse „Detektion und Verifikation“, „Reaktion“ und „Entwicklung Detektor und Qualitätssicherung“ unterstützen. Damit das Verfahren zuverlässig zur Verfügung gestellt

werden kann, ist ebenfalls der Prozess „Systembetrieb und -entwicklung“ abzubilden. Die Prozesse werden im Folgenden beschrieben. Aus diesen Prozessen werden Anwendungsfälle (engl. use case, UC) und aus diesen wiederum Anforderungen an die Daten abgeleitet (engl. data requirement, DR).

2.5.1 Prozess „Detektion und Verifikation“

PDEV-CA muss im Kern den Prozess Detektion und Verifikation von sicherheitsrelevanten Ereignissen abbilden. Die Detektion ist vollständig automatisiert. Die Verifikation erfolgt manuell bzw. teil-automatisiert. Die Verifikation wird durch den Analysten durchgeführt (siehe Kapitel 2.6) und ist erforderlich, da die Detektion falsch-positive Ergebnisse liefern kann.

2.5.1.1 Aktivität „Detektieren“

Detektieren basiert immer auf einem Detektor (bzgl. der Anforderung zur Entwicklung eines Detektors siehe Kapitel 2.5.3). Detektoren lassen sich in drei Kategorien einteilen, welche durch die folgenden Anwendungsfälle beschrieben werden:

- *UC.001* Signaturbasierter Detektor
- *UC.002* Vorgehensbasierter Detektor
- *UC.005* Statistischer Detektor

Es können beliebig viele Detektoren auf die Daten angewendet werden. Ein Detektor ordnet jedem Ergebnis eine Zuverlässigkeit (engl. confidence) zu. Diese gibt an, wie wahrscheinlich es ist, dass es sich nicht um ein falsch-positives sicherheitsrelevantes Ereignis handelt. Zusätzlich ist dem Detektor eine Gefahrenstufe (engl. threat level) zugeordnet. Diese gibt an, wie groß die Bedrohung eines durch den Detektor erkanntes Ereignis ist, sofern dieses kein falsch-positives sicherheitsrelevantes Ereignis ist. Zusätzlich können die Detektoren über Korrelationen (z. B. zeitliche Korrelation) miteinander in Verbindung gesetzt werden. D. h. ein sicherheitsrelevantes Ereignis entspricht entweder dem Ergebnis eines Detektors oder der korrelierten Ergebnisse mehrerer Detektoren. Ein Detektor ist ein automatisierter Prozess und kann damit auch auf die Klartextdaten zugreifen.

UC.001 Signaturen prüfen / Abgleich mit Indikatoren

Bei diesem Anwendungsfall erfolgt entweder zum Zeitpunkt der Erfassung der Protokollierungsdaten oder zu einem späteren Zeitpunkt während der Speicherfrist (siehe Kapitel 2.3) ein Abgleich des Datums mit einer bekannten Liste von Signaturen/ Indikatoren. Diese Liste der Signaturen kann anlassbezogen ergänzt werden. Oder sie wird durch einen Signatur-Server automatisch aktualisiert. Es ist eine mindestens tägliche automatisierte Prüfung aller derzeit gespeicherten Protokollierungsdaten gegen die Signatur-Liste erforderlich.

Schlägt eine Signatur/ ein Indikator an, kann hieraus noch nicht unmittelbar auf einen Angriff geschlossen werden. Das Verdachtsmoment muss dazu häufig noch erhärtet werden (siehe *UC.003*).

DR.001: Zum Abgleich mit einer Signatur müssen die Daten in unveränderter Form vorliegen oder es muss eine Transformationsregel existieren, welche die Signatur auf die gespeicherten Daten abbilden kann.

UC.002 Vorgehen erkennen

Die Signaturprüfung prüft gegen bereits bekannte Erkenntnisse. Diese sind im Kontext der Erkennung von fortgeschrittenen Angriffen (APTs) jedoch mehr ein notwendiges Erfordernis als letztlich der ausschlaggebende Faktor, um APTs zu finden (z. B. könnte im Rahmen einer Incident Response in einem anderen EU-Land durchaus eine Signatur gefunden werden, die auch in der Bundesverwaltung anschlägt). Ein erster Schritt APTs zu erkennen, ist die Abstraktion von bekannt gewordenen Angriffen auf das zu Grunde liegende Vorgehen des Angreifers. Hieraus wird ein Modell entwickelt und im Anschluss wird geprüft, ob die Protokollierungsdaten dem Modell entsprechen. Es ist sehr wahrscheinlich, dass diese Erkennungsmethode falsch-positive Ergebnisse liefert, so dass auch hier eine Erhärtung des Verdachtsmoments erforderlich wird (siehe *UC.003*).

DR.002: Für diese Methode ist es ausreichend, wenn einzelne Daten oder deren Bestandteile verändert vorliegen. Allerdings dürfen die technischen Parameter der Datensätze nicht verändert worden sein (z. B. durch weglassen technischer Eigenschaften).

DR.003: Darüber hinaus wird für diese Methode immer eine Menge von Protokollierungsdaten verwendet (ggf. auch aus verschiedenen Quellen). D. h. es muss auf den gespeicherten Daten weiterhin Möglichkeiten geben, Beziehungen zwischen Daten herstellen zu können.

UC.005 Statistisches Verhalten erkennen

Im Anwendungsfall *UC.004* (siehe Kapitel 2.5.3) wird die Idee für eine statistische Erkennungsmethode konzipiert, welche dann in diesem Anwendungsfall implementiert und kontinuierlich verfeinert wird. Auch dieses Verfahren wird gerade zu Beginn eine ganze Reihe von falsch-positiven Ergebnissen liefern, so dass auch hier im Anschluss der Anwendungsfall *UC.003* erforderlich ist, um die Ergebnisse weiter zu filtern.

Wie *UC.004*: *DR.006* und *DR.007*

Zusätzlich:

DR.008: Darüber hinaus besteht die Anforderung, dass die generierten statistischen Modelle der Verfahren unbegrenzt über den Zeitraum von 90 Tagen gespeichert werden können, so dass auch Anomalien, die sich ggf. erst über einen längeren Zeitraum ergeben, analysiert werden können. Diese Modelle werden keine personenbezogenen Daten beinhalten.

2.5.1.2 Aktivität „Verifizieren“

Verifizieren erfolgt dadurch, dass die Zuverlässigkeit (confidence) und Gefahrenstufe (threat level) zu einer Priorisierung der sicherheitsrelevanten Ereignisse führen. Der Analyst wird daher höher priorisierte Ereignisse vor anderen Ereignissen bearbeiten. Ausgehend von dem sicherheitsrelevanten Ereignis (welches in sich keinerlei personenbezogene Daten enthält) schaut sich der Analyst nun alle mit diesem Ereignis in Verbindung stehenden Protokollierungsereignisse an und prüft, ob es sich um ein falsch-positives sicherheitsrelevantes Ereignis handelt oder nicht. Die Anzahl von Protokollierungsereignissen, die hierzu betrachtet werden müssen, kann im Vorhinein nicht eingegrenzt werden. Gleichzeitig hat ein Analyst jedoch eine begrenzte Zeit zur Verifikation, da davon auszugehen ist, dass sehr viele Ereignisse pro Tag verifiziert werden müssen. Aus dieser zeitlichen Restriktion ergibt sich ein maximales Abbruchkriterium. Ist ein sicherheitsrelevantes Ereignis als solches bestätigt, wird das positive Ergebnis der Verifikation dem De-Pseudonymisierungsbeauftragten vorgelegt und gleichzeitig an den Prozess der Reaktion übergeben.

UC.003 Verdachtsmoment erhärten

Ausgangspunkt bei diesem Anwendungsfall ist ein bereits in den Protokollierungsdaten festgestelltes sicherheitsrelevantes Ereignis, zu welchem geprüft werden soll, ob dies zu einem tatsächlichen Angriff gehört oder ein falsch-positives sicherheitsrelevantes Ereignis ist. Aus mehreren Gesichtspunkten ist die Feststellung, ob es sich um eine legitime Interaktion oder tatsächlich eine schädliche Interaktion handelt nicht möglich:

1. Die meisten protokollierten Ereignisse stehen nur in einem mittelbaren Zusammenhang zu der intendierten Interaktion mit der IT.
2. Das Verhältnis der Falsch-Positiven Ereignisse zu den tatsächlichen Angriffen ist typischerweise sehr hoch, so dass es zeitlich nicht abbildbar ist, alle betroffenen Mitarbeiter zu befragen.
3. Es besteht der Anspruch, möglichst wenig unmittelbar personenbezogene Daten zu erheben und nur in begründeten oder unvermeidbaren Fällen den Rückschluss auf eine tatsächliche Person herzustellen.
   Beispiel: Ein APC ist als Ausgangspunkt für eine Command & Control Kommunikation ermittelt worden. Wenn dieser APC nun forensisch untersucht wird (siehe *UC.006*), ist es nicht mehr vermeidbar auch die Identität der Person zu kennen.

Diese drei Punkte bedeuten, dass zur Erhärtung des Verdachtsmomentes Daten aus verschiedenen Quellen im jeweiligen Kontext miteinander in Verbindung gebracht werden müssen. Außerdem kann sich das Erfordernis ergeben, weitere Ereignisse im zeitlichen Kontext zum zuerst identifizierten Protokollierungsdatum analysieren zu müssen. Diese Schritte müssen so oft wiederholt werden, bis der Verdacht erhärtet wurde, oder nicht, oder das oben beschriebene zeitliche Abbruchkriterium greift.

Wie UC.002: *DR.002*, *DR.003*

Zusätzlich:

DR.004: Darüber hinaus muss es möglich sein, Protokollierungsdaten um weitere Daten anzureichern, die bei der erstmaligen Einlagerung noch nicht bekannt waren. Ausschließlich für diesen Prozess der Anreicherung muss auf die nicht pseudonymisierten Daten zurückgegriffen werden.

DR.005: Als Besonderheit zu diesem Anwendungsfall ergibt sich auch das organisatorische Erfordernis, den Zugriff dynamisch auf weitere Protokollierungsdaten zu gewähren, ohne dass hier schon absehbar wäre, ob diese zu einem Angriff gehören oder nicht.

2.5.2 Prozess „Reaktion“ (BSI; Einzelbehörde optional)

Qualifizierte sicherheitsrelevante Ereignisse bedürfen der unmittelbaren Reaktion. Dies übernimmt zunächst der Ermittler, welcher die Aufgabe hat, sich die durch den Analysten gesichteten Ereignisse genauer anzuschauen und daraufhin Kontakt mit dem IT-Betrieb aufnimmt, um zu bestätigen, ob es sich hierbei nicht um eine Fehlkonfiguration oder ein anderes betrieblich hervorgerufenes Ereignis handelt. Ist dies doch der Fall, dann übernimmt der IT-Betrieb. Ansonsten handelt es sich sehr wahrscheinlich um einen Angriff und der Ermittler bearbeitet ab diesem Moment einen Sicherheitsvorfall. Hierzu kann der Ermittler die Freigabe des De-Pseudonymisierungsbeauftragten nutzen, um die Klartextdaten einzusehen. Hat der De-Pseudonymisierungsbeauftragte bisher keine Freigabe erteilt, kann der Antrag mit den Erkenntnissen des Ermittlers (ggf. erneut) gestellt werden. Als weitere Aktivität schließt sich hier z. B. die forensische Analyse an, welche durch einen forensischen Ermittler durchgeführt wird.

UC.006 Sicherheitsvorfall bearbeiten / Incident Response

Wurde während UC.003 tatsächlich ein Sicherheitsvorfall festgestellt, muss dieser als solcher bearbeitet werden. In diesem Anwendungsfall werden alle betroffenen Geräte ermittelt und im Anschluss forensisch analysiert, um weitere Spuren sicherzustellen, die in den Protokollierungsdaten nicht enthalten waren. Daraufhin werden die betroffenen Geräte bereinigt. Das heißt, in diesem Anwendungsfall liegt einerseits die Erkenntnis vor, dass es sich um einen Sicherheitsvorfall handelt (ggf. mag dies aber kein gezielter Angriff gewesen sein) und andererseits besteht die Notwendigkeit, tatsächlich einzelne physische Geräte zu identifizieren. Wie zuvor schon beschrieben, ist es hierbei unausweichlich, auch die dazugehörige Person zu ermitteln.

Wie UC.003 (um weitere Betroffene Systeme zu identifizieren)

Zusätzlich:

DR.009: Die Protokollierungsdaten von den betroffenen Systemen müssen in der ursprünglichen Form vorliegen, um die Identifizierung der physischen Geräte und die weitere forensische Analyse zu ermöglichen.

DR.010: Da die Bearbeitung eines Sicherheitsvorfalls sehr viel Zeit beanspruchen kann, müssen die Daten der Systeme, die mit dem Sicherheitsvorfall in Verbindung stehen, für den Zeitraum der Bearbeitung über die Speicherfrist (siehe Kapitel 2.3) hinaus gesichert werden können.

UC.007 Weitergabe von Daten an Dritte entsprechend BSIG

Aus der Arbeit mit den Protokollierungsdaten ergeben sich sehr eingegrenzte Fälle in denen Daten aus dem PDEV-CA für Dritte bereitgestellt werden:

1. So werden für verschieden Berichte des BSI die Ergebnisse der Detektion, Verifikation und Reaktion als Statistiken benötigt. Beispiele sind Lageberichte oder der Bericht nach § 5 BSIG. Hierfür werden keine personenbezogenen Daten weitergegeben.
2. Entsprechend der Regelungen nach § 4 BSIG, sind das BSI und die Bundesbehörden verpflichtet, Informationen bzgl. der Sicherheit der Informationstechnik des Bundes zu teilen bzw. dem BSI unverzüglich mitzuteilen (sogenannte SOFORT-Meldungen). Da das PDEV-CA Meldungen über die IT-Sicherheit in der Behörde generiert, ist es nötig diese Informationen dem Meldewesen nach § 4 BSIG zu Verfügung zu stellen. Nach § 5 Abs. 4 BSIG, müssen, sofern nicht die im Gesetz genannten Ausnahmen zutreffen, die beteiligen Personen, in deren Kommunikation das Schadprogramm detektiert wurde, benachrichtigt werden. Dies ist als Folgeschritt der De-Pseudonymisierung am Ende der Reaktion zu sehen und betrifft nur die nach § 5 BSIG erhobenen Daten.
3. Ferner kann das BSI nach § 5 Abs. 5 und 6 BSIG in begründeten Fällen personenbezogene Daten an die Strafverfolgungsbehörden bzw. Nachrichtendienste weitergeben.

2.5.3 Prozesse „Entwicklung Detektor und Qualitätssicherung“ (BSI)

Während sich signaturbasierte Detektoren unmittelbar aus z. B. forensischen Analysen vergangener Fälle ergeben, bedarf die Erstellung vorgehensbasierter oder statistischer Detektoren eine zunächst anlasslose Interaktion mit den Daten. Basierend auf einer von einem Cyber-Sicherheitsexperten (Kapitel 2.6) generierten Hypothese erstellt ein Data Scientist ein Modell und verifiziert, ob basierend auf diesem statistisch signifikante und relevante Aussagen getroffen werden können. Können relevante Aussagen getroffen werden, wird dies dem Freigabebeauftragten vorgelegt und, sofern dieser die Freigabe erteilt, ein erster Prototyp eines Detektors implementiert. Dieser wird evaluiert und sofern die Evaluierung erfolgreich ist (die Ergebnisse werden erneut dem Freigabebeauftragten vorgelegt), dann zu der Menge der Detektoren hinzugefügt.

Neben der Entwicklung eines Detektors besteht ebenfalls für den Data Engineer die kontinuierliche Notwendigkeit die gespeicherten Daten auf ihre Qualität zu überprüfen. Beispielsweise könnten Daten verloren gehen oder es könnten Daten falsch verarbeitet werden. Hierzu ist es erforderlich, zufällige Einzelereignisse oder Einzelereignisse zu einem gewissen Zeitpunkt (z. B. Anbindung einer neuen Datenquelle) nicht pseudonymisiert manuell zu sichten.

UC.004 Statistiken erstellen

Die Anwendungsfälle UC.001 und UC.002 basieren auf bereits bekannten Ereignissen. Neue Vorgehensweisen von Angreifern könnten unentdeckt bleiben. Aus diesem Grund ist es erforderlich, „statistische Anomalien“ in den Protokollierungsdaten zu identifizieren. Die Implementierung von Anomalieerkennungsverfahren erfordert jedoch, dass genügend Erfahrung für die statistische Verteilung und die Struktur der Protokollierungsdaten vorhanden ist. Aus diesem Grund ist es erforderlich, Statistiken zu erstellen, diese auszuwerten und davon ausgehend weitere Statistiken abzuleiten. Dieser Prozess iteriert so lange, bis eine Idee für die Implementierung eines Anomalieerkennungsverfahrens vorliegt. In diesem Anwendungsfall wird höchstens zufällig ein Angriff entdeckt. Das heißt die Interaktion mit den Daten erfolgt völlig losgelöst eines konkreten Verdachtes.

Entscheidender Unterschied zu den vorherigen Anwendungsfällen ist, dass bei diesem Vorgehen im Ergebnis nie einzelne Protokollierungsdaten ersichtlich werden, sondern ausschließlich aggregierte Daten.

DR.006: Für die statistische Auswertung ist zwingend erforderlich, dass bei allen Veränderungen der gespeicherten Daten die statistische Verteilung der einzelnen Ereignisse nicht verändert wird. Da Angriffe innerhalb weniger Millisekunden erfolgen können, kann auch schon die kleinste Aggregation bei der Speicherung der Daten (z. B. durch Weglassen von Informationen) eine statistische Erkennung verhindern.

DR.007: Die Pseudonymisierung eines Datums verringert dessen sichtbaren Informationsgehalt, d. h. dessen Metadaten (z. B. Wortlänge oder IP-Netzbereich). Daher kann es erforderlich sein, dass auf den ursprünglichen Daten zusätzliche statistische Werte berechnet werden müssen. D. h., es muss zu jedem

Zeitpunkt der Zugang zu den ursprünglichen Werten ermöglicht werden, es sei denn diese statistischen Werte konnten schon bei der Speicherung der Protokollierungsdaten berechnet und dabei gespeichert werden.

2.5.4 Prozess „Systembetrieb und –entwicklung“

Der Systemadministrator für das PDEV-CA verantwortet die Bereitstellung der gesamten notwendigen IT-Infrastruktur. Dieser muss für seine Aufgaben keinen Einblick in die Protokollierungsdaten erhalten. Da er jedoch aufgabenbedingt über die höchsten Systemrechte verfügt, lässt sich dies oftmals nur durch organisatorische Maßnahmen regeln.

2.6 Rollen- und Rechtekonzept

Aus der Prozessbeschreibung können folgende Rollen abgeleitet werden:

1. Analyst/Auswerter (BSI; Einzelbehörde)
2. De-Pseudonymisierungsbeauftragter (BSI; Einzelbehörde)
3. Ermittler, Forensischer Ermittler (BSI; Einzelbehörde optional)
4. IT-Betriebsmitarbeiter (Einzelbehörde)
5. Cyber-Sicherheitsexperte, Data Scientist (BSI)
6. Freigabebeauftragter (BSI)
7. Data Engineer (BSI)
8. Systemadministrator (BSI; Einzelbehörde)
9. Behördlicher Datenschutzbeauftragter (Einzelbehörde)

Die jeweiligen Verfahrensberechtigungen werden im Folgenden beschrieben. In Abbildung 1 sind die Berechtigungen zur Vereinfachung bereits farblich hinterlegt.

2.6.1 Verfahrensberechtigungen des Analysten/Auswerters (BSI; Einzelbehörde)

Der Analyst ist berechtigt, im manuellen Auswertesystem ausgehend von einem sicherheitsrelevanten Ereignis auf die pseudonymisierten Protokollierungsereignisse zuzugreifen. Da zur Verifikation ggf. andere Ereignisse miteinander in Beziehung gesetzt werden müssen, ist eine weitere Einschränkung nicht möglich. Der Analyst ist nicht berechtigt, Klartext-Informationen anzuzeigen.

2.6.2 Verfahrensberechtigungen des De-Pseudonymisierungsbeauftragten (BSI; Einzelbehörde)

Der De-Pseudonymisierungsbeauftragte hat die Funktion die übermäßige, ggf. nicht erforderliche De-Pseudonymisierung von Daten zu verhindern. Er selbst ist nicht berechtigt jegliche Art von Protokollierungsereignissen anzuschauen. Stattdessen bekommt er einen Antrag (entweder durch einen Analysten oder einen Ermittler), dass eine gewisse Menge von Feldern zu de-pseudonymisieren ist und zusätzlich die Begründung des Analysten. Der De-Pseudobeauftragte entscheidet über den Antrag und gibt die De-Pseudonymisierung frei. Der De-Pseudonymisierungsbeauftragte ist im BSI gem. §5 BSIG der Präsident. In Fällen, in denen die Behörde selbst die Protokollierungsdaten erhebt und auswertet, ist zu empfehlen, dass es sich um einen Juristen mit der Befähigung zum Richteramt handelt.

2.6.3 Verfahrensberechtigungen des (forensischen) Ermittlers (BSI; Einzelbehörde optional)

Der Ermittler führt eine tiefergehende Auswertung der Daten durch. Es kann erforderlich sein, dass er Einblick in nicht pseudonymisierte Daten erhalten muss. Hier kann er entweder auf einem Antrag eines Analysten aufbauen oder beim De-Pseudonymisierungsbeauftragten einen erneuten Antrag stellen. Der forensische Ermittler ist noch mal eine weitere Spezialisierung. Während der Ermittler die Daten ausschließlich im PDEV-CA auswertet, ist der forensische Ermittler ggf. auch noch auf weitere Daten angewiesen. Ermittler und forensischer Ermittler können durch ein und denselben Mitarbeiter gestellt werden.

2.6.4 Verfahrensberechtigungen des IT-Betriebsmitarbeiters (Einzelbehörde)

Die Prozesse des IT-Betriebs sind in diesem Konzept nicht abgebildet. Daher wird an dieser Stelle nur darauf verwiesen, dass Mitarbeiter des IT-Betriebs erst nach Aufforderung des Ermittlers auf die Protokollierungsdaten zugreifen dürfen. Hierbei dürfen sie überprüfen, ob die Systeme korrekt konfiguriert sind oder ob es sich um ein betriebliches Problem handelt.

2.6.5 Verfahrensberechtigungen des Cyber-Sicherheitsexperten und des Data-Scientists (BSI)

Seine Aufgabe ist es, Hypothesen zu generieren. Dazu benötigt er im Umfang des Analysten Zugriffsrechte auf das PDEV- CA. Besteht ein Detektor aus einfachen Regeln, so kann der Cyber-Sicherheitsexperte diesen selbst entwickeln. Ansonsten besteht die Notwendigkeit einen Data-Scientist hinzuzuziehen.

Der Cyber-Sicherheitsexperte ist berechtigt, neben dem Auswerten von Protokollierungsereignissen auch übergreifende Statistiken zu erzeugen.

Der Cyber-Sicherheitsexperte kann u. a. auch die Rolle des Analysten ausüben.

Der Data-Scientist ist darüber hinaus zuständig für den Betrieb und die Weiterentwicklung des automatisierten Auswertesystems. Im Auswertesystem besitzt er die höchsten Rechte.

2.6.6 Verfahrensberechtigungen des Freigabebeauftragten (BSI)

Der Freigabebeauftragte hat analog zum De-Pseudonymisierungsbeauftragten keine Berechtigungen, um Protokollierungsdaten anzuzeigen. Dafür müssen ihm alle neu zu implementierenden Detektoren zur Abnahme vorgelegt werden, bevor diese aktiviert werden. Dazu hat er ein Revisionsrecht, welches ihm ermöglicht, die derzeit aktiven Detektoren und die Entwicklungsschritte, die im Repository hinterlegt sind, zu sichten. Der Freigabebeauftragte kann durch dieselbe Person wahrgenommen werden wie der De-Pseudonymisierungsbeauftragte.

2.6.7 Verfahrensberechtigungen des Data Engineers (BSI)

Der Data Engineer ist zuständig für die Daten-Modellierung und das Zusammenspiel der Teilsysteme des PDEV-CA und hier insbesondere für das Speicher- und Einlagerungssystem, um die Anforderungen der gesamten Beteiligten zu erfüllen. Für das Speicher- und Einlagerungssystem hat er die höchsten Rechte. Hierdurch können Risiken für die personenbezogenen Daten entstehen. Als organisatorische Maßnahme dient hier die Datenschutz-Protokollierung (DS.1, DS.2), um nachzuvollziehen, ob unberechtigter Zugang zu den Daten stattgefunden hat.

2.6.8 Verfahrensberechtigungen des Systemadministrators (BSI; Einzelbehörde)

Der Systemadministrator stellt die IT-Infrastruktur bereit, auf der die Systeme des PDEV-CA arbeiten. Er hat systemweit die höchsten Rechte. Da der Systemadministrator die Rechte selbst konfiguriert, lassen sich diese präventiv kaum weiter einschränken. Als organisatorische Maßnahme dient auch hier die

Datenschutz-Protokollierung (DS.1, DS.2). Der Systemadministrator besitzt den Schlüssel für den Schrank des Systems (siehe Kapitel 4.2.1).

2.6.9 Verfahrensberechtigungen des behördlichen Datenschutzbeauftragten (Einzelbehörde)

Damit im Auftrag des behördlichen Datenschutzbeauftragten festgestellt werden kann, ob ein Datenmissbrauch stattgefunden hat, kann sich der Inhaber der Rolle (Datenschutz-)Revision im Protokollierungsspeicher für den Datenschutzaudit alle Ereignisse über die Nutzung von PDEV-CA anschauen.

Die Rolle der (Datenschutz-)Revision kann durch die gleiche Person wie den Freigabebeauftragten und/oder den De-Pseudonymisierungsbeauftragten gestellt werden (mit Ausnahme des BSI, hier ist eine Rollentrennung vorgesehen).

3 Risikofeststellung der personenbezogenen Daten

3.1 Zusammenstellung der Anwendungsfälle und Anforderungen an die Daten

An-wendungs fall	**Anforderungen an Daten**									
	DR.001 Abbildungs-funktion	DR.002 Erhalt technischer Parameter	DR.003 Bezieh-barkeit	DR.004 Anreich-erung externer Quellen	DR.005 Dynamisch weiterer Zugriff	DR.006 Erhalt statistischer Verteilung	DR.007 Anreicher-ung um statistische Kenn-größen	DR.008 Unbe-grenzter Erhalt statistischer Modelle	DR.009 Zugriff auf unverän-derte Daten	DR.010 Speicherung ausgewählter Daten über 90 Tage hinaus
UC.001 Signaturen prüfen	X									
UC.002 Vorgehen erkennen		X	X							
UC.003 Verdachts-momente erhärten		**X**	**X**	**X**	**X**					
UC.004 Statistiken erstellen						X	X			
UC.005 Statistisches Verhalten erkennen						X	X	X		
UC.006 Sicherheitsvorfall bearbeiten						**X**	**X**	**X**	**X**	**X**
UC.007 Weitergabe						X			X	

Tabelle 2: Anforderungen an die Daten

Die in rot gefärbten Spalten zeigen an, dass hier auch nachträglich ein Zugriff auf unveränderte Daten (d. h. auch nicht pseudonymisiert) erforderlich ist bzw. hier eine Abweichung der Speicherfrist (Kapitel 2.3) besteht. Da die Anwendungsfälle *UC.003* und *UC.006* in der Kette sowohl von *UC.001*, UC.002 als auch *UC.005* referenziert werden, sind diese Zeilen als Fett hervorgehoben worden.

3.2 Gefährdungsbetrachtung

Die im PDEV-CA gespeicherten Daten sind gemäß der allgemeinen Verwaltungsvorschrift des BMI zum materiellen und organisatorischen Schutz von Verschlusssachen (VSA) als VS-Nur für den Dienstgebrauch eingestuft. Gemäß BSI-Standard- 200-2 ist für die Daten folgender Schutzbedarf festgestellt:

Schutzziel	**Schutzbedarf**
Verfügbarkeit	Normal
Vertraulichkeit	Hoch
Integrität	Hoch

Tabelle 3: Gefährdungsbetrachtung

In Bezug auf den Datenschutz ergibt sich folgende Betrachtung, wobei PT (engl. privacy threat) die Gefährdung bezeichnet und PRSK (engl. privacy risk, das Risiko also Schadensausmaß des PT x Eintrittswahrscheinlichkeit).

PT.001: Bei einer Speicherung von Protokollierungsdaten über die Speicherfrist (vergl. Abschnitt 2.3) hinaus, besteht die Gefahr, dass der einzelne Mitarbeiter vollständig gläsern wird. Ggf. können aufgrund dieser

Daten nicht nur auf die konkrete Tätigkeit beim Dienstherrn bezogene Informationen ermittelt werden, sondern darüber hinaus auch direkte oder indirekte Informationen über das Privatleben ersichtlich werden. Hierbei ist jedoch zu beachten (ungeachtet juristischer Regelungen), dass die Kenntnis eines einzigen Protokollierungsdatums nicht immer unmittelbar eine Gefährdung darstellt. Häufig führt erst eine Summe von Protokollierungsdaten zu dieser Gefährdung.

PT.002: Bei den hier vorliegenden Daten handelt es sich um graphentheoretisch vollständig miteinander verbundene Daten. Damit ist immer eine De-Pseudonymisierung möglich, sofern die Pseudonymisierung die „Verbundenheit“ nicht unkenntlich macht (im engl. auch bekannt unter de-identification).

Allerdings zeigen die Anwendungsfälle (insbesondere *UC.003*), dass gerade diese Verbundenheit eine erhaltungswürdige Eigenschaft ist, um mit diesen Daten das vorgesehene Ziel erreichen zu können.

PRSK.001: Die Kombination der Gefährdungen *PT.001* und *PT.002* ergibt das Risiko, dass dem Datenschutz oder Fernmeldegeheimnis unterliegende Daten einer Person oder einer Institution längerfristig gespeichert und einer anderen Person zugänglich gemacht werden, sofern *DR.003* bestehen bleibt.

4 Technische und organisatorische Maßnahmen

Das Kapitel gliedert sich in zwei Teile:

1. Beschreibung der für die Protokollierung spezifischen Maßnahmen, welche über das BDSG hinausgehen
2. Beschreibung der Maßnahmen gem. BDSG

4.1 Spezifische Maßnahmen für die Protokollierung

4.1.1 Pseudonymisierte Speicherung und Wiederherstellung des Klartextes

Zunächst werden alle Protokollierungsereignisse (IS.3.1 und IS.3.2 bzw. Pseudonymisierungsgrenze) ausschließlich pseudonymisiert gespeichert. Die Pseudonymisierung erfolgt dabei nach dem im Kapitel 5 dargelegten Pseudonymisierungskonzept. Um einen hohen Schutz der Pseudonyme zu gewährleisten, wird der Auflösungsdatenspeicher in einer vom pseudonymisierten Protokollierungsdatenspeicher getrennten Datenbank gehalten (siehe Abbildung 1).

Die De-Pseudonymisierung muss beim De-Pseudonymisierungsbeauftragten beantragt werden. Hierzu ist ein Workflow (systemunterstützter Prozess) definiert, welcher über die De-Pseudonymisierungsschnittstelle (siehe Abbildung 1) angesprochen werden kann. Durch die Systemunterstützung wird sichergestellt, dass auch Klartexte ausschließlich automatisiert erzeugt werden und keinen manuellen Zugriff auf sensible Daten erfordern.

Für eine ausgewählte Menge von Ereignissen kann eine De-Pseudonymisierung beantragt werden (Antrag). Dieser Antrag erhält der De-Pseudonymisierungsbeauftragte, welcher plausibilisieren muss (u. a. aufgrund der Begründung des Antrags), ob er diesem Antrag stattgeben darf. Wird dem Antrag stattgegeben, dann werden die pseudonymisiert gespeicherten Ereignisse gemäß dem Antrag mit dem Auflösungsdatenspeicher zusammengeführt und in einen gesonderten Datenbankbereich geschrieben. Alle Anträge und die erfolgten Aktionen werden protokolliert und im Protokollierungsspeicher für den Datenschutzaudit zur Verfügung gestellt.

4.1.2 Automatisierte Löschung nach Erreichen der maximalen Speicherfrist

Das Speichersystem (pseudonymisierter Protokollierungs- und Auflösungsdatenspeicher) wird täglich automatisiert bereinigt, so dass die maximale Speicherfrist (siehe Kapitel 2.3) für alle Protokollierungsereignisse eingehalten wird. Die Löschung und das evtl. Fehlschlagen der Löschung der Ereignisse wird protokolliert, so dass die Einhaltung der Speicherfrist überwacht werden kann. Die Protokollierung erfolgt im Protokollierungsspeicher für den Datenschutzaudit.

Ausgenommen von der automatisierten Löschung pseudonymisierter Daten sind qualifizierte sicherheitsrelevante Ereignisse. Diese werden gelöscht, wenn Sie nicht mehr für die Bewertung von Sicherheitsvorfällen benötigt werden.

De-pseudonymisierte Ereignisse werden automatisiert gelöscht, wenn nicht innerhalb der Löschfrist bestätigt wird, dass diese zu einem Sicherheitsvorfall gehören. Wird bestätigt, dass diese zu einem Sicherheitsvorfall gehören, dann ist eine manuelle Löschung nach Abschluss des Sicherheitsvorfalls erforderlich.

Damit die Einhaltung der Löschfrist auch für alle Quellsysteme eingehalten werden kann, werden die Daten auf den Quellsystemen nach erfolgreicher Übertragung gelöscht. Für die Einhaltung dieser Anforderung ist der administrative Eigentümer der Quellsysteme verantwortlich.

4.1.3 Manuelle Sichtung von pseudonymisierten Protokollierungsereignissen

Auch pseudonymisierte Protokollierungsereignisse können nur dann manuell gesichtet werden, wenn eine automatisierte (Vor-)Auswertung (Detektor) festgestellt hat, dass diese zu einem sicherheitsrelevanten Ereignis gehören.

Damit die Qualitätssicherung und Entwicklung von neuen Detektoren möglich ist, ist für bestimmte Rollen der Zugriff auf den pseudonymisierten Protokollierungsdatenspeicher auch anlassunabhängig manuell erlaubt. In diesem Fall werden jedoch ausschließlich aggregierte Pseudonyme zur manuellen Auswerte-Schnittstelle übertragen.

4.2 Maßnahmen gem. BDSG

4.2.1 Zugangskontrolle

Das PDEV-CA ist in abgeschlossenen Server-Schränken mit Schranküberwachung untergebracht. Der Zugang zu den Schlüsseln ist gemäß Rollen- und Rechtekonzept (siehe Kapitel 2.6) geregelt. Jedes Öffnen der Schränke wird alarmiert, so dass unbefugter Zugang erkannt werden kann. Die Alarmierung erfolgt mindestens an die Rolle Administrator des PDEV-CA. Jeder Zugang zu dem System wird dokumentiert.

4.2.2 Zugriffskontrolle

Das PDEV-CA ist in einem eigenen physikalischen Netzwerksegment (Datennetz) untergebracht, in dem ausschließlich das PDEV-CA betrieben wird. Die Systemkomponenten, die zum Management des PDEV-CA erforderlich sind, werden durch einen Paketfilter getrennt vom Datennetz in einem eigenen physikalischen Netzwerksegment untergebracht (Managementnetz). Wenn das Managementnetz auch für andere Systeme genutzt werden soll, dann wird die Absicherung gesondert dargelegt. Abbildung 1 ist dann um diese weitere Schnittstelle zu ergänzen.

Das in Abbildung 1 dargestellte SIGW.1 erlaubt ausschließlich von Protokollierungsquellen eingehende Verbindungen und wird auf die erforderlichen Ports eingeschränkt (Paketfilter). Im Falle von IT-Dienstleistern des Bundes wird diese Verbindungsrichtung durch eine Diode forciert.

Das in Abbildung 1 dargestellte SIGW.2 erlaubt ausschließlich von autorisierten Systemen (IP-Adressen) eingehende Verbindungen. Dabei werden die Zugriffe auf die benannten Schnittstellen (S.Manuell, S.Depseudo und S.Dev) eingeschränkt. Bei IT-Dienstleistern erfolgt die Filterung auf Applikationsprotokoll-Ebene (Application Layer Gateway), um eine größtmögliche Entkopplung des PDEV-CA von den Clients zu erreichen. Die Zugriffe bzw. Zugriffsversuche werden im Protokollierungsspeicher für den Datenschutzaudit protokolliert.

Das PDEV-CA selbst kann automatisiert auf externe Systeme zugreifen und mit diesen Daten austauschen: Benachrichtigungssystem, Regel-Speicher (S.Regel) oder systemnahe Dienste (S.Services) wie NTP, DNS und Update-Server. Diese Zugriffe erfolgen ebenfalls durch SIGW.2. Die systemnahen Dienste können auch über das Management-Netz bereitgestellt werden.

Um die Abgeschlossenheit des PDEV-CA bis zum Client aufrechtzuerhalten, werden mindestens VS-NfD zugelassene Clients mit einer eigenen Sitzung für das PDEV-CA eingesetzt, welche ausschließlich eine Verbindung zu PDEV-CA ermöglicht. Die Schnittstelle S.Client ist damit auch zugelassen verschlüsselt und authentifiziert. Soll die Sitzung für andere Systeme genutzt werden können ist dies gesondert darzulegen und die Maßnahmen entsprechend zu erweitern.

4.2.3 Datenträgerkontrolle

Im PDEV-CA sind alle Dateisysteme verschlüsselt. Der Schlüssel ist ausschließlich der Rolle System-Administrator (siehe Kapitel 2.6) bekannt. Dies schützt gegen einen physisch unberechtigten Zugriff auf das System.

Ein entfernter Zugriff auf die Betriebssystemebene kann ausschließlich aus dem Managementnetz (s. o.) erfolgen und wird damit nicht über eine von außen zugängliche Schnittstelle exponiert.

Unbefugtes Lesen, Kopieren, Verändern oder Löschen kann daher ausschließlich über die Schnittstellen des Speichersystems selbst erfolgen.

4.2.4 Speicherkontrolle

Zunächst dienen zwei grobgranulare Maßnahmen zur Speicherkontrolle:

- wie zuvor in Kapitel 4.1 beschrieben, werden nur pseudonymisierte Daten gespeichert und nur in engen Grenzen (sicherheitsrelevante Ereignisse) zum Client übertragen
- Pseudonymisierte Ereignisse und die zur Auflösung erforderlichen Daten werden in zwei getrennten Systemen gespeichert
- wie in Kapitel 4.2.2 beschrieben, werden alle Schnittstellen zum System durch Paketfilter oder Application Layer Gateways auf das Notwendigste eingeschränkt

Alle weiteren Maßnahmen werden über das in Kapitel 2.6 beschriebene restriktive Rollen- und Rollenkonzept erreicht.

4.2.5 Benutzerkontrolle

Eine Anmeldung an das PDEV-CA ist ausschließlich über die zugelassenen Clients (Anmeldung mit Smart-Card oder vergleichbar) und nach vorhergehender Authentisierung der Anwender am PDEV-CA möglich. Es erfolgt eine Autorisierung gemäß Rollen- und Rechtekonzept (Kapitel 2.6). Zur Authentisierung werden über die Smart-Card am Client hinaus Benutzername und Passwort verwendet.

4.2.6 Übertragungskontrolle

In den Sitzungen der zugelassenen Clients sind alle externen Schnittstellen für Speichermedien deaktiviert. Ein Export personenbezogener Daten aus dem PDEV-CA ist ausschließlich über SIGW.2 möglich und wird an dieser Stelle protokolliert. Die Export-Aufträge müssen über einen Workflow beantragt werden. Die Anträge und die Entscheidungen werden dokumentiert. Beim Export werden die Daten mit einem Public Key des Empfängers verschlüsselt, so dass die exportierten Daten nur von diesem geöffnet werden können.

4.2.7 Eingabekontrolle

Das PDEV-CA ist in der Art konstruiert und durch das Rollen- und Rechtekonzept (siehe Kapitel 2.6) konfiguriert, dass eine Eingabe von personenbezogenen Daten ausschließlich von den Quellsystemen über das Einlagerungssystem möglich ist (siehe 2.6). Eine nachträgliche Änderung der Daten (über die De-Pseudonymisierung hinaus) ist nicht vorgesehen. Eine nachträgliche Überprüfung und Feststellung zu welcher Zeit und von wem die Daten eingegeben wurden, ergibt sich damit während der Speicherfrist aus dem Speichersystem selbst. Damit auch über die Speicherfrist hinaus nachvollzogen werden kann, welche Attribute erfasst werden bzw. wurden, wird die Konfiguration des Einlagerungssystems versioniert gespeichert. Eine Änderung der aktiven Konfiguration des Einlagerungssystems wird protokolliert.

4.2.8 Transportkontrolle

Datenübertragungen über externe und interne Schnittstellen des PDEV-CA (siehe Abbildung 1) sind mit TLS zu verschlüsseln. In diesem Zusammenhang wird auf die Regelungen des Mindeststandards des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden verwiesen. Werden nicht für die Verarbeitung von VS-NfD zugelassene Netzabschnitte verwendet bzw. ist dies nicht sicher gewährleistet, dann werden für externe Schnittstellen zusätzlich zugelassene Verschlüsselungsgeräte eingesetzt. Der Transport von Datenträgern des PDEV-CA ist nur dann erlaubt, wenn alle Daten auf diesen Datenträgern zuvor sicher gelöscht wurden.

4.2.9 Wiederherstellbarkeit, Zuverlässigkeit, Datenintegrität, Verfügbarkeitskontrolle

Die Aspekte werden in diesem Abschnitt zusammengefasst, da in Bezug auf einzelne Protokollierungsereignisse mit Personenbezug nur sehr schwache Anforderungen an die Verfügbarkeit gelten. Dies leitet sich aus der begrenzten Speicherfrist ab.

Das PDEV-CA wird aufgrund der Skalierbarkeit auf sehr viele Protokollierungsereignisse als verteiltes System aufgebaut. Bei der Bestimmung der Anzahl der erforderlichen Knoten wird auch die Zuverlässigkeit berücksichtigt. Somit führt ein Ausfall einzelner Knoten zu keinem Datenverlust. Die Konfiguration des PDEV-CA selbst wird regelmäßig und mindestens vor jeder Konfigurationsänderung gesichert, so dass das System selbst wiederhergestellt werden kann.

Die Protokollierungsereignisse werden nicht gesichert, da diese im Widerspruch zur festgelegten Speicherfrist stehen würde. Ein Ausfall ist durch die hohe Redundanz sehr unwahrscheinlich.

In Bezug auf die Datenintegrität der personenbezogenen Daten beschränkt sich die Absicherung auf eine schwache Feststellung einer Integritätsverletzung ohne die Möglichkeit, diese zu beheben. Die Feststellung der Integritätsverletzung erfolgt indirekt durch folgende zwei Mechanismen:

- Soll ein Datensatz de-pseudonymisiert werden und es kann kein zugehöriger Klartext im Auflösungsdatenspeicher gefunden werden, handelt es sich mit hoher Wahrscheinlichkeit um eine Integritätsverletzung.
- Das verteilte Speichern der Daten erfordert implizit eine Integritätssicherung, können Daten nicht mehr gelesen werden, obwohl ansonsten alle Systemkomponenten einwandfrei arbeiten, dann handelt es sich mit gewisser Wahrscheinlichkeit um eine Integritätsverletzung.

4.2.10 Auftragskontrolle

Zur Kontrolle wird die Protokollierung des Speichersystems für den Datenschutzaudit (DS.2) verwendet.

Bei IT-Dienstleistern des Bundes werden alle Änderungen der Konfigurationen des Einlagerungssystems, des automatisierten Auswertesystems und der Entwicklungsschnittstelle in einem Repository protokolliert (DS.3).

Insbesondere der Export von Daten (vergl. UC.007), aber auch Zugriffsversuche können zusätzlich aus den Protokollen des SIGW.2 nachvollzogen werden (DS.1). Bei IT-Dienstleistern ist dies auch auf Applikationsprotokollebene gewährleistet.

4.2.11 Trennbarkeit

Durch den physikalisch getrennten Aufbau des Systems und durch das Rollen- und Rechtekonzept (Kapitel 2.6), sowie die zugehörige Autorisierung wird sichergestellt, dass die Daten ausschließlich für den vorgesehenen Auftrag „*Feststellung von sicherheitsrelevanten Ereignissen und die zugehörigen Ermittlungen*“ eingesetzt werden kann. Werden die Daten zusammen mit Daten für die allgemeine Betriebssicherheit gespeichert, dann ist das Konzept in Bezug auf Trennbarkeit zu erweitern.

5 Pseudonymisierungskonzept

5.1 Anforderungsanalyse

Die Anwendungsfall- /Datenanforderungsmatrix (siehe Tabelle 2) zeigt, dass für manche Datenanforderungen eine Pseudonymisierung ausreichend ist (z. B. DR.001), für manche jedoch die unveränderten Daten (*DR.004*, *DR.007*, *DR.009*) zugänglich gemacht werden müssen. Bei *DR.004* und *DR.007* ist ausschließlich ein automatisierter Zugriff (ohne menschliche Interaktion) erforderlich. Bei *DR.009* ist dagegen eine menschliche Interaktion erforderlich.

Die Anforderungen *DR.002*, *DR.003* und *DR.006* stellen die Randbedingungen an die gewählte Pseudonymisierungslösung dar. Dabei ist die Anforderung *DR.006* immer dann automatisch erfüllt, wenn keine Form der Datenaggregation, z. B. durch Anonymisierung, verwendet wird.

Die übrigen Anforderungen *DR.005*, *DR.008* und *DR.010* liegen außerhalb der Pseudonymisierungslösung, da diese sich entweder mit anderen Daten (z. B. statistische Modelle) oder mit lediglich organisatorisch oder anderweitig technischen Maßnahmen regulieren lassen (z. B. bietet eine Pseudonymisierungslösung alleine noch keine Zugriffsbeschränkung).

Bei personenbezogenen Daten nach Typ 1 ist im Sinne der Datenvermeidung bereits durch den IT-Betrieb sicherzustellen, dass ausschließlich pseudonymisierte Daten bei den Systemkennungen anfallen, wie in den Anforderungen PRB.I.4.1.1.3 und PRB.I.4.1.1.4 der PR-B beschrieben. Sofern MAC- und IP-Adressen in der Verwaltungshoheit des Bundes für den Zweck der Protokollierung und Detektion begründet nicht pseudonymisiert werden können, kann von der Pseudonymisierung abgesehen werden. In diesem Fall sind organisatorische Maßnahmen zu treffen, sodass eine Zuordnung dieser Adressen zu einer Person für die mit der Protokollierungsdatenauswertung betrauten Personen nicht möglich ist. Die Adressen müssen weiterhin wie personenbezogene Daten behandelt werden.

Für personenbezogene Daten nach Typ 2 wird das vorliegende Pseudonymisierungskonzept verwendet. Für Protokollierungsdaten, die für die Bundesverwaltung verpflichtend zu protokollieren sind, enthalten die technischen Informationen zur PR-B einen Hinweis auf zu pseudonymisierende Daten. Generell sind alle Felder zu pseudonymisieren, die personenbezogene Daten enthalten. Als Beispiele seien der Postfach-Anteil an E-Mail-Adressen oder externe IP-Adressen genannt.

5.2 Allgemeines Konzept

Das grundsätzliche Konzept sieht vor, dass die Protokollierungsdaten zum Zeitpunkt der Speicherung bereits pseudonymisiert werden. Der Prozess ist nachfolgend in Abbildung 2 dargestellt.

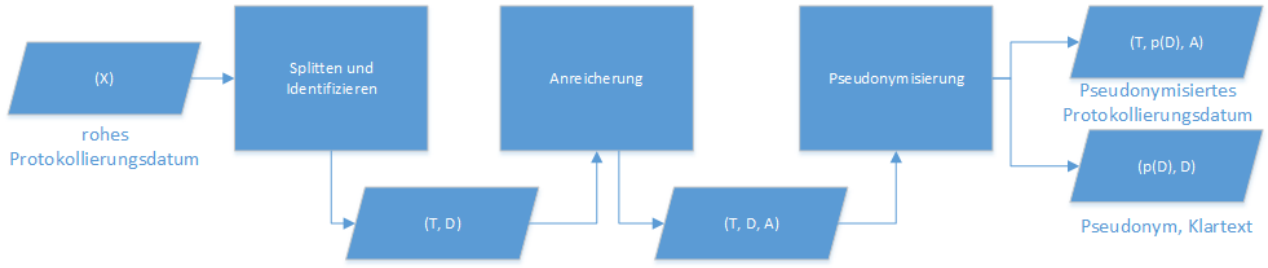

Abbildung 2: Prozess Ingest

Dieser Prozess wird nachfolgend anhand eines Beispiels erläutert. Den Prozess erreicht als Eingabemenge ein Protokollierungsdatum mit einer Menge an Feldern X:

Zeitstempel	Hostname	Src.IP	Dst.IP	Dst.Port	URL
2017-03-01 15:35:35.10	Firewall11.bsi.bund.de	10.10.22.10	95.166.12.33	443	https://lb11.booking.airlines.de/?param1=Value1&param2=Value2

Die erste Aktivität des Prozesses zerlegt das Protokollierungsdatum nun entsprechend des anhand des Hostnamens identifizierten Parsers i. Dieser identifiziert die Felder, welche unter Datenschutz und/oder Fernmeldegeheimnis fallen (Menge D). Alle restlichen Felder der Menge X, bilden jetzt die Menge T. Der Parser lässt sich also auch schreiben als i: (X) → (T, D). Die folgende Tabelle stellt die Menge D in Rot dar:

Zeitstempel	Hostname	Src.IP	Dst.IP	Dst.Port	URL
2017-03-01 15:35:35.10	Firewall11.bsi.bund.de	10.10.22.10	95.166.12.33	443	https://lb11.booking.airlines.de/?param1=Value1&param2=Value2

Zur Begründung, warum das Feld *Src.IP* nicht pseudonymisiert ist, wurde Eingangs dargelegt.

Sofern zum Zeitpunkt des Speicherns bereits Anreicherungen (*DR.004*, *DR.007*) bekannt sind, die auf den Feldern der Menge D durchgeführt werden sollen, findet in der nächsten Aktivität diese Anreicherung statt. Es existiert also eine Funktion a: (T, D) → (T, D, A), wobei A die Menge der zusätzlich angereicherten Felder ist. Es sei hier angenommen, dass derzeit nur eine Anreicherung um Geo-IP-Informationen vorgesehen ist (*Dst.Town*, *Dst.Country*).

Zeitstempel	Hostname	Src.IP	Dst.IP	Dst.Port	URL	Dst.Town	Dst.Country
2017-03-01 15:35:35.10	Firewall11.bsi.bund.de	10.10.22.10	95.166.12.33	443	https://lb11.booking.airlines.de/?param1=Value1&param2=Value2	Köln	Deutschland

Bei der Anreicherung wird bereits darauf geachtet, dass nicht um Informationen angereichert wird, die datenschutz- oder fernmeldegeheimnisrelevant sind. Im nächsten Schritt werden die Felder der Menge D pseudonymisiert. Hierbei wird eine Pseudonymisierungsfunktion eingesetzt, welche als Parameter die Menge der zu pseudonymisierenden Felder hat und als Ausgabemenge eine Menge an pseudonymisierten Feldern p: D → DP. Als Abbildungsfunktion wird hier eine Hash-Funktion mit zufällig gewählten Zeichenfolgen (Salt) empfohlen. Da eine Rückabbildung nicht (ohne größeren Rechenaufwand) möglich ist, wird in einer Auflösetabelle das Paar (D, DP) gespeichert. Das Ergebnis der Pseudonymisierungs-Aktivität ist somit das pseudonymisierte Protokolldatum, welches aus den Mengen (T, DP, A) besteht.

Beispiel pseudonymisiertes Protokollierungsdatum:

Zeitstempel	Hostname	Src.IP	Dst.IP	Dst.Port	URL	Dst.Town	Dst.Country
2017-03-01 15:35:35.10	Firewall11.bsi.bund.de	10.10.22.10	gBLSx1Cl6OlSJoErxf68FC1aoC3+03IHm32czwNYPVU=	443	https://AJrXYJk871ReZl2b14KGsX4h4e64E1gLv3eSaCI9RSw=.airlines.de/?param1=0GoKo76861Zx10qvKm/HQ1it3rLX73A/a5MtmE4a9/4=&param2=4mL74ODKHiXAw1um3QEkMoJf34WmU9q2+KnDTskHvkE=	Köln	Deutschland

Beispiel Auflösetabelle:

Pseudonym	Plaintext	Type	Last Seen
gBLSx1Cl6OlSJoErxf68FC1aoC3+03IHm32czwNYPVU=	95.166.12.33	IP	2017-03-01
AJrXYJk871ReZl2b14KGsX4h4e64E1gLv3eSaCI9RSw=	lb11.booking	LLD	2017-03-01
0GoKo76861Zx10qvKm/HQ1it3rLX73A/a5MtmE4a9/4=	Value1	HTTP-Param	2017-03-01
4mL74ODKHiXAw1um3QEkMoJf34WmU9q2+KnDTskHvkE=	Value2	HTTP-Param	2017-03-01

Die Auflösetabelle speichert noch weitere Informationen, u. a. den Typ des pseudonymisierten Klartextes und das Datum, wo dieser Klartext zuletzt in einem Protokollierungsdatum aufgetaucht ist. Dadurch ist sichergestellt, dass, auch wenn eine Kombination aus Pseudonym und Klartext nur einmal abgespeichert wird, diese nach 90 Tagen gelöscht wird, wenn in diesem Zeitraum der Klartext nicht erneut aufgetaucht ist.

Folgende Voraussetzungen werden als gültig angenommen:

- *i* identifiziert zuverlässig alle Felder, die pseudonymisiert werden müssen.
- *a* reichert nur um Felder an, die ihrerseits nicht wieder pseudonymisiert werden müssten.
- *p* pseudonymisiert die durch i identifizierten Felder in der Form, dass der Klartext nicht ohne Auflösetabelle in vertretbarem Zeitaufwand berechnet werden kann wird das Protokollierungsdatum während der Speicherfrist (siehe Kapitel 2.3) keinem Sicherheitsvorfall zugeordnet, wird es zuverlässig gelöscht.

Damit ist eine Maßnahme gegen die Gefährdung *PT.001* getroffen, sofern sichergestellt ist, dass der Zugriff auf die Auflösetabelle sehr stark eingeschränkt ist (d. h. es erhält keine Person Zugriff auf diese Tabelle), wobei *PRSK.001* wie oben beschrieben bestehen bleibt.

PT.003: Eine weitere Gefährdung, die auch außerhalb der Pseudonymisierung liegt, wäre nun, dass die o.g. Voraussetzungen aus irgendeinem Grunde nicht gültig sind.

Damit auch nach der Speicherung die Anforderungen *DR.004* und *DR.007* erfüllt werden können, muss die Aktivität „Anreicherung“ auch nachträglich durchgeführt werden können. Hierzu wird der anzureichernde Typ (als Beispiel siehe Auflösungstabelle) an die Funktion a übergeben, welche dann alle für diesen Typ definierten Anreicherungen vornimmt, indem es diese auf der Auflösungstabelle berechnet (siehe Abbildung 3).

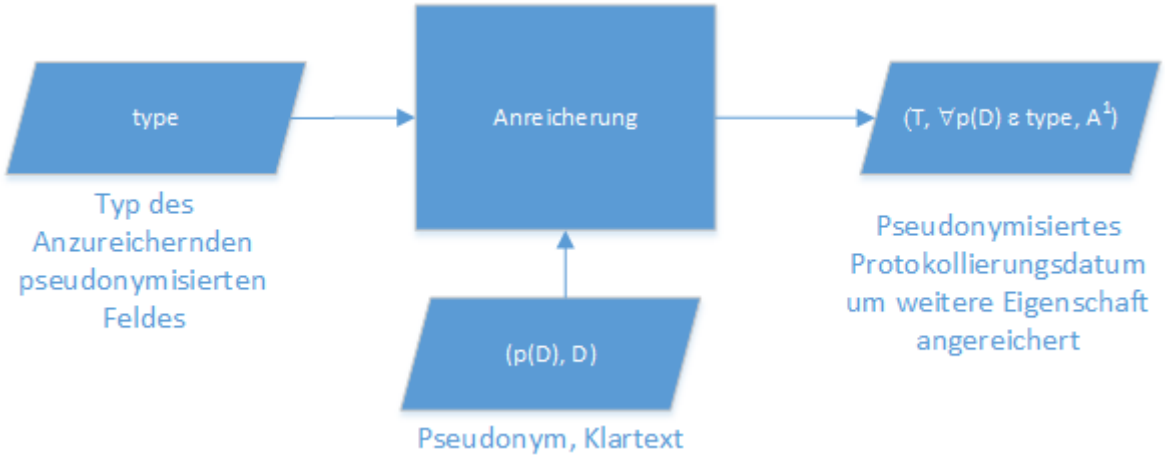

Abbildung 3: nachträgliche Anreicherung

Bisher wurde die gesamte Lower-Level-Domain pseudonymisiert. Für gewisse statistische Berechnungen sind jedoch weitere Informationen hierüber relevant, beispielsweise wie viele Lower-Level-Domains es gibt und was die maximale und minimale Entropie dieser Domains sind. Das Ergebnis der Aktivität Anreicherung sähe wie folgt aus:

Zeit-stempel	Host-name	Src.IP	Dst.IP	Dst.Port	URL	Dst. Town	Dst.Country	Domain. MinEntropy	Domain. MaxEntropy	Domain.LLDCount
2017-03-01 15:35:35.10	Firewall11.bsi.bund.de	10.10.22.10	gBLSx1Cl6OlSJoErxf68FC1aoC3+03IHm32czwNYPVU=	443	https://AJrXYJk871ReZl2b14KGsX4h4e64E1gLv3eSaCI9RSw=.airlines.de/?param1=0GoKo76861Zx10qvKm/HQ1it3rLX73A/a5MtmE4a9/4=&param2=4mL74ODKHiXAw1um3QEkMoJf34WmU9q2+KnDTskHvkE=	Köln	Deutschland	1,5	2,521641	2

PT.004: Hier besteht die Gefährdung, dass die Aktivität Anreicherung den Klartext der Auflösungstabelle direkt oder indirekt preisgibt. Während die direkte Preisgabe des Klartextes schnell auffällt, kann die indirekte Preisgabe möglicherweise erst verspätet bemerkt und behoben werden (siehe Abbildung 4).

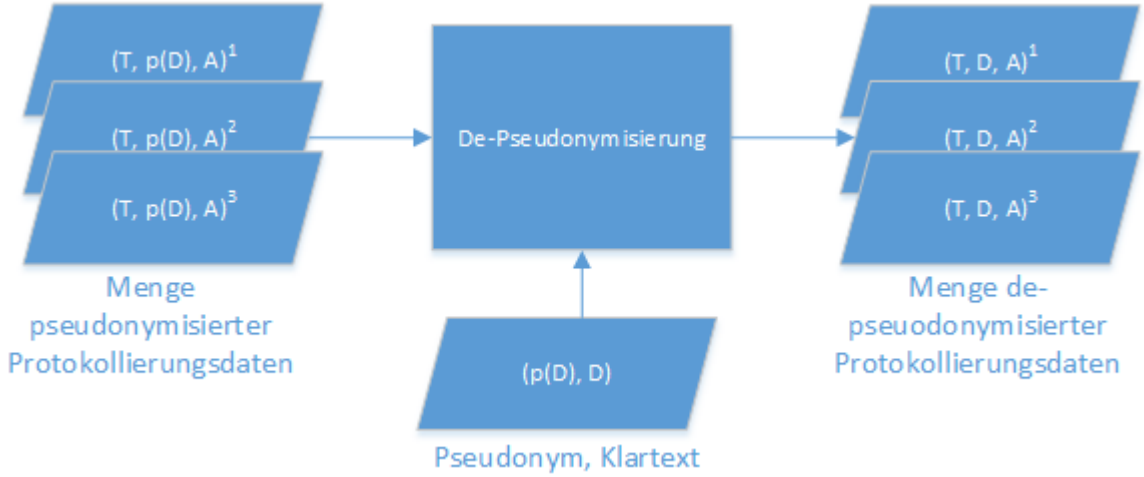

Abbildung 4: De-Pseudonymisierung

Schließlich bleibt noch die Anforderung *DR.009* zu erfüllen. Hier liegt eine Menge von pseudonymisierten Protokollierungsdaten vor, die als Ergebnis der Erhärtung der Verdachtsmomente mit einem Sicherheitsvorfall in Verbindung stehen. Diese müssen nun de-pseudonymisiert werden. Die Funktion ist mit der Auflösungstabelle sehr einfach abzubilden.

PT.005: Da diese Funktion prinzipiell die De-Pseudonymisierung aller Daten ermöglicht, ergibt sich hier eine sehr große Gefährdung.

Tabelle 4 stellt dar, dass alle Anforderungen durch die Pseudonymisierungslösung erfüllt werden können, wenn diese generell durch eine Pseudonymisierungslösung erfüllbar sind und listet ebenfalls die zusätzlich eingeführten Gefährdungen auf, welche insgesamt auf die Gefährdung *PT.001* zurückführen sind.

Anforderungen an Daten	Pseudonymisierung	Anreicherung	De-Pseudonymisierung
DR.001	PT.003		
DR.002	PT.003		
DR.003	PT.003		
DR.004		PT.004	
DR.005	Außerhalb der Pseudonymisierung		
DR.006		PT.004	
DR.007	PT.003	PT.004	
DR.008	Außerhalb der Pseudonymisierung		
DR.009			PT.005
DR.010	Außerhalb der Pseudonymisierung		

Tabelle 4: Anforderungen durch die Pseudonymisierungslösung

5.3 Vom Pseudonym zum Anonym

Eine Möglichkeit dem Analysten eine erweiterte Sicht auf die Daten zu erlauben besteht darin sie zu anonymisieren. Aus der vorgestellten Pseudonymisierung ergibt sich ein einfaches Konzept, das aufgrund von fehlender Eindeutigkeit Anonymität schafft.

Angenommen wird hier, dass Pseudonyme als base64-codierte, mit sha265-Algorithmus berechnete Hash-Werte gespeichert werden. Ein gutes Anonym ist nun bereits damit erzeugt, nur die ersten zwei Zeichen eines Pseudonyms auszuwählen. Statistische Tests haben gezeigt, dass so Mengen von rund hundert Pseudonymen entstehen. D. h., hinter einem solchen Anonym verbergen sich rund hundert Pseudonyme von z. B. IP-Adressen, was eine angemessen und nicht reversible Anonymisierung darstellt.

Referenzdokumente

Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen, Version 1.0

Protokollierungsrichtlinie Bund (PR-B) - Protokollierung zur Detektion von Cyber-Angriffen auf die Informationstechnik des Bundes, einschließlich der Umsetzungsrichtlinie zu § 5 Abs. 1 Satz 1 Nr. 1 und i. V. m. Satz 4 BSIG, Version 2.0

Umsetzungsplan Bund 2017 - Leitlinie für Informationssicherheit in der Bundesverwaltung

Abkürzungsverzeichnis

APC	Arbeitsplatzcomputer
APT	Advanced Persistent Threat (engl.)
BDSG	Bundesdatenschutzgesetz
BfDI	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
DSGVO	Datenschutz-Grundverordnung
PDEV-CA	Protokollierungsdatenerhebung und -verwendung für die Detektion von Cyber-Angriffen
PITS	Protokollierungsdaten aus IT-System-Sicht
PN	Protokollierungsdaten aus Netz-Sicht
PR-B	Protokollierungsrichtlinie Bund
PT	Privacy Threat (engl.)
PRSK	Privacy Risk (engl.)