Baustein 43 „Protokollierung“

Version: V1.0
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Hinweis: Dieser Baustein wurde von den Aufsichtsbehörden aus Hessen, Mecklenburg-Vorpommern, Sachsen, Schleswig-Holstein und der Evangelischen Kirche Deutschlands zur Erprobung der SDM-Methode erarbeitet und veröffentlicht. Dieser Baustein ist keine Publikation der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder.

1. Bezug zu Gewährleistungszielen

Transparenz

2. Beschreibung

Die Protokollierung dient der Prüfbarkeit einer Verarbeitung, die in der Vergangenheit stattfand. Zusammen mit der Spezifikation und Dokumentation ist sie eine wesentliche Voraussetzung, um eine Verarbeitung datenschutzrechtlich beurteilen zu können. Prüfbarkeit bedeutet, dass Ist- und Soll-Werte aller relevanten Verarbeitungseigenschaften ermittelt und verglichen werden und somit Prüfergebnisse erzeugt werden können, mit denen fachliche, organisatorische, technische und administrative Aktivitäten und Entscheidungen, die in der Vergangenheit im Rahmen einer Verarbeitung stattfanden, überprüfbar sind. Die Prüfbarkeit ist somit eine Voraussetzung für den Nachweis einer wirksamen Umsetzung der gesetzlichen Datenschutzanforderungen und deren Beurteilung.

Eine Protokollierung muss die Frage beantworten können, welche Instanzen (Organisationseinheiten, Systeme oder handelnde Personen) welche Aktivitäten zu bestimmten Zeitpunkten ausgeführt und welche Instanz das Protokoll darüber geführt hat. Protokolle werden in aller Regel automatisiert erstellt („Logging“), können aber auch händisch geführt werden.

Um einen lückenlosen Nachweis führen zu können, müssen Protokolldaten valide, reliabel, aktuell und vollständig sein. Zumindest bei hohem Schutzbedarf ist eine gesicherte Revisionsfestigkeit von Protokollen begründet. Weisen Protokolldaten einen Personenbezug auf, dürfen sie nur zu ausgewiesenen Zwecken von speziell dazu Befugten ausgewertet werden.

Für die Protokollierung der Tätigkeiten von Mitarbeiter/-innen, Administrationstätigkeiten sowie der Aktivitäten von IT-Systemen und an Schnittstellen gelten ebenfalls der datenschutzrechtliche Zweckbindungsgrundsatz und die Regelungen des Beschäftigtendatenschutzes. Protokolldaten dürfen daher nur zu den Zwecken geprüft werden, die Anlass für ihre Speicherung waren. Um festzustellen, ob die Zweckbindung

eingehalten wird, müssen Protokolldaten unterschiedlicher Ebenen – Protokollierung auf der Ebene der Sachbearbeitung, der Fachprogramme, der IT-Infrastruktur, der Administration – miteinander in eine Beziehung gesetzt werden können, um die Rechtskonformität aller Aktivitäten auf den verschiedenen Ebenen, die sich letztlich zumeist aus den gesetzlichen Regelungen der Fachlichkeit herleiten, nachweisen zu können (M43.20).

Besondere Beachtung ist der Einrichtung einer Protokollierung zu schenken, die auch die Durchführung von Prüfungen der Protokolle dokumentiert (M43.23).

Die Bezeichnung „Protokolldaten“ wird umfassend verwendet und kann neben Logdaten in einem gewissen Sinne auch Akteneinträge auf der fachlichen Ebene sowie von Hand geführte Protokollnotizen etwa von Sitzungen umfassen. Die Bezeichnung „Logdaten“ wird dagegen spezifischer für solche Protokolldaten bezeichnet, die automatisiert von Systemen, Programmen und Diensten erzeugt werden.

Es ist zu empfehlen, „Protokollierung“ als einen Verarbeitungen-übergreifendenProzess, mit Ausweis des Zwecks, der Verantwortung, der verwendeten Mittel sowie der getroffenen Schutzmaßnahmen zu konzipieren und umzusetzen (M43.22).

Was ist zu protokollieren? Zeit, Instanz, Aktivität, Speicherinstanz

Damit eine Verarbeitung vollständig geprüft werden kann, sind folgende Protokolldaten erforderlich:

a) **Zeitkomponente** („Wann?“),
b) **Instanz**, die eine Aktivität auslöst („Wer?“),
c) **Aktivität** bzw. **Ereignis**, das durch die Instanz ausgelöst wurde („Was?“) sowie
d) **Speicherinstanz (Quelle und Ziel)**, die diese Protokolldaten speichert („Protokollierung durch wen?“).

a) **Zeitkomponente**: Der Zeitpunkt des Ereignisses, das protokolliert wird, soll es ermöglichen, kausal zusammenhängende Systemaktivitäten über Programmteile, Server-, Dienst- oder Abteilungs- und Organisationsgrenzen hinweg als zusammenhängende Abläufe nachzuvollziehen. Dies erfordert bei automatisierter Protokollierung gesichert verlässliche Zeitstempel der ausgelösten Ereignisse in Logdateien in sämtlichen Systemen. Die Zeitstempel sollten in einer standardisierten Form, idealerweise über sämtliche zu einer Verarbeitung gehörenden Systeme, Programme und Dienste hinweg, notiert werden (M43.01). Der Zeitpunkt des Ereignisses und der Zeitpunkt des Eintrags in die Log- bzw. Protokolldatei sollten so wenig wie möglich voneinander abweichen.

b) **Instanz**: Diejenige funktionale Instanz, die einen Protokolleintrag erzeugt, muss mit einem eindeutigen Bezeichner im Protokolldatensatz erkennbar und innerhalb eines Systems oder einer Netzinfrastruktur von anderen Instanzen und deren Bezeichnungen unterscheidbar sein (M43.02).

Diese Protokolleinträge müssen es ermöglichen, Bezüge zu den Instanzenbezeichnungen aus Inventarverzeichnissen für Systemkomponenten und Organisationsplänen, Geschäftsverteilungsplänen und Rechte- und Rollenkonzepten herzustellen.

c) **Aktivität**: Die Aktivitäten dieser Instanzen müssen anhand zweifelsfreier Bezeichner eindeutig identifizierbar sein. Das Herausschreiben der bezeichneten Aktivität geschieht typischerweise aus dem Programmcode und nach der Abarbeitung eines Funktionsaufrufes heraus (M43.03).

d) **Protokollierende Instanz**: Wenn es sich um die Logdatei einer Applikation eines Servers handelt, so muss für diese Logdatei eine entsprechende, für Eindeutigkeit sorgende, Namenskonvention festgesetzt sein, aus der die Protokolle-speichernde Instanz und der Zeitraum der Log-Datenerfassungen hervorgehen (M43.04).

Um zu prüfen, ob die Protokollierung aussagekräftig ist, sollte für verschiedene Szenarien (Usecases) geprüft werden, ob die vorhandenen Protokolldaten ausreichen. Dabei ist auch zu prüfen, ob die Protokolldaten-Einträge für Zeitstempel, Aktivitäten und Instanzen verständlich sind (M43.24).

Für Protokolldatenbestände müssen Löschfristen festgelegt werden. In der Regel sind zwei Löschfristen zueinander ins Verhältnis zu setzen: Zum einen die Löschfrist, die aus der Fachlichkeit abzuleiten ist, zum zweiten die Löschfrist, die aus funktionalen Gründen auf der jeweiligen Protokollierungsebene bestehen kann. Die fachlich begründete Löschfrist ist maßgebend (M43.05).

Protokollierung der Nutzeraktivitäten einer Fachapplikation

Die Protokollierung eines Anwendungsprogramms („Fachapplikation“) ist entweder auf dem Client oder zentral auf einem Server einzurichten (M43.04). Die Protokollierung der Fachapplikation muss sicherstellen, dass folgendes geprüft werden kann:

- die Aktivitäten des Sachbearbeiters;
- die Funktionen des Programms, insbesondere die Aktivitäten an Schnittstellen (typisch: Fachprogramm/Datenbank);
- die Aktivitäten der Administration an dem Fachprogramm und
- die Authentisierungs- und Autorisierungsmechanismen auf der Ebene der Sachbearbeitung.

Bei den Aktivitäten der Sachbearbeitung im Fachprogramm ist zu prüfen, welche der folgenden Aktivitäten zu protokollieren sind (M43.06):

- das Lesen von Daten;
- die Eingabe von Daten;
- die Änderung von Daten;
- das Sperren von Daten;

- die manuelle Löschung von Daten;
- die Übermittlung von Daten;
- die Nutzung eines automatisierten Abrufverfahrens;
- der Aufruf von Programmen.

Wenn diese Aktivitäten zu protokollieren sind, müssen die folgenden Eigenschaften festgehalten werden:

- der Zeitpunkt des Zugriffs;
- der Name des Zugreifenden;
- die Bezeichnung der Aktivität (Lesen, Erfassen, Ändern, Sperren, Löschen, Übermitteln).

Es ist festzulegen, ob nur die Tatsache des Zugriffs auf einen Datensatz oder eine Datei protokolliert wird oder ob zusätzlich auch (Auszüge aus den) Inhaltsdaten, die bei einem schreibenden Zugriff verändert wurden im Protokoll notiert werden sollen (etwa nach dem Schema Vorher / Nachher). Die Protokolldaten müssen einem konkreten Fall zugeordnet werden können (bspw. über das Akten- oder Vorgangszeichen). Im Regelfall sollte jedoch auf eine Speicherung von Inhaltsdaten auch im Protokolldatenbestand verzichtet werden (Prinzip der Datenminimierung).

Viele Programme bieten eine Historie an, mit der über einen längeren Zeitraum hinweg jede einzelne Änderung rückgängig gemacht werden kann. Wenn Zeitpunkt und Autor in der Historie erfasst werden, dann entspricht dies einer Vollprotokollierung der Änderungsvorgänge. Der Umfang einer Historie ist bei der Konfiguration eines Programms festzulegen. Die Historie ist entsprechend den Anforderungen zu konfigurieren und in der Regel wie eine Vollprotokollierung zu behandeln.

Wenn rechtlich begründete Sperr- und Löschvorschriften für Daten bestehen, dann muss sichergestellt sein, dass anhand von Protokollauszügen fachlich nachvollzogen und belegt werden kann, dass diese Daten gelöscht bzw. gesperrt wurden.

Die Protokolldaten sind so zu sichern, dass bearbeitende Bedienstete diese einsehen, aber nicht ändern können (M43.07).

Protokollierung der Systemaktivitäten

Ziel der Protokollierung der Systemaktivitäten ist es, Implementationen von Funktionalitäten und wesentliche Veränderungen an den IT-Systemen, den Prozessen, den Betriebssystemen, den Netzen und den Speicherfunktionen und deren Anwendungen im laufenden Betrieb nachträglich nachvollziehen zu können, um deren Rechtmäßigkeit und Sicherheit, die bis auf die Sachbearbeitungsebene ausstrahlen können, nachweisen zu können.

Die folgenden Komponenten müssen anhand von Protokollen bzw. Logdaten überprüfbar sein und als zu protokollierende Instanzen festgelegt werden (M43.08):

- Applikationen (Fachanwendungen);
- Datenbanken;
- Dienste (wie Webserver, Mailserver, Fileserver);
- Betriebssysteme, inkl. virtualisierte Systeme;
- aktive Netzkomponenten (wie z. B. Router, Switche);
- Sicherheitskomponenten im Netz (wie Firewall, Proxy, Intrusion-Detection-System);
- Speichersysteme (SAS, NAS);
- Sicherheitskomponenten auf Servern (wie Sicherheitsgateways, Virus-Scanner),;
- physikalische Zutrittssysteme.

Bei der Prüfung von Protokolldaten sollte besondere Aufmerksamkeit bzgl. Systemaktivitäten den Prozessen mit speziellen Datenschutz-Schutzfunktionen – Hashwertbildungen für Integritätsprüfungen, Verschlüsselungen, Pseudonymisierungen, Anonymisierungen – gelten. Hier könnten die Prüfanlässe enger als zur Prüfung anderer Eigenschaften geregelt werden (bzgl. der Regelmäßigkeit, der Häufigkeit, jedenfalls nicht nur anlassgetrieben).

Protokollierung der Administrationstätigkeiten

Ziel der Protokollierung von Administrationstätigkeiten bei personenbezogenen Verarbeitungen ist es, die Aktivitäten der Administratoren prüfen zu können. Administratoren verfügen in der Regel über umfangreiche Rechte, die es ihnen erlauben, die Strukturen einer Verarbeitung und die Rechte- und Rollen der Nutzer zu ändern sowie mitunter auch unbefugt auf Inhaltsdaten zuzugreifen. Wenn die Aktivitäten der Administration kaum wirkungsvoll eingeschränkt werden können, müssen diese wenigstens nachträglich überprüfbar sein. Eine Protokollierung der Aktivitäten schützt Administratoren zudem vor pauschalen Verdächtigungen und dient dem Nachweis ordnungsgemäßer Tätigkeit.

Bei der Administration von IT-Systemen sind die folgenden Aktivitäten im Administrationskonzept festzulegen und zu protokollieren (M43.09):

- Systemgenerierung und Modifikation von Systemparametern;
- Verwalten von Benutzern (Einrichtung, Änderungen, Austragungen);
- Erstellung von Rechteprofilen (Aktivitäten und Berechtigungen);
- Einspielen und Änderung von Anwendungssoftware;
- Durchführung von Datensicherungsmaßnahmen;
- Sonstiger Aufruf von Administrationsprogrammen und Verfolgen der Aktivitäten;
- Versuche unbefugten Einloggens und Überschreitung von Befugnissen.

Die Protokollierung von Administrationsaktivitäten ermöglicht die Prüfbarkeit (M43.25):

- des Zugriffs auf Inhaltsdaten, in Bezug auf Lesen, Eingabe, Änderung, Sperren oder Löschen;

- des Zugriffs auf Protokolldaten, in Bezug auf Lesen, Eingabe, Änderung, Sperren oder Löschung;
- des Zugriffs auf Daten zur Nutzerverwaltung, in Bezug auf Lesen, Eingabe, Änderung oder Löschung;
- der Änderungen von Rechteprofilen an Programmen, Datenbeständen und Verzeichnissen, insbesondere Änderungen von Datensicherungsmaßnahmen;
- des Anlegens, Änderns und Löschens von Verzeichnissen;
- des Anlegens, Änderns, Sperrens und Löschens von Nutzern und Nutzergruppen, um klären zu können, welcher Nutzer von wem für welchen Zeitraum das Recht eingeräumt bekommen hat, bestimmte IT-Komponenten zu nutzen oder bestimmte Übermittlungen auszulösen oder bestimmten anderen Nutzer bestimmte Rechte eingeräumt zu haben;
- des Aufsetzens (Installation, Konfiguration) von Systemen, Hardware und Software;
- des Aufrufs von Administrationstools;
- der Übermittlung von Daten;
- des Härtens von Systemen, Integrationssicherungsmaßnahmen der Systeme (durch Hashwertbildungen und Verwaltung) unmittelbar vor der Produktivstellung;
- der Installation, des Patchens, der Konfiguration von Betriebssystemen, Middleware und Applikationen;
- des Zugangs zu IT-Systemen und zu Räumen.

Protokollierung von Schnittstellenaktivitäten

Ziel der Protokollierung an Schnittstellen ist es, die Übermittlung von Daten prüfen zu können. Dies ist von besonderer Bedeutung, weil Übermittlungen oft mit einer Änderung des Zwecks einhergehen oder zu einer Verarbeitung unter einer anderen Rechtsgrundlage und mit anderen Verantwortlichen führen.

Für den Einsatz der Protokollierung an Schnittstellen (Routern, Sicherheitsgateways) sollten die folgenden Aspekte beachtet werden (M43.10):

- Den organisationsinternen Protokolldaten müssen den einzelnen IT-Systemen (oder Rollen) und Fachprogrammen der Organisation eindeutig zugeordnet sein.
- Die Größe des freien Protokollspeicherplatzes auf dem verwendeten Speichermedium sollte regelmäßig kontrolliert werden, da an Schnittstellen grundsätzlich damit zu rechnen ist, dass insbesondere bei unbefugten Datentransporten zahlreiche Übermittlungsvorgänge stattfinden. Bei hohem Schutzbedarf sollte sämtlicher Verkehr automatisch blockiert werden, wenn keine Schnittstellenprotokollierung des Datenstroms erfolgt.
- Ereignisse wie unzulässige Verbindungsversuche oder der Aufruf unsicherer Protokolle für ungesicherte Kommunikationsverbindungen sollten im Protokolldatenbestand hervorgehoben werden. Sie sollten zu einer unverzüglichen

Warnung des Administrators und/oder des fachlich Verantwortlichen über einen gesicherten Kommunikationskanal führen.

Eine spezielle Beachtung bzgl. Protokollierung muss Paketfiltern und Proxys geschenkt werden. Hierbei gibt es wesentliche Überschneidungen aber auch Konflikte mit den Interessen an der IT-Sicherheit.

Die Aktivitäten dieser IT-Systeme müssen durch hinreichend genaue Zeitstempel sowie konsistente Bezeichnungen in eine kausal-prüfbare Beziehung sowohl zu den Aktivitäten auf der Ebene der Sachbearbeitung als auch zu den Aktivitäten der Systemadministration gesetzt werden können.

Verarbeitung von Protokolldaten

Eine Voraussetzung zur Prüfung von Protokolldaten besteht darin zu kontrollieren, welche Protokolldaten die Fachapplikationen, die verschiedenen IT-Systeme und Prozesse insbesondere auf der Infrastrukturebene sowie die Administrationstätigkeiten an diesen Systemen erzeugen.

Bei bestehenden Systemen müssen sämtliche Protokolldaten inventarisiert werden inklusive den Nachweis darüber, dass diese Protokollinhalte gesichtet und deren Relevanz für den Datenschutz beurteilt wurde (M43.11).

Bereits in der Spezifikationsphase muss definiert werden, für welche Fragen und Prüfungen welche Protokolldaten erforderlich sind. Insbesondere wenn marktgängige Standard-Programme eingesetzt werden sollen wird es notwendig sein, noch vor der Inbetriebnahme zu prüfen, welche Protokolldaten standardmäßig erzeugt werden und ggfs. datenschutzrechtlich erforderliche Änderungen beim Hersteller zu verlangen.

Protokolldaten werden von verschiedenen Systemen erzeugt und liegen daher in der Regel in verschiedenen Formaten vor. Um die Prüfung der Protokolle zu erleichtern ist es vielfach hilfreich, die „rohen“ Protokolldaten wie folgt aufzubereiten:

- **Filterung:** Protokolldaten sollten so gefiltert werden, dass unnötige Protokollmeldungen aussortiert werden (M43.12).
- **Normalisierung:** Protokolldaten sollten bspw. durch Konvertieren in ein einheitliches Datenformat standardisiert werden (M43.13).
- **Aggregation**: Protokolldaten identischen Inhalts sollen zusammengefasst werden (M43.014).
- **Kategorisierung:** Protokollmeldungen sollten nach Systemen, Aktivitäten oder nach Risikobereichen kategorisiert werden, um den Informationsgehalt zu erhöhen (M43.15).
- **Priorisierung:** Die Ausgabe von Protokollmeldungen sollten dynamisch priorisiert werden können, um deren Beurteilung zu vereinfachen (M43.16).

Generell ist für diese Verarbeitungsschritte von Protokolldaten sicherzustellen, dass die Skripte zur Verarbeitung von Protokolldaten integritätsgesichert zum Einsatz kommen und genau nur das ausführen, was sie vorgeben auszuführen (M43.17).

Beispiele für weitere aufbereitete Ausgaben von Protokolldaten, mit denen der laufende Betrieb insbesondere durch die Administration sichergestellt wird, sind:

- **Gruppierung** und Markierung zusammengehörender Protokolldaten;
- Anzeige **relevanter Protokolldaten** aufgrund charakteristischer Zeichenketten bzw. Ausblenden irrelevanter Daten mittels regulärer Ausdrücke;
- **statistische Analyse** der Protokolldaten (z. B. auf die Frage: Wie oft traten welche Meldungen auf?).

Um die Aussagekraft relevanter Protokolldaten zu erhöhen sollten Tools eingesetzt werden, die abhängig von einer erkannten Auffälligkeit Aktionen (z. B. Ausführen eines Befehls) ermöglichen (M43.31). Auffällige Protokolleinträge sind beispielsweise:

- Gehäuft auftretende Anfragen an Ports, auf denen keine Dienste laufen;
- nicht erfolgreiche Zugriffsversuche auf Komponenten eines Servers, insbesondere auf Sicherheitsgateways;
- aus einem nicht-vertrauenswürdigen Netz eintreffende Pakete mit IP-Adressen des vertrauenswürdigen Netzes (Hinweis auf IP-Spoofing);
- verdächtige, ausgehende Verbindungen von Servern aus dem vertrauenswürdigen Netz (diese können ein Anzeichen dafür sein, dass nach einem erfolgreichen Einbruch der Angreifer Daten aus dem vertrauenswürdigen Netz nach außen kopiert oder von außen Dateien nachlädt, die er für seine weiteren Aktivitäten braucht.);
- nicht-spezifizierte Protokolleinträge;
- unberechtigter Zugang und Zugriff;
- Autorisierungsverstöße
- …

Zur Analyse von Protokolldaten sollten „Logfile-Analyzer“ eingesetzt werden (M43.21). Zeichenketten, nach denen Protokolldatenbstände durchsucht werden, sollten dokumentiert werden (M43.18). Dadurch können die Verantwortlichen nachvollziehen, welche Analysen durch die Systemadministration durchgeführt werden.

Vorverarbeitete Protokolldaten sind, zumeist geleitet von bestimmten inhaltlichen Fragestellungen, zu Reports zusammenzustellen, die den Verantwortlichen zur Prüfung der datenschutzrechtlichen Konformität der Datenverarbeitung vorgelegt werden. Dabei sind Protokolldaten in der Regel mit inhaltlichen Daten zu korrelieren.

Behandlung von Prüfergebnissen

Um relevante Prüfergebnisse erzeugen zu können, müssen Prüfprozesse hinreichend spezifiziert sein. Für die Spezifikation sind folgende Fragen relevant (M43.27):

- Welche Prüfdaten sind zu erzeugen, um die Wirksamkeit der Maßnahmen zur Umsetzung der Gewährleistungsziele nachweisen zu können oder um die fehlende Wirksamkeit der Maßnahmen im laufenden Betrieb entdecken zu können?
- Welche darauf bezogenen Prüfergebnisse sind einer gesonderten, über verschiedene Systeme hinweg, zu vertiefenden Beurteilung zu unterziehen?
- Wer ist für die Herstellung und die nachfolgende Beurteilung von Prüfergebnissen zuständig (Rollen oder Personen)?
- Auf welche Weise müssen Prüf- und Beurteilungsergebnis übermittelt werden?
- Bei welchen Warnungen und Vorfällen, die im Rahmen der Überwachung des Datenschutzes und der IT-Sicherheit anfallen, ist auch der/die IT-Sicherheitsbeauftragte bzw. Datenschutzbeauftragte zu beteiligen?

Die Ursachenforschung bei der Feststellung von fehlerhaften bzw. nicht-rechtskonformen Abweichungen ist wichtig. Es muss das Ziel sein, den laufenden Betrieb rechtskonform zu machen bzw. zu halten und Fehler in Zukunft zu verhindern oder zumindest möglichst schnell zu beheben. Die Analyse von Fehlern, die Entscheidungen und die eingeleiteten Maßnahmen nach erfolgter Ursachenforschung sind zu dokumentieren (M43.28).

Zwei spezielle Aspekte des Protokollierens sollen noch kurz angesprochen werden: Das „Monitoring“ und das „Quittieren“. Im Unterschied zur Protokollierung ist ein Monitoring eine Feststellung, welche Aktivitäten von welcher Instanz aktuell ausgeführt werden, um unmittelbare Entscheidungen über den Fortgang zu (z.B. Pförtner-Aktivitäten). In der Regel werden die Entscheidung, der Zeitpunkt und die betroffene Instanz in einem Protokoll notiert. Und „Quittungen“ werden vielfach eingesetzt, um Betroffenen die korrekte Ausführung in Bezug auf ein bestimmtes Ereignis, dass eine bestimmte Instanz zu einem Zeitpunkt ausgelöst hat, zu bestätigen. Auch Quittungsdaten werden zumeist gesammelt und sind als Protokolldaten geeignet, um Systemzustände in der Vergangenheit bei den Beteiligten zu dokumentieren.

3. Differenzierung bei hohem Schutzbedarf

Aus Datenschutzsicht bedeutet ein hoher Schutzbedarf bzgl. der Transparenz einer Verarbeitung, dass erhöhte Anforderungen an die Qualität insbesondere der Revisionsfestigkeit und des Beweiswerts der Protokolldaten bestehen. Es müssen die Prüfinteressen nicht nur der Organisation selber, sondern auch der Betroffenen sowie der Aufsichtsbehörden beachtet werden.

Ein hoher Schutzbedarf für einen Protokolldatenbestand wirkt sich grundsätzlich auf die Inhalte sowie die Auswahl und Ausgestaltung von Maßnahmen aus, mit denen die Inhalte eines Protokolls bzw. Logs generiert, gespeichert, transformiert, übermittelt und geschützt werden. Eine generelle Strategie zur Umsetzung von Schutzmaßnahmen für hohen Schutzbedarf besteht darin, die Schutzmaßnahmen der verschiedenen Gewährleistungsziele auch auf die Schutzmaßnahmen selber anzuwenden. So sollte bspw. die Integrität von

Protokolldaten durch regelmäßiges Hashen und die Vertraulichkeit dieser Daten durch Verschlüsselung sichergestellt werden.

Sofern bei normalem Schutzbedarf rechtlich gut begründet keine Vollprotokollierung von Zugriffen vorgesehen ist, muss bei Anforderungen mit hohem Schutzbedarf an die Transparenz in der Regel eine Vollprotokollierung eingeschaltet werden.

Für Verarbeitungen mit hohem Schutzbedarf ist ein zertifizierter Zeitstempel zu nutzen (M43.19).

Zur Speicherung aller Protokoll- und Logdaten sollte ein dedizierter Protokolleserver betrieben werden, für dessen Implementation, Konfiguration und Betrieb wiederum Schutzmaßnahmen anhand des vollständigen Sets an Gewährleistungszielen zu treffen sind (M43.29). Insbesondere sind Protokolldaten beim Transfer von Produktivsystemen auf andere Computer, wie bspw. einen Protokolleserver, gegen unbefugte Kenntnisnahmen und Änderungen zu schützen (M43.30).

4. Referenzen

BSI: *OPS.1.1.5 Protokollierung*
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_5_Protokollierung.html;jsessionid=8B275BA38F10A2449C5258B4839E9CE4.1_cid369

B 5.22 Protokollierung
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05022.html

5. Zusammenfassung der Maßnahmen

Ebene Daten

M43.01 Zeitstempel standardisieren
M43.02 Bezeichner der Instanz festlegen
M43.03 Bezeichner für Aktivität festlegen
M43.04 Protokollierungsinstanz festlegen
M43.05 Löschfristen für Protokolldaten festlegen
M43.06 Inhalte der Protokollierung der Sachbearbeitung festlegen
M43.07 Integritätssicherung der Protokollierung auf Ebene Sachbearbeitung
M43.08 Inhalte der Protokollierung der Systemaktivitäten
M43.09 Inhalte der Protokollierung von Administrationstätigkeiten festlegen
M43.10 Inhalte der Protokollierung der Schnittstellen festlegen
M43.11 Protokolldaten inventarisieren (kontrollieren, prüfen, beurteilen)
M43.12 Protokolldaten filtern
M43.13 Protokolldaten normalisieren / standardisieren

M43.14 Protokolldaten aggregieren / zusammenfassen
M43.15 Protokolldaten kategorisieren
M43.16 Protokolldaten priorisieren
M43.17 Protokollbearbeitungsskripte integritätssichern
M43.18 Liste mit kritischen Zeichenketten für Protokolldatenanalyse erstellen
M43.19 Einsatz von zertifizierten Zeitstempeln in Protokolleinträgen

Ebene Systeme

M43.20 Korrelationen von Protokollen über verschiedene Ebenen der Verarbeitungstätigkeiten prüfen zwecks Zweckbindung
M43.21 Protokolldaten mit „Log-Analyzern“ analysieren
M43.22 Ausführen von Befehlen, wenn bestimmte Protokolleinträge erscheinen

Ebene Prozesse

M43.23 Protokollierungskonzept erstellen
M43.24 Prüfungen von Protokollen protokollieren
M43.25 Auswertungsszenarien formulieren
M43.26 Aktivitäten der Systemadministration protokollieren
M43.27 Reports aus Protokolldaten erstellen
M43.28 Fragen zur Spezifikation von Protokolldaten
M43.29 Dokumentation von Prüfergebnissen
M43.30 Einsatz eines Protokolleservers
M43.31 Sichern des Transfers von Protokolldaten

6. Anmerkung zur Nutzung dieses Bausteins