



OPS.1.1.5 Protokollierung

1. Beschreibung

1.1. Einleitung

Damit ein verlässlicher IT-Betrieb gewährleistet ist, sollten IT-Systeme und Anwendungen entweder alle oder zumindest ausgewählte betriebs- und sicherheitsrelevante Ereignisse protokollieren, d. h. sie automatisch speichern und für die Auswertung bereitstellen. Eine Protokollierung wird in vielen Institutionen eingesetzt, um Hard- und Softwareprobleme sowie Ressourcenengpässe rechtzeitig entdecken zu können. Aber auch Sicherheitsprobleme und Angriffe auf die betriebenen Netzdienste können anhand von Protokollierungsdaten nachvollzogen werden. Ebenso können mit solchen Daten durch forensische Untersuchungen Beweise gesichert werden, nachdem ein Angriff auf IT-Systeme oder Anwendungen bekannt wurde.

In jedem Informationsverbund werden lokal Protokollierungsdaten von einer Vielzahl von IT-Systemen und Anwendungen generiert. Um jedoch einen Gesamtüberblick über einen Informationsverbund zu erhalten, können die von verschiedenen IT-Systemen und Anwendungen generierten Protokollierungsereignisse an eine dedizierte Protokollierungsinfrastruktur gesendet und dort zentral gespeichert werden. Nur so lassen sich die Protokollierungsdaten an einer zentralen Stelle auswählen, filtern und systematisch auswerten.

1.2. Zielsetzung

Ziel des Bausteins ist es, alle relevanten Daten sicher zu erheben, zu speichern und geeignet für die Auswertung bereitzustellen, damit möglichst alle sicherheitsrelevanten Ereignisse protokolliert werden können.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.5 *Protokollierung* ist einmal auf den gesamten Informationsverbund anzuwenden.

Im vorliegenden Baustein werden ausschließlich übergreifende Aspekte betrachtet, die für eine angemessene Protokollierung erforderlich sind. Die Protokollierung spezifischer IT-Systeme oder Anwendungen wird hier nicht behandelt, sondern in den jeweiligen Bausteinen des IT-Grundschutz-Kompendiums beschrieben.

In vielen Betriebssystemen oder Anwendungen sind Protokollierungsfunktionen bereits vorhanden oder können dort mittels Zusatzprodukten integriert werden. Um diese Funktionen und die

gespeicherten Protokollierungsdaten abzusichern, muss das zugrundeliegende Betriebssystem geschützt sein. Das ist jedoch nicht Bestandteil dieses Bausteins. Dafür sind die betriebssystemspezifischen Bausteine umzusetzen, z. B. SYS.1.2.3 *Windows Server*.

Im Vorfeld der Protokollierung von sicherheitsrelevanten Ereignissen ist es wichtig, dass Zuständigkeiten und Kompetenzen klar definiert und zugewiesen werden. Es sollte insbesondere auf den Grundsatz der Funktionstrennung geachtet werden. Dieses Thema ist nicht Bestandteil dieses Bausteins, sondern wird im Baustein ORP.1 *Organisation* behandelt.

Auch ist dieser Baustein abzugrenzen von der Detektion von sicherheitsrelevanten Ereignissen (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen*) sowie der Reaktion auf Sicherheitsvorfälle (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*). Beide Aspekte werden im vorliegenden Baustein nicht oder nur am Rande behandelt.

Ebenfalls an anderer Stelle beschrieben werden die Auswertung von Protokollierungsdaten sowie deren langfristige, sichere, unveränderbare und reproduzierbare Speicherung (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen* bzw. OPS.1.2.2 *Archivierung*).

Vorgaben, wie mit personenbezogenen Daten umzugehen ist, werden im Baustein CON.2 *Datenschutz* beschrieben.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.5 *Protokollierung* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Protokollierung

In einem Informationsverbund gibt es häufig IT-Systeme oder Anwendungen, bei denen die Protokollierung in der Grundeinstellung nicht aktiviert wurde. Auch können einzelne IT-Systeme oder Anwendungen manchmal gar nicht protokollieren. In beiden Fällen können wichtige Informationen verloren gehen und Angriffe nicht rechtzeitig erkannt werden. Das ist auch dann möglich, wenn die Protokollierung bei einzelnen IT-Systemen oder Anwendungen zwar genutzt wird, aber die Protokollierungsdaten nicht an einer zentralen Stelle zusammengeführt werden. In Informationsverbänden ohne zentrale Protokollierung lässt sich schwer sicherstellen, dass die relevanten Protokollinformationen aller IT-Systeme und Anwendungen erhalten bleiben und ausgewertet werden.

Weiterhin müssen Protokollierungsdaten aussagekräftige Informationen enthalten. Welche Ereignisse protokolliert werden, hängt unter anderem auch vom Schutzbedarf der jeweiligen IT-Systeme oder Anwendungen ab. Wird dieser missachtet, indem beispielsweise bei der Protokollierung nur auf Standard-Einstellungen der IT-Systeme bzw. Anwendungen zurückgegriffen wird, kann dies dazu führen, dass besonders relevante Sicherheitsereignisse nicht protokolliert werden. Somit werden Angriffe eventuell nicht erkannt.

2.2. Fehlerhafte Auswahl von relevanten Protokollierungsdaten

Protokollierungsdaten liefern oft wichtige Informationen, die dabei helfen, Sicherheitsvorfälle zu erkennen. Eine besondere Herausforderung ist es, die relevanten Meldungen aus der großen Menge der verschiedenen Protokollierungsereignisse herauszufiltern. Denn viele Protokollierungsereignisse haben nur informativen Charakter und lenken von den wirklich wichtigen Meldungen ab. Werden zu viele Protokollierungsereignisse ausgewählt, lässt sich die Fülle an Informationen nur schwer und mit hohem Zeitaufwand auswerten.

Des Weiteren können Protokollierungsereignisse verworfen oder überschrieben werden, wenn der Arbeitsspeicher oder die Festplattenkapazität des IT-Systems bzw. der Protokollierungsinfrastruktur nicht ausreichen. Werden dadurch zu wenige oder nicht ausreichend relevante Protokollierungsereignisse aufgezeichnet, dann könnten sicherheitskritische Vorfälle unerkannt bleiben.

2.3. Fehlende oder fehlerhafte Zeitsynchronisation bei der Protokollierung

Wenn in einem Informationsverbund die Zeit nicht auf allen IT-Systemen synchronisiert wird, können die Protokollierungsdaten eventuell nicht miteinander korreliert werden bzw. kann die Korrelation eventuell zu fehlerhaften Aussagen führen. Grund dafür ist, dass die unterschiedlichen Zeitstempel von Ereignissen keine gemeinsame Basis aufweisen. Eine fehlende Zeitsynchronisation erschwert es somit, erhobene Protokollierungsdaten auszuwerten, insbesondere, wenn diese auf einem zentralen Logserver gespeichert werden. Weiterhin kann eine fehlerhafte oder fehlende Zeitsynchronisation dazu führen, dass die Protokollierung nicht zur Beweissicherung herangezogen werden kann.

2.4. Fehlplanung bei der Protokollierung

Wird die Protokollierung nicht ausreichend geplant, dann kann dies dazu führen, dass IT-Systeme oder Anwendungen nicht überwacht und sicherheitsrelevante Ereignisse somit nicht erkannt und angemessen behandelt werden. Datenschutzverstöße könnten ebenfalls nicht nachvollzogen werden.

2.5. Vertraulichkeits- und Integritätsverlust von Protokollierungsdaten

Einige IT-Systeme in einem Informationsverbund generieren Protokollierungsdaten wie Anmeldenamen, IP-Adressen, E-Mail-Adressen und Rechnernamen, die konkreten Personen zugeordnet werden können. Solche Informationen lassen sich kopieren, abhören und manipulieren, wenn sie nicht verschlüsselt übertragen und gesichert gespeichert werden. Dies kann dazu führen, dass Angreifende auf vertrauliche Informationen zugreifen oder dass, durch manipulierte Protokollierungsdaten, Sicherheitsvorfälle bewusst verschleiert werden. Ebenso können Angreifende, wenn sie an eine größere Menge von Protokollierungsdaten gelangen, diese Informationen nutzen, um die interne Struktur des Informationsverbunds aufzudecken und dadurch ihre Angriffe gezielter ausrichten.

2.6. Falsch konfigurierte Protokollierung

Wenn die Protokollierung in IT-Systemen falsch konfiguriert ist, werden wichtige Informationen entweder fehlerhaft oder gar nicht aufgezeichnet. Auch kann es sein, dass zu viele oder falsche Informationen protokolliert werden. So können z. B. personenbezogene Daten unberechtigt protokolliert und gespeichert werden. Die Institution könnte dadurch gegen gesetzliche Anforderungen verstoßen.

Durch eine falsch konfigurierte Protokollierung ist es ebenso möglich, dass die Protokollierungsdaten in inkonsistenten oder proprietären Formaten vorliegen. Dadurch lassen sich die Protokolle eventuell nur schwer auswerten und Sicherheitsvorfälle bleiben unentdeckt.

2.7. Ausfall von Datenquellen für Protokollierungsdaten

Liefern IT-Systeme in einem Informationsverbund nicht mehr die notwendigen Protokollierungsdaten, lassen sich Sicherheitsvorfälle nicht mehr angemessen detektieren. Ursache für solche Ausfälle von Datenquellen können Fehler in der Hard- und Software oder auch fehlerhaft

administrierte IT-Systeme sein. Besonders, wenn nicht bemerkt wird, dass Datenquellen ausgefallen sind, kann dies zu einem falschen Bild der Sicherheitslage in der Institution führen. Dadurch können Angreifende z. B. sehr lange unbemerkt bleiben und institutionskritische Informationen abgreifen oder Produktionssysteme manipulieren.

2.8. Ungenügend dimensionierte Protokollierungsinfrastruktur

Aufgrund der komplexen Informationsverbünde und der vielfältigen Angriffsszenarien steigen die Anforderungen an die Protokollierung, da sehr viele Protokollierungsdaten gespeichert und verarbeitet werden müssen. Weiterhin ist es bei Sicherheitsvorfällen üblich, die Intensität der Protokollierung zu erhöhen. Ist die Protokollierungsinfrastruktur dafür jedoch nicht ausgelegt, kann es passieren, dass Protokollierungsdaten unvollständig gespeichert werden. Somit lassen sich sicherheitsrelevante Ereignisse nicht mehr oder nur unzureichend auswerten und Sicherheitsvorfälle bleiben unentdeckt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.5 *Protokollierung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.5.A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung (B) [Fachverantwortliche]

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

Die spezifische Sicherheitsrichtlinie MUSS von dem oder der ISB gemeinsam mit den Fachverantwortlichen erstellt werden. Sie MUSS allen für die Protokollierung zuständigen Mitarbeitenden bekannt und grundlegend für ihre Arbeit sein. Wird die spezifische Sicherheitsrichtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem oder der ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist. Die Ergebnisse der Überprüfung MÜSSEN dokumentiert werden.

OPS.1.1.5.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene (B)

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

In angemessenen Intervallen MUSS stichpunktartig überprüft werden, ob die Protokollierung noch korrekt funktioniert. Die Prüfintervalle MÜSSEN in der Protokollierungsrichtlinie definiert werden.

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

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

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

OPS.1.1.5.A5 Einhaltung rechtlicher Rahmenbedingungen (B)

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

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

Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden.

Protokollierungsdaten MÜSSEN nach einem festgelegten Prozess gelöscht werden. Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.1.5.A6 Aufbau einer zentralen Protokollierungsinfrastruktur (S)

Alle gesammelten sicherheitsrelevanten Protokollierungsdaten SOLLTEN an einer zentralen Stelle gespeichert werden. Dafür SOLLTE eine zentrale Protokollierungsinfrastruktur im Sinne eines Logserver-Verbunds aufgebaut und in einem hierfür eingerichteten Netzsegment platziert werden (siehe NET.1.1 *Netzarchitektur und -design*).

Zusätzlich zu sicherheitsrelevanten Ereignissen (siehe OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene*) SOLLTE eine zentrale Protokollierungsinfrastruktur auch allgemeine Betriebsereignisse protokollieren, die auf einen Fehler hindeuten.

Die Protokollierungsinfrastruktur SOLLTE ausreichend dimensioniert sein. Die Möglichkeit einer Skalierung im Sinne einer erweiterten Protokollierung SOLLTE berücksichtigt werden. Dafür SOLLTEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein.

OPS.1.1.5.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.5.A8 Archivierung von Protokollierungsdaten (S)

Protokollierungsdaten SOLLTEN archiviert werden. Dabei SOLLTEN die gesetzlich vorgeschriebenen Regelungen berücksichtigt werden.

OPS.1.1.5.A9 Bereitstellung von Protokollierungsdaten für die Auswertung (S)

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

Damit sich die Daten automatisiert auswerten lassen, SOLLTEN die Protokollanwendungen über entsprechende Schnittstellen für die Auswertungsprogramme verfügen.

Es SOLLTE sichergestellt sein, dass bei der Auswertung von Protokollierungsdaten die Sicherheitsanforderungen eingehalten werden, die in der Protokollierungsrichtlinie definiert sind. Auch wenn die Daten bereitgestellt werden, SOLLTEN betriebliche und interne Vereinbarungen berücksichtigt werden.

Die Protokollierungsdaten SOLLTEN zusätzlich in unveränderter Originalform aufbewahrt werden.

OPS.1.1.5.A10 Zugriffsschutz für Protokollierungsdaten (S)

Es SOLLTE sichergestellt sein, dass die ausführenden Administrierenden selbst keine Berechtigung haben, die aufgezeichneten Protokollierungsdaten zu verändern oder zu löschen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.5.A11 Steigerung des Protokollierungsumfangs (H)

Bei erhöhtem Schutzbedarf von Anwendungen oder IT-Systemen SOLLTEN grundsätzlich mehr Ereignisse protokolliert werden, sodass sicherheitsrelevante Vorfälle möglichst lückenlos nachvollziehbar sind.

Um die Protokollierungsdaten in Echtzeit auswerten zu können, SOLLTEN sie in verkürzten Zeitabständen von den protokollierenden IT-Systemen und Anwendungen zentral gespeichert werden. Die Protokollierung SOLLTE eine Auswertung über den gesamten Informationsverbund ermöglichen. Anwendungen und IT-Systeme, mit denen eine zentrale Protokollierung nicht möglich ist, SOLLTEN bei einem erhöhten Schutzbedarf NICHT eingesetzt werden.

OPS.1.1.5.A12 Verschlüsselung der Protokollierungsdaten (H)

Um Protokollierungsdaten sicher übertragen zu können, SOLLTEN sie verschlüsselt werden. Alle gespeicherten Protokolle SOLLTEN digital signiert werden. Auch archivierte und außerhalb der Protokollierungsinfrastruktur gespeicherte Protokollierungsdaten SOLLTEN immer verschlüsselt gespeichert werden.

OPS.1.1.5.A13 Hochverfügbare Protokollierungsinfrastruktur (H)

Eine hochverfügbare Protokollierungsinfrastruktur SOLLTE aufgebaut werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) regelt in seinem Mindeststandard „Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen“ die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen (SRE). Die Mindeststandards sind von den in § 8 Abs. 1 Satz 1 BSIG genannten Stellen der Bundesverwaltung umzusetzen.

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27001:2013 im Kapitel A.12.4 „Protokollierung und Überwachung“ Vorgaben zur Protokollierung.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ in Kapitel TM1.2 - Security Event Logging - Vorgaben zur Protokollierung.

Das National Institute of Standards and Technology (NIST) beschreibt in seiner Special Publication 800-92 „Guide to Computer Security Log Management“, wie Protokollierung sicher eingesetzt werden kann.