|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Protokollierung"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300012 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Protokollierung" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc79384530)

[Dokumentenhistorie 3](#_Toc79384531)

[Inhaltsverzeichnis 4](#_Toc79384532)

[Allgemeine Festlegungen 5](#_Toc79384533)

[Ziel / Zweck 5](#_Toc79384534)

[Geltungsbereich 5](#_Toc79384535)

[Zuständigkeiten 6](#_Toc79384536)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79384537)

[Aufbau des Dokuments 6](#_Toc79384538)

[Sicherheitsrichtlinie „Protokollierung" 7](#_Toc79384539)

[Basismaßnahmen 7](#_Toc79384540)

[Festlegung von Rollen und Verantwortlichkeiten (OPS.1.1.5.A2) 7](#_Toc79384541)

[Konfiguration der Protokollierung auf System- und Netzebene (OPS.1.1.5.A3) 7](#_Toc79384542)

[Zeitsynchronisation der IT-Systeme (OPS.1.1.5.A4) 7](#_Toc79384543)

[Einhaltung rechtlicher Rahmenbedingungen (OPS.1.1.5.A5) 7](#_Toc79384544)

[Standardmaßnahmen 8](#_Toc79384545)

[Aufbau einer zentralen Protokollierungsinfrastruktur (OPS.1.1.5.A6) 8](#_Toc79384546)

[Sichere Administration von Protokollierungsservern (OPS.1.1.5.A7) 8](#_Toc79384547)

[Archivierung von Protokollierungsdaten (OPS.1.1.5.A8) 9](#_Toc79384548)

[Bereitstellung von Protokollierungsdaten für die Auswertung (OPS.1.1.5.A9) 9](#_Toc79384549)

[Zugriffsschutz für Protokollierungsdaten (OPS.1.1.5.A10) 9](#_Toc79384550)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc79384551)

[Steigerung des Protokollierungsumfangs (OPS.1.1.5.A11 - CA) 9](#_Toc79384552)

[Verschlüsselung der Protokollierungsdaten (OPS.1.1.5.A12 - CIA) 10](#_Toc79384553)

[Hochverfügbare Protokollierungssysteme (OPS.1.1.5.A13 - A) 10](#_Toc79384554)

# Allgemeine Festlegungen

## Ziel / Zweck

Um einen verlässlichen IT-Betrieb gewährleisten zu können, sollten Cloud-Services, Netzkomponenten, Sicherheitskomponenten, IT-Systeme, Anwendungen entweder alle oder zumindest ausgewählte betriebs- und sicherheitsrelevante Ereignisse protokollieren, d. h. sie automatisch speichern und für die Auswertung bereitstellen. Eine Protokollierung wird eingesetzt, um Netz-, Hard- und Softwareprobleme sowie Ressourcenengpässe rechtzeitig entdecken zu können. Aber auch Sicherheitsprobleme und Angriffe auf die betriebenen Services können anhand von Protokollierungsdaten nachvollzogen werden. Ebenso können mit solchen Daten durch forensische Untersuchungen Beweise gesichert werden, nachdem ein Angriff bekannt wurde.

Bei einer Vielzahl von IT-Systemen und Anwendungen werden lokal Protokollierungsdaten generiert. Um jedoch einen Gesamtüberblick zu erhalten, müssen die von verschiedenen IT-Systemen und Anwendungen generierten Protokollinformationen 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.

Ziel dieser Sicherheitsrichtlinie ist es aufzuzeigen, wie die Protokollierung möglichst aller sicherheitsrelevanten Ereignisse umgesetzt werden kann. Ebenfalls ist es das Ziel, alle hierfür relevanten Daten sicher zu erheben, zu speichern und geeignet für die Auswertung bereitzustellen sowie deren ordnungsgemäße Entsorgung sicherzustellen. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines OPS.1.1.5 "Protokollierung" beachtet.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Das Dokument „Sicherheitsrichtlinie Protokollierung“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Protokollierung"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Festlegung von Rollen und Verantwortlichkeiten (OPS.1.1.5.A2)

Für die definierten IT-Systeme und Anwendungen sind Verantwortliche benannt. Diese stellen sicher, dass die Maßnahmen und Vorgaben der Protokollierungsrichtlinie eingehalten werden.

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

Alle sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen werden protokolliert. Wenn die Protokollierung eingerichtet wird, werden dabei die Herstellervorgaben für die jeweiligen IT-Systeme oder Anwendungen beachtet und in einem angemessenen Rahmen angewendet.

Es wird in geeigneten Intervallen stichpunktartig überprüft, ob die Protokollierung noch korrekt funktioniert. Die Intervalle werden an die betrachteten Zielobjekte und den Schutzbedarf der Informationen angepasst und dokumentiert.

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

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

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. Zum Zwecke einer übergreifenden Auswertung von Ereignissen muss die Zeit-Synchronisation mit den etablierten und freigegebenen Zeitquellen der <Institution> erfolgen.

Zur Vermeidung von fehlerhaften Zeitstempel muss die Erkennung eines FalseTickers durch die NTP-Infrastruktur sichergestellt sein. Dies bedeutet, es sollten mindestens drei Zeit-Instanzen pro Stratum-Hierarchie im Netz positioniert und betrieben werden.

### Einhaltung rechtlicher Rahmenbedingungen (OPS.1.1.5.A5)

Bei der Protokollierung werden die gesetzlichen Bestimmungen aus den aktuellen Gesetzen eingehalten. Dazu zählen unter anderem die gesetzlichen Anforderungen der EU-DSGVO und des BDSG-neu. Die Protokollierungsdaten werden unter Berücksichtigung der Verwendungszwecke nach einem festgelegten Aufbewahrungsprozess gelöscht.

Seitens der <Institution> wird technisch unterbunden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.

Um auf Sicherheitsvorfälle angemessen und zeitnah reagieren zu können sind die Logdateien durch ein Security Information und Event Management (SIEM) automatisiert auszuwerten. Die Basis dafür bildet das eingesetzte Log Management System im SIEM. Das SIEM sollte die Möglichkeit bieten, Log Informationen zu Sicherheitsvorfällen in eine weitere Datenbank zu kopieren. Die Vorgaben des SIEM und der Sicherheitsrichtlinie Protokollierung sind unter anderem in den Prozessen Forensik, Audit, Revision, Zugriff, Sicherheitsvorfallsbehandlung zu berücksichtigen.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

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

Alle gesammelten sicherheitsrelevanten Protokollierungsdaten sollten an einer zentralen Stelle gespeichert werden. Dafür sollte eine zentrale Protokollierungsinfrastruktur im Sinne eines Logserver-Verbunds genutzt und in einem hierfür eingerichteten Netzsegment (Sicherheitsbereich/Sicherheitszonen) etabliert werden. Auf Basis des Need-to-know-Prinzips ist der Zugriff auf die Logdateien ist nur berechtigten und autorisierten Mitarbeitenden gestattet.

Der Logserver-Verbund bezieht die Protokollierungsdaten von IT-Systemen und Anwendungen ausschließlich nach dem Pull-Verfahren. Wird dies von IT-Systemen und Anwendungen nicht unterstützt, werden die Protokollierungsdaten auf vorgelagerten IT-Systemen gesammelt und dort vom Logserver-Verbund abgeholt. Die hierfür erforderlichen Kommunikationsverbindungen erfolgen restriktiv. Um sicherzustellen zu können, dass unberechtigte Dritte durch Manipulation der Kommunikationssysteme oder Verbindungen auf die Log-Dateien unbemerkt zugreifen können, wird die Kommunikation verschlüsselt.

Zusätzlich zu sicherheitsrelevanten Ereignissen protokolliert die zentrale Protokollierungsinfrastruktur auch allgemeine Betriebsereignisse, die auf einen Fehler hindeuten. Zum Beispiel das Ausbleiben von Protokollierungsdaten beziehungsweise die Nichterreichbarkeit eines protokollierenden IT-Systems und Betriebsereignisse, die auf eine außergewöhnliche Auslastung oder Beanspruchung einzelner Dienste hindeuten.

Die Protokollierungsinfrastruktur ist ausreichend dimensioniert, sodass eine Skalierung im Sinne einer erweiterten Protokollierung berücksichtigt werden kann. Dafür werden genügen technische, finanzielle und personelle Ressourcen zur Verfügung gestellt. Falls die Protokollierungsinfrastruktur extern aufgebaut und betrieben werden soll, ist ein spezialisierter Dienstleister zu beauftragen.

### Sichere Administration von Protokollierungsservern (OPS.1.1.5.A7)

Der Logserver-Verbund wird ausschließlich über ein separates Managementnetz administriert. Für die Administrationszugriffe liegt ein Berechtigungskonzept vor. Es können nur Administratoren auf die Protokollierungsserver zugreifen, die speziell dafür verantwortlich sind.

### Archivierung von Protokollierungsdaten (OPS.1.1.5.A8)

Für die Speicherung und Sicherung von Protokollierungsdaten sollte ein Konzept erstellt werden. Dabei sind die gesetzlich vorgeschriebenen Regelungen zu berücksichtigen und im Konzept zu dokumentieren. Die Protokollierungsdaten sollten in unveränderter Originalform aufbewahrt werden.

Die Log-Dateien werden bis zu 7 Tage im Original auf dem lokalen System gespeichert und zusätzlich für einen schnellen Zugriff bis zu 90 Tage zentralisiert bereitgestellt. Nach 90 Tagen sollten die Log-Dateien archiviert und nach maximal 160 Tagen sicher gelöscht werden.

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

Die gesammelten Protokollierungsdaten werden mithilfe einer Protokollierungsanwendung gefiltert, normalisiert, aggregiert und korreliert. Die so bearbeiteten Protokollierungsdaten werden geeignet verfügbar gemacht, damit sie ausgewertet werden können. Damit sich die Daten automatisiert auswerten lassen, verfügt die Protokollanwendungen über entsprechende Schnittstellen für die Auswertungsprogramme. Es ist sichergestellt, dass bei der Auswertung die Bestimmungen der Sicherheitsrichtlinie "Protokollierung" eingehalten werden. Auch wenn die Daten bereitgestellt werden, werden betriebliche und interne Vereinbarungen berücksichtigt. Die Protokollierungsdaten werden entsprechend Kapitel „Archivierung von Protokollierungsdaten“ aufbewahrt.

### Zugriffsschutz für Protokollierungsdaten (OPS.1.1.5.A10)

Alle Protokollierungsdaten sind so zu speichern, dass keine Unbefugten darauf zugreifen können. Über das Zugriffskonzept ist zu regeln, wer auf welche protokollierten Daten zugreifen darf und wie Interessenkonflikte vermieden werden. Dabei sind die Berechtigungen so restriktiv wie möglich zu vergeben.

Es ist sicherzustellen, dass auf die Protokollierungsdaten grundsätzlich nur bei berechtigtem fachlichem Bedarf zugegriffen wird. Zum Beispiel, wenn sicherheitsrelevante Vorfälle aufzuklären sind. Jeder Zugriff auf die Log-Dateien ist zu dokumentieren.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Steigerung des Protokollierungsumfangs (OPS.1.1.5.A11 - CA)

Bei erhöhtem Schutzbedarf von Anwendungen oder IT-Systemen wird die Menge und Art der protokollierten Ereignisse erweitert, sodass sicherheitsrelevante Vorfälle möglichst lückenlos und historisiert nachvollziehbar sind.

Um eine Echtzeitauswertung der Protokollierungsdaten zu ermöglichen, werden in verkürzten Zeitabständen die Protokollierungsdaten von den protokollierenden IT-Systemen und Anwendungen zentral gespeichert. Die Protokollierung ermöglicht eine Auswertung über die gesamten Infrastrukturen der <Institution>.

Anwendungen und IT-Systeme, mit denen eine zentrale Protokollierung nicht möglich ist, werden bei einem erhöhten Schutzbedarf nicht eingesetzt.

### Verschlüsselung der Protokollierungsdaten (OPS.1.1.5.A12 - CIA)

Um Protokollierungsdaten sicher übertragen zu können, sind diese zu verschlüsseln oder durch einen kryptographischen Tunnel zu übertragen. Weiterhin sollten alle gespeicherten Protokolle digital signiert werden. Auch archivierte und außerhalb der Protokollierungsinfrastruktur gespeicherte Protokollierungsdaten sollten immer verschlüsselt gespeichert werden.

### Hochverfügbare Protokollierungssysteme (OPS.1.1.5.A13 - A)

Bei erhöhtem Schutzbedarf sollte eine hochverfügbare Geo-redundante Protokollierungsinfrastruktur aufgebaut werden.