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

Sicherheitsrichtlinie "Detektion von sicherheitsrelevanten Ereignissen"

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 Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300020 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [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](#_Toc79910372)

[Dokumentenhistorie 3](#_Toc79910373)

[Inhaltsverzeichnis 4](#_Toc79910374)

[Allgemeine Festlegungen 5](#_Toc79910375)

[Ziel / Zweck 5](#_Toc79910376)

[Geltungsbereich 5](#_Toc79910377)

[Zuständigkeiten 6](#_Toc79910378)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79910379)

[Aufbau des Dokuments 6](#_Toc79910380)

[Sicherheitsrichtlinie „Detektion von sicherheitsrelevanten Ereignissen" 7](#_Toc79910381)

[Basismaßnahmen 7](#_Toc79910382)

[Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokolldaten (DER.1.A2) 7](#_Toc79910383)

[Festlegung von Meldewegen für sicherheitsrelevante Ereignisse (DER.1.A3) 7](#_Toc79910384)

[Sensibilisierung der Mitarbeiter (DER.1.A4) 7](#_Toc79910385)

[Einsatz von mitgelieferten Systemfunktionen zur Detektion (DER.1.A5) 7](#_Toc79910386)

[Standardmaßnahmen 8](#_Toc79910387)

[Kontinuierliche Überwachung und Auswertung von Protokolldaten (DER.1.A6) 8](#_Toc79910388)

[Schulung von Verantwortlichen (DER.1.A7) 8](#_Toc79910389)

[Festlegung von zu schützenden Segmenten (DER.1.A8) 8](#_Toc79910390)

[Einsatz zusätzlicher Detektionssysteme (DER.1.A9) 8](#_Toc79910391)

[Einsatz von TLS/SSH-Proxies (DER.1.A10) 8](#_Toc79910392)

[Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse (DER.1.A11) 9](#_Toc79910393)

[Auswertung von Informationen aus externen Quellen (DER.1.A12) 9](#_Toc79910394)

[Regelmäßige Audits der Detektionssysteme (DER.1.A13) 9](#_Toc79910395)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc79910396)

[Auswertung der Protokolldaten durch spezialisiertes Personal (DER.1.A14 - CI) 10](#_Toc79910397)

[Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen (DER.1.A15 - CIA) 10](#_Toc79910398)

[Zentrale Detektion und Echtzeitüberprüfung von Flow-Meldungen (DER.1.bd.A1 - CIA) 10](#_Toc79910399)

[Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen (DER.1.A16 - CIA) 10](#_Toc79910400)

[Automatische Reaktion auf sicherheitsrelevante Ereignisse (DER.1.A17 - CI) 11](#_Toc79910401)

[Durchführung regelmäßiger Integritätskontrollen (DER.1.A18 - CI) 11](#_Toc79910402)

# Allgemeine Festlegungen

## Ziel / Zweck

Um IT-Systeme bzw. IT-Services schützen zu können, müssen sicherheitsrelevante Ereignisse rechtzeitig erkannt und behandelt werden. Dazu ist es notwendig, dass die <Institution> im Vorfeld geeignete organisatorische, personelle und technische Maßnahmen plant, implementiert und regelmäßig übt. Denn wenn auf ein vorgegebenes und erprobtes Verfahren aufgesetzt werden kann, lassen sich Reaktionszeiten verkürzen und vorhandene Prozesse optimieren.

Als sicherheitsrelevantes Ereignis wird ein Ereignis bezeichnet, das sich auf die Sicherheit von Informationen auswirkt und die Vertraulichkeit oder die Integrität oder die Verfügbarkeit oder eine Kombination dieser Werte beeinträchtigen kann. Typische Folgen solcher Ereignisse sind ausgespähte, manipulierte oder zerstörte Informationen. Die Ursachen hierfür sind dabei vielfältig: So spielen unter anderem Malware, veraltete Systeminfrastrukturen oder Innentäter eine Rolle. Angreifer nutzen aber auch oft Zero-Day-Exploits aus. Eine weitere erst zunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APT). Dabei handelt es sich um zielgerichtete Cyber-Angriffe, bei denen sich ein Angreifer dauerhaften Zugriff zum Netz verschafft und diesen auf weitere IT-Systeme und deren Anwendungen ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind oft schwer zu detektieren.

Das vorliegende Dokument definiert verbindliche Vorgaben für die <Institution> zur Detektion von sicherheitsrelevanten Ereignissen und beachtet die Anforderungen des BSI Bausteines DER.1 "Detektion von sicherheitsrelevanten Ereignissen".

## 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 Detektion von sicherheitsrelevanten Ereignissen“ 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 „Detektion von sicherheitsrelevanten Ereignissen"

## Basismaßnahmen

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

### Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokolldaten (DER.1.A2)

Alle gesetzlichen Bestimmungen zum Datenschutz sind bei der Auswertung von Protokolldaten einzuhalten. Ebenfalls sind beim Einsatz von Detektionssystemen die Persönlichkeitsrechte der Mitarbeitenden zu wahren. Es ist sicherzustellen, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden.

### Festlegung von Meldewegen für sicherheitsrelevante Ereignisse (DER.1.A3)

Die Melde- und Alarmierungswege sind festzulegen und zu dokumentieren. Es ist zu definieren, welcher Personenkreis wann zu informieren ist und wie dieser erreicht werden kann. Potentielle Sicherheitsvorfälle sind umgehend über die etablierten Prozesse zu melden.

Die Melde- und Alarmierungswege liegen allen Mitarbeitenden vor. Alle Schritte des Prozesses sind ausführlich beschrieben. Die für die Meldung beziehungsweise Alarmierung relevanten Person sind über ihre Aufgaben informiert. Die eingerichteten Melde- und Alarmierungswege werden regelmäßig geprüft, erprobt und, falls erforderlich, aktualisiert.

### Sensibilisierung der Mitarbeiter (DER.1.A4)

Alle Mitarbeitenden der <Institution> sind entsprechend zu sensibilisieren. Hierzu finden regelmäßige Schulungen statt, in denen gängige und aktuelle Bedrohungen sowie die Vorgehensweisen der Cyberkriminellen aufgezeigt werden.

Die Mitarbeitenden sind dahingehend zu sensibilisieren, dass Sie keine Ereignismeldungen ignorieren oder schließen, sondern die Sicherheitsmeldungen über die etablierten Wege an das Service Desk vom IT-Support und das Sicherheitsmanagement weiterreichen. Jeder Mitarbeitende ist verpflichtet einen von ihm vermuteten bzw. erkannten Sicherheitsvorfall unverzüglich zu melden.

### Einsatz von mitgelieferten Systemfunktionen zur Detektion (DER.1.A5)

Verfügen von der <Institution> eingesetzte IT-Systeme oder Anwendungen über Funktionen, mit denen sich sicherheitsrelevante Ereignisse detektieren lassen, sind diese zu aktivieren und zu benutzen.

Auf allen eingesetzten Komponenten ist die Protokollierung einzuschalten. Liegt ein sicherheitsrelevanter Vorfall vor, sind die Meldungen mindestens lokal auszuwerten. Zusätzlich sind die protokollierten Ereignisse anderer IT-Systeme zu überprüfen. Die gesammelten Meldungen sind in verbindlich festgelegten Zeiträumen stichpunktartig zu kontrollieren.

Es ist zu prüfen, ob zusätzliche Scanner für die Erkennung von Schadcode auf zentralen IT-Systemen installiert werden muss. Ist dies der Fall, ist dem Scanner ein zentraler Zugriff zu ermöglichen, die Meldungen und Protokolle sind proaktiv auszuwerten. Die Software und Routinen der Scanner sind regelmäßig zu aktualisieren. Es ist sicherzustellen, dass die Scanner automatisch sicherheitsrelevante Ereignisse an IT-Operation und das Sicherheitsmanagement meldet. Seitens des Sicherheitsmanagement ist sicherzustellen, dass die Meldungen auch ausgewertet und untersucht werden.

## Standardmaßnahmen

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

### Kontinuierliche Überwachung und Auswertung von Protokolldaten (DER.1.A6)

Es findet eine permanent aktive Überwachung und Auswertung von Protokolldaten statt. Die hierfür verantwortlichen Mitarbeitenden sind benannt. Zu diesem Zweck werden ausreichend personelle Ressourcen und Zeit bereitgestellt. Für die aktive Suche nach eingetretenen sicherheitsrelevanten Ereignissen existieren entsprechende Verfahrensanleitungen.

### Schulung von Verantwortlichen (DER.1.A7)

Alle für die aktive Überwachung und Auswertung von Protokolldaten verantwortlichen Mitarbeitenden erhalten weiterführende Schulungen und Qualifikationen. Werden IT-Komponenten beschafft, wird ebenfalls ein Budget für Schulungen eingeplant und sollte ein kurzes Schulungskonzept erstellt werden.

### Festlegung von zu schützenden Segmenten (DER.1.A8)

Anhand von schematischen Netzplänen ist festzulegen, welche Netzsegmente (Sicherheitsbereiche bzw. Sicherheitszonen) durch zusätzliche Detektionssysteme geschützt werden müssen.

### Einsatz zusätzlicher Detektionssysteme (DER.1.A9)

Um sicherheitsrelevante Ereignisse besser zu erkennen, sollten in die zu schützenden Netzsegemente Netzwerk- und Securityscanner (bspw. der Firma Greenbone und Rapid7) und Sensoren (IDS/IPS) zusätzlich integriert werden. Um netzbasierte Intrusion Detection Systeme (NIDS) sollten mindestens die im Netzplan definierten Übergange zwischen Sicherheitsbereichen ergänzt werden.

### Einsatz von TLS/SSH-Proxies (DER.1.A10)

An den Übergängen zu externen Netzen sollten TLS/SSH-Proxies eingesetzt werden, die die verschlüsselte Verbindung auf dem Proxy terminieren und so unterbrechen und es anschließend ermöglichen, die übertragenen Daten auf Malware zu prüfen. Alle TLS/SSH-Proxies sind vor unbefugten Zugriffen zu schützen. Sicherheitsrelevante Ereignisse auf den TLS/SSH-Proxies sind automatisch zu detektieren. Zur Erfüllung der datenschutzrechtlichen Voraussetzungen sind eine organisatorische Regelung zu etablieren, unter der die Logging-Informationen manuell ausgewertet werden dürfen.

### Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse (DER.1.A11)

Die gesammelten Meldungen (Logging-Informationen, SNMP-Meldungen, Flow-Informationen, etc.) der verwendeten Cloud-Services, IT-Systeme, Anwendungssysteme und Anwendungen sollten auf einer zentralen Protokollinfrastruktur aufbewahrt werden. Die gewonnen Meldungen sind mithilfe eines Tools bzw. Tool-Infrastruktur zentral auszuwerten und für selektive Abrufe bereitzustellen. Um die Daten der unterschiedlichen Quellen korreliert und abgeglichen zu können, müssen alle Meldungen zeitlich synchronisiert sein. Die gesammelten Ereignismeldungen sind regelmäßig auf betriebliche und sicherheitstechnische Auffälligkeiten zu kontrollieren. Für die nachträglich Erkennung von sicherheitsrelevanten Ereignissen, sollten die Signaturen der Detektionssysteme durchgängig aktuell und auf dem gleichen Stand sein.

### Auswertung von Informationen aus externen Quellen (DER.1.A12)

Um neue Erkenntnisse für die <Institution> über sicherheitsrelevante Ereignisse zu gewinnen werden externe Quellen mit herangezogen und ausgewertet. Es wird sichergestellt, dass Meldungen von in die Auswertung involvierten Mitarbeitenden als relevant erkannt und an die richtigen internen Stellen weitergeleitet werden.

Stammen Informationen aus qualifizierten Quellen (z. B. öffentliche CERTs), werden diese Informationen grundsätzlich ausgewertet. Alle eingelieferten Informationen werden hinsichtlich ihrer Relevanz bewertet. Sind die eingelieferten Informationen relevant, wird entsprechend der Sicherheitsvorfallbehandlung unter zur Hilfenahme der hierfür bereitgestellten Dokumentenvorlagen eskaliert.

### Regelmäßige Audits der Detektionssysteme (DER.1.A13)

Die von der <Institution> eingesetzten Detektionssysteme werden regelmäßig auditiert. Es werden die Messgrößen ausgewertet, die beispielsweise anfallen, wenn sicherheitsrelevante Ereignisse aufgenommen, gemeldet und eskaliert werden. Die Ergebnisse der Audits werden dokumentiert und mit dem Soll-Zustand abgeglichen. Abweichungen wird nachgegangen.

## 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).

### Auswertung der Protokolldaten durch spezialisiertes Personal (DER.1.A14 - CI)

Es sollten für die zentrale und übergreifende Auswertung und Überwachung der Protokolldaten hier für spezialisierte Mitarbeitende eingesetzt werden. Diese erhalten spezialisierte weiterführende Schulungen und Qualifikationen.

### Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen (DER.1.A15 - CIA)

Es sollten seitens der <Institution> zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. Zentrale automatisierte Analysen mit Softwaremitteln sollten dazu eingesetzt werden, um alle in den Systemumgebungen anfallenden Ereignisse aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen.

Alle eingelieferten Daten sollten lückenlos in der Protokollverwaltung einsehbar und auswertbar sein. Die tatsächlichen Daten sollten möglichst permanent ausgewertet werden. Werden definierte Schwellwerten überschritten, sollte automatisch alarmiert werden. Durch die Mitarbeitenden der <Institution> sollte sichergestellt werden, dass bei einem Alarm unverzüglich eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. In diesem Zusammenhang sollte auch der betroffene Mitarbeitende und Organisationsbereich sofort informiert werden.

### Zentrale Detektion und Echtzeitüberprüfung von Flow-Meldungen (DER.1.bd.A1 - CIA)

Auf Netzebene sollten Systeme zur Flow-basierten Analyse eingesetzt und proaktiv ausgewertet werden, um das Risiko von unautorisierten Verbindungen oder den Verbreitungsweg von Malware frühzeitig erkennen und nachgelagert analysieren zu können.

Werden definierte Schwellwerten überschritten, sollte automatisch alarmiert werden. Durch die Mitarbeitenden der <Institution> sollte sichergestellt werden, dass bei einem Alarm unverzüglich eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. In diesem Zusammenhang sollte auch der betroffene Mitarbeitende und Organisationsbereich sofort informiert werden.

### Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen (DER.1.A16 - CIA)

Anwendungen mit erhöhtem Schutzbedarf sollten durch zusätzliche Detektionsmaßnahmen geschützt werden. Dafür sollten Detektionssysteme eingesetzt werden, mit denen sich der erhöhte Schutzbedarf technisch auch sicherstellen lässt.

### Automatische Reaktion auf sicherheitsrelevante Ereignisse (DER.1.A17 - CI)

Bei einem sicherheitsrelevanten Ereignis sollten die eingesetzten Detektionssysteme mit automatischen Meldungen reagieren und entsprechende geeignete Schutzmaßnahmen einleiten. Hierbei werden Verfahren eingesetzt, die automatisch mögliche Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen erkennen. Ein automatischer Eingriff in den Datenstrom, um einen möglichen Sicherheitsvorfall zu unterbinden, ist möglich.

### Durchführung regelmäßiger Integritätskontrollen (DER.1.A18 - CI)

Alle Detektionssysteme sollten regelmäßig daraufhin überprüft werden, ob sie noch integer sind. Auch sollten die Benutzerrechte kontrolliert werden. Zusätzlich sollten die Sensoren eine Integritätskontrolle von Dateien durchführen und bei sich ändernden Werten eine automatische Alarmierung auslösen.