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

Sicherheitsrichtlinie "Behandlung von Sicherheitsvorfällen"

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 | ISMS300021 | [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](#_Toc79912965)

[Dokumentenhistorie 3](#_Toc79912966)

[Inhaltsverzeichnis 4](#_Toc79912967)

[Allgemeine Festlegungen 6](#_Toc79912968)

[Ziel / Zweck 6](#_Toc79912969)

[Geltungsbereich 6](#_Toc79912970)

[Zuständigkeiten 7](#_Toc79912971)

[Genehmigungs- und Änderungsverfahren 7](#_Toc79912972)

[Aufbau des Dokuments 7](#_Toc79912973)

[Sicherheitsrichtlinie „Behandlung von Sicherheitsvorfällen" 8](#_Toc79912974)

[Basismaßnahmen 8](#_Toc79912975)

[Definition eines Sicherheitsvorfalls (DER.2.1.A1) 8](#_Toc79912976)

[Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen (DER.2.1.A3) 8](#_Toc79912977)

[Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen (DER.2.1.A4) 8](#_Toc79912978)

[Behebung von Sicherheitsvorfällen (DER.2.1.A5) 8](#_Toc79912979)

[Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen (DER.2.1.A6) 9](#_Toc79912980)

[Standardmaßnahmen 9](#_Toc79912981)

[Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen (DER.2.1.A7) 9](#_Toc79912982)

[Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen (DER.2.1.A8) 10](#_Toc79912983)

[Festlegung von Meldewegen für Sicherheitsvorfälle (DER.2.1.A9) 10](#_Toc79912984)

[Eindämmen der Auswirkung von Sicherheitsvorfällen (DER.2.1.A10) 10](#_Toc79912985)

[Einstufung von Sicherheitsvorfällen (DER.2.1.A11) 11](#_Toc79912986)

[Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung (DER.2.1.A12) 11](#_Toc79912987)

[Einbindung in das Sicherheits- und Notfallmanagement (DER.2.1.A13) 11](#_Toc79912988)

[Eskalationsstrategie für Sicherheitsvorfälle (DER.2.1.A14) 11](#_Toc79912989)

[Schulung der Mitarbeitenden der zentralen Anlaufstelle des IT-Betriebs zur Behandlung von Sicherheitsvorfällen (DER.2.1.A15) 12](#_Toc79912990)

[Dokumentation der Behandlung von Sicherheitsvorfällen (DER.2.1.A16) 12](#_Toc79912991)

[Nachbereitung von Sicherheitsvorfällen (DER.2.1.A17) 12](#_Toc79912992)

[Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen (DER.2.1.A18) 12](#_Toc79912993)

[Maßnahmen bei erhöhtem Schutzbedarf 13](#_Toc79912994)

[Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen (DER.2.1.A19 - CIA) 13](#_Toc79912995)

[Einrichtung einer internen Meldestelle für Sicherheitsvorfälle (DER.2.1.A20 - CIA) 13](#_Toc79912996)

[Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen (DER.2.1.A21 - CIA) 13](#_Toc79912997)

[Überprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen (DER.2.1.A22 - CIA) 14](#_Toc79912998)

# Allgemeine Festlegungen

## Ziel / Zweck

Um Schäden zu begrenzen und um weitere Schäden zu vermeiden, müssen erkannte Sicherheitsvorfälle schnell und effizient bearbeitet werden. Hierfür ist es notwendig innerhalb der <Institution>, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen zu etablieren (Security Incident Handling oder auch Security Incident Response).

Ein Sicherheitsvorfall kann sich extremst auf die <Institution> auswirken und große Schäden und Strafzahlungen nach sich ziehen. Solche Vorfälle sind beispielsweise Fehlkonfigurationen, die dazu führen, dass vertrauliche Informationen offengelegt werden, oder kriminelle Handlungen, wie z. B. das Hacking von Servern, der Diebstahl von vertraulichen Informationen sowie Sabotage oder Erpressung mit IT-Bezug.

Die Ursachen für Sicherheitsvorfälle sind vielfältig: So spielen unter anderem Malware, veraltete Systeminfrastrukturen oder Innentäter eine Rolle. Angreifer nutzen aber auch oft Zero-Day-Exploits aus, also Sicherheitslücken in Programmen, für die es noch keinen Patch gibt. Eine weitere ernstzunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APT).

Außerdem könnten sich Benutzer, Administratoren oder externe Dienstleister falsch verhalten, sodass Systemparameter sicherheitskritisch geändert werden oder sie gegen interne Richtlinien verstoßen. Weiter ist als Ursache denkbar, dass Zugriffsrechte verletzt werden, dass Software und Hardware geändert oder schutzbedürftige Räume und Gebäude unzureichend gesichert werden.

Ziel dieser Sicherheitsrichtlinie ist es, einen systematischen Weg aufzuzeigen, wie ein Konzept zur Behandlung von Sicherheitsvorfällen erstellt werden kann. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines DER.2.1 "Behandlung von Sicherheitsvorfällen" zurückgegriffen.

## 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 Behandlung von Sicherheitsvorfällen“ 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 „Behandlung von Sicherheitsvorfällen"

## Basismaßnahmen

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

### Definition eines Sicherheitsvorfalls (DER.2.1.A1)

Ein Sicherheitsvorfall liegt vor, wenn Prozesse oder Ressourcen nicht wie vorgesehen funktionieren. Das Ausmaß bzw. die Gefährdung eines Sicherheitsvorfalls sind größer, als die einer Störung. Die Eintrittsschwellen basieren auf dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Dienste, IT-Systeme und IT-Anwendungen.

Sicherheitsvorfälle sind so weit wie möglich von Störungen im Tagesbetrieb abzugrenzen. Alle Mitarbeitenden des Service Desk, des IT-Betriebes und IT- und OT-Lösungsarchitekten sind über die Definition eines Sicherheitsvorfalls aufzuklären.

### Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen (DER.2.1.A3)

Bei der Behandlung von Sicherheitsvorfällen sind Verantwortlichkeiten und Ansprechpartner festzulegen. Alle Mitarbeitenden sind über ihre Aufgaben und Kompetenzen zu unterrichten. Es ist zu regeln, wer die mögliche Entscheidung für eine forensische Untersuchung trifft, nach welchen Kriterien diese vorgenommen wird und wann sie erfolgen soll.

Die Ansprechpartner für alle dokumentierten Arten von Sicherheitsvorfällen werden den Mitarbeitenden bekannt gegeben. Die aktuellen Kontaktinformationen liegen in praktikabler Form vor.

### Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen (DER.2.1.A4)

Beim Auftreten eines Sicherheitsvorfalls werden alle betroffenen Stellen sowohl interne als auch externe zeitnah informiert. Es ist zu prüfen, ob der Data Protection Commissioner sowie externe Rechtsunterstützung einbezogen werden müssen. Zusätzlich sind die Meldepflichten für Behörden und Kunden zu berücksichtigen. Die betroffenen Stellen sind zudem über die erforderlichen Maßnahmen zu informieren.

### Behebung von Sicherheitsvorfällen (DER.2.1.A5)

Um einen Sicherheitsvorfall erfolgreich zu beheben, ist der folgende Prozessablauf vom Verantwortlichen einzuhalten:

* Eingrenzung des Problems,
* Finden der Ursache,
* Auswahl erforderlicher Maßnahmen zur Behebung,
* Einholen einer Freigabe zur Umsetzung,
* Beseitigen der Ursache und
* Herstellung eines sicheren Zustandes.

Es ist eine aktuelle Liste von internen und externen Sicherheitsexperten, die bei Sicherheitsvorfällen für Fragen aus den verschiedenen erforderlichen Themenbereichen hinzugezogen werden können, zu führen. Die Kommunikation erfolgt über sichere Kommunikationsverfahren.

### Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen (DER.2.1.A6)

Zur Wiederherstellung des Normalzustandes nach dem Auftreten von Schadenssoftware sind grundsätzlich folgende Maßnahmen erforderlich:

* Betroffene IT-Systeme vom Netz trennen, relevante Protokolldateien sichern,
* Untersuchung von IT-Systemen und Applikationen auf Veränderungen,
* Wiederherstellen von Original Datenträgern oder (nachweisbar nicht vom Sicherheitsvorfall betroffenen) Datensicherungen mit allen sicherheitsrelevanten Konfigurationen und Patches,
* Passwörter ändern, sofern erforderlich,
* Penetrationstests der betroffenen Komponenten durchführen.

Bei der Wiederherstellung der sicheren Betriebsumgebung werden die Benutzer bzw. Kunden in die Anwendungsfunktionstests einbezogen. Nachdem der sichere Zustand wiederhergestellt ist, wird unter anderem die Geschäftsführung der <Institution> in Verbindung mit weiteren relevanten Stellen entsprechend informiert. Ebenfalls sind die Komponenten inklusive der Netzübergänge gezielt zu überwachen, um erneute Angriffsversuche feststellen zu können.

Wird auf externe Dienstleister zurückgegriffen, um Störungen zu beheben, ist zu regeln, welche Informationen über den Sicherheitsvorfall wem zugänglich gemacht werden.

## Standardmaßnahmen

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

### Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen (DER.2.1.A7)

Die Bearbeitung von Sicherheitsvorfällen erfolgt standardisiert. Hierzu wurden Abläufe, Prozesse und Vorgaben für die verschiedenen Sicherheitsvorfälle eindeutig geregelt und geeignet dokumentiert.

Die Vorgehensweise wurde in Kraft gesetzt und innerhalb der <Institution> veröffentlicht. Die dokumentierten Abläufe, Prozesse und Vorgaben werden regelmäßig geprüft und aktualisiert.

### Aufbau von Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen (DER.2.1.A8)

Es ist ein <Informationssicherheitsteam> zur Behandlung von Sicherheitsvorfällen aufzustellen. Das <Informationssicherheitsteam> der <Institution> besteht grundsätzlich aus den Personen, die folgende Rollen wahrnehmen:

* <Informationssicherheitsbeauftragter>
* <Datenschutzbeauftragter>
* <Leiter IT>

In Abwesenheit der genannten Personen übernehmen deren Vertreter. Zu Bearbeitung und Einstufung von Sicherheitsvorfällen kann das <Informationssicherheitsteam> bei Bedarf weitere Personen aus den erforderlichen Fachbereichen hinzuziehen. Der Aufbau des <Informationssicherheitsteam> wird regelmäßig aktualisiert.

### Festlegung von Meldewegen für Sicherheitsvorfälle (DER.2.1.A9)

Ein erkannter oder vermuteter Sicherheitsvorfall ist unverzüglich entsprechend der jeweils passenden Meldewege aufzuzeigen. Die Kommunikation sollte schnell und einfach über verlässliche und vertrauenswürdige Kanäle erfolgen. Alle Anlaufstellen für die Meldung von Störungen oder Sicherheitsvorfällen wurden an alle Mitarbeitenden kommuniziert.

Die Kommunikations- und Kontaktstrategie sollte insbesondere diese Regeln definieren:

* Wer informiert werden muss und darf,
* Wer informiert,
* In welcher Reihenfolge und Tiefe informiert wird,
* Wie die Informationsweitergabe über Sicherheitsvorfälle an Dritte erfolgt.

Es ist sicherzustellen, dass keine unautorisierten Personen Informationen über den Sicherheitsvorfall weitergeben.

### Eindämmen der Auswirkung von Sicherheitsvorfällen (DER.2.1.A10)

Parallel zur Analyse der Ursachen eines Sicherheitsvorfalls ist zu entscheiden, ob es wichtiger ist, den aufgetretenen Schaden einzudämmen oder ihn aufzuklären. Die Abschätzung der Auswirkung eines Sicherheitsvorfalls sollte anhand ausreichender Informationen erfolgen. Für die folgenden Szenarien von Sicherheitsvorfällen sind im Vorfeld Betrachtungen durchzuführen.

* Eindringen in Windows-Systeme
* Eindringen in Unix/Linux-Systeme
* Eindringen in macOS-Systeme
* Malware speziell für Windows-Systeme
* Malware speziell für Smartphones und Tablets
* Wurm-Infektion
* Ransomware
* Phishing
* DOS/DDOS
* Bösartiges Netzwerk-Verhalten
* Website-Defacement
* Erpressung
* Social-Engineering
* Informationsleckage
* Insider-Missbrauch
* Betrug
* Verletzung von Markenrechten

### Einstufung von Sicherheitsvorfällen (DER.2.1.A11)

Zur Einstufung von Sicherheitsvorfällen wird ein einheitliches Verfahren etabliert. Das Einstufungsverfahren werden zwischen dem Sicherheitsmanagement und der Störungs- und Fehlerbehebung (Incident-Management) abgestimmt.

### Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung (DER.2.1.A12)

Die Schnittstellen zwischen Störungs- und Fehlerbehebung, Notfallmanagement und Sicherheitsmanagement sind zu analysieren. Die gemeinsam benutzbaren Ressourcen sind ebenfalls zu identifizieren. Alle beteiligten Mitarbeitenden sind für Belange der Sicherheitsvorfallbehandlung sowie des Notfallmanagements zu sensibilisieren. Das Sicherheitsmanagement besitzt lesenden Zugriff auf eingesetzte Incident-Management-Werkzeuge.

### Einbindung in das Sicherheits- und Notfallmanagement (DER.2.1.A13)

Die Behandlung von Sicherheitsvorfällen ist als Teil des Sicherheitsmanagements in der Leitlinie zur Informationssicherheit erfasst. Die Behandlung von Sicherheitsvorfällen wird eng mit dem Notfallmanagement abgestimmt.

### Eskalationsstrategie für Sicherheitsvorfälle (DER.2.1.A14)

Es ist eine Eskalationsstrategie zu formulieren. Diese ist zwischen den Verantwortlichen für Störungs- und Fehlerbehebung und dem Informationssicherheitsmanagement abzustimmen.

Die Eskalationsstrategie enthält eindeutige Handlungsanweisungen, wer auf welchem Wege bei welcher Art von erkennbaren oder vermuteten Sicherheitsstörungen, in welchem Zeitraum zu involvieren ist. Darüber hinaus ist geregelt, zu welchen Maßnahmen eine Eskalation führt und welche Aktivitäten ausgelöst werden sollen.

Für die festgelegte Eskalationsstrategie werden geeignete Werkzeuge ausgewählt. Diese müssen auch für vertrauliche Informationen geeignet sein. Es wird sichergestellt, dass die Werkzeuge auch während eines Sicherheitsvorfalls bzw. Notfalls verfügbar sind.

Die Eskalationsstrategie wird regelmäßig überprüft und gegebenenfalls aktualisiert. Vorhandene Checklisten (Matching Szenarios) für Störungs- und Fehlerbehebung werden regelmäßig um sicherheitsrelevante Themen ergänzt bzw. aktualisiert. Die festgelegten Eskalationswege sollten im Rahmen von Übungen erprobt werden.

### Schulung der Mitarbeitenden der zentralen Anlaufstelle des IT-Betriebs zur Behandlung von Sicherheitsvorfällen (DER.2.1.A15)

Es werden regelmäßige Schulungen für die Behandlung von Sicherheitsvorfällen für die Mitarbeitenden des Service Desk und des IT-Betriebes durchgeführt. Den Mitarbeitenden werden geeignete Hilfsmittel zur Verfügung gestellt, damit sie solche Vorfälle erkennen können. Zum Umgang mit den Hilfsmitteln werden ebenfalls ausreichende Schulungen durchgeführt. Die Mitarbeitenden des Service Desk und des IT-Betriebes werden auf den Schutzbedarf der betroffenen Systeme hingewiesen. Die Checklisten des Service Desk beinhalten auch Fragen, um Sicherheitsvorfälle identifizieren zu können.

### Dokumentation der Behandlung von Sicherheitsvorfällen (DER.2.1.A16)

Alle durchgeführten Aktionen sind möglichst zeitnah detailliert und nach einem standardisierten Verfahren zu dokumentieren. Es werden sowohl alle durchgeführten Aktionen inklusive der Zeitpunkte, als auch die Protokolldaten der betroffenen Komponenten dokumentiert. Dabei ist die Vertraulichkeit bei der Dokumentation und Archivierung der Berichte zu gewährleisten.

Bevor die Störung als beendet und als abgeschlossen markiert wird, sind die benötigten Informationen in die jeweiligen Dokumentationssysteme einzutragen. Hierfür wurden die erforderlichen Qualitätssicherungsanforderungen im Vorfeld mit dem Sicherheitsmanagement definiert.

### Nachbereitung von Sicherheitsvorfällen (DER.2.1.A17)

Sicherheitsvorfälle sind standardisiert nachzubereiten. Dabei ist zu untersuchen,

* Wie schnell Sicherheitsvorfälle erkannt und behoben wurden,
* Ob die Meldewege funktionierten,
* Ausreichend Informationen für die Bewertung verfügbar waren und
* Ob die Detektionsmaßnahmen wirksam waren.

Es ist zu prüfen, ob die ergriffenen Maßnahmen und Aktivitäten wirksam und effizient waren.

Sollten Erfahrungen aus vergangenen Sicherheitsfällen existieren, sind diese für die Erstellung von Handlungsanweisungen für vergleichbare Sicherheitsvorfälle zu nutzen. Diese Handlungsanweisungen sind den relevanten Personengruppen bekannt zu geben und auf Basis neuer Erkenntnisse regelmäßig zu aktualisieren.

Die Geschäftsführung wird jährlich über die Sicherheitsvorfälle unterrichtet. Bei sofortigem Handlungsbedarf erfolgt die Unterrichtung umgehend.

### Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen (DER.2.1.A18)

Die Reaktionen auf Sicherheitsvorfälle werden analysiert und daraufhin untersucht, ob die Prozesse und Abläufe geändert oder weiterentwickelt werden müssen. Erfahrungsberichte von denen in die Reaktionen auf Sicherheitsvorfälle involvierten als auch den zuständigen Beteiligten sind zu erfassen.

Es ist kontinuierlich zu prüfen, ob neue Entwicklungen im Incident Management und in der Forensik existieren und in die jeweiligen Dokumente und in die Abläufe eingebracht werden können.

Werden Hilfsmittel und Checklisten eingesetzt, wird geprüft, ob diese um erforderliche relevante Fragestellungen und Informationen zu erweitern sind.

## 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).

### Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen (DER.2.1.A19 - CIA)

Um die Ursachen von Sicherheitsvorfällen und die entstandenen Schäden effizient und in einer sinnvollen Reihenfolge beheben zu können, wurden die Prioritäten vorab festgelegt. Diese werden regelmäßig aktualisiert. Dabei ist die vorgenommene Einstufung von Sicherheitsvorfällen zu berücksichtigen.

Die Prioritäten wurden von der Geschäftsführung in Zusammenarbeit mit dem Informationssicherheitsbeauftragten genehmigt und in Kraft gesetzt. Die Prioritäten wurden allen Leitungsebenen bekannt gegeben, die in die Behandlung von Sicherheitsvorfällen involviert sind.

### Einrichtung einer internen Meldestelle für Sicherheitsvorfälle (DER.2.1.A20 - CIA)

Interne Meldungen von Sicherheitsvorfällen sind dem Service Desk zu melden. Die Erreichbarkeit des Service Desk wird zu den üblichen Arbeitszeiten gewährleistet. Die Mitarbeitenden des Service Desk sind ausreichend geschult und für die Belange der Informationssicherheit sensibilisiert.

Alle Informationen über Sicherheitsvorfälle werden vertraulich behandelt.

### Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen (DER.2.1.A21 - CIA)

Um Sicherheitsvorfälle durch den gesamten Lebenszyklus des Sicherheitsvorfallbehandlungsprozesses kompetent begleiten zu können, ist hierfür ein Team mit erfahrenen und vertrauenswürdigen Spezialisten zusammen zu stellen. Neben dem technischen Verständnis der Teammitglieder ist auch der Besitz von Kompetenzen in der Kommunikationsfähigkeit sicherzustellen. Die Vertrauenswürdigkeit der Mitglieder des Expertenteams ist zu überprüfen. Der Aufbau des Expertenteams wird regelmäßig aktualisiert.

Die Mitglieder des Expertenteams werden in die Eskalations- und Meldewege eingebunden. Das Expertenteam wird für die Analyse von Sicherheitsvorfällen an den eingesetzten Systemen geschult. Es erfolgt eine regelmäßige Weiterbildung des Expertenteams, sowohl zu den eingesetzten Systemen als auch zu Detektion und Reaktion auf Sicherheitsvorfälle.

Um Sicherheitsvorfälle schnell und diskret behandeln zu können, werden dem Expertenteam alle vorhandenen Dokumentationen sowie finanzielle und technische Ressourcen zur Verfügung gestellt. Das Expertenteam wird in geeigneter Weise in den Organisationsstrukturen berücksichtigt und in diese integriert. Die Verantwortlichkeiten des Expertenteams wurden mit denen des <Informationssicherheitsteam> abgestimmt.

### Überprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen (DER.2.1.A22 - CIA)

Das Managementsystem zur Behandlung von Sicherheitsvorfällen wird regelmäßig auf Aktualität und Wirksamkeit überprüft. Hierfür sollten sowohl angekündigte als auch nicht angekündigte Übungen durchgeführt werden. Die Übungen sind vorher mit der Geschäftsführung abzustimmen. Es werden die Messgrößen ausgewertet, die beispielsweise anfallen, wenn Sicherheitsvorfälle aufgenommen, gemeldet und eskaliert werden. Außerdem werden Planspiele zur Behandlung von Sicherheitsvorfällen durchgeführt, um die notwendige Praxis zu fördern.