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

Sicherheitsrichtlinie "IT-Forensik und Bereinigung 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 Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300022 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "IT-Forensik und Bereinigung von Sicherheitsvorfällen" | [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](#_Toc79942309)

[Dokumentenhistorie 3](#_Toc79942310)

[Inhaltsverzeichnis 4](#_Toc79942311)

[Allgemeine Festlegungen 5](#_Toc79942312)

[Ziel / Zweck 5](#_Toc79942313)

[Geltungsbereich 6](#_Toc79942314)

[Zuständigkeiten 6](#_Toc79942315)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79942316)

[Aufbau des Dokuments 7](#_Toc79942317)

[Sicherheitsrichtlinie „IT-Forensik und Bereinigung von Sicherheitsvorfällen" 8](#_Toc79942318)

[Basismaßnahmen 8](#_Toc79942319)

[Vorsorge für die IT-Forensik 8](#_Toc79942320)

[Bereinigung weitreichender Sicherheitsvorfälle 8](#_Toc79942321)

[Standardmaßnahmen 10](#_Toc79942322)

[Vorsorge für die IT-Forensik 10](#_Toc79942323)

[Bereinigung weitreichender Sicherheitsvorfälle 12](#_Toc79942324)

[Maßnahmen bei erhöhtem Schutzbedarf 12](#_Toc79942325)

[Vorsorge für die IT-Forensik 12](#_Toc79942326)

[Bereinigung weitreichender Sicherheitsvorfälle 13](#_Toc79942327)

# Allgemeine Festlegungen

## Ziel / Zweck

**Vorsorge für die IT-Forensik**

IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Datennetzen zur Aufklärung von Sicherheitsvorfällen in IT-Systemen. Erkannte IT-Sicherheitsvorfälle forensisch zu untersuchen (Live-Response bzw. Post-Mortem-Analyse), ist immer dann notwendig, wenn entstandene Schäden bestimmt, Angriffe abgewehrt, zukünftige Angriffe vermieden und Angreifer identifiziert werden sollen. Ob ein IT-Sicherheitsvorfall forensisch untersucht wird, entscheidet sich, während der bestätigte Vorfall behandelt wird. Eine IT-forensische Untersuchung im Sinne dieser Sicherheitsrichtlinie besteht aus den folgenden Phasen:

* Strategische Vorbereitung
* Initialisierung
* Spurensicherung
* Analyse
* Ergebnisdarstellung

**Bereinigung weitreichender Sicherheitsvorfälle**

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf die <Institution> sowie Einrichtungen. Dabei verschafft sich ein Angreifer dauerhaften Zugriff zu einem Netz und weitet diesen Zugriff auf weitere IT-Systeme aus. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und umfassende technische Fähigkeiten auf Seiten der Angreifer aus. Angriffe dieser Art sind in der Regel schwierig zu detektieren.

Nachdem ein APT-Angriff entdeckt wurde, stehen die Verantwortlichen in der <Institution> vor großen Herausforderungen. Denn die Verantwortlichen müssen eine Bereinigung durchführen, die über das übliche Vorgehen zur Behandlung von IT-Sicherheitsvorfällen hinausgeht. Es ist davon auszugehen, dass die entdeckten Angreifer bereits seit längerer Zeit auf die betroffene IT-Infrastruktur der Office-IT und/oder der SaaS-Lösung zugreifen können. Außerdem nutzen sie komplexe Angriffswerkzeuge, um die Standard-Sicherheitsmechanismen zu umgehen und diverse Hintertüren zu etablieren. Zudem besteht die Gefahr, dass die Angreifer die infizierte Umgebung genau beobachten und auf Versuche zur Bereinigung reagieren, indem sie ihre Spuren verwischen und die Untersuchung sabotieren.

In dieser Sicherheitsrichtlinie wird von einer hohen Bedrohungslage durch einen gezielten Angriff hochmotivierter Täter mit überdurchschnittlichen Ressourcen ausgegangen. Grundsätzlich sollte bei einem solchen Vorfall immer auch ein (zertifizierter) Forensik-Dienstleister hinzugezogen werden. Forensik-Dienstleister sollten dabei bereits in der Phase der forensischen Analyse mit einbezogen werden. Der Forensik-Dienstleister sollte jedoch auch bei der Bereinigung zumindest beratend einbezogen werden.

Diese Sicherheitsrichtlinie zeigt auf, welche Vorsorgemaßnahmen notwendig sind, um IT-forensische Untersuchungen zu ermöglichen. Dabei wird vor allem darauf eingegangen, wie die Spurensicherung vorbereitet und durchgeführt werden kann. Führen Forensik-Dienstleister Spurensicherungen ganz oder teilweise durch, gelten diese Anforderungen auch für die Dienstleister. Durch vertragliche Vereinbarungen und Prüfungen ist dabei sicherzustellen, dass sich der Dienstleister auch daranhält. Ebenfalls beschreibt diese Sicherheitsrichtlinie, wie die <Institution> vorgehen sollten, um nach einem APT-Angriff die IT-Systeme zu bereinigen und den regulären und sicheren Betriebszustand der Office-IT und SaaS-Lösungen wiederherzustellen. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben der BSI Bausteine DER.2.2 "Vorsorge für die IT-Forensik" und DER.2.3 "Bereinigung weitreichender Sicherheitsvorfälle"" 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

Die Sicherheitsrichtlinie „IT-Forensik und Bereinigung 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 „IT-Forensik und Bereinigung von Sicherheitsvorfällen"

## Basismaßnahmen

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

### Vorsorge für die IT-Forensik

#### Prüfung rechtlicher und regulatorischer Rahmenbedingungen zur Erfassung und Auswertbarkeit (DER.2.2.A1)

Die <Institution> gewährleistet, dass sie alle rechtlichen und regulatorischen Rahmenbedingungen vor der Erfassung und Auswertung von forensischen Untersuchungen identifiziert und einhält. Dabei wird sichergestellt, dass keine Widersprüche gegenüber internen Regelungen und Vereinbarungen mit Mitarbeitenden bestehen. Insofern müssen in Einzelfällen die Interessen der <Institution> mit den Interessen des Mitarbeitenden abgewogen werden. Es wird sichergestellt, dass der <Datenschutzbeauftragte>angemessen involviert ist.

#### Erstellung eines Leitfadens für Erstmaßnahmen bei einem IT-Sicherheitsvorfall (DER.2.2.A2)

Um sicherzustellen, dass nach einem Sicherheitsvorfäll möglichst wenig forensische Spuren vernichtet werden, werden in einem Leitfaden Erstmaßnahmen beschrieben, die für die unterschiedlichen IT-Systeme im Falle eines IT-Sicherheitsvorfalls zu ergreifen sind. Der Leitfaden beschreibt dabei ebenso Handlungen, die potentielle Spuren vernichten und wie diese verhindert werden können.

#### Vorauswahl von Forensik-Dienstleistern (DER.2.2.A3)

Sofern die <Institution> über kein eigenes Forensik-Team verfügt, wird bereits in der Vorbereitungsphase gewährleistet, dass ein angemessener Forensik-Dienstleister identifiziert wird. Dies kann durch einen Rahmenvertrag oder durch eine Versicherung oder durch die Rückstellung eins Budgets für Forensik für Einzelbeauftragungen mit zuvor identifizierten Partnern realisiert werden. In diesem Zusammenhang dokumentiert die <Institution> jegliche Dienstleister, die für die Beauftragung in Frage kommen.

### Bereinigung weitreichender Sicherheitsvorfälle

#### Einrichtung eines Leitungsgremiums (DER.2.3.A1)

Zur Bereinigung von APT-Vorfällen („Advanced Persistent Threats“, zu Deutsch „fortgeschrittene, andauernde Bedrohung“) richtet die <Institution> ein Leitungsgremium ein, das alle notwendigen Aktivitäten plant, koordiniert und überwacht. Dabei wird sichergestellt, dass dem Gremium angemessene Weisungsbefugnisse zur Erfüllung ihrer Aufgaben eingeräumt werden.

Insofern ein solches Gremium bereits eingerichtet wurde, als APT-Vorfälle erkannt und klassifiziert wurden, plant und leitet das entsprechende Gremium die Bereinigung des APT-Vorfalls. Sollte ein zusätzlicher Forensik-Dienstleister in die Analyse von APT-Vorfällen involviert sein, wird dieser ebenso in die Bereinigung des Vorfalls einbezogen.

Falls das IT-System zu stark kompromittiert ist oder umfangreiche Bereinigungsmaßnahmen notwendig sind, überprüft die <Institution>, ob zur Behebung ein Krisenstab eingerichtet werden muss. Sofern ein Krisenstab eingeführt wird, überwacht das Leitungsgremium die Bereinigungsmaßnahmen und berichtet die Ergebnisse an den Krisenstab.

#### Entscheidung für eine Bereinigungsstrategie (DER.2.3.A2)

Vor der Durchführung von jeglichen Bereinigungsmaßnahmen definiert das Leitungsgremium eine Bereinigungsstrategie. Innerhalb der Bereinigungsstrategie wird entschieden, ob die Malware vom IT-System entfernt werden kann, das IT-System neu installiert wird oder ob das IT-System inklusive Hardware vollständig ausgetauscht werden muss. Die Bereinigungsstrategie legt außerdem fest, welche IT-Systeme bereinigt werden. Die <Institution> gewährleistet, dass alle Entscheidungen einer Bereinigungsstrategie auf Basis einer zuvor durchgeführten forensischen Untersuchung erfolgen.

Grundsätzlich werden die betroffenen IT-Systeme neu installiert und anschließend gemäß der Reihenfolge der Wiederanlaufpläne mit einer Datensicherung bespielt. Dabei wird vor der Einspielung der Datensicherung durch forensische Untersuchungen sichergestellt, dass hierdurch keine manipulierten Daten oder Programme auf das IT-System übertragen werden.

Insofern IT-Systeme nicht neu installiert werden, setzt die <Institution> eine gezielte APT-Bereinigung um. Um das Risiko übersehener Hintertüren zu minimieren, wird das IT-System auf potenzielle Kommunikation mit dem Angreifer überwacht.

#### Isolierung der betroffenen Netzabschnitte (DER.2.3.A3)

Netzabschnitte, die von einem APT-Vorfall betroffen sind, werden im Rahmen der Bereinigung vollständig vom Netzwerk und insbesondere dem Internet isoliert (Cut-Off). Um dem Angreifer effektiv auszusperren und ihm die Möglichkeit zu nehmen, weitere IT-Systeme anzugreifen oder potenzielle forensische Spuren zu verwischen, werden die betroffenen Netzabschnitte gleichzeitig isoliert.

Die Auswahl der zu isolierenden Netzabschnitte ergibt sich aus einer zuvor durchgeführten forensischen Analyse. Dabei werden sämtliche betroffene Abschnitte identifiziert. Falls die Identifizierung nicht gewährleistet werden kann, werden alle verdächtigen sowie theoretisch infizierten Netzabschnitte isoliert.

Um die Netzabschnitte möglichst vollständig zu isolieren, werden jegliche lokalen Netz- und Internetanschlüsse in Subnetzen erfasst und mitberücksichtigt.

#### Sperrung und Änderung von Zugangsdaten und kryptografischen Schlüsseln (DER.2.3.A4)

Die <Institution> geht für jedes kompromittierte IT-System davon aus, dass sich der Angreifer die entsprechenden Zugangsdaten angeeignet hat und ändert diese nach der Isolierung des Netzes. Zusätzlich werden alle zentral verwalteten Zugangsdaten, die in einem Microsoft Azure AD oder einem Lightweight Directory Access Protocol (LDAP) benutzt wurden, zurückgesetzt.

Insofern der zentrale Authentisierungsserver kompromittiert wurde, werden sämtliche Zugänge gesperrt und die dazugehörigen Passwörter geändert. Die Änderung wird dabei durch erfahrene Administratoren mit der etwaigen Unterstützung von internen oder externen Experten für Forensik umgesetzt.

Insofern TLS-Schlüssel oder eine interne Certification Authority (CA) durch den APT-Angriff kompromittiert wurden, werden die entsprechenden Schlüssel und Infrastrukturen neu erzeugt und verteilt. Die <Institution> stellt über angemessene Maßnahmen sicher, dass kompromittierte Schlüssel zuverlässig gesperrt werden.

#### Schließen des initialen Einbruchswegs (DER.2.3.A5)

Insofern die forensischen Untersuchungen ergeben, dass ein Angreifer durch die Ausnutzung einer technischen Schwachstelle in das IT-System eingedrungen ist, wird die entsprechende Schwachstelle geschlossen. Insofern der Angriff jedoch auf Basis von menschlichen oder organisatorischen Fehlhandlungen erfolgte, ergreift die <Institution> organisatorische, personelle oder technische Maßnahmen, um ähnliche APT-Vorfälle in Zukunft zu verhindern.

#### Rückführung in den Produktivbetrieb (DER.2.3.A6)

Nach der erfolgreichen Bereinigung des Netzes werden die IT-Systeme geordnet in den Produktivbetrieb zurückgeführt. IT-Systeme, Programme und Kollaborationswerkzeuge, die zur Identifikation, Analyse und Bereinigung von Angriffen genutzt wurden, werden vor der Produktivnahme entweder entfernt oder angemessen in den Produktivbetrieb überführt. Jegliche Beweismittel oder ausgesonderten IT-Systeme werden entweder sicher gelöscht bzw. vernichtet oder archiviert.

## Standardmaßnahmen

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

### Vorsorge für die IT-Forensik

#### Festlegung von Schnittstellen zum Krisen- und Notfallmanagement (DER.2.2.A4)

Schnittstellen, die sich zwischen dem Krisen- und Notfallmanagement und der Durchführung von IT-forensischen Untersuchung ergeben, werden definiert und dokumentiert. In diesem Zusammenhang wird festgelegt, welche Mitarbeitenden für welche Maßnahmen verantwortlich sind und wie mit ihnen zu kommunizieren ist. Die <Institution> gewährleistet über angemessene Maßnahmen eine entsprechende Erreichbarkeit dieser Ansprechpartner.

#### Erstellung eines Leitfadens für Beweissicherungsmaßnahmen bei IT-Sicherheitsvorfällen (DER.2.2.A5)

Die <Institution> erstellt für spezifische Fälle einen Leitfaden, wie forensische Beweise zu sichern sind und beschreibt darin die Vorgehensweise, einzusetzende technische Werkzeuge, rechtliche Rahmenbedingungen sowie Dokumentationsvorgaben.

#### Schulung des Personals für die Umsetzung der forensischen Sicherung (DER.2.2.A6)

Die <Institution> stellt bei Bedarf durch das Anbieten entsprechender Schulungen sicher, dass alle verantwortlichen Mitarbeitenden die Kompetenzen besitzen, forensische Spuren richtig zu sichern und forensische Werkzeuge korrekt einsetzen zu können.

#### Auswahl von Forensik-Werkzeugen (DER.2.2.A7)

Die <Institution> stellt sicher oder delegiert dies an den beauftragten Dienstleister, dass die zur Sicherung von forensischen Spuren ausgewählten Werkzeuge für diesen Zweck geeignet sind. Vor jedem Einsatz der forensischen Werkzeuge werden diese hinsichtlich ihrer korrekten Funktionalität überprüft. Durch regelmäßige Überprüfung wird sichergestellt, dass forensische Werkzeuge nicht manipuliert wurden. Die Ergebnisse dieser Überprüfung werden im Anschluss dokumentiert.

#### Auswahl und Reihenfolge der zu sichernden Beweismittel (DER.2.2.A8)

Jede forensische Untersuchung beginnt mit der Definition eines konkreten Zieles bzw. Arbeitsauftrages. Anhand des Ziels werden alle notwendigen Datenquelle identifiziert und die Reihenfolge und Vorgehensweise der Erfassung festgelegt. Bei der Festlegung der Reihenfolge wird sichergestellt, dass die Flüchtigkeit der zu sichernden Daten berücksichtigt werden. Die <Institution> bzw. der beauftragte Dienstleister sichert daher flüchtige Daten unverzüglich, ehe es bspw. Festplatten oder Backups sichert.

#### Vorauswahl forensisch relevanter Daten (DER.2.2.A9)

Die <Institution> definiert für sekundäre Datenquellen, wie z.B. Log-Daten oder Traffic-Mitschnitte, gemäß der rechtlichen Rahmenbedingungen Aufbewahrungszeiten und Verfahren um die entsprechenden Daten für forensische Analysen vorhalten zu können.

#### IT-forensische Sicherung von Beweismitteln (DER.2.2.A10)

Bei der Sicherung von Beweismitteln stellt die <Institution> oder ihr beauftragter Dienstleister sicher, dass die kompletten Datenträger forensisch dupliziert werden. Insofern dies nicht möglich ist, da beispielsweise flüchtige Daten im RAM oder SAN-Partitionen vorliegen, werden Methoden zur Duplizierung gewählt, die die Daten so gering wie möglich verändern.

Um die Integrität der Datenträger auch nachträglich nachzuweisen, werden Originaldatenträger versiegelt aufbewahrt. Insofern kryptografische Prüfsummen vorliegen, kann die Integrität von forensischen Kopien oder Originalträgern auch alternativ über diese sichergestellt werden. Zu diesem Zwecke dokumentiert die <Institution> kryptografische Prüfsummen schriftlich und bewahrt diese getrennt und in mehrfacher Kopie auf. Durch den Einsatz angemessener Maßnahmen wird sichergestellt, dass die dokumentierten Prüfsummen nicht verändert werden können. Um sicherzustellen, dass die gesicherten Daten gerichtlich verwendet werden können, bestätigt ein Zeuge, wie die Beweissicherung erfolgte und beglaubigt die erstellten Prüfsummen.

Die <Institution> stellt sicher, dass ausschließlich geschultes Personal oder ein angemessener Forensik-Dienstleister für die forensische Sicherung von Beweismitteln eingesetzt wird.

#### Dokumentation der Beweissicherung (DER.2.2.A11)

Die <Institution> stellt durch angemessene Maßnahmen sicher, dass alle durchgeführten Schritte bei der forensischen Beweissicherung dokumentiert werden. Die Dokumentation stellt lückenlos dar, welche Methoden zur Beweissicherung eingesetzt wurden und wie mit den gesicherten Originalbeweismitteln umgegangen wurde. Der Verantwortliche hält im Rahmen der Dokumentation ebenso fest, aus welchem Grund er sich für die eingesetzte Methode entschieden hat.

#### Sichere Verwahrung von Originaldatenträgern und Beweismitteln (DER.2.2.A12)

Sichergestellte Originaldatenträger werden so gelagert, dass nur ermittelnde und namentlich bekannte Mitarbeitende Zugriff besitzen. Insofern Beweismittel und Originaldatenträger eingelagert werden, wird festgelegt, wie lange diese aufzubewahren sind. Sobald die Aufbewahrungsfrist abgelaufen ist, wird überprüft, ob die Datenträger oder Beweise weiterhin aufbewahrt werden müssen. Falls nicht, werden die Beweismittel sicher gelöscht oder vernichtet und die Originaldatenträger wieder ausgehändigt.

### Bereinigung weitreichender Sicherheitsvorfälle

#### Gezielte Systemhärtung (DER.2.3.A7)

Alle betroffenen IT-Systeme werden nach einem APT-Angriff durch zusätzlichen Härtungsmaßnahmen geschützt. Im Rahmen von forensischen Analysen wird überprüft, ob das IT-System und die Gesamtumgebung noch sicher ist und welche Härtungsmaßnahmen abzuleiten sind.

Sofern die Möglichkeiten gegeben sind, werden bereits während der Bereinigung Härtungsmaßnahmen auf dem IT-System ausgeführt. Alle weiteren Härtungsmaßnahmen, die nicht kurzfristig umgesetzt werden können, werden auf einem Maßnahmenplan dokumentiert und mittelfristig umgesetzt. Der <Informationssicherheitsbeauftragter> der <Institution> gewährleistet die Erstellung, Überprüfung und Umsetzung der Maßnahmenplanung.

#### Etablierung sicherer, unabhängiger Kommunikationskanäle (DER.2.3.A8)

Für die angemessene Kommunikation zwischen dem Leitungsgremium und den beteiligten Mitarbeitenden etabliert die <Institution> einen möglichst sicheren Kommunikationskanal.

## 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).

### Vorsorge für die IT-Forensik

#### Rahmenverträge mit externen Dienstleistern (DER.2.2.A13 - CIA)

Die <Institution> sollte eine Abrufvereinbarungen bzw. Rahmenverträge mit Forensik-Dienstleistern abschließen, damit IT-Sicherheitsvorfälle schneller forensisch untersucht werden können.

#### Festlegung von Standardverfahren für die Beweissicherung (DER.2.2.A14 - CI)

Für Anwendungen, IT-Systeme und IT-Systemverbunde mit hohen Schutzbedarf sowie verbreitete Systemkonfigurationen leitet die <Institution> Standardverfahren ab, die die möglichst vollständige Sicherung von flüchtigen und nichtflüchtigen Daten erlauben.

Diese systemspezifischen Standardverfahren werden durch erprobte und möglichst automatisierte Prozesse realisiert. Darüber hinaus werden die Standardverfahren durch den Einsatz angemessener Werkzeuge wie Checklisten, Softwaretools oder IT-forensischer Hardware wie Schreibblockern unterstützt.

#### Durchführung von Übungen zur Beweissicherung (DER.2.2.A15 - CIA)

Die <Institution> gewährleistet, dass alle, an forensischen Analysen beteiligten Mitarbeitenden regelmäßige Übungen zur Beweissicherung bei IT-Sicherheitsvorfällen wahrnehmen.

### Bereinigung weitreichender Sicherheitsvorfälle

#### Hardwaretausch betroffener IT-Systeme (DER.2.3.A9 - CIA)

Für jedes IT-System mit hohen Schutzbedarf überprüft die <Institution>, ob ein kompletter Austausch nach einem APT-Vorfall durchzuführen ist. Insofern nach einer Bereinigung weiterhin verdächtiges Verhalten auf dem IT-System festgestellt wird, wird das betroffene IT-System in jedem Fall ausgetauscht.

#### Umbauten zur Erschwerung eines erneuten Angriffs durch denselben Angreifer (DER.2.3.A10 - CIA)

Um denselben Angreifer das erneute Durchführen eines APT-Angriffs auf die IT-Systeme zu erschweren, stellt die <Institution> sicher, dass die Netzumgebung bzw. Cloud-Infrastruktur angepasst und angemessene Mechanismen zur Detektion eines wiederkehrenden Angreifers implementiert werden.