



# DER.1 Detektion von sicherheitsrelevanten Ereignissen

## 1. Beschreibung

### 1.1. Einleitung

Um IT-Systeme schützen zu können, müssen sicherheitsrelevante Ereignisse rechtzeitig erkannt und behandelt werden. Dazu ist es notwendig, dass Institutionen im Vorfeld geeignete organisatorische, personelle und technische Maßnahmen planen, implementieren und regelmäßig üben. 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 Informationssicherheit auswirkt und die Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen kann. Typische Folgen solcher Ereignisse sind ausgespähte, manipulierte oder zerstörte Informationen. Die Ursachen dafür sind dabei vielfältig. So spielen unter anderem Malware, veraltete IT-Systeminfrastrukturen oder Innentäter und Innentäterinnen eine Rolle. Angreifende nutzen aber auch oft Zero-Day-Exploits aus, also Sicherheitslücken in Programmen, bevor es für diese einen Patch gibt. Eine weitere ernstzunehmende Gefährdung sind sogenannte Advanced Persistent Threats (APTs). Dabei handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich Angreifende dauerhaften Zugriff zu einem Netz verschaffen und diesen Zugriff in der Folge auf weitere IT-Systeme ausweiten. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifenden aus und sind oft schwer zu detektieren.

### 1.2. Zielsetzung

Dieser Baustein zeigt einen systematischen Weg auf, wie Informationen gesammelt, korreliert und ausgewertet werden können, um sicherheitsrelevante Ereignisse möglichst vollständig und zeitnah zu detektieren. Die aus der Detektion gewonnenen Erkenntnisse sollen die Fähigkeit von Institutionen verbessern, sicherheitsrelevante Ereignisse zu erkennen und angemessen darauf zu reagieren.

### 1.3. Abgrenzung und Modellierung

Der Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* ist auf den Informationsverbund einmal anzuwenden.

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn sicherheitsrelevante Ereignisse detektiert werden sollen. Voraussetzung hierfür ist jedoch, dass umfassend protokolliert wird. Die dafür notwendigen Anforderungen werden nicht im vorliegenden Baustein beschrieben, sondern sind im Baustein OPS.1.1.5 *Protokollierung* enthalten.

Im Vorfeld der Detektion 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.

Außerdem beschreibt der Baustein nicht, wie mit sicherheitsrelevanten Ereignissen umzugehen ist, nachdem sie detektiert worden sind. Anforderungen dazu werden in den Bausteinen DER.2.1 *Behandlung von Sicherheitsvorfällen* und DER.2.2 *Vorsorge für die IT-Forensik* aufgeführt. Ebenso wird nicht auf das Thema Datenschutz eingegangen, dieses wird im Baustein CON.2 *Datenschutz* behandelt.

Um sicherheitsrelevante Ereignisse zu erkennen, sind oft zusätzliche Programme erforderlich, z. B. Antivirenprogramme, Firewalls oder Intrusion Detection /Intrusion Prevention Systeme (IDS/IPS). Sicherheitsaspekte dieser Systeme sind ebenfalls nicht Gegenstand des vorliegenden Bausteins. Sie werden z. B. in den Bausteinen OPS.1.1.4 *Schutz vor Schadprogrammen* bzw. NET.3.2 *Firewall* thematisiert.

## 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 DER.1 *Detektion von sicherheitsrelevanten Ereignissen* von besonderer Bedeutung.

### 2.1. Missachtung von gesetzlichen Vorschriften und betrieblichen Mitbestimmungsrechten

Programme, die sicherheitsrelevante Ereignisse detektieren und Protokolldaten auswerten, sammeln oft viele Informationen über die Netzstruktur und die internen Abläufe einer Institution. Darin können schützenswerte Informationen wie personenbezogene Daten, vertrauliche Daten oder Arbeitsabläufe von Mitarbeitenden enthalten sein. Dadurch, dass solche Daten gespeichert werden, können jedoch Persönlichkeitsrechte bzw. Mitbestimmungsrechte verletzt werden. Auch verstößt die Institution unter bestimmten Voraussetzungen eventuell gegen die jeweiligen Datenschutzgesetze.

### 2.2. Unzureichende Qualifikation der Mitarbeitenden

Im täglichen IT-Betrieb einer Institution können viele Störungen und Fehler auftreten, z. B. könnten ankommende Protokolldaten plötzlich stark zunehmen. Sind die Zuständigen nicht ausreichend sensibilisiert und geschult, kann es passieren, dass sie sicherheitsrelevante Ereignisse nicht als solche identifizieren und so Angriffe unerkannt bleiben. Und auch wenn die Zuständigen ausreichend für die Belange der Informationssicherheit sensibilisiert und geschult sind, kann trotzdem nicht ausgeschlossen werden, dass sie Sicherheitsvorfälle nicht erkennen. Beispiele dafür sind:

- Eine Person, die seit längerer Zeit nicht im lokalen Netz ihrer Institution angemeldet war, stuft es als normal ein, dass ihr Notebook seit einer Woche während des Internetzugangs deutlich langsamer ist. Sie bemerkt nicht, dass ein Schadprogramm im Hintergrund aktiv ist. Sie wurde nicht oder nur unzureichend geschult, bei verdächtigen Auffälligkeiten das Incident Management zu informieren.
- Eine Produktionsleitung bemerkt nicht, dass die Daten in den Produktionssystemen und auch die Steuerungsanzeigesysteme heimlich verändert wurden. Sie schöpft keinen Verdacht, als die SCADA-Steuerung der Produktionsanlage seltsame Werte anzeigt, da dies nur kurzzeitig

erfolgte. Der Vorfall wird nicht gemeldet, da alle Werte wieder den erwarteten Anzeigewerten entsprechen. Dass eine Schadsoftware die Anzeigewerte manipuliert hat, fällt somit niemandem auf.

## 2.3. Fehlerhafte Administration der eingesetzten Detektionssysteme

Fehlerhafte Konfigurationen können dazu führen, dass eingesetzte Detektionssysteme nicht ordnungsgemäß funktionieren. Ist beispielsweise die Alarmierung falsch eingestellt, können vermehrt Fehlalarme auftreten. Die Zuständigen können dann eventuell nicht mehr zwischen einem Fehlalarm und einem sicherheitsrelevanten Ereignis unterscheiden. Auch nehmen sie die Meldungen möglicherweise nicht schnell genug wahr, da zu viele Alarme generiert werden. Dadurch bleiben möglicherweise Angriffe unerkannt. Ebenso steigt der Aufwand stark an, um die Menge der Meldungen auszuwerten.

## 2.4. Fehlende Informationen über den zu schützenden Informationsverbund

Sind keine oder nur ungenügende Informationen über den zu schützenden Informationsverbund vorhanden, kann es passieren, dass wesentliche Bereiche des Informationsverbunds nicht ausreichend durch Detektionssysteme abgesichert werden. Dadurch können Angreifende leicht in das Netz der Institution eindringen und z. B. schützenswerte Informationen abgreifen. Auch ist es ihnen so möglich, lange unbemerkt im System zu bleiben und dauerhaft auf das Netz zuzugreifen.

## 2.5. Unzureichende Nutzung von Detektionssystemen

Wenn keine Detektionssysteme eingesetzt werden und auch die in IT-Systemen und Anwendungen vorhandenen Funktionen zur Detektion von sicherheitsrelevanten Ereignissen nicht benutzt werden, können Angreifende leichter unbemerkt in das Netz der Institution eindringen. Dort könnten sie unbefugt auf sensible Informationen zugreifen. Besonders kritisch ist es, wenn die Übergänge zwischen Netzgrenzen nur unzureichend überwacht werden.

## 2.6. Unzureichende personelle Ressourcen

Ist nicht genügend Personal vorhanden, um Protokolldaten auszuwerten, können sicherheitsrelevante Ereignisse nicht vollständig detektiert werden. So bleiben Angriffe eventuell lange verborgen oder werden erst entdeckt, nachdem z. B. schon sehr viele schützenswerte Informationen abgeflossen sind. Auch wenn durch zu wenig Personal keine externen Informationsquellen ausgewertet werden, bleiben Sicherheitslücken eventuell zu lange offen. Dann können sie ausgenutzt werden, um unerlaubt in die IT-Systeme der Institution einzudringen.

# 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.1 *Detektion von sicherheitsrelevanten Ereignissen* 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	Mitarbeitende, Fachverantwortliche, Benutzende, Vorgesetzte

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.

#### **DER.1.A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen (B)**

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen erstellt werden. In der spezifischen Sicherheitsrichtlinie MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben werden, wie die Detektion von sicherheitsrelevanten Ereignissen geplant, aufgebaut und sicher betrieben werden kann. Die spezifische Sicherheitsrichtlinie MUSS allen im Bereich Detektion zuständigen Mitarbeitenden bekannt und grundlegend für ihre Arbeit sein. Falls die spezifische Sicherheitsrichtlinie verändert wird oder von den Anforderungen abgewichen wird, dann MUSS dies mit dem oder der verantwortlichen ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist. Die Ergebnisse der Überprüfung MÜSSEN sinnvoll dokumentiert werden.

#### **DER.1.A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokollierungsdaten (B)**

Wenn Protokollierungsdaten ausgewertet werden, dann MÜSSEN dabei die Bestimmungen aus den aktuellen Gesetzen zum Bundes- und Landesdatenschutz eingehalten werden. Wenn Detektionssysteme eingesetzt werden, dann MÜSSEN die Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitendenvertretungen gewahrt werden. Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden, z. B. das Telemediengesetz (TMG), das Betriebsverfassungsgesetz und das Telekommunikationsgesetz.

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

Für sicherheitsrelevante Ereignisse MÜSSEN geeignete Melde- und Alarmierungswege festgelegt und dokumentiert werden. Es MUSS bestimmt werden, welche Stellen wann zu informieren sind. Es MUSS aufgeführt sein, wie die jeweiligen Personen erreicht werden können. Je nach Dringlichkeit MUSS ein sicherheitsrelevantes Ereignis über verschiedene Kommunikationswege gemeldet werden.

Alle Personen, die für die Meldung bzw. Alarmierung relevant sind, MÜSSEN über ihre Aufgaben informiert sein. Alle Schritte des Melde- und Alarmierungsprozesses MÜSSEN ausführlich beschrieben sein. Die eingerichteten Melde- und Alarmierungswege SOLLTEN regelmäßig geprüft, erprobt und aktualisiert werden, falls erforderlich.

#### **DER.1.A4 Sensibilisierung der Mitarbeitenden (B) [Vorgesetzte, Benutzende, Mitarbeitende]**

Alle Benutzenden MÜSSEN dahingehend sensibilisiert werden, dass sie Ereignismeldungen ihrer Clients nicht einfach ignorieren oder schließen. Sie MÜSSEN die Meldungen entsprechend der Alarmierungswege an das verantwortliche Incident Management weitergeben (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

Alle Mitarbeitenden MÜSSEN einen von ihnen erkannten Sicherheitsvorfall unverzüglich dem Incident Management melden.

## **DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion (B) [Fachverantwortliche]**

Falls eingesetzte IT-Systeme oder Anwendungen über Funktionen verfügen, mit denen sich sicherheitsrelevante Ereignisse detektieren lassen, dann MÜSSEN diese aktiviert und benutzt werden. Falls ein sicherheitsrelevanter Vorfall vorliegt, dann MÜSSEN die Meldungen der betroffenen IT-Systeme ausgewertet werden. Zusätzlich MÜSSEN die protokollierten Ereignisse anderer IT-Systeme überprüft werden. Auch SOLLTEN die gesammelten Meldungen in verbindlich festgelegten Zeiträumen stichpunktartig kontrolliert werden.

Es MUSS geprüft werden, ob zusätzliche Schadcodescanner auf zentralen IT-Systemen installiert werden sollen. Falls zusätzliche Schadcodescanner eingesetzt werden, dann MÜSSEN diese es über einen zentralen Zugriff ermöglichen, ihre Meldungen und Protokolle auszuwerten. Es MUSS sichergestellt sein, dass die Schadcodescanner sicherheitsrelevante Ereignisse automatisch an die Zuständigen melden. Die Zuständigen MÜSSEN die Meldungen auswerten und untersuchen.

## **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.

### **DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten (S)**

Alle Protokollierungsdaten SOLLTEN möglichst permanent aktiv überwacht und ausgewertet werden. Es SOLLTEN Mitarbeitende benannt werden, die dafür zuständig sind.

Falls die zuständigen Mitarbeitenden aktiv nach sicherheitsrelevanten Ereignissen suchen müssen, z. B. wenn sie IT-Systeme kontrollieren oder testen, dann SOLLTEN solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein.

Für die Detektion von sicherheitsrelevanten Ereignissen SOLLTEN genügend personelle Ressourcen bereitgestellt werden.

### **DER.1.A7 Schulung von Zuständigen (S) [Vorgesetzte]**

Alle Zuständigen, die Ereignismeldungen kontrollieren, SOLLTEN weiterführende Schulungen und Qualifikationen erhalten. Wenn neue IT-Komponenten beschafft werden, SOLLTE ein Budget für Schulungen eingeplant werden. Bevor die Zuständigen Schulungen für neue IT-Komponenten bekommen, SOLLTE ein Schulungskonzept erstellt werden.

### **DER.1.A8 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

### **DER.1.A9 Einsatz zusätzlicher Detektionssysteme (S) [Fachverantwortliche]**

Anhand des Netzplans SOLLTE festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen. Der Informationsverbund SOLLTE um zusätzliche Detektionssysteme und Sensoren ergänzt werden. Schadcodedetektionssysteme SOLLTEN eingesetzt und zentral verwaltet werden. Auch die im Netzplan definierten Übergänge zwischen internen und externen Netzen SOLLTEN um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.

### **DER.1.A10 Einsatz von TLS-/SSL-Proxies (S) [Fachverantwortliche]**

An den Übergängen zu externen Netzen SOLLTEN TLS-/SSL-Proxies eingesetzt werden, welche die verschlüsselte Verbindung unterbrechen und es so ermöglichen, die übertragenen Daten auf Malware zu prüfen. Alle TLS-/SSL-Proxies SOLLTEN vor unbefugten Zugriffen geschützt werden. Auf den TLS-/SSL-Proxies SOLLTEN sicherheitsrelevante Ereignisse automatisch detektiert werden. Es SOLLTE eine

organisatorische Regelung erstellt werden, unter welchen datenschutzrechtlichen Voraussetzungen die Logdaten manuell ausgewertet werden dürfen.

### **DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse (S) [Fachverantwortliche]**

Die auf einer zentralen Protokollinfrastruktur gespeicherten Ereignismeldungen der IT-Systeme und Anwendungen (siehe OPS.1.1.5 *Protokollierung*) SOLLTEN mithilfe eines Tools abgerufen werden können. Mit dem ausgewählten Tool SOLLTEN die Meldungen ausgewertet werden können. Die gesammelten Ereignismeldungen SOLLTEN regelmäßig auf Auffälligkeiten kontrolliert werden. Die Signaturen der Detektionssysteme SOLLTEN immer aktuell und auf dem gleichen Stand sein, damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können.

### **DER.1.A12 Auswertung von Informationen aus externen Quellen (S) [Fachverantwortliche]**

Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, SOLLTEN externe Quellen herangezogen werden. Meldungen über unterschiedliche Kanäle SOLLTEN von den Mitarbeitenden auch als relevant erkannt und an die richtige Stelle weitergeleitet werden. Informationen aus zuverlässigen Quellen SOLLTEN grundsätzlich ausgewertet werden. Alle gelieferten Informationen SOLLTEN danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind. Ist dies der Fall, SOLLTEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.

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

Die vorhandenen Detektionssysteme und getroffenen Maßnahmen SOLLTEN in regelmäßigen Audits daraufhin überprüft werden, ob sie noch aktuell und wirksam sind. Es SOLLTEN die Messgrößen ausgewertet werden, die beispielsweise anfallen, wenn sicherheitsrelevante Ereignisse aufgenommen, gemeldet und eskaliert werden. Die Ergebnisse der Audits SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

## **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.

### **DER.1.A14 Auswertung der Protokollierungsdaten durch spezialisiertes Personal (H)**

Es SOLLTEN Mitarbeitende speziell damit beauftragt werden, alle Protokollierungsdaten zu überwachen. Die Überwachung der Protokollierungsdaten SOLLTE die überwiegende Aufgabe der beauftragten Mitarbeitenden sein. Die beauftragten Mitarbeitenden SOLLTEN spezialisierte weiterführende Schulungen und Qualifikationen erhalten. Ein Personenkreis SOLLTE benannt werden, der ausschließlich für das Thema Auswertung von Protokollierungsdaten verantwortlich ist.

### **DER.1.A15 Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen (H)**

Zentrale Komponenten SOLLTEN eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten. Zentrale, automatisierte Analysen mit Softwaremitteln SOLLTEN eingesetzt werden. Mit diesen zentralen, automatisierten Analysen mit Softwaremitteln SOLLTEN alle in der Systemumgebung anfallenden Ereignisse aufgezeichnet und in Bezug zueinander gesetzt werden. Die sicherheitsrelevanten Vorgänge SOLLTEN sichtbar gemacht werden. Alle eingelieferten Daten SOLLTEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein. Die Daten SOLLTEN

möglichst permanent ausgewertet werden. Werden definierte Schwellwerte überschritten, SOLLTE automatisch alarmiert werden. Das Personal SOLLTE sicherstellen, dass bei einem Alarm unverzüglich eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird. In diesem Zusammenhang SOLLTEN auch die betroffenen Mitarbeitenden sofort informiert werden.

Die Systemverantwortlichen SOLLTEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist. Zusätzlich SOLLTEN bereits überprüfte Daten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.

### **DER.1.A16 Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen (H)**

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

### **DER.1.A17 Automatische Reaktion auf sicherheitsrelevante Ereignisse (H)**

Bei einem sicherheitsrelevanten Ereignis SOLLTEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und mit geeigneten Schutzmaßnahmen reagieren. Hierbei SOLLTEN Verfahren eingesetzt werden, die automatisch mögliche Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen erkennen. Es SOLLTE möglich sein, automatisch in den Datenstrom einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden.

### **DER.1.A18 Durchführung regelmäßiger Integritätskontrollen (H)**

Alle Detektionssysteme SOLLTEN regelmäßig daraufhin überprüft werden, ob sie noch integer sind. Auch SOLLTEN die Berechtigungen der Benutzenden kontrolliert werden. Zusätzlich SOLLTEN die Sensoren eine Integritätskontrolle von Dateien durchführen. Bei sich ändernden Werten SOLLTE eine automatische Alarmierung ausgelöst 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.

Das BSI hat das weiterführende Dokument „BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen, Version 1.0“ zum Themenfeld Intrusion Detection veröffentlicht.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel TS1.5 Intrusion Detection Vorgaben für den Einsatz von Intrusion Detection Systemen.



# DER.2.1 Behandlung von Sicherheitsvorfällen

## 1. Beschreibung

### 1.1. Einleitung

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

Ein Sicherheitsvorfall kann sich stark auf eine Institution auswirken und große Schäden nach sich ziehen. Solche Vorfälle sind beispielsweise Fehlkonfigurationen, die dazu führen, dass vertrauliche Informationen offengelegt werden, oder kriminelle Handlungen, wie z. B. Angriffe auf Server, 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 sowie Innentäter und Innentäterinnen eine Rolle. Angreifende 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 Benutzende, der IT-Betrieb oder externe Dienstleistende 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.

### 1.2. Zielsetzung

Ziel dieses Bausteins ist es, einen systematischen Weg aufzuzeigen, wie ein Konzept zur Behandlung von Sicherheitsvorfällen erstellt werden kann.

### 1.3. Abgrenzung und Modellierung

Der Baustein DER.2.1 *Behandlung von Sicherheitsvorfällen* ist für den Informationsverbund einmal anzuwenden.

Der Fokus dieses Bausteins liegt auf der Behandlung von Sicherheitsvorfällen aus Sicht der Informationstechnik. Bevor Sicherheitsvorfälle behandelt werden können, müssen sie jedoch erkannt



werden. Sicherheitsanforderungen dazu sind im Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* enthalten und werden im vorliegenden Baustein vorausgesetzt. Die Vorsorgemaßnahmen, die notwendig sind, um IT-forensische Untersuchungen zu ermöglichen, sind im Baustein DER.2.2 *Vorsorge für die IT-Forensik* beschrieben. Die Bereinigung nach einem APT-Vorfall ist Thema im Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle*. Ein besonderer Bereich der Behandlung von Sicherheitsvorfällen ist das Notfallmanagement, das im Baustein DER.4 *Notfallmanagement* thematisiert und hier nicht weiter betrachtet wird. Es ist jedoch zu beachten, dass die Entscheidung darüber, ob ein Notfall vorliegt oder nicht, im vorliegenden Baustein getroffen wird.

## 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 DER.2.1 *Behandlung von Sicherheitsvorfällen* von besonderer Bedeutung.

### 2.1. Ungeeigneter Umgang mit Sicherheitsvorfällen

In der Praxis kann nie ausgeschlossen werden, dass Sicherheitsvorfälle auftreten. Das gilt auch dann, wenn viele Sicherheitsmaßnahmen umgesetzt sind. Wird auf akute Sicherheitsvorfälle jedoch nicht oder nicht angemessen reagiert, können daraus große Schäden mit katastrophalen Folgen entstehen. Beispiele hierfür sind:

- In den Protokolldateien einer Firewall finden sich auffällige Einträge. Wird nicht zeitnah untersucht, ob dies erste Anzeichen für einen Einbruchversuch sind, können Angreifende die Firewall mit einem erfolgreichen Angriff unbemerkt überwinden und in das interne Netz der Institution eindringen.
- Es werden Sicherheitslücken in den verwendeten IT-Systemen bzw. Anwendungen bekannt. Beschafft sich die Institution diese Informationen nicht rechtzeitig und leitet sie die notwendigen Gegenmaßnahmen nicht zügig ein, können diese Sicherheitslücken bei einem Angriff ausgenutzt werden.
- Ein Einbruchdiebstahl in einer Filiale wird für einen Fall von Beschaffungskriminalität gehalten, da Notebooks und Flachbildschirme entwendet wurden. Der Tatsache, dass sich auf den Notebooks vertrauliche Informationen und Zugangsdaten für IT-Systeme im Intranet befunden haben, wird keine größere Bedeutung beigemessen. Der oder die Informationssicherheitsbeauftragte (ISB) wird daher nicht informiert. Auf die nachfolgenden Angriffe auf die IT-Systeme anderer Standorte und der Firmenzentrale ist die Institution daher nicht vorbereitet. Für den Angriff wurden die auf den gestohlenen Notebooks gefundenen Daten verwendet.

Wenn für den Umgang mit Sicherheitsvorfällen keine geeignete Vorgehensweise vorgegeben ist, können in Eile und unter Stress falsche Entscheidungen getroffen werden. Diese können z. B. dazu führen, dass die Presse falsch informiert wird. Außerdem könnten Dritte durch die eigenen IT-Systeme geschädigt werden und Schadenersatz fordern. Auch ist es möglich, dass keinerlei Ausweich- oder Wiederherstellungsmaßnahmen vorgesehen sind und sich somit der Schaden für die Institution deutlich erhöht.

### 2.2. Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen

Wenn nach einem Sicherheitsvorfall unvorsichtig oder nicht nach Vorgaben gehandelt wird, kann das dazu führen, dass wichtige Beweisspuren für die Aufklärung oder die spätere juristische Verfolgung unbeabsichtigt zerstört oder nicht gerichtsverwertbar gemacht werden.

Beispiele hierfür sind:

- Auf einem Client wurde bei einem Angriff eine Schadsoftware platziert, deren Arbeitsweise und Ziel nur im laufenden Zustand analysiert werden kann. Dafür müssten Informationen über die aktiven Prozesse und der Inhalt des Hauptspeichers gesichert und ausgewertet werden. Wird der Client nun voreilig heruntergefahren, können die Informationen nicht mehr für eine Analyse und Aufklärung des Sicherheitsvorfalls herangezogen werden.
- Der IT-Betrieb findet auf einem Server einen laufenden Prozess, der eine überdurchschnittliche CPU-Auslastung verursacht. Zusätzlich erzeugt dieser Prozess temporäre Dateien und versendet unbekannte Informationen über das Internet. Wird der Prozess voreilig beendet und werden die temporären Dateien einfach gelöscht, kann nicht herausgefunden werden, ob vertrauliche Informationen entwendet wurden.
- Ein wichtiger Server wird kompromittiert, weil der IT-Betrieb durch die starke Arbeitsbelastung und ein fehlendes Wartungsfenster die letzten Sicherheitsupdates nicht wie geplant einspielen konnte. Um möglichen disziplinarischen Konsequenzen zu entgehen, spielt der IT-Betrieb die fehlenden Updates ein, bevor ein Sicherheitsteam die Einbruchursache und den entstandenen Schaden analysieren kann. Eine mangelhafte Fehlerkultur hat somit eine Analyse des Problems verhindert.

### 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.2.1 *Behandlung von Sicherheitsvorfällen* 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	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	IT-Betrieb, Institutionsleitung, Fachverantwortliche, Datenschutzbeauftragte, Notfallbeauftragte

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.

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

In einer Institution MUSS klar definiert sein, was ein Sicherheitsvorfall ist. Ein Sicherheitsvorfall MUSS so weit wie möglich von Störungen im Tagesbetrieb abgegrenzt sein. Alle an der Behandlung von Sicherheitsvorfällen beteiligten Mitarbeitenden MÜSSEN die Definition eines Sicherheitsvorfalls kennen. Die Definition und die Eintrittsschwellen eines solchen Vorfalls SOLLTEN sich nach dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Systeme bzw. Anwendungen richten.

### **DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen (B)**

Eine Richtlinie zur Behandlung von Sicherheitsvorfällen MUSS erstellt werden. Darin MÜSSEN Zweck und Ziel der Richtlinie definiert sowie alle Aspekte der Behandlung von Sicherheitsvorfällen geregelt werden. So MÜSSEN Verhaltensregeln für die verschiedenen Arten von Sicherheitsvorfällen beschrieben sein. Zusätzlich MUSS es für alle Mitarbeitenden zielgruppenorientierte und praktisch anwendbare Handlungsanweisungen geben. Weiterhin SOLLTEN die Schnittstellen zu anderen Managementbereichen berücksichtigt werden, z. B. zum Notfallmanagement.

Die Richtlinie MUSS allen Mitarbeitenden bekannt sein. Sie MUSS mit dem IT-Betrieb abgestimmt und durch die Institutionsleitung verabschiedet sein. Die Richtlinie MUSS regelmäßig geprüft und aktualisiert werden.

### **DER.2.1.A3 Festlegung von Verantwortlichkeiten und Ansprechpersonen bei Sicherheitsvorfällen (B)**

Es MUSS geregelt werden, wer bei Sicherheitsvorfällen wofür verantwortlich ist. Für alle Mitarbeitenden MÜSSEN die Aufgaben und Kompetenzen bei Sicherheitsvorfällen festgelegt werden. Insbesondere Mitarbeitende, die Sicherheitsvorfälle bearbeiten sollen, MÜSSEN über ihre Aufgaben und Kompetenzen unterrichtet werden. Dabei MUSS auch geregelt sein, wer die mögliche Entscheidung für eine forensische Untersuchung trifft, nach welchen Kriterien diese vorgenommen wird und wann sie erfolgen soll.

Die Ansprechpartner oder Ansprechpartnerinnen für alle Arten von Sicherheitsvorfällen MÜSSEN den Mitarbeitenden bekannt sein. Kontaktinformationen MÜSSEN immer aktuell und leicht zugänglich sein.

### **DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen (B) [Institutionsleitung, IT-Betrieb, Datenschutzbeauftragte, Notfallbeauftragte]**

Von einem Sicherheitsvorfall MÜSSEN alle betroffenen internen und externen Stellen zeitnah informiert werden. Dabei MUSS geprüft werden, ob der oder die Datenschutzbeauftragte, der Betriebs- und Personalrat sowie Mitarbeitende aus der Rechtsabteilung einbezogen werden müssen. Ebenso MÜSSEN die Meldepflichten für Behörden und regulierte Branchen berücksichtigt werden. Außerdem MUSS gewährleistet sein, dass betroffene Stellen über die erforderlichen Maßnahmen informiert werden.

### **DER.2.1.A5 Behebung von Sicherheitsvorfällen (B) [IT-Betrieb]**

Damit ein Sicherheitsvorfall erfolgreich behoben werden kann, MÜSSEN die Zuständigen zunächst das Problem eingrenzen und die Ursache finden. Danach MÜSSEN die erforderlichen Maßnahmen ausgewählt werden, um das Problem zu beheben. Die Leitung des IT-Betriebs MUSS eine Freigabe erteilen, bevor die Maßnahmen umgesetzt werden. Anschließend MUSS die Ursache beseitigt und ein sicherer Zustand hergestellt werden.

Eine aktuelle Liste von internen und externen Sicherheitsfachleuten MUSS vorhanden sein, die bei Sicherheitsvorfällen für Fragen aus den erforderlichen Themenbereichen hinzugezogen werden können. Es MÜSSEN sichere Kommunikationsverfahren mit diesen internen und externen Stellen etabliert werden.

### **DER.2.1.A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen (B) [IT-Betrieb]**

Nach einem Sicherheitsvorfall MÜSSEN die betroffenen Komponenten vom Netz genommen werden. Zudem MÜSSEN alle erforderlichen Daten gesichert werden, die Aufschluss über die Art und Ursache des Problems geben könnten. Auf allen betroffenen Komponenten MÜSSEN das Betriebssystem und alle Applikationen auf Veränderungen untersucht werden.

Die Originaldaten MÜSSEN von schreibgeschützten Datenträgern wieder eingespielt werden. Dabei MÜSSEN alle sicherheitsrelevanten Konfigurationen und Patches mit aufgespielt werden. Wenn Daten aus Datensicherungen wieder eingespielt werden, MUSS sichergestellt sein, dass diese vom Sicherheitsvorfall nicht betroffen waren. Nach einem Angriff MÜSSEN alle Zugangsdaten auf den betroffenen Komponenten geändert werden, bevor sie wieder in Betrieb genommen werden. Die betroffenen Komponenten SOLLTEN einem Penetrationstest unterzogen werden, bevor sie wieder eingesetzt werden.

Bei der Wiederherstellung der sicheren Betriebsumgebung MÜSSEN die Benutzenden in die Anwendungsfunktionstests einbezogen werden. Nachdem alles wiederhergestellt wurde, MÜSSEN die Komponenten inklusive der Netzübergänge gezielt überwacht 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.

### **DER.2.1.A7 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen (S) [Institutionsleitung]**

Es SOLLTE eine geeignete Vorgehensweise zur Behandlung von Sicherheitsvorfällen definiert werden. Die Abläufe, Prozesse und Vorgaben für die verschiedenen Sicherheitsvorfälle SOLLTEN dabei eindeutig geregelt und geeignet dokumentiert werden. Die Institutionsleitung SOLLTE die festgelegte Vorgehensweise in Kraft setzen und allen Beteiligten zugänglich machen. Es SOLLTE regelmäßig überprüft werden, ob die Vorgehensweise noch aktuell und wirksam ist. Bei Bedarf SOLLTE die Vorgehensweise angepasst werden.

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

Für den Umgang mit Sicherheitsvorfällen SOLLTEN geeignete Organisationsstrukturen festgelegt werden. Es SOLLTE ein Sicherheitsvorfall-Team aufgebaut werden, dessen Mitglieder je nach Art des Vorfalls einberufen werden können. Auch wenn das Sicherheitsvorfall-Team nur für einen konkreten Fall zusammentritt, SOLLTEN bereits im Vorfeld geeignete Mitglieder benannt und in ihre Aufgaben eingewiesen sein. Es SOLLTE regelmäßig geprüft werden, ob die Zusammensetzung des Sicherheitsvorfall-Teams noch angemessen ist. Gegebenenfalls SOLLTE das Sicherheitsvorfall-Team neu zusammengestellt werden.

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

Für die verschiedenen Arten von Sicherheitsvorfällen SOLLTEN die jeweils passenden Meldewege aufgebaut sein. Es SOLLTE dabei sichergestellt sein, dass Mitarbeitende Sicherheitsvorfälle über verlässliche und vertrauenswürdige Kanäle schnell und einfach melden können.

Wird eine zentrale Anlaufstelle für die Meldung von Störungen oder Sicherheitsvorfällen eingerichtet, SOLLTE dies an alle Mitarbeitende kommuniziert werden.

Eine Kommunikations- und Kontaktstrategie SOLLTE vorliegen. Darin SOLLTE geregelt sein, wer grundsätzlich informiert werden muss und wer informiert werden darf, durch wen dies in welcher Reihenfolge erfolgt und in welcher Tiefe informiert wird. Es SOLLTE definiert sein, wer Informationen über Sicherheitsvorfälle an Dritte weitergibt. Ebenso SOLLTE sichergestellt sein, dass keine unautorisierten Personen Informationen über den Sicherheitsvorfall weitergeben.

### **DER.2.1.A10 Eindämmen der Auswirkung von Sicherheitsvorfällen (S) [Notfallbeauftragte, IT-Betrieb]**

Parallel zur Ursachenanalyse eines Sicherheitsvorfalls SOLLTE entschieden werden, ob es wichtiger ist, den entstandenen Schaden einzudämmen oder den Vorfall aufzuklären. Um die Auswirkung eines Sicherheitsvorfalls abschätzen zu können, SOLLTEN ausreichend Informationen vorliegen. Für

ausgewählte Sicherheitsvorfallszenarien SOLLTEN bereits im Vorfeld Worst-Case-Betrachtungen durchgeführt werden.

#### **DER.2.1.A11 Einstufung von Sicherheitsvorfällen (S) [IT-Betrieb]**

Ein einheitliches Verfahren SOLLTE festgelegt werden, um Sicherheitsvorfälle und Störungen einzustufen. Das Einstufungsverfahren für Sicherheitsvorfälle SOLLTE zwischen Sicherheitsmanagement und der Störungs- und Fehlerbehebung (Incident Management) abgestimmt sein.

#### **DER.2.1.A12 Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung (S) [Notfallbeauftragte]**

Die Schnittstellen zwischen Störungs- und Fehlerbehebung, Notfallmanagement und Sicherheitsmanagement SOLLTEN analysiert werden. Dabei SOLLTEN auch eventuell gemeinsam benutzbare Ressourcen identifiziert werden.

Die bei der Störungs- und Fehlerbehebung beteiligten Mitarbeitenden SOLLTEN für die Behandlung von Sicherheitsvorfällen sowie für das Notfallmanagement sensibilisiert werden. Das Sicherheitsmanagement SOLLTE lesenden Zugriff auf eingesetzte Incident-Management-Werkzeuge haben.

#### **DER.2.1.A13 Einbindung in das Sicherheits- und Notfallmanagement (S) [Notfallbeauftragte]**

Die Behandlung von Sicherheitsvorfällen SOLLTE mit dem Notfallmanagement abgestimmt sein. Falls es in der Institution eine spezielle Rolle für Störungs- und Fehlerbehebung gibt, SOLLTE auch diese mit einbezogen werden.

#### **DER.2.1.A14 Eskalationsstrategie für Sicherheitsvorfälle (S) [IT-Betrieb]**

Über die Kommunikations- und Kontaktstrategie hinaus SOLLTE eine Eskalationsstrategie formuliert werden. Diese SOLLTE zwischen den Verantwortlichen für Störungs- und Fehlerbehebung und dem Informationssicherheitsmanagement abgestimmt werden.

Die Eskalationsstrategie SOLLTE eindeutige Handlungsanweisungen enthalten, wer auf welchem Weg bei welcher Art von erkennbaren oder vermuteten Sicherheitsstörungen wann einzubeziehen ist. Es SOLLTE geregelt sein, zu welchen Maßnahmen eine Eskalation führt und wie reagiert werden soll.

Für die festgelegte Eskalationsstrategie SOLLTEN geeignete Werkzeuge wie z. B. Ticket-Systeme ausgewählt werden. Diese SOLLTEN sich auch dafür eignen, vertrauliche Informationen zu verarbeiten. Es SOLLTE sichergestellt sein, dass die Werkzeuge auch während eines Sicherheitsvorfalls bzw. Notfalls verfügbar sind.

Die Eskalationsstrategie SOLLTE regelmäßig überprüft und gegebenenfalls aktualisiert werden. Die Checklisten (Matching Szenarios) für Störungs- und Fehlerbehebung SOLLTEN regelmäßig um sicherheitsrelevante Themen ergänzt bzw. aktualisiert werden. Die festgelegten Eskalationswege SOLLTEN in Übungen erprobt werden.

#### **DER.2.1.A15 Schulung der Mitarbeitenden des Service Desks (S) [IT-Betrieb]**

Dem Personal des Service Desk SOLLTEN geeignete Hilfsmittel zur Verfügung stehen, damit sie Sicherheitsvorfälle erkennen können. Sie SOLLTEN ausreichend geschult sein, um die Hilfsmittel selbst anwenden zu können. Die Mitarbeitenden des Service Desk SOLLTEN den Schutzbedarf der betroffenen IT-Systeme kennen.

#### **DER.2.1.A16 Dokumentation der Behebung von Sicherheitsvorfällen (S)**

Die Behebung von Sicherheitsvorfällen SOLLTE nach einem standardisierten Verfahren dokumentiert werden. Es SOLLTEN alle durchgeführten Aktionen inklusive der Zeitpunkte sowie die Protokolldaten

der betroffenen Komponenten dokumentiert werden. Dabei SOLLTE die Vertraulichkeit bei der Dokumentation und Archivierung der Berichte gewährleistet sein.

Die benötigten Informationen SOLLTEN in die jeweiligen Dokumentationssysteme eingepflegt werden, bevor die Störung als beendet und als abgeschlossen markiert wird. Im Vorfeld SOLLTEN mit dem oder der ISB die dafür erforderlichen Anforderungen an die Qualitätssicherung definiert werden.

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

Sicherheitsvorfälle SOLLTEN standardisiert nachbereitet werden. Dabei SOLLTE untersucht werden, wie schnell die Sicherheitsvorfälle erkannt und behoben wurden. Weiterhin SOLLTE untersucht werden, ob die Meldewege funktionierten, ausreichend Informationen für die Bewertung verfügbar und ob die Detektionsmaßnahmen wirksam waren. Ebenso SOLLTE geprüft werden, ob die ergriffenen Maßnahmen und Aktivitäten wirksam und effizient waren.

Die Erfahrungen aus vergangenen Sicherheitsvorfällen SOLLTEN genutzt werden, um daraus Handlungsanweisungen für vergleichbare Sicherheitsvorfälle zu erstellen. Diese Handlungsanweisungen SOLLTEN den relevanten Personengruppen bekanntgegeben und auf Basis neuer Erkenntnisse regelmäßig aktualisiert werden.

Die Institutionsleitung SOLLTE jährlich über die Sicherheitsvorfälle unterrichtet werden. Besteht sofortiger Handlungsbedarf, MUSS die Institutionsleitung umgehend informiert werden.

### **DER.2.1.A18 Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen (S) [Fachverantwortliche]**

Nachdem ein Sicherheitsvorfall analysiert wurde, SOLLTE untersucht werden, ob die Prozesse und Abläufe im Rahmen der Behandlung von Sicherheitsvorfällen geändert oder weiterentwickelt werden müssen. Dabei SOLLTEN alle Personen, die an dem Vorfall beteiligt waren, über ihre jeweiligen Erfahrungen berichten.

Es SOLLTE geprüft werden, ob es neue Entwicklungen im Bereich Incident Management und in der Forensik gibt und ob diese in die jeweiligen Dokumente und Abläufe eingebracht werden können.

Werden Hilfsmittel und Checklisten eingesetzt, z. B. für Service-Desk-Mitarbeitende, SOLLTE geprüft werden, ob diese um relevante Fragen und Informationen zu erweitern sind.

## **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.

### **DER.2.1.A19 Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen (H) [Institutionsleitung]**

Es SOLLTEN Prioritäten für die Behandlung von Sicherheitsvorfällen vorab festgelegt und regelmäßig aktualisiert werden. Dabei SOLLTE auch die vorgenommene Einstufung von Sicherheitsvorfällen berücksichtigt werden.

Die Prioritäten SOLLTEN von der Institutionsleitung genehmigt und in Kraft gesetzt werden. Sie SOLLTEN allen Verantwortlichen bekannt sein, die mit der Behandlung von Sicherheitsvorfällen zu tun haben. Die festgelegten Prioritätsklassen SOLLTEN außerdem im Incident Management hinterlegt sein.

### **DER.2.1.A20 Einrichtung einer dedizierten Meldestelle für Sicherheitsvorfälle (H)**

Eine dedizierte Stelle zur Meldung von Sicherheitsvorfällen SOLLTE eingerichtet werden. Es SOLLTE gewährleistet sein, dass die Meldestelle zu den üblichen Arbeitszeiten erreichbar ist. Zusätzlich SOLLTE es möglich sein, dass Sicherheitsvorfälle auch außerhalb der üblichen Arbeitszeiten gemeldet werden können. Die Mitarbeitenden der Meldestelle SOLLTEN ausreichend geschult und für die Belange der Informationssicherheit sensibilisiert sein. Alle Informationen über Sicherheitsvorfälle SOLLTEN bei der Meldestelle vertraulich behandelt werden.

### **DER.2.1.A21 Einrichtung eines Teams von Fachleuten für die Behandlung von Sicherheitsvorfällen (H)**

Es SOLLTE ein Team mit erfahrenen und vertrauenswürdigen Fachleuten zusammengestellt werden. Neben dem technischen Verständnis SOLLTEN die Teammitglieder auch über Kompetenzen im Bereich Kommunikation verfügen. Die Vertrauenswürdigkeit der Mitglieder des Teams SOLLTE überprüft werden. Die Zusammensetzung des Teams SOLLTE regelmäßig überprüft und, wenn nötig, geändert werden.

Die Mitglieder des Teams SOLLTEN in die Eskalations- und Meldewege eingebunden sein. Das Experten- und Expertinnenteam SOLLTE für die Analyse von Sicherheitsvorfällen an den in der Institution eingesetzten Systemen ausgebildet werden. Die Mitglieder des Experten- und Expertinnenteams SOLLTEN sich regelmäßig weiterbilden, sowohl zu den eingesetzten Systemen als auch zur Detektion und Reaktion auf Sicherheitsvorfälle. Dem Experten- und Expertinnenteam SOLLTEN alle vorhandenen Dokumentationen sowie finanzielle und technische Ressourcen zur Verfügung stehen, um Sicherheitsvorfälle schnell und diskret zu behandeln.

Das Experten- und Expertinnenteams SOLLTE in geeigneter Weise in den Organisationsstrukturen berücksichtigt und in diese integriert werden. Die Zuständigkeiten des Teams SOLLTEN vorher mit denen des Sicherheitsvorfall-Teams abgestimmt werden.

### **DER.2.1.A22 Überprüfung der Effizienz des Managementsystems zur Behandlung von Sicherheitsvorfällen (H)**

Das Managementsystem zur Behandlung von Sicherheitsvorfällen SOLLTE regelmäßig daraufhin geprüft werden, ob es noch aktuell und wirksam ist. Dazu SOLLTEN sowohl angekündigte als auch unangekündigte Übungen durchgeführt werden. Die Übungen SOLLTEN vorher mit der Institutionsleitung abgestimmt sein. Es SOLLTEN die Messgrößen ausgewertet werden, die anfallen, wenn Sicherheitsvorfälle aufgenommen, gemeldet und eskaliert werden, z. B. die Zeiträume von der Erstmeldung bis zur verbindlichen Bestätigung eines Sicherheitsvorfalls.

Außerdem SOLLTEN Planspiele zur Behandlung von Sicherheitsvorfällen durchgeführt werden.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 „Information technology - Security techniques - Information security management systems - Requirements“ im Anhang A16 „Information security incident management“ Vorgaben für die Behandlung von Sicherheitsvorfällen.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27035:2016 „Information technology - Security techniques - Information security incident management“ Vorgaben für die Behandlung von Sicherheitsvorfällen.

Das National Institute of Standards and Technology (NIST) macht in seiner Special Publication 800-61 Revision 2 „Computer Security Incident Handling Guide“ generelle Vorgaben zur Behandlung von Sicherheitsvorfällen.

Das National Institute of Standards and Technology (NIST) macht in seiner Special Publication 800-83 Revision 1 „Guide to Malware incident Prevention and Handling for Desktops and Laptops“ spezifische Vorgaben zum Umgang mit Malware-Infektionen bei Laptops und Desktops.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel TS1.4 „Technical Security Management; Identity and Access Management“ Vorgaben für die Behandlung von Sicherheitsvorfällen.





# DER.2.2 Vorsorge für die IT-Forensik

## 1. Beschreibung

### 1.1. Einleitung

IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Datennetzen zur Aufklärung von Sicherheitsvorfällen in IT-Systemen.

IT-Sicherheitsvorfälle forensisch zu untersuchen, ist immer dann notwendig, wenn entstandene Schäden bestimmt, Angriffe abgewehrt, zukünftige Angriffe vermieden und Angreifende identifiziert werden sollen. Ob ein IT-Sicherheitsvorfall forensisch untersucht wird, entscheidet sich, während der Vorfall behandelt wird. Eine IT-forensische Untersuchung im Sinne dieses Bausteins besteht aus den folgenden Phasen:

- **Strategische Vorbereitung:** In dieser Phase werden Prozesse geplant und aufgebaut, die sicherstellen, dass eine Institution IT-Sicherheitsvorfälle forensisch analysieren kann. Sie ist auch dann notwendig, wenn die Institution über keine eigene Forensik-Expertise verfügt.
- **Initialisierung:** Nachdem die verantwortlichen Mitarbeitenden entschieden haben, einen IT-Sicherheitsvorfall forensisch zu untersuchen, werden die vorher geplanten Prozesse angestoßen. Des Weiteren wird der Untersuchungsrahmen festgelegt und es werden Erstmaßnahmen durchgeführt.
- **Spurensicherung:** Hier werden die zu sichernden Beweismittel ausgewählt und die Daten forensisch gesichert. Dabei wird zwischen Live-Forensik und Post-Mortem-Forensik unterschieden: Die Live-Forensik stellt sicher, dass flüchtige Daten, wie z. B. Netzverbindungen oder RAM, von einem laufenden IT-System gesichert werden. Bei der Post-Mortem-Forensik hingegen werden forensische Kopien von Datenträgern erstellt.
- **Analyse:** Die gesammelten Daten werden forensisch analysiert. Dabei werden die Daten sowohl für sich als auch im Gesamtzusammenhang betrachtet.
- **Ergebnisdarstellung:** Die relevanten Untersuchungsergebnisse werden zielgruppengerecht aufbereitet und vermittelt.

## 1.2. Zielsetzung

Der Baustein 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-Dienstleistende Spurensicherungen ganz oder teilweise durch, gelten die Anforderungen auch für die Dienstleistenden. Durch vertragliche Vereinbarungen und Prüfungen kann dabei sichergestellt werden, dass sich die Dienstleistenden auch daran halten.

## 1.3. Abgrenzung und Modellierung

Der Baustein DER.2.2 *Vorsorge für die IT-Forensik* ist für den gesamten Informationsverbund einmal anzuwenden.

Der Baustein befasst sich mit Vorsorgemaßnahmen, die grundlegend für spätere IT-forensische Untersuchungen sind.

Wie die eigentliche forensische Analyse durchgeführt wird, ist daher nicht Thema dieses Bausteins. Es werden keine Anforderungen beschrieben, die sicherstellen, dass Angriffe erkannt werden. Diese sind im Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* enthalten und werden im vorliegenden Baustein vorausgesetzt. Auch werden keine Kriterien und Prozesse erläutert, anhand derer die Verantwortlichen entscheiden können, ob ein IT-Sicherheitsvorfall forensisch untersucht werden muss oder nicht. Die Entscheidung darüber wird getroffen, während der Sicherheitsvorfall behandelt wird (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

Ebenso bezieht sich der Baustein nicht auf IT-forensische Untersuchungen bei Straftaten.

Letztlich geht der Baustein auch nicht darauf ein, wie sich IT-Infrastrukturen bereinigen lassen, nachdem sie angegriffen worden sind (siehe dazu DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle*). Die dort beschriebenen Tätigkeiten können jedoch durch die Ergebnisse von IT-forensischen Untersuchungen maßgeblich unterstützt werden.

## 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 DER.2.2 *Vorsorge für die IT-Forensik* von besonderer Bedeutung.

### 2.1. Verstoß gegen rechtliche Rahmenbedingungen

Für IT-forensische Untersuchungen werden oft alle für notwendig befundenen Daten kopiert, sichergestellt und ausgewertet. Darunter befinden sich meistens auch personenbezogene Daten von Mitarbeitenden oder externen Partner und Partnerinnen. Wird darauf z. B. unbegründet und ohne Einbeziehung der oder die Datenschutzbeauftragte zugegriffen, verstößt die Institution gegen gesetzliche Regelungen, etwa wenn dabei die Zweckbindung missachtet wird. Auch ist es möglich, dass aus den erhobenen Daten beispielsweise abgeleitet werden kann, wie sich Mitarbeitende verhalten, oder es kann ein Bezug zu ihnen hergestellt werden. Dadurch besteht die Gefahr, dass auch gegen interne Regelungen verstoßen wird.

## 2.2. Verlust von Beweismitteln durch fehlerhafte oder unvollständige Beweissicherung

Werden Beweismittel falsch oder nicht schnell genug gesichert, können dadurch wichtige Daten verloren gehen, die später nicht wiederhergestellt werden können. Im ungünstigsten Fall führt das zu einer ergebnislosen forensischen Untersuchung. Mindestens ist jedoch die Beweiskraft eingeschränkt.

Die Gefahr, wichtige Beweismittel zu verlieren, steigt stark an, wenn Mitarbeitende die Werkzeuge zur Forensik fehlerhaft benutzen, Daten zu langsam sichern oder zu wenig üben. Oft gehen auch Beweismittel verloren, wenn die Verantwortlichen flüchtige Daten nicht als relevant erkennen und sichern.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.2.2 *Vorsorge für die IT-Forensik* 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	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Fachverantwortliche, Datenschutzbeauftragte, Institutionsleitung

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:

#### **DER.2.2.A1 Prüfung rechtlicher und regulatorischer Rahmenbedingungen zur Erfassung und Auswertbarkeit (B) [Datenschutzbeauftragte, Institutionsleitung]**

Werden Daten für forensische Untersuchungen erfasst und ausgewertet, MÜSSEN alle rechtlichen und regulatorischen Rahmenbedingungen identifiziert und eingehalten werden (siehe ORP.5 *Compliance Management (Anforderungsmanagement)*). Auch DARF NICHT gegen interne Regelungen und Mitarbeitendenvereinbarungen verstoßen werden. Dazu MÜSSEN der Betriebs- oder Personalrat sowie der oder die Datenschutzbeauftragte einbezogen werden.

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

Es MUSS ein Leitfaden erstellt werden, der für die eingesetzten IT-Systeme beschreibt, welche Erstmaßnahmen bei einem IT-Sicherheitsvorfall durchgeführt werden müssen, um möglichst wenig Spuren zu zerstören. Darin MUSS auch beschrieben sein, durch welche Handlungen potenzielle Spuren vernichtet werden könnten und wie sich das vermeiden lässt.

### **DER.2.2.A3 Vorauswahl von Forensik-Dienstleistenden (B)**

Verfügt eine Institution nicht über ein eigenes Forensik-Team, MÜSSEN bereits in der Vorbereitungsphase mögliche geeignete Forensik-Dienstleistenden identifiziert werden. Welche Forensik-Dienstleistende infrage kommen, MUSS dokumentiert 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.

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

Die Schnittstellen zwischen IT-forensischen Untersuchungen und dem Krisen- und Notfallmanagement SOLLTEN definiert und dokumentiert werden. Hierzu SOLLTE geregelt werden, welche Mitarbeitenden für welche Aufgaben verantwortlich sind und wie mit ihnen kommuniziert werden soll. Darüber hinaus SOLLTE sichergestellt werden, dass die zuständigen Kontaktpersonen stets erreichbar sind.

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

Es SOLLTE ein Leitfaden erstellt werden, in dem beschrieben wird, wie Beweise gesichert werden sollen. Darin SOLLTEN Vorgehensweisen, technische Werkzeuge, rechtliche Rahmenbedingungen und Dokumentationsvorgaben aufgeführt werden.

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

Alle verantwortlichen Mitarbeitenden SOLLTEN wissen, wie sie Spuren korrekt sichern und die Werkzeuge zur Forensik richtig einsetzen. Dafür SOLLTEN geeignete Schulungen durchgeführt werden.

### **DER.2.2.A7 Auswahl von Werkzeugen zur Forensik (S)**

Es SOLLTE sichergestellt werden, dass Werkzeuge, mit denen Spuren forensisch gesichert und analysiert werden, auch dafür geeignet sind. Bevor ein Werkzeug zur Forensik eingesetzt wird, SOLLTE zudem geprüft werden, ob es richtig funktioniert. Auch SOLLTE überprüft und dokumentiert werden, dass es nicht manipuliert wurde.

### **DER.2.2.A8 Auswahl und Reihenfolge der zu sichernden Beweismittel (S) [Fachverantwortliche]**

Eine forensische Untersuchung SOLLTE immer damit beginnen, die Ziele bzw. den Arbeitsauftrag zu definieren. Die Ziele SOLLTEN möglichst konkret formuliert sein. Danach SOLLTEN alle notwendigen Datenquellen identifiziert werden. Auch SOLLTE festgelegt werden, in welcher Reihenfolge die Daten gesichert werden und wie genau dabei vorgegangen werden soll. Die Reihenfolge SOLLTE sich danach richten, wie flüchtig (volatil) die zu sichernden Daten sind. So SOLLTEN schnell flüchtige Daten zeitnah gesichert werden. Erst danach SOLLTEN nichtflüchtige Daten wie beispielsweise Festspeicherinhalte und schließlich Backups folgen.

### **DER.2.2.A9 Vorauswahl forensisch relevanter Daten (S) [Fachverantwortliche]**

Es SOLLTE festgelegt werden, welche sekundären Daten (z. B. Logdaten oder Verkehrsmitsschnitte) auf welche Weise und wie lange im Rahmen der rechtlichen Rahmenbedingungen für mögliche forensische Beweissicherungsmaßnahmen vorgehalten werden.

### **DER.2.2.A10 IT-forensische Sicherung von Beweismitteln (S) [Fachverantwortliche]**

Datenträger SOLLTEN möglichst komplett forensisch dupliziert werden. Wenn das nicht möglich ist, z. B. bei flüchtigen Daten im RAM oder in SAN-Partitionen, SOLLTE eine Methode gewählt werden, die möglichst wenige Daten verändert.

Die Originaldatenträger SOLLTEN versiegelt aufbewahrt werden. Es SOLLTEN schriftlich dokumentierte kryptografische Prüfsummen von den Datenträgern angelegt werden. Diese SOLLTEN getrennt und in mehreren Kopien aufbewahrt werden. Zudem SOLLTE sichergestellt sein, dass die so dokumentierten Prüfsummen nicht verändert werden können. Damit die Daten gerichtlich verwertbar sind, SOLLTE ein Zeuge bestätigen, wie dabei vorgegangen wurde und die erstellten Prüfsummen beglaubigen.

Es SOLLTE ausschließlich geschultes Personal (siehe DER.2.2.A6 *Schulung des Personals für die Umsetzung der forensischen Sicherung*) oder ein Forensik-Dienstleistender (siehe DER.2.2.A3 *Vorauswahl von Forensik-Dienstleistenden*) eingesetzt werden, um Beweise forensisch zu sichern.

### **DER.2.2.A11 Dokumentation der Beweissicherung (S) [Fachverantwortliche]**

Wenn Beweise forensisch gesichert werden, SOLLTEN alle durchgeführten Schritte dokumentiert werden. Die Dokumentation SOLLTE lückenlos nachweisen, wie mit den gesicherten Originalbeweismitteln umgegangen wurde. Auch SOLLTE dokumentiert werden, welche Methoden eingesetzt wurden und warum sich die Verantwortlichen dafür entschieden haben.

### **DER.2.2.A12 Sichere Verwahrung von Originaldatenträgern und Beweismitteln (S) [Fachverantwortliche]**

Alle sichergestellten Originaldatenträger SOLLTEN physisch so gelagert werden, dass nur ermittelnde und namentlich bekannte Mitarbeitende darauf zugreifen können. Wenn Originaldatenträger und Beweismittel eingelagert werden, SOLLTE festgelegt werden, wie lange sie aufzubewahren sind. Nachdem die Frist abgelaufen ist, SOLLTE geprüft werden, ob die Datenträger und Beweise noch weiter aufbewahrt werden müssen. Nach der Aufbewahrungsfrist SOLLTEN Beweismittel sicher gelöscht oder vernichtet und Originaldatenträger zurückgegeben werden.

## **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.

### **DER.2.2.A13 Rahmenverträge mit externen Dienstleistenden (H)**

Die Institution SOLLTE Abrufvereinbarungen bzw. Rahmenverträge mit Forensik-Dienstleistenden abschließen, damit IT-Sicherheitsvorfälle schneller forensisch untersucht werden können.

### **DER.2.2.A14 Festlegung von Standardverfahren für die Beweissicherung (H)**

Für Anwendungen, IT-Systeme bzw. IT-Systemgruppen mit hohem Schutzbedarf sowie für verbreitete Systemkonfigurationen SOLLTEN Standardverfahren erstellt werden, die es erlauben, flüchtige und nichtflüchtige Daten möglichst vollständig forensisch zu sichern.

Die jeweiligen systemspezifischen Standardverfahren SOLLTEN durch erprobte und möglichst automatisierte Prozesse umgesetzt werden. Sie SOLLTEN zudem durch Checklisten und technische Hilfsmittel unterstützt werden, z. B. durch Software, Software-Tools auf mobilen Datenträgern und IT-forensische Hardware wie Schreibblocker.

## **DER.2.2.A15 Durchführung von Übungen zur Beweissicherung (H)**

Alle an forensischen Analysen beteiligten Mitarbeitenden SOLLTEN regelmäßig in Form von Übungen trainieren, wie Beweise bei einem IT-Sicherheitsvorfall zu sichern sind.

# **4. Weiterführende Informationen**

## **4.1. Wissenswertes**

Das BSI gibt in dem „Leitfaden IT-Forensik“ weiterführende Informationen in die Thematik und kann auch als Nachschlagewerk für einzelne praxisbezogene Problemstellungen dienen.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27042:2015 und 27043:2015 01:2013 Vorgaben für die Durchführung von forensischen Analysen.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel TM 2.4 Forensik Investigations Vorgaben für die Durchführung von forensischen Analysen.

Der Request for Comments (RFC) 3227 „Guidelines for Evidence Collection and Archiving“ gibt in seinem Leitfaden Hinweise zur grundlegenden Vorgehensweise bei einer forensischen Sicherung.



# DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle

## 1. Beschreibung

### 1.1. Einleitung

Bei Advanced Persistent Threats (APTs) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen. Dabei verschaffen sich Angreifende dauerhaften Zugriff zu einem Netz und weiten diesen Zugriff auf weitere IT-Systeme aus. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und umfassende technische Fähigkeiten auf Seiten der Angreifenden aus. Angriffe dieser Art sind in der Regel schwierig zu detektieren.

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

In diesem Baustein wird von einer hohen Bedrohungslage durch einen gezielten Angriff hochmotivierter Personen mit überdurchschnittlichen Ressourcen ausgegangen. In der Praxis ist es üblich, dass bei einem solchen Vorfall immer auch auf (zertifizierte) forensische Dienstleistung zurückgegriffen wird, wenn die Institution selbst nicht über entsprechende eigene forensische Expertise verfügt. Forensikdienstleistende werden dabei bereits in der Phase der forensischen Analyse herangezogen. Die Dienstleistenden werden jedoch auch bei der Bereinigung zumindest beratend einbezogen.

### 1.2. Zielsetzung

Dieser Baustein beschreibt, wie eine Institution vorgehen sollte, um nach einem APT-Angriff die IT-Systeme zu bereinigen und den regulären und sicheren Betriebszustand des Informationsverbunds wiederherzustellen.

## 1.3. Abgrenzung und Modellierung

Der Baustein DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* ist immer dann anzuwenden, wenn nach einem APT-Vorfall die IT-Systeme bereinigt werden sollen, um den regulären und sicheren Betriebszustand eines Informationsverbunds wiederherzustellen. Der Baustein ist auf den Informationsverbund anzuwenden.

Ein Informationsverbund kann nur bereinigt werden, wenn der APT-Vorfall vorher erfolgreich detektiert und forensisch analysiert wurde. Detektion und Forensik sind jedoch nicht Thema dieses Bausteins. Diese Themen werden in den Bausteinen DER.1 *Detektion von sicherheitsrelevanten Ereignissen* bzw. DER.2.2 *Vorsorge für die IT-Forensik* behandelt.

Im vorliegenden Baustein geht es ausschließlich um die Bereinigung von APT-Vorfällen. Andere Vorfälle werden im Baustein DER.2.1 *Behandlung von Sicherheitsvorfällen* behandelt. Auch beschreibt der Baustein nicht, wie sogenannte Indicators of Compromise (IOCs), also Einbruchsspuren, abzuleiten sind und wie diese benutzt werden können, um wiederkehrende Angreifende zu erkennen. Ebenso wird nicht darauf eingegangen, wie sich eventuell bei der Analyse und Bereinigung übersehene Hintertüren finden lassen.

Es werden ausschließlich Cyber-Angriffe berücksichtigt. Das heißt, es werden keine Angriffe betrachtet, mit denen sich z. B. physischen Zugriff auf den Informationsverbund verschafft wird. So werden Angriffsformen, bei denen in Rechenzentren eingebrochen, Administrierende bestochen, neu beschaffte Hardware abgefangen und manipuliert oder elektromagnetische Strahlung abgehört werden, nicht in diesem Baustein betrachtet.

Bereinigen Forensikdienstleistende die IT-Systeme ganz oder teilweise, gelten die Anforderungen dieses Bausteins auch für diese Dienstleistenden. Durch vertragliche Vereinbarungen und Prüfungen kann dabei sichergestellt werden, dass sich die Dienstleistenden auch daran halten (siehe OPS.2.3 *Nutzung von Outsourcing*).

## 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 DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* von besonderer Bedeutung.

### 2.1. Unvollständige Bereinigung

APT-Angreifende wollen üblicherweise einen Informationsverbund dauerhaft infiltrieren. Sie verfügen über die dafür notwendigen Ressourcen und sind in der Lage, langfristige Angriffskampagnen durchzuführen. Dafür benutzen sie Werkzeuge und Methoden, die auf ihr Angriffsziel abgestimmt sind. Auch wenn ein APT-Vorfall entdeckt wird, kann nicht davon ausgegangen werden, dass sämtliche Zugangswege der Angreifenden gefunden, alle Infektionen und Kommunikationswege von Schadsoftware beseitigt und alle Hintertüren entfernt wurden. Bei einer unvollständigen Bereinigung ist es jedoch sehr wahrscheinlich, dass Angreifende zu einem späteren Zeitpunkt, z. B. nach einer längeren Ruhephase, erneut auf die IT-Systeme zugreifen und ihren Zugang wieder ausbauen. Das können sie beispielsweise, indem sie Hintertüren nicht nur in Betriebssystemen und Anwendungssoftware platzieren, sondern auch hardwarenahe Komponenten wie etwa Firmware manipulieren. Solche Modifikationen sind sehr schwer zu identifizieren und das notwendige Wissen, um sie zu extrahieren und zu analysieren, ist nur wenig verbreitet. Versuchen die Zuständigen z. B. die IT-Komponenten zu bereinigen, indem sie die Firmware überschreiben oder aktualisieren, kann es trotzdem passieren, dass die Angreifenden auch die Update-Routinen modifiziert haben. Auf diesem Weg können sie dann wieder auf die IT-Systeme zugreifen.



## 2.2. Vernichtung von Spuren

Nach einem APT-Vorfall werden IT-Systeme oft neu installiert oder ganz ausgemustert. Wurde jedoch zuvor von den IT-Systemen keine forensische Kopie angefertigt, können Spuren vernichtet werden, die für eine weitere Aufklärung des Vorfalls oder sogar für ein Gerichtsverfahren notwendig wären.

## 2.3. Vorzeitige Alarmierung der Angreifenden

Üblicherweise wird vor der Bereinigung eines APT-Vorfalles der Angriff über längere Zeit hinweg beobachtet und forensisch analysiert, um so alle Zugangswege sowie die verwendeten Werkzeuge und Methoden zu identifizieren. Bemerkten die Angreifenden während dieser Phase, dass sie entdeckt wurden, greifen sie eventuell zu Gegenmaßnahmen. Beispielsweise können sie versuchen, ihre Spuren zu verwischen, oder sie sabotieren noch weitere IT-Systeme. Auch könnten sie den Angriff zunächst abbrechen oder weitere Hintertüren einrichten, um den Angriff später fortzuführen.

Da bei einem APT-Angriff grundsätzlich davon ausgegangen werden muss, dass die gesamte IT-Infrastruktur der Institution kompromittiert wurde, ist das Risiko hoch, dass die Angreifenden die Bereinigungsaktivitäten entdecken. Das gilt insbesondere, wenn die kompromittierte IT-Infrastruktur benutzt wird, um die Bereinigung zu planen und zu koordinieren. Finden die wesentlichen Schritte zur Bereinigung nicht in der korrekten Reihenfolge statt oder werden kritische Maßnahmen nicht gleichzeitig und aufeinander abgestimmt durchgeführt, erhöht sich die Gefahr, dass die Angreifenden alarmiert werden. Isolieren die Zuständigen beispielsweise das Netz schrittweise statt auf einmal, werden die Angreifenden eventuell gewarnt, bevor ihr Zugriff effektiv beendet ist.

## 2.4. Datenverlust und Ausfall von IT-Systemen

Bei der Bereinigung eines APT-Vorfalles werden verschiedene IT-Systeme neu installiert und auch Netze temporär isoliert. Dadurch fallen zwangsweise IT-Systeme aus und Dienste sind damit z. B. nur noch eingeschränkt oder gar nicht mehr verfügbar. Dauert die Bereinigung sehr lange, kann dadurch die Produktivität der Institution ausfallen. Das kann wiederum signifikante wirtschaftliche Einbußen zur Folge haben, die sogar existenzbedrohend sein können. Dies ist insbesondere dann der Fall, wenn keine oder keine ausreichende Dokumentation für einen Wiederaufbau verfügbar ist.

## 2.5. Fehlender Netzaufbau nach einem APT-Angriff

Bei einem APT-Angriff erlangen die Angreifenden detaillierte Kenntnisse darüber, wie die Zielumgebung aufgebaut und konfiguriert ist. Zum Beispiel kennen sie die existierenden Netzsegmente, Namensschemata für IT-Systeme, Konten sowie eingesetzte Software und Services. Durch dieses Wissen können sich dieselben Angreifenden unter Umständen auch nach einer Bereinigung erneut Zugang zur Zielumgebung verschaffen. Sie können sich sehr gezielt, effizient und unauffällig innerhalb des Netzes bewegen und in kurzer Zeit erneut einen hohen Infektionsgrad erreichen.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* 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

Zuständigkeiten	Rollen
Weitere Zuständigkeiten	Keine

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.

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

Um einen APT-Vorfall zu bereinigen, MUSS ein Leitungsgremium eingerichtet werden, das alle notwendigen Aktivitäten plant, koordiniert und überwacht. Dem Gremium **MÜSSEN** alle für die Aufgaben erforderlichen Weisungsbefugnisse übertragen werden.

Wenn ein solches Leitungsgremium zu dem Zeitpunkt, als der APT-Vorfall detektiert und klassifiziert wurde, bereits eingerichtet ist, SOLLTE dasselbe Gremium auch die Bereinigung planen und leiten. Wurden schon spezialisierte Forensikdienstleistende hinzugezogen, um den APT-Vorfall zu analysieren, SOLLTEN diese auch bei der Bereinigung des Vorfalls miteinbezogen werden.

Ist die IT zu stark kompromittiert, um weiter betrieben zu werden, oder sind die notwendigen Reinigungsmaßnahmen sehr umfangreich, SOLLTE geprüft werden, ob ein Krisenstab eingerichtet werden soll. In diesem Fall MUSS das Leitungsgremium die Reinigungsmaßnahmen überwachen. Das Leitungsgremium MUSS dann dem Krisenstab berichten.

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

Bevor ein APT-Vorfall tatsächlich bereinigt wird, MUSS das Leitungsgremium eine Bereinigungsstrategie festlegen. Dabei MUSS insbesondere entschieden werden, ob die Schadsoftware von kompromittierten IT-Systemen entfernt werden kann, ob IT-Systeme neu installiert werden müssen oder ob IT-Systeme inklusive der Hardware komplett ausgetauscht werden sollen. Weiterhin MUSS festgelegt werden, welche IT-Systeme bereinigt werden. Grundlage für diese Entscheidungen **MÜSSEN** die Ergebnisse einer zuvor durchgeführten forensischen Untersuchung sein.

Es SOLLTEN alle betroffenen IT-Systeme neu installiert werden. Danach **MÜSSEN** die Wiederanlaufpläne der Institution benutzt werden. Bevor jedoch Backups wieder eingespielt werden, MUSS durch forensische Untersuchungen sichergestellt sein, dass dadurch keine manipulierten Daten oder Programme auf das neu installierte IT-System übertragen werden.

Entscheidet sich eine Institution dagegen, alle IT-Systeme neu zu installieren, MUSS eine gezielte APT-Bereinigung umgesetzt werden. Um das Risiko übersehener Hintertüren zu minimieren, **MÜSSEN** nach der Bereinigung die IT-Systeme gezielt daraufhin überwacht werden, ob sie noch mit den Angreifenden kommunizieren.

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

Die von einem APT-Vorfall betroffenen Netzabschnitte **MÜSSEN** vollständig isoliert werden (Cut-Off). Insbesondere **MÜSSEN** die betroffenen Netzabschnitte vom Internet getrennt werden. Um die Angreifenden effektiv auszusperrern und zu verhindern, dass sie ihre Spuren verwischen oder noch weitere IT-Systeme sabotieren, **MÜSSEN** die Netzabschnitte auf einen Schlag isoliert werden.

Welche Netzabschnitte isoliert werden müssen, MUSS vorher durch eine forensische Analyse festgelegt werden. Es **MÜSSEN** dabei sämtliche betroffenen Abschnitte identifiziert werden. Kann das nicht sichergestellt werden, **MÜSSEN** alle verdächtigen sowie alle auch nur theoretisch infizierten Netzabschnitte isoliert werden.

Um Netzabschnitte effektiv isolieren zu können, MÜSSEN sämtliche lokalen Internetanschlüsse, z. B. zusätzliche DSL-Anschlüsse in einzelnen Subnetzen, möglichst vollständig erfasst und ebenfalls berücksichtigt werden.

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

Alle Zugangsdaten MÜSSEN geändert werden, nachdem das Netz isoliert wurde. Weiterhin MÜSSEN auch zentral verwaltete Zugangsdaten zurückgesetzt werden, z. B. in Active-Directory-Umgebungen oder wenn das Lightweight Directory Access Protocol (LDAP) benutzt wurde.

Ist der zentrale Authentisierungsserver (Domaincontroller oder LDAP-Server) kompromittiert, MÜSSEN sämtliche dort vorhandenen Zugänge gesperrt und ihre Passwörter ausgetauscht werden. Dies MÜSSEN erfahrene Administrierende umsetzen, falls erforderlich, auch mithilfe interner oder externer Expertise aus dem Bereich Forensik.

Wurden TLS-Schlüssel oder eine interne Certification Authority (CA) durch den APT-Angriff kompromittiert, MÜSSEN entsprechende Schlüssel, Zertifikate und Infrastrukturen neu erzeugt und verteilt werden. Auch MÜSSEN die kompromittierten Schlüssel und Zertifikate zuverlässig gesperrt und zurückgerufen werden.

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

Wurde durch eine forensische Untersuchung herausgefunden, dass die Angreifenden durch eine technische Schwachstelle in das Netz der Institution eingedrungen sind, MUSS diese Schwachstelle geschlossen werden. Konnten die Angreifenden die IT-Systeme durch menschliche Fehlhandlungen kompromittieren, MÜSSEN organisatorische, personelle und technische Maßnahmen ergriffen werden, um ähnliche Vorfälle künftig zu verhindern.

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

Nachdem das Netz erfolgreich bereinigt wurde, MÜSSEN die IT-Systeme geordnet in den Produktivbetrieb zurückgeführt werden. Dabei MÜSSEN sämtliche zuvor eingesetzten IT-Systeme und installierten Programme, mit denen der Angriff beobachtet und analysiert wurde, entweder entfernt oder aber in den Produktivbetrieb überführt werden. Dasselbe MUSS mit Kommunikations- und Kollaborationssystemen erfolgen, die für die Bereinigung angeschafft wurden. Beweismittel und ausgesonderte IT-Systeme MÜSSEN entweder sicher gelöscht bzw. vernichtet oder aber geeignet archiviert 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.

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

Nach einem APT-Angriff SOLLTEN alle betroffenen IT-Systeme gehärtet werden. Grundlage hierfür SOLLTEN die Ergebnisse der forensischen Untersuchungen sein. Zusätzlich SOLLTE erneut geprüft werden, ob die betroffene Umgebung noch sicher ist.

Wenn möglich, SOLLTEN IT-Systeme bereits während der Bereinigung gehärtet werden. Maßnahmen, die sich nicht kurzfristig durchführen lassen, SOLLTEN in einen Maßnahmenplan aufgenommen und mittelfristig umgesetzt werden. Der oder die ISB SOLLTE den Plan aufzustellen und prüfen, ob er korrekt umgesetzt wurde.

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

Es SOLLTEN sichere Kommunikationskanäle für das Leitungsgremium und die mit der Bereinigung beauftragten Mitarbeitenden etabliert werden. Wird auf Kommunikationsdienste Dritter

zurückgegriffen, SOLLTE auch hier darauf geachtet werden, dass ein sicherer Kommunikationskanal ausgewählt wird.

### **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.

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

Es SOLLTE erwogen werden, nach einem APT-Vorfall die Hardware komplett auszutauschen. Auch wenn nach einer Bereinigung bei einzelnen IT-Systemen noch verdächtiges Verhalten beobachtet wird, SOLLTEN die betroffenen IT-Systeme ausgetauscht werden.

#### **DER.2.3.A10 Umbauten zur Erschwerung eines erneuten Angriffs durch dieselben Angreifenden (H)**

Damit dieselben Angreifenden nicht noch einmal einen APT-Angriff auf die IT-Systeme der Institution durchführen können, SOLLTE der interne Aufbau der Netzumgebung geändert werden. Außerdem SOLLTEN Mechanismen etabliert werden, mit denen sich wiederkehrende Angreifende schnell detektieren lassen.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

Das BSI hat folgende Dokumente zum Themenfeld APT veröffentlicht:

- Advanced Persistent Threats - Teil 4 Reaktion - Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung
- Common Criteria Protection Profile for Remote-Controlled Browsers Systems (ReCoBS): BSI-PP-0040

Das CERT-EU hat das weiterführende Dokument „CERT-EU Security Whitepaper 2014-007: Kerberos Golden Ticket Protection: Mitigating Pass-the-Ticket on Active Directory“ zum Themenfeld APT veröffentlicht.



# DER.3.1 Audits und Revisionen

## 1. Beschreibung

### 1.1. Einleitung

Audits und Revisionen sind grundlegend für jedes erfolgreiche Managementsystem für Informationssicherheit (ISMS). Nur wenn etablierte Sicherheitsmaßnahmen und -prozesse regelmäßig daraufhin überprüft werden, ob sie noch wirksam, vollständig, angemessen und aktuell sind, lässt sich der Gesamtzustand der Informationssicherheit beurteilen. Audits und Revisionen sind somit ein Werkzeug, um ein angemessenes Sicherheitsniveau festzustellen, zu erreichen und aufrechtzuerhalten. Durch Audits und Revisionen ist es möglich, Sicherheitsmängel und Fehlentwicklungen zu erkennen und entsprechende Gegenmaßnahmen zu ergreifen.

Als Audit (audire = hören, zuhören) wird eine systematische, unabhängige Prüfung von Aktivitäten und deren Ergebnissen bezeichnet. Dabei wird geprüft, ob definierte Anforderungen wie Normen, Standards oder Richtlinien eingehalten werden. In einer Revision (revidieren = kontrollieren, prüfen) wird untersucht, ob Dokumente, Zustände, Gegenstände oder Vorgehensweisen korrekt, wirksam und angemessen sind. Im Gegensatz zum Audit muss die Revision nicht unbedingt unabhängig erfolgen. Zudem kann die Revision im Sinne einer Wartung auch bereits die Nachbesserung umfassen.

### 1.2. Zielsetzung

Der Baustein DER.3.1 *Audits und Revisionen* definiert Anforderungen an Audits und Revisionen mit dem Ziel, die Informationssicherheit in einer Institution zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und Sicherheitsmaßnahmen und -prozesse zu optimieren.

### 1.3. Abgrenzung und Modellierung

Der Baustein ist auf den gesamten Informationsverbund anzuwenden. Das betrifft interne Audits (Erstparteien-Audits) und Revisionen sowie Audits bei Dienstleistenden der Institution (Zweitparteien-Audits) oder anderen Institutionen, mit denen die Institution eine Partnerschaft eingegangen ist. Zertifizierungsaudits (Drittparteien-Audits) werden in diesem Baustein nicht berücksichtigt.

Ebenso wird die für Bundesbehörden verpflichtende IS-Revision nicht betrachtet. Diese wird im Baustein DER 3.2 *Revisionen auf Basis des Leitfadens IS-Revision* behandelt.

## 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 DER.3.1 *Audits und Revisionen* von besonderer Bedeutung.

### 2.1. Unzureichende oder nicht planmäßige Umsetzung von Sicherheitsmaßnahmen

Das Schutzniveau einer Institution hängt davon ab, dass Sicherheitsmaßnahmen vollständig und korrekt umgesetzt werden. Insbesondere in der kritischen Phase von Projekten oder unter bestimmten Rahmenbedingungen kann es aber vorkommen, dass Sicherheitsmaßnahmen temporär ausgesetzt werden. Wird dann vergessen, sie wieder zu reaktivieren, kann ein zu niedriges Sicherheitsniveau entstehen.

### 2.2. Wirkungslose oder nicht wirtschaftliche Umsetzung von Sicherheitsmaßnahmen

Werden Sicherheitsmaßnahmen umgesetzt, ohne dabei bestimmte Aspekte aus der Praxis zu berücksichtigen, sind die Maßnahmen eventuell wirkungslos. Beispielsweise ist es sinnlos, den Eingangsbereich mit Drehkreuzen abzusperren, wenn Mitarbeitende das Gebäude einfach durch einen offenen Seiteneingang betreten können.

Ebenso können Einzelmaßnahmen ergriffen werden, die wirtschaftlich nicht sinnvoll sind. So ist für den Schutz von Informationen mit einer normalen Vertraulichkeit ein sauber implementiertes Rechte- und Rollenkonzept besser geeignet und wirtschaftlicher als eine komplexe, zertifikatsbasierte Verschlüsselung des Fileservers.

### 2.3. Unzureichende Umsetzung des ISMS

In vielen Institutionen überprüft der oder die Informationssicherheitsbeauftragte selbst, ob Sicherheitsmaßnahmen umgesetzt wurden. Oft wird darüber aber die Prüfung des eigentlichen ISMS vergessen, insbesondere da dies durch unabhängige Dritte erfolgen sollte. Dadurch könnten die Prozesse eines ISMS ineffizient oder nicht angemessen umgesetzt sein. In der Folge kann das Sicherheitsniveau der Institution beeinträchtigt werden.

### 2.4. Unzureichende Qualifikation der Prüfenden

Sind die Personen, die ein Audit oder eine Revision durchführen sollen, nicht ausreichend qualifiziert oder bereiten sich ungenügend auf die Prüfungen vor, schätzen sie den Sicherheitszustand einer Institution möglicherweise falsch ein. Dies könnte zu fehlenden oder sogar falschen Korrekturmaßnahmen im Prüfbericht führen. Im schlimmsten Fall hat dies dann eine zu hohe und damit nicht wirtschaftliche bzw. eine zu niedrige und damit sehr risikobehaftete Absicherung der Informationen zur Folge.

### 2.5. Fehlende langfristige Planung

Werden Audits und Revisionen nicht langfristig und zentral geplant, kann es passieren, dass einzelne Bereiche sehr häufig und andere überhaupt nicht geprüft werden. Dadurch ist es nur sehr schwer oder gar nicht möglich, den Sicherheitszustand des Informationsverbunds einzuschätzen.

## 2.6. Fehlende Planung und Abstimmung bei der Durchführung eines Audits

Wenn ein Audit mangelhaft geplant und nicht ausreichend mit der Institution abgestimmt wurde, sind während der Vor-Ort-Prüfung eventuell nicht alle benötigten Personen anwesend. Dadurch lassen sich dann möglicherweise einzelne Bereiche überhaupt nicht auditieren. Auch wenn die Termine für die einzelnen Bereiche zu eng gesetzt wurden, könnte die Untersuchung nur oberflächlich durchgeführt werden, weil zu wenig Zeit eingeplant wurde.

## 2.7. Fehlende Abstimmung mit der Personalvertretung

In Audits und Revisionen können auch Aspekte geprüft werden, aus denen sich Rückschlüsse auf die Leistung von Mitarbeitenden ziehen lassen. Somit könnten diese Prüfungen als Leistungsbeurteilung gewertet werden. Wird die Personalvertretung nicht beteiligt, kann dies zu Verstößen gegen das geltende Mitbestimmungsrecht führen.

## 2.8. Absichtliches Verschweigen von Abweichungen

Mitarbeitende könnten befürchten, dass bei der Prüfung ihre Fehler aufgedeckt werden, und darum versuchen, Sicherheitsprobleme zu kaschieren. Dadurch könnte ein falsches Bild über den tatsächlichen Status quo vermittelt werden.

# 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.3.1 *Audits und Revisionen* 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	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Auditteam, Institutionsleitung

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.

### DER.3.1.A1 Definition von Verantwortlichkeiten (B) [Institutionsleitung]

Die Institutionsleitung MUSS eine Person benennen, die dafür zuständig ist, Audits bzw. Revisionen zu planen und zu initiieren. Dabei MUSS die Institutionsleitung darauf achten, dass keine Interessenkonflikte entstehen.

Die Institution MUSS die Ergebnisse der Audits und Revisionen dazu verwenden, um die Sicherheitsmaßnahmen zu verbessern.

### **DER.3.1.A2 Vorbereitung eines Audits oder einer Revision (B)**

Vor einem Audit oder einer Revision MUSS die Institution den Prüfgegenstand und die Prüfungsziele festlegen. Das betroffene Personal MUSS unterrichtet werden. Abhängig vom Untersuchungsgegenstand MUSS die Personalvertretung über das geplante Audit oder die geplante Revision informiert werden.

### **DER.3.1.A3 Durchführung eines Audits (B) [Auditteam]**

Bei einem Audit MUSS das Auditteam prüfen, ob die Anforderungen aus Richtlinien, Normen, Standards und anderen relevanten Vorgaben erfüllt sind. Die geprüfte Institution MUSS die Anforderungen kennen.

Das Auditteam MUSS bei jedem Audit eine Dokumentenprüfung sowie eine Vor-Ort-Prüfung durchführen. Beim Vor-Ort-Audit MUSS das Auditteam sicherstellen, dass es niemals selbst aktiv in Systeme eingreift und keine Handlungsanweisungen zu Änderungen am Prüfgegenstand erteilt.

Das Auditteam MUSS sämtliche Ergebnisse eines Audits schriftlich dokumentieren und in einem Auditbericht zusammenfassen. Der Auditbericht MUSS der zuständigen Stelle in der Institution zeitnah übermittelt werden.

### **DER.3.1.A4 Durchführung einer Revision (B)**

Bei einer Revision MUSS das Revisionsteam prüfen, ob die Anforderungen vollständig, korrekt, angemessen und aktuell umgesetzt sind. Die Institution MUSS festgestellte Abweichungen so schnell wie möglich korrigieren. Die jeweiligen Revisionen MÜSSEN mit einer Änderungsverfolgung dokumentiert 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.

### **DER.3.1.A5 Integration in den Informationssicherheitsprozess (S)**

Die Institution SOLLTE eine Richtlinie zur internen ISMS-Auditierung vorgeben. Außerdem sollte sie eine Richtlinie zur Lenkung von Korrekturmaßnahmen erstellen. Die Richtlinien SOLLTEN vorgeben, dass regelmäßige Audits und Revisionen ein Teil des Sicherheitsprozesses sind und durch diesen initiiert werden.

Der oder die ISB SOLLTE sicherstellen, dass die Ergebnisse der Audits und Revisionen in das ISMS zurückfließen und dieses verbessern. Der oder die ISB SOLLTE die durchgeführten Audits und Revisionen und deren Ergebnisse in den regelmäßigen Bericht an die Institutionsleitung aufnehmen. Auch SOLLTE dort festgehalten werden, welche Mängel beseitigt wurden und wie die Qualität verbessert wurde.

### **DER.3.1.A6 Definition der Prüfungsgrundlage und eines einheitlichen Bewertungsschemas (S)**

Die Institution SOLLTE eine einheitliche Prüfungsgrundlage für Audits festlegen. Für die Bewertung der Umsetzung von Anforderungen SOLLTE ein einheitliches Bewertungsschema festgelegt und dokumentiert werden.

### **DER.3.1.A7 Erstellung eines Auditprogramms (S)**

Der oder die ISB SOLLTE ein Auditprogramm für mehrere Jahre aufstellen, das alle durchzuführenden Audits und Revisionen erfasst. Für das Auditprogramm SOLLTEN Ziele definiert werden, die sich insbesondere aus den Institutionszielen sowie aus den Informationssicherheitszielen ableiten.



Der oder die ISB SOLLTE Reserven für unvorhergesehene Ereignisse in der jährlichen Ressourcenplanung vorsehen. Das Auditprogramm SOLLTE einem eigenen kontinuierlichen Verbesserungsprozess unterliegen.

### **DER.3.1.A8 Erstellung einer Revisionsliste (S)**

Der oder die ISB SOLLTE eine oder mehrere Revisionslisten pflegen, die den aktuellen Stand der Revisionsobjekte sowie die geplanten Revisionen dokumentieren.

### **DER.3.1.A9 Auswahl eines geeigneten Audit- oder Revisionsteams (S)**

Die Institution SOLLTE für jedes Audit bzw. für jede Revision ein geeignetes Team zusammenstellen. Es SOLLTE eine Person benannt werden, die das Audit oder die Revision leitet. Diese SOLLTE die Gesamtverantwortung für die Durchführung der Audits bzw. der Revisionen tragen.

Die Größe des Audit- bzw. Revisionsteams SOLLTE dem Prüfbereich entsprechen. Die Institution SOLLTE insbesondere die Kompetenzanforderungen der Prüft Themen sowie die Größe und die örtliche Verteilung des Prüfbereichs berücksichtigen. Die Mitglieder des Audit- bzw. Revisionsteams SOLLTEN angemessen qualifiziert sein.

Die Neutralität des Auditteams SOLLTE sichergestellt werden. Darüber hinaus SOLLTE auch das Revisionsteam unabhängig sein. Werden externe Dienstleistende mit einem Audit oder einer Revision beauftragt, SOLLTEN diese auf ihre Unabhängigkeit hin überprüft und zur Verschwiegenheit verpflichtet werden.

### **DER.3.1.A10 Erstellung eines Audit- oder Revisionsplans (S) [Auditteam]**

Vor einem Audit oder einer größeren Revision SOLLTE ein Audit- bzw. Revisionsplan erstellt werden. Bei Audits SOLLTE der Auditplan Teil des abschließenden Auditberichts sein. Der Auditplan SOLLTE während des gesamten Audits fortgeschrieben und bei Bedarf angepasst werden. Kleinere Revisionen SOLLTEN anhand der Revisionsliste geplant werden.

Die Institution SOLLTE genügend Ressourcen für das Audit- bzw. Revisionsteam vorsehen.

### **DER.3.1.A11 Kommunikation und Verhalten während der Prüfungen (S) [Auditteam]**

Das Auditteam bzw. Revisionsteam SOLLTE klare Regelungen dafür aufstellen, wie das Audit- bzw. Revisionsteam und die Mitarbeitenden der zu prüfenden Institution bzw. Abteilung miteinander Informationen austauschen. Das Auditteam SOLLTE durch geeignete Maßnahmen sicherstellen, dass die bei einem Audit ausgetauschten Informationen auch vertraulich und integer bleiben.

Personen, die das Audit begleiten, SOLLTEN NICHT die Prüfungen beeinflussen. Zudem SOLLTEN sie zur Vertraulichkeit verpflichtet werden.

### **DER.3.1.A12 Durchführung eines Auftaktgesprächs (S) [Auditteam]**

Das Auditteam bzw. das Revisionsteam SOLLTE ein Auftaktgespräch mit den betreffenden Ansprechpartnern oder Ansprechpartnerinnen führen. Das Audit- bzw. Revisionsverfahren SOLLTE erläutert und die Rahmenbedingungen der Vor-Ort-Prüfung abgestimmt werden. Die jeweiligen Verantwortlichen SOLLTEN dies bestätigen.

### **DER.3.1.A13 Sichtung und Prüfung der Dokumente (S) [Auditteam]**

Die Dokumente SOLLTEN durch das Auditteam anhand der im Prüfplan festgelegten Anforderungen geprüft werden. Alle relevanten Dokumente SOLLTEN daraufhin geprüft werden, ob sie aktuell, vollständig und nachvollziehbar sind. Die Ergebnisse der Dokumentenprüfung SOLLTEN dokumentiert werden. Die Ergebnisse SOLLTEN auch in die Vor-Ort-Prüfung einfließen, soweit dies sinnvoll ist.

**DER.3.1.A14 Auswahl von Stichproben (S) [Auditteam]**

Das Auditteam SOLLTE die Stichproben für die Vor-Ort-Prüfung risikoorientiert auswählen und nachvollziehbar begründen. Die ausgewählten Stichproben SOLLTEN dokumentiert werden. Wird das Audit auf der Basis von Baustein-Zielobjekten und Anforderungen durchgeführt, SOLLTEN diese anhand eines vorher definierten Verfahrens ausgewählt werden. Bei der Auswahl von Stichproben SOLLTEN auch die Ergebnisse vorangegangener Audits berücksichtigt werden.

**DER.3.1.A15 Auswahl von geeigneten Prüfmethoden (S) [Auditteam]**

Das Auditteam SOLLTE für die jeweils zu prüfenden Sachverhalte geeignete Methoden einsetzen. Außerdem SOLLTE darauf geachtet werden, dass alle Prüfungen verhältnismäßig sind.

**DER.3.1.A16 Ablaufplan der Vor-Ort-Prüfung (S) [Auditteam]**

Das Auditteam SOLLTE den Ablaufplan für die Vor-Ort-Prüfung gemeinsam mit der Institution erarbeiten. Die Ergebnisse SOLLTEN im Auditplan dokumentiert werden.

**DER.3.1.A17 Durchführung der Vor-Ort-Prüfung (S) [Auditteam]**

Zu Beginn der Vor-Ort-Prüfung SOLLTE das Auditteam ein Eröffnungsgespräch mit der betreffenden Institution führen. Danach SOLLTEN alle im Prüfplan festgelegten Anforderungen mit den vorgesehenen Prüfmethoden kontrolliert werden. Weicht eine ausgewählte Stichprobe vom dokumentierten Status ab, SOLLTE die Stichprobe bedarfsorientiert erweitert werden, bis der Sachverhalt geklärt ist. Nach der Prüfung SOLLTE das Auditteam ein Abschlussgespräch führen. Darin SOLLTE es kurz die Ergebnisse ohne Bewertung sowie die weitere Vorgehensweise darstellen. Das Gespräch SOLLTE protokolliert werden.

**DER.3.1.A18 Durchführung von Interviews (S) [Auditteam]**

Das Auditteam SOLLTE strukturierte Interviews führen. Die Fragen SOLLTEN knapp, präzise und leicht verständlich formuliert werden. Zudem SOLLTEN geeignete Fragetechniken eingesetzt werden.

**DER.3.1.A19 Überprüfung des Risikobehandlungsplans (S) [Auditteam]**

Das Auditteam SOLLTE prüfen, ob die verbleibenden Restrisiken für den Informationsverbund angemessen und tragbar sind. Es SOLLTE außerdem prüfen, ob sie verbindlich durch die Institutionsleitung getragen werden. Maßnahmen, die grundlegend zur Informationssicherheit der gesamten Institution beitragen, DÜRFEN NICHT in diese Risikoübernahme einfließen.

Das Auditteam SOLLTE stichprobenartig verifizieren, ob bzw. wie weit die im Risikobehandlungsplan festgelegten Maßnahmen umgesetzt sind.

**DER.3.1.A20 Durchführung einer Abschlussbesprechung (S) [Auditteam]**

Das Auditteam SOLLTE mit der auditierten Institution eine Abschlussbesprechung durchführen. Darin SOLLTEN die vorläufigen Auditergebnisse dargelegt werden. Die weiteren Tätigkeiten SOLLTEN vorgestellt werden.

**DER.3.1.A21 Auswertung der Prüfungen (S) [Auditteam]**

Nach der Vor-Ort-Prüfung SOLLTE das Auditteam die gewonnenen Informationen weiter konsolidieren und auswerten. Nachdem auch nachgeforderte Dokumentationen und zusätzliche Informationen ausgewertet wurden, SOLLTEN die geprüften Maßnahmen endgültig bewertet werden. Um die nachgeforderten Dokumentationen bereitstellen zu können, SOLLTE das Auditteam der Institution ein ausreichendes Zeitfenster gewähren. Dokumente, die bis zum vereinbarten Termin nicht eingegangen sind, SOLLTEN als nicht existent gewertet werden.

**DER.3.1.A22 Erstellung eines Auditberichts (S) [Auditteam]**

Das Auditteam SOLLTE die gewonnenen Erkenntnisse in einen Auditbericht überführen und dort nachvollziehbar dokumentieren.

Die geprüfte Institution SOLLTE sicherstellen, dass alle betroffenen Stellen innerhalb einer angemessenen Frist die für sie wichtigen und notwendigen Passagen des Auditberichts erhalten.

#### **DER.3.1.A23 Dokumentation der Revisionsergebnisse (S)**

Die Ergebnisse einer Revision SOLLTEN einheitlich durch das Revisionsteam dokumentiert werden.

#### **DER.3.1.A24 Abschluss des Audits oder der Revision (S) [Auditteam]**

Nach dem Audit bzw. der Revision SOLLTE das Auditteam alle relevanten Dokumente, Datenträger und IT-Systeme zurückgeben oder vernichten. Das SOLLTE mit der geprüften Institution abgestimmt werden. Aufbewahrungspflichten aus gesetzlichen oder anderen verbindlichen Anforderungen SOLLTEN hierbei entsprechend berücksichtigt werden. Der oder die ISB SOLLTE alle für das Audit- oder Revisionsteam genehmigten Zugriffe wieder deaktivieren oder löschen lassen.

Mit der geprüften Institution SOLLTE vereinbart werden, wie mit den Ergebnissen umzugehen ist. Dabei SOLLTE auch festgelegt werden, dass die Auditergebnisse nicht ohne Genehmigung der geprüften Institution an andere Institutionen weitergeleitet werden dürfen.

#### **DER.3.1.A25 Nachbereitung eines Audits (S)**

Die Institution SOLLTE die im Auditbericht oder bei einer Revision festgestellten Abweichungen oder Mängel in einer angemessenen Zeit abstellen. Die durchzuführenden Korrekturmaßnahmen inklusive Zeitpunkt und Zuständigkeiten SOLLTEN dokumentiert werden. Auch abgeschlossene Korrekturmaßnahmen SOLLTEN dokumentiert werden. Die Institution SOLLTE dazu ein definiertes Verfahren etablieren und einsetzen.

Gab es schwerwiegende Abweichungen oder Mängel, SOLLTE das Audit- bzw. Revisionsteam überprüfen, ob die Korrekturmaßnahmen durchgeführt wurden.

#### **DER.3.1.A26 Überwachen und Anpassen des Auditprogramms (S)**

Das Auditprogramm SOLLTE kontinuierlich überwacht und angepasst werden, sodass Termine, Auditziele, Auditinhalte und die Auditqualität eingehalten werden.

Mithilfe der bestehenden Anforderungen an das Auditprogramm und mit den Ergebnissen der durchgeführten Audits SOLLTE überprüft werden, ob das Auditprogramm angemessen ist. Bei Bedarf SOLLTE es angepasst werden.

#### **DER.3.1.A27 Aufbewahrung und Archivierung von Unterlagen zu Audits und Revisionen (S)**

Die Institution SOLLTE Auditprogramme sowie Unterlagen zu Audits und Revisionen entsprechend den regulatorischen Anforderungen nachvollziehbar und revisionssicher ablegen und aufbewahren. Dabei SOLLTE sichergestellt werden, dass lediglich berechnigte Personen auf Auditprogramme und Unterlagen zugreifen können. Die Institution SOLLTE die Auditprogramme und Unterlagen nach Ablauf der Aufbewahrungsfrist sicher vernichten.

### **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.

#### **DER.3.1.A28 ENTFALLEN (H)**

Diese Anforderung ist entfallen.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

Die International Organization for Standardization hat in der Norm „ISO 19011:2011“ Richtlinien zur Auditierung von Managementsystemen beschrieben.

Die International Organization for Standardization hat in der Norm „ISO ISO/IEC 27007:2011“ Richtlinien zur Auditierung eines ISMS beschrieben.

Das Information Security Forum hat im Dokument „The Standard of Good Practice for Information Security“ Richtlinien zur Auditierung eines ISMS beschrieben.



# DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision

## 1. Beschreibung

### 1.1. Einleitung

Eine besondere Form der Revision ist die Informationssicherheitsrevision (IS-Revision) auf Basis des Dokuments *Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz* (kurz „Leitfaden IS-Revision“).

Der „Leitfaden IS-Revision“ ist ein vom BSI veröffentlichtes Dokument, das die Vorgehensweise der IS-Revision beschreibt. Bundesbehörden sind dazu verpflichtet, ihr Managementsystem für Informationssicherheit (ISMS) durch IS-Revisionen zu überprüfen. Andere Institutionen können, anstelle einer regulären IT-Revision, eine IS-Revision auf Basis des Leitfadens durchführen, wenn sie die Umsetzung ihres ISMS überprüfen wollen.

Die IS-Revision auf Basis des Leitfadens zeichnet sich durch einen ganzheitlichen Ansatz aus. Das bedeutet, dass vom Aufbau einer Informationssicherheitsorganisation über Personalaspekte bis hin zur Konfiguration von IT-Systemen und -Anwendungen alle Ebenen eines ISMS geprüft werden. Dabei werden die Wirtschaftlichkeit und Ordnungsmäßigkeit, die bei klassischen IT-Revisionen im Vordergrund stehen, nur nachrangig betrachtet. Die Informationssicherheit (einschließlich der Angemessenheit der Sicherheitsmaßnahmen) ist somit das wesentliche Prüfkriterium der IS-Revision.

Die IS-Revision ist ein wesentlicher Bestandteil eines erfolgreichen Informationssicherheitsmanagements. Denn nur wenn die etablierten Maßnahmen und die Prozesse zur Informationssicherheit regelmäßig überprüft werden, kann beurteilt werden, ob diese wirksam umgesetzt, vollständig, aktuell und angemessen sind. Die IS-Revision ist somit ein geeignetes Werkzeug, um ein angemessenes Sicherheitsniveau in einer Institution festzustellen, zu erreichen, zu erhalten und kontinuierlich zu verbessern.

Die Hauptaufgabe der IS-Revision ist es, die Leitung der Institution, das IS-Management-Team und insbesondere den oder die ISB so zu unterstützen und zu begleiten, dass diese ein möglichst hohes Niveau der Informationssicherheit in der Institution erreichen können.

## 1.2. Zielsetzung

Der Baustein definiert Anforderungen an eine IS-Revision mit dem Ziel, die Informationssicherheit in einer Institution zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und die Sicherheitsmaßnahmen und -prozesse zu optimieren.

## 1.3. Abgrenzung und Modellierung

Der Baustein ist immer dann anzuwenden, wenn eine Institution dazu verpflichtet ist, Revisionen auf Basis des „Leitfadens IS-Revision“ durchzuführen oder diese freiwillig durchführen will. Der Baustein ist auf den gesamten Informationsverbund anzuwenden.

Es wird nicht berücksichtigt, wie sich die IS-Revision in eine bereits bestehende, übergeordnete Prüforganisation einer Institution (z. B. interne Revision) integrieren lässt. Der Baustein DER.3.2 *Revisionen auf Basis des Leitfadens IS-Revision* ist eine konkrete Ausgestaltung der im Baustein DER.3.1 *Audits und Revisionen* allgemein beschriebenen Anforderungen. Institutionen, die den vorliegenden Baustein umsetzen, müssen den Baustein DER.3.1 *Audits und Revisionen* nicht mehr umsetzen, da dessen Anforderungen vollständig in diesem Baustein enthalten sind.

Die IS-Revision und die Zertifizierung eines ISMS nach ISO 27001 auf der Basis von IT-Grundschutz ergänzen sich gegenseitig. IS-Revisionen können den Weg zur Zertifizierung begleiten und im Gegensatz hierzu bereits bei der Initiierung des Sicherheitsprozesses in der Institution durchgeführt werden. Sie zeigen der Institution auf, wo dringender Handlungsbedarf besteht und welche Sicherheitsmängel vorrangig bearbeitet werden sollten. Sind einzelne Informationsverbünde der Institution nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert, sollten Re-Zertifizierung und IS-Revision für diese Informationsverbünde nach Möglichkeit zusammen durchgeführt werden. Erkenntnisse aus Überwachungsaudits oder den Zertifizierungsverfahren können für die IS-Revision genutzt werden.

Liegt für die gesamte Institution ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz vor, lösen die im Zertifizierungsverfahren geforderten Überwachungsaudits die IS-Revisionen ab.

Die Vorschriften des Geheimschutzes und der Verschlusssachenanweisung des Bundes (VSA) bleiben unberührt und gelten unabhängig von den Anforderungen dieses Bausteins.

## 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 DER.3.2 *Revisionen auf Basis des Leitfadens* von besonderer Bedeutung.

### 2.1. Verstoß gegen die Vorgaben des UP Bund

Der „Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (UP Bund 2017) ist als Leitlinie für Informationssicherheit in der Bundesverwaltung festgelegt. Somit befinden sich Bundesbehörden in einem ressortübergreifenden Management für Informationssicherheit, bei dem jede Behörde dafür verantwortlich ist, ihr spezifisches Sicherheitskonzept zu erstellen und umzusetzen. Nicht nur die Behörden des Bundes, sondern auch andere Institutionen können durch gesetzliche, vertragliche oder anderweitige Regelungen verpflichtet sein, den UP Bund 2017 umzusetzen. Der UP Bund 2017 legt dabei ausdrücklich fest, dass die Standards des BSI zur Informationssicherheit und zum IT-Grundschutz sowie die darin beschriebene Vorgehensweise der Standard-Absicherung als Mindestanforderung umgesetzt werden müssen. Weiterhin legt der UP Bund 2017 verbindlich fest, dass alle verpflichteten Institutionen den Stand des eigenen ISMS, z. B. durch eine geeignete IS-Revision, regelmäßig überprüfen und dabei den „Leitfaden für die

*Informationssicherheitsrevision*“ anwenden müssen. Geschieht dies nicht, verstoßen diese Institutionen gegen die Vorgaben des UP Bund.

## **2.2. Aussetzen von Sicherheitsmaßnahmen**

Das Sicherheitsniveau von Institutionen wird davon beeinflusst, ob Sicherheitsmaßnahmen vollständig und korrekt umgesetzt werden. Insbesondere in der kritischen Phase von Projekten oder unter bestimmten Rahmenbedingungen werden Sicherheitsmaßnahmen häufig temporär ausgesetzt. Teilweise wird dann jedoch vergessen, sie wieder zu reaktivieren, sodass ein zu niedriges Sicherheitsniveau bestehen bleibt.

## **2.3. Wirkungslose oder nicht wirtschaftliche Umsetzung von Sicherheitsmaßnahmen**

Werden Sicherheitsmaßnahmen umgesetzt, ohne dabei vorhandene Praxisaspekte zu berücksichtigen, sind diese Maßnahmen unter Umständen wirkungslos. So ist es zum Beispiel sinnlos, einen Eingangsbereich mit Drehkreuzen abzusperren, wenn die Mitarbeitenden das Gebäude stattdessen durch einen offenen Seiteneingang betreten können.

Ebenso kann es passieren, dass Einzelmaßnahmen ergriffen werden, die wirtschaftlich nicht sinnvoll sind. So ist für den Schutz von Informationen mit einem normalen Schutzbedarf bezüglich der Vertraulichkeit ein angemessen implementiertes Rechte- und Rollenkonzept sinnvoller und wirtschaftlicher als der Aufbau einer komplexen, zertifikatsbasierten Verschlüsselung auf dem Fileserver.

## **2.4. Unzureichende Umsetzung des Managementsystems für Informationssicherheit**

In vielen Institutionen überprüft der oder die ISB selbst, ob Sicherheitsmaßnahmen umgesetzt werden. Oft wird in diesem Zusammenhang die Prüfung des eigentlichen ISMS vergessen, da der oder die ISB als Teil des ISMS nicht unparteilich ist. Folglich könnten die Prozesse eines ISMS ineffizient oder nicht angemessen umgesetzt worden sein, was zu einem ungewollt niedrigen Sicherheitsniveau der Institution geführt haben könnte.

## **2.5. Unzureichende Qualifikation des Prüfteams**

Ist das Prüfteam nicht ausreichend qualifiziert oder bereitet sich ungenügend auf die Prüfungen vor, kann es während einer IS-Revision eventuell den Sicherheitszustand einer Institution falsch einschätzen. Unter Umständen empfiehlt es dann in seinem Prüfbericht nicht die nötigen oder sogar die falschen Korrekturmaßnahmen. In diesem Fall kann es passieren, dass die Informationen unwirtschaftlich oder sehr risikobehaftet geschützt werden.

## **2.6. Befangenheit interner IS-Revisionsteams**

Innerhalb von Institutionen können IS-Revisionsteams aus internem Personal gebildet werden. Sind diese Teams nicht ausreichend von anderen Abläufen abgegrenzt, könnten sie beeinflusst oder befangen sein. Dies ist insbesondere dann der Fall, wenn Mitglieder des IS-Revisionsteams an der Planung oder Umsetzung des ISMS beteiligt sind oder waren.

## **2.7. Fehlende langfristige Planung**

Werden IS-Revisionen nicht langfristig und zentral geplant, kann es passieren, dass einzelne Organisationseinheiten einer Institution sehr häufig und andere überhaupt nicht geprüft werden.

Auch ist es möglich, dass Veränderungen am ISMS nicht ausreichend untersucht werden, wenn Prüfungen nur unregelmäßig durchgeführt werden. In diesem Fall ist es nur sehr schwer oder gar nicht möglich, den Sicherheitszustand des gesamten Informationsverbunds geeignet zu bewerten.

## 2.8. Mangelhafte Planung und Abstimmung bei der Durchführung von IS-Revisionen

Wenn eine IS-Revision mangelhaft geplant und nicht mit dem zuständigen Personal der Institution abgestimmt wurde, sind während der Vor-Ort-Prüfung eventuell nicht die richtigen Personen verfügbar. Folglich lassen sich möglicherweise einzelne Bereiche überhaupt nicht prüfen. Auch wenn die Termine für die Prüfung der einzelnen Bereiche zu eng gesetzt wurden und nicht genügend Zeit eingeplant wurde, könnte es passieren, dass die Institution nur oberflächlich geprüft wird.

## 2.9. Fehlende Abstimmung mit der Personalvertretung

Im Rahmen von IS-Revisionen können auch Aspekte geprüft werden, aus denen Rückschlüsse gezogen werden könnten, wie sich Personen bei ihrer Arbeit verhalten und wie leistungsfähig sie sind. Somit könnten diese Prüfungen als Verhaltens- und Leistungskontrolle gewertet werden. Wird die Personalvertretung nicht mit einbezogen, kann die Vor-Ort-Prüfung verzögert oder sogar abgebrochen werden.

## 2.10. Absichtliches Verschweigen von Abweichungen oder Problemen

Personen könnten befürchten, dass bei einer IS-Revision ihre eigenen Fehler aufgedeckt werden. Um dies zu vermeiden, könnten sie Sicherheitsprobleme kaschieren und so ein falsches Bild über den tatsächlichen Sicherheitsstand vermitteln. So blieben Sicherheitsmängel unentdeckt und könnten nicht korrigiert werden. Darüber hinaus könnte die Institutionsleitung das mit diesem Sicherheitsmangel einhergehende Risiko falsch einschätzen.

## 2.11. Vertraulichkeitsverlust von schützenswerten Informationen

Während einer IS-Revision werden vertrauliche Informationen (z. B. Schwachstellen und Angriffsmöglichkeiten) durch das IS-Revisionsteam erhoben. Auch werden gegebenenfalls Defizite in der Informationssicherheit der geprüften Institution benannt. Werden diese Mängel unberechtigten Dritten bekannt, könnten sie dazu benutzt werden, die Institution anzugreifen oder in einen schlechten Ruf zu bringen.

# 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.3.2 *Revisionen auf Basis des Leitfadens IS-Revision* 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	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	IS-Revisionsteam, Institutionsleitung

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.

#### **DER.3.2.A1 Benennung von Verantwortlichen für die IS-Revision (B) [Institutionsleitung]**

Die Institution MUSS eine verantwortliche Person für die IS-Revision benennen. Diese MUSS die IS-Revisionen planen, initiieren und die Ergebnisse nachverfolgen.

#### **DER.3.2.A2 Erstellung eines IS-Revisionshandbuches (B)**

Für die IS-Revision MUSS ein IS-Revisionshandbuch erstellt werden, das die angestrebten Ziele, einzuhaltende gesetzliche Vorgaben, Informationen über die Organisation, die Ressourcen und die Rahmenbedingungen enthält. Außerdem MUSS darin die Archivierung der Dokumentation beschrieben sein. Das Handbuch MUSS von der Leitungsebene verabschiedet werden.

#### **DER.3.2.A3 Definition der Prüfungsgrundlage (B)**

Die BSI-Standards 200-1 bis 200-3 sowie das IT-Grundschutz-Kompendium MÜSSEN die Prüfungsgrundlagen für die IS-Revision sein. Dabei SOLLTE die Standard-Absicherung des IT-Grundschutzes verwendet werden. Diese Prüfungsgrundlagen MÜSSEN allen Beteiligten bekannt sein.

#### **DER.3.2.A4 Erstellung einer Planung für die IS-Revision (B)**

Wenn die Institution nicht nach ISO 27001 auf Basis von IT-Grundschutz zertifiziert ist, MUSS sichergestellt werden, dass mindestens alle drei Jahre eine IS-Kurz- oder Querschnitts-Revision durchgeführt wird. Darüber hinaus SOLLTEN weitere Revisionen eingeplant werden, falls der Informationsverbund wesentlich verändert wird.

Es SOLLTE eine mehrjährige Grobplanung für die Revisionsvorhaben erstellt werden. Diese SOLLTE dann durch eine jährliche Detailplanung konkretisiert werden.

#### **DER.3.2.A5 Auswahl eines geeigneten IS-Revisionsteams (B)**

Es MUSS ein aus mindestens zwei Personen bestehendes IS-Revisionsteam zusammengestellt oder beauftragt werden. Dem IS-Revisionsteam MUSS ein uneingeschränktes Informations- und Einsichtnahmerecht für seine Tätigkeit eingeräumt werden. Bei eigenen IS-Revisionsteams MÜSSEN die einzelnen Mitglieder unparteilich sein. Die Mitglieder eines IS-Revisionsteams DÜRFEN NICHT an der Planung oder Umsetzung des ISMS beteiligt sein oder gewesen sein.

#### **DER.3.2.A6 Vorbereitung einer IS-Revision (B) [IS-Revisionsteam]**

Es MUSS ein IS-Revisionsteam mit einer IS-Revision beauftragt werden. Das IS-Revisionsteam MUSS festlegen, welche Referenzdokumente für eine IS-Revision benötigt werden. Die zu prüfende Institution MUSS das Sicherheitskonzept und alle weiteren erforderlichen Dokumente an das IS-Revisionsteam übergeben.

#### **DER.3.2.A7 Durchführung einer IS-Revision (B) [IS-Revisionsteam]**

Im Rahmen einer IS-Revision MÜSSEN eine Dokumenten- und eine Vor-Ort-Prüfung durch das IS-Revisionsteam durchgeführt werden. Sämtliche Ergebnisse dieser beiden Prüfungen MÜSSEN dokumentiert und in einem IS-Revisionsbericht zusammengefasst werden.

Bevor erstmalig eine IS-Querschnittsrevision durchgeführt wird, MUSS als IS-Revisionsverfahren eine IS-Kurzrevision ausgewählt werden. Die IS-Kurzrevision MUSS mit positivem Votum abgeschlossen werden, bevor eine IS-Querschnittsrevision durchgeführt wird.

### **DER.3.2.A8 Aufbewahrung von IS-Revisionsberichten (B)**

Die Institution MUSS den IS-Revisionsbericht und die diesem zugrundeliegenden Referenzdokumente mindestens für zehn Jahre ab Zustellung des Berichts sicher aufbewahren, sofern keine anders lautenden Gesetze oder Verordnungen gelten. Die Institution MUSS sicherstellen, dass lediglich berechnete Personen auf die IS-Revisionsberichte und die Referenzdokumente zugreifen können.

## **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.

### **DER.3.2.A9 Integration in den Informationssicherheitsprozess (S)**

Die Institution SOLLTE sicherstellen, dass IS-Revisionen ein Teil des Sicherheitsprozesses sind. Außerdem SOLLTEN die Ergebnisse von IS-Revisionen in das ISMS zurückfließen und zu dessen Verbesserung beitragen.

Weiter SOLLTEN die Ergebnisse der IS-Revisionen sowie die Aktivitäten, um Mängel zu beseitigen und um die Qualität zu verbessern, in den regelmäßigen Bericht des oder der ISB an die Institutionsleitung aufgenommen werden.

### **DER.3.2.A10 Kommunikationsabsprache (S)**

Es SOLLTE klar geregelt werden, wie Informationen zwischen dem IS-Revisionsteam und der zu prüfenden Institution auszutauschen sind. So SOLLTE sichergestellt werden, dass diese Informationen vertraulich und integer bleiben.

### **DER.3.2.A11 Durchführung eines Auftaktgesprächs für eine IS-Querschnittsrevision (S) [IS-Revisionsteam]**

Für eine IS-Querschnittsrevision SOLLTE ein Auftaktgespräch zwischen dem IS-Revisionsteam und der zu prüfenden Institution durchgeführt werden. Darin SOLLTEN folgende Inhalte besprochen werden:

- Die Erläuterung und Darstellung des IS-Revisionsverfahrens,
- die Vorstellung der Institution (Arbeitsschwerpunkte und Überblick der eingesetzten IT) sowie
- die Übergabe der Referenzdokumente an das IS-Revisionsteam.

### **DER.3.2.A12 Erstellung eines Prüfplans (S) [IS-Revisionsteam]**

Vor einer IS-Revision SOLLTE das IS-Revisionsteam einen Prüfplan erstellen. Ist es während der IS-Revision notwendig, die geplanten Abläufe zu erweitern oder anderweitig anzupassen, SOLLTE der Prüfplan entsprechend angepasst werden. Der Prüfplan SOLLTE zudem in den abschließenden IS-Revisionsbericht aufgenommen werden.

Bei der IS-Kurzrevision SOLLTE die verbindlich festgelegte Prüfthemenliste des BSI an die Stelle des Prüfplans treten.

### **DER.3.2.A13 Sichtung und Prüfung der Dokumente (S) [IS-Revisionsteam]**

Bei der Dokumentenprüfung SOLLTE das IS-Revisionsteam die im Prüfplan festgelegten Anforderungen prüfen. Das IS-Revisionsteam SOLLTE überprüfen, ob alle relevanten Dokumente aktuell und vollständig sind. Bei der Prüfung auf Aktualität SOLLTE die Granularität der Dokumente berücksichtigt werden. Es SOLLTE darauf geachtet werden, dass alle wesentlichen Aspekte erfasst und geeignete Rollen zugewiesen wurden.

Weiter SOLLTE geprüft werden, ob die vorliegenden Dokumente und die darin getroffenen Entscheidungen nachvollziehbar sind. Die Ergebnisse der Dokumentenprüfung SOLLTEN dokumentiert werden und, soweit sinnvoll, in die Vor-Ort-Prüfung einfließen.

### **DER.3.2.A14 Auswahl der Zielobjekte und der zu prüfenden Anforderungen (S) [IS-Revisionsteam]**

In einer IS-Querschnittsrevision oder IS-Partialrevision SOLLTE das IS-Revisionsteam anhand der Ergebnisse der Dokumentenprüfung die Baustein-Zielobjekte für die Vor-Ort-Prüfung auswählen. Der Baustein zum Informationssicherheitsmanagement (siehe ISMS.1 *Sicherheitsmanagement*) des IT-Grundschutz-Kompodiums einschließlich aller zugehörigen Anforderungen SOLLTE jedoch immer vollständig geprüft werden. Weitere dreißig Prozent der modellierten Baustein-Zielobjekte SOLLTEN risikoorientiert zur Prüfung ausgewählt werden. Die Auswahl SOLLTE nachvollziehbar dokumentiert werden. Von den so ausgewählten Baustein-Zielobjekten SOLLTEN dreißig Prozent der jeweiligen Anforderungen bei der IS-Revision geprüft werden.

Darüber hinaus SOLLTEN bei der Auswahl der zu prüfenden Baustein-Zielobjekte die bemängelten Anforderungen aus vorhergehenden IS-Revisionen berücksichtigt werden. Alle Anforderungen mit schwerwiegenden Sicherheitsmängeln aus vorhergehenden IS-Revisionen SOLLTEN mit geprüft werden.

### **DER.3.2.A15 Auswahl von geeigneten Prüfmethoden (S) [IS-Revisionsteam]**

Das IS-Revisionsteam SOLLTE sicherstellen, dass geeignete Prüfmethoden eingesetzt werden, um die zu prüfenden Sachverhalte zu ermitteln. Alle Prüfungen SOLLTEN verhältnismäßig sein.

### **DER.3.2.A16 Erstellung eines Ablaufplans für die Vor-Ort-Prüfung (S) [IS-Revisionsteam]**

Gemeinsam mit der zu prüfenden Institution SOLLTE das IS-Revisionsteam einen Ablaufplan für die Vor-Ort-Prüfung erarbeiten. Die Ergebnisse SOLLTEN zusammen mit dem IS-Prüfplan dokumentiert werden.

### **DER.3.2.A17 Durchführung der Vor-Ort-Prüfung (S) [IS-Revisionsteam]**

Bei der Vor-Ort-Prüfung SOLLTE das IS-Revisionsteam untersuchen und feststellen, ob die ausgewählten Maßnahmen die Anforderungen des IT-Grundschutzes angemessen und praxistauglich erfüllen.

Die Prüfung SOLLTE mit einem Eröffnungsgespräch beginnen. Danach SOLLTEN alle für die Prüfung ausgewählten Anforderungen des Prüfplans bzw. alle Themenfelder der Prüftemenliste überprüft werden. Dafür SOLLTEN die vorgesehenen Prüfmethoden angewandt werden. Werden bei einer ausgewählten Stichprobe Abweichungen zum dokumentierten Status festgestellt, SOLLTE die Stichprobe bedarfsorientiert erweitert werden, bis der Sachverhalt geklärt ist.

Während der Vor-Ort-Prüfung SOLLTEN das IS-Revisionsteam niemals aktiv in IT-Systeme eingreifen und auch keine Handlungsanweisungen zu Änderungen am Revisionsgegenstand erteilen.

Alle wesentlichen Sachverhalte und Angaben zu Quellen-, Auskunft- und Vorlage-Ersuchen sowie durchgeführten Besprechungen SOLLTEN schriftlich festgehalten werden.

In einem Abschlussgespräch SOLLTE das IS-Revisionsteam der geprüften Institution wesentliche Feststellungen kurz darstellen. Dabei SOLLTE das IS-Revisionsteam die Feststellungen nicht konkret bewerten, sondern Hinweise auf etwaige Mängel und die weitere Verfahrensweise geben. Auch dieses Abschlussgespräch SOLLTE protokolliert werden.

### **DER.3.2.A18 Durchführung von Interviews (S) [IS-Revisionsteam]**

Interviews durch das IS-Revisionsteam SOLLTEN strukturiert erfolgen. Fragen SOLLTEN knapp, präzise und leicht verständlich formuliert werden. Zudem SOLLTEN geeignete Fragetechniken eingesetzt werden.

### **DER.3.2.A19 Überprüfung der gewählten Risikobehandlungsoptionen (S) [IS-Revisionsteam]**

Das IS-Revisionsteam SOLLTE prüfen, ob die verbleibenden Restrisiken für den Informationsverbund angemessen und tragbar sind und ob sie verbindlich durch die Institutionsleitung getragen werden. Das IS-Revisionsteam SOLLTE stichprobenartig verifizieren, ob bzw. inwieweit die gewählten Risikobehandlungsoptionen umgesetzt sind.

### **DER.3.2.A20 Nachbereitung der Vor-Ort-Prüfung (S) [IS-Revisionsteam]**

Nach der Vor-Ort-Prüfung SOLLTEN die erhobenen Informationen weiter durch das IS-Revisionsteam konsolidiert und ausgewertet werden. Nachdem die eventuell nachgeforderten Dokumente, Dokumentationen und zusätzlichen Informationen ausgewertet wurden, SOLLTEN die geprüften Anforderungen endgültig bewertet werden.

### **DER.3.2.A21 Erstellung eines IS-Revisionsberichts (S) [IS-Revisionsteam]**

Das IS-Revisionsteam SOLLTE die gewonnenen Ergebnisse in einen IS-Revisionsbericht überführen und dort nachvollziehbar dokumentieren. Eine Entwurfsversion des Berichts SOLLTE der geprüften Institution vorab übermittelt werden. Es SOLLTE verifiziert werden, ob die durch das IS-Revisionsteam festgestellten Sachverhalte richtig aufgenommen wurden.

Die geprüfte Institution SOLLTE sicherstellen, dass alle betroffenen Stellen in der Institution innerhalb einer angemessenen Frist die für sie wichtigen und notwendigen Passagen des IS-Revisionsberichts erhalten. Insbesondere SOLLTEN die Inhalte an die Institutionsleitung, an die Verantwortlichen für die IS-Revision sowie den oder die ISB kommuniziert werden.

IS-Revisionsberichte SOLLTEN aufgrund der enthaltenen schützenswerten Informationen mit einer geeigneten Vertraulichkeitseinstufung versehen werden.

Es SOLLTE überlegt werden, die Ergebnisse der IS-Revision der Institutionsleitung vom IS-Revisionsteam in Form einer Präsentation vorzustellen.

### **DER.3.2.A22 Nachbereitung einer IS-Revision (S)**

Die im IS-Revisionsbericht festgestellten Abweichungen SOLLTEN in einer angemessenen Zeit durch die Institution korrigiert werden. Die durchzuführenden Korrekturmaßnahmen SOLLTEN mit Zuständigkeiten, Umsetzungstermin und dem jeweiligen Status dokumentiert sein. Die Umsetzung SOLLTE kontinuierlich nachverfolgt und der Umsetzungsstatus fortgeschrieben werden.

Grundsätzlich SOLLTE geprüft werden, ob ergänzende IS-Revisionen notwendig sind. Die Institution SOLLTE die Grob- und Detailplanung zur IS-Revision anpassen.

## **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.

### **DER.3.2.A23 ENTFALLEN (H)**

Diese Anforderung ist entfallen.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt in seinem Leitfaden „Informationssicherheitsrevision: Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz“, wie eine IS-Revision durchgeführt werden muss.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt in seinem Dokument „Verbindliche Prüfthemen für die IS-Kurzrevision“, welche Themen bei einer IS-Kurzrevision geprüft werden sollen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit einem „Revisionshandbuch zur Informationssicherheit nach UP Bund“ ein Musterhandbuch für die IS-Revision bereit.

Das Bundesministerium des Inneren (BMI) beschreibt in der Verschlusssachenanweisung (VSA), welche Vorgaben beim Umgang mit Verschlusssachen zu beachten sind.



# DER.4 Notfallmanagement

## 1. Beschreibung

### 1.1. Einleitung

In Notfällen müssen Institutionen weiter auf Informationen zugreifen können, um einen Geschäftsprozess, ein IT-System oder eine Fachaufgabe wiederherstellen zu können. Um die Informationssicherheit auch in einem Notfall aufrechterhalten zu können, sollten deshalb entsprechende Prozesse geplant, etabliert und überprüft werden.

Nur wenn geplant und organisiert vorgegangen wird, ist eine optimale Notfallvorsorge und Notfallbewältigung möglich. Ein professioneller Prozess zum Notfallmanagement reduziert die Auswirkungen eines Notfalls und sichert somit den Betrieb und Fortbestand der Institution. Es sind geeignete Maßnahmen zu identifizieren und umzusetzen, durch die zeitkritischen Geschäftsprozesse und Fachaufgaben zum einen robuster und ausfallsicherer werden. Zum anderen sollten diese Maßnahmen ermöglichen, einen Notfall schnell und zielgerichtet zu bewältigen.

Die Aufrechterhaltung der Informationssicherheit im Notfall ist in ein übergreifendes Notfallmanagement, idealerweise in ein Notfallmanagementsystem, einzubinden. Das Notfallmanagement hat jedoch einen eigenen Prozessverantwortlichen, den Notfallbeauftragten oder die Notfallbeauftragte, der oder die sich mit dem oder der ISB abstimmt.

### 1.2. Zielsetzung

Ziel dieses Bausteins ist es, Anforderungen zu beschreiben, um die Informationssicherheit in Institutionen selbst in kritischen Situationen zu gewährleisten. Dazu sind die entsprechenden Maßnahmen in ein ganzheitliches Notfallmanagement einzubetten. Zudem sind alle Aspekte zu betrachten, die erforderlich sind, um die Informationssicherheit auch bei Schadensereignissen oder Notfällen aufrechterhalten zu können. Dies reicht von der Planung bis zur Überprüfung aller Prozesse.

### 1.3. Abgrenzung und Modellierung

Der Baustein DER.4 *Notfallmanagement* ist immer für den gesamten Informationsverbund einmal anzuwenden.

Tritt ein Schadensereignis ein, müssen die richtigen Informationen vollständig und korrekt zur Verfügung stehen. Im vorliegenden Baustein werden weder Kriterien noch Prozesse erläutert, anhand derer die Verantwortlichen entscheiden können, ob ein Notfall vorliegt oder nicht. Die Entscheidung

darüber wird getroffen, während der Sicherheitsvorfall behandelt wird (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

Krisen werden im Rahmen eines eigenen Krisenmanagements betrachtet und in diesem Baustein nur als Schnittstelle behandelt, z. B. im Rahmen der weiteren Eskalation von Notfällen. Weiterführende Informationen zu den einzelnen Phasen des Notfallmanagements sowie der Abgrenzung des Notfallmanagements zum Krisenmanagement sind im BSI-Standard 100-4 „Notfallmanagement“ enthalten.

## **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 DER.4 *Notfallmanagement* von besonderer Bedeutung.

### **2.1. Personalausfall**

Fällt Personal aus, kann das schnell bedeuten, dass eine Institution ihre Fachaufgaben und Geschäftsprozesse nicht mehr ausführen kann. Die Gründe für einen Personalausfall können vielfältig sein. Durch Keime in der Kantine oder einen Streik können beispielsweise viele Mitarbeitende gleichzeitig ausfallen. Auch der Tod eines Mitarbeitenden kann zu Ausfällen oder Beeinträchtigungen von wichtigen Geschäftsprozessen oder Fachaufgaben führen. Zudem könnten relevante Informationen zum Wiederanlauf des Geschäftsprozesses oder der IT-Systeme nicht mehr zugänglich sein. Oft verfügen einzelne Personen über spezifisches Fachwissen (Kopfmonopole), sodass ein Schaden auch dann eintreten kann, wenn der Personalausfall zahlenmäßig nur sehr gering ist.

### **2.2. Ausfall von IT-Systemen**

Fallen Komponenten eines IT-Systems aus, z. B. durch defekte Hardware oder einen Stromausfall, kann der gesamte IT-Betrieb gestört werden. Dadurch ist die Verfügbarkeit der jeweiligen Informationen und damit auch des jeweiligen Geschäftsprozesses gefährdet. Zudem können wichtige Informationen, die für Wiederanlaufmaßnahmen benötigt werden, nicht zur Verfügung stehen.

### **2.3. Ausfall eines Weitverkehrsnetzes (WAN)**

Die Ursachen für den Ausfall eines Weitverkehrsnetzes (Wide Area Network, WAN) können vielfältig sein. Daher ist es möglich, dass sich ein Netzausfall lediglich auf einzelne Benutzende, einen Anbietenden oder eine bestimmte Region auswirkt. Häufig stören solche Ausfälle nur kurz und betreffen dann nur die Geschäftsprozesse und Fachaufgaben, die eine entsprechend hohe Verfügbarkeit des WAN benötigen. Es gibt aber auch immer wieder längere Ausfälle, die massive Probleme in der Kommunikation und Erreichbarkeit nach sich ziehen können.

### **2.4. Ausfall eines Gebäudes**

Gebäude können unvorhergesehen unbenutzbar werden, z. B. weil sie durch Feuer, Sturm, Hochwasser, Erdbeben oder eine Explosion teilweise oder vollständig zerstört wurden. Ein Gebäude kann aber auch ausfallen, weil die Polizei oder die Feuerwehr das Umfeld sperrt und das Gebäude nicht mehr betreten werden kann oder verlassen werden muss, etwa weil Strom, Wasser, Abwasser, Heizung oder Klimatisierung über einen gewissen Zeitraum nicht mehr funktionieren.

## 2.5. Ausfall einer Lieferung oder Dienstleistung

Sind Institutionen von Dienstleistungen abhängig, kann dies schnell zu Unterbrechungen der eigenen betrieblichen Kontinuität führen, wenn die dienstleistende oder liefernde Institution teilweise oder vollständig ausfällt. Wird beispielsweise zur Produktion die Lieferung eines bestimmten Werkstoffs benötigt und diese Lieferung fällt aus, so ist möglicherweise die gesamte Produktion gefährdet. Aber auch der Ausfall eines extern bereitgestellten Dienstes, wie z. B. einer Cloud oder auch E-Mail, kann den eigenen Betrieb sehr stark einschränken, bzw. sogar komplett unterbrechen. Dies gefährdet insbesondere kritische Geschäftsprozesse und Fachaufgaben.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.4 *Notfallmanagement* 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	Notfallbeauftragte
Weitere Zuständigkeiten	Informationssicherheitsbeauftragte (ISB), Vorgesetzte, Institutionsleitung, Personalabteilung

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.

### 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.

#### DER.4.A1 Erstellung eines Notfallhandbuchs (S)

Es SOLLTE ein Notfallhandbuch erstellt werden, in dem die wichtigsten Informationen zu

- Rollen,
- Sofortmaßnahmen,
- Alarmierung und Eskalation sowie
- Kommunikations-, grundsätzlichen Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungsplänen

enthalten sind. Zuständigkeiten und Befugnisse SOLLTEN zugewiesen, kommuniziert und im Notfallhandbuch festgehalten werden. Es SOLLTE sichergestellt sein, dass im Notfall entsprechend geschultes Personal zur Verfügung steht. Es SOLLTE regelmäßig durch Tests und Übungen überprüft werden, ob die im Notfallhandbuch beschriebenen Maßnahmen auch wie vorgesehen funktionieren.



Es SOLLTE regelmäßig geprüft werden, ob das Notfallhandbuch noch aktuell ist. Gegebenenfalls SOLLTE es aktualisiert werden. Es SOLLTE auch im Notfall zugänglich sein. Das Notfallhandbuch SOLLTE um Verhaltensregeln für spezielle Fälle ergänzt werden, z. B. Brand. Die Regeln SOLLTEN allen Mitarbeitenden bekanntgegeben werden.

### **DER.4.A2 Integration von Notfallmanagement und Informationssicherheitsmanagement (S) [Informationssicherheitsbeauftragte (ISB)]**

Die Prozesse im Sicherheitsmanagement SOLLTEN mit dem Notfallmanagement abgestimmt werden (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

## **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.

### **DER.4.A3 Festlegung des Geltungsbereichs und der Notfallmanagementstrategie (H) [Institutionsleitung]**

Der Geltungsbereich für das Notfallmanagementsystem SOLLTE eindeutig festgelegt werden. Die Institutionsleitung SOLLTE eine Notfallmanagementstrategie festlegen, welche die angestrebten Ziele und das Risikoakzeptanzniveau darlegen.

### **DER.4.A4 Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Institutionsleitung (H) [Institutionsleitung]**

Die Institutionsleitung SOLLTE eine Leitlinie zum Notfallmanagement verabschieden. Diese SOLLTE die wesentlichen Eckpunkte des Notfallmanagements enthalten. Die Leitlinie zum Notfallmanagement SOLLTE regelmäßig überprüft und gegebenenfalls überarbeitet werden. Sie SOLLTE allen Mitarbeitenden bekanntgegeben werden.

### **DER.4.A5 Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement (H) [Institutionsleitung]**

Die Rollen für das Notfallmanagement SOLLTEN für die Gegebenheiten der Institution angemessen festgelegt werden. Dies SOLLTE mit den Aufgaben, Pflichten und Kompetenzen der Rollen schriftlich dokumentiert werden. Es SOLLTEN für alle Rollen im Notfallmanagement qualifizierte Mitarbeitende benannt werden. Die Organisationsstruktur im Notfallmanagement SOLLTE regelmäßig darauf überprüft werden, ob sie praxistauglich, effektiv und effizient ist.

### **DER.4.A6 Bereitstellung angemessener Ressourcen für das Notfallmanagement (H) [Institutionsleitung]**

Die finanziellen, technischen und personellen Ressourcen für die angestrebten Ziele des Notfallmanagements SOLLTEN angemessen sein. Der oder die Notfallbeauftragte bzw. das Notfallmanagement-Team SOLLTE über genügend Zeit für die Aufgaben im Notfallmanagement verfügen.

### **DER.4.A7 Erstellung eines Notfallkonzepts (H) [Institutionsleitung]**

Alle kritischen Geschäftsprozesse und Ressourcen SOLLTEN identifiziert werden, beispielsweise mit einer Business-Impact-Analyse (BIA). Es SOLLTEN die wichtigsten relevanten Risiken für die kritischen Geschäftsprozesse und Fachaufgaben sowie deren Ressourcen identifiziert werden. Für jedes identifizierte Risiko SOLLTE entschieden werden, welche Risikostrategien zur Risikobehandlung eingesetzt werden sollen. Es SOLLTEN Kontinuitätsstrategien entwickelt werden, die einen

Wiederanlauf und eine Wiederherstellung der kritischen Geschäftsprozesse in der geforderten Zeit ermöglichen. Es SOLLTE ein Notfallkonzept erstellt werden. Es SOLLTEN solche Notfallpläne und Maßnahmen entwickelt und implementiert werden, die eine effektive Notfallbewältigung und eine schnelle Wiederaufnahme der kritischen Geschäftsprozesse ermöglichen. Im Notfallkonzept SOLLTE die Informationssicherheit berücksichtigt und entsprechende Sicherheitskonzepte für die Notfalllösungen entwickelt werden.

#### **DER.4.A8 Integration der Mitarbeitenden in den Notfallmanagement-Prozess (H) [Vorgesetzte, Personalabteilung]**

Alle Mitarbeitenden SOLLTEN regelmäßig für das Thema Notfallmanagement sensibilisiert werden. Zum Notfallmanagement SOLLTE es ein Schulungs- und Sensibilisierungskonzept geben. Die Mitarbeitenden im Notfallmanagement-Team SOLLTEN regelmäßig geschult werden, um die benötigten Kompetenzen aufzubauen.

#### **DER.4.A9 Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse (H) [Institutionsleitung]**

Es SOLLTE sichergestellt werden, dass Aspekte des Notfallmanagements in allen Geschäftsprozessen und Fachaufgaben der Institution berücksichtigt werden. Die Prozesse, Vorgaben und Verantwortlichkeiten im Notfallmanagement SOLLTEN mit dem Risikomanagement und Krisenmanagement abgestimmt werden.

#### **DER.4.A10 Tests und Notfallübungen (H) [Institutionsleitung]**

Alle wesentlichen Sofortmaßnahmen und Notfallpläne SOLLTEN in angemessener Weise regelmäßig und anlassbezogen getestet und geübt werden. Der zeitliche Rahmen und die fachliche Abdeckung aller Übungen SOLLTEN übergreifend in einem Übungsplan dokumentiert werden. Im Notfallmanagement SOLLTEN ausreichend Ressourcen für die Planung, Konzeption, Durchführung und Auswertung der Tests und Übungen bereitgestellt werden.

#### **DER.4.A11 ENTFALLEN (H)**

Diese Anforderung ist entfallen.

#### **DER.4.A12 Dokumentation im Notfallmanagement-Prozess (H)**

Der Ablauf des Notfallmanagement-Prozesses, die Arbeitsergebnisse der einzelnen Phasen und wichtige Entscheidungen SOLLTEN dokumentiert werden. Ein festgelegtes Verfahren SOLLTE sicherstellen, dass diese Dokumente regelmäßig aktualisiert werden. Darüber hinaus SOLLTE der Zugriff auf die Dokumentation auf autorisierte Personen beschränkt werden.

#### **DER.4.A13 Überprüfung und Steuerung des Notfallmanagement-Systems (H) [Institutionsleitung]**

Die Institutionsleitung SOLLTE sich regelmäßig anhand von Managementberichten über den Stand des Notfallmanagements informieren. Sie SOLLTE so das Notfallmanagement-System regelmäßig überprüfen, bewerten und gegebenenfalls korrigieren.

#### **DER.4.A14 Regelmäßige Überprüfung und Verbesserung der Notfallmaßnahmen (H) [Institutionsleitung]**

Alle Notfallmaßnahmen SOLLTEN regelmäßig oder bei größeren Änderungen daraufhin überprüft werden, ob sie noch eingehalten und korrekt umgesetzt werden. Es SOLLTE geprüft werden, ob sie sich noch dazu eignen, die definierten Ziele zu erreichen.

Dabei SOLLTE untersucht werden, ob technische Maßnahmen korrekt implementiert und konfiguriert wurden und ob organisatorische Maßnahmen effektiv und effizient umgesetzt sind. Bei Abweichungen SOLLTEN die Ursachen für die Mängel ermittelt und Verbesserungsmaßnahmen veranlasst werden. Diese Ergebnisübersicht SOLLTE von der Institutionsleitung freigegeben werden. Es SOLLTE zudem

ein Prozess etabliert werden, der steuert und überwacht, ob und wie die Verbesserungsmaßnahmen umgesetzt werden. Verzögerungen SOLLTEN frühzeitig an die Institutionsleitung gemeldet werden.

Es SOLLTE von der Institutionsleitung festgelegt sein, wie die Überprüfungen koordiniert werden. Die Überprüfungen SOLLTEN so geplant werden, dass kein relevanter Teil ausgelassen wird. Insbesondere SOLLTEN die im Bereich der Revision, der IT, des Sicherheitsmanagements, des Informationssicherheitsmanagements und des Notfallmanagements durchgeführten Überprüfungen miteinander koordiniert werden. Dazu SOLLTE geregelt werden, welche Maßnahmen wann und von wem überprüft werden.

#### **DER.4.A15 Bewertung der Leistungsfähigkeit des Notfallmanagementsystems (H) [Institutionsleitung]**

Es SOLLTE regelmäßig bewertet werden, wie leistungsfähig und effektiv das Notfallmanagement-System ist. Als Grundlage SOLLTEN Mess- und Bewertungskriterien wie z. B. Leistungskennzahlen definiert werden. Diese Messgrößen SOLLTEN regelmäßig ermittelt und mit geeigneten vorangegangenen Werten, mindestens aber mit den Vorjahreswerten, verglichen werden. Weichen die Werte negativ ab, SOLLTEN die Ursachen ermittelt und Verbesserungsmaßnahmen definiert werden. Die Ergebnisse der Bewertung SOLLTEN an die Leitung berichtet werden.

Die Leitung SOLLTE entscheiden, mit welchen Maßnahmen das Notfallmanagement weiterentwickelt werden soll. Alle Entscheidungen der Institutionsleitung SOLLTEN dokumentiert und die bisherigen Aufzeichnungen aktualisiert werden.

#### **DER.4.A16 Notfallvorsorge- und Notfallreaktionsplanung für ausgelagerte Komponenten (H) [Institutionsleitung]**

Bei der Notfallvorsorge- und Notfallreaktionsplanung für ausgelagerte Komponenten SOLLTE regelmäßig das Notfallmanagement der liefernden oder dienstleistenden Institution in den unterzeichneten Verträgen geprüft werden. Auch SOLLTEN die Abläufe in Notfalltests und -übungen mit der liefernden oder bereitstellenden Institution abgestimmt und, wenn angemessen, gemeinsam durchgeführt werden.

Die Ergebnisse und Auswertungen SOLLTEN regelmäßig zwischen der Institutionsleitung und den liefernden Institutionen oder Dienstleistenden ausgetauscht werden. In den Auswertungen SOLLTEN auch eventuelle Verbesserungsmaßnahmen enthalten sein.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 „Information technology - Security techniques - Information security management systems - Requirements“ im Anhang A17 „Information security aspects of business continuity management“ Vorgaben für die Sicherstellung der Informationssicherheit im Notfall.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 22301:2012 „Societal security - Business continuity management systems - Requirements“ ein Rahmenwerk für ein Business Continuity Management (BCM), in das die Anforderungen aus der oben genannten Norm ISO/IEC 27001:2013 beispielsweise integriert werden können.

Der BSI-Standard 100-4 „Notfallmanagement“ beschreibt, wie ein BCM etabliert, aufrechterhalten und kontinuierlich verbessert werden kann.

Das vom BSI veröffentlichte Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4 (UMRA) beinhaltet weitere Hilfsmittel, um die Etablierung eines BCMSs zu erleichtern.

Zusätzlich bietet der Webkurs „Notfallmanagement“ nach dem BSI-Standard 100-4 eine Einführung in das Thema.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ in der Kategorie BC - Business Continuity - Vorgaben zur Business Continuity. Es fordert dort unter anderem auch, dass die Kontinuitätsstrategie mit der Informationssicherheitsstrategie abgestimmt sein soll.

Das National Institute of Standards and Technology (NIST) stellt in seiner Special Publication 800-34, Rev. 1, „Contingency Planning Guide for Federal Information Systems“, einen Leitfaden zur Erstellung einer Kontinuitätsplanung von (bundesstaatlichen) Informationssystemen zur Verfügung, der auch die Informationssicherheit berücksichtigt. Zusätzlich liefert dieses Dokument auch Informationen über Zusammenhänge zwischen einer solchen Kontinuitätsplanung von Informationssystemen und anderen Arten von sicherheits- und notfallmanagementbezogenen Kontinuitätsplänen, z. B. einem Business Continuity Plan.