Bundesamt
für Sicherheit in der
Informationstechnik

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 Einbruchsversuch 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 Einbruchsursache 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 auswählt 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.