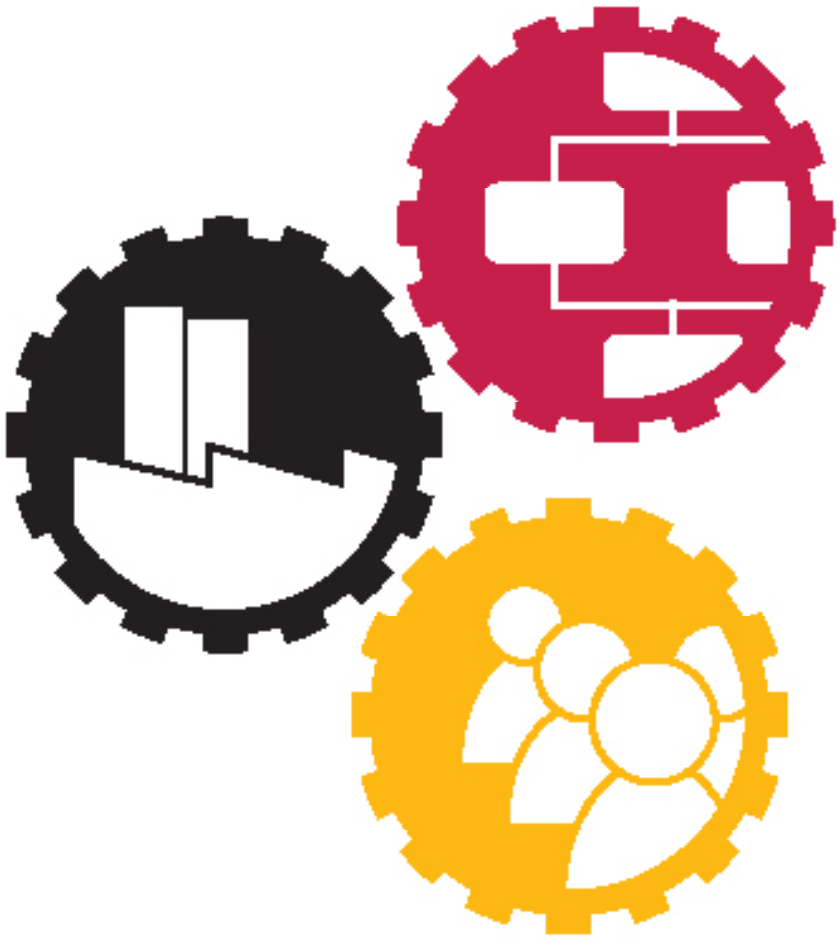
Bundesamt für Verfassungsschutz

Bundesamt für Sicherheit in der Informationstechnik

ASW Bundesverband

Wirtschaftsgrundschutz

Baustein ÜA2 Sicherheitsvorfallmanagement



1 Relevanzentscheidung für diesen Baustein

1. Verfügt die Institution über **Schutzgüter**, die für den Erfolg der Institution wesentlich sind?
2. Verfügt die Institution bereits über ein **Notfall- und Krisenmanagement**?
3. Verfügt die Institution bereits über einen **Prozess zur Behandlung von IT-Sicherheitsvorfällen**?
4. Verfügt die Institution bereits über einen **Prozess zur Behandlung von Sicherheitsvorfällen** rund um die genutzten Gelände und Gebäude sowie für deren Infrastrukturen?

Eine **zeitnahe Erkennung** von und die **angemessene Reaktion** auf Vorfälle sind die elementare **Grundlage**, um die schutzwürdigen Werte einer Institution wirksam abzusichern.

Das hierfür geeignete Verfahren ist in diesem Baustein „Sicherheitsvorfallmanagement“ beschrieben.

Nicht Bestandteil dieses Bausteins ist die Behandlung IT-basierter Sicherheitsvorfälle. Diese folgt grundsätzlich den gleichen Strukturen zur Erkennung und Bewältigung, ist aber oftmals bereits implementiert. Als Referenz bietet sich hier das **IT-Grundschutzhandbuch** mit den entsprechenden Bausteinen und Maßnahmen an. Eine enge **Verzahnung und** idealerweise **Integration** der **institutionsspezifischen Strukturen ist empfehlenswert**.

Dieser Baustein richtet sich an die Leitung der Institution, die die

Gesamtverantwortung für ein Reaktionsmanagement als zentrales Element in einem **modernen Risikomanagement** trägt.

Die Behandlung von Sicherheitsvorfällen ist von übergreifender Bedeutung für ein **umfassendes und ganzheitliches Sicherheitsmanagement**. Aufgrund der Vielfältigkeit besitzt das Sicherheitsvorfallmanagement oftmals **Schnittstellen zu** diversen anderen **Managementsystemen der Institution**. Diese sind bspw.:

1. Management von Wirtschaftskriminalität
2. Gebäudesicherheit
3. Personalwesen
4. IT-Störungs-/Sicherheitsvorfallmanagement
5. Notfallmanagement
6. Krisenmanagement

Zielsetzung Sicherheitsvorfallmanagement

Mit der Definition eines **einheitlichen Erkennungs-, Melde- und Behandlungsprozesses** stellt die Institution sicher, dass anhand definierter Schwellenwerte das **Schadenspotential** von Sicherheitsvorfällen frühzeitig erkannt und Gegenmaßnahmen eingeleitet werden können. Das **Sicherheitsvorfallmanagement** stellt somit das steuernde Bindeglied zwischen dem Regelbetrieb und dem Reaktionsmanagement, bestehend aus **Vorfall-, erweitertem Vorfall-**[1]**, Notfall- und Krisenmanagement** (vgl. Wirtschaftsgrundschutz Glossar), zur Verfügung.

In der nachfolgenden Abbildung wird dies verdeutlicht.

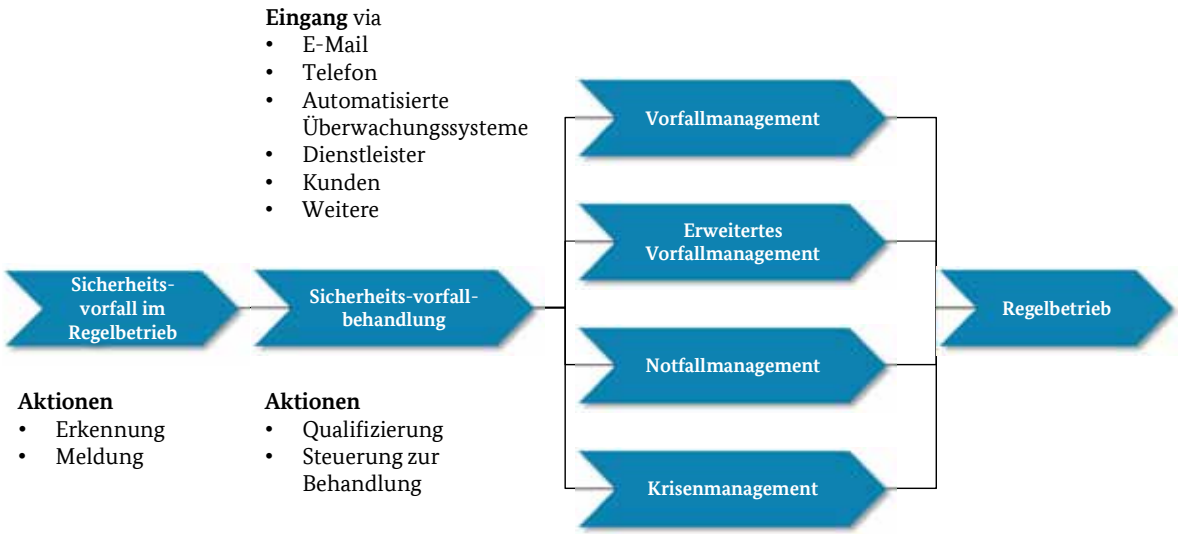


Abbildung 1: Übersicht Prozess Sicherheitsvorfallbehandlung

[1] Erweiterter Vorfall: Vorfälle, die aufgrund der Verletzung der Sicherheitsvorgaben, der erwarteten Dauer oder anderer Faktoren mit spezialisierten Reaktionsteams, aber dennoch als Vorfall, behandelt werden.

Die Institution setzt die Sicherheitsvorfallbehandlung so um, dass das gemeinsame Wirken oftmals getrennt umgesetzter Reaktionsprozesse ermöglicht wird. Auf diese Weise realisiert die Institution neben **Kostenvorteilen** eine **schnellere und zielgerichtete Reaktion**.

2 Beschreibung

Definition Vorfall

Vorfälle mit Auswirkungen auf und schädigenden Folgen für die beteiligten Personen oder den regulären Geschäftsbetrieb **können** trotz aller Sorgfalt **immer auftreten**. Die damit einhergehenden **Gefährdungen** der zentralen Werte der Institution (bspw. Mitarbeiter, Gäste und Partner, materielle und immaterielle Werte[2]) werden im Rahmen des Wirtschaftsgrundschutzes anhand ihres Schadenspotentials (Vorfall, Notfall und Krise) kategorisiert **und** die **Behandlung** eingetretener oder möglicher Gefährdungen **in diesem Baustein dargestellt**.

Vorfälle im Betrieb können trotz aller Sorgfalt immer auftreten. Einige der **Vorfälle verletzen** zudem **Sicherheitsvorgaben** und **bedürfen** deshalb der **besonderen Aufmerksamkeit durch die Institution**. Um die Sicherheit des laufenden Betriebs aufrechtzuerhalten, **plant und konzipiert** die Institution **im Vorfeld**, **wie** sie **mit** auftretenden **Sicherheitsvorfällen umgehen** wird.

Definition Sicherheitsvorfall

Beispielhafte Definition eines Sicherheitsvorfalls:
Als Sicherheitsvorfall wird eine bestehende oder drohende Abweichung vom definierten Sicherheitsniveau der Werte der Institution bezeichnet, die durch menschliches Fehlverhalten, technische Fehler, durch höhere Gewalt oder auch durch vorsätzliches Handeln herbeigeführt wurde.

Hierbei ist unerheblich, ob der Sicherheitsvorfall bereits ein unerwünschtes Ergebnis oder eine Auswirkung auf die Institution bewirkt oder nur das Potential dazu hat. Der **entscheidende Faktor** ist, **ob** die

[2] Vgl. Wirtschaftsgrundschutz Standard 2000-1, Kapitel 2.2.1.

definierten **Sicherheitsparameter**[3] der **Werte der Institution** bereits **negativ beeinflusst** wurden, es noch werden oder es werden können. **Typische Folgen von Sicherheitsvorfällen** können bspw. sein:

Folgen von Sicherheitsvorfällen

1. **Schädigung von Leib oder Leben** von Mitarbeitern, Kunden, Geschäftspartnern oder Besuchern
2. **Verlust oder Beschädigung von Eigentum** der Institution (insbesondere ihrer besonders schutzbedürftigen Werte)
3. **Schädigung des Ansehens** der Institution
4. sonstige **kriminelle Handlungen**
5. **Ausspähung oder Manipulation** von Informationen in elektronischer oder nicht elektronischer Form

Die hiermit bereits angedeutete **Komplexität der Sicherheitsvorfallbehandlung erfordert** eine der jeweiligen Institution **angemessene Organisations- und Prozessstruktur**. Diese gliedert sich ggf. an bereits etablierte **Vorfallbewältigungsprozesse** an. So aufgestellt ist die Institution in der Lage, schnell und effizient Sicherheitsvorfälle von klassischen Vorfällen zu unterscheiden und sie angemessen zu behandeln. Wird hierbei ein vorgegebenes und erprobtes Verfahren genutzt, können **Reaktionszeiten und mögliche Folgeschäden** oder weitere Eskalationen **minimiert** werden.

Mit der **Sicherheitsvorfallbehandlung** stellt die Institution sicher, dass **potentiell sicherheitsrelevante Vorfälle** aus verschiedenen Bereichen (bspw. einem Geschäftsbereich) **bei der Überschreitung definierter Schwellenwerte erkannt** werden. Sie **ermöglicht** damit auch ein **strukturiertes Sammeln sicherheitsrelevanter Informationen** sowie eine **einheitliche Bewertung** durch eine zentrale Instanz. Je nach **Klassifikation** des Vorfalls (bspw. Issue, Störung, Notfall oder Krise) erfolgt die **Eskalation** an die jeweils zuständigen Gremien. Dies sind die Geschäftsbereiche, die mit eigenen spezialisierten organisatorischen Einheiten eine Vorfallbehebung vornehmen, oder auch die Sonderorganisationsformen **Notfallstab** oder **Krisenstab**.

Das Management von Vorfällen verantwortet der jeweils betroffene Geschäftsbereich. Auch beim Management erweiterter Vorfälle verbleibt die Verantwortung im betroffenen Geschäftsbereich, es können aber zusätzlich **spezialisierte Reaktionsteams** eingebunden werden.

[3] Bspw. Verfügbarkeit, Integrität, Vertraulichkeit, aber auch Unversehrtheit.

Der betroffene Geschäftsbereich ist üblicherweise der, der für den betroffenen Wert unmittelbar verantwortlich ist.

Notfälle und **Krisen bewältigt** die **Institution** hingegen **mit Sonderorganisationsformen wie** einem **Notfall- oder Krisenstab**, denen die Institution zu diesem Zweck die notwendigen Kompetenzen und Verantwortlichkeiten überträgt (vergleiche Wirtschaftsgrundschutz Standard 2000-3). Im Unterschied zu Vorfällen erfordern Notfälle oder Krisen in der Regel Maßnahmen einer Geschäftsfortführungsplanung, um die Aufrechterhaltung betroffener kritischer Geschäftsprozesse zu ermöglichen. Krisen wiederum unterscheiden sich von Notfällen durch ihre Unvorhersagbarkeit, die damit einhergehende begrenzte Planbarkeit sowie durch die besondere Schwere der Auswirkungen auf die Institution.

Die **Institution richtet** eine **zentrale Instanz ein zur Entgegennahme von Meldungen von Sicherheitsvorfällen** (bspw. per E-Mail, Ticket oder Telefon). Die zentrale Instanz **qualifiziert die einzelnen Vorfälle** und **übergibt** sie dann **dem jeweils zuständigen Reaktionssystem** als Vorfall, Notfall oder Krise.

Dieser Baustein zeigt einen systematischen Weg auf, wie ein Konzept zur Behandlung von Sicherheitsvorfällen erstellt und dessen Umsetzung und Einbettung in einer Institution sichergestellt werden können.

3 Gefährdungslage

Sicherheitsvorfälle können **durch** eine **Vielzahl von Gefahren ausgelöst** werden. Da es sich bei der Sicherheitsvorfallbehandlung um ein **übergreifendes Verfahren für den systematischen Umgang mit Sicherheitsvorfällen** handelt, sind grundsätzlich alle in der Institution identifizierten Gefährdungen relevant.

In diesem Baustein werden daher die Gefährdungen betrachtet, die direkt mit der Sicherheitsvorfallbehandlung verbunden sind:

G 1 Fehlende Strukturen für den Umgang mit Sicherheitsvorfällen
G 2 Ungeeigneter Umgang mit Sicherheitsvorfällen
G 3 Nicht erkannte Sicherheitsvorfälle
G 4 Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen
G 5 Fehlerhafte oder unpassende Qualifizierung von Sicherheitsvorfällen
G 6 Ungeeigneter Betrieb der Meldestelle
G 7 Unzureichende Ausstattung der Meldestelle
G 8 Nicht wirksame Eskalationskette

4 Maßnahmen

Ziele der Sicherheitsvorfallbehandlung

Die Sicherheitsvorfallbehandlung hat im Wesentlichen folgende Ziele:

1. **Definition einer geeigneten Organisationsstruktur** einschließlich notwendiger Rollen oder Gremien, Aufgaben und Verantwortlichkeiten sowie von Informations- oder Eskalationsprozessen
2. **effiziente und zielgerichtete Methoden oder Verfahren sowie Hilfsmittel** zur strukturierten und möglichst einheitlichen Meldung, Analyse, Bearbeitung und Behandlung von Sicherheitsvorfällen
3. **Sicherstellung der Reaktions-, Entscheidungs- und Handlungsfähigkeit** bei Auftreten eines Sicherheitsvorfalls, um den Schaden für die Institution zu begrenzen
4. **Definition einer einheitlichen Bewertungsmatrix** zur Kategorisierung von Sicherheitsvorfällen
5. **Sicherstellung**, dass bei **Dienstleistern auftretende Sicherheitsvorfälle an die zentrale Instanz der Institution gemeldet** werden, wenn sie die Dienstleistung der Institution direkt oder indirekt betreffen

Die Institution beschreibt ihre Ziele und führt zu ihrer Erreichung die nachfolgend detailliert beschriebenen Maßnahmen entsprechend ihren individuellen Anforderungen ein.

Die Maßnahmen folgen hierbei dem Plan-Do-Check-Act-Regelkreis und unterteilen sich in diese drei wesentlichen Prozessblöcke:

1. Führungsprozess

2. Betriebsprozess (Planung, Umsetzung, Überprüfung, Verbesserung)
3. Berichts-/Kontrollwesen

Abbildung 2 stellt diese grafisch dar.

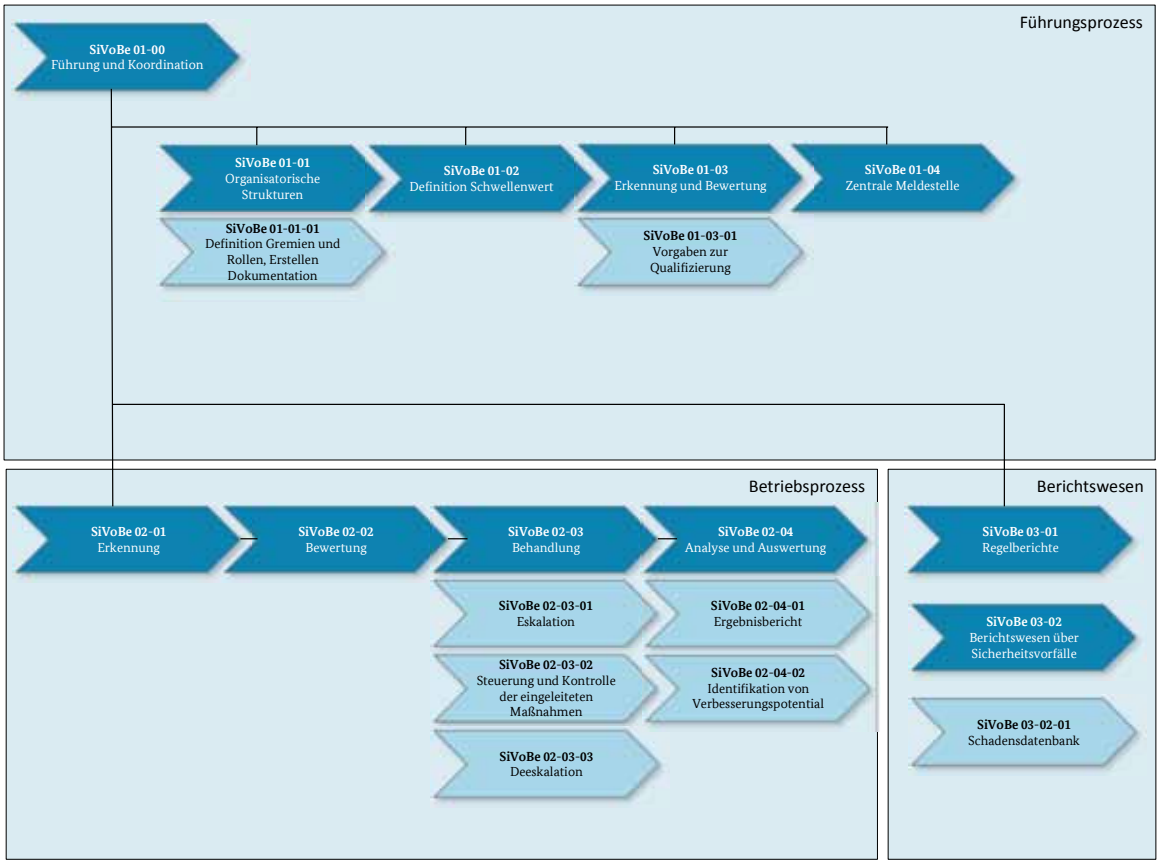


Abbildung 2: Der Prozess Sicherheitsvorfallbehandlung im Überblick

Maßnahmenkategorien

Die **Maßnahmen** dieses Bausteins sind in **drei Kategorien** eingeteilt. Sie richten sich **nach** dem **erforderlichen Detailgrad bzw.** der **gewünschten Ausprägung** (siehe Relevanzentscheidung) auf Basis der Anwendungsentscheidung gemäß Standard 2000-1:

A-Kategorie – Basismaßnahmen: unabdingbarer Wirtschaftsgrundschutz
B-Kategorie – Standardmaßnahmen: vollständiger Wirtschaftsgrundschutz
C-Kategorie – erweiterte Maßnahmen: erweiterter Schutz bei hohem Risikopotential

M 1 Schaffen der organisatorischen Strukturen (A)

Die **Sicherheitsvorfallbehandlung ist ein bereichs- und themenübergreifender Prozess**. In ihm sind in einer **zentralen Instanz** Maßnahmen aller betroffenen Organisationseinheiten (sowohl solcher, in denen Sicherheitsvorfälle entstehen können, als auch der zentral steuernden Einheit) zusammengeführt. Die relevanten Geschäftsbereiche sind über **eindeutige Schnittstellen und Informationswege** mit dieser zentralen Instanz verbunden. Hierfür schafft die Institution zunächst die organisatorischen Strukturen, bestehend aus

organisatorische Strukturen

1. Organisationsstruktur
2. Rollen und Verantwortlichkeiten
3. Prozesslandschaft
4. Verfahrensanweisungen
5. Vorgehensweisen und Methoden

Die Institution regelt, wer welche Verantwortung und Kompetenzen beim Auftreten von Sicherheitsvorfällen hat und durch wen welche Informationen weitergegeben werden.

Anmerkung: Die Organisationsstruktur umfasst verschiedene Gremien, die im Detail teilweise auch in anderen Bausteinen geregelt sind (bspw. Notfall- und Krisenmanagement). An dieser Stelle erfolgt daher nur eine Referenz auf andere mitwirkende Bausteine.

Die festgelegten Verfahrensanweisungen haben das Ziel, die Betroffenen zum richtigen Umgang mit den Auswirkungen der Sicherheitsvorfälle zu befähigen. Dies umfasst sowohl die **unverzügliche Meldung** an die festgelegte zentrale Instanz als auch die **weitere Behandlung** durch diese.

Die **Vorgehensweisen und Methoden der Sicherheitsvorfallbehandlung** umfassen Regelungen zu

Vorgehensweisen und Methoden der Vorfallbehandlung

1. Identifikation
2. Meldung
3. Bewertung
4. Eskalation
5. Behandlung von Sicherheitsvorfällen

Hierzu beschreibt die Institution in einem Regelwerk geeignete Prozesse. Sie macht diese den jeweils handelnden Rollen in geeigneter Weise bekannt. Neben der **Prozessdokumentation** erstellt die Institution für den Anwender **geeignete Hilfsmittel wie Alarm- und Eskalationsplan, Checklisten oder Schaubilder**. Dies erhöht das Verständnis für die Abläufe.

M 2 Erstellen einer Richtlinie zur Sicherheitsvorfallbehandlung (A)

Die Richtlinie **beschreibt** alle **zu implementierenden Informations- und Meldewege**, um eine **zielgerichtete und verzugslose Information, Alarmierung und Eskalation** für alle Sicherheitsvorfälle der Institution zu gewährleisten.

Darüber hinaus beschreibt die Richtlinie alle **Vorgehensweisen und Methoden für die Meldung, Alarmierung, Eskalation und Deeskalation** von Vorfällen sowie für die Bewältigung von Sicherheitsvorfällen.

Mindestanforderungen der Richtlinie

Die Richtlinie regelt **mindestens die folgenden Aspekte**:

1. Definition der Meldequellen
2. Definition der Meldestellen
3. meldepflichtige Sicherheitsvorfälle
4. Alarmierungsverfahren
5. Dokumentations- und Berichtswege
6. Definition der Reaktionsteams inkl. Aufgaben und Kompetenzen

Die Richtlinie beschreibt zudem alle **Schnittstellen zu den Reaktionsprozessen des Notfall- und Krisenmanagements** eindeutig.

M 3 Definieren spezialisierter Reaktionsteams (A)

Die s**achgemäße Behandlung von Sicherheitsvorfällen erfordert** nicht nur **betriebliches Fachwissen**. Oftmals sind **spezielle Kenntnisse** (bspw. Forensik) oder auch **Wissen über übergreifende Zusammenhänge** notwendig. Die Reaktionsteams wenden dieses Wissen unter Zeitdruck an und treffen schnelle Entscheidungen.

Aufgabe der Institution

Die **Institution definiert** ein oder mehrere **Reaktionsteams**, die mit der Behandlung eines Sicherheitsvorfalls betraut werden. Da ggf. nicht alle erforderlichen Fähigkeiten in einer Organisationseinheit vereint sind, sind Reaktionsteams **in der Regel bereichsübergreifend**.

Solche Teams können unter anderem die folgenden Aufgaben erfüllen:

1. **Sicherheitsvorfallbehandlungsteams** (fach- und institutionsspezifisch)
2. **Notfallteams** (fachspezifisch)
3. **Notfallstab** (institutionsspezifisch)
4. **Krisenstab** (institutionsspezifisch)

Je nach Art und Schweregrad des Vorfalls übernimmt das entsprechende Team die koordinierende und führende Funktion.

M 4 Definieren von Eskalationsstufen und Schwellenwerten (A)

Damit jeder Sicherheitsvorfall mit einer **angemessenen Priorität** und von der **richtigen Stelle** bearbeitet werden kann, entwickelt die Institution eine **Taxonomie**, mit der sie alle **Sicherheitsvorfälle bewertet und einstuft**.

Anhand dieser Einstufung wird festgestellt, ob ein Sicherheitsvorfall durch das **reguläre Vorfallmanagement** (und wenn ja durch welchen Geschäftsbereich) oder durch eines der **spezialisierten Reaktionsteams** zu behandeln ist.

Welches Team dabei zum Einsatz kommt, hängt einerseits von der **Eskalationsstufe** des Sicherheitsvorfalls, andererseits vom jeweils **überschrittenen Schwellenwert** ab.

Beispiele für Eskalationsstufen

Beispiele für Eskalationsstufen in Bezug auf die in Maßnahme 3 dargestellten Reaktionsteams sind:

Klassifikation	Reaktionsteam	Organisation
Vorfall	Fachbereichsteam	Vorfallmanagement
erweiterter Vorfall	Problemmanagementteam Sicherheitsvorfallbehandlungsteam	Problemmanagement Sicherheitsvorfall
Notfall	Notfallteam Notfallstab	Notfallmanagement
Krise	Krisenstab	Krisenmanagement

Tabelle 1: Beispiele für Eskalationsstufen in Bezug auf die in Maßnahme 3 dargestellten Reaktionsteams

Beispiele für Schwellenwerte

Einfache **Beispiele für Schwellenwerte** sind:

1. **Schweregrad** des Sicherheitsvorfalls
2. **Betroffenheit** der Sicherheitsvorgaben
3. **erwartete Störungszeit** des Sicherheitsvorfalls
4. zeitlicher **Verlauf einer Behebung**
5. **Öffentlichkeitswirksamkeit**

Jeden Sicherheitsvorfall bewertet die Institution hierbei immer in Bezug auf den betroffenen **Wert und** dessen im Vorfeld definierte **Schutzklasse**. Dies bedeutet, dass idealerweise für alle relevanten Werte Eskalationsstufen mit Schwellenwerten definiert sind, die so eine Qualifizierung erleichtern.

M 5 Definieren einer einheitlichen Methodik zur Qualifizierung von Sicherheitsvorfällen (B)

Aufgaben der Institution

Die Institution legt eine **einheitliche Methodik zur Qualifizierung** fest und dokumentiert diese. Sie stellt so sicher, dass **Sicherheitsvorfälle vergleichbar und nachvollziehbar** bewertet werden. Sie **berücksichtigt** hierbei auch **relevante Parameter der Außen- und Innenwirkung** des Sicherheitsvorfalls.

Anhand dieser Verfahrensweise entscheidet die Institution auf einheitlicher Basis, welche Eskalationsstufe gewählt wird.

M 6 Definieren meldepflichtiger Sicherheitsvorfälle (B)

Aus Effizienzgründen und zur Entlastung der eigentlichen Meldestel-

len erfolgt eine **Vordefinition von Sicherheitsvorfällen**.

Das Ergebnis der Vordefinition ist eine **kategorisierte Liste meldepflichtiger Sicherheitsvorfälle**, die eine noch schnellere Reaktion ermöglicht. Individuell zu bewerten sind bei Vorhandensein dieser Liste lediglich noch alle nicht in der Liste aufgeführten Vorfälle. Abbildung 3 stellt dies beispielhaft dar.

Abbildung 3: Beispielhafte Kategorisierung meldepflichtiger Sicherheitsvorfälle

Anmerkung: Auf die Kategorie „erweiterter Vorfall“ wurde hier bewusst verzichtet, da es sich dabei im Wesentlichen um einen Vorfall mit höherer Sicherheitsrelevanz, aber noch keinen Notfall handelt, was wiederum institutionsspezifisch definiert wird.

Im **Verfahren zur Definition** meldepflichtiger Sicherheitsvorfälle sind hierbei **mindestens** die **nachfolgend genannten Aspekte** zu beschreiben:

1. Klassifizierung
2. Priorisierung
3. Entscheidung (Entscheidungs- und Kontrollinstanz)

Innerhalb der Institution ist zu regeln und zu kommunizieren, dass **diese Sicherheitsvorfälle verpflichtend und formal der zentralen Meldestelle zu melden** sind.

M 7 Identifizieren und Definieren der Meldequellen (A)

Für die Behandlung von Sicherheitsvorfällen **erfasst** die Institution **alle relevanten Meldequellen**, die in **nachvollziehbaren und strukturierten Prozessen** die Sicherheitsvorfälle an **etablierte und/oder zentrale Meldestellen** leiten. Meldequellen sind hierbei all **diejenigen Stellen** einer Institution, **die Informationen über potentielle Vorfälle erhalten und erkennen können**. Als Meldequelle kommt daher eine **Vielzahl von Personengruppen, Funktionen und Systemen** in Betracht, bspw.:

1. automatisierte Überwachungssysteme
2. Datenschutzbeauftragter
3. Dienstleister, Geschäftspartner
4. Empfang und Telefonzentrale
5. Gebäudemanagement (bspw. Gefahrenmeldeanlagen, Gebäudeleittechnik)
6. IT-Support, IT-Monitoring, User Help Desk
7. Kunden
8. Medien
9. Mitarbeiter
10. öffentliche Stellen (bspw. Verwaltung, Polizei oder Feuerwehr)
11. Sicherheitsbeauftragter

Wichtig bei der Konzeption ist, dass **keine relevante Meldequelle ausgelassen** wird, da widrigenfalls mögliche Sicherheitsvorfälle nicht zeitnah erfasst werden könnten.

M 8 Identifizieren und Definieren der Meldestellen (A)

Die **Institution richtet** für die Aufnahme und Bearbeitung der von den Meldequellen gemeldeten Sicherheitsvorfälle eine **zentrale Meldestelle ein**. Aufgrund der **organisatorischen Struktur** der Institution bzw. der Aufgabe einer bestimmten Meldestelle (bspw. zum Melden doloser Handlungen) können **auch mehrere Meldestellen** zum Einsatz kommen. In diesem Fall dokumentiert die Institution die jeweilige Aufgabe und stellt sicher, dass **eingehende Meldungen** dennoch **einheitlich erfasst, weitergemeldet und behandelt** werden.

Als **Meldestellen** fungieren **typischerweise** der **User Help Desk**, eine **Whistleblower-Hotline**, das **Gebäudemanagement** und das **Sicherheitsmanagement**. Um die **Effizienz** der Meldestellen zu erhöhen, können diese Funktionen **zentralisiert** werden.

Die **Meldestelle** hat üblicherweise die nachfolgenden **Aufgaben**:

Aufgaben der Meldestelle

1. **Aufnahme** von Vorfallmeldungen
2. **Klassifizierung** von Vorfällen
3. **Weiterleitung** an die koordinierende Stelle

Als Meldestelle eignen sich auch bereits eingerichtete Stellen, deren Funktionsumfang entsprechend erweitert wird, bspw.

1. Sicherheitszentrale
2. User Help Desk/Service Desk
3. Empfang
4. Sicherheitsabteilung

Die Institution stellt sicher, dass die Meldestelle über **geeignete Hilfsmittel** verfügt und **hinreichend qualifiziert** ist, um die Funktion wahrzunehmen.

Die Institution macht die Meldestelle intern auf geeignete Weise bekannt.

M 9 Definieren der Informations-, Melde- und Eskalationspfade (B)

Die **Institution definiert** vorab für **jede Kategorie von Sicherheitsvorfällen** (Vorfall, erweiterter Vorfall, Notfall, Krise), ob und in welcher **Art und Weise** die weitere **Information oder Eskalation** des jeweiligen Sicherheitsvorfalls **durch die Meldestelle** abgewickelt wird.

Die Meldestelle setzt dies entsprechend um und übermittelt zudem die ihr zu diesem Zeitpunkt bekannten Sachverhalte.

Ggf. ist die Alarmierung einer nächsthöheren Instanz noch nicht notwendig. Bspw. wird ein Vorfall als Notfall klassifiziert und entsprechend durch das Notfallmanagement abgewickelt. Dennoch sollte

die nächsthöhere Instanz über solche Sicherheitsvorfälle informiert werden.

Der **Eskalationsprozess unterscheidet** daher zwischen **Information und Alarmierung**. Die Information dient hierbei ausschließlich der Verteilung von Informationen an die Empfänger und erfordert keine Aktion. Erst die **Alarmierung erfordert** eine **Aktion durch den Empfänger**. Im Eskalationsprozess ist eindeutig zu kennzeichnen, ob informiert oder alarmiert wird.

Nachfolgende Abbildung verdeutlicht diesen **Vorgang am Beispiel eines Notfalls**, der die Alarmierung des Notfallmanagements und die Information des Krisenmanagements auslöst.

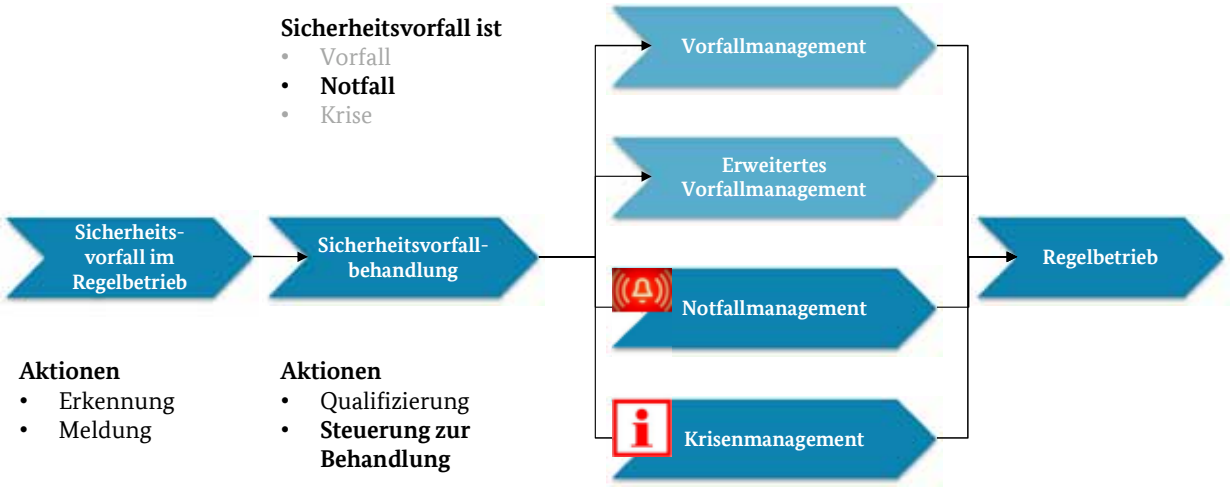


Abbildung 4: Eskalationsprozess - Information und Alarmierung

M 10 Erstellen von Alarmierungsplänen (A)

Alarmierungspläne enthalten die **notwendigen Maßnahmen und Kontaktdaten für die Ausführung einer Eskalation** in Form eines Alarms für ein bestimmtes Szenario oder einen bestimmten Vorfall. Die Institution bereitet Alarmierungspläne **für häufiger und in der Regel in der Alarmierung gleich ablaufende Vorfälle** vor und **hinterlegt** diese **bei der Meldestelle**.

Die Institution identifiziert die für sie relevanten Sicherheitsvorfälle und erstellt für diese individuelle oder allgemeine Alarmierungspläne.

M 11 Erfassen der Meldungen in einer zentralen Vorfalldatenbank (B)

Die Institution erfasst **alle** gemeldeten **Sicherheitsvorfälle in einer zentralen Datenbank**. Die entsprechenden Anforderungen an die Umsetzung und den Betrieb der Datenbank ermittelt die Institution **aufgrund** ihrer **individuellen technischen und organisatorischen Anforderungen**. Bei der Planung und dem Betrieb sind **neben Sicherheitsanforderungen auch** solche des **Datenschutzes** zu **beachten**. IT-Sicherheitsanforderungen können bspw. über den BSI IT-Grundschutz bedient werden.

Vgl. auch Maßnahme M 12 Definieren der Vorgaben zur Protokollierung von Sicherheitsvorfällen (B).

M 12 Definieren der Vorgaben zur Protokollierung von Sicherheitsvorfällen (B)

Die Institution definiert **Anforderungen an die Dokumentation von Sicherheitsvorfällen**. So stellt die Institution sicher, dass im laufenden Betrieb **jeder Sicherheitsvorfall von** seiner **Entstehung bis** zu seiner **Behebung nachvollziehbar dokumentiert** ist. In der Dokumentation sind **alle wesentlichen Merkmale des Vorfalls und Maßnahmen zu seiner Behebung** (Auftreten, Einordnung des Vorfalls, getroffene Gegenmaßnahme(n), Bestätigung der Behebung des Vorfalls) enthalten.

Die Institution entscheidet frühzeitig, ob die Dokumentation des Sicherheitsvorfalls einer sich **möglicherweise anschließenden gerichtlichen Auseinandersetzung standzuhalten** hat. In diesem Fall achtet sie darauf, dass die Dokumentation zwingend auf gerichtsfeste Art und Weise erfolgt und hierfür ausschließlich entsprechend geschulte und qualifizierte Personen eingesetzt werden. Diese Personen sind zwingend mit den Besonderheiten einer gerichtsfesten forensischen Untersuchung vertraut und geübt.

Weiterhin wenden die Meldequellen und Meldestellen eine geeignete Protokollierung an. Diese macht die korrekte Funktion der jeweiligen

Systeme überprüfbar.

Um die Effektivität und Effizienz der Sicherheitsvorfallbehandlung und der angrenzenden Prozesse zu erhöhen, kann die Institution eine **Vorfall- und Schadensdatenbank** einrichten. Durch die Auswertung dieser Datenbanken können **Trends frühzeitig erkannt** und entsprechende **Gegenmaßnahmen eingeleitet** werden.

M 13 Einschalten von Ermittlungsbehörden (A)

Sicherheitsvorfälle einer Institution **können** auch **strafrechtliche Relevanz haben**. Beispielsweise können sie Offizialdelikte sein oder dazu werden. Diese sind dann **zeitnah zur Anzeige** bei der zuständigen Ermittlungsbehörde **zu bringen**, auch wenn kein Eigenverschulden der Institution vorliegt.

Im Falle eines Sicherheitsvorfalls legt die Institution deshalb **in regelmäßigen Abständen mit ihrem juristischen Beistand** fest, ob die Einschaltung einer Ermittlungsbehörde geboten ist.

M 14 Analysieren und Auswerten von Sicherheitsvorfällen (B)

Die Institution definiert ein **Verfahren zur Auswertung und Analyse des Sicherheitsvorfalls**, um so eine Optimierung und Verbesserung der bestehenden Regelungen und Maßnahmen zu erreichen. Hierzu analysiert sie die Zusammenhänge eines Sicherheitsvorfalls sowie seiner Bewältigung und fasst die Erkenntnisse in einem Bericht zusammen.

Hauptbestandteil dieses Verfahrens ist die **Identifikation von Verbesserungsmaßnahmen**, die das Sicherheitsniveau der Institution aufgrund der gemachten Erfahrungen verbessern können.

M 15 Schulung und Sensibilisierung (A)

Da die Sicherheitsvorfallbehandlung maßgeblich davon abhängt, dass **sicherheitsrelevante Abweichungen frühzeitig erkannt und** auch **berichtet** werden, **informiert und sensibilisiert** die Institution ihre

Mitarbeiter zielgruppengerecht. Erfolgsfaktor hierbei ist die **zielgruppengerechte Aufbereitung von Informationen**, da Mitarbeiter sehr unterschiedliche Voraussetzungen und Erkennungsmöglichkeiten haben können. Beispielsweise sind Mitarbeiter eines technischen Überwachungscenters grundsätzlich anders zu schulen und zu sensibilisieren als Sachbearbeiter einer Institution.

Die Maßnahmen sind in einem **Schulungs- und Sensibilisierungskonzept**, wie bspw. im Baustein Schulung und Sensibilisierung beschrieben, zusammengefasst.

M 16 Sicherstellen der Vertraulichkeit (A)

Sicherheitsvorfälle betreffen die Werte einer Institution und sind dadurch **in der Regel vertraulich zu behandeln**.

Sowohl die **Informationen über den Vorfall als auch** die seitens der Institution **eingeleiteten Gegenmaßnahmen unterliegen** daher einer **besonderen Vertraulichkeit**. Diese definiert die Institution auf geeignete Weise im Vorfeld. Beim Eintreten eines Sicherheitsvorfalls **klärt** die Institution die Beteiligten darüber **auf und verpflichtet** sie **schriftlich zur Einhaltung** der Vertraulichkeit.

Gegebenenfalls ist es erforderlich, eine gesonderte **Vertraulichkeitsvereinbarung für einen spezifischen Vorfall** zu treffen.

Entsprechend werden alle Vertraulichkeitsvereinbarungen zum Sicherheitsvorfall genauso vertraulich behandelt und zusammen mit der Dokumentation des Sicherheitsvorfalls sicher verwahrt.

M 17 Erheben des Bedarfs für elektronische Hilfsmittel zur Kommunikation und Alarmierung (C)

Im Rahmen der Sicherheitsvorfallbehandlung ist bereits frühzeitig der **Bedarf umfassender Information einer Vielzahl Beteiligter** zu **prüfen**. Mit zunehmender Anzahl der zu Informierenden stellt dies eine große Herausforderung für die Meldestelle dar. In diesem Fall prüft die Institution, ob und ggf. welche **Hilfsmittel für die Information,**

Kommunikation und Alarmierung genutzt werden können.

Dies können beispielsweise die folgenden sein:

1. Pager
2. SMS-/E-Mail-Massenversandservice
3. Sprechfunkgeräte
4. Telefonkonferenzräume
5. spezielle Alarmierungswerkzeuge

Bei der Betrachtung der Hilfsmittel wägt die Institution immer den **Nutzen** gegenüber den ggf. entstehenden **Kosten** ab. Des Weiteren berücksichtigt sie insbesondere **bestehende systemische Grenzen**.

M 18 Aufbauen einer präventiven Sicherheitsanalytik (C)

Die Institution nutzt die vorhandene Sicherheitsvorfalldatenbank (vgl. Maßnahmen M 11 und M 12) und etabliert **Verfahren zur Analyse und Ableitung präventiver Maßnahmen aufgrund des eigenen Vorfallprofils**.

Durch das systematische Auswerten können **bestehende Schwachstellen** sowie aufkommende **wiederkehrende Muster von Gefährdungspotentialen entdeckt und präventiv behandelt** werden. So lassen sich bestehende Lücken gezielter und damit ressourcenschonender beseitigen und Maßnahmen zur Abwehr aufkommender Gefährdungen frühzeitig entwickeln.

5 Weiterführende Informationen

Weiterführende Informationen zur Sicherheitsvorfallbehandlung können den nachfolgenden Veröffentlichungen[4] entnommen werden.

- *Bundesamt für Sicherheit in der Informationstechnik 2008: BSI-Standard 100-4 Notfallmanagement*
- *Bundesamt für Sicherheit in der Informationstechnik 2009: BSI IT-Grundschutz - Baustein 1.8, Behandlung von Sicherheitsvorfällen*
- *National Institute of Standards and Technology 2014: Framework for Improving Critical Infrastructure Cybersecurity*
- *The Business Continuity Institute (BCI) 2013: Good Practice Guidelines - A Guide to Global Good Practice in Business Continuity*

6 Anlage

Das Wichtigste auf einen Blick (Themenübersicht)

Organisation	Dokumentation	Eskalation
Organisationsstruktur Rollen und Verantwortlichkeiten Prozesse und Verfahren Meldequellen Meldestellen	Richtlinie Methoden meldepflichtige Sicherheitsvorfälle Alarmierungspläne	Reaktionsteams Eskalationsstufen Schwellenwerte Eskalationsprozess

Werkzeuge	Verbesserung	Behörden
Hilfsmittel zur Kommunikation und Alarmierung	Analysieren und Auswerten Schulung und Sensibilisierung	Einbinden von Ermittlungsbehörden

Maßnahmenübersicht und -kategorien

A - Basismaßnahmen	B - Standardmaßnahmen	C - erweiterte Maßnahmen
M 1 Schaffen der organisatorischen Strukturen M 2 Erstellen einer Richtlinie zur Sicherheitsvorfallbehandlung M 3 Definieren spezialisierter Reaktionsteams M 4 Definieren von Eskalationsstufen und Schwellenwerten M 7 Identifizieren und Definieren der Meldequellen M 8 Identifizieren und Definieren der Meldestellen M 10 Erstellen von Alarmierungsplänen M 13 Einschalten von Ermittlungsbehörden M 15 Schulung und Sensibilisierung M 16 Sicherstellen der Vertraulichkeit	A + M 5 Definieren einer einheitlichen Methodik zur Qualifizierung von Sicherheitsvorfällen M 6 Definieren meldepflichtiger Sicherheitsvorfälle M 9 Definieren der Informations-, Melde- und Eskalationspfade M 11 Erfassen der Meldungen in einer zentralen Vorfalldatenbank M 12 Definieren der Vorgaben zur Protokollierung von Sicherheitsvorfällen M 14 Analysieren und Auswerten von Sicherheitsvorfällen	A und B + M 17 Erheben des Bedarfs für elektronische Hilfsmittel zur Kommunikation und Alarmierung M 18 Aufbauen einer präventiven Sicherheitsanalytik

Danksagung

Wir bedanken uns bei den vielen Experten, die ihr Fachwissen bei der Erstellung dieses Bausteins einfließen ließen und durch ihr Engagement die Entstehung erst ermöglicht haben. Insbesondere gilt unser Dank folgenden Autoren und Mitwirkenden: Herr Marcel Knop und Herr Matthias Müller, Herr Stefan Nees und Herr Björn Schmelter (HiSolutions AG).

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Merianstraße 100, 50765 Köln
www.verfassungsschutz.de

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189, 53175 Bonn
www.bsi.bund.de

Herausgeber
ASW Bundesverband
Allianz für Sicherheit in der Wirtschaft e.V.
Rosenstraße 2, 10178 Berlin
asw-bundesverband.de

Redaktion/Bezugsquelle/Ansprechpartner
Prof. Timo Kob (Gesamtprojektleitung)

Gestaltung, Produktion
HiSolutions AG

Stand
Februar 2017

Auflage
1. Auflage