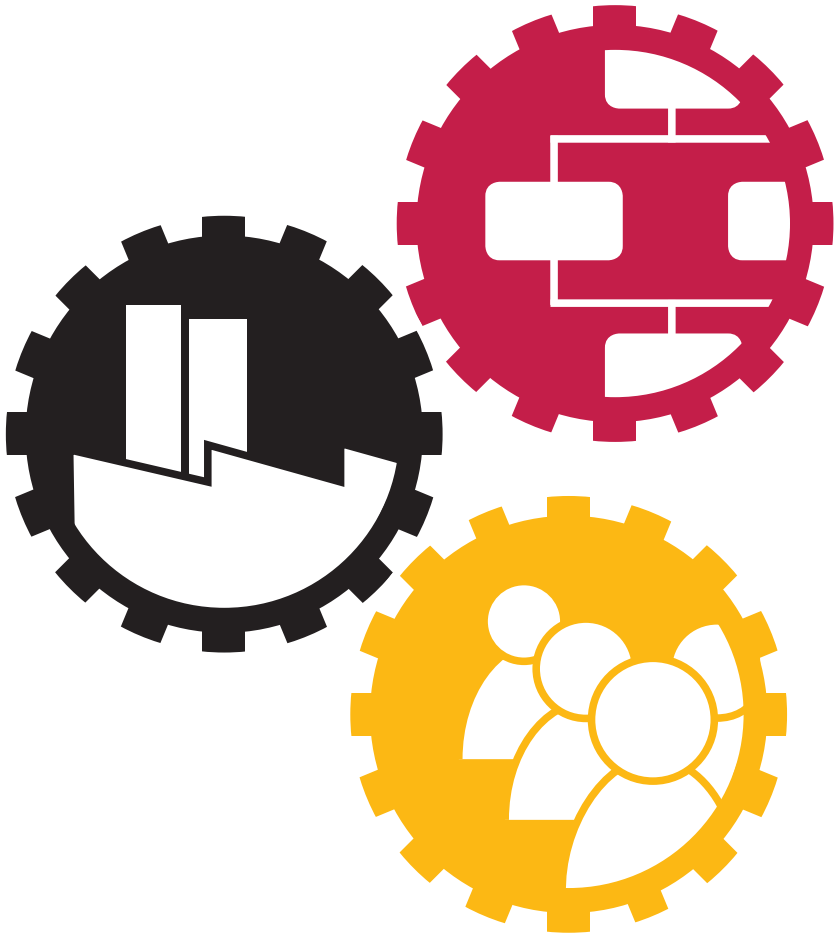
Bundesamt für Verfassungsschutz

Bundesamt für Sicherheit in der Informationstechnik

ASW Bundesverband

# Wirtschaftsgrundschutz

## Baustein ÜA1 Schulung und Sensibilisierung



# 1 Relevanzentscheidung für diesen Baustein

1. Hat die Institution ein **Sicherheitsmanagementsystem eingeführt** oder plant die Einführung?
2. Besteht bereits ein **allgemeines Schulungskonzept**?
3. **Fordern Kunden und Geschäftspartner** ein Managementsystem zum Schutz von Informationen?
4. Bestehen **vertragliche Verpflichtungen** zum sicheren Umgang mit Informationen?
5. Beabsichtigt oder betreibt die Institution **Dienstleistungen für Kunden in regulierten Branchen** (bspw. Finanzdienstleister, Telekommunikation) **oder für solche, die nach gängigen Sicherheitsstandards zertifiziert sind**?

**Nur qualifizierte und sensibilisierte Menschen können Werte angemessen schützen.**

Sicherheitsmanagementsystem als Voraussetzung für ein einheitliches Schutzniveau

Die Leitung der Institution stellt mit dem **Sicherheitsmanagementsystem** ein **umfassendes Regelwerk** zur Verfügung. Die **Ziele, Vorgehensweisen und Inhalte des Sicherheitsmanagementsystems** sind dort definiert und beschrieben. Eine **Dokumentation allein reicht** allerdings **nicht aus,** um das **Ziel** eines **einheitlichen Schutzniveaus** tatsächlich zu erreichen.

Herausforderung: aktive Anwendung

Der **Faktor Mensch** ist hierbei ein **wesentliches Schlüsselelement** zum Erreichen des Ziels. Somit stellt sich die Herausforderung, das oftmals eher theoretische **Wissen und** die **Regelungen** so aufzubereiten, dass der Mensch sie aufnimmt und nachvollzieht und so selber

auch **aktiv anwenden** kann.

**Ein Ziel der Institution ist es, ihre Mitarbeiter oder Externe vor spezifischen Gefährdungen zu schützen.** Sie verdeutlicht daher die Hintergründe der **institutionsspezifischen Vorgaben und Regeln**, bspw. an praktischen Beispielen der alltäglichen Arbeit. Durch das **Verstehen und Wissen um die Gefährdungen** ist die Wahrscheinlichkeit deutlich höher, dass diese **Vorgaben und Regeln beachtet** werden.

Notwendigkeit regelmäßiger Wiederholung

Der Mensch neigt allerdings auch dazu, das **Wissen** wieder zu **verdrängen**. Insbesondere in unserer heutigen schnelllebigen Zeit mit ihrer Informationsflut und vielen dringlichen Terminen bedarf es einer besonderen Aufmerksamkeit, damit **Wissen erhalten** bleibt.

**Schulungen** beinhalten g**rundsätzliche und spezifische Inhalte zum Sicherheitsmanagement** und dienen der Wissensvermittlung. Idealerweise sind sie in das Schulungssystem der Institution integriert.

**Kampagnen zur Sensibilisierung** greifen hingegen aktuelle oder relevante Themen auf, um Informationen zu vermitteln oder in Erinnerung zu rufen. Je nach gewähltem Kommunikationsmedium sind sie dauerhaft, auf einen längeren Zeitraum oder auch spontan ausgelegt. Wecken die Kampagnen das Interesse der Zielgruppe, ist der Zugang für die zu vermittelnden Informationen aufgebaut. Es entsteht ein Bezug und diese **Informationen bleiben in Erinnerung**. Sie **beeinflussen** damit **das Verhalten positiv**.

Inhalt des Bausteins: konkrete Hilfestellung für eine strukturierte Herangehensweise

Dieser **Baustein liefert** Verantwortlichen einer Institution eine **Hilfestellung für eine strukturierte Herangehensweise**. Er **ergänzt** damit die **allgemeinen Anforderungen an ein Schulungs- und Sensibilisierungskonzept des Wirtschaftsgrundschutzstandards 2000-1**.

# 2 Beschreibung

**Mit Schulungen stellt die Institution sicher, dass die Teilnehmer einen definierten Wissensstand vermittelt bekommen.** Die Institution **etabliert** zudem einen **geeigneten Steuerungsprozess**, sodass die Vermittlung an die Teilnehmer **dokumentiert und belegbar** ist.

**Schulungen sind ein wichtiger Grundstein, um das angestrebte Sicherheitsniveau in der Institution erreichen zu können**. Die Institution entwickelt daher ein **Schulungskonzept**, das

1. ihren **individuellen Bedürfnissen** entspricht
2. auf die ggf. **unterschiedlichen Zielgruppen** ausgerichtet ist
3. neben **Basisschulungen** auch **Vertiefungs- und Wiederholungsschulungen** umfasst

Ein **Sensibilisierungskonzept** ist eine **Ergänzung zum klassischen Schulungswesen** und **unterstützt** die **Qualifizierung der Mitarbeiter aktiv** mit aktuellen Informationskampagnen. Üblicherweise sind Kampagnen zur Sensibilisierung so ausgelegt, dass sie der Zielgruppe **Wissen über einen bestimmten Zeitraum und in einem alltäglichen Umfeld vermitteln**. Dies sind bspw. Aktionen mit Plakaten, Aushängen, im Intranet oder mit Informationsständen zu bestimmten Themen.

Das **Ziel eines Sensibilisierungskonzepts** ist es, die **Mitarbeiter**, aber auch **Besucher und Externe auf** die **Gefährdungen** im alltäglichen Gebrauch von Informationen **aufmerksam** zu **machen**. Mit **möglichst praktischen Beispielen** vermittelt die Institution so bspw. den Zusam-

menhang von verbindlich dokumentierten Regeln und den Tätigkeiten in der Institution **auf anschauliche Weise**.

Mittels eines **gesteigerten Hintergrundwissens** und einer **erhöhten Aufmerksamkeit reduzieren** sich so **potentielle Sicherheitsvorfälle** oder werden früher erkannt. Beides stellt einen enormen **Nutzen für die Institution** dar. Zum einen sind dadurch die **Werte weniger stark bedroht**. Zum anderen werden **aufwendige Reaktionsprozesse oder Korrekturmaßnahmen vermieden oder zumindest reduziert**, die üblicherweise mit Ausfallzeiten und hohen Kosten verbunden sind.

positive Effekte von Schulungen und Sensibilisierungsmaßnahmen

Das **Ergebnis** eines wirksamen Schulungs- und Sensibilisierungskonzepts ist der **angemessene Umgang mit den Informationen** durch die Mitarbeiter oder Besucher der Institution und in der Folge der **Schutz der Werte**.

Der Wirtschaftsgrundschutz sieht daher **beide Aspekte** vor. Neben einem **Schulungskonzept** nutzt die Institution die **Sensibilisierung als zweite Säule** zur Information und Aufklärung ihrer Mitarbeiter oder Besucher.

# 3 Gefährdungslage

Die meisten der organisatorischen und viele der technischen **Maßnahmen zur Sicherstellung eines bestimmten Sicherheitsniveaus erfordern** den **Einsatz oder** die **Mitwirkung der Mitarbeiter** der Institution. Die **erlassenen Regeln dokumentiert** die Institution **und macht sie** mittels Veröffentlichung den Mitarbeitern **bekannt**.

Die **Mitarbeiter**, aber in angepassten Umfang auch Externe, Besucher oder Gäste der Institution, **kennen** damit grundsätzlich diese **Regeln**. **Ob die Regeln auch angewendet und beachtet werden, bleibt allerdings offen.** Zudem ist bekannt, dass Regeln oftmals aus den verschiedensten Gründen umgangen werden. Dies meist nicht aus böser Absicht, sondern um den Arbeitsablauf zu erleichtern oder zu optimieren.

Regeln funktionieren nur, wenn sie angewendet werden

Die Erfahrung zeigt, dass Menschen Regeln immer dann korrekt oder zumindest korrekter anwenden, wenn ihnen der **Zusammenhang und die Hintergründe bekannt und bewusst** sind. Eine Abweichung und das damit verbundene Risiko wägt ein **gut informierter Mensch** also eher ab als ein uninformierter. Die Institution macht sich dies zunutze, um das **gewünschte Sicherheitsniveau** zu **erreichen**.

**Zu der Gefährdung durch einen spezifischen Sachverhalt kommt also eine durch den unsachgemäßen Umgang mit Verfahren, Hilfsmitteln oder Vergleichbarem hinzu.**

In der Praxis betreffen eine Institution die **folgenden Gefährdungen besonders häufig**:

G 1 Unzureichende Schulungen für Mitarbeiter
G 2 Unzureichende Schulungen für Funktionsträger
G 3 Unzureichendes Schulungskonzept zum Sicherheitsmanagement
G 4 Fehlende oder unzureichende Sensibilisierung der Mitarbeiter
G 5 Ungeeigneter Umgang mit schutzwürdigen Informationen
G 6 Unzureichende Einweisung von Besuchern oder Gästen
G 7 Unzureichende Schulung länger anwesender Externer
G 8 Unzureichende oder fehlende Kontrolle verpflichtender Sicherheitsschulungen
G 9 Nichtbeachtung von Sicherheitsmaßnahmen

# 4 Maßnahmen

**Sicherheitsschulungen und Sensibilisierungen sind ein wesentlicher Erfolgsfaktor für die Aufrechterhaltung eines angestrebten Sicherheitsniveaus.**

Die Institution legt ein **Prozessmodell** fest, das einen **angemessenen Wissensgrad** zum **Ziel** hat. Mit dem Prozessmodell sind die **grundlegenden Aufgaben zur Errichtung eines Sicherheitsschulungs- und Sensibilisierungskonzepts** beschrieben. Dies umfasst die **Festlegungen von Verantwortlichkeiten und Rollen** ebenso wie die **Dokumentation, Hilfsmittel und eine längerfristige Planung**. Die längerfristige Planung stellt sicher, dass Inhalte aufeinander aufbauend und abgestuft im Sinne von Einstieg und Auffrischung vermittelt werden können. **Sensibilisierungskampagnen** plant die Institution **eher im Hinblick auf Aktualität und kurzfristigen Bedarf**. Diese unterliegen dabei dem gleichen Ablauf im Prozessmodell.

Der **Betriebsprozess für Sicherheitsschulungs- und Sensibilisierungsmanagement** ist **als klassischer Regelkreis** ausgelegt. Er **umfasst das Planen, Durchführen, Auswerten und Anpassen von Schulungen oder Kampagnen**. So **unterstützt** die Institution auch die **strategischen Ziele des Sicherheitsmanagements** mit abgestimmten und geeigneten Schulungen und Kampagnen.

Neben der **Qualität** und der **Wirkung** der einzelnen Maßnahmen erfasst die Institution insbesondere auch die **Teilnahme** an Schulungen. Dies ist von großer Bedeutung, wenn ein **Nachweis gegenüber**

**Dritten** zu erbringen ist.

Die Maßnahmen folgen 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 1 stellt dies grafisch dar.

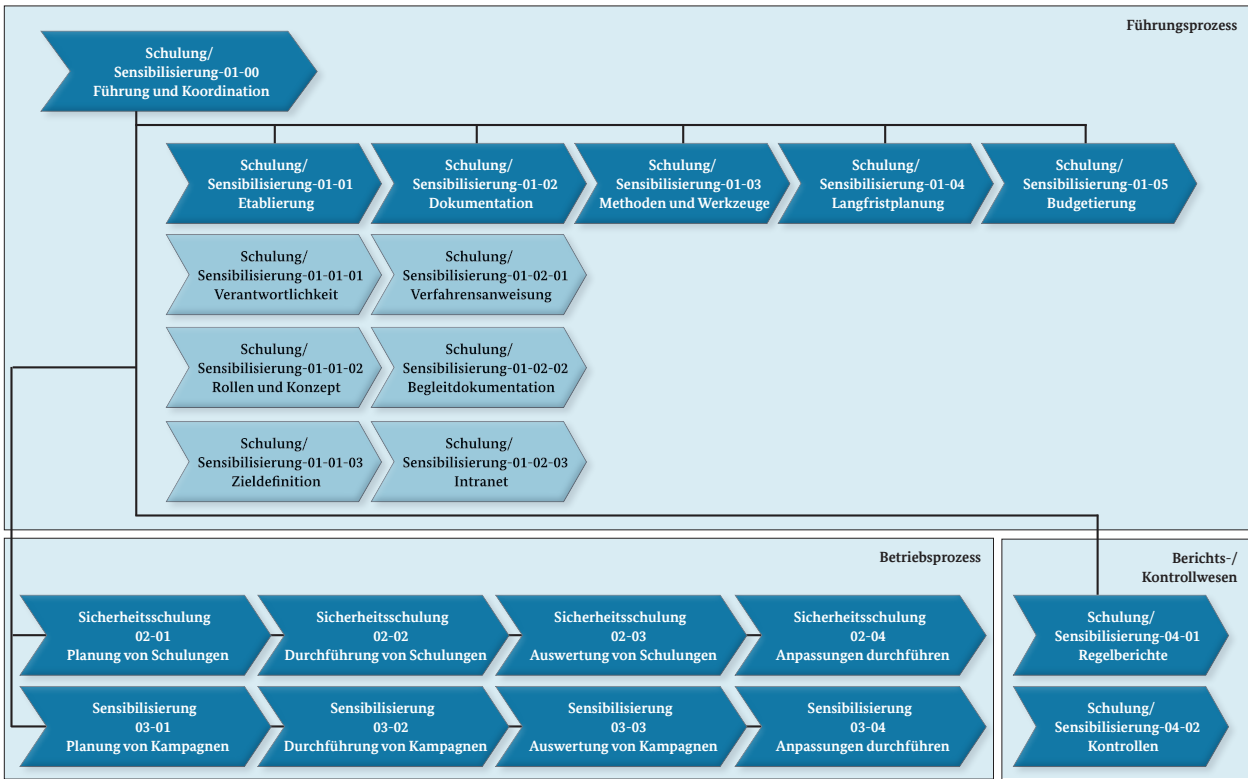


Abbildung 1: Prozessschaubild Sicherheitsschulungs- und Sensibilisierungsmanagement

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 Verantwortung der Institution (A)*

Die **Sicherstellung einer angemessenen Schulung und Sensibilisierung** der Mitarbeiter oder ihrer Besucher **obliegt der Leitung** der Institution. Sie delegiert dies an einen Verantwortlichen zur Umsetzung.

### *M 2 Identifizieren des Sicherheitsschulungsbedarfs (A)*

Der **tatsächliche Bedarf an Sicherheitsschulungen** in der Institution stellt den **Rahmen eines Sicherheitsschulungs- und Sensibilisierungsmanagements**. Der Bedarf hängt hierbei von der individuellen Exposition, Auflagen und Anforderungen, einer eigenen Zertifizierung und weiteren Aspekten der jeweiligen Institution ab.

Die Institution erhebt den **Bedarf in den definierten sicherheitsrelevanten und den bereichsübergreifenden Themengebieten**. Mittels dieser Erhebung leitet die Institution den für sie relevanten Schulungsbedarf ab.

Die Institution identifiziert **relevante andere Geschäftsbereiche** und stimmt sich mit diesen ab, wenn dort bereits Schulungen durchgeführt werden oder ein Schulungsmanagement betrieben wird. In diesen Fällen kann die Institution **alle Schulungsmaßnahmen integrieren** und sie gemeinsam anbieten.

### *M 3 Definieren und Umsetzen eines Sicherheitsschulungs- und Sensibilisierungskonzepts (A)*

Die Institution definiert ein **Sicherheitsschulungs- und Sensibilisierungskonzept**. Sie legt hierin **Rahmenbedingungen**, bspw. **Ziele, Verantwortlichkeiten und Vorgehensweisen**, fest.

Bei der Entwicklung des Konzepts werden **folgende Aspekte berücksichtigt**:

1. individuelle **Gefährdungslage**
2. **Auflagen** aus Gesetzen, Verträgen oder internen Vorgaben
3. ggf. unterschiedliche **Anforderungen verschiedener Standorte**

4. spezifische **Anforderungen von Funktionsträgern**[1]
5. **modularer Aufbau** (bspw. Einführung, spezifische Aspekte, Auffrischung)
6. **Laufzeit** von drei bis fünf Jahren
7. **Prozess** für Planung, Durchführung, Auswertung und Verbesserung
8. **Dokumentation**
9. bereits etablierte **Hilfsmittel** (bspw. Schulungscenter, Intranet o. ä.)

Die Sicherheitsschulungen werden **zielgruppengerecht** aufbereitet. Dies bedeutet, dass es neben **allgemeinen Schulungen** auch **spezielle Schulungen für spezielle Funktionsträger** gibt. Dies gilt bspw. für Rollen im Reaktionsmanagement oder dem Sicherheitsrisikomanagement, aber ebenso für **im Umgang mit Sicherheitsvorfällen besonders prädestinierte Rollen** wie bspw. Empfang, Telefonzentrale, Kundenservice.

Die **Dauer der Schulungen** hängt von ihrer Umsetzungsart und einem evtl. bestehenden allgemeinen Schulungskonzept ab. Einzelne Schulungen dauern **idealerweise max. zwei Stunden**, um auch während der regulären Arbeitszeit **ohne größere Auswirkungen durchgeführt** werden zu können. Allerdings lassen sich einzelne Schulungen auch kombinieren und zu vollständigen **Seminarveranstaltungen** zusammenführen. Dies obliegt der Institution und den jeweiligen Bedürfnissen.

Die Institution definiert **verpflichtende Schulungen** inkl. einer **Wiederholungshäufigkeit** (bspw. jährlich oder zweijährlich) und **dokumentiert die Teilnahme** revisionssicher.

Mit dem Sicherheitsschulungs- und Sensibilisierungskonzept **steuert** die Institution die **Qualifizierung und** damit indirekt den **Reifegrad des Sicherheitsmanagementsystems**.

[1] bspw. im Reaktionsmanagement, Sicherheitsrisikomanagement oder der Sicherheitsvorfallbehandlung

## *M 4 Planen und Durchführen von Sicherheitsschulungen (A)*

Die Institution etabliert Vorgehensweisen, mit denen sie die Sicherheitsschulungen **langfristig plant, vorbereitet und durchführt**. Sie stellt diese Planung bspw. in einem eigenen **Schulungsplan** dar **und kommuniziert diesen** den Mitarbeitern auf geeignete Weise.

Im Rahmen der Planung **prüft** die Institution, **ob alle sicherheitsrelevanten Themen** dem Bedarf entsprechend **enthalten sind**. Ggf. passt die Institution den Schulungsplan entsprechend an.

Bei der Planung berücksichtigt die Institution, dass die **Zielgruppen verschieden** sind und **Schulungen** idealerweise **aufeinander aufbauen**. So können **Basisschulungen** bspw. häufiger angeboten werden und **Vertiefungsschulungen** seltener. Die Häufigkeit und die Ausgestaltung hängen allerdings vom individuellen Bedarf der Institution ab.

Die Institution stellt sicher, dass für die Sicherheitsschulungen geeignetes **Begleit- oder Lehrmaterial** zur Verfügung steht. Werden die Schulungen **online** angeboten, bietet es sich an, dies ebenfalls online bereitzustellen. Bei **Präsenzschulungen** können zusätzlich ausgedruckte Unterlagen bereitgestellt werden.

## *M 5 Sicherheitsschulungen für Funktionsträger der Institution (B)*

**Die Institution stellt Funktionsträgern im Sicherheitsmanagement spezifische Schulungen entsprechend den Anforderungen der wahrgenommenen Funktion bereit.**

Funktionsträger sind bspw. **in folgenden Themengebieten** zu erwarten:

1. Notfall- oder Krisenmanagement
2. Sicherheitsrisikomanagement
3. Sicherheitsvorfallmanagement

Den Bedarf hierfür erhebt sie im Vorfeld (vergleiche Maßnahme M 2).

### *M 6 Sicherheitsschulungen für länger anwesende Externe der Institution (B)*

Die Institution berücksichtigt bei der Planung der Schulungstätigkeiten auch **Externe, die längere Zeit in der Institution tätig sind**.

Ggf. bedürfen die Schulungen einer Anpassung oder werden ausschließlich elektronisch bereitgestellt. Auch hier gilt, dass ein ggf. bereits etabliertes Schulungsmanagement genutzt werden kann.

### *M 7 Definieren von Verfahrensanweisungen für die Besucher- und Gästebetreuung (B)*

Die Institution berücksichtigt, dass auch Besucher und Gäste einen **Bedarf an Sicherheitsinformationen** haben.

Da diese ggf. nur kurz in der Institution verweilen, definiert die Institution eine **Verfahrensanweisung, wie Besucher und Gäste empfangen werden** und dabei auf die **relevanten Sicherheitsvorschriften und -aspekte** aufmerksam gemacht werden.

Die Institution stellt hierfür **geeignete Informationen oder Unterlagen für Gäste und Besucher** bereit.

### *M 8 Auswerten und Verbessern von Sicherheitsschulungen (A)*

Die Institution wertet bspw. anhand von **Kommentarbögen der Teilnehmer** die durchgeführten Schulungen aus.

Ergeben sich hier **inhaltliche oder organisatorische Verbesserungsbedarfe**, passt die Institution die jeweilige Schulung entsprechend an.

**Verpflichtende Schulungen** wertet die Institution auf **Teilnahmevollständigkeit** aus. Sie stellt sicher, dass die Vollständigkeit gewährleistet wird.

## *M 9 Planen und Durchführen von Sensibilisierungskampagnen (C)*

Mit **Sensibilisierungskampagnen unterstützt** die Institution die **Schulungsmaßnahmen** aktiv. Sie stellt in den Kampagnen aktuelle oder institutionsspezifische Themen dar. Die Institution prüft neben dem Inhalt der Kampagne auch die Umsetzungsform. Hier stehen diverse Möglichkeiten zur Auswahl, bspw.

1. Aushänge und Plakate
2. Flyer
3. Hauspost
4. Informationsstände
5. Intranet
6. E-Mail

Die Institution stimmt die **Form und den zeitlichen Rahmen der Kampagnen** auf die zu vermittelnden Informationen ab.

Insbesondere die **Planung von Sensibilisierungskampagnen** übersteigt oftmals die internen Möglichkeiten einer Institution. In diesem Fall prüft die Institution den **Einsatz geeigneter Dienstleister** (vergleiche Maßnahme M 10).

## *M 10 Auswählen und Beauftragen von Dienstleistern (C)*

Die Institution prüft, ob **Dienstleister** sie im Sicherheitsschulungs- und Sensibilisierungsmanagement **wirksam unterstützen** können. Für den Einsatz von Dienstleistern gelten die Anforderungen dieses Bausteins.

Die **Institution stellt sicher, dass**

1. die **Inhalte** dem erhobenen **Bedarf entsprechen**
2. die dem Dienstleister **überlassenen Informationen entsprechend** den **internen Sicherheitsvorgaben** und den geltenden **Datenschutzbestimmungen** behandelt werden
3. der Dienstleister **Auswertungen über verpflichtende Schulungen** erstellt und der Institution überlässt
4. weitere **interne Vorgaben berücksichtigt** werden

# 5 Weiterführende Informationen

Weiterführende Informationen zu Sicherheitsschulungen und Sensibilisierungskampagnen können den nachfolgenden Veröffentlichungen entnommen werden.

- *Röniger, Jacobs 2014: Security Awareness – Aufbau & Umsetzungsleitfaden für Sensibilisierungs- & eLearning-Programme*
- *Helisch & Pokoyski 2009: Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*

# 6 Anlage

Das Wichtigste auf einen Blick (Themenübersicht)

| Etablierung | Organisation | Umsetzung |
|---|---|---|
| Verantwortung der Organisation<br>Identifizieren des Sicherheitsschulungsbedarfs | Definieren und Umsetzen eines Sicherheitsschulungs- und Sensibilisierungskonzepts<br>Sicherheitsschulungen für Funktionsträger der Institution<br>Sicherheitsschulungen für länger anwesende Externe der Institution<br>Auswählen und Beauftragen von Dienstleistern | Planen und Durchführen von Sicherheitsschulungen<br>Auswerten und Verbessern von Sicherheitsschulungen<br>Planen und Durchführen von Sensibilisierungskampagnen |
| **Dokumentation** | | |
| Definieren von Verfahrensanweisungen für die Besucher- und Gästebetreuung | | |

Maßnahmenübersicht und -kategorien

| A - Basismaßnahmen | B - Standardmaßnahmen | C - erweiterte Maßnahmen |
|---|---|---|
| | **A +** | **A und B +** |
| M1 Verantwortung der Institution<br>M2 Identifizieren des Sicherheitsschulungsbedarfs<br>M3 Definieren und Umsetzen eines Sicherheitsschulungs- und Sensibilisierungskonzepts<br>M4 Planen und Durchführen von Sicherheitsschulungen<br>M 8 Auswerten und Verbessern von Sicherheitsschulungen | M 5 Sicherheitsschulungen für Funktionsträger der Institution<br>M 6 Sicherheitsschulungen für länger anwesende Externe der Institution<br>M7 Definieren von Verfahrensanweisungen für die Besucher- und Gästebetreuung | M9 Planen und Durchführen von Sensibilisierungskampagnen<br>M 10 Auswählen und Beauftragen von Dienstleistern |

# 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 Mathias Köppe und Herr Matthias Müller (HiSolutions AG) sowie den Mitgliedern des ASW Kompetenzcenters Aus- und Weiterbildung.

# 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

**Druck**
SunCopy GmbH, Berlin

**Stand**
August 2016

**Auflage**
1. Auflage