Zielgruppengerechte Vermittlung von Themen der Informationssicherheit

Autor: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Stand: Dezember 2008

1 Einleitung

Informationssicherheit hat viele Facetten und geht weit über den Betrieb von Firewall und Virenschutz hinaus. Ein ganzheitliches Sicherheitskonzept enthält daher zahlreiche Maßnahmen aus den Bereichen Organisation, Personal, Technik sowie Infrastruktur. Es gibt eine Reihe von Standardwerken zur Informationssicherheit, die detailliert beschreiben, welche Standard-Sicherheitsmaßnahmen den Stand der Technik definieren. Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gilt dabei in Deutschland als der bekannteste und umfassendste Standard für die Erstellung von Sicherheitskonzepten. Er wurde 2005 in die BSI-Standards zur Informationssicherheit, die die Methodik des IT-Grundschutzes beschreiben und die IT-Grundschutz-Kataloge, die die detaillierten Sicherheitsmaßnahmen in Form von Bausteinen enthalten, aufgeteilt.

Der wichtigste Erfolgsfaktor für die Erreichung eines angemessenen Sicherheitsniveaus sind verantwortungsbewusste und kompetente Mitarbeiter, die koordiniert zusammenarbeiten. Dabei bringen Management, IT-Benutzer, Administratoren und IT-Sicherheitsexperten sehr individuelle fachliche Voraussetzungen mit und nehmen ganz unterschiedliche Aufgaben wahr. Während die Unternehmens- bzw. Behördenleitung die Gesamtverantwortung trägt, Ziele vorgibt und Rahmenbedingungen definiert, müssen Administratoren technisch hochqualifiziert sein und Detailwissen besitzen, um Systeme bedienen und sicher konfigurieren zu können.

IT-Experten sind mit den Standards zur Informationssicherheit und IT-Grundschutz-Katalogen in der Lage, ein umfassendes Sicherheitskonzept zu erstellen. Wenn alle Bereiche der Informationssicherheit damit abgedeckt werden sollen, wird ein Sicherheitskonzept in der Praxis viele Seiten umfassen. Es ist einem "normalen" IT-Benutzer allerdings nicht zuzumuten, das Sicherheitskonzept komplett durchzulesen, um die für ihn relevanten Teile herauszusuchen.

Um sicherzustellen, dass jeder Mitarbeiter die ihn betreffenden Aspekte der Informationssicherheit kennt und beachtet, ist die zielgruppengerechte Aufbereitung und Vermittlung der Inhalte des Sicherheitskonzepts eine zentrale und vielleicht auch die wichtigste Aufgabe des IT-Sicherheitsbeauftragten.

Das BSI empfiehlt daher, unterschiedliche Sicherheitsrichtlinien und Teilkonzepte zu erstellen, die einzelne Informationssicherheitsthemen bedarfsgerecht darstellen. So erhalten Mitarbeiter genau die Informationen, die sie zu einem bestimmten Thema wirklich benötigen. Sie werden nicht mit unnötigen Details konfrontiert, die vom Wesentlichen abhalten, unverständlich sind und verwirren. Die Richtlinien sind dazu in einer Sprache geschrieben, die für die jeweilige Zielgruppe verständlich ist.

Die Erstellung von einzelnen Richtlinien bietet noch einen weiteren Vorteil: Es ist bei jedem Projekt sinnvoll, zunächst die grundlegenden Voraussetzungen zu erarbeiten und Vorgaben zu kennen, bevor technische Detaillösungen umgesetzt werden.

2 Hierarchischer Aufbau von Richtlinien

Bei der Formulierung von Richtlinien hat es sich bewährt, auf verschiedenen Ebenen zu arbeiten.

Zunächst sollten in der ersten Ebene kurz und prägnant die allgemeinen Sicherheitsziele und eine Strategie zur Erreichung dieser Ziele formuliert werden. Die Strategie enthält keine technischen Details, wird vom Management verabschiedet und selten geändert.

In der nächsten Ebene sollten aus der Strategie grundlegende technische Anforderungen ableitet werden. Zur zweiten Ebene gehören wenige Dokumente, die verschiedene Aspekte der Informationssicherheit beschreiben (z. B. eine Richtlinie zur Internetnutzung oder ein Virenschutzkonzept), ohne auf konkrete Produkte einzugehen.

In der dritten Ebene werden technische Details, konkrete Maßnahmen und produktspezifische Einstellungen beschrieben. Diese Ebene enthält viele Dokumente, die regelmäßig geändert und nur von den zuständigen Experten gelesen werden.

Abbildung 1 stellt den hier beschriebenen Aufbau graphisch dar.

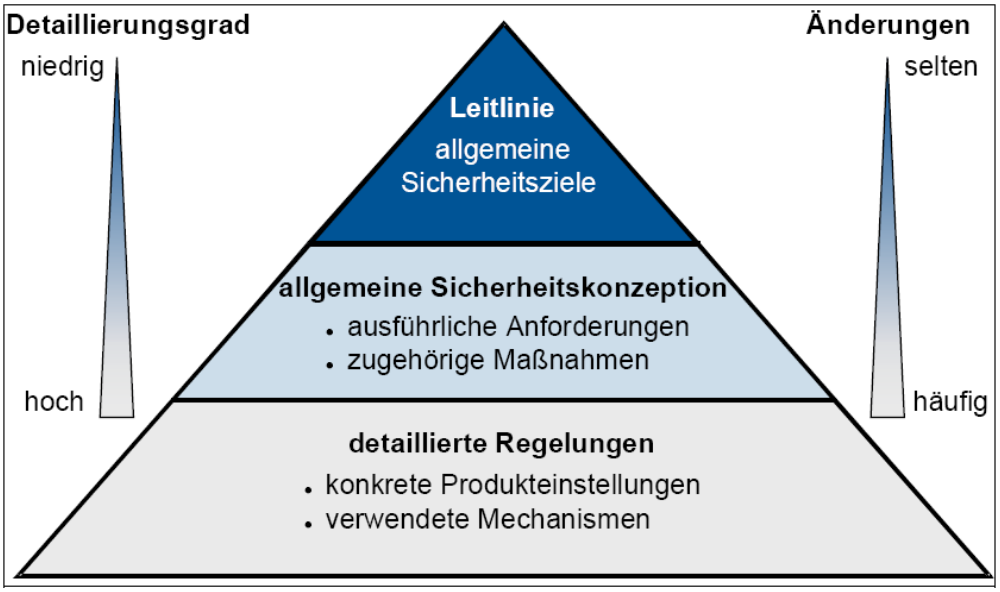

Abbildung 1: Hierarchischer Aufbau von Richtlinien

3 Musterrichtlinien und Beispielkonzepte des BSI

Das BSI hat in Zusammenarbeit mit der UIMC Dr. Voßbein GmbH & Co. KG einige Musterrichtlinien erarbeitet. Die Musterdokumente zeigen, welche Themen der Informationssicherheit besonders wichtig sind und wie eine hierarchische Anordnung von Richtlinien aussehen kann.

Alle Richtlinien sind Vorschläge und beruhen auf den Empfehlungen der IT-Grundschutz-Kataloge. Sie sind so geschrieben, dass sie ohne große Änderungen von Unternehmen und Behörden übernommen werden können. Jedes Muster enthält zudem Verweise auf entsprechende Maßnahmen der IT-Grundschutz-Kataloge, damit Leser sich ausführlich über die Hintergründe einer Handlungsempfehlung informieren können.

Die Dokumente dürfen frei verwendet werden und können an individuelle Bedürfnisse angepasst werden. Aus diesem Grund werden sie in einer Word für Windows und PDF-Version zur Verfügung gestellt.

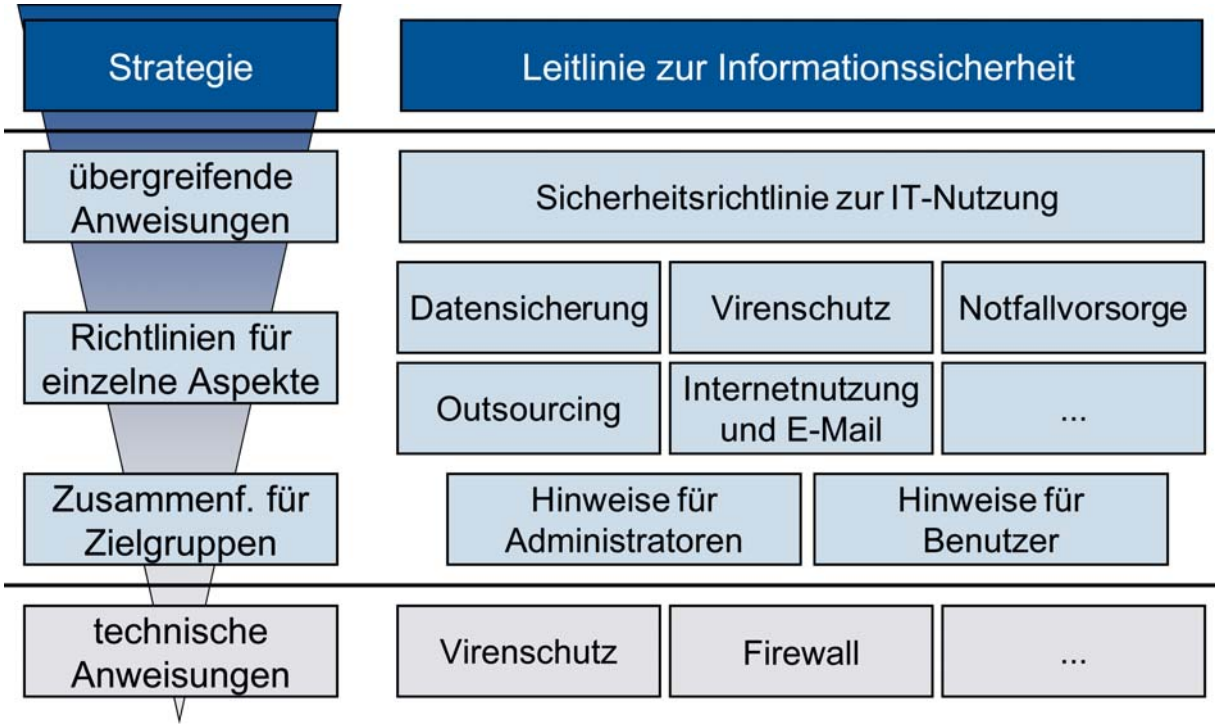

Abbildung 2: Einordnung der Musterdokumente

Abbildung 2 stellt den Zusammenhang zwischen den Musterrichtlinien dar und ordnet die Dokumente in das Ebenenmodell ein. Im folgenden Text werden die Musterdokumente kurz beschrieben. Es wird erklärt, warum eine bestimmte Richtlinie erstellt werden sollte und welche Inhalte sie enthält. Einige Beispielsätze aus den Dokumenten helfen dabei, einen Eindruck von der Beschreibungstiefe zu bekommen.

3.1 Die Sicherheitsleitlinie als Basisdokument

Von entscheidender Bedeutung ist, dass die Unternehmensleitung strategische Vorgaben zur Informationssicherheit macht und für alle sichtbar Verantwortung übernimmt. Die "Sicherheitsphilosophie" eines Unternehmens sollte daher in einer Leitlinie zur Informationssicherheit (englisch: information security policy oder IT security policy) erläutert werden. Die Sicherheitsleitlinie sollte dabei den Stellenwert der IT für das Unternehmen deutlich machen und die grundlegenden Sicherheitsziele, die sich aus den Unternehmenszielen und den Geschäftsprozessen ableiten, beschreiben. Weiterhin sollte sie Aussagen zur Organisationsstruktur (z. B. die Ernennung eines IT-Sicherheitsbeauftragten) enthalten und grundlegende Rahmenbedingungen vorgeben. Die Leitlinie ist kurz und prägnant (wenige Seiten) und wird in der Regel sehr selten geändert bzw. aktualisiert. Sie gehört damit in die erste Ebene des oben beschriebenen Modells.

Beispiel für eine typische Passage in einer Sicherheitsleitlinie:

"Aufgrund gesetzlicher Vorgaben hat die Vertraulichkeit der Kundendaten einen hohen Stellenwert. Unberechtigte Datenzugriffe sollen daher verhindert werden. Virenschutz, eine sichere Internetanbindung sowie eine gute Ausbildung der Mitarbeiter sind daher zu gewährleisten."

3.2 Richtlinien zur IT-Nutzung, Internetnutzung und zum Outsourcing

Die nachfolgenden Dokumente gehören zur zweiten Ebene und füllen die Aussagen der Leitlinie zur Informationssicherheit mit organisatorischen und technischen Inhalten.

Sicherheitsrichtlinie zur IT-Nutzung

Es empfiehlt sich, die allgemeinen Zielvorgaben der Leitlinie zu konkretisieren und die wichtigsten organisationsweiten Maßnahmen des Sicherheitskonzeptes allgemeinverständlich und ohne technische Details in einer Richtlinie zusammenzufassen. Diese Richtlinie beschreibt die Grundzüge der organisationsweiten IT-Nutzung und führt die Mitarbeiter wie ein "roter Faden" durch das Sicherheitskonzept.

Gut durchdachte organisatorische Vorgaben sorgen dafür, dass bereits vor der Umsetzung konkreter technischer Maßnahmen eine Linie vorgegeben wird. Jeder Projektleiter hat so die Möglichkeit vor Projektbeginn (z. B. vor Beschaffungen oder der Konzeption von neuen Anwendungen) anhand der organisatorischen Richtlinien, die Sicherheitsanforderungen an sein Projekt zu definieren. Es zeigt sich in der Praxis immer wieder, dass es bei neuen Projekten wesentlich kostengünstiger und auch für alle Beteiligten verständlicher ist, Sicherheitsaspekte direkt von Anfang an zu berücksichtigen, als diese im nachhinein mühselig gegen vielerlei Widerstände einzuarbeiten.

Folgende Themen sollten in einer allgemeinen Sicherheitsrichtlinie zur IT-Nutzung behandelt werden:

- Umgang mit schützenswerten Informationen (Festlegung von Informationseigentümern, Pflicht zur Klassifizierung von Informationen nach Schutzbedürftigkeit)
- relevante Gesetze und Vorgaben
- Kurzbeschreibung wichtiger Rollen (z. B. IT-Sicherheitsbeauftragter, Administrator, IT-Benutzer)
- Ausbildung des Personals
- Pflicht zur Einrichtung von Vertretungsregelungen
- Anforderungen an die Verwaltung von IT (Beschaffung, Einsatz, Wartung, Revision und Entsorgung)
- grundlegende Sicherheitsmaßnahmen (Zutritt zu Räumen und Zugang zu IT-Systemen, Verschlüsselung, Virenschutz, Datensicherung, Notfallvorsorge)
- Regelungen für spezifische IT-Dienste (Datenübertragung, Internetnutzung)

Beispiel für einige typische Passage in einer Sicherheitsrichtlinie zur IT-Nutzung:

"Es ist ein Viren-Schutzprogramm zu installieren. Es sind regelmäßig Updates durchzuführen und die Viren-Signaturen zu aktualisieren. Näheres regelt ein Viren-Schutzkonzept."

"Vertrauliche Daten sind verschlüsselt zu speichern und dürfen nicht ungeschützt über Netze übertragen werden. Zur Verschlüsselung wird IT-Benutzern auf Antrag ein Programm zur Verfügung gestellt."

Weitere Richtlinien, die in der Praxis häufig benötigt werden, sind Richtlinien zur E-Mail- und Internetnutzung sowie zum Outsourcing, wenn Arbeits- oder Geschäftsprozesse einer Organisation ganz oder teilweise zu externen Dienstleistern ausgelagert werden sollen. Die Beispieldokumente bewegen sich wieder auf der zweiten, nicht technischen Ebene:

Richtlinie für Internet- und E-Mail-Nutzung

Aufgrund der großen Bedeutung einerseits und der nicht zu leugnenden Sicherheitsrisiken andererseits, sollten in einer speziellen Richtlinie kurz die Eckpunkte der Internetnutzung beschrieben werden. Unumgänglich ist dabei die Klarstellung, ob private Internetnutzung erlaubt oder verboten ist. Weiterhin können folgende Punkte geregelt werden:

- Aussagen zur Netzarchitektur
- organisatorische Regelungen (personen- und funktionsbezogene E-Mail-Adressen, Vertretungsregeln, ...)
- Anforderungen an eine Firewall
- erlaubte bzw. nicht erlaubte Dienste und Protokolle
- grundlegende Einstellungen von Browser und E-Mail-Client
- Verhaltensregeln
- ...

Richtlinie für das Outsourcing von IT-Leistungen

Um die Risiken von Outsourcing-Projekten zu begrenzen und Projektleitern klare Richtlinien an die Hand zu geben, sollten alle Unternehmen, die Outsourcing-Verträge abschließen möchten, die wichtigsten Sicherheitsvorgaben zusammenstellen. Das Musterdokument macht einen Vorschlag zur Formulierung einer entsprechenden Richtlinie.

3.3 Konzepte für Virenschutz, Datensicherung, Archivierung und Notfallvorsorge

Zentrale Themen der Informationssicherheit sind Virenschutz, Datensicherung und Notfallvorsorge. In der Richtlinie zur IT-Nutzung wird daher gefordert, dass diese Themen im Sicherheitskonzept zu behandeln sind. Um alle Mitarbeiter über die wichtigsten Sicherheitsmaßnahmen zu informieren, sollten die elementaren Regeln allgemein verständlich zusammengestellt werden, ohne auf technische Details (wie die Konfiguration des Viren-Schutzprogramms) einzugehen. Ziel ist es, dass alle Mitarbeiter wissen, welche konkreten Pflichten sie persönlich haben und aus welchen Gründen die Maßnahmen durchgeführt werden sollen.

Aufgrund ihres Umfangs werden die Musterdokumente des BSI nicht "Richtlinien", sondern "Konzepte" genannt. Da die Musterkonzepte keine technischen Details enthalten, gehören sie ebenfalls in die zweite Ebene.

Die Konzepte enthalten aber nicht nur Regelungen, sondern dienen auch zur Sensibilisierung und Ausbildung der Mitarbeiter. Da sie für alle Mitarbeiter und nicht nur für IT-Experten relevant sind, werden die wichtigsten Sicherheitsmaßnahmen ausführlich begründet. So enthält beispielsweise das Viren-Schutzkonzept ein Glossar mit den wichtigsten Fakten zu Computer-Viren und beschreibt die häufigsten Infektionswege.

Viren-Schutzkonzept

Um einen umfassenden Virenschutz zu erreichen, sind Sicherheitsmaßnahmen aus unterschiedlichen Bereichen erforderlich. Neben technischen Maßnahmen sind z. B. Zuständigkeiten und Verantwortungen festzulegen, Abläufe zu beschreiben und Mitarbeiter zu schulen. Auch Maßnahmen zur sicheren Internutzung sind ein wichtiger Bestandteil des Virenschutzes. Ein erfolgreicher Virenschutz hängt entscheidend davon ab, dass sich alle Mitarbeiter und nicht nur die Administratoren beteiligen und wissen, wie man Virenangriffe im Vorfeld erkennen und vermeiden kann. Die IT-Grundschutz-Kataloge empfehlen daher die Erstellung eines Viren-Schutzkonzeptes. Es bildet den organisatorischen Rahmen für viele Einzelmaßnahmen und stellt übersichtlich die wichtigsten Aspekte des Virenschutzes dar.

Folgende Gliederung bietet sich an:
- Darstellung von Schadensszenarien zur Sensibilisierung
- Beschreibung der gängigen Infektionswege (E-Mail, Internet, internes Netz, Datenträger)
- Pflicht zur Erfassung der bedrohten Systeme
- Festlegung der Sicherheitsmaßnahmen
- Schulung
- Viren-Schutzprogramme
- E-Mail
- Internet
- Download
- Firewall
- Dialerschutz

- Schutz vor Makro-Viren
- BIOS-Einstellungen
- Benennung eines Computer-Viren-Verantwortlichen
- Verhaltensregeln zur Vorbeugung (Administrator, Benutzer)
- Verhaltensregeln bei Viren-Vorfall (Administrator, Benutzer)
- Glossar

Datensicherungskonzept

Die Datensicherung ist eine der wichtigsten Standard-Sicherheitsmaßnahmen. Sie muss in der Weise durchgeführt werden, dass bei einem Schadensfall alle wichtigen Daten problemlos und zügig wiederhergestellt werden können. In der Praxis ist in vielen Unternehmen nur unzureichend geregelt,

- wo Daten gespeichert werden,
- welche Daten überhaupt gesichert werden,
- wer für Datensicherungen zuständig ist,
- wie gesichert wird (Technik, Sicherungsmedien, Intervalle),
- wie lange Datensicherungen aufbewahrt werden,
- wie mit Notebooks zu verfahren ist, die nicht ständig am Netz angeschlossen sind,
- wie überprüft wird, ob die Datensicherungen tatsächlich zuverlässig funktioniert haben,
- wie Daten im Schadensfall rekonstruiert werden können.

In einem Datensicherungskonzept müssen daher die wichtigsten organisatorischen Rahmenbedingungen festgelegt werden (ohne auf spezielle Produkte oder Details einzugehen).

Archivierungskonzept

Die Archivierung ist unabhängig von der Datensicherung zu betrachten. Bei der Archivierung kommt es darauf an, elektronische Dokumente und andere Daten dauerhaft und unveränderbar zu speichern. Dabei kommt der Integrität der archivierten Dokumente eine besondere Bedeutung zu.

Ein Archivierungskonzept sollte die folgenden Punkte regeln:

- Aufbewahrungsfristen (einschlägige Gesetze, Vorschriften und interne Regelungen)
- Auswahl eines geeigneten Archivsystems (technische, organisatorische und rechtliche Einflussfaktoren)
- Gestaltung der Archivierung (Archivräume, Archivmedien, Datenformate, Aufbewahrungsstruktur, Indizierung, Entnahme, Vernichtung)
- Aktualisierung des Archivierungskonzepts (besonders wichtig aufgrund veränderter technischer Gegebenheiten wie aktualisierte Hardware oder neue Datenformate)

Wartungs- und Test-Prozeduren sind bei der Archivierung besonders wichtig, um auch nach einer längeren Archivierungszeit noch alle elektronisch gespeicherte Dokumente fehlerfrei rekonstruieren und lesen zu können.

Notfallvorsorgekonzept

Die Notfallvorsorge umfasst Maßnahmen, die auf die Wiederherstellung der Betriebsfähigkeit nach (technisch bedingtem bzw. durch fahrlässige oder vorsätzliche Handlungen herbeigeführtem) Ausfall eines IT-Systems ausgerichtet sind. Im Notfall hat die Aufrechterhaltung der wichtigsten Geschäftsprozesse oberste Priorität. Im Vorfeld muss daher ein Notfall sorgfältig vorbereitet werden. Im Ernstfall wissen dann alle Beteiligten, was zu tun ist und haben die Chance, ruhig und routiniert den Wiederanlauf aller Systeme zu bewältigen.

Ein Notfallvorsorgekonzept gibt die organisatorischen Rahmenbedingungen für Notfälle vor und sollte unter anderem Folgendes behandeln:

- Regelung der Verantwortlichkeiten (z. B. Notfall-Verantwortlicher, Notfall-Team, Leitungsebene, Pressestelle)
- Erstellung spezieller Notfallpläne (z. B. für Brand, Stromausfall, Hardware-Ausfall, Ausfall von Fachanwendungen, Virenbefall, Sabotage)
- Erstellung von Dokumentationen (Prozesse, Anwendungen, IT-Systeme, Verfügbarkeitsanforderungen, Wiederanlaufreihenfolge, Ersatzverfahren und Ausweichmöglichkeiten etc.)

- Verhaltensregeln bei Sicherheitsvorfällen und Notfällen
- Alarmierungspläne
- Eskalationsstrategie
- Notfallübungen

3.4 Sicherheitshinweise für Benutzer und Administratoren

In jeder Richtlinie bzw. in jedem Konzept werden an vielen unterschiedlichen Stellen Verhaltensregeln und Aufgaben für Benutzer und Administratoren beschrieben. Fassen die IT-Sicherheitsbeauftragten die wichtigsten Aufgaben und Pflichten der Benutzer sowie der Administratoren übersichtlich und leicht verständlich in entsprechenden Papieren zusammen, können diese als "Sicherheitshinweise für Benutzer" bzw. "Sicherheitshinweise für Administratoren" zur Sensibilisierung genutzt, und auch als Arbeitsanweisung oder Zusatz zum Arbeitsvertrag verwendet werden.

Folgende Themen könnten in extra Papieren als Sicherheitshinweise zusammengestellt werden:

- Verpflichtung auf die Einhaltung der relevanten Gesetze
- Teilnahme an Schulungen vor Programmnutzung
- Regelungen zur Nutzung privater Hard- und Software
- Installation und Konfiguration von Anwendungen
- Regeln für sichere Passwortgestaltung
- Umgang mit vertraulichen Informationen
- Hinweise Die Notfallvorsorge umfasst Maßnahmen, die auf die Wiederherstellung der Betriebsfähigkeit nach (technisch bedingtem bzw. durch fahrlässige oder vorsätzliche Handlungen herbeigeführten) Ausfall eines IT-Systems ausgerichtet sind.
- Verhaltung bei Sicherheitsvorfällen

4 Veröffentlichung von Musterkonzepten

Viele Anwender der IT-Grundschutz-Kataloge wünschen sich mehr konkrete Beispiele. Das BSI freut sich daher, wenn Unternehmen und Behörden ihre individuellen Sicherheitsrichtlinien und -konzepte (gerne auch anonymisiert) anderen IT-Grundschutz-Anwendern als Musterbeispiele zur Verfügung stellen. Wer möchte, kann entsprechendes Material an das IT-Grundschutz-Referat unter grundschutz@bsi.bund.de einschicken. Die eingesandten Papiere werden auf der Webseite in der Rubrik Hilfsmittel veröffentlicht.