Bundesamt
für Sicherheit in der
Informationstechnik

Online-Kurs IT-Grundschutz

Druckversion

Stand: 07.08.2018

Änderungshistorie

Dieses Dokument enthält die Druckversion des Online-Kurses IT-Grundschutz

Version	Datum	Name	Beschreibung
0.9	06.06.2018	Fraunhofer SIT	Finaler Entwurf
1.0	07.08.2018	Fraunhofer SIT	Finale Version

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5369
E-Mail: grundschutz@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Lektion 1:Einstieg ... 7
Lerneinheit 1.1:Warum IT-Grundschutz? ... 8
Lerneinheit 1.2:IT-Grundschutz – Bestandteile ... 9
Lerneinheit 1.3:Über diesen Kurs ... 10
Lektion 2:Sicherheitsmanagement ... 13
Lerneinheit 2.1:Der Sicherheitsprozess ... 14
Lerneinheit 2.2:Die Phasen des Sicherheitsprozesses ... 15
Lerneinheit 2.3:Verantwortung und Aufgaben der Leitung ... 16
Lerneinheit 2.4:Der Informationssicherheitsbeauftragte ... 17
Lerneinheit 2.5:Der ICS-Informationssicherheitsbeauftragte ... 17
Lerneinheit 2.6:Das IS-Management-Team ... 18
Lerneinheit 2.7:Die Sicherheitsleitlinie ... 20
Lerneinheit 2.8:Das Sicherheitskonzept ... 21
Lerneinheit 2.9:Wahl der Vorgehensweise ... 22
Lerneinheit 2.10:Testfragen ... 23
Lektion 3:Strukturanalyse ... 25
Lerneinheit 3.1:Das Beispielunternehmen RECPLAST ... 26
Lerneinheit 3.2:Objekte gruppieren ... 27
Lerneinheit 3.3:Geschäftsprozesse und Informationen erheben ... 28
Lerneinheit 3.4:Anwendungen erheben ... 29
Lerneinheit 3.5:Netzplan erheben ... 31
Lerneinheit 3.6:IT-Systeme erheben ... 33
Lerneinheit 3.7:Räume erheben ... 36
Lerneinheit 3.8:Testfragen ... 37
Lektion 4:Schutzbedarfsfeststellung ... 39
Lerneinheit 4.1:Grundlegende Definitionen ... 39
Lerneinheit 4.2:Schutzbedarfskategorien ... 40
Lerneinheit 4.3:Vorgehen und Vererbung ... 41
Lerneinheit 4.4:Schutzbedarfsfeststellung für Prozesse und Anwendungen ... 42
Lerneinheit 4.5:Schutzbedarfsfeststellung für IT-Systeme ... 43
Lerneinheit 4.6:Schutzbedarfsfeststellung für Räume ... 45
Lerneinheit 4.7:Schutzbedarfsfeststellung für Kommunikationsverbindungen ... 46
Lerneinheit 4.8:Testfragen ... 47
Lektion 5:Modellierung gemäß IT-Grundschutz ... 49
Lerneinheit 5.1:IT-Grundschutz-Bausteine ... 50
Lerneinheit 5.2:Schichtenmodell ... 51
Lerneinheit 5.3:Vorgehen ... 52
Lerneinheit 5.4:Dokumentation ... 53
Lerneinheit 5.5:Anforderungen anpassen ... 54
Lerneinheit 5.6:Testfragen ... 54

Lektion 6:IT-Grundschutz-Check ... 56
Lerneinheit 6.1:Anforderungen ... 57
Lerneinheit 6.2:Vorbereitung und Durchführung ... 57
Lerneinheit 6.3:Dokumentation ... 58
Lerneinheit 6.4:Entscheidungskriterien ... 60
Lerneinheit 6.5:Beispiel ... 61
Lerneinheit 6.6:Testfragen ... 62
Lektion 7:Risikoanalyse ... 64
Lerneinheit 7.1:Organisatorische Rahmenbedingungen ... 65
Lerneinheit 7.2:Zielobjekte zusammenstellen ... 65
Lerneinheit 7.3:Die elementaren Gefährdungen ... 66
Lerneinheit 7.4:Gefährdungsübersicht anlegen ... 67
Lerneinheit 7.5:Gefährdungsübersicht ergänzen ... 68
Lerneinheit 7.6:Häufigkeit und Auswirkungen einschätzen ... 70
Lerneinheit 7.7:Risiken bewerten ... 71
Lerneinheit 7.8:Beispiel für die Risikobewertung ... 72
Lerneinheit 7.9:Risiken behandeln ... 73
Lerneinheit 7.10:Die nächsten Schritte ... 75
Lerneinheit 7.11:Testfragen ... 76
Lektion 8:Umsetzungsplanung ... 78
Lerneinheit 8.1:Maßnahmen konsolidieren ... 79
Lerneinheit 8.2:Aufwände schätzen ... 80
Lerneinheit 8.3:Umsetzungsreihenfolge und Verantwortlichkeit festlegen ... 81
Lerneinheit 8.4:Begleitende Maßnahmen planen ... 82
Lerneinheit 8.5:Planung dokumentieren ... 83
Lerneinheit 8.6:Testfragen ... 83
Lektion 9:Aufrechterhaltung und Verbesserung ... 85
Lerneinheit 9.1:Leitfragen für die Überprüfung ... 86
Lerneinheit 9.2:Überprüfungsverfahren ... 87
Lerneinheit 9.3:Kennzahlen ... 88
Lerneinheit 9.4:Reifegradmodelle ... 89
Lerneinheit 9.5:IT-Grundschutz-Zertifizierung ... 90
Lerneinheit 9.6:Testfragen ... 92
Anhang: Lösungen zu den Testfragen ... 94
Zu Lektion 2: Sicherheitsmanagement ... 94
Zu Lektion 3: Strukturanalyse ... 95
Zu Lektion 4: Schutzbedarfsfeststellung ... 96
Zu Lektion 5: Modellierung ... 97
Zu Lektion 6: IT-Grundschutz-Check ... 98
Zu Lektion 7: Risikoanalyse ... 100
Zu Lektion 8: Umsetzungsplanung ... 101
Zu Lektion 9: Aufrechterhaltung und Verbesserung ... 102

Abbildungsverzeichnis

Abbildung 1: Komponenten eines ISMS ... 13
Abbildung 2: PDCA-Zyklus ... 14
Abbildung 3: Phasen des Sicherheitsprozesses ... 15
Abbildung 4: Organisation der Informationssicherheit – Rollen ... 18
Abbildung 5: Varianten der IT-Grundschutz-Methodik ... 23
Abbildung 6: Schritte bei der Variante Standard-Absicherung der IT-Grundschutz-Methodik ... 24
Abbildung 7: Organigramm der RECPLAST GmbH ... 27
Abbildung 8: Vereinfachter Netzplan der RECPLAST GmbH ... 28
Abbildung 9: Bereinigter Netzplan ... 34
Abbildung 10: Schichtenmodell ... 52
Abbildung 11: Anforderungen der IT-Grundschutz-Bausteine und Varianten der Vorgehensweise ... 58
Abbildung 12: Entscheidungsprozess beim IT-Grundschutz-Check ... 60
Abbildung 13: Beispiel einer Risikomatrix ... 72
Abbildung 14: Risikomatrix mit eingetragener Gefährdung ... 74
Abbildung 15: Risikobehandlung ... 75
Abbildung 16: Phasen des Sicherheitsprozesses ... 87
Abbildung 17: Beispiel für die Visualisierung von Reifegraden ... 90
Abbildung 18: ISO 27001-Zertifizierung auf Basis von IT-Grundschutz - Prozess ... 92

Tabellenverzeichnis

Tabelle 1: Liste der Geschäftsprozesse der RECPLAST GmbH (Auszug) ... 30
Tabelle 2: Liste der Anwendungen (Auszug) ... 32
Tabelle 3: Zuordnung von Anwendungen zu Geschäftsprozessen ... 32
Tabelle 4: Liste der IT-Systeme (Auszug) ... 36
Tabelle 5: Zuordnung der Anwendungen zu Netzkomponenten (Auszug) ... 36
Tabelle 6: Liste der Räume (Auszug) ... 37
Tabelle 7: Schutzbedarf von Anwendungen (Auszug) ... 44
Tabelle 8: Schutzbedarf der IT-Systeme (Auszug) ... 45
Tabelle 9: Schutzbedarf der Räume (Auszug) ... 46
Tabelle 10: kritische Kommunikationsverbindungen (Auszug) ... 48
Tabelle 11: Sprachgebrauch in den IT-Grundschutz-Bausteinen ... 51
Tabelle 12: Dokumentation der IT-Grundschutz-Modellierung ... 54
Tabelle 13: Beispiel für die Dokumentation des IT-Grundschutz-Checks ... 63
Tabelle 14: Beispiele für elementare Gefährdungen ... 68
Tabelle 15: Beispiel für die Klassifikation von Häufigkeiten ... 71
Tabelle 16: Beispiel für die Klassifikation von Schadensauswirkungen ... 71
Tabelle 17: Beispiel für die Klassifikation von Risiken ... 72
Tabelle 18: Beispiel für die tabellarische Dokumentation der Risikoanalyse ... 74
Tabelle 19: Beispiel für die Dokumentation der Umsetzungsplanung ... 84
Tabelle 20: Beispiele für Kennzahlen zur Informationssicherheit ... 89
Tabelle 21: Beispiel für die Definition von Reifegraden ... 90

Lektion 1: Einstieg

Für Unternehmen und Behörden ist es heutzutage unerlässlich, dass **Informationen** korrekt vorliegen und vertraulich behandelt werden. Entsprechend wichtig ist auch, dass die **technischen Systeme**, auf denen Informationen gespeichert, verarbeitet oder übertragen werden, reibungslos funktionieren und **wirksam gegen vielfältige, immer wieder neuartige Gefährdungen geschützt** sind.

- Wüssten Sie gerne, ob die bei Ihnen umgesetzten Maßnahmen für Informationssicherheit ausreichen, um schwere Schäden zu verhindern und auf Sicherheitsvorfälle angemessen reagieren zu können?
- Benötigen Sie Hilfe bei der Entwicklung eines Sicherheitskonzepts?
- Suchen Sie Unterstützung für die systematische Überprüfung der in Ihrem Zuständigkeitsbereich vorhandenen oder geplanten Sicherheitsmaßnahmen?
- Möchten Sie, dass diese Maßnahmen allgemein anerkannten Standards genügen?

Wenn Sie eine dieser Fragen mit „Ja“ beantworten, dann sollten Sie sich mit dem **IT-Grundschutz** beschäftigen. Dort wird detailliert beschrieben, welche **Anforderungen** erfüllt sein müssen, um kostengünstig ein für übliche Einsatzbereiche und Schutzanforderungen angemessenes und bei höherem Schutzbedarf leicht ausbaufähiges Sicherheitsniveau zu erlangen. Er bietet zudem eine weithin anerkannte **Methodik**, mit der Sie auf effiziente Weise ein zu den Gegebenheiten Ihrer Einrichtung passendes Sicherheitskonzept entwickeln und überprüfen können.

Es gibt viele Wege zur Informationssicherheit, mit dem IT-Grundschutz haben Sie die Möglichkeit, dieses Ziel effizient zu erreichen, unterwegs Umwege zu vermeiden und mögliche Gefährdungen im Blick zu behalten. Bildlich gesprochen: **IT-Grundschutz ist nicht nur eine Landkarte, sondern ein Wegweiser für Informationssicherheit!**

Lerneinheit 1.1: Warum IT-Grundschutz?

Informationssicherheit muss **vielfältigen Herausforderungen** gerecht werden:

- **Komplexität der Gefährdungslage:** Gefährdungen können unterschiedlichste Ursachen haben und auf mannigfaltigen Wegen die Ziele der Informationssicherheit verletzen. Angriffe von Hackern, Fahrlässigkeiten oder technische Mängel sind ebenso im Blick zu behalten wie Naturkatastrophen und andere Formen höherer Gewalt.
- **Ganzheitlichkeit der Sicherheitskonzepte:** Informationssicherheit erfordert Maßnahmen auf mehreren Ebenen: Betroffen sind nicht nur die IT-Systeme, sondern auch die Organisation, das Personal, die räumliche Infrastruktur, die Arbeitsplätze und die betrieblichen Abläufe.
- **Zusammenwirken der Sicherheitsmaßnahmen**: Damit die eingesetzten Sicherheitsmaßnahmen die komplexe Gefährdungslage hinreichend in den Griff bekommen können, müssen die organisatorischen, technischen und infrastrukturellen Schutzvorkehrungen zu der jeweiligen Institution passen, an der tatsächlich bestehenden Gefährdungslage ausgerichtet sein, sinnvoll zusammenwirken und von der Leitung und den Beschäftigten unterstützt und beherrscht werden.
- **Angemessenheit der Sicherheitsmaßnahmen**: Es ist auch auf die Wirtschaftlichkeit und Angemessenheit der Sicherheitsmaßnahmen zu achten. Den bestehenden Gefährdungen muss zwar wirkungsvoll begegnet werden, die eingesetzten Maßnahmen sollten aber an dem tatsächlich bestehenden Schutzbedarf ausgerichtet sein und dürfen eine Institution nicht überfordern. Unangemessen kostspielige Maßnahmen sind zu vermeiden, ebenso solche Vorkehrungen, durch die wichtige Abläufe einer Institution über Gebühr behindert werden.
- **Erfüllung externer Anforderungen**: Es wird heutzutage für viele Unternehmen und Behörden immer wichtiger, nachweisen zu können, dass sie in ausreichendem Maße für Informationssicherheit gesorgt haben. Dieser Nachweis fällt leichter, wenn eine Institution ihre Vorkehrungen für Informationssicherheit an allgemein anerkannten Standards ausrichtet.
- **Nachhaltigkeit der Sicherheitsmaßnahmen**: Und nicht zuletzt gilt: Sicherheit ist kein einmal erreichter und fortan andauernder Zustand. Unternehmen und Behörden ändern sich und damit auch die in ihnen schützenswerten Informationen, Prozesse und Güter. Neuartige Schwachstellen und Bedrohungen

machen es in gleicher Weise erforderlich, die vorhandenen Sicherheitskonzepte zu überprüfen und weiterzuentwickeln.

Der **IT-Grundschutz des BSI** bietet eine gute Grundlage dafür, diesen Herausforderungen auf professionelle Weise gerecht zu werden und die Bemühungen für Informationssicherheit zu strukturieren. Er ermöglicht es Unternehmen und Behörden, systematisch nach Schwachstellen zu suchen, die Angemessenheit umgesetzter Schutzmaßnahmen zu prüfen und Sicherheitskonzepte zu entwickeln und fortzuschreiben, die zu den Geschäftsprozessen, Fachaufgaben und Organisationsstrukturen der Institution passen und allgemein anerkannten Standards genügen.

Lerneinheit 1.2: IT-Grundschutz – Bestandteile

Das **Angebot des BSI zum IT-Grundschutz** besteht aus einer Reihe von Einzelkomponenten. Den Kern bilden

- die **BSI-Standards zum IT-Grundschutz** mit Empfehlungen für den organisatorischen Rahmen und das methodische Vorgehen zur Gewährleistung von Informationssicherheit sowie
- das **IT-Grundschutz-Kompendium**, mit dem die in den BSI-Standards formulierten allgemeinen Empfehlungen zum Management von Informationssicherheit konkretisiert und umgesetzt werden können.

In diesem Kurs werden Sie diese Veröffentlichungen genauer kennenlernen und erfahren, welche Hilfestellungen sie Ihnen bei der Steuerung der Informationssicherheit in Ihrer Institution im Einzelnen geben. Nachfolgend einige grundlegende Informationen zur Einordnung dieser und weiterer Dokumente und Hilfsmittel zum IT-Grundschutz.

Die BSI-Standards zum IT-Grundschutz

Der BSI-Standard 200-1: *Managementsysteme für Informationssicherheit (ISMS)* beschreibt, welche grundlegenden Anforderungen ein Managementsystem für Informationssicherheit erfüllen muss, welche Komponenten es enthält und welche Aufgaben zu bewältigen sind. Die Darstellung orientiert sich an den Vorgaben der Norm ISO 27001 und weiterer aktueller internationaler Standards zur Informationssicherheit.

Der BSI-Standard 200-2: *IT-Grundschutz-Methodik* bietet methodische Hilfestellungen zur schrittweisen Einführung eines ISMS in einer Institution an und beschreibt effiziente Verfahren, um die allgemeinen Anforderungen des BSI-Standards 200-1 und der zugrunde liegenden Norm ISO/IEC 27001 zu konkretisieren.

In dem BSI-Standard 200-3: *Risikoanalyse auf der Basis von IT-Grundschutz* ist ein gegenüber anderen Methoden vereinfachtes Verfahren zur Risikoanalyse beschrieben. Diese Methode ist dann wichtig und hilfreich, wenn Komponenten abzusichern sind, bei denen fraglich ist, ob die Erfüllung von Basis- und Standard-Anforderungen für eine ausreichende Sicherheit genügt.

Das IT-Grundschutz-Kompendium

Das IT-Grundschutz-Kompendium ist ein modular aufgebautes umfangreiches **Arbeitsinstrument und Nachschlagewerk zur Informationssicherheit**. Es besteht aus den **IT-Grundschutz-Bausteinen**, die in zehn thematische Schichten eingeordnet sind und jeweils unterschiedliche Aspekte betrachten.

Jeder Baustein beginnt mit einer kurzen Einleitung, gefolgt von der Zielsetzung und Abgrenzung des betrachteten Gegenstands zu anderen Bausteinen mit thematischem Bezug. Im Anschluss daran wird pauschal die spezifische Gefährdungslage beschrieben. Danach folgen Sicherheitsanforderungen, die für den betrachteten Gegenstand relevant sind.

Der große Vorteil, den Sie als Anwender des IT-Grundschutz-Kompendiums haben: Sie müssen für die in den Bausteinen beschriebenen Sachverhalte bei normalem Schutzbedarf in der Regel keine aufwändigen Risikoanalysen mehr durchführen. Diese Arbeit wurde von erfahrenen Sicherheitsexperten vorab vorgenommen und ist in die Formulierung der Sicherheitsanforderungen eingeflossen.

Die Anforderungen in den Bausteinen beschreiben, **was** für eine angemessene Sicherheit getan werden sollte. **Wie** dies erfolgen kann oder sollte, ist in ergänzenden **Umsetzungshinweisen** beschrieben, die das BSI für die meisten Bausteine veröffentlicht.

Weitere Veröffentlichungen und Hilfsmittel

Darüber hinaus bietet das BSI weitere Dokumente, Werkzeuge und Hilfsmittel an, die dabei unterstützen, ein angemessenes Sicherheitsniveau umzusetzen. Hier sind die **IT-Grundschutz-Profile** zu nennen, Musterlösungen für ausgewählte Anwendungsbereiche, die Unternehmen oder Behörden einer Branche als Schablone für die Entwicklung ihrer Sicherheitskonzepte verwenden können. Ebenso die **ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz**, mit der eine Institution belegen kann, dass ihr Umgang mit Informationssicherheit sowie die umgesetzten technischen und organisatorischen Maßnahmen anerkannten Standards entsprechen.

Die **Webseiten des BSI** zum **Thema IT-Grundschutz** informieren umfassend über diese und weitere nützliche Angebote. Sie finden dort ebenfalls elektronische Versionen der BSI-Standards und des IT-Grundschutz-Kompendiums sowie Hinweise zum Bezug der gedruckten Fassungen dieser Dokumente.

Zur Unterstützung der IT-Grundschutz-Methodik gibt es auch von unterschiedlichen Herstellern eine Reihe an **Software-Tools**. Der Einsatz eines solchen Werkzeugs ist zweckmäßig und ab einer gewissen Größe der Institution auch anzuraten. Im Informationsangebot des BSI finden Sie auch hierzu eine Übersicht und weitere Hinweise.

Falls Sie den **fachlichen Austausch zum IT-Grundschutz** suchen und mit anderen Anwendern und Interessenten in Kontakt treten möchten, haben Sie hierzu in einer eigenen Gruppe zum IT-Grundschutz bei XING Gelegenheit. Alle **aktuellen Neuigkeiten** zum IT-Grundschutz finden Sie auch bei TWITTER. Wenn Sie zeitnah über den IT-Grundschutz auf dem Laufenden bleiben möchten, können Sie sich ferner beim BSI für den Bezug des **IT-Grundschutz-Newsletters** registrieren lassen (zur Registrierung).

Lerneinheit 1.3: Über diesen Kurs

Unterschiedliche Institutionen haben auch unterschiedliche Voraussetzungen und Ausgangspunkte für eine ganzheitliche Umsetzung von Informationssicherheit. So haben insbesondere kleinere und mittelgroße Institutionen oft nicht die personellen und finanziellen Ressourcen für eine umfassende Absicherung in einem Schritt. Für sie kann es daher zielführender sein, sich zunächst auf die Umsetzung elementarer

Sicherheitsmaßnahmen oder die gezielte Absicherung besonders schützenswerter Bereiche zu konzentrieren. Die im BSI-Standard 200-2 beschriebene **IT-Grundschutz-Methodik** sieht daher **drei Varianten** vor, mit denen eine Institution ein ihren Anforderungen und Gegebenheiten gemäßes Sicherheitsniveau erreichen kann:

- Die **Basis-Absicherung** bietet einen einfachen Einstieg in das systematische Management der Informationssicherheit und zeigt, wie eine Institution ohne differenzierte Bewertungen des Schutzbedarfs und ergänzende Risikoanalysen ihr Sicherheitsniveau durch die Erfüllung besonders wichtiger Basis-Anforderungen signifikant erhöhen kann. Wenn Sie genauer wissen möchten, wie es geht: Der Leitfaden zur Basis-Absicherung nach IT-Grundschutz: In drei Schritten zur Informationssicherheit liefert einen kompakten und übersichtlichen Einstieg in das besonders für kleine und mittlere Unternehmen und Behörden interessante Vorgehen.
- Mit Hilfe der **Standard-Absicherung** kann eine Institution ausgehend von einer systematischen Erfassung der verschiedenen Komponenten, die im Sicherheitskonzept zu berücksichtigen sind, und der Bewertung ihres Schutzbedarfs mit Hilfe des IT-Grundschutz-Kompendiums und mit in Einzelfällen zusätzlich erforderlichen Risikoanalysen eine umfassende Absicherung erreichen.
- Die **Kern-Absicherung** umfasst alle Schritte der Standard-Absicherung, konzentriert sich dabei aber auf ausgewählte, besonders wichtige Bereiche (die „Kronjuwelen“) einer Institution.

Gliederung

Die Entscheidung für eine dieser Vorgehensweisen und ihre Anwendung setzt voraus, dass eine Institution gewisse organisatorische Grundlagen geschaffen hat. Was dazu gehört, erfahren Sie in diesem Kurs in der Lektion 2: *Sicherheitsmanagement*.

In darauf folgenden Lektionen lernen Sie detailliert die einzelnen **Schritte bei der Standard-Absicherung** gemäß IT-Grundschutz kennen:

- Lektion 3: *Strukturanalyse*,
- Lektion 4: *Schutzbedarfsfeststellung*,
- Lektion 5: *Modellierung gemäß IT-Grundschutz*,
- Lektion 6: *IT-Grundschutz-Check*,
- Lektion 7: *Risikoanalyse,*
- Lektion 8: *Umsetzungsplanung*.

Sicherheit ist kein einmal herzustellender Zustand, sondern ein kontinuierlicher Prozess, bei dem einmal getroffene Entscheidungen und umgesetzte Maßnahmen immer wieder auf ihre Angemessenheit und Wirksamkeit geprüft und an neue Gegebenheiten angepasst werden müssen. In der abschließenden Lektion 9: *Aufrechterhaltung und Verbesserung* lernen Sie Verfahren kennen, mit denen Sie für ein nachhaltig gutes Sicherheitsniveau in Ihrer Einrichtung sorgen können. Dort erfahren Sie auch mehr zur **Zertifizierung gemäß ISO 27001 auf der Basis von IT-Grundschutz**.

Das Beispielunternehmen RECPLAST GmbH

Die einzelnen Schritte der IT-Grundschutz-Methodik werden mithilfe eines durchgängig verwendeten Beispiels veranschaulicht. Es handelt sich dabei um das fiktive Unternehmen RECPLAST GmbH, das auch in den BSI-Standards als Beispiel dient. Dort wie auch im Kurs werden Ihnen Auszüge aus den Ergebnisdokumenten der verschiedenen Phasen der IT-Grundschutz-Methodik vorgestellt. Eine umfassende Darstellung finden Sie in einem eigenem PDF-Dokument.

Zu den verwendeten Piktogrammen

In diesem Kurs dienen die folgenden Piktogramme zur Hervorhebung von Textpassagen:

Merksätze, Empfehlungen oder aus anderen Gründen besonders wichtige Textteile sind durch ein Ausrufezeichen hervorgehoben.

Hinweise auf vertiefende oder ergänzende Informationen in den grundlegenden Dokumenten zum IT-Grundschutz oder in anderen Quellen werden durch ein Buch illustriert.

Dieses Symbol kennzeichnet Fragen und Übungen, mit denen Sie Ihr neu erworbenes Wissen zum IT-Grundschutz überprüfen können.

Dieses Symbol kennzeichnet Abschnitte, in denen auf das in diesem Kurs durchgängig verwendete (fiktive) Beispielunternehmen, die RECPLAST GmbH, eingegangen wird.

Hinweis zum Sprachgebrauch

Aus Gründen der Lesbarkeit wird auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet. Alle Angaben beziehen sich auf Angehörige beider Geschlechter.

Lektion 2: Sicherheitsmanagement

Jede Institution benutzt heute Sicherheitstechnik, um sich vor Gefahren aus dem Internet abzusichern. Dazu gehören fast immer Virenschutzprogramme und Spamfilter, oft aber auch komplexere Lösungen wie gestaffelte Firewalls und Software zur Angriffserkennung. Darüber hinaus ergreifen Behörden und Unternehmen organisatorische Maßnahmen, etwa indem sie Richtlinien für die Benutzung mobiler Systeme erlassen oder die ihre Mitarbeiter über Gefahren im Internet informieren. Sowohl die Anwendung von Technik als auch die Einführung organisatorischer Maßnahmen erfolgt oft jedoch ohne Konzept und Erfolgskontrolle.

Für eine angemessene Informationssicherheit ist die isolierte Umsetzung einzelner technischer oder organisatorischer Maßnahmen erfahrungsgemäß allerdings weder effektiv noch effizient. Vielmehr ist ein Rahmen erforderlich, der dafür sorgt, dass alle Maßnahmen zielgerichtet gesteuert und überwacht werden. Ein solches **Informationssicherheitsmanagementsystem (ISMS)** besteht aus folgenden Komponenten:

- **Managementprinzipien**,
  etwa der Vorgabe von Zielen in der Organisation, der Erstellung von Kommunikationsgrundsätzen oder Regelungen für Kosten-Nutzen-Analysen,
- **Ressourcen und Mitarbeitern**,
  dies umfasst die Steuerung des Einsatzes von Technik und Personal sowie
- der Beschreibung eines **Sicherheitsprozesses**.

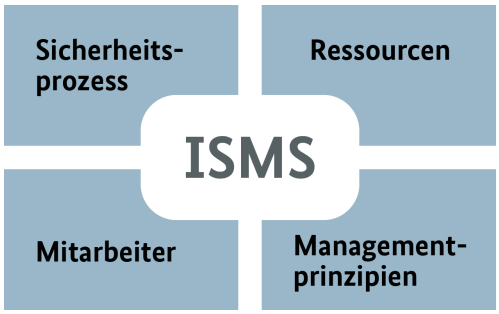


Abbildung 1: Komponenten eines ISMS

Aber worauf sollten Sie beim Aufbau und Betrieb eines ISMS achten?

Antworten hierzu finden Sie im BSI-Standard 200-1: *Managementsysteme für Informationssicherheit (ISMS)*. Die dort genannten Empfehlungen werden im BSI-Standard 200-2: *IT-Grundschutz-Methodik* konkretisiert. In den Kapiteln 3 und 4 erfahren Sie dort beispielsweise, worauf bei der Initiierung und Organisation des Sicherheitsprozesses zu achten ist.

In dieser Lektion lernen Sie die wesentlichen Aspekte des Managements von Informationssicherheit gemäß IT-Grundschutz kennen:

- Wie gestaltet sich der Sicherheitsprozess?
- Was sind die grundlegenden Managementprinzipien?
- Wie wird eine gute Sicherheitsorganisation aufgebaut?
- Wie wird eine Sicherheitsleitlinie formuliert?
- Was sind die grundlegenden Schritte zum Sicherheitskonzept?
- Wie sieht eine gute Dokumentation aus?

Lerneinheit 2.1: Der Sicherheitsprozess

Informationssicherheit ist kein Zustand, der einmal erreicht wird und dann fortbesteht, sondern ein Prozess, der kontinuierlich angepasst werden muss. Geänderte Verfahren und Prozesse in einer Institution, der Wandel in den gesetzlichen Rahmenbedingungen, neue Technik, aber auch bislang unbekannte Schwachstellen und daraus erwachsende Gefährdungen stellen immer wieder neue Anforderungen, so dass die nachhaltige Angemessenheit und Wirksamkeit nicht automatisch gewährleistet sind. Der gesamte **Sicherheitsprozess unterliegt daher einem Lebenszyklus**, der sich in folgende Phasen gliedert:

- **Plan** – Planung von Sicherheitsmaßnahmen,
- **Do** – Umsetzung der Maßnahmen,
- **Check** – Erfolgskontrolle, Überwachung der Zielerreichung,
- **Act** – Beseitigung von Defiziten, Verbesserung.

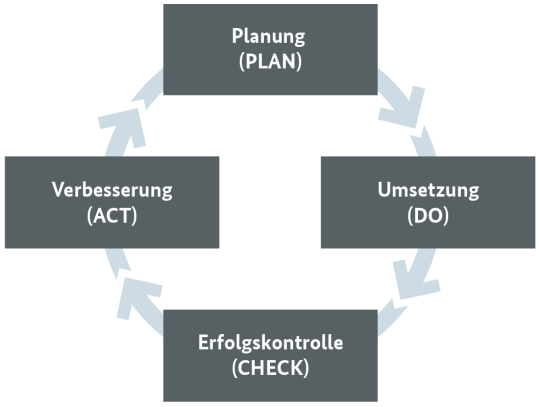


Abbildung 2: PDCA-Zyklus

Dieser **PDCA-Zyklus** nach William Edwards Deming ist ein bewährter Bestandteil vieler Managementsysteme, etwa auch des Qualitäts- und Umweltmanagements.

Insbesondere die **Erfolgskontrolle und die kontinuierliche Verbesserung** gehören zu den wichtigsten Managementprinzipien im Sicherheitsprozess. Ohne regelmäßige Überprüfung ist die Wirksamkeit der organisatorischen und technischen Schutzmaßnahmen auf Dauer nicht sichergestellt.

Dokumentation ist kein Selbstzweck, eine **gute Dokumentation** trägt aber dazu bei, den Sicherheitsprozess und getroffene Entscheidungen nachvollziehbar zu gestalten und Missverständnisse zu vermeiden. Sie muss nicht in Papierform vorliegen. Eine elektronische Form hat den Vorteil, leicht aktualisierbar und bei Bedarf schnell verfügbar zu sein, wobei die Zugriffsrechte sorgfältig zu regeln sind.

Um Informationen angemessen schützen zu können, muss ihre Bedeutung für die Institution klar sein. Dies kann durch eine **Informationsklassifizierung** unterstützt werden, bei der Dokumente gemäß ihrer Vertraulichkeit klassifiziert werden und für deren Behandlung Regeln festgelegt sind, die dieser Klassifizierung entsprechen. Durch einen Klassifizierungsvermerk kann jeder Mitarbeiter unmittelbar erkennen, wie er mit den eingestuften Informationen umzugehen hat.

Weitere wichtige Hinweise über die Anforderungen an die Dokumentation sowie über die Gestaltung von Informationsflüssen und Meldewegen im Sicherheitsprozess finden Sie in Kapitel 5 des BSI-Standards 200-2: *IT-Grundschutz-Methodik*. Am Beginn dieses Kapitels ist auch ein Vorgehensmodell zur Informationsklassifizierung beschrieben.

Lerneinheit 2.2: Die Phasen des Sicherheitsprozesses

Damit ein geregelter Sicherheitsprozess etabliert werden kann, muss die Leitungsebene ihn initiieren, Ziele und Rahmenbedingungen festlegen, eine Organisationsstruktur aufbauen und Ressourcen bereitstellen.

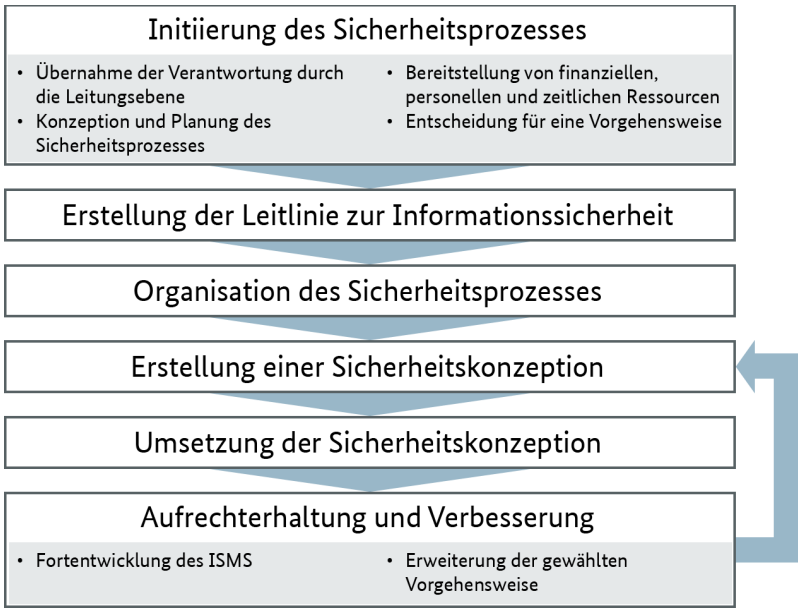


Abbildung 3: Phasen des Sicherheitsprozesses

Im Einzelnen gliedert sich der Sicherheitsprozess in die nachfolgend dargestellten Phasen und Teilaktivitäten.

1. Initiierung, Erstellung einer Informationssicherheitsleitlinie und Aufbau einer Sicherheitsorganisation

Damit der Sicherheitsprozess den eigenen Erfordernissen entspricht, müssen zunächst die relevanten **Rahmenbedingungen** identifiziert und analysiert werden. Hierzu gehören etwa die Sicherheitsanforderungen, die Kunden stellen oder Behörden als Auflagen formulieren. Wenn es regulatorische Auflagen gibt, werden diese die Sicherheitsziele und die zu entwickelnden Konzepte stark beeinflussen. Wenn es bereits Initiativen in der Institution gibt, Informationssicherheit voranzutreiben, müssen diese ermittelt und bewertet werden, und sollten bereits technische oder organisatorische Maßnahmen umgesetzt sein, müssen diese in den neu zu gestalteten Prozess integriert werden.

Großen Einfluss auf den Sicherheitsprozess haben die Ziele, die sich mit ihm verbinden. Dabei werden aus den Zielen der Institution und den Rahmenbedingungen die **Informationssicherheitsziele** abgeleitet. Sie werden in der **Leitlinie zur Informationssicherheit** festgehalten und allen Mitarbeitern bekannt gemacht. Aus diesen Zielen leitet sich auch das angestrebte Sicherheitsniveau für die Geschäftsprozesse ab.

Um die erforderlichen Maßnahmen umzusetzen, ist der Aufbau einer **Sicherheitsorganisation** erforderlich und sind Verantwortlichkeiten zu schaffen. **Weitere Ressourcen** wie Räumlichkeiten, Budget und Zeit sind bereitzustellen.

Und letztlich ist Informationssicherheit nicht nur eine Aufgabe der Leitung und des Sicherheitsorganisationsteams, sondern **alle Mitarbeiter sind hierfür in ihrem Wirkungsbereich verantwortlich**. Ohne ihre Mitwirkung wird eine Institution ihre Sicherheitsziele verfehlen.

2. Erstellung eines Sicherheitskonzepts

Um die Sicherheitsziele zu erreichen, müssen in einem Konzept geeignete **technische und organisatorische Maßnahmen** festgelegt werden. Dies sind beispielsweise:

- Maßnahmen zur physischen Absicherung von Gebäuden und Räumlichkeiten,
- technische Vorkehrungen zur Absicherung der Schnittstellen eines Netzes und seiner Segmente,
- Regelungen zum Umgang mit klassifizierten Informationen,
- ein geeignetes Identitäts- und Berechtigungsmanagement,
- die Anwendung kryptographischer Maßnahmen,
- ausreichende Datensicherungsverfahren,
- Verfahren zur Erkennung und Abwehr von Schadsoftware.

In den folgenden Lektionen dieses Kurses wird die Sicherheitskonzeption gemäß IT-Grundschutz detailliert beschrieben.

3. Umsetzung des Konzepts

Im Sicherheitskonzept muss dargestellt werden, wie die Maßnahmen umzusetzen und zu überprüfen sind. Dies ist eine Vorgabe für die Bewertung durch die Leitungsebene.

4. Aufrechterhaltung und Verbesserung

Informationssicherheit ist kein zeitlich begrenztes Projekt, sondern ein Prozess, der kontinuierlich das Sicherheitskonzept an veränderte Anforderungen anpasst. Mit geeigneten Instrumenten, etwa Kennzahlen oder internen und externen Audits, muss regelmäßig geprüft werden, ob die Informationssicherheitsziele erreicht werden. Abweichungen müssen zur Behebung und Verbesserung führen.

Lerneinheit 2.3: Verantwortung und Aufgaben der Leitung

Ob eine Institution ein gutes ISMS einführt und kontinuierlich weiterentwickelt, hängt im wesentlichen davon ab, wie die oberste Leitungsebene ihre Aufgaben und ihre Verantwortung wahrnimmt. Dies sind ihre wichtigsten Pflichten:

- Sie kennt die Risiken bei Verletzung der Informationssicherheit, setzt einen Rahmen und trifft die grundlegenden Entscheidungen zum Umgang mit diesen Risiken.
- Sie initiiert, steuert und kontrolliert den Sicherheitsprozess und sorgt dafür, dass Informationssicherheit sich in alle Prozesse und Projekte der Institution integriert.
- Sie stellt erforderliche Ressourcen (Personal, Budget, Zeit) für das Sicherheitsmanagement bereit und wägt Aufwände und Ertrag ab.
- Sie wirkt durch ihr sicherheitsgemäßes Verhalten als Vorbild.

Die oberste Leitungsebene trägt die **Gesamtverantwortung** für ein angemessenes ISMS. Auch wenn sie operative Aufgaben delegiert und die Mitarbeiter zu sicherheitsbewusstem Verhalten anhält, entbindet sie dies nicht von der Gesamtverantwortung.

Ist Ihre Leitung bereit, die genannten Aufgaben und Verantwortlichkeiten zu übernehmen? Falls nicht, ist damit eine grundlegende Voraussetzung für Informationssicherheit nicht erfüllt. Im Baustein ISMS.1 *Sicherheitsmanagement* des IT-Grundschutz-Kompendiums werden daraus resultierende Gefährdungen dargestellt und wird beschrieben, welche Anforderungen erfüllt sein müssen, um ihnen zu begegnen.

Lerneinheit 2.4: Der Informationssicherheitsbeauftragte

Um Zuständigkeiten und Verantwortung für operative Aufgaben eindeutig zuordnen zu können, ist ein Informationssicherheitsbeauftragter (ISB) zu ernennen.

Zuständigkeiten und Aufgaben

Ein Informationssicherheitsbeauftragter ist für alle Fragen rund um die Informationssicherheit in der Institution zuständig. Zu seinen Aufgaben gehört es,

- den Sicherheitsprozess zu steuern und zu koordinieren,
- die Leitung bei der Erstellung der Sicherheitsleitlinie zu unterstützen,
- die Erstellung des Sicherheitskonzepts und zugehöriger Teilkonzepte und Richtlinien zu koordinieren,
- Realisierungspläne für Sicherheitsmaßnahmen anzufertigen sowie ihre Umsetzung zu initiieren und zu überprüfen,
- der Leitungsebene und anderen Sicherheitsverantwortlichen über den Status der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- sicherheitsrelevante Vorfälle zu untersuchen sowie
- Sensibilisierungen und Schulungen zur Informationssicherheit zu initiieren und zu koordinieren.

Ein ISB sollte Erfahrung und Wissen sowohl auf den Gebieten der Informationssicherheit als auch der IT besitzen. Darüber hinaus sollte er die Geschäftsprozesse der Institution kennen.

Zur **Wahrung der Unabhängigkeit** sollte der ISB direkt der obersten Leitung zugeordnet sein. Eine Integration in die IT-Abteilung kann zu Rollenkonflikten führen, da der ISB seine Verpflichtung zur Kontrolle der Sicherheitsmaßnahmen nicht frei von Beeinflussung wahrnehmen kann. Auch eine Personalunion mit dem Datenschutzbeauftragten ist nicht unkritisch. Sollte dies der Fall sein, müssen die Schnittstellen dieser beiden Aufgaben klar definiert werden, um Rollenkonflikte zu vermeiden.

Ein ISB benötigt darüber hinaus ausreichend **Ressourcen und Zeit für erforderliche Fortbildungen**. Es muss einen **direkten Berichtsweg zur Leitung** geben, um in Konfliktfällen schnell entscheiden zu können.

Je nach Größe des Unternehmens oder der Behörde kann es auch **weitere ISB** etwa für verschiedene Bereiche, Standorte oder auch große Projektvorhaben der Institution geben.

Weitere Informationen zum Anforderungsprofil eines ISB finden Sie in Kapitel 4.4 des BSI-Standards 200-2: *IT-Grundschutz-Methodik*. Auch in den Umsetzungshinweisen zum Baustein ISMS.1 finden sich bei ISMS.1.M4 wichtige Hinweise zu den Aufgaben und dem Qualifikationsprofil des ISB.

Lerneinheit 2.5: Der ICS-Informationssicherheitsbeauftragte

Die Sicherheitsanforderungen im Bereich der industriellen Produktion unterscheiden sich in vielen Bereichen von denen der Büro-IT. Um angemessene Sicherheitsmaßnahmen für industrielle Steuerungen (Industrial Control Systems, ICS) zu planen, umzusetzen und zu kontrollieren, wird ein großes spezifisches Wissen über diese technischen Systeme und deren Einsatzanforderungen benötigt. Es ist daher sinnvoll, in Unternehmen des produzierenden Gewerbes einen hinreichend erfahrenen **ICS-Informationssicherheitsbeauftragten (ICS-ISB)** zu ernennen. Dieser sollte in die Sicherheitsorganisation eingebunden sein und insbesondere mit dem ISB eng kooperieren.

Die **Aufgaben des ICS-ISB** sind im Wesentlichen:

- gemeinsame Ziele zwischen dem Bereich der industriellen Steuerung und dem gesamten ISMS verfolgen und Projekte aktiv unterstützen,
- allgemeine Sicherheitsvorgaben und Richtlinien für den ICS-Bereich umsetzen,
- Risikoanalysen für den ICS-Bereich durchführen,
- Sicherheitsmaßnahmen für den ICS-Bereich festlegen und umsetzen,
- Sicherheitsrichtlinien und Konzepte für den ICS-Bereich unter Berücksichtigung von Anforderungen der Funktionssicherheit („Safety") erstellen und die Mitarbeiter schulen,
- Ansprechpartner für die Mitarbeiter vor Ort und für die gesamte Institution sein,
- Schulungen und Maßnahmen zur Sensibilisierung konzipieren,
- Sicherheitsvorfälle zusammen mit dem ISB bearbeiten,
- Dokumentation.

Weitere Informationen zum Anforderungsprofil eines ICS-ISB finden Sie in Kapitel 4.7 des BSI-Standards 200-2: *IT-Grundschutz-Methodik*.

Lerneinheit 2.6: Das IS-Management-Team

In größeren Institutionen sollte ein Team aus mehreren Zuständigen für Informationssicherheit gebildet werden, um den Informationssicherheitsbeauftragten zu unterstützen. Es ist für die Regelung sämtlicher übergreifender Belange der Informationssicherheit zuständig und koordiniert, berät und kontrolliert die zugehörigen Analysen, Konzepte und Richtlinien.

In einem solchen **IS-Management-Team** sollten der ISB, sofern vorhanden der ICS-ISB, IT-Verantwortliche, Zuständige für Datenschutz sowie Vertreter der Fachverfahren und Geschäftsprozesse zusammenwirken, gegebenenfalls ergänzt durch Informationssicherheitsbeauftragte, die für einzelne Bereiche, Projekte oder IT-Systeme (etwa die industriellen Steuerungen) benannt wurden. Die nachfolgende Abbildung veranschaulicht eine mögliche Organisationsstruktur:

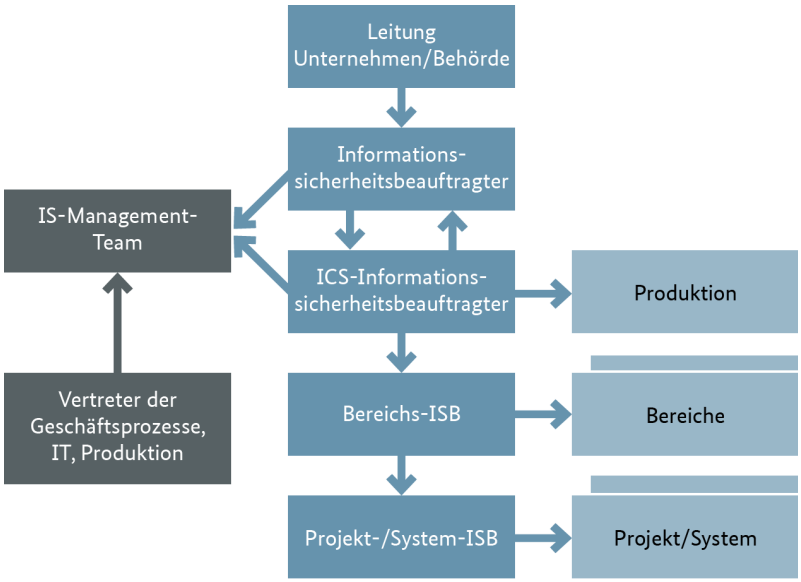


Abbildung 4: Organisation der Informationssicherheit – Rollen

Die **Aufgaben des IS-Management-Teams** sind:

- die Sicherheitsziele und -strategien festlegen sowie die Leitlinie zur Informationssicherheit entwickeln,
- die Umsetzung der Sicherheitsleitlinie überprüfen,
- den Sicherheitsprozess initiieren, steuern und kontrollieren,
- bei der Entwicklung des Sicherheitskonzepts mitwirken,
- überprüfen, ob die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen geeignet und wirksam sind und wie beabsichtigt funktionieren,
- Schulungs- und Sensibilisierungsprogramme für Informationssicherheit konzipieren sowie
- die Fachverantwortlichen, den IT-Betrieb, eventuell die ISB für einzelne Bereiche und den ICS-ISB sowie die Leitungsebene beraten.

Ob es sinnvoll ist, ein IS-Management-Team einzurichten oder mehrere ISBs für Bereiche oder Projekte zu benennen, hängt von der Größe einer Institution ab. In kleineren Institutionen genügt ein einziger mit den erforderlichen Kompetenzen ausgestatteter ISB.

Modelle zum Aufbau der Sicherheitsorganisation in großen, mittelgroßen und kleinen Institutionen sowie Erläuterungen zu den Aufgaben von ISB, ICS-ISB und IS-Management-Teams finden Sie in Kapitel 4 *Organisation des Sicherheitsprozesses* des BSI-Standards 200-2: *IT-Grundschutz-Methodik*, ferner im Baustein ISMS.1 *Sicherheitsmanagement* des IT-Grundschutz-Kompendiums.

Beispiel: Aufbau einer Sicherheitsorganisation im Unternehmen

Im Beispielunternehmen RECPLAST GmbH möchte die Geschäftsführung ein verbindliches **Sicherheitskonzept** für das gesamte Unternehmen ausarbeiten lassen. Dazu müssen die vorhandenen Grundsätze und Richtlinien zur Informationssicherheit präzisiert werden.

In einem ersten Schritt wird ein **Informationssicherheitsbeauftragter** ernannt, der die zugehörigen Arbeiten koordinieren soll. Da diese Aufgabe umfangreiche IT-Kenntnisse erfordert, wird hierfür ein Mitarbeiter der Abteilung „Informationstechnik“ bestimmt, in seinen Aufgaben aber gleichzeitig der Geschäftsführung unterstellt. Zusätzlich ernennt diese einen **ICS-Informationssicherheitsbeauftragten**, der Sicherheitsanforderungen und -maßnahmen für den Produktionsbereich entwickeln und kontrollieren soll. Danach wird ein zeitlich befristetes Projekt „Sicherheitskonzept“ eingerichtet, das folgende Ergebnisse erzielen soll:

1. Vorschläge und Entscheidungsvorlage für eine Leitlinie zur Informationssicherheit,
2. einen Vorschlag für ein Sicherheitskonzept und einen zugehörigen Realisierungsplan,
3. Vorschläge für Maßnahmen zur Aufrechterhaltung der Informationssicherheit sowie
4. Dokumentation aller Entscheidungsvorlagen, Entscheidungen und der umgesetzten Maßnahmen des Informationssicherheitsprozesses.

Da der ISB die Geschäftsprozesse nicht im Detail kennt, wird ein **IS-Management-Team** gebildet, das den ISB und den ICS-ISB bei der Erstellung der Leitlinie und dem Sicherheitskonzept unterstützt. Ihm gehören der Datenschutzbeauftragte, der Leiter des kaufmännischen Bereichs und der Rechtsabteilung und, um Kundenanforderungen einzubeziehen, ein Mitarbeiter des Vertriebs an. So sind alle Geschäftsbereiche vertreten und können weitere Informationen über die Betriebsabläufe und externe Anforderungen einholen.

Das Projekt wird dem Betriebsrat vorgestellt, der regelmäßig über Zwischenergebnisse informiert wird. Auch die Mitarbeiter werden in einer Betriebsversammlung mit dem Projekt und seinen Zielen bekannt gemacht.

Übung zur Anwendung

Lässt sich dieses Beispiel auf Ihr Unternehmen, Ihre Behörde übertragen?

- Gibt es einen ISB, wie wurde er bestimmt, aus welchem Bereich kommt er?

- Wie ist er organisatorisch zugeordnet?
- Gibt es ein IS-Management-Team? Wie ist es besetzt?
- Falls Sie einen Produktionsbereich haben, gibt es einen ICS-ISB? Wie arbeitet er mit dem ISB zusammen?

Bitte vergleichen Sie die Regelungen in Ihrer Institution mit denen im Beispielunternehmen RECPLAST und der Darstellung im BSI-Standard 200-2: *IT-Grundschutz-Methodik*. Wo sehen Sie Unterschiede? Wie bewerten Sie diese? Sehen Sie Verbesserungsbedarf in Ihrer Organisation?

Lerneinheit 2.7: Die Sicherheitsleitlinie

Die Leitlinie zur Informationssicherheit ist ein wichtiges **Grundsatzdokument der Leitung** zu dem Stellenwert, den verbindlichen Prinzipien und dem anzustrebenden Niveau der Informationssicherheit in einer Institution. Für die betroffenen Mitarbeiter verständlich, wird auf wenigen Seiten beschrieben, welche Sicherheitsziele angestrebt und in welchem organisatorischen Rahmen diese umgesetzt werden sollen. Die Entwicklung der Leitlinie muss von der Leitung der Institution angestoßen und aktiv begleitet werden. Der ISB wird die Leitlinie in enger Kooperation mit der Leitung erarbeiten und dabei (sofern vorhanden) vom IS-Management-Team und weiteren Verantwortlichen für Informationssicherheit unterstützt.

Die Leitlinie muss **allen betroffenen Mitarbeitern bekannt gegeben** und **kontinuierlich aktualisiert** werden.

Was sollte in der Leitlinie zur Informationssicherheit festgelegt werden?

- Der Geltungsbereich wird konkretisiert.
- Die Bedeutung, die Informationssicherheit für eine Institution hat, wird hervorgehoben, etwa indem darauf hingewiesen wird, dass ein Ausfall der Informationstechnik oder Verletzungen der Vertraulichkeit und Integrität von Informationen die Existenz der Institution gefährden.
- Die Verantwortung der Leitung wird betont, sowohl im Hinblick auf die Initiierung des Sicherheitsprozesses als auch auf dessen kontinuierliche Verbesserung.
- Es wird auf einschlägige Gesetze und Regulierungsauflagen hingewiesen und die Mitarbeiter werden verpflichtet, diese zu beachten.
- Es werden für die Informationssicherheit besonders wichtige Geschäftsprozesse genannt, etwa Produktionsabläufe, Forschungsverfahren oder Personalbearbeitung, und auf die strikte Einhaltung von Sicherheitsregeln hingewiesen.
- Die Organisationsstruktur für Informationssicherheit und die Aufgaben der verschiedenen Sicherheitsverantwortlichen werden vorgestellt.
- Sinnvoll ist auch der Hinweis auf Sicherheitsschulungen und Sensibilisierungsmaßnahmen.

Im Baustein ISMS.*1 Sicherheitsmanagement* werden die Anforderungen an eine Leitlinie formuliert. Hinweise zum Vorgehen und zur inhaltlichen Struktur finden sich in den zugehörigen Umsetzungshinweisen.

Beispiel: Leitlinie für die Informationssicherheit bei der RECPLAST GmbH

Auch das Unternehmen RECPLAST GmbH hat eine Sicherheitsleitlinie entwickelt. Folgende Themen werden adressiert:

- Stellenwert der Informationssicherheit und Bedeutung der Leitlinie,
- Sicherheitsniveau und Ziele,

- Verantwortlichkeiten,
- Verstöße und Folgen,
- Geltungsbereich und Verweis auf Konkretisierung.

Sie finden dieses Muster in Kapitel 2 der ausführlichen Darstellung zur RECPLAST GmbH.

Übung zur Anwendung

Bitte überlegen Sie, wie Sie eine Sicherheitsleitlinie für Ihr Unternehmen oder Ihre Behörde gestalten würden.

- Wie definieren Sie den Geltungsbereich?
- Welche Ziele nennen Sie?
- Gibt es bereits Beauftragte für Informationssicherheit oder einzelne Aspekte dieser Aufgabe? Wie würden Sie diese in den Entwicklungsprozess einbeziehen?
- Wie stellen Sie die Verantwortung und die Aufgaben der Mitarbeiter dar?
- Gibt es besonders kritische Geschäftsprozesse, deren Anforderungen Sie in der Leitlinie hervorheben möchten?

Lerneinheit 2.8: Das Sicherheitskonzept

Mit welchen Maßnahmen die in der **Leitlinie zur Informationssicherheit** vorgegebenen Ziele und Strategien verfolgt werden sollen, wird in einem Sicherheitskonzept beschrieben. Ein solches Sicherheitskonzept hat immer einen festgelegten Geltungsbereich. Dieser wird in der IT-Grundschutz-Methodik als **Informationsverbund** bezeichnet.

Festlegung des Informationsverbundes

Ein Informationsverbund muss eine **sinnvolle Mindestgröße** haben. Für eine umfassende Sicherheit ist es grundsätzlich empfehlenswert, die gesamte Institution zu betrachten. Insbesondere bei größeren Institutionen und dann, wenn Sicherheitsmaßnahmen bislang eher punktuell und ohne ein zugrunde liegendes systematisches Konzept vorgenommen wurden, ist es allerdings oft praktikabler sich (zunächst) auf **Teilbereiche** zu konzentrieren. Diese sollten jedoch

- aufgrund ihrer organisatorischen Strukturen oder Anwendungen **gut abgrenzbar** sein und
- **wesentliche Aufgaben und Geschäftsprozesse** der betrachteten Institution umfassen.

Sinnvolle Teilbereiche sind zum Beispiel eine oder mehrere Organisationseinheiten, Geschäftsprozesse oder Fachaufgaben. Einzelne Clients, Server oder Netzverbindungen sind hingegen als Untersuchungsgegenstand ungeeignet.

Achten Sie bei der Definition des Informationsverbundes darauf, dessen Schnittstellen genau zu beschreiben. Dies gilt insbesondere auch dann, wenn die einbezogenen Geschäftsprozesse oder Fachaufgaben von den Diensten externer Partner abhängen.

Erstaufnahme des Informationsverbundes

In der initialen Phase des Sicherheitsprozesses ist es nicht erforderlich, Anwendungen und IT-Infrastruktur detailliert zu beschreiben. Zunächst geht es vielmehr darum, besonders wichtige Geschäftsprozesse, die im Geltungsbereich des Konzepts angesiedelt sind, hinsichtlich ihrer Anforderungen an die Informations-

sicherheit zu charakterisieren. Dabei reicht es zu wissen, welche Prozesse sehr hohe, hohe oder lediglich normale Schutzanforderungen haben.

Auf dieser Basis wird dann eine **Erstaufnahme des Informationsverbundes** angefertigt. Folgende Informationen und Detailangaben müssen dabei strukturiert (z. B. tabellarisch) zusammengetragen werden:

- Geschäftsprozesse im Informationsverbund (Name, Beschreibung, fachverantwortliche Stelle),
- Anwendungen in diesen Prozessen (Name und Beschreibungen),
- IT-Systeme und ICS-Komponenten (Name, Systemplattform und eventuell Aufstellungsort),
- für den Informationsverbund wichtige Räume wie Rechenzentrum oder Serverräume (Art, Raumnummer und Gebäude) sowie
- virtuelle Systeme (entsprechend gekennzeichnet und benannt).

Ein grafischer Netzplan ist eine hilfreiche Ergänzung zur tabellarischen Zusammenstellung der IT-Systeme.

Die ermittelten Komponenten, wie auch der Informationsverbund als Ganzes, sind **Zielobjekte** des Sicherheitskonzepts. Bereits vor dessen eigentlicher Entwicklung sollten Sie einschätzen, welches Schutzniveau für die verschiedenen Zielobjekte erforderlich ist, die Sie bei der Erstaufnahme identifiziert haben.

Lerneinheit 2.9: Wahl der Vorgehensweise

Bevor diese Ergebnisse detailliert werden, ist eine Entscheidung über die Vorgehensweise erforderlich. Die IT-Grundschutz-Methodik sieht hierfür **drei Varianten** vor, zwischen denen sich eine Institution abhängig von ihren spezifischen Gegebenheiten entscheiden kann. Diese drei Varianten unterscheiden sich in der Breite und Tiefe der umgesetzten Schutzmaßnahmen:

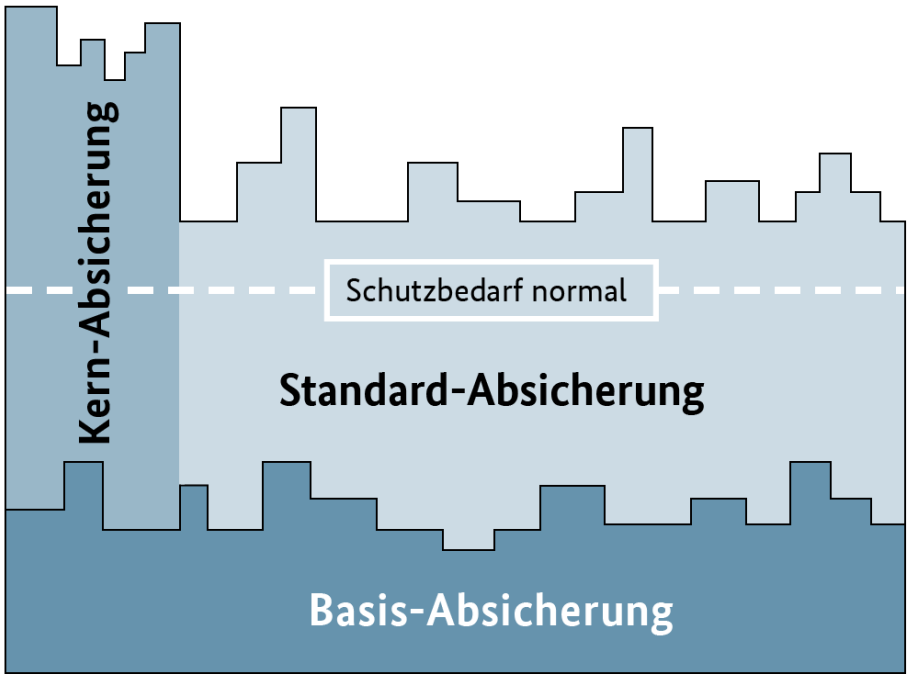


Abbildung 5: Varianten der IT-Grundschutz-Methodik

- Die **Basis-Absicherung** ist für Institutionen interessant, die einen Einstieg in den IT-Grundschutz suchen und schnell alle relevanten Geschäftsprozesse mit Basismaßnahmen absichern möchten.

- Die **Kern-Absicherung** lenkt die Sicherheitsmaßnahmen auf die „Kronjuwelen“ einer Institution, also besonders wichtige Geschäftsprozesse und *Assets*. Diese Variante zielt damit auf die vertiefte Absicherung der kritischsten Bereiche ab.
- Die **Standard-Absicherung** entspricht der empfohlenen IT-Grundschutz-Vorgehensweise (vgl. früherer BSI-Standard 100-2).
- Sie hat einen umfassenden Schutz für alle Prozesse und Bereiche der Institution als Ziel.

Sowohl die Basis- als auch die Kern-Absicherung können als Einstieg und Grundlage für eine umfassende Absicherung nach IT-Grundschutz dienen.

In diesem Kurs wird die Vorgehensweise der **Standard-Absicherung** beschrieben und dabei, falls sinnvoll, auch auf die beiden anderen Varianten verwiesen. Die folgende Abbildung zeigt die zugehörigen Schritte:

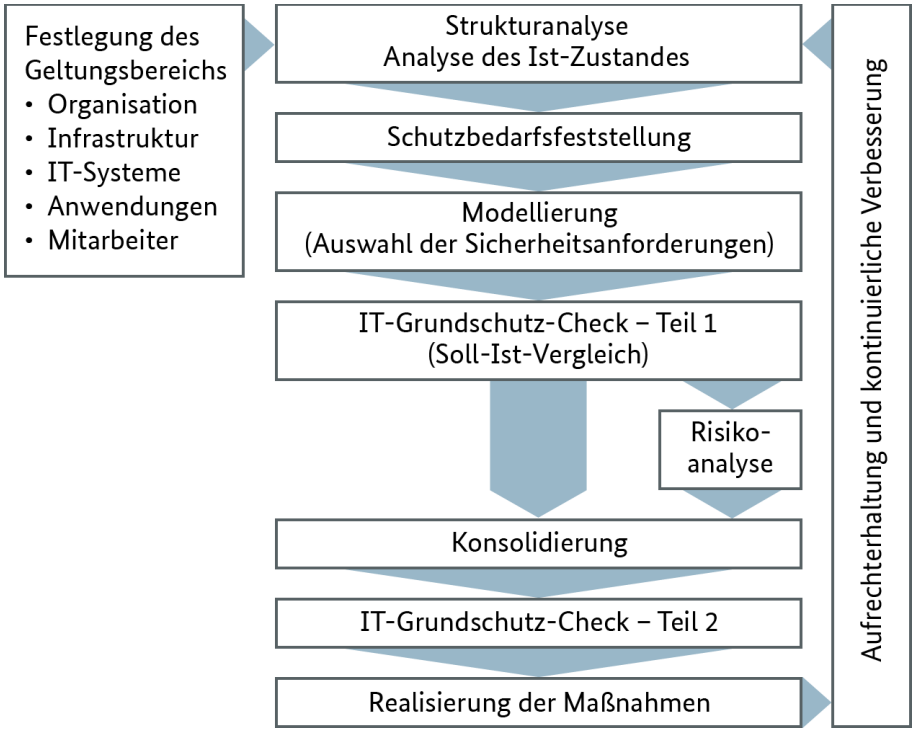


Abbildung 6: Schritte bei der Variante Standard-Absicherung der IT-Grundschutz-Methodik

Die drei Varianten der IT-Grundschutz-Methodik werden in den Kapiteln 6, 7 und 8 des BSI-Standards 200-2 detailliert dargestellt. Die Basis-Absicherung wird darüber hinaus in einem eigenen Leitfaden zur Basis-Absicherung nach IT-Grundschutz ausführlich beschrieben. Umsetzungsempfehlungen finden sich auch in ISMS1.M10: *Erstellung eines Sicherheitskonzepts*.

Lerneinheit 2.10: Testfragen

Wenn Sie möchten, können Sie mit den nachfolgenden Fragen Ihre Kenntnisse zum Management der Informationssicherheit überprüfen. Die Auflösungen zu den Fragen finden Sie im Anhang.
Es können mehrere Antwortmöglichkeiten zutreffend sein.

1 **Welches Modell liegt dem in BSI-Standard 200-1 beschriebenen Sicherheitsprozess zugrunde?**

a ein Zyklus aus den Schritten Plan, Do, Check und Act

b ein Verfahren zur Definition eines State-of-the-Art-Informationssicherheitsniveaus

c ein auf stetige Verbesserung angelegtes Modell

d ein Modell aus technischen Sicherheitsmaßnahmen

2 **Was sollte eine Leitlinie zur Informationssicherheit enthalten?**

a detaillierte technische Vorgaben für die Konfiguration wichtiger IT-Systeme

b Aussagen zur Bedeutung der Informationssicherheit für die betroffene Institution

c grundlegende Regelungen zur Organisation der Informationssicherheit

d konkrete Verhaltensregelungen für den Umgang mit vertraulichen Informationen

3 **Welche Aufgaben haben üblicherweise Informationssicherheitsbeauftragte?**

a die Entwicklung von Sicherheitskonzepten zu koordinieren

b die eingesetzte Sicherheitstechnik zu konfigurieren

c der Leitungsebene über den Stand der Informationssicherheit zu berichten

d Presseanfragen zum den Stand der Informationssicherheit im Unternehmen zu beantworten

4 **Wie setzt sich ein IS-Management-Team geeignet zusammen?**

a Aus jeder Abteilung des Unternehmens oder der Behörde werden Mitarbeiter entsandt, damit alle Bereich gut vertreten sind.

b Nur der IT-Leiter ordnet einige Mitarbeiter in das Team ab.

c Die Zusammensetzung sollte auf Freiwilligkeit beruhen. Jeder der Interesse hat, wird aufgenommen.

d Die Geschäftsleitung setzt das Team aus Verantwortlichen für bestimmte IT-Systeme, Anwendungen, Datenschutz und IT-Service und (sofern vorhanden) dem ICS-ISB zusammen.

5 **Wer ist für die Freigabe der Leitlinie zur Informationssicherheit verantwortlich?**

a das IS-Management-Team

b der ISB

c die Unternehmens- oder Behördenleitung

d die Öffentlichkeitsabteilung eines Unternehmens oder einer Behörde

6 **Warum kann es sinnvoll sein, sich für eine Sicherheitskonzeption gemäß der Basis-Absicherung zu entscheiden?**

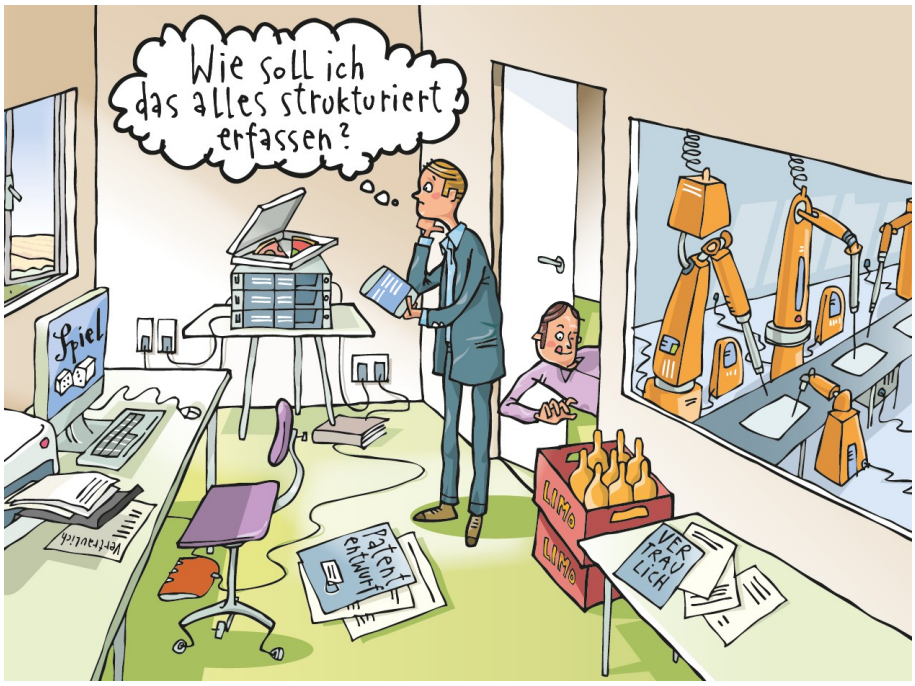
a Die Erfüllung der zugehörigen Anforderungen reicht in der Regel für ein normales Unternehmen völlig aus.

b Weil schnell Informationssicherheit umgesetzt werden muss und die Basis-Absicherung hierfür einen geeigneten Einstieg bietet.

c Weil Informationssicherheit Schritt für Schritt umgesetzt werden soll. Mittelfristig kann das Sicherheitskonzept nach Standard-Absicherung ausgebaut werden.

d Weil die hochwertigen Informationen dringend geschützt werden müssen. Die Basis-Absicherung sorgt für den angemessenen Schutz der „Kronjuwelen“ einer Institution.

Lektion 3: Strukturanalyse



Was sind die wichtigen Aufgaben und Geschäftsprozesse von Behörden, Unternehmen oder anderen Institutionen? Welche Informationen werden in diesen Prozessen und Aufgaben benötigt, bearbeitet oder gespeichert? Mit welchen Anwendungen geschieht dies und in welchem infrastrukturellen Umfeld? Welche informationstechnischen Systeme sind beteiligt?

Je genauer diese Fragen für den betrachteten Informationsverbund beantwortet werden, desto zielgerichteter können die einzelnen im Sicherheitskonzept zusammengefassten Schutzvorkehrungen festgelegt werden. **Ziel der Strukturanalyse** ist es, die hierfür erforderlichen Kenntnisse zusammenzustellen und aufzubereiten. In der Strukturanalyse vervollständigen Sie damit die Ergebnisse der zuvor durchgeführten Erstaufnahme der Prozesse, Anwendungen und IT-Systeme (siehe Lerneinheit 2.8: *Das Sicherheitskonzept*).

In dieser Lektion erfahren Sie am Beispiel der RECPLAST GmbH, welche Informationen Sie bei der Strukturanalyse im Einzelnen für die verschiedenen Komponenten des Informationsverbundes erheben:

- Wie dokumentieren Sie **Geschäftsprozesse**, **Anwendungen** und die in ihnen verwendeten wichtigen **Informationen**?
- Wie sollte ein **Netzplan** beschaffen sein, welche Angaben sollte er enthalten?
- Welche Informationen sind zu den verschiedenen Arten von **IT-Systemen** nötig, die im Informationsverbund in Betrieb sind oder deren Einsatz geplant wird?
- Wie erfassen Sie die **räumlichen Gegebenheiten** (Liegenschaften, Gebäude, Räume, auch Produktionsstätten)?

Lerneinheit 3.1: Das Beispielunternehmen RECPLAST

Die Strukturanalyse soll, wie auch die weiteren Schritte der Standard-Absicherung gemäß IT-Grundschutz-Methodik, am Beispiel der RECPLAST GmbH verdeutlicht werden – daher vorab ein paar einführende Informationen zu diesem fiktiven Unternehmen.

Geschäftszweck und Standorte

Die RECPLAST GmbH hat rund 500 Mitarbeiter und stellt aus Recyclingmaterialien etwa 400 unterschiedliche Kunststoffprodukte her. Verwaltung sowie Produktion und Lager der Firma befinden sich in Bonn, allerdings an unterschiedlichen Standorten: Die Geschäftsführung hat zusammen mit den Verwaltungsabteilungen sowie den Abteilungen „Einkauf“ und „Marketing und Vertrieb“ vor kurzem ein neues Gebäude in Bad Godesberg bezogen, während die Entwicklungsabteilung, Produktion, Material- und Auslieferungslager am ursprünglichen Firmensitz im Stadtteil Beuel verblieben sind. Zusätzlich gibt es Vertriebsbüros in Berlin, München und Paderborn.

Organisatorischer Aufbau

Das folgende Organigramm veranschaulicht die organisatorische Gliederung des Unternehmens. Die grau hinterlegten Abteilungen sind am Standort Bonn-Beuel ansässig, alle anderen (bis auf die Vertriebsbüros) am Verwaltungssitz in Bad Godesberg.

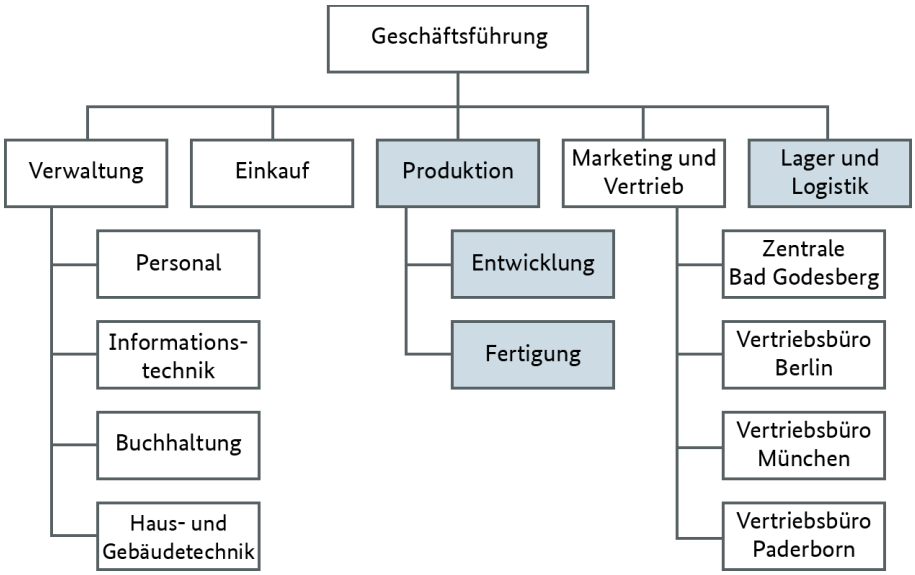


Abbildung 7: Organigramm der RECPLAST GmbH

In Lerneinheit 3.3: *Geschäftsprozesse und Informationen erheben* erfahren Sie mehr zu den Geschäftsprozessen, die in dieser Organisationsstruktur durchgeführt werden.

IT-Systeme und Vernetzung

Die beiden Standorte in Bonn sind über eine angemietete Standleitung miteinander vernetzt. Die Außenbüros haben über eine abgesicherte Verbindung Anschluss an das Unternehmensnetz. Einen ersten Eindruck zu den IT-Systemen und deren Netzverbindungen vermittelt folgender Netzplan:

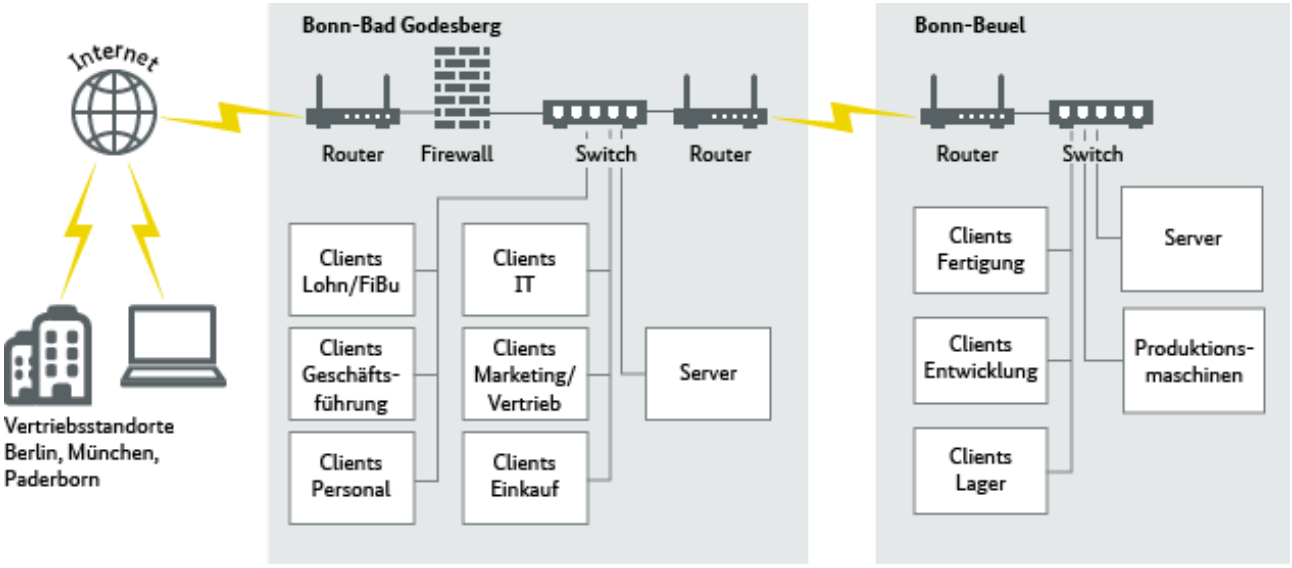


Abbildung 8: Vereinfachter Netzplan der RECPLAST GmbH

In den Lerneinheiten 3.5: *Netzplan erheben* und 3.6: *IT-Systeme erheben* erfahren Sie mehr zu den dargestellten IT-Systemen, deren Vernetzung und ihrem Zusammenhang mit den Geschäftsprozessen und Anwendungen der RECPLAST GmbH.

Lerneinheit 3.2: Objekte gruppieren

Ziel der Strukturanalyse ist es, diejenigen Objekte zu identifizieren und in ihrem Zusammenwirken zu beschreiben, für die in einem Sicherheitskonzept angemessene Schutzmaßnahmen festgelegt werden müssen. Daher ist es wichtig, diese Schutzobjekte vollständig und hinreichend zu erfassen.

Ein wichtiger Hinweis vorab zu dieser Aufgabe:

Wenn es in Ihrer Institution bereits Zusammenstellungen zu den zu erfassenden Sachverhalten gibt, etwa Inventare, Geschäftsprozessmodelle oder Netzpläne, sollten Sie diese auch für die Strukturanalyse auswerten.

Ziel der Strukturanalyse ist es nicht, ein vollständiges Inventar über alle eingesetzten technischen Komponenten zu erhalten. Vielmehr sollten Sie bei allen Teilerhebungen Objekte **sinnvoll zu Gruppen zusammenfassen**, die Sie in den Folgeschritten der Konzeptentwicklung als ein einziges Objekt behandeln können. Zum Beispiel ist es zweckmäßig, IT-Systeme, die gleich oder ähnlich konfiguriert sind und für die gleichen Aufgaben genutzt werden, zu einer Gruppe zusammenzufassen.

Generell gilt, dass Sie Komponenten zusammenfassen sollten, die

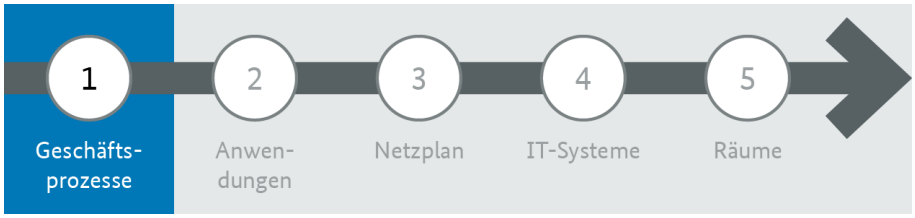
- vom gleichen Typ sind,
- gleich oder nahezu gleich konfiguriert sind,
- gleich oder nahezu gleich in das Netz eingebunden sind,
- den gleichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen,
- die gleichen Anwendungen bedienen **und**
- den gleichen **Schutzbedarf** aufweisen.

In der Regel bietet sich an, Clients in Gruppen zusammenzufassen. Gruppierungen sind aber auch für Server möglich, wenn diese die oben genannten Kriterien erfüllen. Dies trifft z. B. auf redundant ausgelegte Server

zu. Weitere typische Beispiele für Gruppierungen sind gleich ausgestattete und genutzte Büroräume oder die Kommunikationsverbindungen zwischen einem Switch und den Clients einer Gruppe. In den nachfolgenden Abschnitten werden weitere Beispiele für zweckmäßige Gruppenbildungen genannt.

Überlegen Sie sich sorgfältig, welche Objekte Sie zu Gruppen zusammenfassen. Wenn Sie Komponenten zusammenfassen, die unterschiedlichen Schutzbedarf haben, dann können Sicherheitslücken entstehen.

Lerneinheit 3.3: Geschäftsprozesse und Informationen erheben



Ein Sicherheitskonzept soll die **wesentlichen Informationen** einer Institution schützen. Welche dazu zählen, wird in der Regel bei einer Betrachtung der **Geschäftsprozesse** deutlich: Welche Informationen sind erforderlich, damit diese reibungslos funktionieren? Welche haben einen besonderen Geheimhaltungsbedarf und dürfen daher nur Befugten zugänglich sein? Welche Informationen unterliegen den Vorgaben des Datenschutzes, welche anderen rechtlichen Verpflichtungen (beispielsweise um die Nachweisbarkeit von geschäftlichen Vorgängen zu sichern)?

Oft kann auf eine bereits vorhandene Aufstellung der wesentlichen Geschäftsprozesse oder Fachaufgaben zurückgegriffen werden (eine „Prozesslandkarte“) oder die Prozesse können anhand von Aufgabenbeschreibungen oder eines Organigramms der Institution identifiziert werden.

Ergebnisdarstellung

Tabellen bieten eine übersichtliche Möglichkeit, die Ergebnisse der Erhebung der Prozesse und Informationen darzustellen. Für jeden Geschäftsprozess sollten Sie die folgenden Angaben vermerken:

- eine eindeutige Kennung (Nummer oder Kürzel),
- einen Namen für den Prozess,
- eine kurze Beschreibung des Ziels, der Abläufe und der verarbeiteten Informationen,
- die für den Prozess Verantwortlichen,
- wichtige Anwendungen, die für den Prozess benötigt werden.

Beispiel

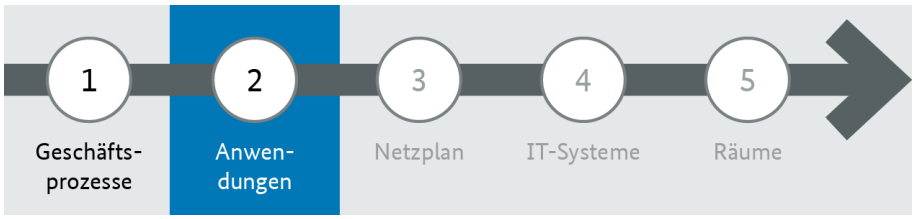
Die folgende Tabelle zeigt einen Teil der für die RECPLAST GmbH erfassten Geschäftsprozesse. Diese werden durch das Präfix „GP“ als Geschäftsprozess gekennzeichnet und fortlaufend durchnummeriert.

Die für einen Prozess benötigten Anwendungen werden in einer separaten Tabelle zugeordnet.

Kennung	Name (Art) und Beschreibung des Prozesses sowie der verwendeten Informationen	Verantwortlicher	Mitarbeiter
GP001	**Produktion (Kerngeschäft):** Die Produktion der Kunststoffartikel umfasst alle Phasen von der Materialbereitstellung bis hin zur Einlagerung des produzierten Materials. Hierzu gehören innerhalb der Produktion die internen Transportwege, die Produktion und Fertigung der verschiedenen Komponenten und das Verpacken der Teile. Es werden alle Informationen über Aufträge, Lagerbestände und Stücklisten verarbeitet.	Leiter Produktion	Alle Mitarbeiter
GP002	**Angebotswesen (unterstützender Prozess):** In der Angebotsabwicklung werden die Kundenanfragen für Produkte verarbeitet. Im Regelfall werden Kundenanfragen formlos per E-Mail oder Fax geschickt. Die Angebote werden elektronisch erfasst und ein schriftliches Angebot per Post an den Kunden versendet. Im Angebotswesen werden Kundendaten, Lagerbestände, Anfragen und Angebote bearbeitet.	Leiter Angebotswesen	Vertrieb
GP003	**Auftragsabwicklung (Kerngeschäft):** Kunden schicken die Bestellungen im Regelfall per Fax oder E-Mail. Alle Belege müssen ausgedruckt und elektronisch erfasst werden. Eine Auftragsbestätigung erhält der Kunde nur, wenn er dies ausdrücklich wünscht oder der Produktionsprozess von der üblichen Produktionszeit abweicht. Die Auftragsabwicklung verwendet Kundendaten, Lagerbestände, Aufträge und Bestellungen.	Leiter Auftragsabwicklung	Vertrieb
GP004	**Einkauf (unterstützender Prozess):** In der Einkaufsabteilung werden alle erforderlichen Artikel bestellt, die nicht für den Produktionsprozess erforderlich sind. In dieser Abteilung werden externe Projekte verhandelt, IT-Verträge gestaltet und Verbrauchsmaterial im organisatorischen Umfeld (Papier, Toner etc.) beschafft. Die verwendeten Informationen sind Lagerbestände, Bedarfsmeldungen und Informationen über Lieferanten.	Leiter Einkauf	Einkauf
GP005	**Disposition (Kerngeschäft):** In der Disposition werden alle für die Produktion benötigten Materialien (Kunststoffe, Schrauben, Tüten etc.) beschafft. Hierzu liegen normalerweise Rahmenverträge vor. Geplant wird in diesem Umfeld anhand von Jahresplanmengen und verschiedenen Bestellwerten.	Leiter Disposition	Disposition, Produktion

Tabelle 1: Liste der Geschäftsprozesse der RECPLAST GmbH (Auszug)

Lerneinheit 3.4: Anwendungen erheben



Als Anwendungen erfassen Sie **IT-Lösungen**, die Geschäftsprozesse und die Erledigung von Fachaufgaben unterstützen und die aufgrund ihres Bedarfs an Geheimhaltung, Korrektheit und Unverfälschtheit oder Verfügbarkeit zumindest ein **Mindestmaß an Schutz** erfordern. Zur Identifikation der in dieser Hinsicht wesentlichen und folglich in der Strukturanalyse zu dokumentierenden Anwendungen bieten sich Gespräche oder gemeinsame Workshops mit Benutzern, Anwendungs- und Geschäftsprozessverantwortlichen sowie sachkundigen Mitarbeitern der IT-Abteilung an.

Für jede als wesentlich identifizierte Anwendung sollten Sie **folgende Angaben** in einer Tabelle erfassen:

- eine eindeutige Kennung (Nummer oder Kürzel),
- einen Namen für die Anwendung,
- eine kurze Beschreibung des Ziels, der Funktion und der verarbeiteten Informationen,
- die für die Anwendung Verantwortlichen,
- die Benutzer dieser Anwendung.

Zusätzlich müssen Sie die Abhängigkeiten zwischen Anwendungen und Geschäftsprozessen oder Fachaufgaben dokumentieren, also festhalten, in welchen Prozessen und Fachaufgaben eine gegebene Anwendung benutzt wird.

Achten Sie bei der Erfassung der Anwendungen auf eine **angemessene Granularität**. Beispielsweise ist es in der Regel nicht sinnvoll, ein Office-Produkt in seine einzelnen Bestandteile (z. B. Textverarbeitung, Präsentation, Tabellenkalkulation) zu zerlegen und diese dann gesondert zu beschreiben. Wenn Sie zu feinteilig erfassen, erzeugen Sie einen unnötigen Aufwand für die nachfolgenden Phasen der Sicherheitskonzeption durch ein Übermaß an zu behandelnden Objekten. Bei einer zu groben Betrachtung der Anwendungen verhindern Sie erforderliche Differenzierungen, insbesondere auch bei der Festlegung erforderlicher Schutzmaßnahmen.

Beispiel: Anwendungen der RECPLAST GmbH

Eine vollständige Übersicht aller Anwendungen, die in den Geschäftsprozessen der RECPLAST GmbH bedeutsam sind, würde den Rahmen dieses Kurses sprengen. Die nachfolgenden Tabellen enthalten daher nur einen Ausschnitt, um zu verdeutlichen, wie Sie Anwendungen und ihren Zusammenhang mit den Geschäftsprozessen dokumentieren.

Bezeichnung	Name und Beschreibung der Anwendung	Anzahl	Benutzer	Verantwortlich/Administrator
A001	**Textverarbeitung, Präsentation, Tabellenkalkulation:** Alle geschäftlichen Informationen werden in einem Office-Produkt verarbeitet: Geschäftsbriefe, Analysen oder Präsentationen.	290	Alle Mitarbeiter	IT-Betrieb
A002	**Lotus Notes:** Diese Anwendung wird von allen Mitarbeitern für die Bearbeitung von -E-Mails, Terminen und Kontakten genutzt.	290	Alle Mitarbeiter	IT-Betrieb
...				
A009	**Auftrags- und Kundenverwaltung** Mit dieser datenbankgestützten Anwendung werden Kundenstammdaten und Auftragsdaten verarbeitet sowie die Informationen für Produktion und Lieferung vorbereitet.	55	Marketing & Vertrieb	Marketing & Vertrieb
A010	**Active Directory:** Diese Anwendung soll dem IT-Betrieb die Arbeit erleichtern und doppelte Benutzereingaben reduzieren. Zu allen Nutzern der IT-Systeme werden Informationen zu Gruppenzugehörigkeit, Rechten und Authentisierungsmerkmalen verarbeitet und gespeichert. Diese Anwendung ist über beide Domain Controller verfügbar.	2	Administratoren	IT-Betrieb
...				
A013	**Druckservice BG:** Über diesen Dienst können alle Mitarbeiter in Bad Godesberg die dortigen Drucker benutzen. Er ist auf dem Druckserver in Bad Godesberg verfügbar, kann aber bei Bedarf auch auf dem Druckserver in Beuel gestartet werden.	1	Alle Mitarbeiter in Bad Godesberg	IT-Betrieb

Bezeichnung	Name und Beschreibung der Anwendung	Anzahl	Benutzer	Verantwortlich/Administrator
A014	**Druckservice Beuel:** Über diesen Dienst können alle Mitarbeiter in Beuel die dortigen Drucker benutzen. Er ist auf dem Druckserver in Beuel verfügbar, kann aber bei Bedarf auch auf dem Druckserver in Bad Godesberg gestartet werden.	1	Alle Mitarbeiter in Beuel	IT-Betrieb
A015	**Firewall:** Die Anwendung steuert die Kommunikation zwischen dem Firmennetz und dem Internet und ermöglicht die verschlüsselte Kommunikation der Vertriebsbüros über VPN-Tunnel.	1	Alle Mitarbeiter	IT-Betrieb
A016	**TK-Vermittlung:** Über die beiden miteinander gekoppelten TK-Anlagen in Bad Godesberg und Beuel werden ein- und ausgehende Telefongespräche und Fax-Dokumente vermittelt und ein Telefonverzeichnis gepflegt.	2	Alle Mitarbeiter	IT-Betrieb

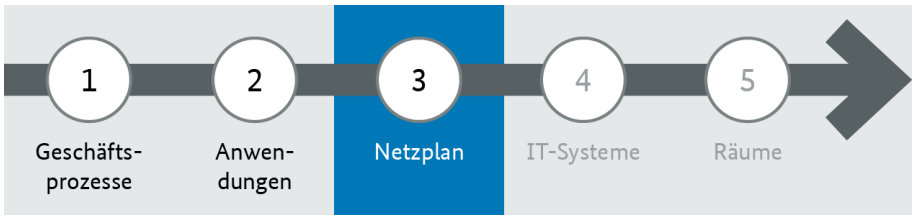
Tabelle 2: Liste der Anwendungen (Auszug)

Die folgende Tabelle zeigt auszugsweise, in welchen Geschäftsprozessen diese Anwendungen verwendet werden:

Geschäftsprozess	Anwendung								
	A001	**A002**	**...**	**A009**	**A010**	**...**	**A013**	**A014**	**...**
GP001 *Produktion*	X			X	X			X	
GP002 *Angebotswesen*	X	X		X	X		X		
GP003 *Auftragsabwicklung*	X	X		X	X		X		
GP004 *Einkauf*	X	X			X		X		
GP005 *Disposition*	X	X		X	X		X		

Tabelle 3: Zuordnung von Anwendungen zu Geschäftsprozessen

Lerneinheit 3.5: Netzplan erheben



Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihre Verbindungen. Im Einzelnen sollte der Plan mindestens die folgenden Objekte enthalten:

- die in das Netz eingebundenen **IT-Systeme**;
  dazu zählen Computer (Clients und Server), Netzdrucker sowie aktive Netzkomponenten (Switches Router, WLAN Access Points) usw.
- die **Verbindungen zwischen diesen IT-Systemen**;
  LAN-Verbindungen (z. B. Ethernet), Backbone-Technik (z. B. ATM) usw.
- die **Außenverbindungen der IT-Systeme**;
  bei diesen sollte zusätzlich die Art der Verbindung gekennzeichnet sein (z. B. Internet-Anbindung, DSL) usw.

In der Regel hat Ihre IT-Administration einen solchen Netzplan bereits erstellt. Ein Netz und die darin eingesetzten Komponenten unterliegen jedoch häufigen Veränderungen, sodass die Aktualität der vorhandenen Pläne nicht unbedingt gewährleistet ist.

Überprüfen Sie daher, ob der Netzplan, den Sie für die Strukturanalyse verwenden, in allen Angaben noch korrekt ist. Befragen Sie z. B. den IT-Verantwortlichen, den Administrator oder Netz- und Systemmanager zur Aktualität der Ihnen vorliegenden Pläne.

Viele Unternehmen oder Behörden verwenden Software, mit denen ein Netzplan automatisch aufgrund der im Netz vorgefundenen Gegebenheiten erzeugt werden kann. Eine solche Darstellung enthält in der Regel jedoch weitaus mehr Informationen als für die Strukturanalyse tatsächlich benötigt werden. Insbesondere fehlt eine angemessene Zusammenfassung der IT-Systeme zu Gruppen. Es empfiehlt sich daher derartige Netzpläne zu „bereinigen", also den Umfang der Informationen auf das tatsächlich Benötigte zu beschränken und die einzelnen Komponenten zweckmäßig zu gruppieren.

Beispiel

Die untenstehende Abbildung zeigt einen solchen bereinigten Netzplan für die RECPLAST GmbH. Hier wurden unter anderem die folgenden Gruppen gebildet:

- Die Desktops der Abteilungen „**Fertigung**" und „**Lager**" wurden zusammengefasst, da sie grundsätzlich gleich ausgestattet sind und mit ihnen auf weitgehend identische Datenbestände zugegriffen werden kann.
- Die drei **Vertriebsbüros** zeichnen sich durch eine einheitliche IT-Ausstattung, übereinstimmende Aufgaben und Regelungen sowie eine identische Zugangsmöglichkeit zum Firmennetz aus. Sie lassen sich in gewisser Weise mit häuslichen Telearbeitsplätzen vergleichen. Sie wurden deswegen zu einer Gruppe zusammengefasst.
- Die nicht vernetzten Komponenten **Faxgeräte** und **TK-Anlagen** wurden jeweils standortübergreifend zu einer Gruppe zusammengefasst, da für den Umgang mit diesen Geräten übereinstimmende organisatorische Regelungen gelten.
- Die **Laptops** wurden getrennt von den Arbeitsplatzrechnern einer Abteilung gruppiert, da für sie wegen der mobilen Nutzung zusätzliche Sicherheitsanforderungen beachtet werden müssen.

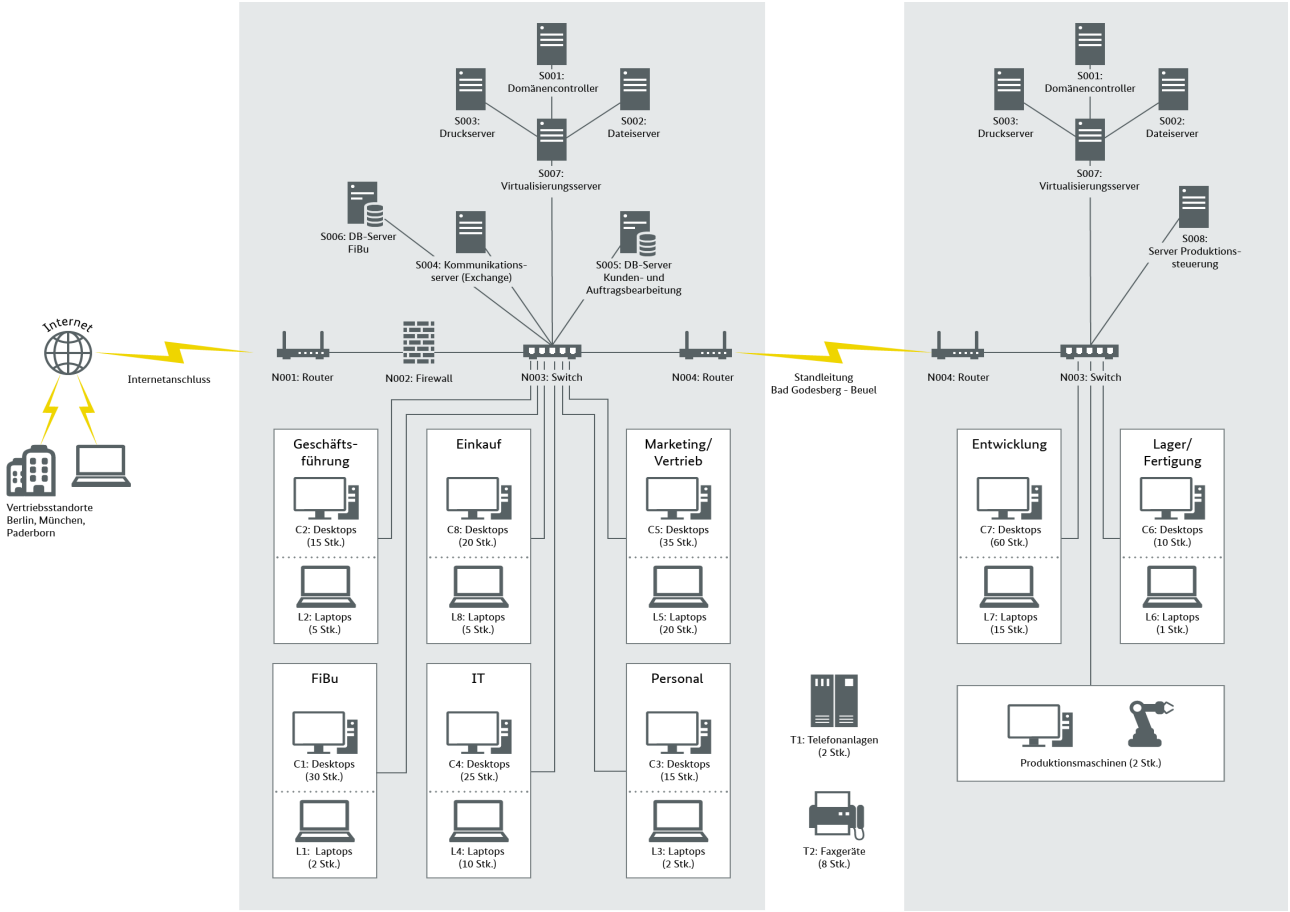
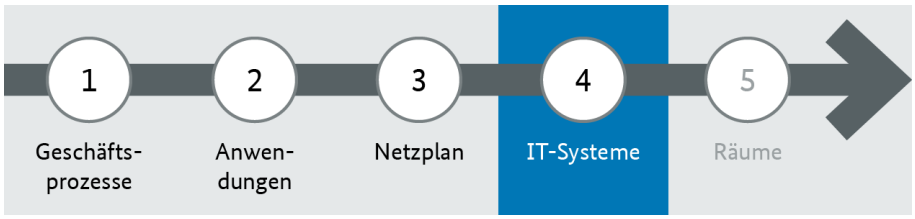


Abbildung 9: Bereinigter Netzplan

Lerneinheit 3.6: IT-Systeme erheben



Bei der Erhebung der IT-Systeme stellen Sie die vorhandenen und geplanten IT-Systeme und anderen IT-Komponenten des Informationsverbundes und die sie jeweils charakterisierenden Angaben zusammen. Dabei dokumentieren Sie auch, für welche Anwendungen ein IT-System jeweils relevant ist. Aufgrund der damit verbundenen besseren Übersichtlichkeit empfehlen sich auch dafür tabellarische Darstellungen.

Was zählt zu den IT-Systemen?

Zu den IT-Systemen zählen

- alle im Netz vorhandenen Computer (Clients und Server), Gruppen von Computern, aktive Netzkomponenten, Netzdrucker, aber auch
- industrielle Steuerungen (Industrial Control Systems, ICS), dazu zählen

  - Geräte, die im Bereich Produktion und Fertigung zur Steuerung oder Überwachung eingesetzt werden, z. B. speicherprogrammierbare Steuerungen (SPS), Maschinen, die über WLAN gesteuert werden, autonome Fahrzeuge, aber auch
  - Arbeitsplatz-PCs zur Steuerung einer Maschine und die Endgeräte wie Scanner oder Drucker, die an diese PCs angeschlossen sind,
- Telekommunikationsgeräte, Mobiltelefone oder andere mobile Geräte sowie
- Objekte aus dem Bereich des Internet of Things (IoT), also Geräte, die vernetzt sind und Daten erfassen, speichern, verarbeiten und übertragen können, z. B. Webcams, Smart-Home-Komponenten oder Sprachassistenten (auch für solche Geräte finden Sie IT-Grundschutz-Bausteine).

Welche Angaben sind für IT-Systeme erforderlich?

Eine tabellarische Übersicht sollte für jedes IT-System die folgenden Angaben enthalten:

- eindeutige Bezeichnung,
- bei Gruppen: Anzahl der zusammengefassten IT-Systeme,
- Beschreibung (insbesondere sollten Sie hier den Einsatzzweck und den Typ anführen z. B. „Server für Personalverwaltung“, „Router zum Internet“),
- Plattform (Welcher Hardwaretyp, welches Betriebssystem?),
- Standort (Gebäude und Raumnummer),
- Status (z. B. in Betrieb, im Test, in Planung) und
- Benutzer und Administrator.

Zur Dokumentation der Beziehungen zwischen IT-Systemen und Anwendungen empfiehlt sich eine Matrix, wie sie in Lerneinheit 3.4: *Anwendungen erheben* auch zur Darstellung der Abhängigkeiten zwischen Geschäftsprozessen und Anwendungen verwendet wird.

Achten Sie bei den vernetzten IT-Systemen darauf, dass die Angaben in der Liste der IT-Systeme mit den Angaben im Netzplan übereinstimmen.

Beispiel

Die folgende Tabelle zeigt einen Auszug der IT-Systeme bei der RECPLAST GmbH. Durch unterschiedliche Buchstaben als erstes Zeichen der Bezeichnung wird der Typ eines IT-Systems verdeutlicht (z. B. kennzeichnet ein „S“ Server oder ein „N“ Netzkkomponenten).

Bezeichnung	Beschreibung des Objekts	Standort	Anzahl	Status	Benutzer	Verantwortlich/Administrator
N001	**Router Internetanbindung:** Dieser Router regelt die Kommunikation zwischen dem Internet und dem internen Netz.	Serverraum BG	1	In Betrieb	Administratoren	IT-Betrieb
N002	**Firewall Internet-Eingang:** Diese Firewall dient als Schutz zwischen dem Internet und dem internen Netz	Serverraum BG	1	In Betrieb	Administratoren	IT-Betrieb
N003	**Switches – Verteilung:** Der Datenfluss zwischen Internet und lokalem Netz wird über diese Switches gesteuert.	Serverräume BG und Beuel	2	In Betrieb	Administratoren	IT-Betrieb
N004	**Router Bonn BG – Beuel:** Über eine Standleitung sind die beiden Standorte in Bonn verbunden. Diese Router sichern die Verbindung ab.	Serverräume BG und Beuel	2	In Betrieb	Administratoren	IT-Betrieb

Bezeichnung	Beschreibung des Objekts	Standort	Anzahl	Status	Benutzer	Verantwortlich/Administrator
...						
S007	**Virtualisierungsserver (Konfiguration 1):** Auf dem Server können bis zu 20 virtuelle Server konfiguriert werden. Für die Verwaltung der virtualisierten Systeme wird eine Anwendung eingesetzt.	Serverräume BG und Beuel	2	In Betrieb	Administratoren	IT-Betrieb
S003	**Print-Server (VM):** Server für die Druckdienste, die zentral gesteuert werden.	Serverräume BG und Beuel	2	In Betrieb	Administratoren	IT-Betrieb
...						
C001	**Arbeitsplatzrechner Einkauf** Standard-PC mit Standardsoftware	Büros BG		In Betrieb	Mitarbeiter Einkauf	IT-Betrieb
C002	**Arbeitsplatzrechner Geschäftsführung** Standard-PC mit Standardsoftware, vertrauliche Korrespondenz	Büros BG		In Betrieb	Mitarbeiter Geschäftsf.	IT-Betrieb
L001	**Laptops Einkauf** Laptop mit Standardsoftware, mobile Nutzung	Büros BG und mobil		In Betrieb	Mitarbeiter Einkauf	IT-Betrieb
L002	**Laptops Geschäftsführung** Laptop mit Standardsoftware, mobile Nutzung, vertrauliche Korrespondenz	Büros BG und mobil		In Betrieb	Mitarbeiter Geschäftsf.	IT-Betrieb
...						
S200	**Alarmanlage** korrekte Funktion ist sehr wichtig für den Schutz aller Werte in den Gebäuden.	Gebäude in BG und Beuel	2	In Betrieb	Pförtner, FASi	Haustechnik
...						
I001	**SPS der Spritzgussmaschine** Speicherprogrammierbare Steuerung und PC zur Steuerung der Produktionsmaschine	Produktionshalle in Beuel	2	In Betrieb	Mitarbeiter Produktion	IT-Betrieb

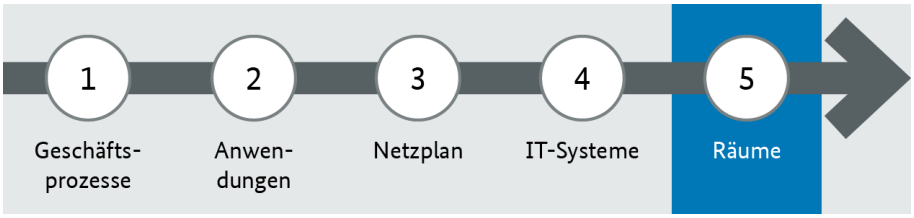
Tabelle 4: Liste der IT-Systeme (Auszug)

Welche Netzkomponenten von den Anwendungen genutzt werden, zeigt auszugsweise die nächste Tabelle:

Bezeichnung	Beschreibung der Anwendung	Router Internet	Firewall	Switche	Router BG-Beuel
A001	Textverarbeitung, Präsentation, Tabellenkalkulation			X	X
A002	Lotus Notes	X	X	X	X
...					
A009	Auftrags- und Kundenverwaltung	X	X	X	X
A010	Active Directory			X	X
...					
A013	Druckservice BG			X	
A014	Druckservice Beuel			X	
...					

Tabelle 5: Zuordnung der Anwendungen zu Netzkomponenten (Auszug)

Lerneinheit 3.7: Räume erheben



Wie gut Informationen und Informationstechnik geschützt sind, hängt immer auch von der Sicherheit der räumlichen Umgebung ab, in der diese benutzt oder aufbewahrt werden. Daher erfassen Sie bei der Strukturanalyse auch alle Gebäude und Räume, die im Zusammenhang mit den betrachteten Informationen und Geschäftsprozessen bedeutsam sind. Dies können Serverräume oder andere ausdrücklich IT-bezogene Räume sein, aber auch Wegstrecken von Kommunikationsverbindungen, normale Büroräume, Schulungs- und Besprechungsräume oder Archivräume.

Zur Dokumentation der Beziehungen zwischen IT-Systemen und Räumen empfiehlt sich eine Matrix, wie sie in Lerneinheit Lerneinheit 3.4: auch zur Darstellung der Abhängigkeiten zwischen Geschäftsprozessen und Anwendungen verwendet wird.

Falls bei Ihnen IT-Systeme, etwa das Datenträgerarchiv, einzelne Server oder Netzkopplungsgeräte, in einem Schutzschrank untergebracht sind, sollten Sie die Schränke auch bei der Erhebung der Räume erfassen.

Beispiel

Nachfolgend sehen Sie einen Auszug aus der Erhebung der Räume der RECPLAST GmbH. Die Liste enthält die beiden Gebäude (Verwaltungs- und Produktionsgebäude), die in ihnen befindlichen Büro- und Serverräume sowie die drei Vertriebsbüros. Die verschiedenen Räume sind zu Gruppen zusammengefasst, durchnummeriert und mit dem Kürzel „GB“ als Gebäude oder dem Kürzel „R“ als Raum gekennzeichnet.

Bezeichnung	Beschreibung	Art	Lokation
GB1	Verwaltungsgebäude	Gebäude	Bonn-Bad Godesberg
GB2	Produktionsgebäude	Gebäude	Bonn-Beuel
...			
R002	Serverraum Bad Godesberg	Serverraum	GB1
...			
R008	Büros Einkauf/Marketing/Vertrieb	Büroräume	GB1, R. 2.03-2.09
...			
R011	Büros Entwicklungsabteilung	Büroräume	GB2, R. 2.14-2.20
...			
R099	Vertriebsbüros	Häuslicher Arbeitsplatz	Berlin, München, Paderborn

Tabelle 6: Liste der Räume (Auszug)

Alternatives Vorgehen: mit den IT-Systemen beginnen

Mit der Erhebung der Räume schließen Sie die Strukturanalyse ab. Im Prinzip ist es auch möglich, abweichend von der hier vorgestellten und empfohlenen Reihenfolge mit der Erhebung der IT-Systeme und des Netzplans zu beginnen. In diesem Fall können Sie die Erhebung wichtiger Anwendungen erleichtern, wenn Sie zunächst Anwendungen betrachten, die von zentralen Komponenten

(z. B. Servern) unterstützt werden, und anschließend diejenigen, die Clients und sonstigen IT-Systemen zugeordnet sind.

Lerneinheit 3.8: Testfragen

Wenn Sie möchten, können Sie mit den nachfolgenden Fragen Ihre Kenntnisse zur Strukturanalyse und ihrer Bedeutung im Rahmen der IT-Grundschutz-Methodik überprüfen. Die Auflösungen zu den Fragen finden Sie im Anhang. Es können mehrere Antwortmöglichkeiten zutreffend sein.

1 **Welche Ziele verfolgt die Strukturanalyse im Rahmen der IT-Grundschutz-Methodik?**

- a die Identifizierung der Objekte, die besonders stark gefährdet sind
- b die Ermittlung der Objekte, die in einem Sicherheitskonzept zu berücksichtigen sind
- c die angemessene Zusammenfassung von Objekten, für die gleiche Sicherheitsmaßnahmen angewendet werden können
- d die Ermittlung der Objekte, für die es passende Bausteine im IT-Grundschutz-Kompendium gibt

2 **Welche Informationen sollten Netzpläne enthalten, die für die Strukturanalyse benötigt werden?**

- a die bei der Erarbeitung des Sicherheitskonzepts beteiligten Organisationseinheiten
- b die Art der Vernetzung der IT-Systeme eines Informationsverbundes
- c die Außenverbindungen des Netzes eines Informationsverbundes
- d die Art der IT-Systeme eines Informationsverbundes

3 **Wann bietet es sich an, IT-Systeme bei der Strukturanalyse zu gruppieren?**

- a wenn diese den gleichen Schutzbedarf und ähnliche Eigenschaften (Betriebssystem, Netzanbindung, unterstützte Anwendungen) haben
- b wenn es für diese Systeme eigene und geeignete Bausteine im IT-Grundschutz-Kompendium gibt
- c wenn diese in denselben Räumlichkeiten untergebracht sind
- d wenn die Anzahl der insgesamt erfassten Objekte zu groß zu werden droht

4 **Welche der folgenden Aufgaben gehören gemäß BSI-Standard 200-2 zur Strukturanalyse?**

- a die angemessene Gruppierung der Komponenten eines Informationsverbundes
- b die Modellierung der Geschäftsprozesse und Fachaufgaben eines Informationsverbundes
- c die Überprüfung, ob die eingesetzte IT die Geschäftsprozesse und Fachaufgaben angemessen unterstützt
- d die Erhebung der Informationen, Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und räumlichen Gegebenheiten eines Informationsverbundes

5 **Welche Angaben sind für IT-Systeme bei der Strukturanalyse zu erfassen?**

- a Typ und Einsatzzweck
- b Lieferant und Preis
- c Benutzer und Administrator
- d Standort (Gebäude und Raum)

6 **Welche Anwendungen sind in der Strukturanalyse zu erfassen?**

a alle Anwendungen, die auf den IT-Systemen im Informationsverbund installiert sind

b alle Anwendungen, die für mindestens einen der bereits erfassten Geschäftsprozesse erforderlich sind

c alle Anwendungen, für die eine gültige Lizenz vorhanden ist

d alle Anwendungen, die von mindestens 20 Prozent der Mitarbeiter genutzt werden

Lektion 4: Schutzbedarfsfeststellung

Wie viel Schutz benötigen der betrachtete Informationsverbund und die ihm zugehörigen Zielobjekte? Wie kommen Sie zu begründeten und nachvollziehbaren Einschätzungen des Schutzbedarfs? Welche Zielobjekte benötigen mehr Sicherheit, bei welchen genügt es, Standard-Anforderungen zu erfüllen?

Ziel der Schutzbedarfsfeststellung ist es, diese Fragen zu klären und damit die Festlegung der Sicherheitsanforderungen und die Auswahl angemessener Sicherheitsmaßnahmen für die einzelnen Zielobjekte des betrachteten Informationsverbundes zu steuern.

In dieser Lektion lernen Sie das Vorgehen bei der Schutzbedarfsfeststellung kennen. Im Einzelnen erfahren Sie,

- wie Sie mithilfe von Schadensszenarien die Schutzbedarfskategorien definieren,
- in welcher Reihenfolge Sie sinnvollerweise den Schutzbedarf für die verschiedenen Zielobjekt-Typen eines Informationsverbundes feststellen,
- wie sich Abhängigkeiten zwischen den Zielobjekten auf die Ergebnisse der Schutzbedarfsfeststellung auswirken sowie
- welche Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung gezogen werden können.

Bei der Basis-Absicherung sind für den betrachteten Informationsverbund nur die Basis-Anforderungen verpflichtend. Daher ist eine Schutzbedarfsfeststellung bei dieser Variante der IT-Grundschutz-Methodik nicht erforderlich.

Lerneinheit 4.1: Grundlegende Definitionen

Bei der Schutzbedarfsfeststellung ist danach zu fragen, welcher Schaden entstehen kann, wenn für ein Zielobjekt die **Grundwerte** Vertraulichkeit, Integrität oder Verfügbarkeit verletzt werden. Dies wäre der Fall, wenn

- vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden (Verletzung der **Vertraulichkeit**),
- die Korrektheit der Informationen und der Funktionsweise von Systemen nicht mehr gegeben ist (Verletzung der **Integrität**),
- autorisierte Benutzer am Zugriff auf Informationen und Systeme behindert werden (Verletzung der **Verfügbarkeit**).

Der Schutzbedarf eines Objekts bezüglich eines dieser Grundwerte orientiert sich an dem Ausmaß des bei Verletzungen jeweils drohenden Schadens. Da dessen Höhe in der Regel vorab nicht genau bestimmt werden kann, sollten Sie eine für Ihren Anwendungszweck passende Anzahl von Kategorien definieren, anhand derer Sie den Schutzbedarf unterscheiden. Die IT-Grundschutz-Methodik empfiehlt hierfür drei **Schutzbedarfskategorien**:

- **normal:** Die Schadensauswirkungen sind begrenzt und überschaubar.
- **hoch**: Die Schadensauswirkungen können beträchtlich sein.
- **sehr hoch**: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Der Schaden, der von einer Verletzung der Grundwerte ausgehen kann, kann sich auf verschiedene **Schadensszenarien** beziehen:

- Verstöße gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts,
- Beeinträchtigungen der persönlichen Unversehrtheit,
- Beeinträchtigungen der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung oder
- finanzielle Auswirkungen.

Wie wichtig ein Szenario jeweils ist, unterscheidet sich von Institution zu Institution. Unternehmen schauen beispielsweise besonders intensiv auf die finanziellen Auswirkungen eines Schadens, da diese bei einer entsprechenden Höhe existenzgefährdend sein können. Für eine Behörde kann es hingegen besonders wichtig sein, das öffentliche Ansehen zu wahren und daher negative Außenwirkungen zu vermeiden.

Lerneinheit 4.2: Schutzbedarfskategorien

Wann hat ein Objekt einen normalen, wann einen hohen und wann einen sehr hohen Schutzbedarf?

Eine allgemeingültige Antwort auf diese Frage ist nicht bei allen Schadensszenarien möglich. Eine erste Abgrenzung der Kategorien finden Sie in Kapitel 8.2.1 des BSI-Standards 200-2: *IT-Grundschutz-Methodik*. Die dort angeführten relativ allgemein gehaltenen Definitionen können Sie als Ausgangspunkt nehmen, an die besonderen Gegebenheiten Ihrer Institution anpassen und gegebenenfalls ergänzen.

Beispielsweise finden Sie dort für die Schutzbedarfskategorie „normal“ und das Schadensszenario „Finanzielle Auswirkungen“ die Festlegung:

- „Der finanzielle Schaden bleibt für die Institution tolerabel.“

Was aber heißt für ein Unternehmen „tolerabel“? Für ein sehr großes Unternehmen spielen einige Millionen Euro mehr oder weniger vielleicht keine große Rolle, kleinere und mittlere Unternehmen kann ein Schaden

in dieser Höhe dagegen zum Bankrott bringen. Bei der Abgrenzung der Schadenskategorien müssen Sie also die Besonderheiten der betrachteten Institution berücksichtigen, zum Beispiel

- in Bezug auf das Szenario „finanzielle Auswirkungen“ die Höhe des Umsatzes oder des Gewinns eines Unternehmens oder die Höhe des bewilligten Budgets einer Behörde,
- in Bezug auf das Szenario „Beeinträchtigung der Aufgabenerfüllung“ das Vorhandensein von Ausweichverfahren bei einem Ausfall eines Verfahrens.

Beispiel

Für das Beispielunternehmen, die RECPLAST GmbH, wurde bezüglich der Schadensszenarien „finanzielle Auswirkungen“ und „Beeinträchtigung der Aufgabenerfüllung“ folgendes festgelegt:

- Normaler Schutzbedarf:
  - „Der mögliche finanzielle Schaden ist kleiner als 50.000 Euro.“
  - „Die Abläufe bei RECPLAST werden allenfalls unerheblich beeinträchtigt. Ausfallzeiten von mehr als 24 Stunden können hingenommen werden.“
- Hoher Schutzbedarf:
  - „Der mögliche finanzielle Schaden liegt zwischen 50.000 und 500.000 Euro.“
  - „Die Abläufe bei RECPLAST werden erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen.“
- Sehr hoher Schutzbedarf:
  - „Der mögliche finanzielle Schaden liegt über 500.000 Euro.“
  - „Die Abläufe bei RECPLAST werden so stark beeinträchtigt, dass Ausfallzeiten, die über zwei Stunden hinausgehen, nicht toleriert werden können.“

Lerneinheit 4.3: Vorgehen und Vererbung

Die Objekte im Informationsverbund werden eingesetzt, um Geschäftsprozesse und Anwendungen zu unterstützen. Daher hängt der Schutzbedarf eines Objekts vom Schutzbedarf derjenigen Geschäftsprozesse und Informationen ab, für deren Bearbeitung es benötigt wird.

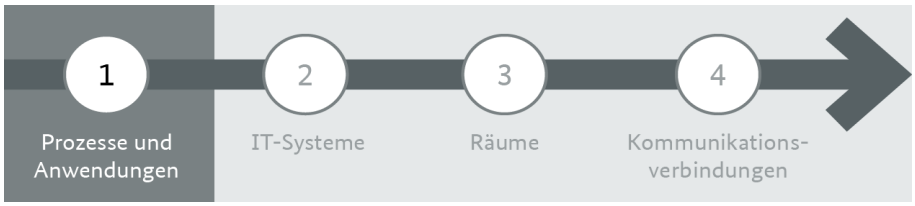
Zunächst wird deshalb der Schutzbedarf der Geschäftsprozesse und zugehörigen Informationen bestimmt. Deren Schutzbedarf vererbt sich auf den der Anwendungen, IT-Systeme, Räume und Kommunikationsverbindungen.

Bei der **Vererbung** lassen sich, am Beispiel von IT-Systemen veranschaulicht, **folgende Fälle** unterscheiden:

- In vielen Fällen lässt sich der höchste Schutzbedarf aller Anwendungen, die das IT-System benötigen, übernehmen (**Maximumprinzip**).
- Wenn eine Anwendung auf die Ergebnisse einer anderen Anwendung angewiesen ist, überträgt sich ihr Schutzbedarf auf diese liefernde Anwendung. Werden diese beiden Anwendungen auf verschiedenen IT-Systemen ausgeführt, dann muss auch der Schutzbedarf des einen auf das liefernde System übertragen werden (**Betrachtung von Abhängigkeiten**).
- Der Schutzbedarf des IT-Systems kann höher sein als der Schutzbedarf der einzelnen Anwendungen (**Kumulationseffekt**). Dies ist z. B. der Fall, wenn auf einem Server mehrere Anwendungen mit normalem Schutzbedarf betrieben werden. Der Ausfall einer dieser Anwendungen könnte überbrückt werden. Wenn aber alle Anwendungen gleichzeitig ausfallen, kann ein hoher Schaden entstehen.

- Der Schutzbedarf kann niedriger sein als der Schutzbedarf der zugeordneten Anwendungen, wenn eine Anwendung mit hohem Schutzbedarf auf mehrere Systeme verteilt ist und auf dem betreffenden IT-System nur weniger wichtige Teile dieser Anwendung ausgeführt werden (**Verteilungseffekt**). Bei Anwendungen, die personenbezogene Daten verarbeiten, sind z. B. Komponenten weniger kritisch, in denen die Daten nur in pseudonymisierter Form verwendet werden.

Lerneinheit 4.4: Schutzbedarfsfeststellung für Prozesse und Anwendungen



Um die Schäden einzuschätzen, die aus Verletzungen der Integrität, Vertraulichkeit oder Verfügbarkeit bei den Prozessen und Anwendungen entstehen können, sollten Sie **aus Sicht der Anwender** realistische Schadensszenarien entwickeln.

Dabei kann es Ihnen helfen, **„Was wäre wenn ...?“-Fragen** zu jedem Schadensszenario zu formulieren, z. B. was wäre, wenn geheime Geschäftsdaten aus der Anwendung „Finanzbuchhaltung“ bekannt werden?

- Gegen welche Gesetze oder Vorschriften wird verstoßen? Welche rechtlichen Konsequenzen oder Sanktionen können mit dem Vorfall verbunden sein?
- Gibt es Personen, deren informationelles Selbstbestimmungsrecht beeinträchtigt wird? Wenn ja, mit welchen Folgen?
- Wie stark werden Abläufe in der Firma behindert?
- Droht ein Image-Schaden und mit welchen Folgen wäre er verbunden?
- Kann dieser Vorfall finanzielle Auswirkungen haben und falls ja, in welcher Höhe?

Im Anhang des BSI-Standards 200-2 finden Sie zu jedem Schadensszenario beispielhafte Fragestellungen, die Sie für Ihre Schutzbedarfsfeststellung anpassen und eventuell ergänzen können.

Im nächsten Schritt beantworten Sie für alle Anwendungen, die Sie in der Strukturanalyse erfasst haben, die zu den Schadensszenarien entwickelten Fragen und schätzen so den Schutzbedarf der Anwendungen im Hinblick auf die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit ein.

Bei der Abschätzung des Schadens sollten Sie unbedingt die Verantwortlichen und die Benutzer der Anwendung einbeziehen. Diese wissen meist sehr genau, welche Schäden bei falschen Daten oder bei einem Ausfall einer Anwendung auftreten. Es ist trotzdem möglich, dass der Schutzbedarf innerhalb der Projektgruppe oder von befragten Mitarbeitern unterschiedlich eingeschätzt wird. Falls kein Konsens erzielt werden kann, muss die Leitungsebene entscheiden.

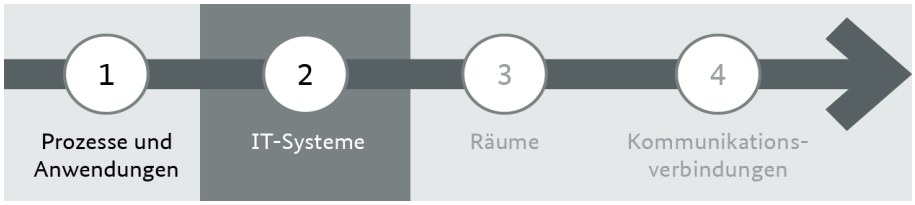
Wichtig ist, dass Sie die Schutzbedarfsfeststellungen begründen und zwar so ausführlich, dass die getroffenen Entscheidungen auch von anderen Personen (z. B. der Leitungsebene) und zu späteren Zeitpunkten nachvollzogen und gegebenenfalls auch korrigiert werden können. So können Geschäftsführung, Benutzer und Abteilungsleiter durchaus unterschiedlicher Auffassung darüber sein, wie wichtig eine Anwendung für die Geschäftsvorgänge ist.

Nachfolgend als Beispiel die Schutzbedarfsfeststellung für einige Anwendungen der RECPLAST GmbH.

Bezeichnung	Beschreibung der Anwendung	Schutzziel und Schutzbedarf	Begründung
A001	Textverarbeitung, Präsentation, Tabellenkalkulation	Vertraulichkeit: **normal**	Die Office-Anwendung selbst enthält keine Informationen
		Integrität: **normal**	Die Office-Anwendung selbst enthält keine Informationen
		Verfügbarkeit: **normal**	Die Anwendung ist lokal installiert; eine Neuinstallation ist schnell möglich. Die Lizenzen sind sicher verwahrt. Eine Ausfallzeit von 24 Stunden oder mehr ist akzeptabel.
A002	Lotus Notes	Vertraulichkeit: **hoch**	Es werden Mails mit vertraulichem Inhalt bearbeitet; die Informationen über Geschäftskontakte und Treffen mit Partnern oder Kunden sind vertraulich.
		Integrität: **normal**	Fehlerhafte Daten können in der Regel leicht erkannt werden.
		Verfügbarkeit: **sehr hoch**	Mails, Kontaktdaten und Terminvereinbarungen sind wesentlich für die Geschäftsvorgänge. Ein Ausfall von mehr als 2 Stunden kann nicht hingenommen werden.

Tabelle 7: Schutzbedarf von Anwendungen (Auszug)

Lerneinheit 4.5: Schutzbedarfsfeststellung für IT-Systeme



IT-Systeme werden eingesetzt, um Anwendungen zu unterstützen. Der Schutzbedarf eines IT-Systems hängt damit im Wesentlichen von dem Schutzbedarf derjenigen Anwendungen ab, für deren Ausführung es benötigt wird. Der Schutzbedarf der Anwendung vererbt sich wie oben beschrieben auf den Schutzbedarf des IT-Systems.

Nachfolgend einige Hinweise zu speziellen Typen von IT-Systemen

- In **virtualisierten Infrastrukturen** werden in der Regel mehrere IT-Systeme auf einem Virtualisierungsserver betrieben. Der Schutzbedarf der einzelnen virtuellen IT-Systeme ergibt sich aus dem der Anwendungen, der des Virtualisierungsservers ergibt sich daraus zunächst nach dem Maximumprinzip. Wenn aber mehrere Schäden zu einem höheren Gesamtschaden führen können, kann sich der Schutzbedarf des Virtualisierungsservers durch Kumulation erhöhen. Für das Schutzziel Verfügbarkeit gilt: Wenn durch Konzepte der Virtualisierung Redundanzen geschaffen werden, kann wegen des Verteilungseffekts der Schutzbedarf des Virtualisierungsservers wieder gesenkt werden.
- Den Schutzbedarf von **ICS-Komponenten** sollten Sie gemeinsam mit den Anlagenverantwortlichen auf Grundlage des Anwendungszwecks festlegen. Dabei kann es sinnvoll sein, die Definition der Schutzbedarfskategorien an die besonderen Bedingungen einer Produktionsumgebung anzupassen.
- Für **sonstige Geräte** (z. B. aus dem Bereich Internet of Things) müssen Sie zunächst feststellen, für welche Geschäftsprozesse und Anwendungen sie eingesetzt werden. Zur Ermittlung des Schutzbedarfs eines Geräts betrachten Sie den möglichen Schaden für den jeweiligen Geschäftsprozess. Sie sollten nur Geräte

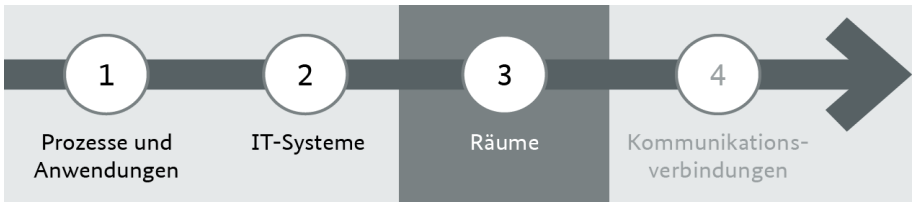
erfassen, die einen nennenswerten Einfluss auf die Informationssicherheit haben, und sie möglichst zu Gruppen zusammenfassen.

Auch der Schutzbedarf für die IT-Systeme sollte für jeden der drei Grundwerte (Vertraulichkeit, Integrität und Verfügbarkeit) festgelegt und anschließend z. B. tabellarisch dokumentiert werden. Ein Beispiel:

Bezeichnung	Beschreibung des Systems	Schutzziel und Schutzbedarf	Begründung
S007	Virtualisierungsserver	Vertraulichkeit: **hoch**	*Maximumprinzip*: Der Domain Controller beinhaltet das Active Directory und damit die Anmeldeinformationen aller Mitarbeiter.
		Integrität: **hoch**	*Maximumprinzip*: Der Dateiserver verwaltet Dateien, deren Korrektheit für den Geschäftsbetrieb sichergestellt sein muss.
		Verfügbarkeit: **hoch**	*Kumulationseffekt*: Sowohl der Domain Controller als auch der Dateiserver haben jeder hohe Verfügbarkeitsanforderungen. Daraus ergibt sich für den Virtualisierungsserver ein sehr hoher Schutzbedarf. Alle virtualisierten Systeme können aber innerhalb kurzer Zeit auf dem anderen Virtualisierungsserver zur Verfügung gestellt werden. Durch diesen *Verteilungseffekt* reduziert sich der Schutzbedarf auf ein nur noch hohes Niveau.
N001	Internet-Router	Vertraulichkeit: **hoch**	Es werden auch vertrauliche Informationen über die Internet-Anbindung übertragen, wenn ein Kunde oder Geschäftspartner eine verschlüsselte Kommunikation nicht unterstützt.
		Integrität: **normal**	Fehlerhafte Daten können in der Regel leicht erkannt werden.
		Verfügbarkeit: **normal**	Ein Ausfall der Internet-Anbindung kann für 24 Stunden toleriert werden.
N002	Firewall	Vertraulichkeit: **hoch**	Es werden auch vertrauliche Informationen über die Internet-Anbindung übertragen, wenn ein Kunde oder Geschäftspartner eine verschlüsselte Kommunikation nicht unterstützt. Außerdem werden die verschlüsselten Verbindungen zu den Vertriebsbüros über die Firewall abgewickelt.
		Integrität: **normal**	Fehlerhafte Daten können in der Regel leicht erkannt werden.
		Verfügbarkeit: **normal**	Ein Ausfall der Internet-Anbindung kann für 24 Stunden toleriert werden.
S200	Alarmanlagen	Vertraulichkeit: **normal**	Die Alarmanlagen verarbeiten keine vertraulichen Informationen.
		Integrität: **sehr hoch**	Das korrekte Funktionieren der Alarmanlagen ist für die Sicherheit der Gebäude sehr wichtig.
		Verfügbarkeit: **sehr hoch**	Das korrekte Funktionieren der Alarmanlagen ist für die Sicherheit der Gebäude sehr wichtig.

Tabelle 8: Schutzbedarf der IT-Systeme (Auszug)

Lerneinheit 4.6: Schutzbedarfsfeststellung für Räume



Bei der Schutzbedarfsfeststellung für Räume berücksichtigen Sie alle Räume und Liegenschaften, die Sie zuvor in der Strukturanalyse identifiziert haben und die für die Informationen, Anwendungen und IT-Systeme des betrachteten Informationsverbundes relevant sind.

Auch hier sind wieder Vererbungsprinzipien zu berücksichtigen. Der Schutzbedarf eines Raums bemisst sich nach dem Schutzbedarf der IT-Systeme, die sich in ihm befinden, sowie der Informationen und Datenträger, die in ihm verarbeitet und gelagert werden. Folglich können Sie (wie schon bei der Schutzbedarfsfeststellung der IT-Systeme) in den meisten Fällen wieder das Maximumprinzip anwenden. Unter Umständen ergibt sich aus der Vielzahl an Objekten, die sich in einem Raum befinden, jedoch ein höherer Schutzbedarf in einem Grundwert als für jedes einzelne Objekt (Kumulationseffekt). Dies kann z. B. für Räume gelten, in denen sich gespiegelte Server mit jeweils normalen Verfügbarkeitsanforderungen befinden, bei Ausfall eines Servers gibt es ja noch einen zweiten, während von einem Ausfall des Raums (zum Beispiel aufgrund eines Brandes) beide Server betroffen sind. Dies gilt nicht, wenn sich die beiden Server in unterschiedlichen Räumen oder sogar Gebäuden befinden.

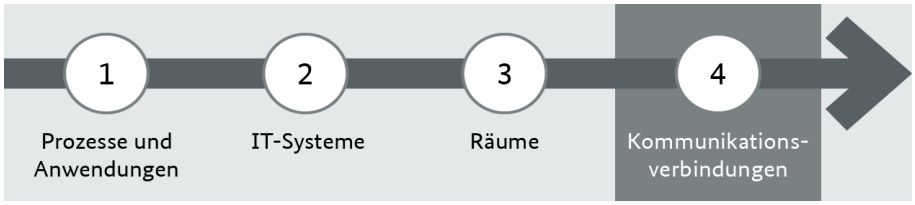
Beispiel

Die folgende Tabelle gibt ein Beispiel für die Dokumentation der Schutzbedarfsfeststellung für die Räume der RECPLAST GmbH.

Raum			IT-Systeme	Schutzbedarf		
Bezeichnung	**Art**	**Lokation**		**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
BG, R. 1.01	Technikraum	GB1	TK-Anlage T1	normal	normal	Hoch
BG, R. 1.02	Serverraum	GB1	N001 bis N004 S001 bis S007	Hoch	Hoch	Hoch
Beuel, R. 2.01	Serverraum	GB2	N004 S003, S007 S040	Hoch	Hoch	Hoch
Beuel, R. 2.10-2.15	Büroraum	GB2	A002, L007	Hoch	normal	normal

Tabelle 9: Schutzbedarf der Räume (Auszug)

Lerneinheit 4.7: Schutzbedarfsfeststellung für Kommunikationsverbindungen



Im nächsten Arbeitsschritt müssen Sie den Schutzbedarf für die Kommunikationsverbindungen feststellen. Es gibt Verbindungen, die gefährdeter sind als andere und durch doppelte Auslegung oder durch besondere Maßnahmen gegen Angriffe von außen oder innen geschützt werden müssen.

Kritische Verbindungen

Sie sollten folgende **Verbindungen** als **kritisch** einstufen:

- Verbindungen, die aus dem Unternehmen oder der Behörde **in ein öffentliches Netz** (z. B. Telefonnetz, Internet) oder **über ein öffentliches Gelände** reichen. Über solche Verbindungen können Schadprogramme in das Datennetz der Institution eingeschleust werden, Server der Institution angegriffen werden oder Mitarbeiter vertrauliche Daten an Unbefugte weiterleiten.
- Verbindungen, über die besonders **schützenswerte Informationen** übertragen werden. Mögliche Gefährdungen sind Abhören, vorsätzliche Manipulation und betrügerischer Missbrauch. Vom Ausfall solcher Verbindungen sind Anwendungen, für die eine hohe Verfügbarkeit erforderlich ist, besonders betroffen.
- Verbindungen, über die vertrauliche Informationen **nicht übertragen werden dürfen**. Personaldaten dürfen zum Beispiel nur von Mitarbeitern der Personalabteilung und der Geschäftsführung eingesehen und bearbeitet werden. Daher muss verhindert werden, dass diese Daten bei ihrer Übertragung von unbefugten Mitarbeitern eingesehen werden können.

In Ihrer Dokumentation sollten Sie die kritischen Verbindungen durch Hervorhebung im Netzplan oder eine tabellarische Zusammenstellung gesondert ausweisen.

Beispiele für kritische Verbindungen

Die folgende Tabelle veranschaulicht am Beispiel der RECPLAST GmbH, wie kritische Verbindungen dokumentiert werden können.

Bezeichnung	Beschreibung	Vertraulichkeit	Integrität	Verfügbarkeit
K001	Firmennetz – Internet	**Hoch:** Vertrauliche Informationen können z. B. an den Wettbewerb gelangen	**Hoch:** Falsche Informationen können den Ruf schädigen.	**Hoch:** Ohne diese Außenverbindung kann keine Kommunikation stattfinden.
K002	Standleitung Bad Godesberg – Beuel	**Hoch:** Interne Informationen müssen vertraulich übertragen werden.	**Normal:** Verfälschung von Informationen ist nur mit hohem Aufwand möglich.	**Hoch:** Die Verbindung ist zur Übermittlung der Aufträge an die Produktion unbedingt erforderlich.

Bezeichnung	Beschreibung	Vertraulichkeit	Integrität	Verfügbarkeit
K011	Anbindung der Arbeitsplätze der Geschäftsführung	**Hoch:** Die Geschäftsführung bearbeitet vertrauliche Korrespondenz	**Normal:** Verfälschung von Informationen ist nur mit hohem Aufwand möglich.	**Hoch:** Die Verbindung ist zum Kontakt mit Geschäftspartnern unbedingt erforderlich.
K012	Anbindung der Arbeitsplätze der Personalabteilung	**Hoch:** Die Personalabteilung arbeitet mit personenbezogenen Daten.	**Normal:** Verfälschung von Informationen ist nur mit hohem Aufwand möglich.	**Normal:** Die Arbeiten sind nicht zeitkritisch. Ein Ausfall von 24 Stunden oder länger ist akzeptabel.
K013	Anbindung der Entwickler-Arbeitsplätze	**Hoch:** Die Ergebnisse der Arbeit sind geheim zu halten.	**Normal:** Verfälschung von Informationen ist nur mit hohem Aufwand möglich.	**Normal:** Die Arbeiten sind nicht zeitkritisch. Ein Ausfall von 24 Stunden oder länger ist akzeptabel.

Tabelle 10: kritische Kommunikationsverbindungen (Auszug)

Lerneinheit 4.8: Testfragen

Wenn Sie möchten, können Sie mit den nachfolgenden Fragen Ihre Kenntnisse zur Schutzbedarfsfeststellung gemäß IT-Grundschutz überprüfen. Die Auflösungen zu den Fragen finden Sie im Anhang. Es können mehrere Antwortmöglichkeiten zutreffend sein.

1 **Welche klassischen Schutzziele werden bei der Schutzbedarfsfeststellung gemäß IT-Grundschutz empfohlen?**

a Authentizität

b Verfügbarkeit

c Vertraulichkeit

d Integrität

2 **In welchen Fällen können Sie gemäß IT-Grundschutz-Methodik auf die Schutzbedarfsfeststellung für ein IT-System verzichten?**

a wenn das IT-System spätestens innerhalb von 18 Monaten ausgesondert wird

b wenn das IT-System nicht eingesetzt wird

c wenn die Anwendungen, die es unterstützt, nur einen normalen Schutzbedarf haben

d wenn der Schutzbedarf bereits im Rahmen einer vor einem Jahr durchgeführten Revision festgestellt wurde

3 **Welche Kriterien berücksichtigen Sie bei der Bestimmung des Bedarfs an Verfügbarkeit eines IT-Systems?**

a die maximal tolerierbare Ausfallzeit des IT-Systems

b den Aufwand, der erforderlich ist, um das IT-System nach einer Beschädigung wiederherzustellen

c die Anzahl der Benutzer des IT-Systems

d die Anschaffungskosten des IT-Systems

4 **Was berücksichtigen Sie, wenn Sie den Schutzbedarf einer Anwendung bestimmen?**

a die Informationen, die im Zusammenhang mit der Anwendung verwendet werden

b die Bedeutung der Anwendung für die Geschäftsprozesse oder Fachaufgaben

c die relevanten Gefährdungen, denen die Anwendung ausgesetzt ist

d die räumliche Umgebung des IT-Systems, das die Anwendung bereitstellt

5 **Unter welchen Bedingungen kann der Schutzbedarf eines IT-Systems bezüglich Verfügbarkeit geringer sein als derjenige der Anwendungen, für die es eingesetzt wird?**

a wenn der Buchwert des IT-Systems einen zuvor definierten Schwellwert unterschreitet

b wenn das IT-System nur solche Teile der Anwendungen bedient, die einen geringeren Schutzbedarf haben

c wenn mindestens ein weiteres redundantes IT-System in Betrieb ist, das die betreffenden Anwendungen bereitstellen kann

d wenn die Anwendungen innerhalb der nächsten drei Monate so umstrukturiert werden sollen, dass das betreffende IT-System nicht mehr benötigt wird

6 **Wenn bei der Schutzbedarfsfeststellung für ein IT-System Kumulationseffekte berücksichtigt werden, bedeutet dies, dass ...**

a ... sich der Schutzbedarf des IT-Systems erhöht, weil sich Einzelschäden zu einem höheren Gesamtschaden addieren.

b ... sich der Schutzbedarf des IT-Systems verringert, weil geeignete, sich gegenseitig verstärkende Sicherheitsmaßnahmen im Einsatz sind.

c ... sich der für das IT-System festgestellte Schutzbedarf auch auf den Schutzbedarf anderer IT-Systeme auswirkt, die mit dem betreffenden IT-System vernetzt sind.

d **...** der Schutzbedarf des IT-Systems erst festgestellt werden kann, wenn der Schutzbedarf der mit diesem vernetzten IT-Systeme festgestellt ist.

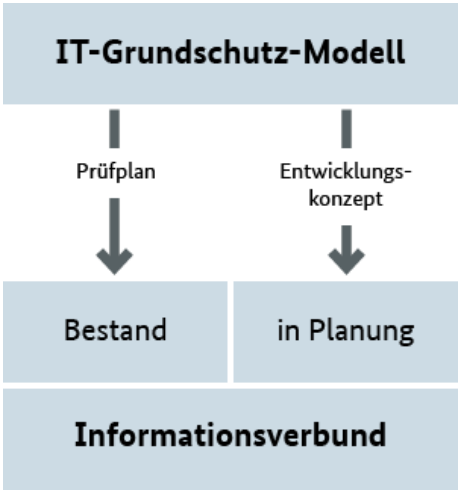
Lektion 5: Modellierung gemäß IT-Grundschutz

In den vorangegangen Schritten haben Sie die einzelnen Komponenten ermittelt, die Zielobjekte des Sicherheitskonzepts für den betrachteten Informationsverbund sind, und detailliert deren Schutzbedarf bewertet. Darauf aufbauend sind im nächsten Schritt, der **Modellierung gemäß IT-Grundschutz**, die relevanten Sicherheitsanforderungen für die einzelnen Zielobjekte zu bestimmen. Als Ergebnis erhalten Sie ein **IT-Grundschutz-Modell** des Informationsverbundes.

Dieses Modell kann sowohl dazu dienen, die Sicherheit bestehender Systeme und Verfahren zu bewerten, als auch zu einer angemessenen Berücksichtigung der Informationssicherheit bei der Einführung neuer Elemente beitragen. Kurz gesagt liefert es

- für bestehende Teile des Informationsverbundes die Vorgaben für einen **Prüfplan** und
- für geplante Teile die Vorgaben für ein **Entwicklungskonzept**

zur Informationssicherheit.



Bei der Entwicklung des IT-Grundschutz-Modells werden Sie durch das **IT-Grundschutz-Kompendium** unterstützt. In dieser Lektion lernen Sie daher den Aufbau und die Inhalte dieses Dokuments kennen und erfahren,

- wie Sie es verwenden, um ein IT-Grundschutz-Modell eines Informationsverbundes anzufertigen,
- wie Sie spezielle Szenarien z. B. virtualisierte Systeme in einem solchen Modell berücksichtigen und
- wie Sie die Ergebnisse der Modellierung geeignet dokumentieren.

Lerneinheit 5.1: IT-Grundschutz-Bausteine

Das IT-Grundschutz-Kompendium ist modular aufgebaut. Den Kern bilden die jeweils rund zehn Seiten langen **IT-Grundschutz-Bausteine**, in denen jeweils für einen bestimmten Aspekt der Informationssicherheit typische Gefährdungen und Sicherheitsanforderungen beschrieben werden. Gegenstand eines Bausteins können übergeordnete Themen sein wie das Informationssicherheits- oder Notfallmanagement, aber auch mehr oder weniger spezielle technische Systeme, die üblicherweise in Unternehmen und Behörden im Einsatz sind, etwa Clients und Server, mobile Systeme oder auch industrielle Steuerungen.

Den Bausteinen sind einleitende Kapitel vorangestellt, die unter anderem Hinweise zur Anwendung des IT-Grundschutz-Kompendiums und eine Übersicht Elementarer Gefährdungen enthalten, zu dieser Übersicht und ihrem Stellenwert im Rahmen der IT-Grundschutz-Methodik erfahren Sie in Lektion 7: Risikoanalyse mehr.

Alle Bausteine sind in gleicher Weise gegliedert:

- Sie beginnen mit einer **kurzen Beschreibung** und Abgrenzung des behandelten Sachverhalts.
- Es folgt eine Darstellung der spezifischen **Gefährdungslage** mit Hilfe exemplarischer Gefährdungen.
- Den Kern bilden die in drei Gruppen unterteilten **Sicherheitsanforderungen**:
  - vorrangig zu erfüllende **Basis-Anforderungen**,
  - für eine vollständige Umsetzung des IT-Grundschutzes und eine dem Stand der Technik gemäße Sicherheit zusätzlich zu erfüllende **Standard-Anforderungen** sowie
  - Anforderungen für den **erhöhten Schutzbedarf**.
- Den Abschluss bilden Verweise auf weiterführende Informationen sowie eine Kreuzreferenztabelle, in der die Anforderungen mit den jeweils zutreffenden elementaren Gefährdungen miteinander in Bezug gesetzt werden.

Die Anforderungen beschreiben, was getan werden MUSS oder SOLLTE. In Großbuchstaben gesetzte Verben zeigen dabei die **Verbindlichkeit einer Anforderung**. Die folgende Tabelle gibt hierzu eine Übersicht:

Ausdruck	Bedeutung
MUSS, DARF NUR	So gekennzeichnete Anforderungen müssen unbedingt erfüllt werden.
DARF NICHT, DARF KEIN	Etwas darf in keinem Fall getan werden.
SOLLTE	Dieser Ausdruck bedeutet, dass eine Anforderung zwar normalerweise erfüllt werden muss, bei stichhaltigen Gründen aber auch davon abgesehen werden kann.
SOLLTE NICHT, SOLLTE KEIN	Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden darf, bei stichhaltigen Gründen aber trotzdem erfolgen kann.

Tabelle 11: Sprachgebrauch in den IT-Grundschutz-Bausteinen

Lerneinheit 5.2: Schichtenmodell

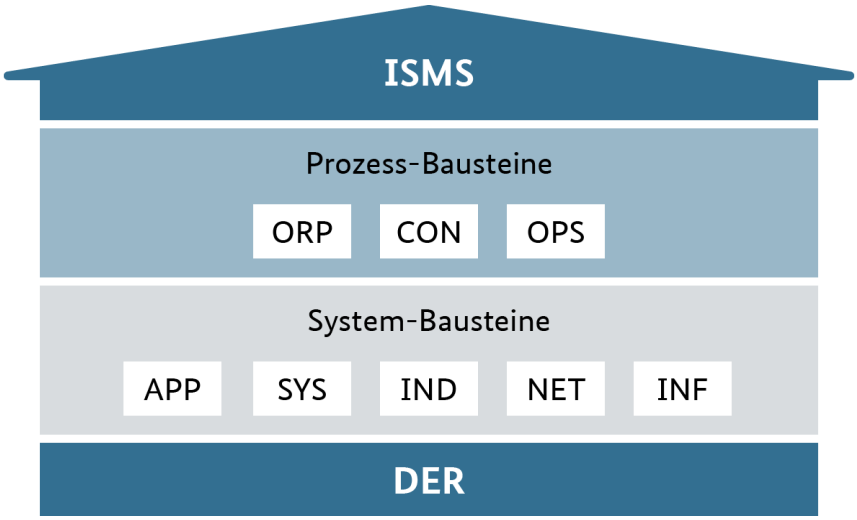


Abbildung 10: Schichtenmodell

Die verschiedenen IT-Grundschutz-Bausteine sind in ein **Schichtenmodell** gegliedert, das wie folgt aufgebaut ist (in Klammern werden exemplarische Bausteine genannt):

- **Prozess-Bausteine:**
  - **ISMS**: Sicherheitsmanagement (ISMS.1 *Sicherheitsmanagement*)
  - **ORP:** Organisation und Personal (ORP.1 *Organisation*, ORP.2 *Personal*, ORP.3 *Sensibilisierung und Schulung*, ORP.4 *Identitäts- und Berechtigungsmanagement*, ORP.5 *Compliance Management*)
  - **CON**: Konzeption und Vorgehensweisen (CON.1 *Kryptokonzept*, CON.2 *Datenschutz*, CON.3 *Datensicherungskonzept*, CON.4 *Auswahl und Einsatz von Standardsoftware*, CON.5 *Entwicklung und Einsatz von Allgemeinen Anwendungen*, CON.6 *Löschen und Vernichten*, CON.7 *Informationssicherheit auf Auslandsreisen*)
  - **OPS**: Betrieb, aufgeteilt in die vier Teilschichten *Eigener IT-Betrieb*, *Betrieb von Dritten*, *Betrieb für Dritte* und *Betriebliche Aspekte* (OPS.1.1.2 *Ordnungsgemäße IT-Administration*, OPS.1.1.3 *Patch- und Änderungsmanagement*, OPS.1.1.4 *Schutz vor Schadprogrammen*, OPS.1.1.5 *Protokollierung*, OPS.2.1 *Outsourcing für Kunden*, OPS.2.4 *Fernwartung*)
  - **DER:** Detektion und Reaktion (DER.1 *Detektion von sicherheitsrelevanten Ereignissen*, DER.2.1 *Behandlung von Sicherheitsvorfällen*, DER2.2 *Vorsorge für die IT-Forensik*, DER.3.1 *Audits und Revisionen*, DER.4 *Notfallmanagement*)
- **System-Bausteine:**
  - **APP**: Anwendungen (APP.1.1 *Office Produkte*, APP.1.2 *Webbrowser*, APP.3.2 *Webserver*, APP.5.1 *Allgemeine Groupware*, APP.5.2 *Microsoft Exchange und Outlook*)
  - **SYS**: IT-Systeme (SYS.1.1 *Allgemeiner Server*, SYS.1.2.2 *Windows Server 2012*, SYS.1.5 *Virtualisierung*, SYS.2.1 *Allgemeiner Client*, SYS.2.3 *Client unter Windows 10*, SYS.3.1 *Laptops*, SYS 3.2.1 *Allgemeine Smartphones und Tablets*, SYS.3.4 *Mobile Datenträger*, SYS.4.4 *Allgemeines IoT-Gerät*)
  - **IND**: Industrielle IT (IND.1 *Betriebs- und Steuerungstechnik*, IND.2.1 *Allgemeine ICS-Komponente*, IND.2.3 *Sensoren und Aktoren)*
  - **NET**: Netze und Kommunikation (NET.1.1 *Netzarchitektur und Design*, NET.1.2 *Netzmanagement*, NET.2.1 *WLAN-Betrieb*, NET.2.2 *WLAN-Nutzung*, NET.3.1 *Router und Switches*, NET.3.2 *Firewall*)

- **INF**: Infrastruktur (INF.1 *Allgemeines Gebäude*, *INF.2 Rechenzentrum sowie Serverraum*, INF.3 *Elektrotechnische Verkabelung*, INF.4 *IT-Verkabelung*, INF.7 *Büroarbeitsplatz*, INF.8 *Häuslicher Arbeitsplatz*)

Vorteile des Schichtenmodells

Die im IT-Grundschutz-Kompendium vorgenommene Einteilung der Bausteine bietet eine Reihe von Vorteilen. So wird durch die vorgenommene Aufteilung der verschiedenen Einzelaspekte der Informationssicherheit die Komplexität dieses Themas zweckmäßig reduziert undRedundanzen werden vermieden. Dies erleichtert es auch, gezielt Einzelaspekte eines entwickelten Sicherheitskonzepts zu aktualisieren, ohne dass davon andere Teile des Konzepts beeinflusst werden.

Die einzelnen Schichten sind darüber hinaus so gewählt, dass Zuständigkeiten gebündelt sind. So adressieren die Schichten ISMS und ORP primär das Sicherheitsmanagement einer Institution, die Schicht INF die Haustechnik und die Schichten SYS, NET und APP die für IT-Systeme, Netze und Anwendungen jeweils zuständigen Verantwortlichen, Administratoren und Betreiber.

Das **IT-Grundschutz-Kompendium** wird **kontinuierlich aktualisiert und erweitert**. Dabei berücksichtigt das BSI mit jährlich durchgeführten Befragungen die Wünsche der Anwender. Wenn Sie regelmäßige aktuelle Informationen zum IT-Grundschutz wünschen oder sich an Befragungen zu dessen Weiterentwicklung beteiligen möchten, können Sie sich beim BSI für den Bezug des **IT-Grundschutz-Newsletters** registrieren lassen (zur Registrierung). Für den fachlichen Austausch und die Information über Aktuelles zum IT-Grundschutz haben Sie hierzu in einer eigenen Gruppe zum IT-Grundschutz bei XING und auch bei TWITTER Gelegenheit.

Lerneinheit 5.3: Vorgehen

Bei der Modellierung wählen Sie diejenigen IT-Grundschutz-Bausteine aus, die Sie für die Sicherheit des betrachteten Informationsverbundes benötigen. Sehen Sie sich dazu die Bausteine der einzelnen Schichten an und entscheiden Sie, ob und auf welche Zielobjekte ein Baustein angewendet werden kann. Hilfestellungen dazu finden Sie in Kapitel 2.2 *Zuordnung anhand Schichtenmodell* des IT-Grundschutz-Kompendiums.

Im Ergebnis sind idealerweise **alle Zielobjekte** des Informationsverbundes **angemessen durch IT-Grundschutz-Bausteine abgebildet**. Für Zielobjekte, für die es **keinen hinreichend passenden Baustein** gibt, muss eine Risikoanalyse durchgeführt werden. Die im Rahmen der Risikoanalyse identifizierten Gefährdungen und Sicherheitsanforderungen können in einem benutzerdefinierten Baustein zusammengeführt werden.

Folgende Punkte sollten Sie darüber hinaus bei der Modellierung berücksichtigen:

- Die **prozessorientierten Bausteine** beschreiben Aspekte, die den technischen Aspekten eines Informationsverbundes übergeordnet und üblicherweise einheitlich zu regeln sind. Diese Bausteine sind daher in der Regel einmal pro Informationsverbund anzuwenden. Besonders wichtig sind die Bausteine zum Informationssicherheitsmanagement, der Organisation des IT-Betriebs, der Schulung und Sensibilisierung des Personals sowie der Detektion und Reaktion auf Sicherheitsvorfälle.
- Die **systemorientierten Bausteine** beziehen sich auf bestimmte technische Objekte und sind auf jedes technische System oder jede Gruppe technischer Systeme anzuwenden, die jeweils im Baustein adressiert werden. Dies können bestimmte Anwendungen, IT-Systeme (z. B. Client, Server oder mobile Geräte), Objekte aus dem Bereich der industriellen IT, Netze oder auch Infrastrukturobjekte (Räume, Rechenzentrum, Verkabelung) sein.
- Für eine Reihe technischer Systeme sind **mehrere Bausteine anzuwenden**, um die Gesamtheit der für das System relevanten Sicherheitsanforderungen abzudecken: So gibt es für Clients und Server zum einen betriebssystemunabhängige Bausteine (SYS.2.1 *Allgemeiner Client*, SYS.1.1 *Allgemeiner Server*), in denen die grundsätzlichen Sicherheitsanforderungen dieser Systeme beschrieben werden, zum anderen

aber auch betriebssystemspezifische Bausteine (z. B. SYS.2.2.3 *Client unter Windows 10*, SYS.1.2.2 *Windows Server 2012*), in denen ergänzend die besonderen Anforderungen dargestellt sind, die für dieses Betriebssystem gelten. Für einen Webserver, der mit einer Unix-Variante betrieben wird, sind damit die folgenden drei Bausteine in das IT-Grundschutz-Modell aufzunehmen:

  - SYS.1.1 *Allgemeiner Server*
  - SYS.1.3 *Server unter Unix*
  - APP.3.2 *Webserver*

- **Virtuelle Systeme** sind in gleicher Weise zu modellieren wie physische, es sind also die Funktionen der Systeme, ihr Betriebssystem und die bereitgestellten Anwendungen und Dienste zu berücksichtigen. Wird z. B. ein Unix-Server als Virtualisierungsserver betrieben, so sind auf diesen die drei Bausteine SYS.1.1 *Allgemeiner Server*, SYS.1.3 *Server unter Unix* und SYS.1.5 *Virtualisierung* anzuwenden. Zusätzlich sind für jeden auf diesem physischen Server bereitgestellten virtuellen Server die üblichen Bausteine für Server anzuwenden. Für auf spezieller Hardware beruhende Virtualisierungsserver (sogenannte Bare Metal Server) gibt es keinen passenden IT-Grundschutz-Baustein. Solche IT-Systeme sind daher für eine Risikoanalyse vorzumerken.

Nicht jeder Baustein ist relevant. Zum Beispiel müssen Sie den Baustein CON.7 *Informationssicherheit auf Auslandsreisen* natürlich nur dann anwenden, wenn solche Reisen in Ihrer Einrichtung üblich sind, und ebenso selbstverständlich erübrigt sich die Anwendung spezieller technischer Bausteine wie SYS.2.2.2 *Clients unter Windows 8.1*, wenn dieser Typ von IT-Systemen bei Ihnen nicht eingesetzt wird. Geben Sie in solchen Fällen gleichwohl eine hinreichende Begründung für die Nichtanwendung eines Bausteins an, sie muss aussagekräftig, aber nicht lang sein.

Lerneinheit 5.4: Dokumentation

Ein Beispiel dafür, wie Sie die vorgenommene Modellierung dokumentieren können, finden Sie in folgendem Auszug aus der Modellierung für die RECPLAST GmbH. In der Spalte *Relevanz* vermerken Sie, ob Bausteine für den Informationsverbund von Bedeutung sind oder nicht. Diese Entscheidung können Sie unter *Begründung* näher erläutern. Wenn Sie einen Baustein für nicht relevant einstufen, ist eine hinreichende Begründung unabdingbar.

Baustein	Zielobjekte	Relevanz	Begründung	Ansprechpartner
APP.5.2 *Microsoft Exchange/Outlook*	S004	Ja		IT-Betrieb
INF.1 *Allgemeines Gebäude*	GB1, GB2	Ja		Haustechnik
INF.2 *Rechenzentrum sowie Serverraum*	R002	Ja		IT-Betrieb
INF.4 *IT-Verkabelung*	Informationsverbund	Ja		
INF.7 *Büroarbeitsplatz*	R008 bis R011	Ja		
INF.8 *Häuslicher Arbeitsplatz*	R099	Ja	Die Vertriebsbüros werden wie Home Offices behandelt.	
IND.2.2 *Speicherprogrammierbare Steuerung (SPS)*	I001	Ja		
SYS.1.5 *Virtualisierung*	S007	Ja		IT-Betrieb
SYS.3.1 *Laptops*	L001 bis L008	Ja		IT-Betrieb
OPS.3.1 *Outsourcing für Dienstleister*		Nein	Solche Dienste werden nicht angeboten.	

Tabelle 12: Dokumentation der IT-Grundschutz-Modellierung

Die Angabe von Ansprechpartnern ist bei der Modellierung optional. Sie kann aber dazu dienen, spätere Phasen der Methodik vorzubereiten, insbesondere den IT-Grundschutz-Check. Bei der Auswahl der betreffenden Personen können die Angaben zu Rollen und Verantwortlichkeiten in den Bausteinen hilfreich sein.

Lerneinheit 5.5: Anforderungen anpassen

Wie bereits erwähnt, beschreiben die IT-Grundschutz-Bausteine Anforderungen, die eine Institution umsetzen MUSS oder SOLLTE. In ihnen ist also dargestellt, **was** zu geschehen ist, nicht aber, **wie** dies zu erfolgen hat. Für die Ausarbeitung von Sicherheitskonzepten wie auch für ein Prüfkonzept ist es notwendig, zu den einzelnen Anforderungen geeignete Sicherheitsmaßnahmen zu formulieren. Als Hilfsmittel hierfür gibt es zu den meisten Bausteinen des IT-Grundschutz-Kompendiums **Umsetzungshinweise**.

Maßnahmen, mit denen eine Anforderung erfüllt wird, müssen **angemessen** sein. Im Einzelnen bedeutet dies, dass sie

- **wirksam** sind, also vor den möglichen Gefährdungen schützen und den identifizierten Schutzbedarf abdecken,
- **geeignet** sind, also tatsächlich umsetzbar sind, ohne die Organisationsabläufe unverhältnismäßig zu behindern oder andere Sicherheitsmaßnahmen aushebeln,
- **praktikabel** sind, also leicht verständlich, einfach anzuwenden und wenig fehleranfällig,
- **Akzeptanz** finden, also auch barrierefrei sind und niemanden diskriminieren oder beeinträchtigen,
- **wirtschaftlich** eingeführt und betrieben werden können, der mit ihrer Umsetzung verbundene Aufwand also in einem angemessenen Verhältnis zu den zu schützenden Werten steht.

Bei der Vorgehensweise Standard-Absicherung sollten neben den verpflichtenden Basis-Anforderungen in der Regel immer auch alle Standard-Anforderungen eines Bausteins erfüllt werden. Gleichwohl kann es in Einzelfällen zu Ausnahmen kommen, etwa weil eine Anforderung nicht relevant ist oder ihre Erfüllung mit der Erfüllung anderer Anforderungen im Widerspruch steht. Dies ist auch Basis-Anforderungen möglich. Solche Abweichungen sollten Sie nachvollziehbar begründen. Für zwar relevante, aber mit vertretbarem Aufwand nicht erfüllbare Anforderungen sollten Sie Ersatzlösungen festlegen.

Lerneinheit 5.6: Testfragen

Wenn Sie möchten, können Sie mit den nachfolgenden Fragen Ihre Kenntnisse zur Modellierung gemäß IT-Grundschutz überprüfen. Die Auflösungen zu den Fragen finden Sie im Anhang. Es können mehrere Antwortmöglichkeiten zutreffend sein.

1 **Welche Aufgaben stellen sich Ihnen bei der Modellierung gemäß IT-Grundschutz?**

a Sie bilden den in der Strukturanalyse dokumentierten Informationsverbund mithilfe der IT-Grundschutz-Bausteine ab.

b Sie entwerfen die Sicherheitsarchitektur des betrachteten Informationsverbundes.

c Sie merken Zielobjekte, die nicht geeignet modelliert werden können, für eine Risikoanalyse vor.

d Sie prüfen, welche IT-Grundschutz-Bausteine für den betrachteten Informationsverbund relevant sind.

2 **Welche Informationen sind Bestandteil eines IT-Grundschutz-Bausteins?**

a Angaben zur spezifischen Gefährdungslage

b Beschreibungen zu Standard-Sicherheitsmaßnahmen

c Verweise auf weiterführende Informationen

d Sicherheitsanforderungen zu einem gegebenen Sachverhalt

3 **Welche Aufgaben stellen sich Ihnen, nachdem Sie bei der Modellierung festgelegt haben, welche Bausteine für den Informationsverbund und seine einzelnen Zielobjekte anzuwenden sind?**

a die Festlegung von Maßnahmen, mit denen die Anforderungen erfüllt werden können

b die Prüfung, ob für einzelne Anforderungen, deren Umsetzung im gegebenen Anwendungskontext mit vertretbarem Aufwand nicht möglich ist, Alternativen erforderlich sind

c die Korrektur der Schutzbedarfsfeststellung für Zielobjekte, bei denen die Erfüllung der Anforderungen unrealistisch erscheint

d die Dokumentation der Ergebnisse der Modellierung

4 **Worauf sollten Sie bei der Auswahl und Anpassung der Sicherheitsmaßnahmen auf Basis der Anforderungen achten?**

a auf die Wirtschaftlichkeit der Maßnahmen

b auf die Wirksamkeit der Maßnahmen

c auf den Innovationsgrad der Maßnahmen

d auf die Benutzerfreundlichkeit der Maßnahmen

5 **Welche Aussagen zur Anwendung von Bausteinen auf Server sind korrekt?**

a Der Baustein SYS.1.1 *Allgemeiner Server* ist nur dann anzuwenden, wenn es keinen betriebssystemspezifischen Baustein für einen Server gibt.

b Neben dem Baustein SYS.1.1 *Allgemeiner Server* ist immer auch der zutreffende betriebssystemspezifische Baustein anzuwenden.

c Wenn es spezielle Bausteine für Server-Anwendungen (z. B. Web- oder Datenbankserver) gibt, muss der betriebssystemspezifische Baustein nicht angewendet werden.

d Für Virtualisierungsserver müssen neben dem Baustein sowohl der Baustein SYS.1.1 *Allgemeiner Server* als auch der zutreffende betriebssystemspezifische Baustein angewendet werden.

6 **Auf welche Zielobjekte ist bei der Modellierung der Baustein ISMS.1 *Sicherheitsmanagement* anzuwenden?**

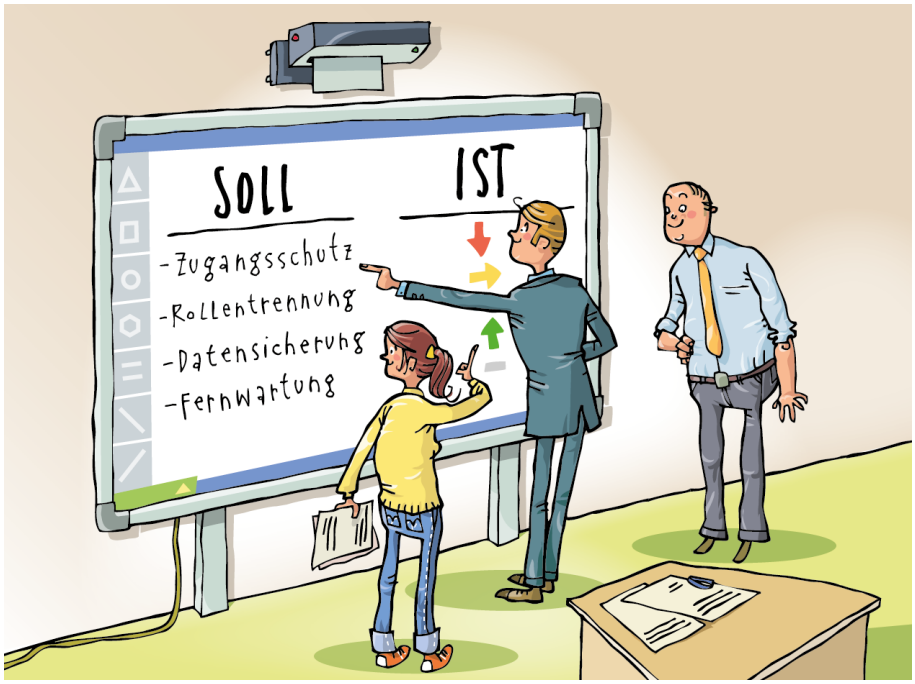
a Er MUSS gesondert auf jeden größeren Standort eines Informationsverbundes angewendet werden.

b Er MUSS einmal angewendet werden, und zwar auf den gesamten Informationsverbund.

c Er ist nur relevant, wenn der Informationsverbund eine gewisse Mindestgröße hat.

d Er MUSS für jedes Teilnetz gesondert angewendet werden, das bei der Strukturanalyse identifiziert wurde.

Lektion 6: IT-Grundschutz-Check



Sind die Informationen und die Informationstechnik in meiner Institution hinreichend geschützt? Was bleibt noch zu tun?

Der IT-Grundschutz-Check ist ein effizientes Instrument zur Beantwortung dieser Fragen. Das Vorgehen ist im Prinzip denkbar einfach: Die bereits umgesetzten Sicherheitsmaßnahmen werden mit den Anforderungen des zuvor mit Hilfe des IT-Grundschutz-Kompendiums entwickelten IT-Grundschutz-Modells verglichen, um das erreichte Sicherheitsniveau zu identifizieren und Verbesserungsmöglichkeiten aufzuzeigen.

Bei einem systematischen Vorgehen greifen Sie dazu auf die **Ergebnisse der vorangegangenen Schritte** zurück:

- Bei der Strukturanalyse haben Sie die vorhandenen Informationen, IT-Systeme, Räume und Kommunikationsverbindungen sowie die von diesen unterstützten Anwendungen erfasst.
- Anschließend haben Sie den Schutzbedarf der Anwendungen, IT-Systeme, Räume und Kommunikationsverbindungen bestimmt und
- bei der Modellierung durch Auswahl und Konkretisierung der anzuwendenden Bausteine einen **Prüfplan** („IT-Grundschutz-Modell“) für den Informationsverbund und dessen Zielobjekte zusammengestellt.

Den Prüfplan wenden Sie beim IT-Grundschutz-Check an, indem Sie für jedes Zielobjekt prüfen, inwieweit die relevanten Anforderungen der IT-Grundschutz-Bausteine durch angemessene technische und organisatorische Maßnahmen erfüllt sind.

In dieser Lektion lernen Sie,

- wie Sie einen IT-Grundschutz-Check vorbereiten,
- worauf Sie bei der Durchführung achten sollten und
- wie Sie die Ergebnisse dokumentieren.

Lerneinheit 6.1: Anforderungen

Der IT-Grundschutz-Check ist ein **Soll-Ist-Vergleich** der Anforderungen an einen Informationsverbund oder eine seiner Komponenten mit den umgesetzten Maßnahmen.

Grundlage des IT-Grundschutz-Checks ist das in der Modellierung aufgrund der vorhandenen Zielobjekte und ihres Schutzbedarfs zusammengestellte **IT-Grundschutz-Modell** des Informationsverbundes. In diesem Modell ist festgelegt, welche Bausteine und damit Anforderungsbündel für die einzelnen Zielobjekte des Informationsverbundes anzuwenden sind.

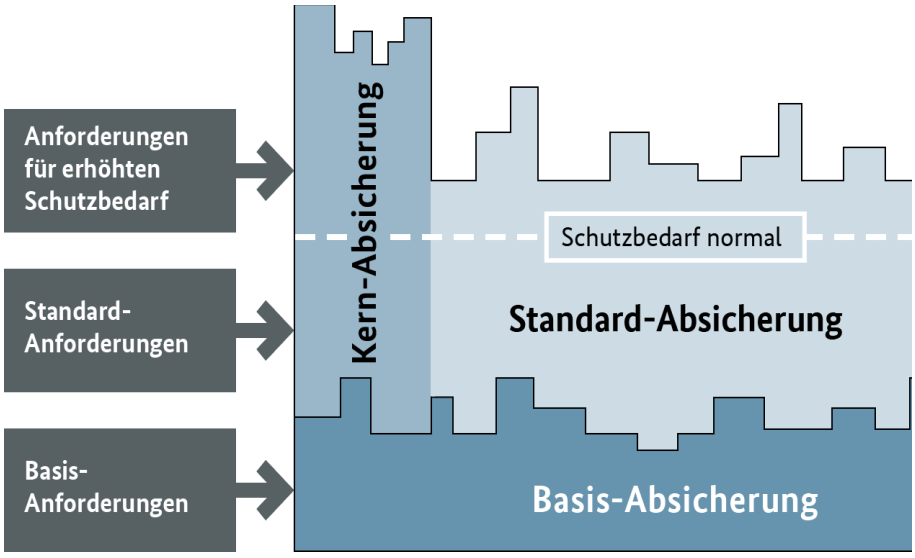


Abbildung 11: Anforderungen der IT-Grundschutz-Bausteine und Varianten der Vorgehensweise

Die Bausteine enthalten drei Arten von Anforderungen: Basis- und Standard-Anforderungen sowie Anforderungen für den erhöhten Schutzbedarf. Welche dieser Anforderungen Sie im IT-Grundschutz-Check berücksichtigen, hängt von der Vorgehensweise der IT-Grundschutz-Methodik ab:

- Bei der Vorgehensweise Basis-Absicherung prüfen Sie lediglich die Erfüllung der Basis-Anforderungen.
- Bei den Vorgehensweisen Standard-Absicherung und Kern-Absicherung berücksichtigen Sie zusätzlich die Standard-Anforderungen.
- Die Anforderungen für den erhöhten Schutzbedarf haben Beispielcharakter und können im Bedarfsfall durch andere Maßnahmen mit starker Schutzwirkung ersetzt oder ergänzt werden. Sie prüfen diese Anforderungen also nur dann, wenn sie als Ergebnis einer Risikoanalyse in das IT-Grundschutz-Modell aufgenommen wurden, also Bestandteil des Sicherheitskonzepts geworden sind. Mehr dazu erfahren Sie in Lektion 7: *Risikoanalyse*.

Lerneinheit 6.2: Vorbereitung und Durchführung

Den Umsetzungsgrad der einzelnen Maßnahmen für das jeweilige Zielobjekt ermitteln und dokumentieren Sie beim IT-Grundschutz-Check in Interviews mit den zuständigen Mitarbeitern und Überprüfungen vor Ort, z. B. durch Begehung von Serverräumen oder Kontrolle von Konfigurationseinstellungen.

Die Qualität der Ergebnisse der Interviews und Begehungen hängt auch von einer guten Vorbereitung und der Beachtung einiger Regeln bei der Durchführung ab:

- Zunächst die wichtigste Regel: Die Informationstechnik ändert sich kontinuierlich, sodass regelmäßig geprüft werden muss, ob die eingeführten Sicherheitsmaßnahmen noch einen angemessenen Schutz bieten. Aus diesem Grund wird das IT-Grundschutz-Kompendium fortlaufend angepasst und um neue Bausteine ergänzt. Benutzen Sie bitte für den IT-Grundschutz-Check die **aktuelle Version des IT-Grundschutz-Kompendiums**, da nur diese eine dem Stand der Technik entsprechende Sicherheit unterstützt.
- Die vorhandenen **Dokumente** über sicherheitsrelevante Abläufe, Regelungen und Sachverhalte enthalten bereits viele Informationen, die Ihnen bei der Ermittlung des Erfüllungsgrads der Anforderungen helfen können. Sichten Sie diese Papiere daher bereits vorab.
- Wählen Sie **geeignete Ansprechpartner** aus. Klären Sie in diesem Zusammenhang auch, ob externe Stellen hinzuzuziehen sind, z. B. Fremdfirmen, an die Teilaufgaben des Informationsverbundes delegiert wurden. Ansprechpartner ergeben sich direkt aus den im Baustein genannten Rollen sowie oft aus dem sachlichen Zusammenhang: So können Mitarbeiter der Personalabteilung oder Benutzerbetreuer gute Ansprechpartner für den Baustein *Personal* sein, während es sich anbietet, für die Systembausteine zu Netzen, IT-Systemen oder Anwendungen die jeweils zuständigen Administratoren und Anwendungsbetreuer zu befragen.
- Vier Augen und Ohren sehen und hören mehr als zwei. Führen Sie die Interviews nach Möglichkeit daher **nicht alleine** durch. Es empfiehlt sich eine Arbeitsteilung: Einer führt das Gespräch und stellt die Fragen, ein anderer protokolliert die Ergebnisse.
- Selbstverständlich sollten Sie bei der Befragung den Inhalt der Anforderungsbeschreibungen sowie die zugehörigen Umsetzungsempfehlungen kennen. Gegebenenfalls können stichpunktartige **Zusammenfassungen** zu einzelnen Anforderungen sowie möglichen Maßnahmen, mit denen sie erfüllt werden können, nützlich sein.
- Zuletzt noch ein ebenso selbstverständlicher Hinweis: Der IT-Grundschutz-Check ist eine Chance, die Informationssicherheit zu verbessern, und kein Verhör. Sorgen Sie daher für ein **entspanntes Klima** und zwar sowohl beim Gespräch als auch bei Begehungen und Überprüfungen vor Ort.

Lerneinheit 6.3: Dokumentation

Den **Erfüllungsgrad** der IT-Grundschutz-Anforderungen für die verschiedenen Zielobjekte des betrachteten Informationsverbundes dokumentieren Sie mit folgenden Kategorien:

- **„entbehrlich“**, wenn die Erfüllung einer Anforderung nicht notwendig ist, da den möglichen Gefährdungen mit mindestens gleichwertigen Ersatzmaßnahmen entgegengewirkt wird (z. B. erübrigen sich Passwortregeln, wenn Chipkarten zusätzlich für die Authentisierung eingesetzt werden) oder wenn die Empfehlungen für den betrachteten Einsatzzweck nicht relevant sind (so ist die Anforderung zur Absicherung von Fernwartung nur dann bedeutsam, wenn tatsächlich auch Systeme von entfernten Standorten aus gewartet werden),
- **„ja“**, wenn die Anforderung durch geeignete Maßnahmen vollständig, wirksam und angemessen erfüllt wird,
- **„teilweise“**, wenn die Anforderung nur teilweise erfüllt wird,
- **„nein“**, wenn die Anforderung nicht erfüllt wird, geeignete Maßnahmen also größtenteils noch nicht umgesetzt sind.

Die folgende Abbildung veranschaulicht den Entscheidungsprozess:

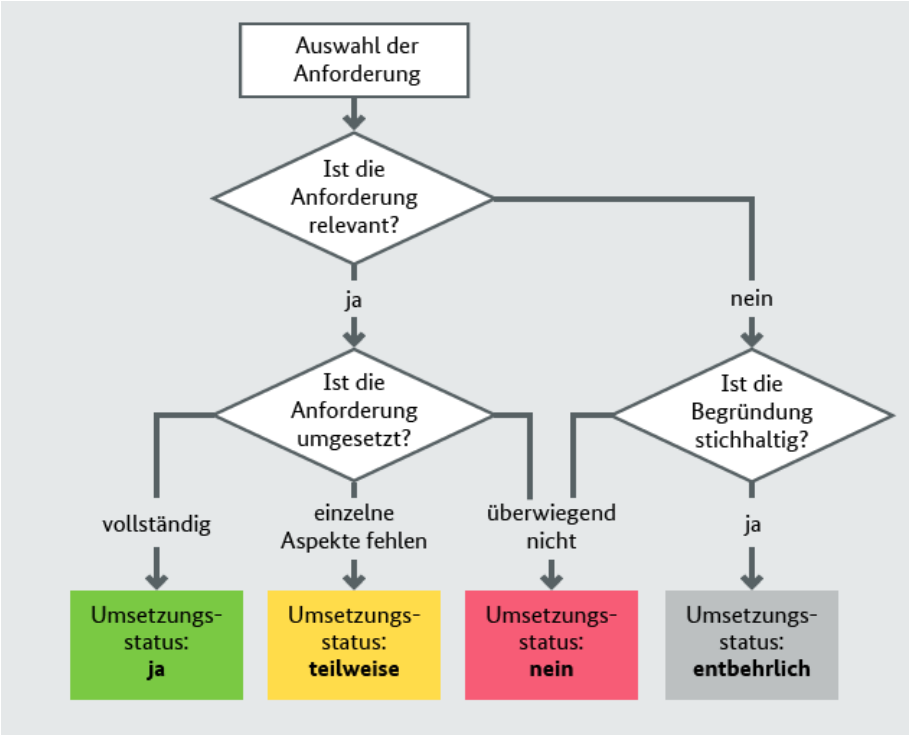


Abbildung 12: Entscheidungsprozess beim IT-Grundschutz-Check

Bitte beachten Sie: Wird die Erfüllung einer Anforderung auf „entbehrlich“ gesetzt, weil Alternativmaßnahmen ergriffen wurden, muss nachgewiesen werden, dass diese Maßnahmen die bestehenden Risiken angemessen minimieren. Identifizieren Sie hierfür über die Kreuzreferenztabelle des jeweiligen Bausteins die zugehörigen elementaren Gefährdungen. Wurden Alternativmaßnahmen ergriffen, begründen Sie, dass diese das von den relevanten Gefährdungen ausgehende Risiko angemessen verringern. Generell gilt, dass Risiken aufgrund der Nichterfüllung von Basis-Anforderungen nicht übernommen werden können. Anforderungen dürfen darüber hinaus nicht quasi automatisch durch pauschale Akzeptanz oder pauschalen Ausschluss einer elementaren Gefährdung als „entbehrlich“ eingestuft werden.

Dokumentation

Damit die Ergebnisse des IT-Grundschutz-Checks später und auch von Dritten nachvollzogen und überprüft werden können, ist es wichtig, dass Sie diese sorgfältig dokumentieren. Vergessen Sie nicht, bei Anforderungen, die Sie als entbehrlich, nur teilweise oder überhaupt nicht erfüllt eingestuft haben, in der Dokumentation Ihre **Begründung** hierfür anzugeben.

Zur Dokumentation gehören natürlich auch **formale Angaben.** Geben Sie bitte bei jedem Interview an,

- auf welches Zielobjekt es sich bezieht,
- wann es stattfand,
- wer es durchgeführt hat und
- wer befragt wurde.

Hilfsmittel

Sie können sich die Dokumentation des IT-Grundschutz-Checks mit Hilfsmitteln vereinfachen:

- So finden Sie unter den Hilfsmitteln zum IT-Grundschutz entsprechende Checklisten für alle Bausteine (zum Download).

- Der IT-Grundschutz-Check wird auch durch eine Reihe an Tools unterstützt, die auf die IT-Grundschutz-Methodik zugeschnitten sind. Bei Verwendung eines solchen Werkzeugs haben Sie den zusätzlichen Vorteil, dass die Daten der Strukturanalyse für die Dokumentation des IT-Grundschutz-Checks konsistent übernommen werden.

Sowohl die Formulare in den Hilfsmitteln zum IT-Grundschutz als auch die Masken in den IT-Grundschutz-Werkzeugen bieten Felder an, in die Sie Angaben zur Umsetzung der als fehlend erkannten Maßnahmen eintragen können (Umsetzungsfristen, Verantwortliche, voraussichtliche Kosten). Diese Angaben sind für die Realisierungsplanung wichtig. Beim IT-Grundschutz-Check ist es noch nicht erforderlich, diese Felder auszufüllen.

Lerneinheit 6.4: Entscheidungskriterien

Als Beispiel für den Entscheidungsprozess zur Bewertung des Status einer Anforderung sollen nachfolgend einige Anforderungen aus dem Prozess-Baustein ISMS.1 Sicherheitsmanagement und dem System-Baustein SYS.2.1 Allgemeiner Client dienen.

Bewertung als „vollständig umgesetzt“

Der Baustein ISMS.1 enthält unter anderem die Basis-Anforderung ISMS.A1: *Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene* mit insgesamt sechs durch das Verb MUSS als verpflichtend gekennzeichneten Teilanforderungen:

„Die Leitungsebene MUSS die Gesamtverantwortung für Informationssicherheit in der Institution übernehmen, sodass dies für alle Beteiligten deutlich erkennbar ist. Die Leitungsebene der Institution MUSS den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Leitungsebene MUSS Informationssicherheit vorleben.
Die Behörden- bzw. Unternehmensleitung MUSS die Zuständigkeiten für Informationssicherheit festlegen und die zuständigen Mitarbeiter mit den erforderlichen Kompetenzen und Ressourcen ausstatten. Die Leitungsebene MUSS sich regelmäßig über den Status der Informationssicherheit informieren lassen, insbesondere MUSS sie sich über mögliche Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen informieren lassen.“

Bewertung als „entbehrlich“

Unter Umständen, etwa bei unzureichendem Know-how innerhalb einer Institution, kann es sich für eine Institution anbieten, Sicherheitsaufgaben an einen externen Informationssicherheitsbeauftragten zu delegieren. Dies enthebt sie allerdings nicht ihrer grundsätzlichen Verantwortung für Informationssicherheit. Rechte und Pflichten des externen ISB sind daher vorab festzulegen und vertraglich zu fixieren. In ISMS.1.A5 *Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten* wird diese Basis-Anforderung näher spezifiziert. Wird die Rolle des ISB durch einen eigenen Mitarbeiter wahrgenommen, ist die Erfüllung dieser Anforderung selbstverständlich entbehrlich.

Bewertung als „teilweise erfüllt“

Der Baustein SYS.2.1 Allgemeiner Client, dessen Anwendung für jede Gruppe von Clients in einem Informationsverbund verbindlich ist, enthält unter anderem die Basis-Anforderung SYS.2.1.A2: *Rollentrennung* mit Vorgaben für die Beschränkung der Benutzerrechte. Sie lautet wie folgt:

„Der Client MUSS so eingerichtet werden, dass normale Tätigkeiten nicht mit Administrationsrechten erfolgen. Nur Administratoren DÜRFEN Administrationsrechte erhalten. Es DÜRFEN nur Administratoren die Systemkonfiguration ändern, Anwendungen installieren bzw. entfernen oder Systemdateien modifizieren bzw. löschen können. Benutzer DÜRFEN ausschließlich lesenden Zugriff auf Systemdateien haben.
Ablauf, Rahmenbedingungen und Anforderungen an administrative Aufgaben sowie die Aufgabentrennungen zwischen den verschiedenen Rollen der Benutzer des IT-Systems SOLLTEN in einem Benutzer- und Administrationskonzept festgeschrieben werden.“

Wird bei der Überprüfung der Umsetzung dieser Anforderung für eine gegebene Gruppe von Clients festgestellt, dass die IT-Systeme so eingerichtet sind, dass übliche Benutzeraktivitäten nur mit entsprechend eingeschränkten Rechten ausgeübt werden und Systemzugriffe Administratoren vorbehalten sind, so ist zumindest ein Teil der Anforderung erfüllt. Das Fehlen eines expliziten Benutzer- und Administrationskonzepts, ohne dass hierfür ein stichhaltiger Grund vorliegt, führt jedoch zu der Einstufung, dass diese Anforderung nur teilweise erfüllt ist.

Bewertung als „nicht erfüllt“

Die Anforderung SYS.2.1.A2: *Rollentrennung* des Bausteins SYS.2.1 Allgemeiner Client wäre hingegen nicht erfüllt, wenn zwar ein solches Konzept vorliegt, dieses aber die Vorgaben dieser Basis-Anforderung nur bedingt widerspiegelt, und insbesondere die geprüften Clients deutliche Abweichungen von den verpflichtenden Anforderungen aufweisen.

Es kann Gründe dafür geben, dass einzelne IT-Systeme auch von Benutzern, die ansonsten keine derartigen Berechtigungen haben, mit Administrationsrechten benutzt werden können, beispielsweise weil eine benötigte Spezialsoftware ansonsten nicht funktionieren würde. In diesem Fall müsste das aus der Nichterfüllung dieser Basis-Anforderung resultierende Risiko mit zusätzlichen Maßnahmen begrenzt werden.

Lerneinheit 6.5: Beispiel

Als Beispiel für die Dokumentation des IT-Grundschutz-Checks zeigt der folgende Auszug dieser Überprüfung für die RECPLAST GmbH die Ergebnisse für drei Basis-Anforderungen und eine Standard-Anforderung des Bausteins ISMS.1 *Sicherheitsmanagement*. Dieser Baustein ist für den gesamten Informationsverbund anzuwenden, im Beispiel also für das gesamte Unternehmen.

Eine ausführliche Dokumentation des IT-Grundschutz-Checks zu diesem Baustein und zu weiteren ausgewählten Bausteinen finden Sie in Kapitel 6 des Beispieldokuments.

Anforderung	Verantwortung	Status	Umsetzung
ISMS.1.A1: Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	Institutionsleitung	erfüllt	Die Geschäftsführung hat die Erstellung der Leitlinie initiiert. Die Leitlinie wurde von der Geschäftsführung unterzeichnet. Die Geschäftsführung hat die gesamte Verantwortung für das Thema Informationssicherheit übernommen und delegiert an den ISB die Umsetzung der geforderten Maßnahmen. Einmal monatlich erhält die Geschäftsführung einen Management-Report, kontrolliert den Umsetzungsstand der Maßnahmen und initiiert bei Bedarf weitere Maßnahmen und bewilligt das entsprechende Budget.
ISMS.1.A5 Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten	Institutionsleitung	entbehrlich	Der Informationssicherheitsbeauftragte ist ein Mitarbeiter der RECPLAST GmbH.
ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen	ISB	teilweise	Alle Mitarbeiter, die Maßnahmen im Sinne der Informationssicherheit umsetzen, sind verpflichtet, diese zu dokumentieren und dem ISB per E-Mail zuzusenden. Eine Auswertung und ausreichende Dokumentation der umgesetzten Maßnahmen gibt es nicht. Umsetzungszeitpunkt für ausführliche Dokumentation: 30.04.
ISMS.1.A11 Aufrechterhaltung der Informationssicherheit	ISB	erfüllt	Alle Dokumente und Prozesse werden einmal jährlich einem internen Audit unterzogen. Der ISB hat dafür die entsprechende fachliche Weisungsbefugnis für die Mitarbeiter, in deren Verantwortungsbereich einzelne Dokumente und Prozesse fallen.

Tabelle 13: Beispiel für die Dokumentation des IT-Grundschutz-Checks

Lerneinheit 6.6: Testfragen

Wenn Sie möchten, können Sie mit den nachfolgenden Fragen Ihre Kenntnisse zum IT-Grundschutz-Check überprüfen. Die Auflösungen zu den Fragen finden Sie im Anhang. Es können mehrere Antwortmöglichkeiten zutreffend sein.

1 **Welche Aussagen zum IT-Grundschutz-Check sind zutreffend?**

a Ein IT-Grundschutz-Check ermöglicht, Defizite bei der Erfüllung von Sicherheitsanforderungen zu ermitteln.

b Bei einem IT-Grundschutz-Check wird lediglich die Erfüllung der Basis-Anforderungen geprüft.

c Ein IT-Grundschutz-Check dient dazu, Sicherheitsprobleme zu identifizieren, die in einer Risikoanalyse genauer untersucht werden müssen.

d Ein IT-Grundschutz-Check ist ein Soll-Ist-Vergleich zwischen Sicherheitsanforderungen und tatsächlich umgesetzten Sicherheitsmaßnahmen.

2 **Welche Vorarbeiten erfordert der IT-Grundschutz-Check?**

a die Festlegung eines Zeitplans

b die Auswahl von geeigneten Gesprächspartnern

c einen Penetrationstest, um Schwachstellen zu identifizieren, die mit den ausgewählten Gesprächspartnern erörtert werden

d die Zusammenstellung und Lektüre der vorhandenen Dokumente zur Informationssicherheit in dem betrachteten Informationsverbund

3 **Welche Verfahren verwenden Sie, um in einem IT-Grundschutz-Check zu prüfen, wie gut eine Gruppe von Clients geschützt ist?**

a Sie führen Interviews mit den zuständigen Systembetreuern.

b Sie versuchen in einem Penetrationstest, Schwachstellen dieser IT-Systeme zu ermitteln, und beziehen dabei sämtliche zur Gruppe gehörenden Clients ein.

c Sie untersuchen stichprobenartig vor Ort, wie die Clients konfiguriert sind.

d Sie lesen die vorhandene Dokumentation zur Konfiguration der Clients.

4 **Wann bewerten Sie beim IT-Grundschutz-Check eine Anforderung eines IT-Grundschutz-Bausteins als erfüllt?**

a wenn zu der Anforderung geeignete Maßnahmen vollständig, wirksam und angemessen umgesetzt sind

b wenn der Gesprächspartner Ihnen glaubhaft versichert hat, dass es bislang zu keinen Sicherheitsproblemen auf dem betreffenden IT-System gekommen ist

c wenn es eine umfangreiche Dokumentation zu den Schutzvorkehrungen für das betreffende IT-System gibt

d wenn sowohl im Interview mit einem für das IT-System Zuständigen als auch bei einer stichprobenartigen Überprüfung keine Sicherheitsmängel festgestellt wurden

5 **Wie verfahren Sie beim ersten IT-Grundschutz-Check, also vor der Durchführung von Risikoanalysen, mit Anforderungen für den erhöhten Schutzbedarf?**

a Sie stufen diese Anforderungen grundsätzlich als entbehrlich ein und verzichten auch dann darauf, diese zu überprüfen, wenn sie in Ihrer Einrichtung umgesetzt sind.

b Sie streichen die Anforderungen aus Ihrem Sollkonzept.

c Sie betrachten Anforderungen für den hohen und sehr hohen Schutzbedarf erst nach Abschluss der Risikoanalyse.

d Sie betrachten im IT-Grundschutz-Check grundsätzlich alle in den IT-Grundschutz-Bausteinen genannten Anforderungen, folglich auch diejenigen für den erhöhten Schutzbedarf.

6 **Sie stellen fest, dass eine Standard-Anforderung für ein IT-System nicht umgesetzt ist, das nur noch kurze Zeit in Betrieb ist. Wie behandeln Sie diese Anforderung beim IT-Grundschutz-Check?**

a Sie streichen die Anforderung aus dem IT-Grundschutz-Modell.

b Sie dokumentieren diese als entbehrlich, da ihre Umsetzung nicht mehr wirtschaftlich ist.

c Sie dokumentieren diese als nicht erfüllt, und merken gegebenenfalls an, dass geprüft werden muss, ob Maßnahmen zur Behebung dieses Defizits angesichts der kurzen Einsatzzeit des IT-Systems noch angemessen sind.

d Sie dokumentieren diese als nicht erfüllt und merken an, dass geprüft werden muss, ob die daraus resultierenden Risiken in der Restlaufzeit des IT-Systems noch tragbar sind.

Lektion 7: Risikoanalyse

Die Basis- und Standard-Anforderungen der IT-Grundschutz-Bausteine wurden so festgelegt, dass dazu passende Maßnahmen für **normalen Schutzbedarf** und für **typische Informationsverbünde** und **Anwendungsszenarien** einen angemessenen und ausreichenden Schutz bieten. Hierfür wurde vorab geprüft, welchen Gefährdungen die in den Bausteinen behandelten Sachverhalte üblicherweise ausgesetzt sind und wie den daraus resultierenden Risiken zweckmäßig begegnet werden kann. Als Anwender des IT-Grundschutzes benötigen Sie daher in der Regel für den weitaus größten Teil eines Informationsverbundes keine aufwändigen Untersuchungen mehr zur Festlegung erforderlicher Sicherheitsmaßnahmen.

Ein **zusätzlicher Analysebedarf** besteht lediglich in folgenden drei Fällen:

- Ein Zielobjekt hat einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit.
- Es gibt für ein Zielobjekt keinen hinreichend passenden Baustein im IT-Grundschutz-Kompendium.
- Es gibt zwar einen geeigneten Baustein, die Einsatzumgebung des Zielobjekts ist allerdings für den IT-Grundschutz untypisch.

Das grundlegende Verfahren zur Untersuchung von Sicherheitsgefährdungen und deren Auswirkungen ist eine **Risikoanalyse**. Der BSI-Standard 200-3: *Risikomanagement* bietet hierfür eine effiziente Methodik.

In dieser Lektion lernen Sie detailliert das **Vorgehen bei einer Risikoanalyse gemäß BSI-Standard 200-3** kennen. Im Einzelnen erfahren Sie,

- welche Voraussetzungen für die Durchführung von Risikoanalysen in einer Institution gegeben sein sollten,
- wie Sie mit Hilfe der Liste elementarer Gefährdungen des IT-Grundschutz-Kompendiums eine Gefährdungsübersicht für ein gegebenes Zielobjekt zusammenstellen,
- wie Sie die aus den Gefährdungen resultierenden Risiken ermitteln und bewerten,
- wie Sie zweckmäßige Entscheidungen zur Behandlung von Risiken treffen sowie
- wie Sie die Ergebnisse der Risikoanalyse in den Sicherheitsprozess zurückführen.

Lerneinheit 7.1: Organisatorische Rahmenbedingungen

Bevor Sie mit der Durchführung von Risikoanalysen beginnen, sollte die Leitung Ihrer Institution grundlegende Aspekte hierfür in einer **Richtlinie zum Umgang mit Risiken** festlegen:

- Unter welchen Voraussetzungen ist eine Risikoanalyse erforderlich?
- Mit welchem Verfahren werden Risiken identifiziert, eingeschätzt, bewertet und behandelt und wie ist dieses Verfahren an die Gegebenheiten der Institution angepasst und in den Sicherheitsprozess integriert?
- Welche Organisationseinheiten sind für die verschiedenen Teilaufgaben des Risikomanagements zuständig?
- Wie sind die Berichtspflichten geregelt?
- Welche Kriterien müssen erfüllt sein, damit Risiken akzeptiert werden?
- In welchen zeitlichen Intervallen und bei welchen Ereignissen müssen Risikoanalysen aktualisiert werden?

Diese Richtlinie und die zugehörigen organisatorischen Umsetzungen sollten regelmäßig auf ihre Aktualität und Angemessenheit geprüft werden.

Beispiel: Risikomanagement bei der RECPLAST GmbH

In der RECPLAST GmbH wurde beschlossen, das Risikomanagement gemäß IT-Grundschutz auszurichten und eine Sicherheitskonzeption gemäß Standard-Absicherung zu entwickeln. Für Objekte mit normalem Schutzbedarf erfolgt die Risikobehandlung mithilfe der Basis- und Standard-Anforderungen des IT-Grundschutz-Kompendiums. Als Methode für unter Umständen erforderliche Risikoanalysen wurde der BSI-Standard 200-3 festgelegt. In einer Richtlinie zur Behandlung von Risiken wurde ferner formuliert, dass Risiken, die aus der Nichterfüllung von Basis-Anforderungen folgen, nicht akzeptiert werden können. Risiken sollen darüber hinaus unter Betrachtung der Kosten möglicher Maßnahmen und ihres Beitrags zur Risikominimierung behandelt werden.

Die Verantwortlichkeit für die Durchführung der Risikoanalyse obliegt dem ISB, der hierfür spezialisierte Teams bildet. Deren Zusammensetzung hängt vom jeweiligen Sachverhalt ab: Anwendungsverantwortliche wirken bei der Bewertung möglicher Schadensfolgen mit; erfordert die Bewertung der Risiken einen hohen technischen Sachverstand, werden kompetente Mitarbeiter der IT-Abteilung beteiligt.

Die durchgeführten Risikoanalysen werden dokumentiert, die Ergebnisse und die Vorschläge zur Risikobehandlung der Geschäftsführung berichtet und mit ihr abgestimmt. Aktualität und Angemessenheit der Risikoanalysen sollen jährlich geprüft werden.

Wie sieht es in Ihrem Unternehmen oder Ihrer Behörde aus: Gibt es einen festgelegten Prozess zur Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken? Werden bei Ihnen Risikoanalysen durchgeführt und falls ja, mit welchem Verfahren? Wer ist für die Durchführung der Analysen verantwortlich? Wer erfährt die Ergebnisse und wie werden Konsequenzen gezogen?

Lerneinheit 7.2: Zielobjekte zusammenstellen

Voraussetzung für die Durchführung von Risikoanalysen im Rahmen der Standard-Absicherung ist, dass bei der Strukturanalyse die Zielobjekte des Informationsverbundes zusammengestellt sind, deren Schutzbedarf festgestellt ist und ihnen bei der Modellierung soweit möglich passende IT-Grundschutz-Bausteine zugeordnet wurden.

Eingangs der Lektion wurde dargestellt, dass eine Risikoanalyse für solche Zielobjekte erfolgen sollte,

- die einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben **oder**
- für die es keinen passenden IT-Grundschutz-Baustein gibt **oder**
- die in Einsatzszenarien betrieben werden, die für den IT-Grundschutz untypisch sind.

Bei einer g**roßen Zahl an Zielobjekten**, die eines dieser Kriterien erfüllen, sollten Sie eine **geeignete Priorisierung** vornehmen. Bei der Vorgehensweise Standard-Absicherung bietet es sich an, zunächst übergeordnete Zielobjekte zu betrachten, etwa den gesamten Informationsverbund, bestimmte Teile des Informationsverbundes oder wichtige Geschäftsprozesse. Bei der Kern-Absicherung sollten Sie vorrangig diejenigen Zielobjekte mit dem höchsten Schutzbedarf untersuchen.

Beispiel

Bei der RECPLAST GmbH wurde aufgrund der Schutzbedarfsfeststellung und der Modellierung eine Reihe von Zielobjekten ermittelt, für die eine Risikoanalyse durchzuführen ist. Dazu gehören unter anderem die folgenden Komponenten:

- die Anwendung A002 *Lotus Notes*, die einen hohen Bedarf an Vertraulichkeit und einen sehr hohen Bedarf an Verfügbarkeit hat,
- die Netzkopplungselemente N001 *Router Internet-Anbindung* und N002 *Firewall Internet-Eingang*, beide wegen der Vertraulichkeit der über sie übertragenen Daten,
- der Virtualisierungsserver S007, der in allen drei Grundwerten aufgrund der auf ihm betriebenen virtuellen Systeme einen hohen Schutzbedarf hat,
- die Alarmanlagen S200 an beiden Standorten in Bonn, deren korrektes Funktionieren als sehr wichtig eingestuft und deren Schutzbedarf bezüglich Integrität und Verfügbarkeit folglich mit „sehr hoch“ bewertet wurde.

Nachfolgend werden die einzelnen Schritte der Risikoanalyse am Beispiel des über beide Standorte hinweg redundant ausgelegten Virtualisierungsservers S007 veranschaulicht.

Lerneinheit 7.3: Die elementaren Gefährdungen

Als wesentliches Hilfsmittel für die Durchführung von Risikoanalysen enthält das IT-Grundschutz-Kompendium eine Liste von insgesamt **47 elementaren Gefährdungen**, die kompatibel mit vergleichbaren Zusammenstellungen in internationalen Standards und Normen ist.

Die einzelnen Gefährdungen werden durch eine eindeutige Kennung und Bezeichnung voneinander unterschieden. Zu jeder Gefährdung gibt es eine kurze produkt- und weitestgehend technikneutral formulierte Beschreibung und eine Angabe dazu, welche der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität unmittelbar von ihr betroffen sein können.

Die nachfolgende Auswahl illustriert das breite Spektrum der berücksichtigten Bedrohungen und Schadensszenarien: Sowohl höhere Gewalt und technisches Versagen als auch organisatorische Mängel und vorsätzliches oder fahrlässiges menschliches Fehlverhalten werden einbezogen. Die jeweils betroffenen Grundwerte werden durch ein „C“ (Confidentiality, Vertraulichkeit), ein „I“ (Integrity, Integrität) und ein „A“ (Availability, Verfügbarkeit) gekennzeichnet.

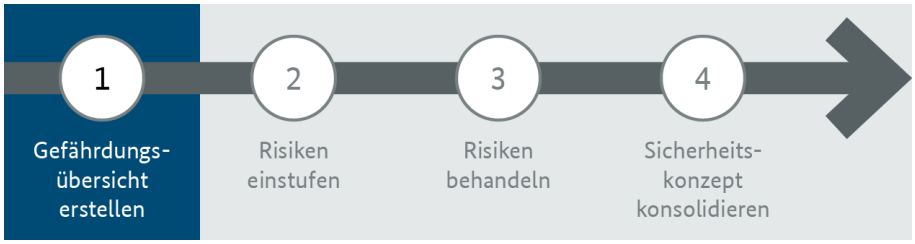
Gefährdung	Betroffene Grundwerte
G 0.1 *Feuer*	A
G 0.5 *Naturkatastrophen*	A
G 0.10 *Ausfall oder Störung von Versorgungsnetzen*	A
G 0.15 *Abhören*	C
G 0.18 *Fehlplanung oder fehlende Anpassung*	C, I, A
G 0.23 *Unbefugtes Eindringen in IT-Systeme*	C, I
G 0.26 *Fehlfunktion von Geräten oder Systemen*	C, I, A
G 0.31 *Fehlerhafte Nutzung oder Administration von Geräten oder Systemen*	C, I, A
G 0.33 *Personalausfall*	A
G 0.39 *Schadprogramme*	C, I, A
G 0.46 *Integritätsverlust schützenswerter Informationen*	I

Tabelle 14: Beispiele für elementare Gefährdungen

Die in den IT-Grundschutz-Bausteinen formulierten Anforderungen wurden unter Berücksichtigung der jeweils relevanten elementaren Gefährdungen zusammengestellt. Aus diesem Grund finden Sie am Ende eines jeden Bausteins auch eine Matrix der Beziehungen zwischen Anforderungen und elementaren Gefährdungen.

Wie Sie die elementaren Gefährdungen für ihre eigenen Risikoanalyse verwenden, erfahren Sie in der nächsten Lerneinheit.

Lerneinheit 7.4: Gefährdungsübersicht anlegen



Der erste Schritt einer Risikoanalyse ist es, die Risiken zu identifizieren, denen ein Objekt oder ein Sachverhalt ausgesetzt ist. Hierfür ist zunächst zu beschreiben, welchen Gefährdungen das Objekt oder der Sachverhalt unterliegt.

Gemäß BSI-Standard 200-3 verwenden Sie hierfür die **elementaren Gefährdungen als Ausgangspunkt**. Hierbei sind zwei Fälle zu unterscheiden:

- **Es gibt für ein Zielobjekt (noch) keinen passenden Baustein.**
  In diesem Fall ziehen Sie die vollständige Liste der elementaren Gefährdungen hinzu und prüfen, welche der Gefährdungen für das betreffende Zielobjekt relevant sind.
- **Es gibt einen passenden Baustein für das Zielobjekt.**
  In diesem Fall wurde bereits vorab eine Risikoanalyse für den betreffenden Zielobjekt-Typ durchgeführt und in den Bausteinen tabellarisch dargestellt, welche elementaren Gefährdungen relevant sind und mit welchen Anforderungen diesen Gefährdungen jeweils begegnet wird. Es ist Ihre Aufgabe, zu prüfen, ob weitere elementare Gefährdungen einen nennenswerten Schaden hervorrufen können.

Die Relevanz einer Gefährdung bestimmen Sie mit Hilfe der möglichen Einwirkung einer Gefährdung. Dabei ist zu unterscheiden, ob eine Gefährdung unmittelbar (direkt) oder nur indirekt über

andere, allgemeinere Gefährdungen auf das betrachtete Objekt einwirkt. Nur Gefährdungen mit direkter Relevanz nehmen Sie in die Gefährdungsübersicht auf.

Beispiel

Für den Virtualisierungsserver S007 sind gemäß der Modellierung die folgenden drei IT-Grundschutz-Bausteine relevant: SYS.1.1 *Allgemeiner Server*, SYS.1.3 *Server unter Unix* und SYS.1.5 *Virtualisierung*. Aus den in diesen Bausteinen referenzierten elementaren Gefährdungen lässt sich die folgende auszugsweise wiedergegebene Übersicht relevanter Gefährdungen zusammenstellen:

- G 0.14 *Ausspähen von Informationen (Spionage)*
- G 0.15 *Abhören*
- G 0.18 *Fehlplanung oder fehlende Anpassung*
- G 0.19 *Offenlegung schützenswerter Informationen*
- G 0.21 *Manipulation von Hard- oder Software*
- G 0.22 *Manipulation von Informationen*
- G 0.23 *Unbefugtes Eindringen in IT-Systeme*
- G 0.25 *Ausfall von Geräten oder Systemen*
- G 0.26 *Fehlfunktion von Geräten oder Systemen*
- G 0.28 *Software-Schwachstellen oder -Fehler*
- G 0.30 *Unberechtigte Nutzung oder Administration von Geräten und Systemen*
- G 0.31 *Fehlerhafte Nutzung oder Administration von Geräten und Systemen*
- G 0.32 *Missbrauch von Berechtigungen*
- G 0.40 *Verhinderung von Diensten (Denial of Service)*
- G 0.43 *Einspielen von Nachrichten*
- G 0.45 *Datenverlust*
- G 0.46 *Integritätsverlust schützenswerter Informationen*

Lerneinheit 7.5: Gefährdungsübersicht ergänzen

Auch wenn die Zusammenstellung elementarer Gefährdungen vielfältige Bedrohungen berücksichtigt, denen Informationen und Informationstechnik ausgesetzt sind, so kann dennoch nicht ausgeschlossen werden, dass weitere Gefährdungen zu betrachten sind. Dies gilt insbesondere dann, wenn es für ein Zielobjekt in untypischen Einsatzszenarien betrieben wird.

Im Anschluss an den ersten Teilschritt prüfen Sie daher, ob neben den relevanten elementaren Gefährdungen weitere Gefährdungen zu untersuchen sind.

Wie finden Sie zusätzliche Gefährdungen?

Ein bewährtes Mittel, mögliche Gefährdungen zu ermitteln, ist ein von dem ISB oder einem anderen Sicherheitsexperten moderierter Workshop, an dem diejenigen Mitarbeiterinnen und Mitarbeiter zu beteiligen sind, die in irgendeiner Weise mit der betrachteten Komponente in Verbindung stehen (zum Beispiel Administratoren, Anwendungsbetreuer, Benutzer). Hinweise auf Gefährdungen können auch weitere Quellen liefern, etwa Herstellerdokumentationen oder Publikationen im Internet.

Die elementaren Gefährdungen wurden so ausgewählt, dass sie eine kompakte, gleichzeitig angemessene und in typischen Szenarien vollständige Grundlage für Risikoanalysen bieten. Daher sollte der Fokus bei der Ermittlung zusätzlicher Gefährdungen nicht darauf liegen, weitere elementare Gefährdungen zu identifizieren. Es kann aber sinnvoll sein, spezifische Aspekte einer elementaren Gefährdung zu betrachten, da dies es erleichtern kann, spezifische Maßnahmen zu identifizieren.

Worauf sollten Sie achten?
Unter Umständen können in dem Workshop zahlreiche und vielfältige Gefährdungen diskutiert werden. Um die sich anschließende Bewertung der Gefährdungen nicht unnötig zu erschweren, sollten Sie

- sich auf diejenigen Gefährdungen konzentrieren, die Grundwerte beeinträchtigen, in denen das betrachtete Zielobjekt den Schutzbedarf sehr hoch oder hoch hat,
- alle Gefahrenbereiche berücksichtigen, nach denen die Gefährdungskataloge gruppiert sind, also höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Angriffe von Außen- und Innentätern, und die Gefährdungen entsprechend gruppieren,
- auf die Relevanz der Vorschläge achten, also nur solche Gefährdungen weiter verfolgen, die zu nennenswerten Schäden führen können und im behandelten Zusammenhang realistisch sind,
- bei jedem vorgebrachten Vorschlag prüfen, ob die betreffende Gefährdung nicht bereits durch eine vorhandene Gefährdung abgedeckt wird, sowie
- die verbleibenden Vorschläge verallgemeinern, um die Anzahl der in den künftigen Schritten zu berücksichtigenden Gefährdungen zu verringern.

Die Ermittlung der Gefährdungen verlangt ebenso wie die weiteren Schritte bei der Risikoanalyse vertiefte Fachkenntnisse. Öffentlich zugängliche Informationen, wie Zeitschriftenartikel oder Quellen im Internet, können Ihnen in vielen Fällen wertvolle Hinweise geben. Oft empfiehlt es sich auch, auf das Know-how externer Experten zurückzugreifen.

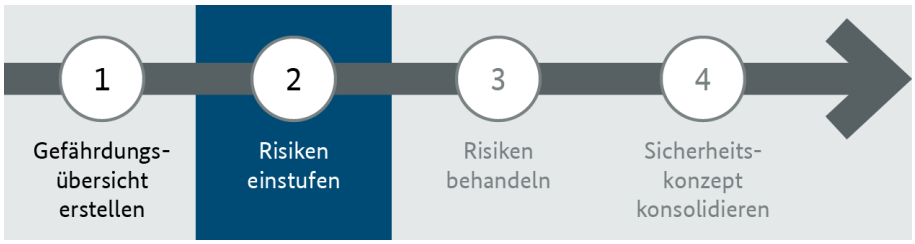
Beispiel

Die Diskussion weiterer zu betrachtender Gefährdungen bei der RECPLAST GmbH ergibt, dass für den gesamten Informationsverbund mögliche Manipulationen durch Familienangehörige und Besucher aufgrund der häufigen Anwesenheit dieser Personengruppen als zusätzliche Gefährdung zu betrachten sind. Diese wird wie folgt beschrieben.

> G z.1 *Manipulation durch Familienangehörige und Besucher*.
> Familienangehörige und Besucher haben zeitweise Zutritt zu bestimmten Räumlichkeiten des Unternehmens. Es besteht die Gefahr, dass diese Personen dies als Gelegenheit nutzen, unerlaubte Veränderungen an Hardware, Software oder Informationen vorzunehmen. Diese zusätzliche Gefährdung konkretisiert die elementaren Gefährdungen G 0.21 *Manipulation von Hard- oder Software* und G 0.22 *Manipulation von Informationen*.

Daneben wurden weitere zusätzliche Gefährdungen ermittelt, etwa die Beschädigung von IT im Fertigungsbereich aufgrund der dort bestehenden besonderen Umgebungsbedingungen (z. B. Staub, Erschütterungen). Diese Gefährdung ist bei Risikoanalysen von ICS-Komponenten mit hohem oder sehr hohem Schutzbedarf zu berücksichtigen.

Lerneinheit 7.6: Häufigkeit und Auswirkungen einschätzen



Die Höhe eines Risikos ergibt sich aus der **Häufigkeit** einer Gefährdung und der drohenden **Schadenshöhe**. Ein Risiko ist umso größer, je häufiger eine Gefährdung ist, umgekehrt sinkt es, je geringer der mögliche Schaden ist.

Grundsätzlich können beide Größen sowohl **quantitativ**, also mit genauen Zahlenwerten, als auch **qualitativ**, also mit Hilfe von Kategorien zur Beschreibung der Größenordnung, bestimmt werden. Erfahrungsgemäß sind jedoch hinreichend verlässliche quantitative Angaben, insbesondere zur Häufigkeit von Schadensereignissen im Bereich der Informationssicherheit, so gut wie nicht vorhanden und auch dort, wo es verlässliche Statistiken gibt, sind daraus abgeleitete exakte Prognosen auf zukünftige Ereignisse problematisch, wenn nicht gar unmöglich. Daher empfiehlt sich ähnlich wie bei der Schutzbedarfsfeststellung ein **qualitativer Ansatz mit einer begrenzten Anzahl an Kategorien**.

Die **Anzahl der Kategorien**, mit denen Sie Eintrittshäufigkeit und Schadenshöhe beschreiben, und deren Definition sollten auf die konkreten Gegebenheiten Ihrer Institution angepasst sein. Im Allgemeinen genügen maximal fünf Stufen zur Abgrenzung von Häufigkeiten und Auswirkungen. Wenn bei Ihnen ein übergeordnetes Risikomanagement bereits eingeführt ist, empfiehlt es sich zudem, Informationssicherheitsrisiken in Übereinstimmung mit den dort verwendeten Systemen zur Bewertung und Klassifikation von Risiken zu verwenden.

Nachfolgend als Beispiel ein Vorschlag aus dem BSI-Standard 200-3 für ein mögliches vierstufiges Klassifikationsschema zur Bewertung von Eintrittshäufigkeiten.

Eintrittshäufigkeit	Beschreibung
selten	Das Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre auftreten.
mittel	Das Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Das Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
Sehr häufig	Das Ereignis tritt mehrmals im Monat ein.

Tabelle 15: Beispiel für die Klassifikation von Häufigkeiten

Auch für die Klassifikation möglicher Schadensauswirkungen enthält der BSI-Standard als Beispiel ein vierstufiges Klassifikationsschema.

Schadenshöhe	Schadensauswirkungen
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß annehmen.

Tabelle 16: Beispiel für die Klassifikation von Schadensauswirkungen

Berücksichtigen Sie bei der Definition der Kategorien zur Bewertung der Auswirkungen einer Gefährdung auch die bei Ihnen vorgenommene Definition der Schutzbedarfskategorien. Beide Systeme sollten in einer Institution zueinander passend definiert werden.

Lerneinheit 7.7: Risiken bewerten

Nachdem Sie die Eintrittshäufigkeiten und Schadensauswirkungen einer Gefährdung eingeschätzt haben, können Sie das aus beiden Faktoren resultierende Risiko bewerten. Es ist auch hierfür zweckmäßig, eine nicht zu große Anzahl an **Kategorien** zu verwenden – drei bis fünf sind üblich, oft werden auch nur zwei Kategorien verwendet. Der BSI-Standard 200-3 enthält ein Beispiel mit vier Stufen, dass Sie an die Gegebenheiten und Erfordernisse Ihrer Institution anpassen können. Die folgende Tabelle ist an dieses Beispiel angelehnt.

Risikokategorie	Definition
gering	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Maßnahmen bieten einen ausreichenden Schutz.
mittel	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Maßnahmen reichen möglicherweise nicht aus.
hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.Das Risiko kann mit einer großen Wahrscheinlichkeit nicht akzeptiert werden.
Sehr hoch	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Das Risiko kann mit einer sehr großen Wahrscheinlichkeit nicht akzeptiert werden.

Tabelle 17: Beispiel für die Klassifikation von Risiken

Zur Darstellung von Eintrittshäufigkeiten, Schadensauswirkungen und Risiken ist eine **Risikomatrix** ein gebräuchliches und sehr anschauliches Instrument. Auch hierzu enthält der BSI-Standard 200-3 einen Vorschlag, den Sie an die Festlegungen Ihrer Institution zur Risikobewertung anpassen können.

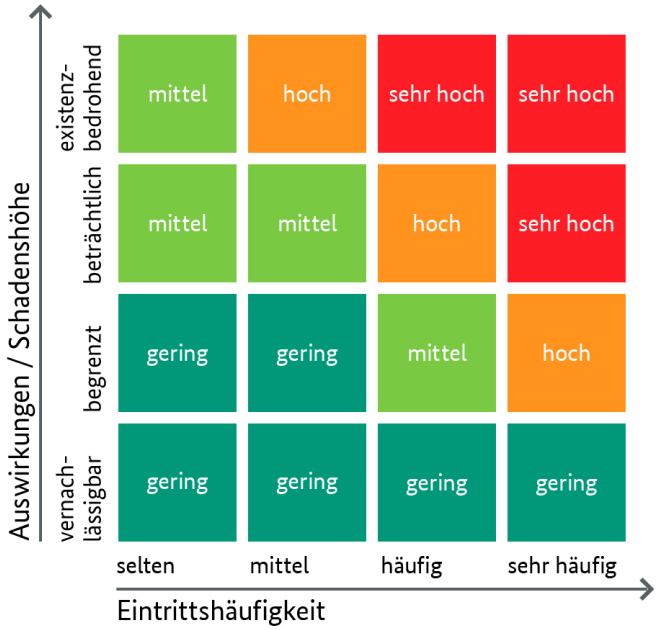


Abbildung 13: Beispiel einer Risikomatrix

Die Risikobewertung nehmen Sie vor, um begründete Entscheidungen zum Umgang mit möglichen Gefährdungen treffen zu können. Eine solche Entscheidung kann sein, durch zusätzliche Maßnahmen die Eintrittshäufigkeit und/oder die Auswirkungen einer Gefährdung zu verringern. Mit Hilfe der Risikomatrix können Sie auch verdeutlichen, wie sich die Umsetzung solcher Maßnahmen auf ein Risiko auswirken würde.

Lerneinheit 7.8: Beispiel für die Risikobewertung

Als Beispiel für die Risikobewertung werden zwei Gefährdungen für den Virtualisierungsserver S007 bei der RECPLAST GmbH betrachtet. Die Risiken werden mit Hilfe der zuvor beschriebenen Kategorien für Häufigkeiten, Auswirkungen und resultierendem Risiko bewertet.

Risikobewertung für die Gefährdung G 0.15 Abhören

Das Risiko besteht, weil zu Wartungszwecken die auf dem Server S007 betriebenen virtuellen Maschinen von Zeit zu Zeit auf einen zweiten Virtualisierungsserver verschoben werden. Bei dieser Live-Migration werden folglich die aktuellen Speicherinhalte der virtuellen Maschinen zwischen beiden Servern übertragen. Da wegen der damit verbundenen Performance-Verluste darauf verzichtet wurde, die Daten zu verschlüsseln, können die übertragenen Informationen grundsätzlich mitgelesen werden. Dies gilt auch für Datenübertragungen vom Virtualisierungsserver S1 zu den angeschlossen zentralen Speichersystemen.

Bei der Bewertung werden die Eintrittshäufigkeit und die möglichen Auswirkungen betrachtet:

- Die **Eintrittshäufigkeit** wird auch ohne zusätzliche Maßnahmen als **selten** bewertet. Diese Entscheidung wurde getroffen, weil durch eine geeignete Netzsegmentierung und Konfiguration dafür gesorgt wurde, dass die Datenübertragungen bei der Live-Migration wie auch zu den Speichersystemen in abgetrennten, von außen nicht zugänglichen Teilnetzen stattfinden, auf die nur die berechtigten und als vertrauenswürdig eingeschätzten Administratoren Zugriff haben.
- Gleichwohl handelt es sich bei den übertragenen Daten um solche, bei denen Verletzungen der Vertraulichkeit beträchtliche negative Folgen haben könnten. Die **Auswirkungen** bei Eintreten der **Gefährdung** werden daher als beträchtlich eingestuft.

Aus diesen Einschätzungen ergibt sich gemäß der festgelegten Kriterien für die Risikobewertung ein insgesamt **mittleres Risiko**.

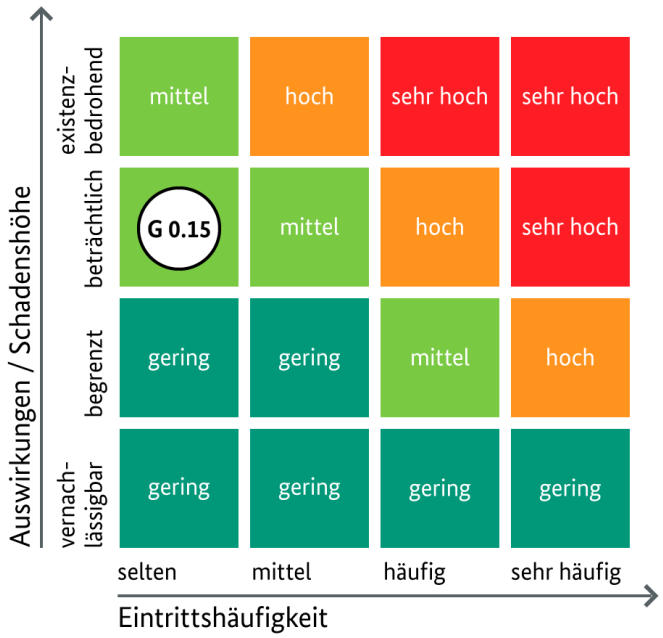


Abbildung 14: Risikomatrix mit eingetragener Gefährdung

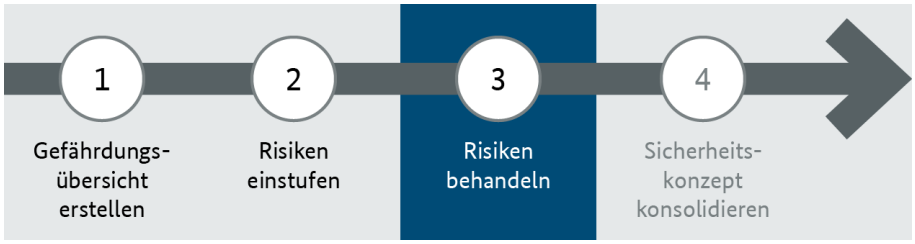
Risikobewertung für die Gefährdung G 0.25 Ausfall von Geräten oder Systemen

Der BSI Standard 200-3 enthält in Kapitel 5.2 verschiedene Beispiele dafür, wie eine Risikobewertung tabellarisch dokumentiert werden kann. Da oftmals eine Vielzahl an Gefährdungen zu berücksichtigen sind, kann auf ausführliche Erläuterungen zu den vorgenommenen Bewertungen verzichtet werden. Die folgende Tabelle zeigt anhand der Gefährdung G 0.25 eine hinreichende Dokumentation der Risikobewertung.

Virtualisierungsserver S007 Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch		
Gefährdung G 0.25 *Ausfall von Geräten oder Systemen*		Beeinträchtigte Grundwerte: Verfügbarkeit
Eintrittshäufigkeit ohne zusätzliche Maßnahmen: mittel	Auswirkungen ohne zusätzliche Maßnahmen: beträchtlich	Risiko ohne zusätzliche Maßnahmen: **mittel**

Tabelle 18: Beispiel für die tabellarische Dokumentation der Risikoanalyse

Lerneinheit 7.9: Risiken behandeln



In der Regel wird die Gefährdungsbewertung aufzeigen, dass nicht alle Gefährdungen durch das vorhandene Sicherheitskonzept ausreichend abgedeckt sind. In diesem Fall müssen Sie überlegen, wie angemessen mit

den verbleibenden Gefährdungen umgegangen werden kann, und eine begründete Entscheidung hierzu treffen.

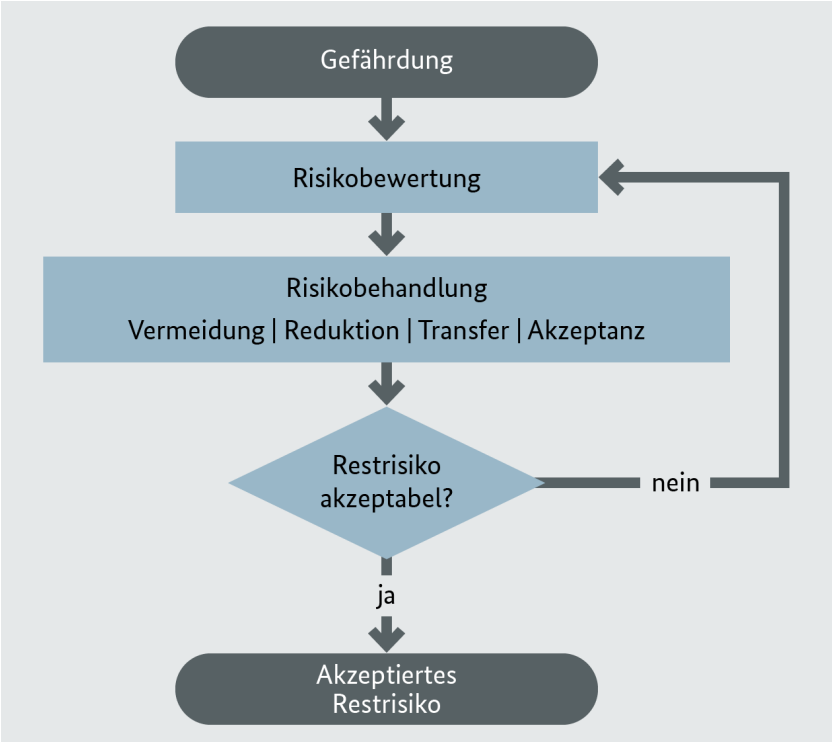


Abbildung 15: Risikobehandlung

Grundsätzlich können vier Möglichkeiten (**Risikooptionen**) unterschieden werden, mit Risiken umzugehen:

- **A: Risikovermeidung durch Umstrukturierung der Geschäftsprozesse**
  Die Risiken können vermieden werden, indem der Informationsverbund so umstrukturiert wird, dass die Gefährdung nicht mehr wirksam werden kann. Dies bietet sich beispielsweise für an, wenn Gegenmaßnahmen zwar möglich sind, aber einen zu hohen Aufwand bedeuten und gleichzeitig das Risiko nicht akzeptiert werden kann.
- **B: Risikoreduktion (Risikomodifikation) durch weitere Sicherheitsmaßnahmen**
  Die Risiken können durch zusätzliche, höherwertige Sicherheitsmaßnahmen verringert werden. Sofern es für das Zielobjekt, das Sie in der Risikoanalyse betrachtet haben, bereits einen Baustein im IT-Grundschutz-Kompendium gibt, finden Sie in den dort genannten Anforderungen für den erhöhten Schutzbedarf und den zugehörigen Umsetzungsempfehlungen erste Hinweise auf geeignete Maßnahmen. Weitere Quellen sind beispielsweise Produktdokumentationen, Standards zur Informationssicherheit oder in Fachveröffentlichungen.
- **C: Risikotransfer**
  Die Risiken werden verlagert. Durch Abschluss von Versicherungen oder durch Auslagerung der risikobehafteten Aufgabe an einen externen Dienstleister kann zum Beispiel ein möglicher finanzieller Schaden (zumindest teilweise) auf Dritte abgewälzt werden. Achten Sie bei dieser Lösung auf eine sachgerechte, eindeutige Vertragsgestaltung!
- **D: Risikoakzeptanz**
  Die Risiken können akzeptiert werden, sei es, weil die Gefährdung nur unter äußerst speziellen Bedingungen zu einem Schaden führen könnte, sei es, weil keine hinreichend wirksamen Gegenmaßnahmen bekannt sind oder aber weil der Aufwand für mögliche Schutzmaßnahmen unangemessen hoch ist.

Ein Risiko kann nur dann akzeptiert werden, wenn das (z. B. nach Umsetzung von Schutzmaßnahmen verbleibende) **Restrisiko** von der Institution getragen werden kann, sich also im Einklang mit den festgelegten Risikoakzeptanzkriterien befindet.

Risiken unter Beobachtung

Manche Risiken können zwar vorübergehend in Kauf genommen werden, es ist aber damit zu rechnen, dass sich die Gefährdungslage in Zukunft verändern wird und die Risiken dann nicht mehr akzeptiert werden können. In solchen Fällen empfiehlt es sich, die Risiken unter Beobachtung zu stellen und von Zeit zu Zeit zu prüfen, ob nicht doch ein Handlungsbedarf besteht. Es ist zudem sinnvoll, bereits im Vorfeld geeignete Schutzmaßnahmen auszuarbeiten, so dass eine rasche Inbetriebnahme möglich ist, sobald die Risiken nicht mehr akzeptabel sind.

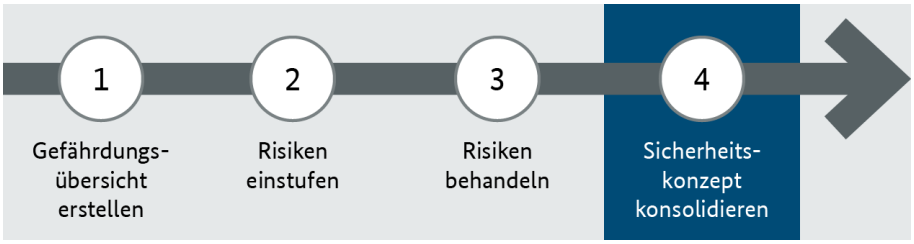
Alle Beschlüsse müssen vom Management getragen werden. Es muss dazu bereit sein, die Kosten für die Reduktion oder den Transfer von Risiken wie auch die Verantwortung für die in Kauf genommenen Risiken zu übernehmen. Binden Sie daher die Leitungsebene angemessen in die Beratungen ein. Dokumentieren Sie die Entscheidungen so, dass sie von Dritten (z. B. Auditoren) nachvollzogen werden können, und lassen Sie dieses Schriftstück **vom Management unterschreiben**.

Beispiel

Die folgende Tabelle zeigt exemplarisch für die beiden zuvor betrachteten Gefährdungen die bei der RECPLAST GmbH für den Virtualisierungsserver getroffenen Entscheidungen zur Risikobehandlung.

Gefährdung	Risikokategorie	Risikobehandlungsoption
G 015 *Abhören* (hier bei Live-Migration)	**mittel**	**D. Risikoakzeptanz** (Risikoübernahme ohne zusätzliche Sicherheitsmaßnahme) Auf das Live-Migration-Netz dürfen nur befugte Administratoren zugreifen. Diesen wird vertraut. Das bestehende Restrisiko wird von der RECPLAST GmbH als vertretbar eingeschätzt und übernommen.
G 0.25 *Ausfall von Geräten oder Systemen* (hier Ausfall des Virtualisierungsservers)	**mittel** Mit ergänzenden Maßnahmen: **gering**	**B: Risikoreduktion** Ergänzende Sicherheitsmaßnahme: Der Server wird redundant ausgelegt, damit sichergestellt ist, dass bei einem Ausfall die virtuelle Infrastruktur weiterhin problemlos betrieben wird. Das System wird so konfiguriert, dass bei Ausfall automatisch auf einen Ersatzrechner innerhalb des Clusters umgeschaltet wird.

Lerneinheit 7.10: Die nächsten Schritte



Als Abschluss der Risikoanalyse sind die zusätzlichen Maßnahmen, deren Umsetzung beschlossen wurde, in das vorhandene Sicherheitskonzept zu integrieren (= Konsolidierung des Sicherheitskonzepts) und darauf aufbauend ist der Sicherheitsprozess fortzusetzen.

Konsolidierung des Sicherheitskonzepts

In diesem Schritt sollten Sie die **Eignung**, **Angemessenheit** und **Benutzerfreundlichkeit** der zusätzlichen Sicherheitsmaßnahmen ebenso prüfen wie deren **Zusammenwirken** mit anderen Maßnahmen. Diese Konsolidierung des Sicherheitskonzepts kann sowohl zu Anpassungen bei den zusätzlich ausgewählten Maßnahmen als auch zu Änderungen im bestehenden Konzept führen.

Weitere Informationen zur Konsolidierung von Sicherheitsmaßnahmen finden Sie in Lerneinheit 8.1: *Maßnahmen konsolidieren*.

Fortführung des Sicherheitsprozesses

Nach der Konsolidierung des Sicherheitskonzepts kann der Sicherheitsprozess mit den nächsten Schritten fortgesetzt werden. Dies bedeutet insbesondere, dass in einem **erneuten IT-Grundschutz-Check** der Umsetzungsstatus der neu hinzugekommenen oder geänderten Maßnahmen zu prüfen und zu dokumentieren ist, wie in der vorherigen Lektion (IT-Grundschutz-Check) beschrieben.

Ein zweiter IT-Grundschutz-Check ist erforderlich, da sich in der Regel durch die Risikoanalyse das Sicherheitskonzept geändert hat und der Umsetzungsstatus der neu hinzugekommenen oder geänderten Maßnahmen zu prüfen ist.

Lerneinheit 7.11: Testfragen

Wenn Sie möchten, können Sie mit den nachfolgenden Fragen Ihre Kenntnisse zur Risikoanalyse gemäß BSI-Standard 200-3 überprüfen. Die Auflösungen zu den Fragen finden Sie im Anhang. Es können mehrere Antwortmöglichkeiten zutreffend sein.

1 **Wer trägt die Verantwortung für die bei einer Risikoanalyse getroffenen Entscheidungen zu einem IT-System?**

a der Administrator des IT-Systems

b die Leitung der Institution

c der Informationssicherheitsbeauftragte

d das IS-Management-Team

2 **Welche Gefährdungen werden bei der Erstellung der Gefährdungsübersicht im ersten Schritt betrachtet?**

a die im Anhang von BSI-Standard 200-3 enthaltenen Risikokataloge

b die relevanten elementaren Gefährdungen aus dem IT-Grundschutz-Kompendium

c die im Anhang der Norm ISO 27005 angeführten Gefährdungen

d die in den Abschnitten zur Gefährdungslage eines Bausteins angeführten spezifischen Gefährdungen

3 **Was bewerten Sie bei der Risikoeinschätzung?**

a die Häufigkeit des Eintretens einer Gefährdung

b das mit einer Gefährdung verbundene Schadensausmaß

c welche Schutzziele von einer Gefährdung betroffen sind

d die Wirksamkeit der geplanten und umgesetzten Maßnahmen gegen eine Gefährdung

4 **Wodurch verlagern Sie ein Risiko?**

a durch den Abschluss einer Versicherung

b durch Outsourcing des risikobehafteten Geschäftsprozesses an einen externen Dienstleister

c durch Umstrukturierung des risikobehafteten Geschäftsprozesses

d durch die Entscheidung, risikomindernde Maßnahmen erst dann umzusetzen, wenn die hierzu erforderlichen Finanzmittel bereitstehen

5 **Aus welchen Gründen kann es gerechtfertigt sein, auch ein hohes Risiko zu akzeptieren?**

a Der Aufwand für mögliche Schutzmaßnahmen ist unangemessen hoch.

b Vergleichbare Institutionen akzeptieren das Risiko ebenfalls.

c Es gibt keine wirksamen Schutzmaßnahmen gegen das Risiko.

d Es ist bislang noch zu keinem nennenswerten Sicherheitsvorfall aufgrund der dem Risiko zugrunde liegenden Gefährdung gekommen.

6 **Wann ist die Risikoakzeptanz grundsätzlich unzulässig?**

a bei der Nichterfüllung von Basis-Anforderungen

b beim Vorhandensein von elementaren Gefährdungen

c bei sehr hohem Schutzbedarf

d bei Nichterfüllung von Standard-Anforderungen

Lektion 8: Umsetzungsplanung

In Ihrer Institution sind alle Basis- und Standard-Anforderungen erfüllt? Sie haben ferner mit Hilfe von Risikoanalysen festgestellt, dass auch solche Zielobjekte angemessen geschützt sind, die einen besonderen Schutzbedarf haben. Dann haben Sie zweifelsfrei ein gutes Sicherheitsniveau in Ihrer Institution erreicht, und können sich darauf konzentrieren, dieses zu erhalten und zu verbessern.

In der Regel führen IT-Grundschutz-Check und zusätzliche Risikoanalysen aber zu einem anderen Ergebnis: Irgendwelche Defizite gibt es immer, seien es Lücken in den vorhandenen organisatorischen Regelungen oder mangelnde Kontrolle der geltenden Regeln, sei es fehlende Sicherheitstechnik oder unzureichender baulicher Schutz gegen Feuer, Wasser oder Diebstahl.

Bei der Umsetzungsplanung geht es darum, diese Lücken wirksam und effizient zu schließen. In dieser Lektion lernen Sie hierfür ein systematisches Vorgehen kennen, an dem Sie sich insbesondere dann orientieren können, wenn viele Einzelmaßnahmen umzusetzen sind. Sie erfahren,

- welche Aspekte Sie bei der Umsetzung von Sicherheitsmaßnahmen berücksichtigen müssen,
- mit welchen Hilfsmitteln Sie der IT-Grundschutz dabei unterstützt,
- was Sie tun sollten, wenn zweckmäßige Sicherheitsmaßnahmen nicht unmittelbar umgesetzt werden können und
- wie Sie die Ergebnisse der Umsetzungsplanung dokumentieren können.

Lerneinheit 8.1: Maßnahmen konsolidieren

Im **ersten Schritt** sind aus den Ergebnissen des IT-Grundschutz-Checks und eventuell durchgeführter Risikoanalysen diejenigen Anforderungen herauszufiltern, die **nicht oder nur teilweise erfüllt** sind.

Eine übersichtliche Dokumentation erhalten Sie, wenn Sie die unzureichend erfüllten Anforderungen **tabellarisch zusammenstellen** und dabei nach den betroffenen Zielobjekten gruppieren, etwa nach dem gesamten Informationsverbund oder bestimmten Räumen und IT-Systemen.

Legen Sie anschließend **Maßnahmen** fest, mit denen Sie diese Sicherheitslücken schließen können. Als Hilfsmittel hierfür können Sie die Umsetzungshinweise zu den einzelnen IT-Grundschutz-Bausteinen verwenden.

Anschließend betrachten Sie die Maßnahmen **im Zusammenhang** und prüfen,

- ob einzelne Maßnahmen überflüssig werden, weil andere zu realisierende Maßnahmen einen mindestens gleichwertigen Schutz für das jeweilige Zielobjekt bewirken,
- welche Maßnahmen noch konkretisiert und an die individuellen Gegebenheiten der Institution angepasst werden müssen und
- ob die Maßnahmen tatsächlich geeignet und angemessen sind, sie also genügend Schutz bieten, ohne die Arbeitsabläufe zu behindern oder die Schutzwirkung anderer Maßnahmen zu beeinträchtigen.

Ziel ist es, durch Streichung der überflüssigen und Konkretisierung der verbleibenden Maßnahmen den erforderlichen finanziellen und personellen Realisierungsaufwand auf das notwendige Maß zu begrenzen.

Das Ergebnis dieses Schritts ist eine auf die jeweilige Institution zugeschnittene und konkretisierte Liste von Maßnahmen. Erleichtern Sie die spätere Nachvollziehbarkeit der Entscheidungen, die Sie bei dem Abgleich und der Anpassung der Maßnahmen getroffen haben, indem Sie die Begründungen dokumentieren.

Beispiele

Einige Beispiele sollen die Fragestellungen und mögliche Lösungen bei der Konsolidierung der Maßnahmen verdeutlichen:

- Wenn eine Risikoanalyse ergab, dass für eine Gruppe von IT-Systemen eine Authentisierung über ein chipkarten- oder token-basiertes Verfahren angewendet werden sollte, können unter Umständen Maßnahmen zur Gewährleistung einer hohen Passwortgüte entfallen.
- Fehler bei der Gebäudeplanung lassen sich nachträglich oft nur mit einem unverhältnismäßig hohen Aufwand korrigieren. Wenn die vollständige Erfüllung von Anforderungen wie die Vermeidung wasserführender Leitungen aufgrund der baulichen Gegebenheiten wirtschaftlich nicht vertretbar ist, sollten zumindest Ersatzmaßnahmen getroffen werden. Beispielsweise können unter den vorhandenen Leitungen wasserableitende Bleche installiert werden, die von einem Wassermelder mit einer im ständig besetzten Pförtnerraum hörbaren Alarmsirene überwacht werden. Dadurch können Wasserschäden zumindest frühzeitig erkannt und in den Auswirkungen begrenzt werden.
- Maßnahmen zum Zugangsschutz versperren unter Umständen im Brandfall mögliche Fluchtwege. Hier empfiehlt sich gegebenenfalls die Rücksprache mit Brandschutzexperten, z. B. der Feuerwehr, um sowohl dem Zugangs- als auch dem Brandschutz gleichermaßen gerecht zu werden.

- Die Verschlüsselung geschäftskritischer Informationen zum Schutz ihrer Vertraulichkeit ist ein Beispiel für eine Maßnahme, die mit anderen Schutzzielen kollidieren kann und bei der daher eine sorgfältige Abwägung der Vor- und Nachteile und unter Umständen ergänzende Maßnahmen nötig sind:
  - Verschlüsselte E-Mails können den zentralen Virenschutz auf einem Server unterlaufen und so zur Infiltration eines Netzes mit Schadsoftware führen.
  - Bei unzureichendem Schlüssel-Management oder fehlerhafter Anwendung kann Verschlüsselung ferner die Verfügbarkeit wichtiger Daten auch für berechtigte Personen gefährden.

Lerneinheit 8.2: Aufwände schätzen

Angesichts des in der Regel begrenzten Budgets für Informationssicherheit ist ein Überblick über die voraussichtlichen fixen und variablen Kosten der einzelnen Maßnahmen nötig. Daher schätzen Sie im nächsten Schritt, welcher einmalige und wiederkehrende finanzielle und personelle Aufwand durch die Umsetzung der einzelnen geplanten Maßnahmen entsteht.

Der Einsatz von Personal und Finanzmitteln muss vom Management getragen werden. Dies gilt insbesondere dann, wenn die bewilligten Finanzmittel nicht für die sofortige Umsetzung sämtlicher Maßnahmen ausreichen und entschieden werden muss, ob das Budget aufgestockt oder das Risiko in Kauf genommen werden soll, das verbleibt, wenn Maßnahmen nicht umgesetzt werden.

Zur Vorbereitung einer Managemententscheidung über die Einführung von Sicherheitsmaßnahmen sollten Sie

- einen Vorschlag für die Verteilung des Budgets erarbeiten,
- kostengünstigere Ersatzmaßnahmen erwägen, falls der Aufwand für die Umsetzung einzelner Maßnahmen das voraussichtliche Budget übersteigt,
- die Restrisiken, die aus der Nichterfüllung von Sicherheitsanforderungen entstehen, dem Management bewusst machen (als Argumentationshilfe können Sie die Kreuzreferenztabellen verwenden, die Sie am Ende eines jeden IT-Grundschutz-Bausteins finden und in denen dargestellt ist, gegen welche Gefährdungen eine Anforderung gerichtet ist) und
- dafür sorgen, dass das Management bei der Entscheidung über das Budget durch Unterschrift dokumentiert, dass es bereit ist, die Restrisiken zu tragen.

Beachten Sie, dass die Erfüllung der relevanten Basis-Anforderungen das Mindest-Sicherheitsniveau gemäß IT-Grundschutz ist. Risiken, die aus der Nichterfüllung solcher Anforderungen erwachsen, sollten daher nicht akzeptiert werden.

Lerneinheit 8.3: Umsetzungsreihenfolge und Verantwortlichkeit festlegen

Wenn Budget oder Personal nicht ausreichen, alle wünschenswerten Sicherheitsmaßnahmen unmittelbar umzusetzen, ist eine sinnvolle Reihenfolge festzulegen. Dabei sollten Sie sich an folgenden Regeln orientieren:

- Einen ersten Indikator zur Umsetzungsreihenfolge liefern die **Kennzeichnungen R1, R2 und R3** bei den Modellierungshinweise in Kapitel 2.2 des IT-Grundschutz-Kompendiums. Anforderungen aus mit „R1“ gekennzeichneten Bausteinen (z. B. ISMS.1 *Sicherheitsmanagement* und die Bausteine der Schicht ORP *Organisation und Personal*) sollten vorrangig erfüllt werden. Anschließend sind Anforderungen aus den mit „R2“ gekennzeichneten Bausteine zu erfüllen und erst zum Schluss solche aus Bausteinen, die mit dem Kürzel „R3“ versehen sind.
- Grundsätzlich sind ferner zunächst diejenigen Maßnahmen umzusetzen, mit denen **Basis-Anforderungen** erfüllt werden, dann diejenigen zur Erfüllung von **Standard-Anforderungen** und erst zuletzt die zur **Gewährleistung eines höheren Schutzbedarfs**.
- Berücksichtigen Sie ferner auch die **sachlogischen Zusammenhänge** der einzelnen Maßnahmen: So sind diejenigen Maßnahmen vorzuziehen, deren Umsetzung eine Voraussetzung für die Realisierung weiterer Maßnahmen ist.

Insbesondere sollten Sie Ihr Augenmerk darauf legen, welche Wirkung die Umsetzung der einzelnen Maßnahmen auf das Sicherheitsniveau des Informationsverbundes hat. Setzen Sie vorrangig solche Maßnahmen um, die

- Komponenten mit höherem Schutzbedarf betreffen (z. B. sollten Server vor Clients abgesichert werden),
- eine große Breitenwirkung entfalten (z. B. zentrale Maßnahmen wie der Einsatz von Netz- und Systemmanagement-Werkzeugen) oder
- Bereiche betreffen, in denen auffallend viele Sicherheitsmaßnahmen fehlen.

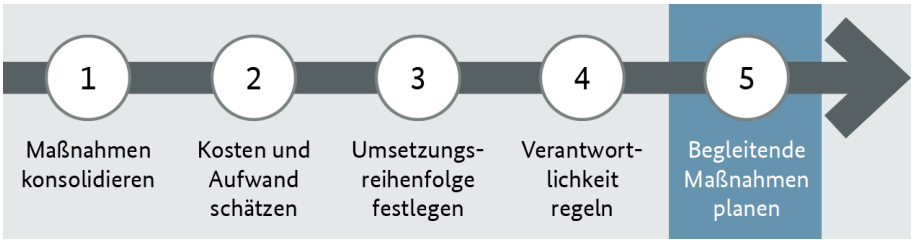
Dokumentieren Sie auch Ihre Entscheidungen zur Umsetzungsreihenfolge und deren Begründungen sorgfältig, damit nachvollziehbar und verständlich wird, warum Sie die aus der zeitlich nachgeordneten Umsetzung bestimmter Maßnahmen resultierenden Restrisiken in Kauf genommen haben. Dies kann insbesondere bei eventuell möglichen juristischen Streitfällen als Nachweis wichtig sein, dass die notwendige Sorgfaltspflicht beachtet wurde.

Aufgaben und Verantwortlichkeiten zuweisen

Maßnahmen werden meist nur dann fristgerecht umgesetzt, wenn geklärt wird, wer bis zu welchem Termin für deren Umsetzung zuständig ist. Der nächste Schritt besteht daher darin, diejenigen Personen zu bestimmen, welche die Umsetzung initiieren und durchführen sollen. Auch diese Entscheidungen sollten mit dem Management abgestimmt sein.

Achten Sie darauf, dass die für die Umsetzung Zuständigen ausreichende Kenntnisse und Kompetenzen besitzen und ihnen die erforderlichen Ressourcen zur Verfügung gestellt werden. Planen Sie erforderliche Fortbildungen ein.

Lerneinheit 8.4: Begleitende Maßnahmen planen



Der Erfolg einer Maßnahme hängt in einem entscheidenden Umfang davon ab, wie diese von den Mitarbeitern akzeptiert und angewendet wird. Achten Sie daher darauf, dass bei Einführung neuer Sicherheitsmaßnahmen die betroffenen Mitarbeiter ausreichend geschult und für mögliche Probleme sensibilisiert werden.

Planen Sie Schulungsmaßnahmen ein!

Die Einführung neuer Sicherheitsmaßnahmen erfordert immer auch aufgaben- und produktbezogene Schulungen für die betroffenen Mitarbeiter. Was nützt zum Beispiel ein neu angeschaffter Feuerlöscher, wenn die Mitarbeiter im Brandfall nicht sachgerecht mit ihm umgehen können? Drei weitere Beispiele für zweckmäßige Schulungen:

- Wenn Sie einem Mitarbeiter besondere Aufgaben im Sicherheitsmanagement übertragen, etwa als ICS-Informationssicherheitsbeauftragter, benötigt er vielfältige und kontinuierlich zu aktualisierende Kenntnisse zu methodischen, organisatorischen und technischen Aspekten seines Aufgabengebiets. Der hierfür erforderliche Zeitaufwand ist bereits vor der Einführung dieser Verantwortlichkeit und der Ernennung des hierfür ausgewählten Mitarbeiters zu berücksichtigen.
- Wenn die Schnittstelle zum Internet durch eine Firewall geschützt werden soll, benötigt der zuständige Netzadministrator Kenntnisse über deren sichere Installation, Konfiguration und Administration.
- Der Einsatz von Verschlüsselungssoftware zum Schutz der Vertraulichkeit personenbezogener oder geschäftskritischer Daten erfordert nicht nur den Aufbau von Know-how zu dem eingesetzten Produkt, sondern auch Regeln für dessen Anwendung: Welche Nachrichten oder Dateien sind zu verschlüsseln? Wie ist der private Schlüssel zu schützen? Wie sichert man, dass im Bedarfsfall berechtigte Vertreter Zugriff auf die verschlüsselten Daten erhalten? Die auf diese und andere Fragen gefundenen Lösungen müssen den Mitarbeitern verständlich gemacht werden.

Sensibilisieren Sie die betroffenen Mitarbeiter!

Gute Schulung alleine garantiert noch kein sicherheitsgerechtes Verhalten. Für die dauerhafte Wirksamkeit der Sicherheitsmaßnahmen ist es wichtig, dass die Mitarbeiter für Informationssicherheit sensibilisiert und bereit sind, die erforderlichen Maßnahmen umzusetzen, die notwendigen Verhaltensregeln zu beachten und unter Umständen auch Unbequemlichkeiten zu akzeptieren. Einige negative Beispiele:

- Brandschutztüren verlieren ihre Schutzwirkung, wenn sie mit Holzkeilen offen gehalten werden, weil den Mitarbeitern das ständige Öffnen der Türen zu umständlich ist.
- Der Kauf von Software zur E-Mail-Verschlüsselung wird zur Fehlinvestition, wenn die Mitarbeiter diese nicht benutzen, weil sie sich der Gefährdungen der Vertraulichkeit nicht bewusst sind, und ihre E-Mails weiterhin unverschlüsselt versenden, auch solche mit vertraulichem Inhalt.
- Passwörter bedeuten immer einen zusätzlichen Arbeitsschritt vor der eigentlichen Aufgabe. Regeln für sichere Passwörter wie periodischer Wechsel oder die Verwendung unterschiedlicher Passwörter für unterschiedliche Systeme erhöhen die Unbequemlichkeit. Wenn die Mitarbeiter diese Anforderungen lediglich als lästige Pflicht betrachten, werden Sie dazu neigen, sie zu umgehen, z. B. indem sie unsichere Passwörter wählen oder Zettel mit den Passwörtern in der Nähe des Rechners platzieren.

- Ein Netzadministrator, der seine Probleme bei der Installation eines Sicherheitsgateways unter Angabe seiner dienstlichen Adresse in einem Internet-Forum diskutiert, gefährdet die Schutzwirkung der Software, um deren Installation er sich bemüht.

Den betroffenen Mitarbeitern muss der Sinn der neuen Sicherheitsmaßnahmen verständlich gemacht werden, sei es in Gesprächen, in eigens anberaumten Versammlungen, während regelmäßig stattfindender Besprechungen oder in schriftlicher Form.

Überprüfen Sie die Akzeptanz der Maßnahmen!

Maßnahmen, die von den Mitarbeitern nicht akzeptiert werden, drohen zu scheitern. Überprüfen Sie daher nach Einführung der Sicherheitsmaßnahmen, ob diese tatsächlich von den Mitarbeitern angenommen werden. Sollte dies nicht oder nur eingeschränkt der Fall sein, so versuchen Sie, die Ursachen dafür zu ermitteln, und leiten Sie bei Bedarf zusätzliche Maßnahmen zur Sensibilisierung ein.

Lerneinheit 8.5: Planung dokumentieren

Der nachfolgende Auszug aus dem Realisierungsplan der RECPLAST GmbH zeigt, wie Sie die Festlegungen zur Umsetzung von Maßnahmen dokumentieren können. Dargestellt sind Maßnahmen für ein ausgewähltes Zielobjekt, den Print Server S003, und die zugehörigen Entscheidungen zu Terminen, Budget und Verantwortlichkeiten.

Anforderung	Umzusetzende Maßnahme	Terminplanung	Budget	Umsetzung durch
SYS.1.1.A3 *Restriktive Rechtevergabe*	Die verbliebenen Gruppenberechtigungen müssen aufgelöst werden	Drittes Quartal des Jahres	Keine Kosten	Herr Schmitt (IT-Betrieb)
SYS.1.1.A4 *Rollentrennung*	Separate Benutzerkennungen für jeden Administrator einrichten	31. Juli des Jahres	Keine Kosten	Herr Schmitt (IT-Betrieb)
SYS.1.1.A8 *Regelmäßige Datensicherung*	Die Datensicherungen werden derzeit auf Bändern im Serverraum aufbewahrt. Ein externes Backup-System ist geplant. Ein Angebot für die Initialisierung liegt bereits vor (15.000 €). Die Betriebskosten müssen noch verhandelt werden.	Erstes Quartal im Folgejahr	Anschaffung: 15.000 € Betrieb: Noch offen	Frau Meyer (Einkauf)

Tabelle 19: Beispiel für die Dokumentation der Umsetzungsplanung

Lerneinheit 8.6: Testfragen

Wir sind am Ende der Lektion zur Umsetzungsplanung. Wenn Sie möchten, können Sie anhand der folgenden Testfragen Ihre Kenntnisse zur Umsetzungsplanung gemäß IT-Grundschutz-Methodik überprüfen. Es können mehrere Antwortmöglichkeiten zutreffend sein.

1 **Was müssen Sie prüfen, wenn Sie die Umsetzung von Sicherheitsmaßnahmen planen?**

a welche begleitenden Maßnahmen für eine erfolgreiche Umsetzung erforderlich sind

b ob die betreffende Maßnahme bereits eingeführt ist

c ob die Maßnahme mit anderen Maßnahmen vereinbar ist

d in welcher Reihenfolge die verschiedenen Maßnahmen umgesetzt werden sollen

2 **Welche Informationen aus dem IT-Grundschutz-Kompendium unterstützen Sie bei der Festlegung einer sinnvollen Umsetzungsreihenfolge der geplanten Maßnahmen?**

a die fünfstufige Kennziffer zur Angabe der Priorität einer Anforderung in den IT-Grundschutz-Bausteinen

b die Aufteilung der Anforderungen in Basis- und Standard-Anforderungen sowie solchen für den höheren Schutzbedarf

c der Vorschlag zur Kennzeichnung einer sinnvollen Bearbeitungsreihenfolge der Bausteine mithilfe der Kürzel R1, R2 und R3

d die Darstellung der Gefährdungslage am Beginn eines Bausteins

3 **Was unternehmen Sie als Informationssicherheitsbeauftragter, wenn die Leitung Ihrer Institution nicht bereit ist, den Aufwand für eine bestimmte Sicherheitsmaßnahme zu tragen?**

a Sie verdeutlichen ihr, welche Risiken mit dem Fehlen der Maßnahme verbunden sind.

b Sie bitten die Leitung, durch Unterschrift zu bestätigen, dass sie die damit verbundenen Gefahren kennt und trägt.

c Sie ignorieren die Leitung und setzen die Maßnahme trotzdem um.

d Sie verzichten auf eine unmittelbare Reaktion, nehmen sich aber vor, nach Ablauf einer gewissen Zeitspanne die Zustimmung der Leitung einzuholen.

4 **Wer sollte in der Regel technische Maßnahmen zur Absicherung eines bestimmten IT-Systems umsetzen?**

a die Leitung der IT-Abteilung

b der Informationssicherheitsbeauftragte

c der zuständige Systemadministrator

d der Benutzer des IT-Systems

5 **Wer sollte üblicherweise prüfen, ob eine Sicherheitsmaßnahme wie geplant umgesetzt ist?**

a die Geschäftsführung

b der Informationssicherheitsbeauftragte

c der zuständige IT-Administrator

d die Leitung der IT-Abteilung

6 **Welches Hilfsmittel im IT-Grundschutz-Kompendium können Sie verwenden, um Ihrer Leitung zu verdeutlichen, welche Risiken die Nichterfüllung von Anforderungen mit sich bringt?**

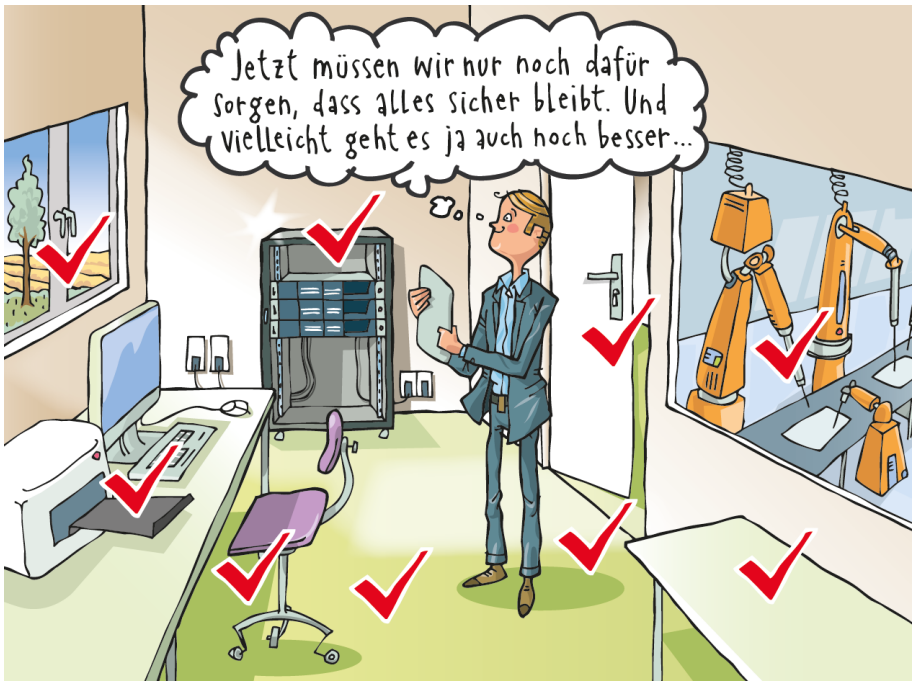
a das Restrisikodeklarationsformular im Anhang des Kompendiums

b die Kreuzreferenztabellen am Ende eines Bausteins

c das Risikokalkulationsschema in der Übersicht der elementaren Gefährdungen

d die Beispiele für eine erfolgreiche Sensibilisierung im Baustein ORP.3 *Sensibilisierung und Schulung*

Lektion 9: Aufrechterhaltung und Verbesserung



Im Realisierungsplan haben Sie festgehalten, welche Maßnahmen Ihres Sicherheitskonzepts zu welchem Zeitpunkt und in welcher Weise umgesetzt sein sollen. Dabei haben Sie erforderliche Ressourcen, eventuelle Zwischentermine und begleitende Maßnahmen berücksichtigt. Damit Sie sicher sein können, dass alles wie geplant umgesetzt ist und funktioniert, müssen Sie die **Einhaltung der Planung** regelmäßig kontrollieren.

Informationssicherheit ist darüber hinaus kein einmalig herzustellender und anschließend stabiler Zustand, sondern ein **stetiger Prozess**, der immer wieder an sich wandelnde und neue Herausforderungen angepasst werden muss.

In dieser Lektion lernen Sie Verfahren kennen, mit denen Sie **Angemessenheit und Wirksamkeit** der technischen und organisatorischen Maßnahmen für Informationssicherheit in Ihrer Institution **kontinuierlich überwachen und verbessern** können. Sie erfahren,

- wie Sie den **Umsetzungsstand** der im Sicherheitskonzept vorgesehenen Maßnahmen prüfen,
- wie Sie bei der Überprüfung der **Wirksamkeit** der Maßnahmen vorgehen sollten,
- wie Sie die Erkenntnisse aus den Überprüfungen in **Maßnahmen zur Verbesserung** Ihres Informationssicherheitsmanagements überführen,
- wie Ihnen **Kennzahlen** bei der Bewertung einzelner Aspekte der Informationssicherheit helfen können,
- was unter einem **Reifegradmodell** der Informationssicherheit zu verstehen ist und welchen Nutzen Sie daraus ziehen können sowie
- wie Sie Dritten Ihr gutes Sicherheitsniveau mit einem **ISO 27001-Zertifikat auf Basis von IT-Grundschutz** nachweisen können.

Lerneinheit 9.1: Leitfragen für die Überprüfung

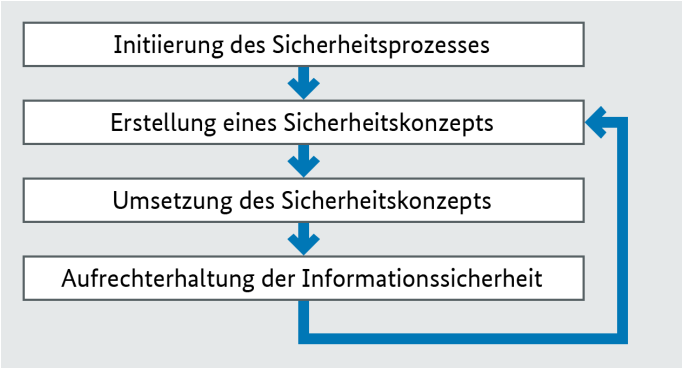


Abbildung 16: Phasen des Sicherheitsprozesses

Um sicherzustellen, dass die Maßnahmen des Sicherheitskonzepts immer den Anforderungen entsprechen, müssen sie kontinuierlich überprüft werden.

Diese Überprüfungen sollten sich an folgenden Leitfragen orientieren:

- **Welche Ziele der Informationssicherheit sind aktuell vordringlich?**
  Die Bedeutung von Sicherheitszielen kann sich im Zeitablauf verändern. So kann es wichtiger werden, die Vertraulichkeit von Informationen zu schützen, wenn sich gesetzliche Rahmenbedingungen ändern oder aber die Institution mit Daten arbeitet, die dies verstärkt erfordern. Alle Maßnahmen zur Erhaltung der Vertraulichkeit müssen daher besonders sorgfältig geprüft werden. Eine weitere wichtige Frage ist, ob die gewählten Sicherheitsmaßnahmen noch der Gefährdungslage entsprechen. Auch ist zu prüfen, ob neue technische Verfahren einen effizienteren und wirksameren Schutz bieten können.
- **Wer ist verantwortlich für die Überwachung des Informationssicherheitsprozesses?**
  Häufig ist die Institution so komplex, dass der ISB nicht alle Überprüfungen leiten und durchführen kann. Dann ist es wichtig, dass für verschiedene Bereiche Personen benannt sind, die diese Maßnahmen konzipieren, umsetzen, Ergebnisse dokumentieren sowie Verbesserungen planen und steuern. Bei einer solchen verteilten Verantwortung ist eine gute Zusammenarbeit mit dem ISB wichtig, der über alle Schritte informiert werden muss.
- **Wie häufig sind die Verfahren zu überprüfen?**
  Für weniger wichtige Schutzmechanismen kann eine Überprüfung seltener erfolgen als für kritische Prozesse. Mindestens einmal pro Jahr muss das Sicherheitskonzept darauf überprüft werden, ob es noch effektiv ist, also den Zielen der Informationssicherheit im Unternehmen oder der Behörde entspricht. Wenn es einen Sicherheitsvorfall gegeben hat, sollte dies Anlass für eine zusätzliche Prüfung sein.

Die Umsetzungshinweise in ISMS.1.M11: *Aufrechterhaltung der Informationssicherheit* geben wichtige Empfehlungen zur Vorgehensweise bei der Überprüfung des Sicherheitsprozesses.

Lerneinheit 9.2: Überprüfungsverfahren

Es gibt eine Reihe von bewährten Verfahren, mit denen Sie die Effizienz und Effektivität Ihrer Vorkehrungen für Informationssicherheit prüfen können, angefangen mit der Abarbeitung einfacher Checklisten und der punktuellen Prüfung der Netzsicherheit mittels Penetrationstests bis hin zu umfassenden Prüfungen der Angemessenheit und Wirksamkeit der umgesetzten technischen und organisatorischen Schutzmaßnahmen.

Grundsätzlich gilt, dass umfassende Prüfungen in **regelmäßigen Intervallen** (jährlich bis maximal drei Jahre) durchgeführt werden sollten. Aber auch **fallweise Prüfungen** sind zweckmäßig, beispielsweise bei der Änderung von Geschäftsprozessen und insbesondere nach Sicherheitsvorfällen.

Sicherheitsvorfälle sollten immer ein Anlass sein, die Sicherheitskonzeption zu hinterfragen. Dies sollte offen und sorgfältig geschehen, um Schwachstellen, die einen Vorfall begünstigt haben, identifizieren und beseitigen zu können.

Zwei zweckmäßige Verfahren, mit den Sie Ihr Sicherheitskonzept und das erreichte Schutzniveau prüfen können, sind die IS-Revision und der Cyber-Sicherheits-Check:

- Mit einer **Informationssicherheitsrevision (IS-Revision)** können Sie nach einem festgelegten Verfahren und von kompetenten Revisoren überprüfen lassen, ob das Sicherheitskonzept Ihrer Institution wie beabsichtigt umgesetzt ist und es nach wie vor den aktuellen Anforderungen gerecht wird. Die IS-Revision liefert sowohl den Verantwortlichen für Informationssicherheit als auch der Leitung einer Institution belastbare Informationen über den aktuellen Zustand der Informationssicherheit. Neben einer umfassenden Prüfung, die auf die vollständige und vertiefte Überprüfung der Informationssicherheit in einer Institution abhebt, gibt es mit der Kurz-, Querschnitts- und Partialrevision Varianten, bei denen Tiefe und Umfang der Prüfung begrenzt sind.
- Wenn Sie noch wenig Erfahrung mit diesem Thema haben, kann der **Cyber-Sicherheits-Check** eine wichtige Hilfe bei der Überprüfung des Sicherheitsniveaus Ihrer Institution sein. Er gibt ihnen Hinweise zur Anfälligkeit gegen Cyberangriffe und ist so angelegt, dass die regelmäßige Durchführung das Risiko verringert, zum Opfer solcher Angriffe zu werden.

Für die Durchführung der IS-Revision hat das BSI ein eigenes Vorgehensmodell entwickelt, das im Leitfaden IS-Revision beschrieben ist. Dort erfahren Sie auch mehr zu Prüfumfang und -tiefe sowie Einsatzzweck der unterschiedlichen Varianten des Verfahrens.
Informationen zur Durchführung des Cyber-Sicherheits-Checks und der sich anschließenden Berichtserstellung finden Sie in einem Handlungsleitfaden. Dort sind auch die Bezüge dieses Prüfverfahrens zum IT-Grundschutz und weiteren wichtigen Standards zur Informationssicherheit beschrieben.

Behandlung der Prüfergebnisse

Die **Ergebnisse** aller Überprüfungen müssen **dokumentiert** und der **Leitung mitgeteilt** werden. Diese benötigt insbesondere Informationen über den Stand der Umsetzung, Erfolge und auch Probleme sowie Risiken aufgrund von Umsetzungsmängeln. Bei Abweichungen von der Planung müssen Vorschläge erarbeitet werden, wie diese anzupassen oder die Umsetzung zu korrigieren ist. Gleiches gilt für Vorschläge zur Verbesserung und Weiterentwicklung der Sicherheitsmaßnahmen. Alle Entscheidungen hierzu, auch die Übernahme von Risiken durch eine verzögerte Umsetzung von Maßnahmen, müssen dokumentiert werden.

Standard-Anforderungen, die Berichte an die Leitungsebene erfüllen SOLLTEN, werden im Baustein ISMS.1 *Sicherheitsmanagement* des IT-Grundschutz-Kompendiums unter ISMS.1.A12 *Management-Berichte zur Informationssicherheit* beschrieben.

Lerneinheit 9.3: Kennzahlen

Kennzahlen können als Indikator für die Güte des gesamten Sicherheitsprozesses oder einzelner Teilprozesse und -aspekte dienen. Sie sind ein bewährtes Instrument in der Kommunikation mit der Leitung einer Institution über Erfolge, aber auch Probleme der Informationssicherheit.

Die folgende Tabelle enthält für verschiedene Schichten des IT-Grundschutz-Kompendiums ein Beispiel für eine mögliche Kennzahl. Diese Beispiele zeigen auch, dass mit Kennzahlen sowohl technische als auch organisatorische Aspekte der Informationssicherheit erfasst werden können.

Baustein	Anforderung	Kennzahl
ISMS.1 *Sicherheitsmanagement*	Die Leitungsebene SOLLTE regelmäßig über den Stand der Informationssicherheit informiert werden.	Anzahl der Leitungsmeetings mit Sicherheitsreport / Anzahl aller Leitungsmeetings
ORP.2 *Personal*	Aufgaben und Zuständigkeiten von Mitarbeitern SOLLTEN in geeigneter Weise dokumentiert sein.	Anzahl der Mitarbeiterverträge mit Verpflichtung zur sicheren Handhabung von Informationen / Anzahl aller Mitarbeiterverträge
CON.3 *Datensicherungskonzept*	Die Datensicherung und ein möglicherweise vorzunehmender Restore SOLLTEN regelmäßig getestet werden.	Anzahl erfolgreicher Tests / Gesamtzahl der Tests zur Wiederherstellung gesicherter Daten
OPS.1.1.2 *Ordnungsgemäße IT-Administration*	Die Befugnisse, Aufgaben und Pflichten der IT-Administratoren SOLLTEN in einer Arbeitsanweisung oder Richtlinie verbindlich festgeschrieben werden.	Anzahl von Arbeitsanweisungen / Anzahl aller Administratoren
DER.1 *Detektion von sicherheitsrelevanten Ereignissen*	Die gesammelten Ereignismeldungen der IT-Systeme und Anwendungssysteme SOLLTEN auf einer zentralen Protokollinfrastruktur aufbewahrt werden.	Anzahl zentral gesammelter Ereignismeldungen / Anzahl aller Ereignismeldungen
APP.1.1 Office-*Produkte*	Neue Office-Produkte SOLLTEN vor dem Einsatz auf Kompatibilität mit etablierten Arbeitsmitteln getestet werden.	Anzahl der eingesetzten getesteten Office-/ Produkte / Anzahl aller eingesetzten Office-Produkte
SYS.1.1 *Allgemeiner Server*	Ablauf, Rahmenbedingungen und Anforderungen an administrative Aufgaben sowie die Aufgabentrennungen zwischen den verschiedenen Rollen der Benutzer des IT-Systems SOLLTEN in einem Benutzer- und Administrationskonzept festgeschrieben werden.	Anzahl von Servern mit detailliertem Administrationskonzept / Anzahl aller Server

Tabelle 20: Beispiele für Kennzahlen zur Informationssicherheit

Diese Beispiele verdeutlichen, dass für eine umfassende Bewertung der Informationssicherheit eine Vielzahl an Kennzahlen nötig ist. Erhebung, Berechnung und Aufbereitung der Kennzahlen erfordern unter Umständen einen sehr hohen Aufwand, wobei technische Kennzahlen oft automatisiert erhoben werden können und damit der bei ihnen anfallende Aufwand meist geringer ist als bei organisatorischen Kennzahlen.

Damit der Aufwand in einem angemessenen Verhältnis zum Ergebnis steht, ist es wichtig, dass die Ziele der Kennzahlen klar formuliert und der erforderliche Aufwand für die Erhebung der Messwerte gut abgeschätzt werden. Wenn Sie planen, in Ihrer Institution Kennzahlen zur Informationssicherheit einzuführen, empfiehlt es sich, zunächst mit wenigen Kennzahlen zu starten und diese dann mit Hilfe der gewonnenen Erfahrungen Schritt für Schritt zu ergänzen.

Lerneinheit 9.4: Reifegradmodelle

Einen sehr umfassenden Blick auf die Qualität des Informationssicherheitsprozesses können Sie mit Hilfe eines Reifegradmodells erhalten. Hierzu muss das ISMS über Jahre hinweg analysiert und bewertet werden. Der Maßstab für die „Reife“ des gesamten ISMS oder aber auch Teilen hiervon ist der **Grad der Strukturierung und der systematischen Steuerung** des Prozesses.

Folgende Tabelle zeigt ein Beispiel für die **Definition von Reifegraden**.

Reifegrad	Kennzeichen
0	Es existiert kein Prozess, es gibt auch keine Planungen hierzu.
1	Es gibt Planungen zur Etablierung eines Prozesse, jedoch keine Umsetzungen.
2	Teile des Prozesse sind umgesetzt, es fehlt jedoch an systematischer Dokumentation.
3	Der Prozess ist vollständig umgesetzt und dokumentiert.
4	Der Prozesse wird darüber hinaus auch regelmäßig auf Effektivität überprüft.
5	Zusätzlich sind Maßnahmen zur kontinuierlichen Verbesserung vorhanden.

Tabelle 21: Beispiel für die Definition von Reifegraden

Ziel der Anwendung eines Reifegradmodells ist es, die Qualität aller Teilbereiche des ISMS zu erhöhen. Durch regelmäßige Analysen können Sie überprüfen, welche Prozesse noch unzureichend gesteuert sind.

Die folgende Grafik stellt beispielhaft die erreichten Reifegrade verschiedener Themenfelder in einer Institution dar. Dort wo der Reifegrad niedrig ist, besteht ein besonderer Handlungsbedarf. Reifegradmodelle können folglich dabei unterstützen, Schwerpunkte für die Weiterentwicklung eines ISMS zu setzen.

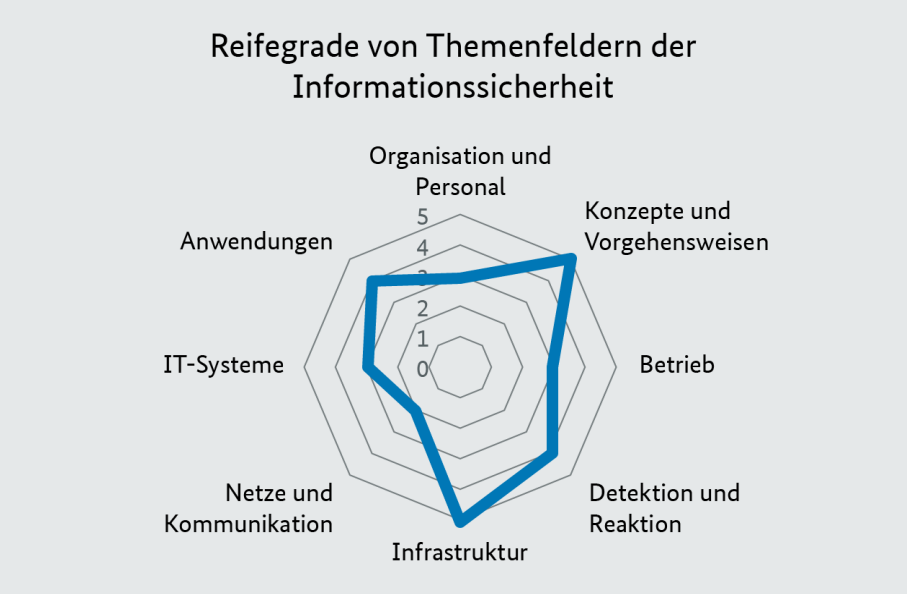


Abbildung 17: Beispiel für die Visualisierung von Reifegraden

Lerneinheit 9.5: IT-Grundschutz-Zertifizierung

Allgemein anerkannte Zertifikate setzen **Maßstäbe** und schaffen **Vertrauen**. Auch im Bereich der Informationssicherheit sind verlässliche Standards wünschenswert, die den Anwendern Orientierung zur Sicherheit von Produkten, Systemen und Verfahren bieten. Daher gibt es bereits seit vielen Jahren international anerkannte Kriterienwerke, auf deren Grundlage die Sicherheitseigenschaften von Produkten und Systemen durch unabhängige Zertifizierungsstellen bestätigt werden können.

Das **ISO 27001-Zertifikat auf Basis von IT-Grundschutz** belegt in besonderer Weise das Bemühen um Informationssicherheit, da Grundlage für die Vergabe nicht nur die Erfüllung der allgemeinen Anforderungen der Norm ISO 27001 an das Sicherheitsmanagement ist, sondern auch die nachgewiesene Umsetzung der wesentlich konkreteren Anforderungen des IT-Grundschutzes.

Die Zertifizierung des Managements für Informationssicherheit kann für **unterschiedliche Zielgruppen** interessant sein, zum Beispiel für

- Anbieter im E-Commerce oder E-Government, die verdeutlichen wollen, dass sie sorgfältig und sicherheitsbewusst mit den Daten der Kunden und Bürger umgehen,
- IT-Dienstleister, die mit einem allgemein anerkannten Maßstab die Sicherheit ihrer Dienstleistungen belegen wollen,
- Unternehmen und Behörden, die mit anderen Einrichtungen kooperieren wollen und Informationen über deren Sicherheitsniveau wünschen.

Ein Zertifizierungsverfahren wirkt aber auch **nach innen**: Es trägt dazu bei, das Bewusstsein der Mitarbeiter für die Notwendigkeit von Informationssicherheit zu stärken, und erleichtert dadurch auch die Umsetzung erforderlicher Sicherheitsmaßnahmen.

Der Zertifizierungsprozess

Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf Basis von IT-Grundschutz ist der Nachweis, dass ein den Anforderungen der Norm entsprechendes **Informationssicherheitsmanagement** eingerichtet ist und die **IT-Grundschutz-Anforderungen** wirksam erfüllt sind. Gegenstand der Zertifizierung muss dabei nicht die gesamte Institution sein. Der betrachtete Informationsverbund kann sich auch auf einzelne Geschäftsprozesse, Fachaufgaben oder Organisationseinheiten beschränken. Diese müssen jedoch sinnvoll abgegrenzt sein und eine gewisse Mindestgröße haben.

Die folgende Abbildung veranschaulicht den **Zertifizierungsprozess**:

Abbildung 18: ISO 27001-Zertifizierung auf Basis von IT-Grundschutz - Prozess

Für den Nachweis, dass die Anforderungen erfüllt sind, ist ein Audit durch einen unabhängigen, vom BSI anerkannten Auditor erforderlich. Jedes Audit setzt sich grundsätzlich aus zwei getrennten, aufeinander aufbauenden Phasen zusammen:

- **Phase 1** umfasst eine **Dokumentenprüfung** der so genannten Referenzdokumente des Antragstellers. Dazu zählen neben den geltenden Sicherheitsrichtlinien (Leitlinie zur Informationssicherheit, Richtlinien zur Risikoanalyse, Richtlinie zur internen ISMS-Auditierung) und dem Risikobehandlungsplan insbesondere auch die Ergebnisdokumente der verschiedenen Phasen der Sicherheitskonzeption (Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, IT-Grundschutz-Check, Risikoanalyse, Realisierungsplanung).
- In **Phase 2** folgt die **Umsetzungsprüfung** durch den Auditor, bei der die Vollständigkeit, Korrektheit, und Wirksamkeit der in den Referenzdokumenten beschriebenen Maßnahmen sowie deren Konformität zu den Anforderungen von ISO 27001 und IT-Grundschutz im Fokus stehen.

Ein Zertifikat wird nur erteilt, wenn der Auditbericht ein positives Gesamtvotum aufweist und durch die Zertifizierungsstelle akzeptiert wurde. Im Rahmen einer Prüfbegleitung wird der Auditbericht gegen die Vorgaben des vom BSI veröffentlichen Zertifizierungsschemas geprüft.

Ein erteiltes Zertifikat ist **drei Jahre lang gültig** und muss in diesem Zeitraum durch ein **jährliches Überwachungsaudit** bestätigt werden.

Das der ISO 27001-Zertifizierung auf Basis von IT-Grundschutz zugrunde liegende Zertifizierungsschema, Hinweise zu den erforderlichen Referenzdokumenten und alle weiteren wichtigen Informationen zum Thema finden Sie in einem eigenen Unterthema gebündelt auf der Website des BSI.

Lerneinheit 9.6: Testfragen

Wir sind am Ende der Lektion angekommen. Wenn Sie möchten, können Sie anhand der folgenden Testfragen Ihre Kenntnisse zum Thema „Aufrechterhaltung und Verbesserung der Informationssicherheit“ überprüfen. Es können mehrere Antwortmöglichkeiten zutreffend sein.

1 **Warum sollten Sie Ihr Sicherheitskonzept regelmäßig überprüfen?**

a weil sich die Gefährdungslage ändert

b weil sich die Prozesse und Strukturen einer Institution ändern

c weil sich die Zielsetzungen und Prioritäten einer Institution ändern

d weil die IT-Sicherheitsbranche ständig neuen Trends unterliegt

2 **Welche Kriterien sollten Sie bei der Überprüfung Ihres Sicherheitskonzepts berücksichtigen?**

a die Aktualität des Sicherheitskonzepts

b den Umfang des Sicherheitskonzepts

c die Akzeptanz des Sicherheitskonzepts bei der Leitung der Institution

d die Vollständigkeit des Sicherheitskonzepts

3 **Welche Vorteile bieten Reifegradmodelle für die Bewertung eines ISMS?**

a Mit einem Reifegradmodell können der Grad der Strukturiertheit und das Maß der systematischen Steuerung eines Prozesses bewertet werden.

b Die Anwendung eines Reifegradmodells ist Voraussetzung für den Erwerb eines IT-Grundschutz-Zertifikats.

c Ein Reifegradmodell kann auf Teilaspekte des ISMS angewendet werden und Defizite bei einzelnen Prozessen abbilden.

d Durch Anwendung eines Reifegradmodells wird eine zentrale Forderung der Norm ISO 27001 erfüllt.

4 **Welche Voraussetzungen müssen für den Erwerb eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz erfüllt sein?**

a ausschließlich die in einem Audit nachgewiesene Erfüllung der Basis-Anforderungen

b die durch Sichtung von Dokumenten und Vor-Ort-Prüfungen begründete Feststellung der erfolgreichen Erfüllung der IT-Grundschutz-Anforderungen durch einen zertifizierten Auditor

c ein positives Resultat bei der Überprüfung des Audit-Berichts durch das BSI

d die Unterschrift eines zertifizierten Auditors unter die Selbsterklärung einer Institution, dass sie die IT-Grundschutz-Anforderungen umfassend erfüllt hat

5 **Welche der folgenden Untersuchungen haben die systematische Überprüfung der Informationssicherheit in einer Institution zum Ziel?**

a die Auswertung von IT-Sicherheitsvorfällen

b Penetrationstests

c die IT-Sicherheitsrevision

d ein Audit im Rahmen einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz

6 **Was sollte vor der Einführung einer Kennzahl zur Informationssicherheit unbedingt festgelegt werden?**

a welches Ziel mit der Kennzahl verfolgt werden soll

b mit welchen Stilmitteln positive und negative Ergebnisse gekennzeichnet werden sollen

c mit welchem Verfahren die Werte eine Kennzahl erhoben werden

d wie die Ergebnisse vor der Leitung der Institution verborgen werden können

Ausblick

Sie sind jetzt am Ende des Online-Kurses IT-Grundschutz angelangt. Wir hoffen, Sie haben einen guten Einblick in die IT-Grundschutz-Methodik und die Anwendung des IT-Grundschutz-Kompendiums bekommen.

Weitere Informationen und Hilfestellungen rund um den IT-Grundschutz finden Sie auf den umliegenden Seiten, Fragen und Anregungen zum Thema können Sie gerne telefonisch oder per E-Mail an uns richten (Ansprechpartner und Adressen).

Anhang: Lösungen zu den Testfragen

Zutreffende Aussagen sind als [**richtig**] gekennzeichnet.

Zu Lektion 2: Sicherheitsmanagement

1 **Welches Modell liegt dem in BSI-Standard 200-1 beschriebenen Sicherheitsprozess zugrunde?**

a ein Zyklus aus den Schritten Plan, Do, Check und Act [**richtig**]

b ein Verfahren zur Definition eines State-of-the-Art-Informationssicherheitsniveaus

c ein auf stetige Verbesserung angelegtes Modell [**richtig**]

d ein Modell aus technischen Sicherheitsmaßnahmen

2 **Was sollte eine Leitlinie zur Informationssicherheit enthalten?**

a detaillierte technische Vorgaben für die Konfiguration wichtiger IT-Systeme

b Aussagen zur Bedeutung der Informationssicherheit für die betroffene Institution [**richtig**]

c grundlegende Regelungen zur Organisation der Informationssicherheit [**richtig**]

d konkrete Verhaltensregelungen für den Umgang mit vertraulichen Informationen

3 **Welche Aufgaben haben üblicherweise Informationssicherheitsbeauftragte?**

a die Entwicklung von Sicherheitskonzepten zu koordinieren [**richtig**]

b die eingesetzte Sicherheitstechnik zu konfigurieren

c der Leitungsebene über den Stand der Informationssicherheit zu berichten [**richtig**]

d Presseanfragen zum den Stand der Informationssicherheit im Unternehmen zu beantworten

4 **Wie setzt sich ein IS-Management-Team geeignet zusammen?**

a Aus jeder Abteilung des Unternehmens oder der Behörde werden Mitarbeiter entsandt, damit alle Bereich gut vertreten sind.

b Nur der IT-Leiter ordnet einige Mitarbeiter in das Team ab.

c Die Zusammensetzung sollte auf Freiwilligkeit beruhen. Jeder der Interesse hat, wird aufgenommen.

d Die Geschäftsleitung setzt das Team aus Verantwortlichen für bestimmte IT-Systeme, Anwendungen, Datenschutz und IT-Service und (sofern vorhanden) dem ICS-ISB zusammen. [**richtig**]

5 **Wer ist für die Freigabe der Leitlinie zur Informationssicherheit verantwortlich?**

a das IS-Management-Team

b der ISB

c die Unternehmens- oder Behördenleitung [**richtig**]

d die Öffentlichkeitsabteilung eines Unternehmens oder einer Behörde

6 **Warum kann es sinnvoll sein, sich für eine Sicherheitskonzeption gemäß der Basis-Absicherung zu entscheiden?**

a Die Erfüllung der zugehörigen Anforderungen reicht in der Regel für ein normales Unternehmen völlig aus.

b Weil schnell Informationssicherheit umgesetzt werden muss und die Basis-Absicherung hierfür einen geeigneten Einstieg bietet. [**richtig**]

c Weil Informationssicherheit Schritt für Schritt umgesetzt werden soll. Mittelfristig kann das Sicherheitskonzept nach Standard-Absicherung ausgebaut werden. [**richtig**]

d Weil die hochwertigen Informationen dringend geschützt werden müssen. Die Basis-Absicherung sorgt für den angemessenen Schutz der „Kronjuwelen" einer Institution.

Zu Lektion 3: Strukturanalyse

1 **Welche Ziele verfolgt die Strukturanalyse im Rahmen der IT-Grundschutz-Methodik?**

a die Identifizierung der Objekte, die besonders stark gefährdet sind

b die Ermittlung der Objekte, die in einem Sicherheitskonzept zu berücksichtigen sind [**richtig**]

c die angemessene Zusammenfassung von Objekten, für die gleiche Sicherheitsmaßnahmen angewendet werden können [**richtig**]

d die Ermittlung der Objekte, für die es passende Bausteine im IT-Grundschutz-Kompendium gibt

2 **Welche Informationen sollten Netzpläne enthalten, die für die Strukturanalyse benötigt werden?**

a die bei der Erarbeitung des Sicherheitskonzepts beteiligten Organisationseinheiten

b die Art der Vernetzung der IT-Systeme eines Informationsverbundes [**richtig**]

c die Außenverbindungen des Netzes eines Informationsverbundes [**richtig**]

d die Art der IT-Systeme eines Informationsverbundes [**richtig**]

3 **Wann bietet es sich an, IT-Systeme bei der Strukturanalyse zu gruppieren?**

a wenn diese den gleichen Schutzbedarf und ähnliche Eigenschaften (Betriebssystem, Netzanbindung, unterstützte Anwendungen) haben [**richtig**]

b wenn es für diese Systeme eigene und geeignete Bausteine im IT-Grundschutz-Kompendium gibt

c wenn diese in denselben Räumlichkeiten untergebracht sind

d wenn die Anzahl der insgesamt erfassten Objekte zu groß zu werden droht

4 **Welche der folgenden Aufgaben gehört gemäß BSI-Standard 200-2 zur Strukturanalyse?**

a die angemessene Gruppierung der Komponenten eines Informationsverbundes [**richtig**]

b die Modellierung der Geschäftsprozesse und Fachaufgaben eines Informationsverbundes

c die Überprüfung, ob die eingesetzte IT die Geschäftsprozesse und Fachaufgaben angemessen unterstützt

d die Erhebung der Informationen, Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und räumlichen Gegebenheiten eines Informationsverbundes [**richtig**]

5 **Welche Angaben sind für IT-Systeme bei der Strukturanalyse zu erfassen?**

a Typ und Einsatzzweck [**richtig**]

b Lieferant und Preis

c Benutzer und Administrator [**richtig**]

d Standort (Gebäude und Raum) [**richtig**]

6 **Welche Anwendungen sind in der Strukturanalyse zu erfassen?**

a alle Anwendungen, die auf den IT-Systemen im Informationsverbund installiert sind

b alle Anwendungen, die für mindestens einen der bereits erfassten Geschäftsprozesse erforderlich sind [**richtig**]

c alle Anwendungen, für die eine gültige Lizenz vorhanden ist

d alle Anwendungen, die von mindestens 20 Prozent der Mitarbeiter genutzt werden

Zu Lektion 4: Schutzbedarfsfeststellung

1 **Welche klassischen Schutzziele werden bei der Schutzbedarfsfeststellung gemäß IT-Grundschutz empfohlen?**

a Authentizität

b Verfügbarkeit [**richtig**]

c Vertraulichkeit [**richtig**]

d Integrität [**richtig**]

2 **In welchen Fällen können Sie gemäß IT-Grundschutz-Methodik auf die Schutzbedarfsfeststellung für ein IT-System verzichten?**

a wenn das IT-System spätestens innerhalb von 18 Monaten ausgesondert wird

b wenn das IT-System nicht eingesetzt wird [**richtig**]

c wenn die Anwendungen, die es unterstützt, nur einen normalen Schutzbedarf haben

d wenn der Schutzbedarf bereits im Rahmen einer vor einem Jahr durchgeführten Revision festgestellt wurde

3 **Welche Kriterien berücksichtigen Sie bei der Bestimmung des Bedarfs an Verfügbarkeit eines IT-Systems?**

a die maximal tolerierbare Ausfallzeit des IT-Systems [**richtig**]

b den Aufwand, der erforderlich ist, um das IT-System nach einer Beschädigung wiederherzustellen

c die Anzahl der Benutzer des IT-Systems

d die Anschaffungskosten des IT-Systems

4 **Was berücksichtigen Sie, wenn Sie den Schutzbedarf einer Anwendung bestimmen?**

a die Informationen, die im Zusammenhang mit der Anwendung verwendet werden [**richtig**]

b die Bedeutung der Anwendung für die Geschäftsprozesse oder Fachaufgaben [**richtig**]

c die relevanten Gefährdungen, denen die Anwendung ausgesetzt ist

d die räumliche Umgebung des IT-Systems, das die Anwendung bereitstellt

5 **Unter welchen Bedingungen kann der Schutzbedarf eines IT-Systems bezüglich Verfügbarkeit geringer sein als derjenige der Anwendungen, für die es eingesetzt wird?**

a wenn der Buchwert des IT-Systems einen zuvor definierten Schwellwert unterschreitet

b wenn das IT-System nur solche Teile der Anwendungen bedient, die einen geringeren Schutzbedarf haben [**richtig**]

c wenn mindestens ein weiteres redundantes IT-System in Betrieb ist, das die betreffenden Anwendungen bereitstellen kann [**richtig**]

d wenn die Anwendungen innerhalb der nächsten drei Monate so umstrukturiert werden sollen, dass das betreffende IT-System nicht mehr benötigt wird

6 **Wenn bei der Schutzbedarfsfeststellung für ein IT-System Kumulationseffekte berücksichtigt werden, bedeutet dies, dass ...**

a ... sich der Schutzbedarf des IT-Systems erhöht, weil sich Einzelschäden zu einem höheren Gesamtschaden addieren. [**richtig**]

b ... sich der Schutzbedarf des IT-Systems verringert, weil geeignete, sich gegenseitig verstärkende Sicherheitsmaßnahmen im Einsatz sind.

c ... sich der für das IT-System festgestellte Schutzbedarf auch auf den Schutzbedarf anderer IT-Systeme auswirkt, die mit dem betreffenden IT-System vernetzt sind.

d ... der Schutzbedarf des IT-Systems erst festgestellt werden kann, wenn der Schutzbedarf der mit diesem vernetzten IT-Systeme festgestellt ist.

Zu Lektion 5: Modellierung

1 **Welche Aufgaben stellen sich Ihnen bei der Modellierung gemäß IT-Grundschutz?**

a Sie bilden den in der Strukturanalyse dokumentierten Informationsverbund mithilfe der IT-Grundschutz-Bausteine ab. [**richtig**]

b Sie entwerfen die Sicherheitsarchitektur des betrachteten Informationsverbundes.

c Sie merken Zielobjekte, die nicht geeignet modelliert werden können, für eine Risikoanalyse vor. [**richtig**]

d Sie prüfen, welche IT-Grundschutz-Bausteine für den betrachteten Informationsverbund relevant sind. [**richtig**]

2 **Welche Informationen sind Bestandteil eines IT-Grundschutz-Bausteins?**

a Angaben zur spezifischen Gefährdungslage [**richtig**]

b Beschreibungen zu Standard-Sicherheitsmaßnahmen

c Verweise auf weiterführende Informationen [**richtig**]

d Sicherheitsanforderungen zu einem gegebenen Sachverhalt [**richtig**]

3 **Welche Aufgaben stellen sich Ihnen, nachdem Sie bei der Modellierung festgelegt haben, welche Bausteine für den Informationsverbund und seine einzelnen Zielobjekte anzuwenden sind?**

a die Festlegung von Maßnahmen, mit denen die Anforderungen erfüllt werden können [**richtig**]

b die Prüfung, ob für einzelne Anforderungen, deren Umsetzung im gegebenen Anwendungskontext mit vertretbarem Aufwand nicht möglich ist, Alternativen erforderlich sind [**richtig**]

c die Korrektur der Schutzbedarfsfeststellung für Zielobjekte, bei denen die Erfüllung der Anforderungen unrealistisch erscheint

d die Dokumentation der Ergebnisse der Modellierung [**richtig**]

4 **Worauf sollten Sie bei der Auswahl und Anpassung der Sicherheitsmaßnahmen auf Basis der Anforderungen achten?**

a auf die Wirtschaftlichkeit der Maßnahmen [**richtig**]

b auf die Wirksamkeit der Maßnahmen [**richtig**]

c auf den Innovationsgrad der Maßnahmen

d auf die Benutzerfreundlichkeit der Maßnahmen [**richtig**]

5 **Welche Aussagen zur Anwendung von Bausteinen auf Server sind korrekt?**

a Der Baustein SYS.1.1 *Allgemeiner Server* ist nur dann anzuwenden, wenn es keinen betriebssystemspezifischen Baustein für einen Server gibt.

b Neben dem Baustein SYS.1.1 *Allgemeiner Server* ist immer auch der zutreffende betriebssystemspezifische Baustein anzuwenden. [**richtig**]

c Wenn es spezielle Bausteine für Server-Anwendungen (z. B. Web- oder Datenbankserver) gibt, muss der betriebssystemspezifische Baustein nicht angewendet werden.

d Für Virtualisierungsserver müssen neben dem Baustein sowohl der Baustein SYS.1.1 *Allgemeiner Server* als auch der zutreffende betriebssystemspezifische Baustein angewendet werden.[**richtig**]

6 **Auf welche Zielobjekte ist bei der Modellierung der Baustein ISMS.1 *Sicherheitsmanagement* anzuwenden?**

a Er MUSS gesondert auf jeden größeren Standort eines Informationsverbundes angewendet werden.

b Er MUSS einmal angewendet werden, und zwar auf den gesamten Informationsverbund. [**richtig**]

c Er ist nur relevant, wenn der Informationsverbund eine gewisse Mindestgröße hat.

d Er MUSS für jedes Teilnetz gesondert angewendet werden, das bei der Strukturanalyse identifiziert wurde.

Zu Lektion 6: IT-Grundschutz-Check

1 **Welche Aussagen zum IT-Grundschutz-Check sind zutreffend?**

a Ein IT-Grundschutz-Check ermöglicht, Defizite bei der Erfüllung von Sicherheitsanforderungen zu ermitteln. [**richtig**]

b Bei einem IT-Grundschutz-Check wird lediglich die Erfüllung der Basis-Anforderungen geprüft.

c Ein IT-Grundschutz-Check dient dazu, Sicherheitsprobleme zu identifizieren, die in einer Risikoanalyse genauer untersucht werden müssen.

d Ein IT-Grundschutz-Check ist ein Soll-Ist-Vergleich zwischen Sicherheitsanforderungen und tatsächlich umgesetzten Sicherheitsmaßnahmen. [**richtig**]

2 **Welche Vorarbeiten erfordert der IT-Grundschutz-Check?**

a die Festlegung eines Zeitplans [**richtig**]

b die Auswahl von geeigneten Gesprächspartnern [**richtig**]

c einen Penetrationstest, um Schwachstellen zu identifizieren, die mit den ausgewählten Gesprächspartnern erörtert werden

d die Zusammenstellung und Lektüre der vorhandenen Dokumente zur Informationssicherheit in dem betrachteten Informationsverbund [**richtig**]

3 **Welche Verfahren nutzen Sie, um in einem IT-Grundschutz-Check zu prüfen, wie gut eine Gruppe von Clients geschützt ist?**

a Sie führen Interviews mit den zuständigen Systembetreuern. [**richtig**]

b Sie versuchen in einem Penetrationstest, Schwachstellen dieser IT-Systeme zu ermitteln, und beziehen dabei sämtliche zur Gruppe gehörenden Clients ein.

c Sie untersuchen stichprobenartig vor Ort, wie die Clients konfiguriert sind. [**richtig**]

d Sie lesen die vorhandene Dokumentation zur Konfiguration der Clients. [**richtig**]

4 **Wann bewerten Sie beim IT-Grundschutz-Check eine Anforderung eines IT-Grundschutz-Bausteins als erfüllt?**

a wenn zu der Anforderung geeignete Maßnahmen vollständig, wirksam und angemessen umgesetzt sind [**richtig**]

b wenn der Gesprächspartner Ihnen glaubhaft versichert hat, dass es bislang zu keinen Sicherheitsproblemen auf dem betreffenden IT-System gekommen ist

c wenn es eine umfangreiche Dokumentation zu den Schutzvorkehrungen für das betreffende IT-System gibt

d wenn sowohl im Interview mit einem für das IT-System Zuständigen als auch bei einer stichprobenartigen Überprüfung keine Sicherheitsmängel festgestellt wurden [**richtig**]

5 **Wie verfahren Sie beim ersten IT-Grundschutz-Check, also vor der Durchführung von Risikoanalysen, mit Anforderungen für den erhöhten Schutzbedarf?**

a Sie stufen diese Anforderungen grundsätzlich als entbehrlich ein und verzichten auch dann darauf, diese zu überprüfen, wenn sie in Ihrer Einrichtung umgesetzt sind.

b Sie streichen die Anforderungen aus Ihrem Sollkonzept.

c Sie betrachten Anforderungen für den hohen und sehr hohen Schutzbedarf erst nach Abschluss der Risikoanalyse. [**richtig**]

d Sie betrachten im IT-Grundschutz-Check grundsätzlich alle in den IT-Grundschutz-Bausteinen genannten Anforderungen, folglich auch diejenigen für den erhöhten Schutzbedarf.

6 **Sie stellen fest, dass eine Standard-Anforderung für ein IT-System nicht umgesetzt ist, das nur noch kurze Zeit in Betrieb ist. Wie behandeln Sie diese Anforderung beim IT-Grundschutz-Check?**

a Sie streichen die Anforderung aus dem IT-Grundschutz-Modell.

b Sie dokumentieren diese als entbehrlich, da ihre Umsetzung nicht mehr wirtschaftlich ist.

c Sie dokumentieren diese als nicht erfüllt, und merken gegebenenfalls an, dass geprüft werden muss, ob Maßnahmen zur Behebung dieses Defizits angesichts der kurzen Einsatzzeit des IT-Systems noch angemessen sind. [**richtig**]

d Sie dokumentieren diese als nicht erfüllt und merken an, dass geprüft werden muss, ob die daraus resultierenden Risiken in der Restlaufzeit des IT-Systems noch tragbar sind. [**richtig**]

Zu Lektion 7: Risikoanalyse

1 **Wer trägt die Verantwortung für die bei einer Risikoanalyse getroffenen Entscheidungen zu einem IT-System?**

a der Administrator des IT-Systems

b die Leitung der Institution [**richtig**]

c der Informationssicherheitsbeauftragte

d das IS-Management-Team

2 **Welche Gefährdungen werden bei der Erstellung der Gefährdungsübersicht im ersten Schritt betrachtet?**

a die im Anhang von BSI-Standard 200-3 enthaltenen Risikokataloge

b die relevanten elementaren Gefährdungen aus dem IT-Grundschutz-Kompendium [**richtig**]

c die im Anhang der Norm ISO 27005 angeführten Gefährdungen

d die in den Abschnitten zur Gefährdungslage eines Bausteins angeführten spezifischen Gefährdungen

3 **Was bewerten Sie bei der Risikoeinschätzung?**

a die Häufigkeit des Eintretens einer Gefährdung [**richtig**]

b das mit einer Gefährdung verbundene Schadensausmaß [**richtig**]

c welche Schutzziele von einer Gefährdung betroffen sind

d die Wirksamkeit der geplanten und umgesetzten Maßnahmen gegen eine Gefährdung

4 **Wodurch verlagern Sie ein Risiko?**

a durch den Abschluss einer Versicherung [**richtig**]

b durch Outsourcing des risikobehafteten Geschäftsprozesses an einen externen Dienstleister [**richtig**]

c durch Umstrukturierung des risikobehafteten Geschäftsprozesses

d durch die Entscheidung, risikomindernde Maßnahmen erst dann umzusetzen, wenn die hierzu erforderlichen Finanzmittel bereitstehen

5 **Aus welchen Gründen kann es gerechtfertigt sein, auch ein hohes Risiko zu akzeptieren?**

a Der Aufwand für mögliche Schutzmaßnahmen ist unangemessen hoch. [**richtig**]

b Vergleichbare Institutionen akzeptieren das Risiko ebenfalls.

c Es gibt keine wirksamen Schutzmaßnahmen gegen das Risiko. [**richtig**]

d Es ist bislang noch zu keinem nennenswerten Sicherheitsvorfall aufgrund der dem Risiko zugrunde liegenden Gefährdung gekommen.

6 **Wann ist die Risikoakzeptanz grundsätzlich unzulässig?**

a bei der Nichterfüllung von Basis-Anforderungen [**richtig**]

b beim Vorhandensein von elementaren Gefährdungen

c bei sehr hohem Schutzbedarf

d bei Nichterfüllung von Standard-Anforderungen

Zu Lektion 8: Umsetzungsplanung

1 **Was müssen Sie prüfen, wenn Sie die Umsetzung von Sicherheitsmaßnahmen planen?**

a welche begleitenden Maßnahmen für eine erfolgreiche Umsetzung erforderlich sind [**richtig**]

b ob die betreffende Maßnahme bereits eingeführt ist

c ob die Maßnahme mit anderen Maßnahmen vereinbar ist [**richtig**]

d in welcher Reihenfolge die verschiedenen Maßnahmen umgesetzt werden sollen [**richtig**]

2 **Welche Informationen aus dem IT-Grundschutz-Kompendium unterstützen Sie bei der Festlegung einer sinnvollen Umsetzungsreihenfolge der geplanten Maßnahmen?**

a die fünfstufige Kennziffer zur Angabe der Priorität einer Anforderung in den IT-Grundschutz-Bausteinen

b die Aufteilung der Anforderungen in Basis- und Standard-Anforderungen sowie solchen für den höheren Schutzbedarf [**richtig**]

c der Vorschlag zur Kennzeichnung einer sinnvollen Bearbeitungsreihenfolge der Bausteine mithilfe der Kürzel R1, R2 und R3 [**richtig**]

d die Darstellung der Gefährdungslage am Beginn eines Bausteins

3 **Was unternehmen Sie als Informationssicherheitsbeauftragter, wenn die Leitung Ihrer Institution nicht bereit ist, den Aufwand für eine bestimmte Sicherheitsmaßnahme zu tragen?**

a Sie verdeutlichen ihr, welche Risiken mit dem Fehlen der Maßnahme verbunden sind. [**richtig**]

b Sie bitten die Leitung, durch Unterschrift zu bestätigen, dass sie die damit verbundenen Gefahren kennt und trägt. [**richtig**]

c Sie ignorieren die Leitung und setzen die Maßnahme trotzdem um.

d Sie verzichten auf eine unmittelbare Reaktion, nehmen sich aber vor, nach Ablauf einer gewissen Zeitspanne die Zustimmung der Leitung einzuholen.

4 **Wer sollte in der Regel technische Maßnahmen zur Absicherung eines bestimmten IT-Systems umsetzen?**

a die Leitung der IT-Abteilung

b der Informationssicherheitsbeauftragte

c der zuständige Systemadministrator [**richtig**]

d der Benutzer des IT-Systems

5 **Wer sollte üblicherweise prüfen, ob eine Sicherheitsmaßnahme wie geplant umgesetzt ist?**

a die Geschäftsführung

b der Informationssicherheitsbeauftragte [**richtig**]

c der zuständige IT-Administrator

d die Leitung der IT-Abteilung

6 **Welches Hilfsmittel im IT-Grundschutz-Kompendium können Sie verwenden, um Ihrer Leitung zu verdeutlichen, welche Risiken die Nichterfüllung von Anforderungen mit sich bringt?**

a das Restrisikodeklarationsformular im Anhang des Kompendiums

b die Kreuzreferenztabellen am Ende eines Bausteins [**richtig**]

c das Risikokalkulationsschema in der Übersicht der elementaren Gefährdungen

d die Beispiele für eine erfolgreiche Sensibilisierung im Baustein ORP.3 *Sensibilisierung und Schulung*

Zu Lektion 9: Aufrechterhaltung und Verbesserung

1 **Warum sollten Sie Ihr Sicherheitskonzept regelmäßig überprüfen?**

a weil sich die Gefährdungslage ändert [**richtig**]

b weil sich die Prozesse und Strukturen einer Institution ändern [**richtig**]

c weil sich die Zielsetzungen und Prioritäten einer Institution ändern [**richtig**]

d weil die IT-Sicherheitsbranche ständig neuen Trends unterliegt

2 **Welche Kriterien sollten Sie bei der Überprüfung Ihres Sicherheitskonzepts berücksichtigen?**

a die Aktualität des Sicherheitskonzepts [**richtig**]

b den Umfang des Sicherheitskonzepts

c die Akzeptanz des Sicherheitskonzepts bei der Leitung der Institution

d die Vollständigkeit des Sicherheitskonzepts [**richtig**]

3 **Welche Vorteile bieten Reifegradmodelle für die Bewertung eines ISMS?**

a Mit einem Reifegradmodell können der Grad der Strukturiertheit und das Maß der systematischen Steuerung eines Prozesses bewertet werden. [**richtig**]

b Die Anwendung eines Reifegradmodells ist Voraussetzung für den Erwerb eines IT-Grundschutz-Zertifikats.

c Ein Reifegradmodell kann auf Teilaspekte des ISMS angewendet werden und Defizite bei einzelnen Prozessen abbilden. [**richtig**]

d Durch Anwendung eines Reifegradmodells wird eine zentrale Forderung der Norm ISO 27001 erfüllt.

4 **Welche Voraussetzungen müssen für den Erwerb eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz erfüllt sein?**

a ausschließlich die in einem Audit nachgewiesene Erfüllung der Basis-Anforderungen

b die durch Sichtung von Dokumenten und Vor-Ort-Prüfungen begründete Feststellung der erfolgreichen Erfüllung der IT-Grundschutz-Anforderungen durch einen zertifizierten Auditor [**richtig**]

c ein positives Resultat bei der Überprüfung des Audit-Berichts durch das BSI [**richtig**]

d die Unterschrift eines zertifizierten Auditors unter die Selbsterklärung einer Institution, dass sie die IT-Grundschutz-Anforderungen umfassend erfüllt hat

5 **Welche der folgenden Untersuchungen haben die systematische Überprüfung der Informationssicherheit in einer Institution zum Ziel?**

a die Auswertung von IT-Sicherheitsvorfällen

b Penetrationstests

c die IT-Sicherheitsrevision [**richtig**]

d ein Audit im Rahmen einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz [**richtig**]

6 **Was sollte vor der Einführung einer Kennzahl zur Informationssicherheit unbedingt festgelegt werden?**

a welches Ziel mit der Kennzahl verfolgt werden soll [**richtig**]

b mit welchen Stilmitteln positive und negative Ergebnisse gekennzeichnet werden sollen

c mit welchem Verfahren die Werte eine Kennzahl erhoben werden [**richtig**]

d wie die Ergebnisse vor der Leitung der Institution verborgen werden können