Bundesamt
für Sicherheit in der
Informationstechnik

Webkurs IT-Grundschutz

IT-Grundschutz
im Selbststudium

Ausgabe April 2011
Druckversion zum Webkurs

Der IT-Grundschutz bietet eine bewährte Methode, Informationssicherheit zu planen und zu überprüfen. Als Einstieg bietet das BSI den **Webkurs IT-Grundschutz** an. Ein etwa vierstündiges Selbststudium ermöglicht Ihnen, eigene Sicherheitskonzepte gemäß IT-Grundschutz anzufertigen. Dieses Dokument enthält eine Druckversion zum Webkurs.

Grundlagen:
BSI-Standard 100-1: *Managementsysteme für Informationssicherheit (ISMS)*, Version 1.5, 2008
BSI-Standard 100-2: *IT-Grundschutz-Vorgehensweise (ISMS), Version 2.0*, 2008
BSI-Standard 100-3: *Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5*, 2008
IT-Grundschutz-Kataloge, 11. Ergänzungslieferung, November 2009

Der Webkurs IT-Grundschutz wurde im Auftrag des BSI vom Fraunhofer-Institut für Sichere Informationstechnologie SIT, Bereich Anwendungs- und Prozesssicherheit APS, Sankt Augustin, entwickelt. Internet: www.sit.fraunhofer.de.

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat 114 - IT-Sicherheitsmanagement und IT-Grundschutz
Postfach 20 03 63
53133 Bonn
Telefon: 0228 99 9582-5369
Telefax: 0228 99 9582-5405
E-Mail: grundschutz@bsi.bund.de
Internet: www.bsi.bund.de

Inhaltsverzeichnis

Kapitel 1: Warum IT-Grundschutz?.....1
1.1 Überblick.....1
1.2 Warum Informationssicherheit?.....2
1.2.1 Gefahrenpotenziale und Sicherheitsmängel.....2
1.2.2 Sicherheitsmängel – Lösungen.....4
1.2.3 Überprüfte Passwörter, Regelungen, Infrastruktur? – Übungsfragen.....4
1.3 IT-Grundschutz und Informationssicherheit.....6
1.3.1 Einstieg.....6
1.3.2 Inhalt der BSI-Standards.....8
1.3.3 Inhalt der IT-Grundschutz-Kataloge.....9
1.4 Aufbau des Kurses.....10
Kapitel 2: Sicherheitsmanagement.....13
2.1 Überblick.....13
2.2 Sicherheitsprozess.....14
2.3 Managementmängel und Maßnahmen.....15
2.4 Rollen und Zuständigkeiten.....16
2.4.1 IT-Sicherheitsbeauftragte.....16
2.4.2 IS-Management-Team.....16
2.4.3 Beispiel: Sicherheitsorganisation im Unternehmen.....17
2.5 Sicherheitsleitlinie.....19
2.5.1 Vorgehen.....19
2.5.2 Aussagen in einer Leitlinie zur Informationssicherheit.....20
2.6 Sicherheitskonzept.....22
2.6.1 Vorgehen.....22
2.6.2 Fragen zum Sicherheitskonzept.....23
2.6.3 Umsetzung des Sicherheitskonzepts.....24
2.7 Test zum Informationssicherheitsmanagement.....25
Kapitel 3: Strukturanalyse.....27
3.1 Überblick.....27
3.2 Erhebung der Informationen, Geschäftsprozesse und Anwendungen.....28
3.2.1 Vorgehen.....28
3.2.2 Beispiel.....30

3.3 Erhebung des Netzplans....32
3.3.1 Ausgangsplan....32
3.3.2 Gruppenbildung....33
3.3.3 Beispiel für Gruppenbildung....34
3.4 Erhebung der IT-Systeme....36
3.5 Erhebung der räumlichen Gegebenheiten....38
3.6 Test zur Strukturanalyse....40
Kapitel 4: Schutzbedarfsfeststellung....42
4.1 Überblick....42
4.2 Schutzbedarfskategorien....43
4.2.1 Definition....43
4.2.2 Abgrenzung der Schutzbedarfskategorien....44
4.2.3 Schutzbedarf und Schutzziele....45
4.3 Schutzbedarfsfeststellung für die Anwendungen....46
4.4 Schutzbedarfsfeststellung für die IT-Systeme....47
4.5 Schutzbedarfsfeststellung für die Kommunikationsverbindungen....48
4.5.1 Kritische Verbindungen....48
4.5.2 Beispiel für kritische Verbindungen....48
4.6 Schutzbedarfsfeststellung für die Räume....50
4.7 Abstimmung mit der Geschäftsleitung....51
4.8 Test zur Schutzbedarfsfeststellung....51
Kapitel 5: Modellierung nach IT-Grundschutz....53
5.1 Überblick....53
5.2 Bausteine....54
5.3 Schichtenmodell....55
5.4 Vorgehen bei der Modellierung....57
5.4.1 Schichten 1 und 2....57
5.4.2 Vorgehen bei der Modellierung – Schichten 3 bis 5....58
5.5 Prüfung auf Vollständigkeit....59
5.6 Test zur Modellierung....60
Kapitel 6: Basis-Sicherheitscheck....62
6.1 Überblick....62
6.2 Hinweise zu den Maßnahmen....63
6.2.1 Zertifikatsrelevanz der Maßnahmen....63

6.2.2 Bestandteile einer Maßnahme....64
6.2.3 Konkrete und generische Maßnahmen....66
6.2.4 Maßnahmen für Planungsphasen....67
6.2.5 Zusammenfassung der Hinweise zu den Maßnahmen....68
6.3 Vorgehen beim Basis-Sicherheitscheck....68
6.3.1 Empfehlungen....68
6.3.2 Dokumentation....69
6.4 Beispiel....71
6.5 Test zum Basis-Sicherheitscheck....72
Kapitel 7: Risikoanalyse....74
7.1 Überblick....74
7.2 Ergänzende Sicherheitsanalyse....75
7.3 Risikoanalyse – traditionelles Vorgehen und Ansatz des BSI....76
7.4 Erstellung der Gefährdungsübersicht....78
7.5 Ermittlung zusätzlicher Gefährdungen....79
7.6 Bewertung der Gefährdungen....80
7.7 Behandlung der Risiken....82
7.7.1 Risikostrategien – Alternativen....82
7.7.2 Dokumentation der gewählten Risikostrategie....83
7.8 Abschließende Arbeiten....84
7.9 Test zur Risikoanalyse....84
Kapitel 8: Realisierungsplanung....86
8.1 Überblick....86
8.2 Schritte 1 und 2....87
8.3 Schritte 3 bis 5....88
8.4 Schritt 6....90
8.5 Beispiel für einen Realisierungsplan....91
8.6 Aufrechterhaltung und Verbesserung der Informationssicherheit....92
8.7 Test zur Realisierungsplanung....93
Kapitel 9: Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz....95
9.1 Warum Zertifizierung?....95
9.2 Zertifizierungsprozess....95
9.3 Zusammenfassung....97

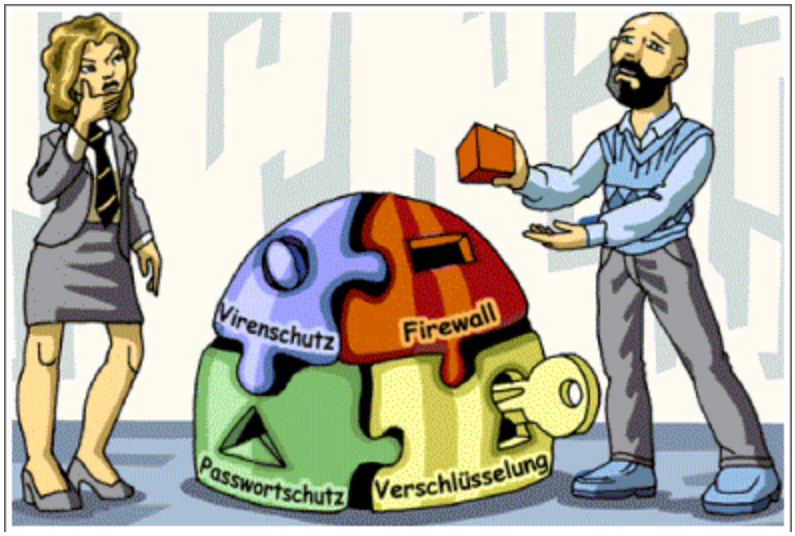
Anhang 1: Auflösungen zu den Tests.....99
Lösungen zu Kapitel 2: Sicherheitsmanagement.....99
Lösungen zu Kapitel 3: Strukturanalyse.....101
Lösungen zu Kapitel 4: Schutzbedarfsfeststellung.....103
Lösungen zu Kapitel 5: Modellierung gemäß IT-Grundschutz.....105
Lösungen zu Kapitel 6: Basis-Sicherheitscheck.....107
Lösungen zu Kapitel 7: Risikoanalyse.....109
Lösungen zu Kapitel 8: Realisierungsplanung.....111
Anhang 2: Kontakte.....113

Kapitel 1: Warum IT-Grundschutz?

1.1 Überblick

Für die wesentlichen Geschäftsprozesse nahezu aller Unternehmen und Behörden ist es heutzutage unerlässlich, dass benötigte **Informationen** korrekt vorliegen und vertraulich behandelt werden. Entsprechend wichtig ist folglich auch, dass die unterstützende **Informationstechnik** reibungslos funktioniert und **wirksame Schutzvorkehrungen** gegen die vielfältigen und immer wieder neuartigen Gefährdungen für die Sicherheit von Informationen, Anwendungen, IT-Systemen und Kommunikationsnetzen getroffen werden.

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



Wenn Sie eine dieser Fragen mit „Ja“ beantworten, dann sollten Sie sich mit dem **IT-Grundschutz** beschäftigen. Dieser bietet eine weithin anerkannte und effiziente **Vorgehensweise**, mit der Sie Ihr Sicherheitskonzept entwickeln und überprüfen können. Er enthält darüber hinaus Empfehlungen für **Maßnahmen**, mit denen auf kostengünstige Weise ein für übliche Einsatzbereiche und Schutzanforderungen angemessenes und bei höherem Schutzbedarf leicht ausbaufähiges Sicherheitsniveau erreicht werden kann.

Dieser Kurs hilft Ihnen dabei, die **IT-Grundschutz-Vorgehensweise zu verstehen und anzuwenden**.

Zu den verwendeten Piktogrammen

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

Besonders wichtige Textteile, z. B. Merksätze und Empfehlungen, sind durch ein Ausrufezeichen hervorgehoben.

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

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

Mit diesem Zeichen eingeleitete Texte empfehlen Ihnen Hilfsmittel z. B. Formulare oder Programme, mit denen Sie Ihre eigenen Ausarbeitungen unterstützen können.

Daneben gibt es zwei Piktogramme, die auf weiterführende Informationen in den grundlegenden Dokumenten des Bundesamts für Sicherheit in der Informationstechnik zum IT-Grundschutz aufmerksam machen:

Dieses Symbol verweist auf die ausführlichen Beschreibungen in den BSI-Standards zur Informationssicherheit und zum IT-Grundschutz zu einem gegebenen Sachverhalt.

In Absätzen, die mit diesem Symbol eingeleitet werden, finden Sie Hinweise auf ergänzende Informationen in den IT-Grundschutz-Katalogen.

1.2 Warum Informationssicherheit?

1.2.1 Gefahrenpotenziale und Sicherheitsmängel

Sicherheit gibt es nicht zum Nulltarif. Sie kostet Zeit und Geld. Doch viel mehr Aufwand kann entstehen, wenn Schäden behoben werden müssen, die bei besseren Schutzvorkehrungen leicht hätten vermieden werden können.

Die regelmäßig veröffentlichten Lageberichte des BSI zur Informationssicherheit in Deutschland und zahlreiche weitere Quellen zeigen, dass die Informationstechnik von Unternehmen, Behörden und auch Privatanwendern nach wie vor hochgradig gefährdet ist. Die heutzutage für Unternehmen und Behörden gleichermaßen unverzichtbare Internetanbindung bedeutet beispielsweise auch ein hohes Risiko für die Vertraulichkeit, Integrität und Verfügbarkeit der internen Netze und der dort vorhandenen Informationen. Die Internetkriminalität wird stetig professioneller, Schadsoftware immer ausgefeilter, Angriffe auf die Verfügbarkeit von Servern und Netzen nehmen zu und gewinnen an

Intensität, der Abstand zwischen der Entdeckung einer Sicherheitslücke in Betriebssystemen oder Anwendungssoftware und deren Ausnutzung für Angriffe wird zunehmend kleiner.

Sicherheitsvorfälle können vielfältige Ursachen haben und drohen nicht nur im Internet. Oft sind die Betroffenen zu wenig dafür sensibilisiert, Gefahren zu erkennen. Es fehlen technische und organisatorische Vorkehrungen zur Vorbeugung und Vermeidung von Schäden. Nicht selten sind gesetzlichen Auflagen, etwa zum Datenschutz, betriebsinterne Richtlinien oder vertragliche Verpflichtungen unbekannt und werden vorsätzlich oder fahrlässig missachtet.

Erkennen Sie mögliche Sicherheitslücken in allen mit Informationstechnik ausgestatteten Bereichen? Finden Sie diese auch in den Regelungen, Konzepten und organisatorischen Vorkehrungen für Informationssicherheit?

Versuchen Sie im folgenden Bild Gefährdungen für die Informationssicherheit in Büros und Serverraum herauszufinden.

Ein Tipp: Insgesamt sind neun Sicherheitslücken oder mögliche Gefahren durch Vernachlässigung üblicher Sicherheitsvorschriften dargestellt.

1.2.2 Sicherheitsmängel – Lösungen

An welche Risiken denken Sie im Hinblick auf die rot markierten Situationen?

1. Türen und Fenster stehen offen: Rechner und Zubehör könnten aus den Räumen gestohlen werden.
2. Der Bildschirm und damit möglicherweise auch vertrauliche Informationen können von Unbefugten eingesehen werden.
3. Ein Zettel mit Passwörtern ist sichtbar und könnte von Unbefugten missbraucht werden.
4. Eine mit „Save“ beschriftete und damit deutlich als Sicherung gekennzeichnete DVD liegt zugänglich herum.
5. Ausdrucke und Kopien mit vertraulichen Daten liegen an Druckern und Kopierern.
6. Rechner mit direkter Verbindung an das Internet können den Schutz des Netzes durch die zentrale Firewall aushebeln.
7. Durch private Datenträger (im Bild eine DVD) kann Schadsoftware in das Unternehmensnetz gelangen.
8. Austretende Flüssigkeiten gefährden die Hardware.
9. Rauchen bedeutet Brandgefahr.

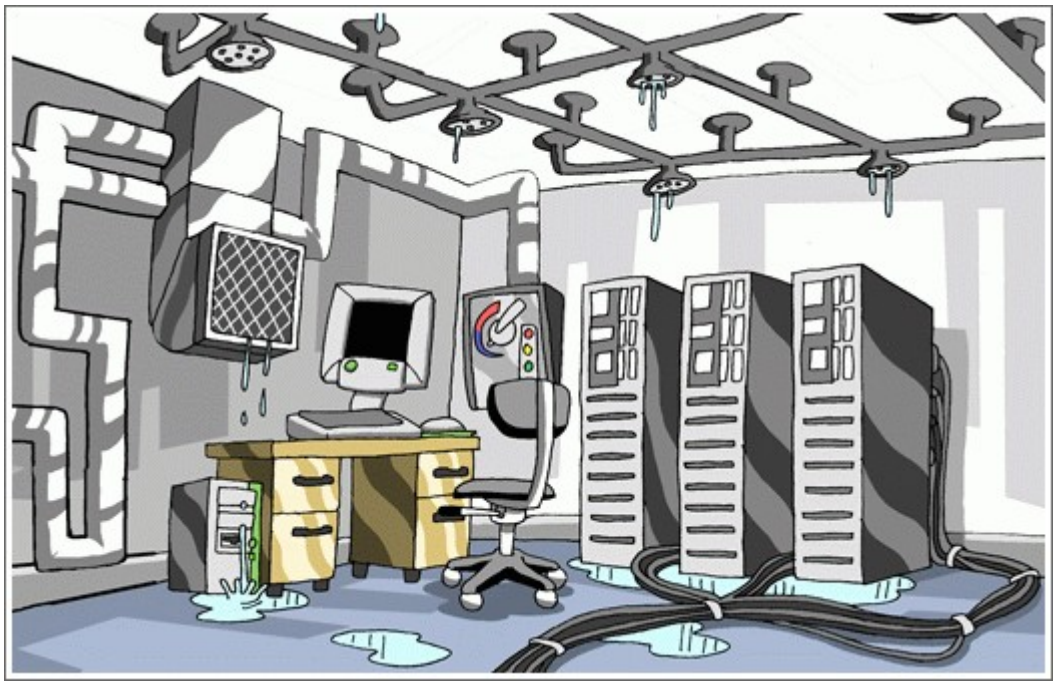
1.2.3 Überprüfte Passwörter, Regelungen, Infrastruktur? – Übungsfragen

Informationssicherheit betrifft nicht nur die **IT-Systeme**, sondern auch die **Organisation**, das **Personal**, die **räumliche Infrastruktur**, die **Arbeitsplätze** und die **Betriebsabläufe**.

Natürlich haben die erfahrenen Zuständigen für Informationssicherheit die in dem Suchbild gezeigten Sicherheitsprobleme rasch herausgefunden. Aber nicht alle Sicherheitsprobleme sind derart offensichtlich. Und selbst wenn Sicherheitsschwachstellen bekannt sind, bedeutet

das noch nicht, dass diese tatsächlich auch behoben werden. Können Sie für Ihre Einrichtung beispielsweise auf die folgenden Fragen ausschließlich positive Antworten geben?

- Vornamen, Automarken, Geburtstage, der Lieblingsfußballverein – haben Sie schon einmal überprüft, wie viele Benutzer derart unsichere Passwörter wählen, da sie sich diese leichter merken können?
- Und – falls Sie Administrator sind – was ist mit Ihrem eigenen Passwort? Haben Sie es sicher beim Vorgesetzten oder Sicherheitsbeauftragten hinterlegt, damit Fehler im Netz auch behoben werden können, wenn Sie krank, auf Dienstreise oder im Urlaub sind?
- Gibt es Regelungen für die Einrichtung von Benutzern und Benutzergruppen sowie für eine angemessene Vergabe von Zugriffsrechten?
- Ist sichergestellt, dass alle Benutzer regelmäßig die Datenbanken der Virenschutzsoftware aktualisieren?
- Haben Sie Festplatten immer sicher gelöscht, ehe Sie diese zum Verschrotten gegeben haben?
- Sind wichtige Server in Ihrem Unternehmen vor Wasserschäden sicher?



- Was geschieht eigentlich mit eingehenden E-Mails an die Marketing- oder Verkaufsabteilung, wenn der zuständige Sachbearbeiter im Urlaub ist?
- Haben Sie Kollegen auch über mögliche Schäden für das Unternehmen durch „undichte Stellen“ und über Möglichkeiten, diese zu vermeiden, informiert?

Zahlreiche Statistiken belegen, dass etwa die Hälfte der sicherheitsrelevanten Vorfälle durch Mitarbeiter im Unternehmen ausgelöst wird. In den wenigsten Fällen geschieht dies absichtlich, meistens ist es Unachtsamkeit, mangelnde Ausbildung oder Leichtfertigkeit.

1.3 IT-Grundschutz und Informationssicherheit

1.3.1 Einstieg

Das Suchbild und die Fragen auf den letzten Seiten zeigen, dass Informationssicherheit mehr erfordert als den isolierten Einsatz von Sicherheitstechnik wie Virenscanner oder Verschlüsselungssoftware. Sie ist vielmehr eine Aufgabe, die professionell geplant werden und vielfältige Aspekte berücksichtigen muss, damit insbesondere auch die folgenden **Anforderungen** bewältigt werden:

- **Komplexität der Gefährdungslage:** Gefährdungen können vielfältige Ursachen haben und auf mannigfaltigen Wegen die Ziele der Informationssicherheit verletzen. Naturkatastrophen und andere Formen höherer Gewalt sind ebenso im Blick zu behalten wie gezielte Angriffe von Hackern, Fahrlässigkeiten oder technische Mängel.
- **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 sollte 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 die Abläufe einer Institution über Gebühr behindert werden.

- **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.
- **Gestiegene externe Anforderungen:** Es wird heutzutage für viele Unternehmen und Behörden immer wichtiger, nachweisen zu können, das sie in ausreichendem Maße für Informationssicherheit gesorgt haben. Dieser Nachweis fällt leichter, wenn ein Unternehmen seine Vorkehrungen für Informationssicherheit an allgemein anerkannten Standards ausrichtet.

Das **Angebot des BSI zum IT-Grundschutz** bietet eine gute Grundlage dafür, diesen Herausforderungen gerecht zu werden und die Bemühungen für Informationssicherheit zu strukturieren. Es erleichtert einem Unternehmen und Behörden, systematisch nach Sicherheitslücken zu suchen, vorhandene Sicherheitsmaßnahmen zu überprüfen und neue in ein Sicherheitskonzept einzuplanen, das zu den Geschäftsprozessen, Fachaufgaben und Organisationsstrukturen der Institution passt und darüber hinaus allgemein anerkannten Standards genügt.

IT-Grundschutz enthält zwei wesentliche Bestandteile und zwar:

- die **BSI-Standards zum IT-Grundschutz** mit Empfehlungen für den organisatorischen Rahmen sowie das methodische Vorgehen zur Gewährleistung von Informationssicherheit sowie
- die **IT-Grundschutz-Kataloge**, mit denen die in den BSI-Standards formulierten allgemeinen Empfehlungen zum Management von Informationssicherheit in Ihrem Unternehmen oder Ihrer Behörde konkretisiert und umgesetzt werden können.

Die in den BSI-Standards beschriebene **IT-Grundschutz-Vorgehensweise** bietet eine systematische Methode zur Entwicklung von Sicherheitskonzepten. In den **IT-Grundschutz-Katalogen** finden Sie Standard-Sicherheitsmaßnahmen für typische und weit verbreitete IT-Systeme, Netze und Anwendungen, deren Einsatz die Notwendigkeit für aufwändige Risikoanalysen auf ein Minimum beschränkt.

Viele Anwender verbinden mit dem Begriff IT-Grundschutz ausschließlich die umfangreichen IT-Grundschutz-Kataloge. IT-Grundschutz ist aber mehr. Das BSI bietet neben den BSI-Standards und den IT-Grundschutz-Katalogen weitere Werkzeuge an, um ein angemessenes Sicherheitsniveau zu erreichen, zum Beispiel das **GSTOOL**. Dieses Werkzeug unterstützt die gesamte Vorgehensweise nach IT-Grundschutz. Dazu gehört auch die **ISO 27001 Zertifizierung auf Basis von IT-Grundschutz**, die sowohl eine Prüfung des Informationssicherheits-managements als auch der konkreten Sicherheitsmaßnahmen auf Basis von IT-Grundschutz umfasst. Erwähnt sei auch der **„Leitfaden IT-Sicherheit“**. Hier wurde bewusst auf die Detailfülle der IT-Grundschutz-Kataloge verzichtet, um einen kompakten und allgemeinverständlichen Überblick über die wichtigsten Maßnahmen für Informationssicherheit zu schaffen. Die Webseiten des BSI zum Thema IT-Grundschutz informieren umfassend über diese und weitere nützliche Werkzeuge.

Bezug der IT-Grundschutz-Standards und IT-Grundschutz-Kataloge

Im Internetangebot des BSI finden Sie die BSI-Standards zum IT-Grundschutz unter den Stichwörtern IT-Grundschutz→IT-Grundschutz-Standards sowie die aktuelle Version der IT-Grundschutz-Kataloge unter IT-Grundschutz→IT-Grundschutz-Kataloge.

Gedruckte Ausgaben der BSI-Standards zum IT-Grundschutz und der IT-Grundschutz-Kataloge werden vom Bundesanzeiger-Verlag herausgegeben. Weitere Informationen dazu finden Sie unter IT-Grundschutz→Bezugsquellen auf den Webseiten des BSI.

1.3.2 Inhalt der BSI-Standards

Die **BSI-Standards** enthalten Empfehlungen für den organisatorischen Rahmen sowie das methodische Vorgehen zur Gewährleistung von Informationssicherheit.

BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)

Dieser Standard beschreibt, welche grundlegenden Anforderungen ein Managementsystem für Informationssicherheit (ISMS) erfüllen muss sowie 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.

BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise

stellung eines ISMS im BSI-Standard 100-1 und beschreibt mit inen effizienten Weg, die allgemeinen Anforderungen dieses Norm ISO 27001 umzusetzen.

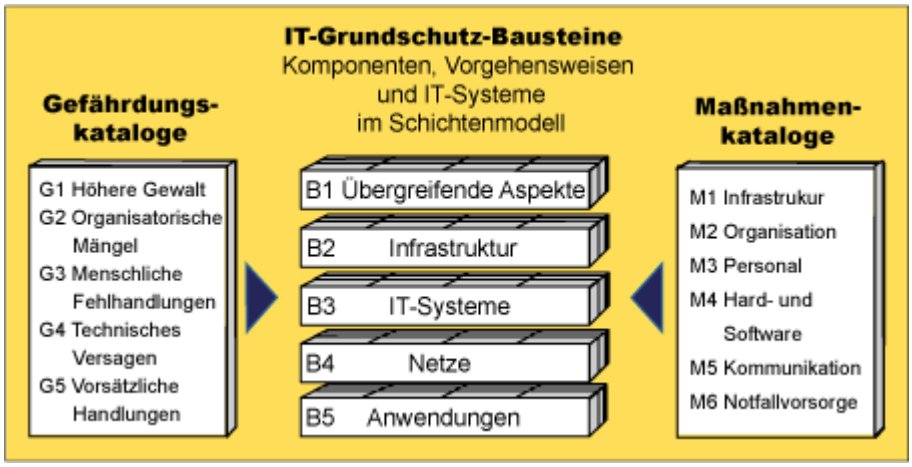
BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz

In diesem Standard ist ein gegenüber anderen Methoden vereinfachtes Verfahren zur Risikoanalyse beschrieben. Diese Methode ist immer dann wichtig und hilfreich, wenn Sie Komponenten absichern wollen, für die unter Umständen die IT-Grundschutz-Maßnahmen alleine keine ausreichende Sicherheit bieten.

BSI-Standard 100-4: Notfallmanagement

Hier wird ein systematischer Weg aufgezeigt, ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen, zu überprüfen und weiterzuentwickeln. Die an einem Lebenszyklus-Modell ausgerichteten Konzepte zielen darauf ab, die Widerstandsfähigkeit einer Institution zu erhöhen und die Kontinuität zumindest der wichtigsten Geschäftsprozesse und Fachaufgaben bei Krisen und Notfällen zu sichern.

1.3.3 Inhalt der IT-Grundschutz-Kataloge



Die nach dem Baukastenprinzip gegliederten IT-Grundschutz-Kataloge umfassen vom BSI kontinuierlich aktualisiertes Wissen, mit dem die in den BSI-Standards enthaltenen allgemeinen Empfehlungen zum Management von Informationssicherheit in Ihrem Unternehmen oder Ihrer Behörde umgesetzt werden können. Sie sind in drei Bestandteile gegliedert:

- In den **Gefährdungs-Katalogen** sind wesentliche Gefährdungen für die Informationssicherheit zusammengestellt und entlang der möglichen Ursachen „Höhere Gewalt“, „Organisatorische Mängel“, „Menschliche Fehlhandlungen“, „Technisches Versagen“ und „Vorsätzliche Handlungen“ gegliedert.
- Die **Maßnahmen-Kataloge** enthalten detailliert beschriebene, in der Praxis bewährte und meist kostengünstige Maßnahmen, mit denen Sie den möglichen Gefährdungen für die Informationssicherheit wirksam begegnen können. Sie sind in die Bereiche „Infrastruktur“, „Organisation“, „Personal“, „Hardware und Software“, „Kommunikation“ und „Notfallvorsorge“ gegliedert.
- Die **Baustein-Kataloge** bilden die Klammer zwischen Gefährdungs- und Maßnahmen-Katalogen. Sie sind in die Schichten „Übergreifende Aspekte“, „Infrastruktur“, „IT-Systeme“, „Netze“ und „Anwendungen“ sortiert. Ein Baustein beschreibt jeweils einen bestimmten Teilaspekt der

Informationssicherheit. Dies kann ein technisches System, ein zu regelnder organisatorischer Sachverhalt oder eine Anwendung sein. Jeder Baustein enthält neben einer kurzen Darstellung seines Anwendungsgebiets Zusammenstellungen der für den beschriebenen Sachverhalt relevanten Gefährdungen und empfohlenen Schutzmaßnahmen.

Mit den IT-Grundschutz-Katalogen können Sie den Aufwand für die Entwicklung eines Sicherheitskonzepts deutlich reduzieren, da es in vielen Fällen genügt, die auf den ausgewählten Einsatzzweck zutreffenden Bausteine auszuwählen (siehe *Kapitel 5: Modellierung nach IT-Grundschutz*) sowie die darin enthaltenen Maßnahmen einzuplanen und konsequent umzusetzen, um ein angemessenes Sicherheitsniveau zu erzielen.

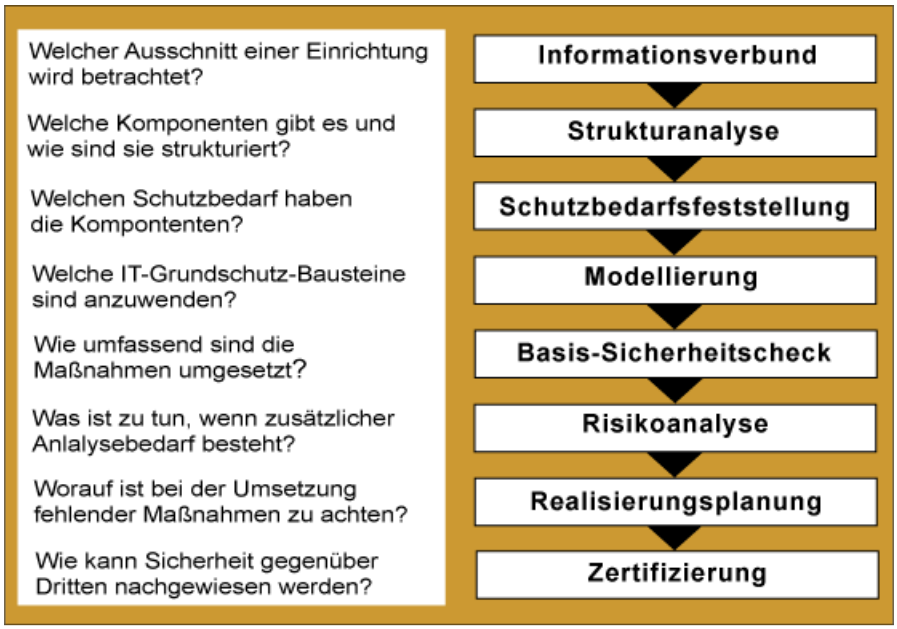
1.4 Aufbau des Kurses

Auf den ersten Blick können die mehrere tausend Seiten umfassenden IT-Grundschutz-Kataloge verwirrend umfangreich erscheinen. Sie müssen diese jedoch nicht von Anfang bis Ende durchlesen. Vielmehr bietet die in den BSI-Standards beschriebene IT-Grundschutz-Vorgehensweise einen Schlüssel für die Auswahl, Lektüre und Anwendung der für Ihre Einrichtung wesentlichen Bausteine.

Dieser Kurs wird Sie in den folgenden Kapiteln mit der IT-Grundschutz-Vorgehensweise vertraut machen und aufzeigen, wie Sie die IT-Grundschutz-Kataloge für Ihr Sicherheitskonzept anwenden können:

- Im Kapitel **„Sicherheitsmanagement“** wird erklärt, mit welchen organisatorischen Strukturen und Maßnahmen ein effektives Management für Informationssicherheit aufgebaut und aufrechterhalten werden kann.

Die darauf folgenden Kapitel entsprechen der IT-Grundschutz-Vorgehensweise zur Entwicklung von Sicherheitskonzepten und konzentrieren sich der Reihe nach auf folgende Fragen:



- Im Kapitel **„Strukturanalyse“** wird dargestellt, welche Informationen erfasst werden müssen, damit ein Sicherheitskonzept die wesentlichen Komponenten (Informationen, Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räumlichkeiten) seines Anwendungsbereichs (des betrachteten Informationsverbundes) hinreichend umfasst.
- Das Kapitel **„Schutzbedarfsfeststellung“** beschreibt, wie Sie den Schutzbedarf der zuvor identifizierten Komponenten bewerten und dokumentieren.
- Im Kapitel **„Modellierung“** wird gezeigt, wie die IT-Grundschutz-Bausteine genutzt werden können, um dem Schutzbedarf entsprechende Sicherheitsmaßnahmen für den Informationsverbund und dessen Komponenten zu ermitteln.
- Im Kapitel **„Basis-Sicherheitscheck“** erfahren Sie, wie Sie in einem einfachen Soll-Ist-Vergleich feststellen können, ob die erforderlichen Sicherheitsmaßnahmen umgesetzt sind und welche Defizite es noch gibt.
- Im Kapitel **„Risikoanalyse“** wird beschrieben, wie Sie mit Hilfe der in BSI-Standard 100-3 dargestellten Risikoanalyse auf Basis von IT-Grundschutz prüfen, ob für Komponenten, die möglicherweise nicht hinreichend mit den IT-Grundschutz-Maßnahmen abgesichert werden können, tatsächlich stärker wirksame oder ergänzende Sicherheitsmaßnahmen erforderlich sind oder nicht.
- Das Kapitel **„Realisierungsplanung“** gibt Hinweise dazu, worauf Sie achten sollten, damit die benötigten Sicherheitsmaßnahmen erfolgreich umgesetzt werden.
- Das Kapitel **„Zertifizierung“** informiert über die Voraussetzungen, die erfüllt sein müssen, damit das erreichte Sicherheitsniveau gegenüber Dritten mit dem ISO 27001-Zertifikat auf Basis von IT-Grundschutz nachgewiesen werden kann.

Das Beispielunternehmen RECPLAST und weitere Beispiele zum IT-Grundschutz

Die einzelnen Schritte der IT-Grundschutz-Vorgehensweise werden mithilfe eines durchgängig verwendeten Beispiels, der „RECPLAST GmbH“, veranschaulicht. Dieses fiktive Unternehmen stellt aus Recyclingmaterialien etwa 400 Kunststoffprodukte her und

vermarktet diese. Eine zusammenhängende Darstellung des Beispiels finden Sie in einem eigenen PDF-Dokument.

Auf der Webseite des BSI finden Sie weitere Beispiele zur Anwendung des IT-Grundschutzes:

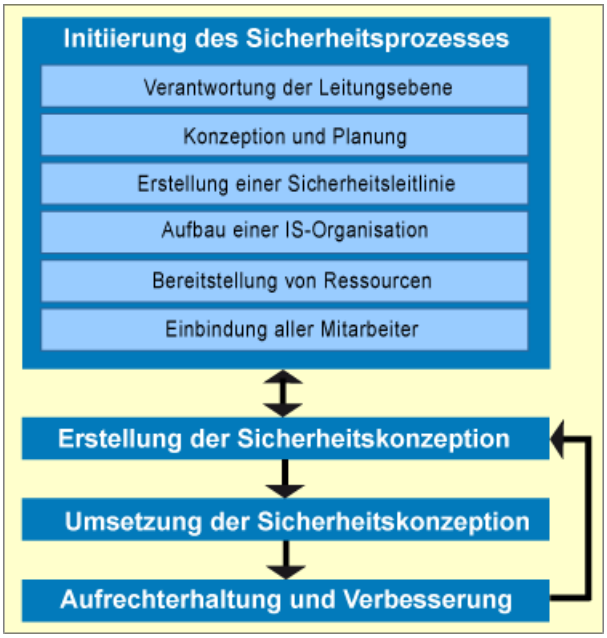
- Ein *IT-Grundschutzprofil für eine kleine Institution* ist speziell für die Anwendergruppe mit wenig IT-Systemen und geringen Sicherheitskenntnissen entwickelt worden.
- *IT-Grundschutz für den Mittelstand* richtet sich an IT-Sicherheitsbeauftragte von mittelgroßen Institutionen, die sich ausführlich mit der IT-Grundschutz-Vorgehensweise beschäftigen wollen, und gibt ein vollständiges Beispiel für den Einsatz des GSTOOLs.
- Das *IT-Grundschutzprofil für eine große Institution* stellt Lösungsvorschläge für häufig auftretende Probleme bei der IT-Grundschutz-Vorgehensweise dar, hier am Beispiel eines Rechenzentrums.
- Das *Anwendungsbeispiel für IT-Grundschutz im produzierenden Gewerbe* zeigt, wie IT-Grundschutz auch in derartigen Umgebungen angewendet werden kann.
- Als Beispiel für die Anwendung der IT-Grundschutz-Vorgehensweise auf eine Behörde dient das fiktive *Bundesamt für Organisation und Verwaltung (BOV)*.

Kapitel 2: Sicherheitsmanagement

2.1 Überblick

Aufgaben und Aktivitäten, mit denen eine Organisation ein angemessenes Sicherheitsniveau erreichen und erhalten will, gehören zum **Informationssicherheitsmanagement**, kurz IS-Management. Zuständig sind dafür Verantwortliche für die Informationssicherheit und für den IT-Betrieb sowie von diesen intern oder extern Beauftragte. Sie tragen zu dieser Aufgabe bei, indem sie **organisatorische Grundlagen** legen sowie **Sicherheitsmaßnahmen planen**, **umsetzen** und ihre Wirksamkeit **kontrollieren**.

Welche Verantwortlichkeiten und welche Prozesse haben sich dafür bewährt? Welche Aufgaben und Ergebnisse sind für Informationssicherheitsmanagement wichtig? Wie kommen die Verantwortlichen zu einer Strategie, zu Zielen, zu einem praktikablen Konzept? Wie können die umgesetzten Konzepte weiterentwickelt werden? Grundsätzliche Antworten zu diesen Fragestellungen finden Sie im BSI-Standard 100-1: *Managementsysteme für Informationssicherheit (ISMS)*.



Die dort genannten Empfehlungen werden im BSI-Standard 100-2: *IT-Grundschutz-Vorgehensweise (ISMS)* konkretisiert, wo im Einzelnen die folgenden Schritte des Sicherheitsprozesses beschrieben werden:

- **Initiierung des Sicherheitsprozesses**, für den die Leitungsebene die Verantwortung übernehmen, Ziele und Strategien formulieren, organisatorische Strukturen aufbauen und ausreichende Ressourcen bereitstellen sowie in den sie die Mitarbeiter einbinden muss,
- **Entwicklung eines Sicherheitskonzepts** gemäß IT-Grundschutz-Vorgehensweise,
- **Umsetzung** durch Beseitigung vorhandener Schwachstellen und Einführung der im Konzept vorgesehenen Maßnahmen,
- **Aufrechterhaltung** und **kontinuierliche Verbesserung** durch Prüfung von Wirksamkeit, Angemessenheit und Aktualität der vorhandenen Konzepte und eingeführten Maßnahmen.

In diesem Kapitel werden Ihnen die folgenden wichtigen Maßnahmen zur systematischen Steuerung eines Sicherheitsprozesses erläutert:

- der Aufbau einer angemessenen **Organisationsstruktur** für Informationssicherheit,
- die Formulierung der grundsätzlichen Vorgaben in einer **Leitlinie zur Informationssicherheit** und
- die Entwicklung dazu passender **Sicherheitskonzepte**.

2.2 Sicherheitsprozess

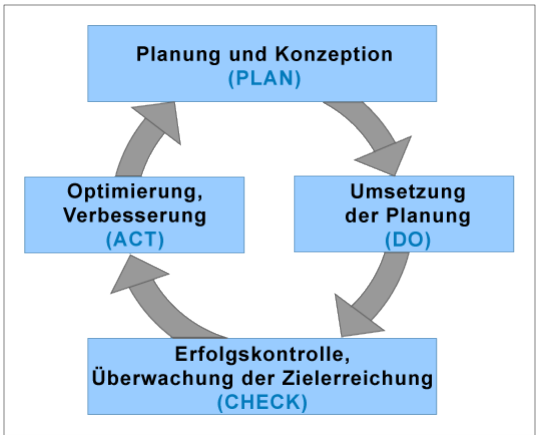
Verantwortung der Leitung

Die **Initiative zum Informationssicherheitsmanagement** muss von der Leitung (des Unternehmens oder der Behörde) ausgehen. Sie trägt die volle Verantwortung dafür, dass in der Institution gesetzliche Anforderungen und Geschäftsbedingungen eingehalten sowie interne Regelungen beachtet werden. Bei Verstößen kann sie haftbar gemacht werden. Beispielsweise sind die Vorstände größerer Kapitalgesellschaften durch das *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich* (*KonTraG*) zu einem angemessenen Risikomanagement verpflichtet.

Die Leitung sollte dementsprechend ein Interesse daran haben, dass auch die Gewährleistung der Informationssicherheit zur Unternehmenskultur gehört. Und es sollte ihr bewusst sein, dass eigenes vorbildliches Sicherheitsverhalten auch motivierend auf die Mitarbeiter wirkt.

Eine wichtige Maßnahme ist die Organisation eines für das Unternehmen **angemessenen** und von einem **gemeinsamen Verständnis** für die Bedeutung der Aufgabe getragenen **Sicherheitsmanagements**. Dieses folgt einem **zyklischen Prozess** mit den Phasen:

1. Planung,
2. Umsetzung der Planung (Durchführung des Vorhabens),
3. Erfolgskontrolle (Überwachung der Zielerreichung) und
4. Beseitigung von erkannten Mängeln und Schwächen (Optimierung und Verbesserung).



Diese Vorstellung eines Lebenszyklus basiert auf dem Modell nach Deming (PDCA-Modell nach den englisch bezeichneten Phasen PLAN, DO, CHECK und ACT), das auch in ISO 27001 und anderen Standards zur Gestaltung von Managementsystemen (zum Beispiel dem Qualitäts- oder dem Umweltmanagement) verwendet wird. Mit dieser Modellvorstellung können der gesamte Sicherheitsprozess wie auch einzelne Komponenten (etwa das Sicherheitskonzept oder die Sicherheitsorganisation) beschrieben werden.

Kontinuierliche Verbesserung

Die Gewährleistung von Informationssicherheit ist eine **strategische Aufgabe des Managements**, das **Ziele festlegen**, effiziente **Organisationsstrukturen aufbauen, Prozesse entwickeln** und angemessene **Schutzmaßnahmen umsetzen** muss. Die getroffenen Entscheidungen müssen kontinuierlich überprüft und bei Bedarf an geänderte Bedingungen angepasst werden, wenn ein bestimmtes Sicherheitsniveau gehalten werden soll. Veränderungen der inneren Strukturen einer Institution (Geschäftsprozesse, Fachaufgaben, organisatorische Gliederung) sind ebenso zu berücksichtigen wie solche in den äußeren Rahmenbedingungen (Gesetze, Verordnungen, Verträge), neuartige Bedrohungsszenarien ebenso wie Weiterentwicklungen der Sicherheitstechnik.

2.3 Managementmängel und Maßnahmen

Vermeidung von Mängeln im Management

Vor allem in kleinen Unternehmen fragen Leiter, ob es nicht ausreicht, die wichtigsten Sicherheitsprodukte von externen Firmen installieren zu lassen und von diesen mitgelieferte Anweisungen an die Beschäftigten zu verteilen. Sie fühlen sich selbst für eine Rolle im Sicherheitsmanagement überfordert. Dies ist nur eine Erscheinungsform von unzureichendem Sicherheitsmanagement. Weitere Gefährdungen wie

- fehlende persönliche Verantwortung,
- mangelnde Unterstützung durch die Leitungsebene,
- unzureichende strategische und konzeptionelle Vorgaben,
- unzureichende und fehlgeleitete Investitionen,
- unzureichende Durchsetzbarkeit von Maßnahmen und Konzepten sowie
- fehlende Aktualisierung im Sicherheitsprozess

und ihre möglichen Folgen finden Sie in den Gefährdungen G 2.66 *Unzureichendes Sicherheitsmanagement* und G 2.107 *Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement* erläutert, auf die im Baustein B 1.0 *Sicherheitsmanagement* verwiesen wird.

Solche organisatorischen Mängel können vermieden werden, wenn das Management folgende Aufgaben und Pflichten erfüllt und in der Praxis bewährte Maßnahmen umsetzt:

- Die **Leitung** des Unternehmens bzw. der Behörde ist sich ihrer **Gesamtverantwortung** und **Vorbildfunktion** für die Informationssicherheit bewusst, vertritt die Sicherheitsziele entschieden und beispielhaft, initiiert, steuert und kontrolliert einen kontinuierlichen Sicherheitsprozess und unterstützt alle zugehörigen Arbeiten.
- In Unternehmen und Behörden ist eine **eigene Kompetenz für Informationssicherheit** aufzubauen und die Hauptverantwortung für das Thema an eine Person zu delegieren, die auch für eine geeignete Organisationsstruktur für Informationssicherheit und deren Aufrechterhaltung sorgt.
- Zur Institution passende Sicherheitsziele und eine Strategie sind in einer **Leitlinie zur Informationssicherheit** festzuschreiben.
- Zur Umsetzung und Integration der angestrebten Sicherheit sind die erforderlichen **organisatorischen Strukturen** aufzubauen, ein **Sicherheitskonzept** zu erstellen, die **Mitarbeiter einzubeziehen** und die **Ressourcen** für Sicherheit **wirtschaftlich** einzusetzen.
- Zur **Aufrechterhaltung und Weiterentwicklung der Informationssicherheit** tragen zielgruppengerechte Sicherheitsrichtlinien ebenso bei wie eine umfassende Dokumentation des Prozesses, regelmäßige Überprüfungen und Statusberichte.

Wie sieht es bei Ihnen aus?

Sind in Ihrem Unternehmen (oder Ihrer Behörde) alle oben genannten Anforderungen an ein Sicherheitsmanagement erfüllt? Wenn nicht, ist es Zeit zu handeln. Halten Sie die erkannten Lücken oder Gefährdungen fest und formulieren Sie konstruktive Argumente für Verbesserungen. Versuchen Sie, der Leitung diese Vorschläge zu vermitteln.

2.4 Rollen und Zuständigkeiten

Für eine wirksame Sicherheitsorganisation empfiehlt der IT-Grundschutz,

- IT-Sicherheitsbeauftragte und
- ein IS-Management-Team

einzusetzen und mit ausreichenden Ressourcen auszustatten. Die Ausgestaltung der Sicherheitsorganisation hängt dabei von den konkreten Bedingungen der jeweiligen Institution ab, also von ihrer Größe, Beschaffenheit und Struktur.

2.4.1 IT-Sicherheitsbeauftragte

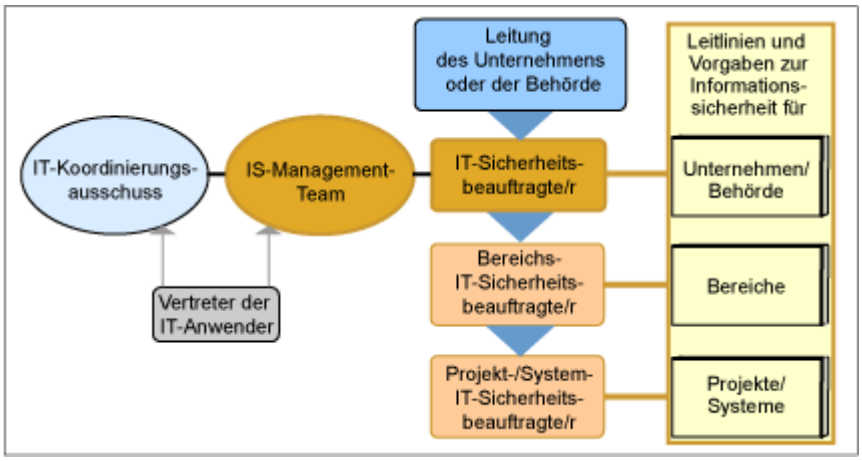
Ein IT-Sicherheitsbeauftragter ist für alle Fragen rund um die Informationssicherheit in der Organisation zuständig. Er sollte organisatorisch unabhängig sein und ein unmittelbares Vortragsrecht bei der Leitung haben. Es empfiehlt sich daher, diese Funktion als Stabsstelle der Organisationsleitung zuzuordnen.

Zu den **Aufgaben** von IT-Sicherheitsbeauftragten 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,
- den Realisierungsplan für Sicherheitsmaßnahmen zu erstellen und ihre Umsetzung zu initiieren und zu überprüfen,
- dem IS-Management-Team und der Leitungsebene über den Status der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- sicherheitsrelevante Vorfälle zu untersuchen und
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu koordinieren.

2.4.2 IS-Management-Team

In **größeren Organisationen** wird ein solches Team aus mehreren Zuständigen für Informationssicherheit gebildet, um den IT-Sicherheitsbeauftragten zu unterstützen. **Zuständig** ist es für die Regelung sämtlicher übergreifenden Belange der Informationssicherheit. Es koordiniert, berät und kontrolliert die zugehörigen Analysen, Konzepte und Richtlinien.



Im IS-Management-Team sollten der IT-Sicherheitsbeauftragte, Verantwortliche aus dem IT-Service, dem Datenschutz und Anwendungsvertreter zusammenwirken, gegebenenfalls ergänzt durch IT-Sicherheitsbeauftrage, die für einzelne Bereiche, Projekte oder IT-Systeme benannt wurden.

Für größere Koordinierungsaufgaben kann bei Bedarf zusätzlich ein **IT-Koordinierungsausschuss** die Zusammenarbeit zwischen dem IS-Management-Team, der Leitung und der Vertretung der Anwender zeitlich befristet abstimmen.

Die **Aufgaben** des IS-Management-Teams sind es,

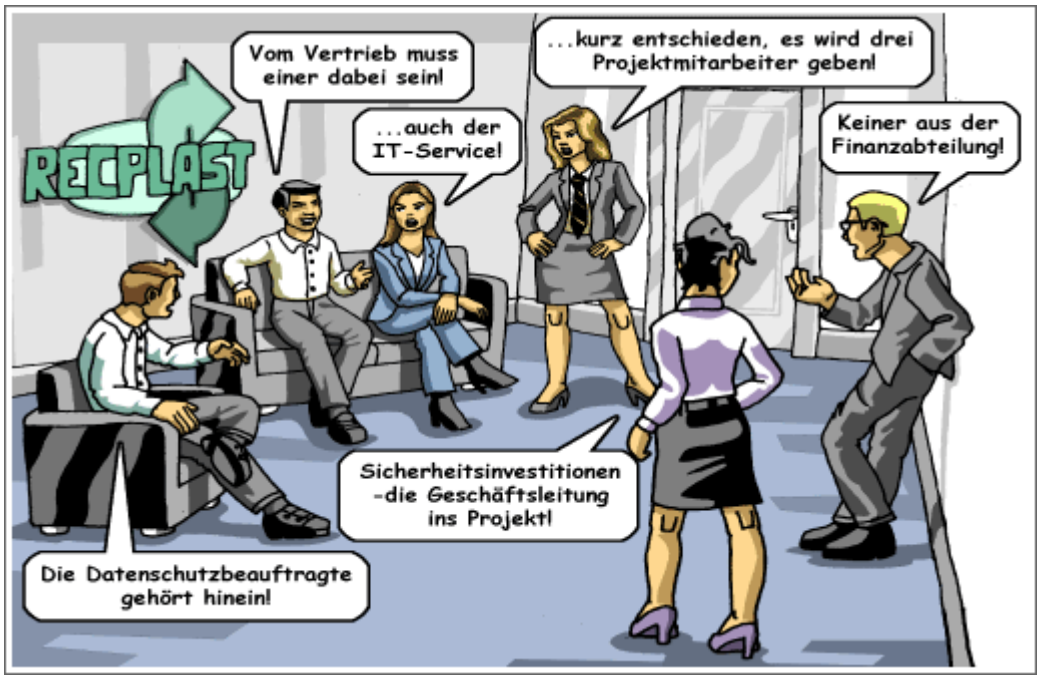
- die Sicherheitsziele und -strategien festzulegen sowie die Sicherheitsleitlinie zu entwickeln,
- die Umsetzung der Sicherheitsleitlinie zu überprüfen,
- den Sicherheitsprozess zu initiieren, zu steuern und zu kontrollieren,
- bei der Entwicklung des Sicherheitskonzepts mitzuwirken,
- zu überprüfen, ob die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen wie beabsichtigt funktionieren sowie geeignet und wirksam sind,
- Schulungs- und Sensibilisierungsprogramme für Informationssicherheit zu konzipieren sowie
- den IT-Koordinierungsausschuss und die Leitungsebene zu beraten.

Diese Aufgaben können in **kleineren Organisationen** auch nur von wenigen Zuständigen oder **einer Person**, dem (oder der) **IT-Sicherheitsbeauftragten**, wahrgenommen werden.

Modelle zum Aufbau der Sicherheitsorganisation in großen, mittelgroßen und kleinen Institutionen sowie Erläuterungen zu den Aufgaben von IT-Sicherheitsbeauftragten und IS-Management-Teams finden Sie in Kapitel 3.4 *Organisation des Sicherheitsprozesses* des BSI-Standards 100-2, ferner in Maßnahme M 2.193 *Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit* der IT-Grundschutz-Kataloge.

2.4.3 Beispiel: Sicherheitsorganisation im Unternehmen

Im Beispielunternehmen RECPLAST beabsichtigt die Geschäftsführung ein **Sicherheitskonzept** für das Unternehmen ausarbeiten zu lassen, das in allen Unternehmensbereichen umgesetzt werden soll. Dazu müssen die Unternehmensgrundsätze zur Informationssicherheit und die vorhandenen Sicherheitsrichtlinien präzisiert werden.



In einem ersten Schritt wird ein IT-Sicherheitsbeauftragter ernannt, der die zugehörigen Arbeiten koordinieren soll. Da diese Aufgabe umfangreiche IT-Kenntnisse erfordert, wird hierfür ein Mitarbeiter der Abteilung „Informationstechnik“ bestimmt. 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, das Maßnahmen zur Notfallvorsorge und Benutzersensibilisierung einschließen soll, und einen zugehörigen Realisierungsplan,
3. Vorschläge für Maßnahmen zur Aufrechterhaltung der Informationssicherheit,
4. Dokumentation aller Entscheidungsvorlagen, Entscheidungen und der umgesetzten Maßnahmen des Informationssicherheitsprozesses.

Mehrere Bereichsleiter wollen, dass auch ein Mitarbeiter aus ihrem Bereich in dem Projektteam vertreten ist. Aus drei Bereichen können wegen dringender Terminarbeiten keine Mitarbeiter am Projekt teilnehmen. Die Geschäftsführung schließt diese Diskussion damit ab, dass höchstens drei Personen mitwirken sollen und zwar der IT-Sicherheitsbeauftragte, der Datenschutzbeauftragte (ein Mitarbeiter aus dem Vertrieb) sowie die kaufmännische Geschäftsleitung.

Alle Abteilungen sollen dem Projekt die erforderlichen Auskünfte über den Stand der Informationssicherheit und vorhersehbare Entwicklungen in ihrem Zuständigkeitsbereich geben. Zwischen- und Endergebnisse sollen mit dem Betriebsrat abgestimmt, von der Geschäftsführung entschieden und den Beschäftigten bekannt gegeben werden.

Übung zur Anwendung

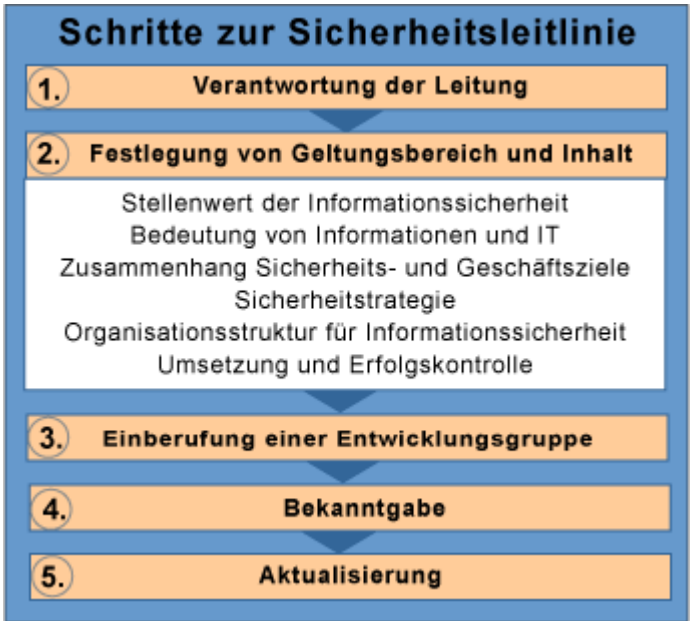
In welchen Gesichtspunkten ist der Sicherheitsprozess in Ihrem Unternehmen (oder Ihrer Behörde) anders initiiert und organisiert? Welche Vorteile und welche Nachteile sehen Sie?

2.5 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. In diesem Dokument soll für alle Mitarbeiter verständlich beschrieben werden, welche Sicherheitsziele angestrebt werden und in welchem organisatorischen Rahmen diese umgesetzt werden sollen. Die Entwicklung der Leitlinie muss von der Geschäftsführung angestoßen und aktiv begleitet werden. Möglichst viele Bereiche der Institution sollten in den Entstehungsprozess einbezogen werden. Dies erleichtert insbesondere auch, dass die Mitarbeiter die enthaltenen Vorgaben mittragen.

2.5.1 Vorgehen

Ausgearbeitet wird die Leitlinie vom IS-Management-Team (bzw. in kleinen Organisationen vom IT-Sicherheitsbeauftragten) in folgenden Schritten:



1. **Verantwortung der Behörden- bzw. Unternehmensleitung**

Es wird schriftlich festgehalten, dass die Organisationsleitung die **Gesamtverantwortung** für die Informationssicherheit hat und in vollem Umfang hinter den in der Leitlinie formulierten Zielen und den daraus abgeleiteten und abzuleitenden Konzepten und Maßnahmen steht. Diese Gesamtverantwortung gilt auch dann, wenn einzelne Aufgaben an bestimmte Mitarbeiter oder Abteilungen delegiert sind.

2. **Festlegung von Geltungsbereich und Inhalt**

Es muss klar beschrieben sein, für welche Teile (Standorte, Abteilungen, Geschäftsprozesse oder Fachaufgaben) einer Institution die Leitlinie gelten soll. Der Geltungsbereich kann auch die gesamte Einrichtung umfassen.

Folgende Sachverhalte sollten in der Sicherheitsleitlinie kurz und verständlich beschrieben sein:

- der Stellenwert der Informationssicherheit und die Bedeutung der wesentlichen Informationen und der Informationstechnik für die Aufgabenerfüllung,
- der Bezug der Sicherheitsziele zu den Geschäftszielen oder Aufgaben der Institution,
- die Sicherheitsziele und die Kernelemente der Sicherheitsstrategie,
- die Zusicherung, dass die Sicherheitsleitlinie von der Leitung durchgesetzt wird, und zusätzliche Leitaussagen zur Erfolgskontrolle sowie
- eine Beschreibung der für die Umsetzung des Sicherheitsprozesses eingeführten Organisationsstruktur.

Ergänzt werden kann die Leitlinie unter anderem durch

- die Aufzählung relevanter Gefährdungen oder einzuhaltender gesetzlicher oder vertraglicher Anforderungen,
- die Beschreibung der Aufgaben und Zuständigkeiten im Sicherheitsprozess und die Benennung von Ansprechpartnern sowie
- Hinweise auf Schulungs- und Sensibilisierungsmaßnahmen.

3. Einberufung einer Entwicklungsgruppe

Gibt es in der Institution noch kein funktionierendes IS-Management-Team, ist für die Entwicklung der Leitlinie eine Gruppe einzuberufen, die später die Funktionen eines solchen Teams weiter ausfüllen kann. In diese Gruppe sollten neben dem IT-Sicherheitsbeauftragten weitere Mitarbeiter mit Kenntnissen über Informationssicherheit, Vertreter des IT-Betriebs und der IT-Anwender sowie idealerweise auch ein Mitglied der Leitungsebene einbezogen werden.

4. Bekanntgabe der Leitlinie

Es ist Aufgabe der Behörden- oder Unternehmensleitung, sich voll hinter die Anforderungen der Leitlinie zu stellen, ihr formell zuzustimmen, sie in Kraft zu setzen und den Mitarbeitern bekannt zu geben. Dazu gehört nicht nur, sie anzukündigen, sondern auch zu ihrer Einhaltung anzuhalten. Alle Mitarbeiter sollten die Aussagen der Sicherheitsleitlinie kennen und einen einfachen Zugang zu dem Dokument haben.

5. Aktualisierung der Leitlinie

Da sich Geschäftsprozesse, dafür benötigte Informationen sowie die unterstützende Technik ändern, ist regelmäßig (z. B. alle zwei Jahre) sowie bei Bedarf zu prüfen, ob die Aussagen der Sicherheitsleitlinie noch aktuell sind. Wenn die Leitlinie an neue Anforderungen angepasst werden muss, werden alle genannten Schritte erneut durchlaufen.

2.5.2 Aussagen in einer Leitlinie zur Informationssicherheit

Bei der Formulierung der **Sicherheitsziele** und der Sicherheitsleitlinie können die folgenden Fragen hilfreich sein:

- Welche Geschäftsprozesse hat die Institution? Welche Ziele werden mit diesen verfolgt?
- Welche Informationen werden für diese Geschäftsprozesse benötigt?
- Für welche Informationen ist es besonders wichtig, Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten? Was droht, wenn diese Sicherheitsziele verletzt werden?
- Welche Bedeutung hat Informationstechnik für die Geschäftsprozesse? Für welche Prozesse ist die Abhängigkeit von einer ordnungsgemäß funktionierenden IT besonders groß?

Beispiel

Für das Beispielunternehmen sind diese Fragen in einem gesonderten Dokument beantwortet und dazu Sicherheitsziele bestimmt worden, z. B.:

1. Für die Gewährleistung der Informationssicherheit sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese sind nur dann hinreichend wirksam, wenn alle Beschäftigten die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Dies soll durch regelmäßige Fortbildungsmaßnahmen zur Informationssicherheit unterstützt werden.

2. Vertraulichkeit und Integrität der für das Unternehmen wichtigen Informationen sind zu schützen. Im Umgang mit elektronisch gespeicherten Dokumenten und Informationen ist daher den Geheimhaltungsanweisungen strikt Folge zu leisten.
3. Die für das Unternehmen relevanten Gesetze und Vorschriften sowie vertragliche und aufsichtsrechtliche Verpflichtungen müssen eingehalten werden.
4. Die Informationstechnik muss so betrieben werden, dass Geschäftsinformationen bei Bedarf hinreichend schnell verfügbar sind. Ausfälle, die zu Terminüberschreitungen von mehr als einem Tag bei der Abwicklung von Aufträgen oder anderen wichtigen Geschäftsvorhaben führen, sind nicht tolerierbar.
5. Durch unsicheren Umgang mit Informationen verursachte finanzielle Schäden und ein negatives Image für das Unternehmen müssen verhindert werden. Der Zugriff auf und der Zugang zu allen wichtigen Informationen im Unternehmen werden daher strikt geregelt und kontrolliert.

Derartige Aussagen zur Bedeutung der Informationssicherheit dokumentiert die Entwicklungsgruppe des Beispielunternehmens in ihrer Leitlinie. Zusätzlich hält sie **Aussagen zur Sicherheitsstrategie** fest, beschreibt also, was unternommen wird, um die Ziele zu erreichen, z. B.:

- Aus der Entwicklungsgruppe für die Leitlinie zur Informationssicherheit soll ein IS-Management-Team aufgebaut werden.
- Die bisher gesetzten Sicherheitsziele sollen noch verfeinert werden und die einzuhaltenden rechtlichen Anforderungen zusammengetragen werden.
- Es soll ein Sicherheitskonzept für das gesamte Unternehmen erstellt werden, das mit Hilfe der IT-Grundschutz-Vorgehensweise entwickelt wird.
- Das Sicherheitskonzept soll unter Einbeziehung aller Unternehmensbereiche in einem Jahr umgesetzt werden.
- Regelmäßige Kontrollen und Aktualisierungen des Konzepts sollen zur Aufrechterhaltung der Informationssicherheit beitragen.

Außerdem werden **organisatorische Definitionen und Regelungen** in der Sicherheitsleitlinie festgehalten, z. B.

- welche Verantwortlichkeiten für bestimmte Informationen und Systeme verteilt werden und welche Verpflichtungen damit verknüpft sind,
- wie die Verwaltung, Nutzung und Kontrolle von Informationen von Unabhängigen überprüft wird und
- welche Verstöße gegen die Sicherheitsleitlinie sanktioniert werden.

Weitere Informationen zur Entwicklung einer Leitlinie finden Sie in der Maßnahme M 2.192 *Erstellung einer Leitlinie zur Informationssicherheit*. Ein Beispieldokument finden Sie in den Musterrichtlinien und Beispielkonzepten unter den Hilfsmitteln zu den IT-Grundschutz-Katalogen.

Übungen

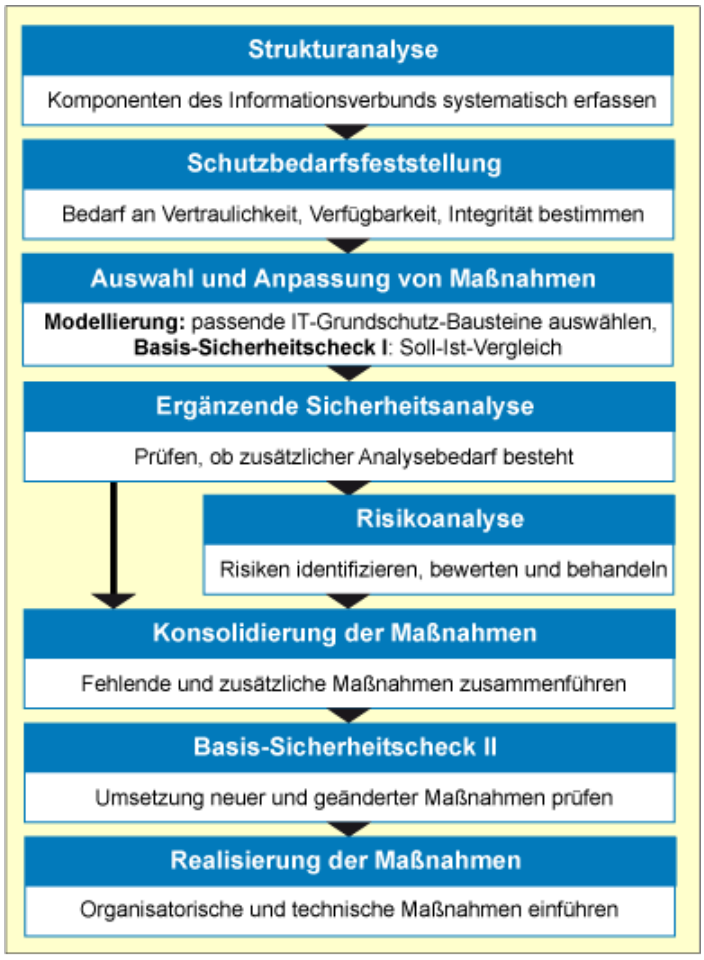
Im PDF-Dokument zum Beispielunternehmen finden Sie den Entwurf einer Sicherheitsleitlinie. Welche grundsätzlichen Sicherheitsziele sollte Ihr Unternehmen oder Ihre Behörde anstreben? Versuchen Sie für sich herauszufinden, worin sich diese Ziele von denen der RECPLAST GmbH unterscheiden. Welche Aussagen der vorgeschlagenen Leitlinie des Beispielunternehmens müssten für Ihr Unternehmen (Ihre Behörde) anders formuliert werden?

2.6 Sicherheitskonzept

Mit welchen Maßnahmen die in der Leitlinie zur Informationssicherheit vorgegebenen Ziele und Strategien verfolgt werden sollen, wird in einem Sicherheitskonzept beschrieben. Dieses Dokument wird folglich unter den organisatorischen Bedingungen, die in der Leitlinie beschrieben sind, und für das dort festgelegte anzustrebende Sicherheitsniveau erarbeitet.

2.6.1 Vorgehen

In einem Sicherheitskonzept wird auf der Grundlage einer Risikobewertung dargestellt, mit welchen Maßnahmen Informationen und Informationstechnik geschützt werden sollen. Die IT-Grundschutz-Vorgehensweise schlägt hierfür die in der folgenden Abbildung dargestellten und in den Kapiteln dieses Kurses näher beschriebenen Schritte vor:



Weitere Ausführungen zur Sicherheitskonzeption nach IT-Grundschutz finden Sie im Kapitel 8 des BSI-Standards 100-1 *Managementsysteme für Informationssicherheit (ISMS)* und im Kapitel 4 des BSI-Standards 100-2 *IT-Grundschutz-Vorgehensweise*.

Eine kurze Zusammenfassung der IT-Grundschutz-Vorgehensweise bietet auch die Maßnahme M 2.195 *Erstellung eines Sicherheitskonzepts* der IT-Grundschutz-Kataloge.

2.6.2 Fragen zum Sicherheitskonzept

Es gibt einige grundsätzliche Fragen zu den aufgezeigten Entwicklungsschritten, auf die Sie Antworten finden sollten, wenn Sie ein Sicherheitskonzept für Ihre Institution entwickeln.

1. Fragen zur Strukturanalyse

- Ist irgendwann zuvor für die Institution bereits ein Sicherheitskonzept erstellt oder aktualisiert worden?
- Gibt es eine Darstellung der Geschäftsprozesse Ihres Unternehmens oder Ihrer Behörde, aus der deutlich wird, welche Ressourcen (Informationen, technische Systeme, Personen, infrastrukturelle Gegebenheiten) diese jeweils benötigen?
- Sind Ihnen oder anderen Personen diese Dokumente zugänglich?

Derartige Zusammenstellungen erleichtern Ihnen den ersten Schritt, die **Strukturanalyse**, die systematische Zusammenstellung der Objekte, die im Sicherheitskonzept zu berücksichtigen sind.

2. Fragen zur Schutzbedarfsfeststellung

- Wie schwerwiegend kann es sich für Ihre Institution auswirken, wenn die Vertraulichkeit, die Integrität oder die Verfügbarkeit von Informationen, Anwendungen und technischen Systemen verletzt werden?
- Bei welchen der Objekte, die in der Strukturanalyse identifiziert wurden, sind solche Verletzungen besonders schwerwiegend?

Bei der **Schutzbedarfsfeststellung** ermitteln Sie auf die konkreten Bedingungen Ihrer Institution zugeschnitten, wie viel Schutz Informationen und Informationstechnik tatsächlich benötigen.

3. Fragen zur Auswahl und Anpassung von Maßnahmen

- Wie können die IT-Grundschutz-Kataloge auf eine Institution angewendet werden? Welche Bausteine sind relevant? Wann müssen Maßnahmen ergänzt werden?
- Sind alle empfohlenen Maßnahmen tatsächlich vollständig umgesetzt? Warum sind gegebenenfalls Maßnahmen nur unzureichend oder überhaupt nicht umgesetzt?

In diesem Kurs erfahren Sie in Kapitel 5, wie Sie die passenden IT-Grundschutz-Bausteine auswählen (**Modellierung**), und in Kapitel 6, wie Sie im **Basis-Sicherheitscheck** in einem einfachen Soll-Ist-Vergleich überprüfen, ob die in den Bausteinen empfohlenen Sicherheitsmaßnahmen hinreichend umgesetzt sind und welche Defizite bestehen.

4. Fragen zur ergänzenden Sicherheitsanalyse und Risikoanalyse

- Wie ist mit Komponenten zu verfahren, die stärker abgesichert werden müssen oder für die es keine passenden Bausteine gibt?
- Wie kann auf eine effiziente Weise eine Risikoanalyse durchgeführt werden?

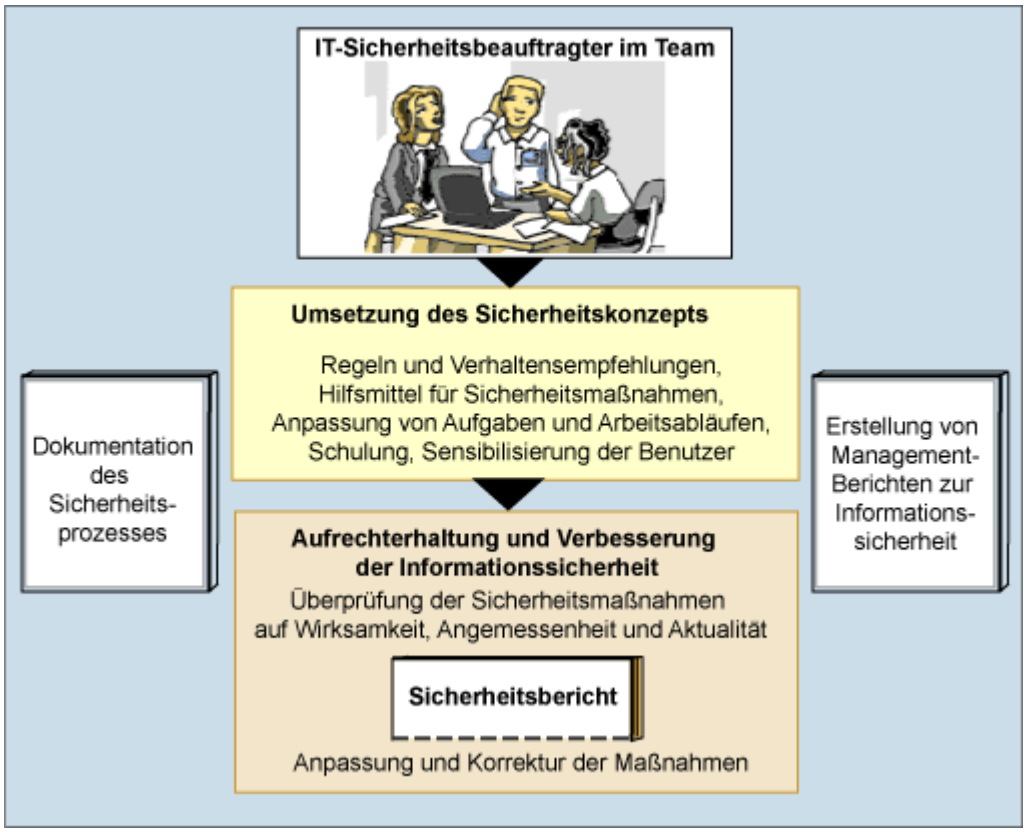
Die folgenden Schritte, eine **ergänzende Sicherheitsanalyse** und gegebenenfalls eine **Risikoanalyse**, sind nur für Komponenten mit mindestens hohem Schutzbedarf erforderlich, oder für solche, für die es keinen angemessenen IT-Grundschutz-Baustein gibt oder die in untypischen Einsatzszenarien betrieben werden. Das Vorgehen wird in *Kapitel 7: Risikoanalyse* erläutert.

5. Fragen zur Realisierungsplanung

- Was ist zu tun, wenn notwendige Sicherheitsmaßnahmen noch nicht umgesetzt sind?
- Passen die als fehlend ermittelten Maßnahmen stimmig zusammen?
- In welcher zeitlichen Reihenfolge sind sie umzusetzen?
- Wer ist dafür verantwortlich?
- Sie haben Zweifel, ob alle Maßnahmen überhaupt aus dem beschränkten Budget der Institution finanziert werden können?

Solche Fragen überprüfen Sie in der abschließenden **Realisierungsplanung**.

2.6.3 Umsetzung des Sicherheitskonzepts



Ist das Sicherheitskonzept von der Geschäftsführung abgenommen, gilt es als Vorgabe dafür, welche Maßnahmen mit welchen Ressourcen umzusetzen sind.

Der Realisierungsplan enthält zu jeder umzusetzenden Maßnahme Aussagen zu ihrer Dringlichkeit und dem beabsichtigten Umsetzungstermin, außerdem wer für die Umsetzung zuständig ist und welche Ressourcen dafür bereitzustellen sind. Das IS-Management-Team sowie der IT-Sicherheitsbeauftragte haben mit folgenden Aufgaben zur Umsetzung des Realisierungsplans beizutragen:

- Aufstellen von Regeln für die praktische Anwendung der Sicherheitsmaßnahmen,
- Empfehlungen zu angemessenen Verhaltensweisen,

- Auswahl und Einsatz geeigneter Hilfsmittel für die Sicherheitsanwendungen,
- organisatorische Anpassung von Aufgaben und Arbeitsabläufen,
- Sensibilisierung, Anleitung und Betreuung der Benutzer,
- Dokumentation des Sicherheitsprozesses und Abfassung von Managementberichten zur Informationssicherheit und
- regelmäßiges Prüfen der Sicherheitsmaßnahmen auf Funktionalität und Aktualität sowie im Bedarfsfall deren Anpassung und Korrektur.

Aufrechterhaltung und Verbesserung

Sicherheitsmaßnahmen sollten regelmäßig überprüft werden und zwar im Allgemeinen mindestens alle zwei Jahre. Sicherheitsvorfälle sollten zu einer unmittelbaren Überprüfung führen.

In einer **Aktualisierungsprüfung** wird beurteilt, ob die Maßnahmen noch angemessen und ausreichend sind und die damit verbundenen Sicherheitsziele noch gelten.

Ausführliche Informationen zu Maßnahmen bei der Umsetzung und Weiterentwicklung des Sicherheitskonzepts finden Sie unter:

- M 2.199 *Aufrechterhaltung der Informationssicherheit*,
- M 2.200 *Managementberichte zur Informationssicherheit*
- M 2.201 *Dokumentation des Sicherheitsprozesses*,

2.7 Test zum Informationssicherheitsmanagement

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.

Gegebenenfalls können auch mehrere Antwortmöglichkeiten zutreffend sein.

1. **Welches Modell liegt dem in BSI-Standard 100-1 beschriebenen Sicherheitsprozess zugrunde?**
   a) ein Zyklus aus den Schritten Plan, Do, Check, Act
   b) ein auf stetige Weiterentwicklung angelegtes Spiralmodell
   c) das IT-Grundschutz-Modell
   d) das Informationssicherheitsmodell

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 IT-Sicherheitsbeauftragte?

a) Sicherheitsvorfälle zu untersuchen

b) die Entwicklung von Sicherheitskonzepten zu koordinieren

c) die eingesetzte Sicherheitstechnik zu konfigurieren

d) der Leitungsebene über den Stand der Informationssicherheit zu berichten

4. Wie wird zweckmäßig ein IS-Management-Team gebildet?

a) Alle Personen werden in das Team aufgenommen, die sich für die Aufgabe interessieren und sich freiwillig melden.

b) Die Geschäftsleitung setzt ein IS-Management-Team aus Verantwortlichen für bestimmte IT-Systeme, Anwendungen, Datenschutz und IT-Service zusammen.

c) Der IT-Leiter beauftragt fachkundige Mitarbeiter aus der IT-Abteilung.

d) Alle Abteilungs- oder Bereichsleitungen entsenden einen Vertreter aus ihrem jeweiligen Zuständigkeitsbereich in das Team.

5. Wer ist für die Bekanntgabe der Leitlinie zur Informationssicherheit verantwortlich?

a) das IS-Management-Team

b) der Sicherheitsbeauftragte

c) die Unternehmens- oder Behördenleitung

d) die Öffentlichkeitsabteilung eines Unternehmens oder einer Behörde

6. Welche Aufgabe obliegt dem Informationssicherheitsmanagement?

a) die Arbeitssicherheit

b) der Schutz der für die Geschäftsprozesse und Fachaufgaben einer Institution wichtigen Informationen

c) der Datenschutz

d) der Schutz der Informationstechnik

Kapitel 3: Strukturanalyse

3.1 Überblick

Die IT-Grundschutz-Vorgehensweise zur Sicherheitskonzeption erfordert,

- zunächst den Geltungsbereich des Sicherheitskonzepts festzulegen (= **Definition des Informationsverbundes**), und
- anschließend die Objekte strukturiert zu erfassen, die Bestandteil dieses Geltungsbereichs und daher im Sicherheitskonzept zu berücksichtigen sind (= **Strukturanalyse**).

Definition des Informationsverbundes

Als Informationsverbund wird gemäß IT-Grundschutz die Gesamtheit der infrastrukturellen, organisatorischen, personellen und technischen Objekte verstanden, die dazu beitragen, die Aufgaben in einem bestimmten Anwendungsbereich der Informationsverarbeitung zu erfüllen. Diese Objekte bilden zusammengenommen den Untersuchungsgegenstand für die nachfolgenden Schritte.

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. Solche Teilbereiche 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.

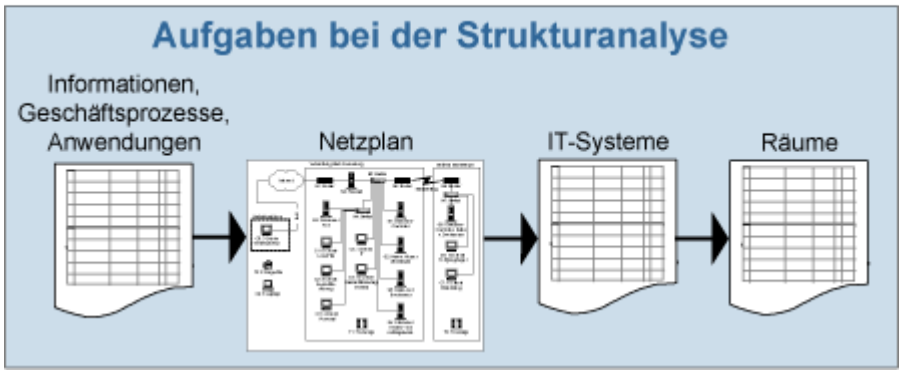
Achten Sie bei der Definition des Informationsverbundes darauf, dessen Schnittstellen genau zu beschreiben. Dies gilt insbesondere auch dann, wenn die einbezogenen Geschäftsprozesse oder Fachaufgaben von den Diensten externer Partner abhängen.

Strukturanalyse

Grundlage eines jeden Sicherheitskonzepts ist die genaue Kenntnis der Informationen, Prozesse und unterstützenden technischen Systeme des betrachteten Informationsverbundes. Ziel der Strukturanalyse ist es, die hierfür erforderlichen Kenntnisse zusammenzustellen und aufzubereiten.

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 beantwortet werden, desto zielgerichteter kann auch im Sicherheitskonzept festgelegt werden, welche Schutzvorkehrungen erforderlich sind.



Im Einzelnen sind die folgenden Informationen zu erheben:

1. die wichtigen **Informationen, Geschäftsprozesse und Anwendungen**,
2. ein **Netzplan** mit den eingesetzten IT-Systemen, Kommunikationsverbindungen und externen Schnittstellen,
3. die vorhandenen **IT-Systeme** (Clients, Server, Netzkopplungselemente usw.) sowie
4. die **räumlichen Gegebenheiten** (Liegenschaften, Gebäude, Räume).

Auf den folgenden Seiten werden diese Schritte detailliert beschrieben und anhand des Beispiels veranschaulicht.

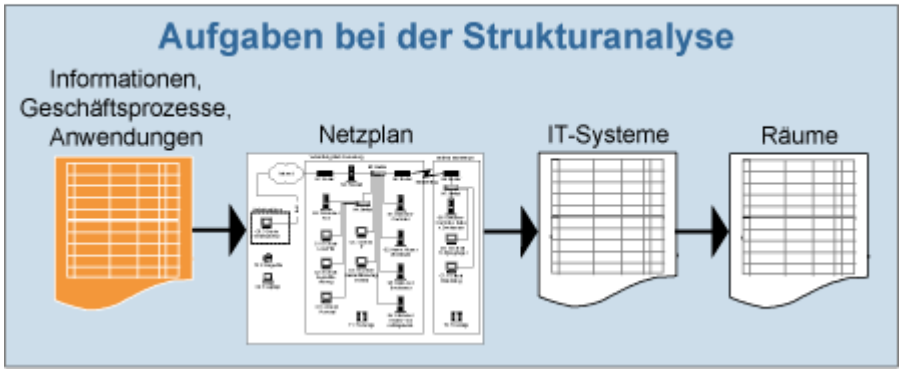
Objekte sinnvoll gruppieren

Bei allen Teilerhebungen sollten Sie Objekte sinnvoll **zu Gruppen zusammenfassen**. Welche Objekte dafür geeignet sind, wird im Zusammenhang mit der Erhebung des Netzplans (in Kapitel 3.3) dargestellt.

Vermeiden Sie Doppelarbeit. Wenn es in Ihrer Institution bereits Zusammenstellungen zu den zu erfassenden Sachverhalten gibt, zum Beispiel Inventare, Geschäftsprozessmodelle oder Netzpläne, sollten Sie diese auch benutzen.

3.2 Erhebung der Informationen, Geschäftsprozesse und Anwendungen

3.2.1 Vorgehen



In diesem Arbeitsschritt werden die wichtigsten Informationen, Geschäftsprozesse und Anwendungen des betrachteten Informationsverbundes erfasst. Tabellen bieten eine übersichtliche Möglichkeit, die Ergebnisse darzustellen.

Welche Objekte sollten Sie erfassen?

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)?

Anwendungen sind Verfahren, mit denen Geschäftsprozesse und Fachaufgaben in Unternehmen und Behörden unterstützt werden. In der Regel kann einem Geschäftsprozess eine Vielzahl an Anwendungen zugeordnet werden. Beispielsweise zählt zu den Aufgaben einer Beschaffungsabteilung die Suche nach neuen Produkten, die schriftliche Korrespondenz mit Lieferanten, die eigentliche Bestellung und die Dokumentation von Beschaffungsvorgängen in den zugehörigen Behörden- oder Unternehmenssystemen. Diesen Aufgaben lassen sich unterschiedliche Anwendungen zuordnen, wie Internet-Recherche, Textverarbeitung, E-Mail, Buchhaltung oder auch Dateiablage.

Wie detailliert und umfassend Sie die Anwendungen erfassen, obliegt Ihrer Entscheidung. Eine vollständige Zusammenstellung ist im Allgemeinen nicht erforderlich. Konzentrieren Sie sich auf die **wichtigsten Anwendungen**. Dies sind solche, die aufgrund ihrer Bedeutung für die zugeordneten Geschäftsprozesse

- den höchsten Bedarf an Geheimhaltung (**Vertraulichkeit**),
- den höchsten Bedarf an Korrektheit und Unverfälschtheit (**Integrität**) oder
- die kürzeste tolerierbare Ausfallzeit (höchster Bedarf an **Verfügbarkeit**)

haben.

Es empfiehlt sich darüber hinaus, auch solche **Datenträger und Dokumente** in der Strukturanalyse zu erheben, die eigenständig, also unabhängig von einer bestimmten Anwendung oder einem bestimmten IT-System, bedeutsam sind, beispielsweise wichtige Verträge, Notfallhandbücher oder Backup-Datenträger.

Sie können die maßgeblichen Anwendungen präziser auswählen, wenn Sie Auskünfte der Benutzer und der fachlich Verantwortlichen einholen. Auch die IT-Verantwortlichen sollten Sie in die Erhebung einbeziehen, da diese aufgrund der Querschnittsfunktion ihrer Abteilung eine übergreifende Sicht auf die Bedeutung von Anwendungen haben.

Welche Angaben sollte die Übersicht zu den Anwendungen enthalten?

Die Anwendungen haben Sie aufgrund ihrer Bedeutung für die Geschäftsprozesse und Fachaufgaben ausgewählt. Sie sollten daher für jede erfasste Anwendung die folgenden Angaben vermerken:

- eine eindeutige Kennung (Nummer, Kürzel),
- die unterstützten Geschäftsprozesse und die Art der verarbeiten Informationen,
- Verantwortliche und Benutzer,
- die Verwendung personenbezogener Daten (zur Unterstützung des Datenschutzbeauftragten).

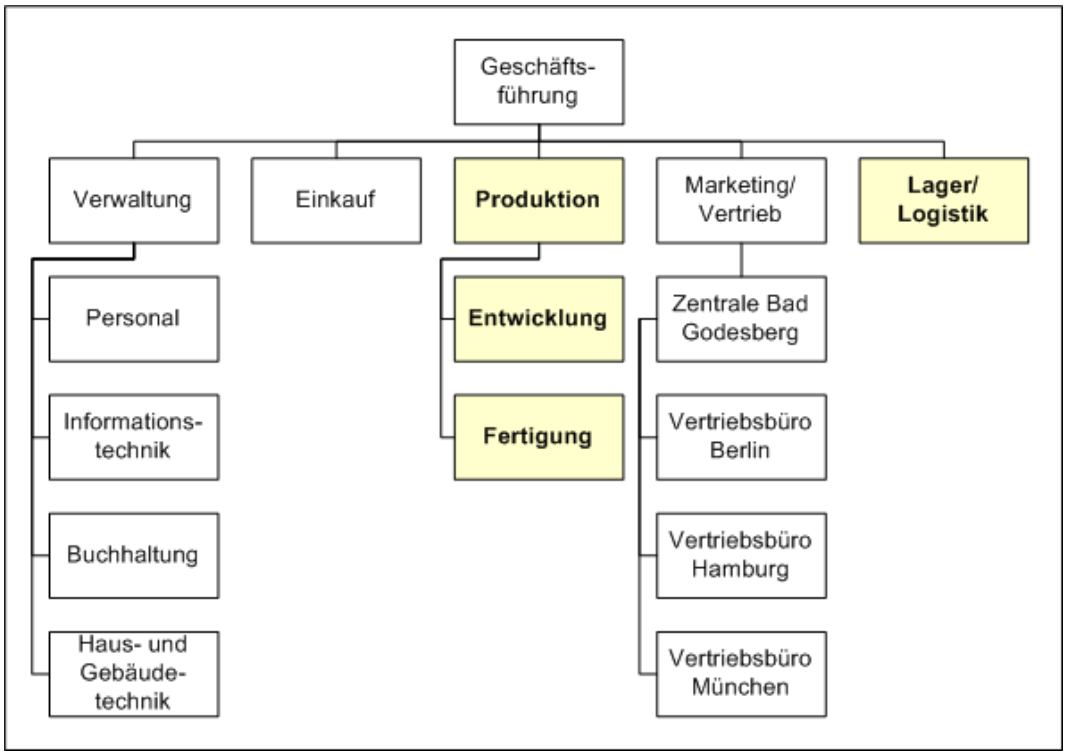
Oft ist es sinnvoll, zusätzlich Abhängigkeiten zwischen den Anwendungen zu erfassen (z. B. dass eine Anwendung eine funktionierende SQL-Server-Installation voraussetzt). Auch dies kann tabellarisch geschehen.

3.2.2 Beispiel

Die Erhebung der Anwendungen soll am Beispiel des fiktiven Beispielunternehmens, der **RECPLAST GmbH**, veranschaulicht werden. Dieses Unternehmen 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, Hamburg und München.

Organisationsstruktur und Geschäftsprozesse

Das nachfolgende Organigramm veranschaulicht die organisatorische Gliederung der RECPLAST GmbH. Die gelb hinterlegten Abteilungen sind am Standort Bonn-Beuel ansässig, alle anderen (bis auf die Vertriebsbüros) am Verwaltungssitz in Bad Godesberg.



Jeder Abteilung lassen sich verschiedene Geschäftsprozesse zuordnen, beispielsweise

- der Abteilung „Einkauf“ Prozesse wie Produktrecherche und Bestellung,
- der Abteilung „Informationstechnik“ Prozesse wie die zum Betrieb von Servern und Clients, Benutzerservice, Druckservice oder Netzadministration,
- der Personalabteilung Prozesse wie Einstellung, Gehaltszahlung und Fortbildung sowie

- der Unterabteilung „Fertigung“ der Produktionsabteilung die beiden Prozesse zur Umwandlung der Altkunststoffe in wiederverwertbare Regranulate sowie zur Herstellung der neuen Produkte aus diesen Rohmaterialien.

Viele dieser Prozesse können weiter untergliedert werden, beispielsweise die Server-Administration in die Teilprozesse Verwaltung von Mail-, Datei- und Datenbankservern zu denen jeweils Aktivitäten wie Patch-Management, Datensicherung, Konfiguration oder Dokumentation gehören.

Anwendungen

Eine vollständige Übersicht aller Anwendungen, die im Zusammenhang mit den oben genannten Prozessen bedeutsam sind, wäre zu umfangreich für diesen Kurs. Die nachfolgende Tabelle enthält daher nur einen Ausschnitt und zwar

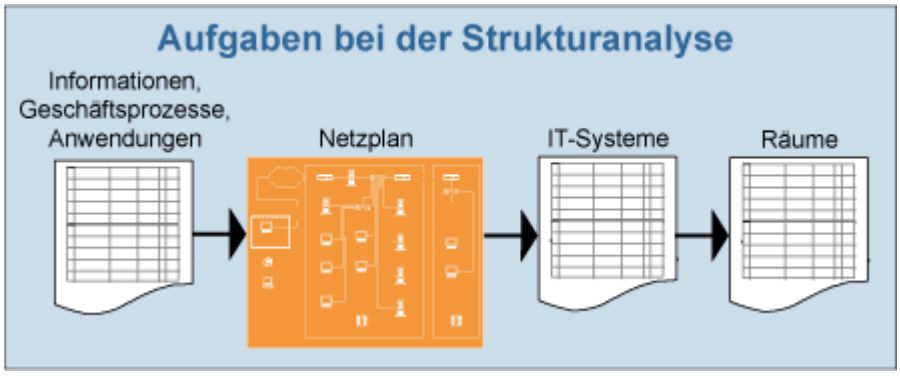
- die fachliche Anwendung „Auftrags- und Kundenverwaltung“, die für die Geschäftsprozesse der Abteilung Marketing und Vertrieb wichtig ist,
- die technische Anwendung „Benutzerauthentisierung“, ohne die ein ordnungsgemäßer Betrieb der IT-Systeme nicht möglich ist,
- die übergreifend genutzten Anwendungen „Druckservice“ in Verwaltungsgebäude und den Büros der Produktionshalle,
- das „Application Gateway“, mit dem die Internet-Anbindung abgesichert wird, sowie
- die für die interne und externe Kommunikation wichtige „TK-Vermittlung“.

Die Geschäftsprozesse sind als Kürzel angegeben (bestehend aus einem Präfix für die Abteilung, in der ein Prozess angesiedelt ist, und einer Zahlenfolge). Anwendungen, die in mehreren Abteilungen benutzt werden oder mehreren Geschäftsprozessen zugeordnet werden können, werden mit „übergreifend“ gekennzeichnet. Die Tabelle enthält zur Vorbereitung auf die sich anschließende Schutzbedarfsfeststellung in der Spalte „Art der Information“ auch Vermerke dazu, ob mit einer Anwendungen personenbezogene Daten (= P), anderweitig vertrauliche und unternehmenskritische Informationen (= V) bearbeitet werden oder diese wichtige Systemdateien verwendet oder erzeugt (= S).

Nr.	Beschreibung	Art der Informationen	Benutzer	Verantwortlich	Geschäftsprozesse
A4	Auftrags- und Kundenverwaltung	P, V	Marketing/ Vertrieb	Marketing/ Vertrieb	MARK_01 MARK_02 MARK_03
A5	Benutzerauthentisierung	P, V, S	übergreifend	IT-Abteilung	übergreifend
A9	Druckservice BG	V	alle Abteilungen in Bad Godesberg	IT-Abteilung	übergreifend
A10	Druckservice Beuel	V	alle Abteilungen in Beuel	IT-Abteilung	übergreifend
A13	Application Gateway	S	übergreifend	IT-Abteilung	übergreifend
A15	TK-Vermittlung	P, S	übergreifend	IT-Abteilung	übergreifend

3.3 Erhebung des Netzplans

3.3.1 Ausgangsplan



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

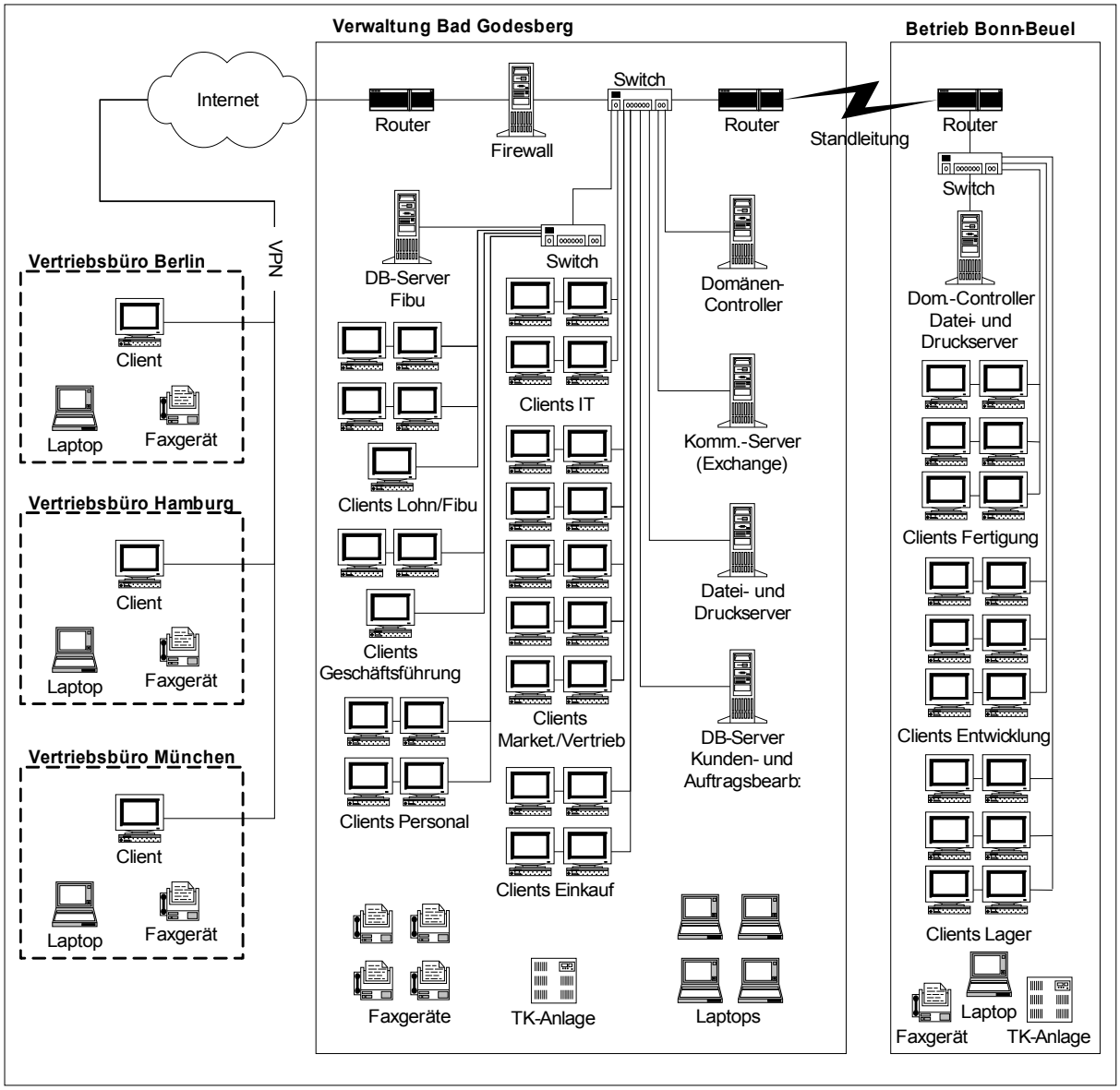
- die in das Netz eingebundenen **IT-Systeme**;
  dazu zählen Computer (Clients und Server), Netzdrucker sowie aktive Netzkomponenten (Hubs, Switches und Router);
- die **Verbindungen zwischen diesen IT-Systemen**;
  LAN-Verbindungen (Ethernet, Token Ring), Backbone-Technik (FDDI, ATM);
- die **Außenverbindungen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

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.

Beispiel

Das Beispiel zeigt den Netzplan unseres fiktiven Beispielunternehmens, der **RECPLAST GmbH.**



Wie das Beispiel zeigt, können auch nicht vernetzte Komponenten wie Laptops oder Telekommunikationsgeräte in den Netzplan aufgenommen werden.

3.3.2 Gruppenbildung

Auch dann, wenn der Netzplan aktuell ist, den Sie als Ausgangspunkt für die Strukturanalyse verwenden, sind gegebenenfalls weitere Arbeiten an ihm erforderlich.

Reduzieren Sie die Komplexität des Netzplans durch sinnvolle Gruppenbildungen!

Oft enthalten die vorliegenden Netzpläne Informationen, die für die weiteren Schritte nicht erforderlich sind. Zum Beispiel ist es sinnvoll, Clients, die gleich oder ähnlich konfiguriert sind und für die gleichen Aufgaben genutzt werden, zu einer Gruppe zusammenzufassen. Eine solche Gruppe kann in einem **bereinigten Netzplan** durch ein einzelnes Objekt dargestellt werden.

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.

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

Verwenden Sie eindeutige und sinnvolle Bezeichner für die einzelnen IT-Systeme, auf die Sie sich dann in den anschließend anzufertigenden Dokumenten beziehen können. Ihre Dokumente lassen sich leichter lesen und werden verständlicher.

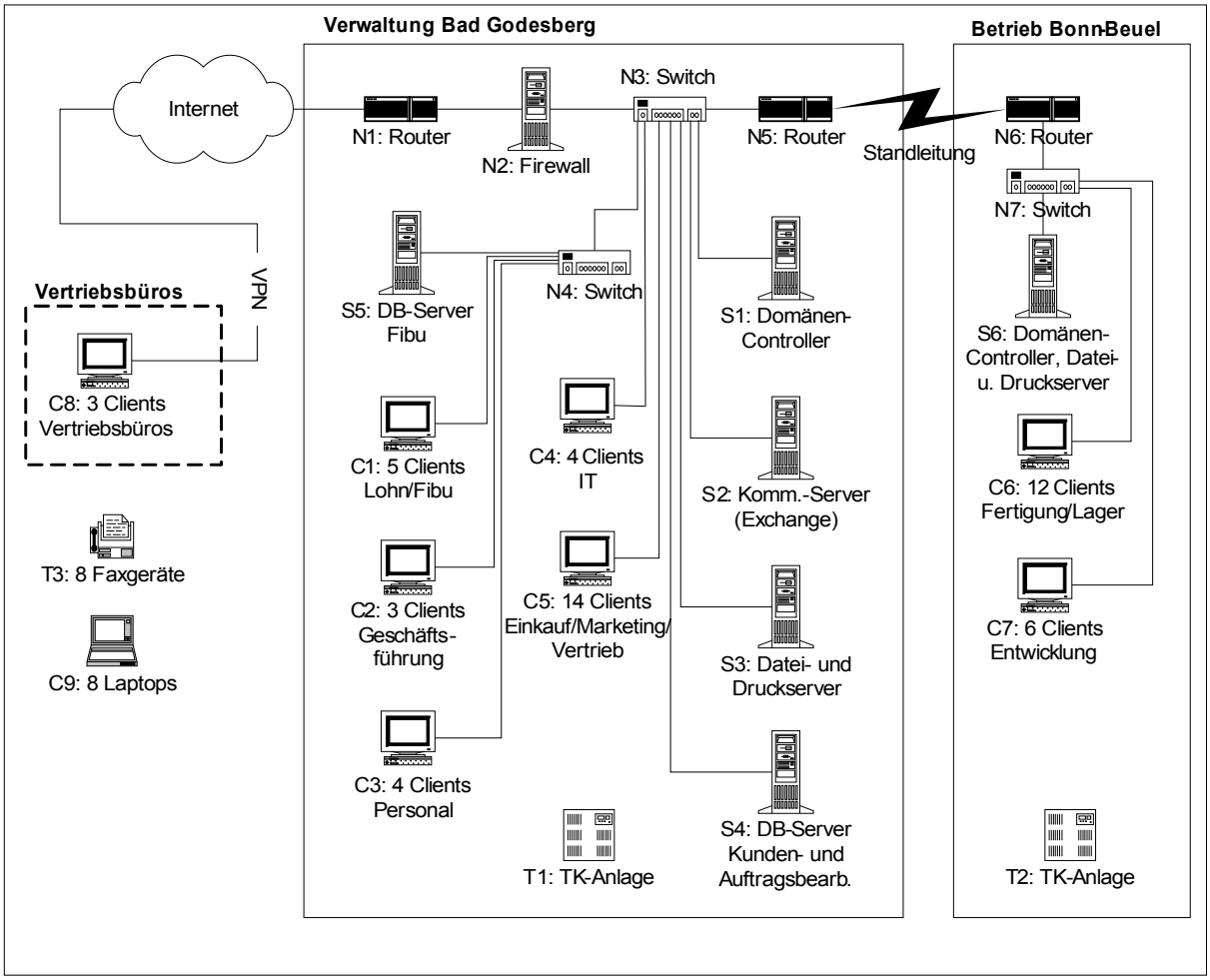
Übungsaufgabe

Schauen Sie sich noch einmal den Netzplan im vorherigen Abschnitt an. Sehen Sie mögliche Gruppenbildungen? Welche Bezeichnungen sind gewählt?

3.3.3 Beispiel für Gruppenbildung

Nachfolgend sehen Sie den bereinigten Netzplan der RECPLAST GmbH. In ihm wurden die folgenden Gruppen gebildet:

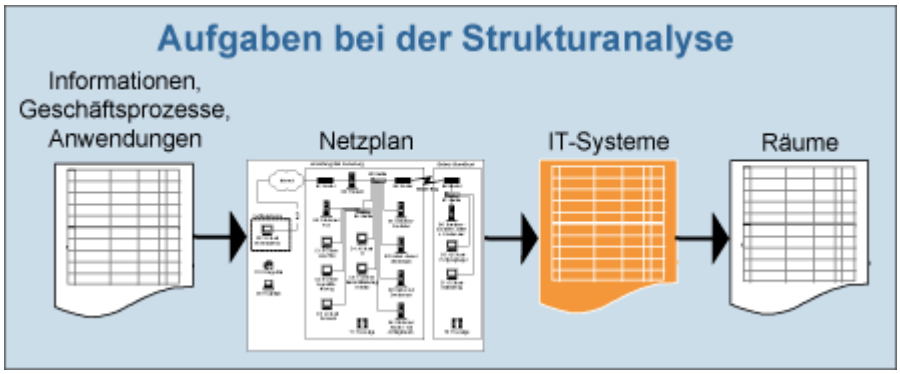
- Die Clients der Abteilungen „**Produktion**“ und „**Lager**“ wurden zusammengefasst, da sie grundsätzlich gleich ausgestattet sind und mit ihnen auf weitgehend identische Datenbestände zugegriffen werden kann.
- Die drei **Vertriebsbüros** zeichnen sich durch eine einheitliche IT-Ausstattung, übereinstimmende Aufgaben und Regelungen sowie einer identischen 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 **Laptops** und **Faxgeräte** wurden standortübergreifend zu jeweils einer Gruppe zusammengefasst, da für den Umgang mit diesen Geräten übereinstimmende organisatorische Regelungen gelten.



Folgende Clients sollten **nicht zusammengefasst** werden:

- Bei den Rechnern der **Geschäftsführung** kann von einem höheren Schutzbedarf ausgegangen werden, z. B. könnte auf ihnen besonders vertrauliche Korrespondenz gespeichert sein.
- Der größere Geheimhaltungsbedarf der Informationen ist auch ein Grund dafür, die Rechner der **Entwicklungsabteilung** gesondert zu erfassen. Auf ihnen befinden sich Konstruktionspläne und unter Umständen kundenspezifische Entwicklungen und Verfahrensbeschreibungen, die z. B. vor Wirtschaftsspionage und damit möglichen gravierenden wirtschaftlichen Folgen für die Firma zu schützen sind.
- Eine hohe Vertraulichkeit besitzen ferner auch die Informationen, die in der **Personalabteilung** bearbeitet werden, sowie die Daten der **Finanz- und Lohnbuchhaltung**.
- Auf den Rechnern der **IT-Administration** laufen Anwendungen, die für die Verwaltung des Netzes erforderlich sind. Von daher verlangen auch diese IT-Systeme eine besondere Aufmerksamkeit.

3.4 Erhebung der IT-Systeme



Bei der Erhebung der IT-Systeme stellen Sie die vorhandenen und geplanten IT-Systeme des Informationsverbundes und die sie jeweils charakterisierenden Angaben zusammen. Aufgrund der damit verbundenen besseren Übersichtlichkeit empfiehlt sich eine tabellarische Darstellung.

Was zählt zu den IT-Systemen?

Zu den IT-Systemen zählen

- alle im Netz vorhandenen Computer (Clients und Server), Gruppen von Computern und aktiven Netzkomponenten, Netzdrucker, aber auch
- nicht vernetzte Computer wie Internet PCs und Laptops sowie
- Telekommunikationsgeräte wie TK-Anlagen, Faxgeräte und Mobiltelefone (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,
- 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),
- bei Gruppen: Anzahl der zusammengefassten IT-Systeme,
- Status (z. B. in Betrieb, im Test, in Planung) und
- Benutzer und Administrator.

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 Ausschnitt aus der Erhebung der IT-Systeme bei der RECPLAST GmbH.

Nr.	Beschreibung	Plattform	Standort	Anzahl	Status	Benutzer/Administrator
S1	Domänen-Controller	Windows Server 2003	BG, R. 1.02 (Serverraum)	1	in Betrieb	alle IT-Benutzer/ IT-Administration
S4	DB-Server Kunden- und Auftragsbearbeitung	Windows Server 2003	BG, R. 1.02 (Serverraum)	1	in Betrieb	Marketing und Vertrieb, Fertigung, Lager/ IT-Administration
C5	Clients Kunden- und Auftrags-bearbeitung	Windows Vista	BG, R. 2.03 – 2.09	14	in Betrieb	Einkauf, Marketing und Vertrieb/ IT-Administration
C7	Clients in Entwicklungsabteilung	Windows Vista	Beuel, R. 2.14 – 2.20	6	in Betrieb	Entwicklung/ IT-Administration
C8	Clients in Vertriebsbüros	Windows Vista	Vertriebsbüros (Berlin, Hamburg, München)	3	in Betrieb	Mitarbeiter in Vertriebsbüros/ IT-Administration
N4	Switch für Personalabteilung	Switch	BG, R. 1.02 (Serverraum)	1	in Betrieb	alle IT-Benutzer/ IT-Administration
N5	Router zur Anbindung des Standorts Beuel	Router	BG, R. 1.02 (Serverraum)	1	in Betrieb	alle Mitarbeiter in BG/ IT-Administration
T1	Telefonanlage BG	ISDN-TK-Anlage	BG, R. 1.01	1	in Betrieb	alle Mitarbeiter in BG/ IT-Administration

Legende: Die IT-Systeme sind typweise durchnummeriert. Der vorangestellte Buchstabe kennzeichnet den Typ: S = Server, C = Client, N = Netzkomponente, T = Telekommunikationskomponente.

Zuordnung von IT-Systemen und Anwendungen

Der Schutzbedarf eines IT-Systems hängt von dem Schutzbedarf der Anwendungen ab, die es unterstützt. Daher ist es sinnvoll, in der Strukturanalyse Anwendungen und IT-Systeme einander zuzuordnen.

Die folgende Tabelle zeigt einen Auszug aus der Tabelle der für das Beispielunternehmen RECPLAST erfassten **Anwendungen** und deren **Zuordnung zu den Clients und Servern**.

Nr.	Beschreibung	Personenbezogene Daten	C2	C5	C6	C8	C9	S1	S3	S4	S6
A4	Auftrags- und Kundenverwaltung	X	X	X	X	X	X			X	
A5	Benutzerauthentisierung	X						X			X
A9	Druckservice BG								X		
A10	Druckservice Beuel										X
A13	Application Gateway										

Nr.	Beschreibung	Personenbezogene Daten	C2	C5	C6	C8	C9	S1	S3	S4	S6
A15	TK-Vermittlung	X									

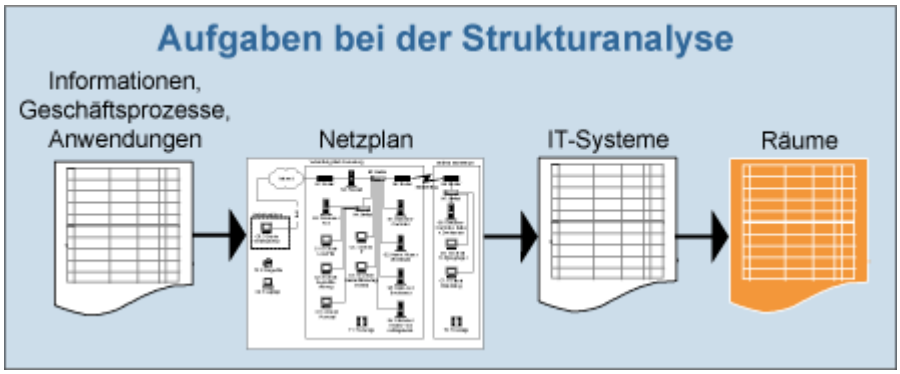
Legende: Die IT-Systeme sind typweise durchnummeriert. Der vorangestellte Buchstabe kennzeichnet den Typ: C = Client, S = Server.

Die folgende Tabelle zeigt die **Zuordnung** dieser Anwendungen zu den **Netz- und den Telekommunikationskomponenten**:

Nr.	Beschreibung	Personenbezogene Daten	N1	N2	N3	N5	N6	N7	T1	T2	T3
A4	Auftrags- und Kundenverwaltung	X			X	X	X	X			
A5	Benutzerauthentisierung	X			X	X	X	X			
A9	Druckservice BG				X						
A10	Druckservice Beuel							X			
A13	Application Gateway			X							
A15	TK-Vermittlung	X							X	X	

Legende: Die IT-Systeme sind typweise durchnummeriert. Der vorangestellte Buchstabe kennzeichnet den Typ: N = Netzkomponente, T = Telekommunikationsanlage.

3.5 Erhebung der räumlichen Gegebenheiten



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

Hinweis: 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 (Verwaltungsgebäude und Produktionshalle), 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.

Gebäude/Raum				**IT/Informationen**
Kürzel	**Bezeichnung**	**Raum**	**Lokation**	**IT-Systeme**
GB1	Verwaltungsgebäude	Gebäude	Bad Godesberg	ergibt sich aus Räumen
GB2	Produktionshalle	Gebäude	Bonn-Beuel	ergibt sich aus Räumen
R2	Serverraum Bad Godesberg (BG, R. 1.02)	Serverraum	GB1	S1 bis S5 N1 bis N5
R6	Büros Einkauf/ Marketing/Vertrieb (BG, R. 2.03 – 2.09)	Büroräume	GB1	C5, einige mit Faxgeräten
R11	Büros Entwicklungs-abteilung (Beuel, R. 2.14 – 2.20)	Büroräume	GB2	C7
R12	Vertriebsbüros (3 Standorte)	Häuslicher Arbeitsplatz	Berlin, Hamburg, München	C8

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 der wichtigen 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.

Hilfsmittel

Eine komfortable Möglichkeit, Anwendungen, IT-Systeme, Räume und alle anderen zu betrachtenden Objekte zu erheben und die erfassten Informationen konsistent weiterzuverarbeiten, bietet das **GSTOOL** des BSI. Auf den GSTOOL-Seiten der BSI-Webseiten finden Sie umfangreiche Informationen zu diesem Werkzeug sowie die Möglichkeit zum Download einer Testversion.

3.6 Test zur Strukturanalyse

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

Gegebenenfalls können auch mehrere Antwortmöglichkeiten zutreffend sein.

1. Bei der Festlegung des Informationsverbundes sollten Sie darauf achten, dass dieser ...

a) … möglichst viele Bereiche einer Institution umfasst.

b) … eindeutig und einfach gegen Bereiche innerhalb der Institution, die nicht einbezogen sind, abgegrenzt werden kann.

c) … eine sinnvolle Mindestgröße hat.

d) … vollständig mit allen externen Schnittstellen beschrieben wird.

2. Welche Ziele verfolgt die Strukturanalyse im Rahmen der IT-Grundschutz-Vorgehensweise?

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 IT-Grundschutz-Bausteine gibt

3. 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

4. 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 etc.) haben

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

c) wenn diese in denselben Räumlichkeiten untergebracht sind

d) wenn der Umfang der insgesamt erfassten Objekte zu groß zu werden droht

5. Welche der folgenden Aufgaben gehören gemäß BSI-Standard 100-2 zur Strukturanalyse?

a) die angemessene Gruppierung der Objekte, die in einem Sicherheitskonzept unterschieden werden müssen

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, Anwendungen, IT-Systeme, Kommunikationsverbindungen und räumlichen Gegebenheiten eines Informationsverbundes

6. Welche der folgenden Aussagen für die Behandlung von Datenträgern bei der Strukturanalyse sind zutreffend?

a) Datenträger dienen lediglich als Backup-Medium und zu Übertragungszwecken und brauchen deswegen bei der Strukturanalyse nicht berücksichtigt zu werden.

b) Datenträger sollten in der Strukturanalyse berücksichtigt werden, wenn sie schutzbedürftige Informationen enthalten.

c) Datenträger, die fest mit einem IT-System verknüpft sind, werden bei der Strukturanalyse nicht erfasst.

d) Sie sollten auf eine angemessene Gruppierung der Datenträger achten, die Sie bei der Strukturanalyse erfassen.

Kapitel 4: Schutzbedarfsfeststellung

4.1 Überblick

Wie viel Schutz benötigen der betrachtete Informationsverbund und die ihm zugehörigen Objekte? Wie kommen Sie zu begründeten und nachvollziehbaren Einschätzungen des Schutzbedarfs? Welche Objekte benötigen mehr Sicherheit, bei welchen genügen elementare Schutzmaßnahmen?

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

Die Schutzbedarfsfeststellung

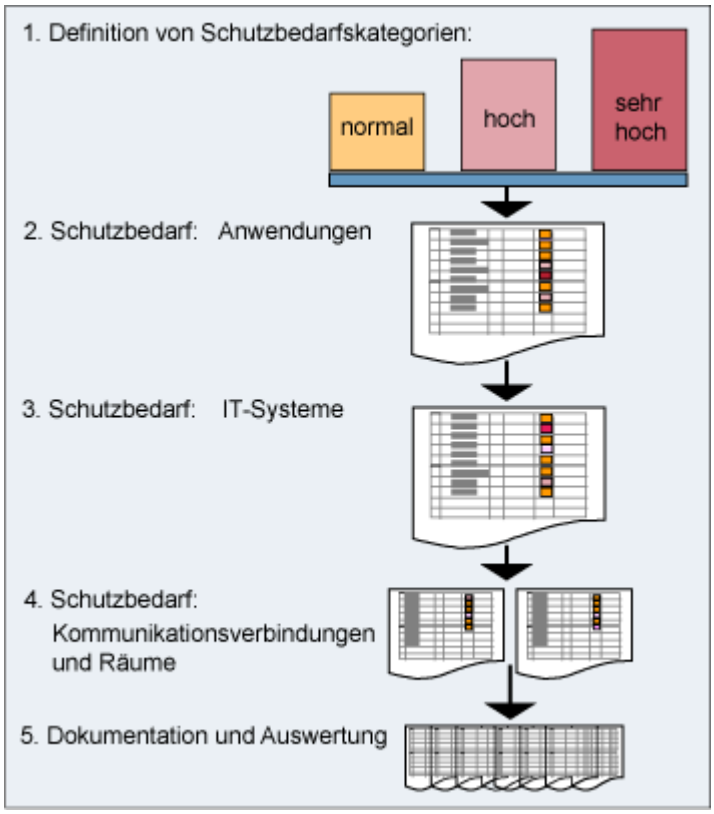
- sensibilisiert die Institution in Bezug auf Informationssicherheit,
- schafft eine einheitliche Sicherheitsdefinition und ein abgestimmtes Sicherheitsverständnis zwischen den Zuständigen,
- erleichtert die Auswahl der IT-Grundschutz-Maßnahmen und
- identifiziert Komponenten, für die eventuell höherwertige Maßnahmen erforderlich sind.

Die Entscheidungen zur Schutzbedarfsfeststellung sollten nachvollziehbar dokumentiert werden und die Zustimmung aller Beteiligten finden, insbesondere auch des Managements.

Was gehört zu einer Schutzbedarfsfeststellung?

Zur Schutzbedarfsfeststellung gehören die folgenden Aktivitäten:

1. die auf Ihre Organisation zugeschnittene Definition der Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“,
2. die Feststellung des Schutzbedarfs der Anwendungen, die in der Strukturanalyse erfasst wurden, mit Hilfe der definierten Kategorien,
3. die Ableitung des Schutzbedarfs der IT-Systeme aus dem Schutzbedarf der Anwendungen,
4. daraus abgeleitet die Feststellung des Schutzbedarfs der Kommunikationsverbindungen und Räume sowie
5. die Dokumentation und Auswertung der vorgenommenen Einschätzungen.



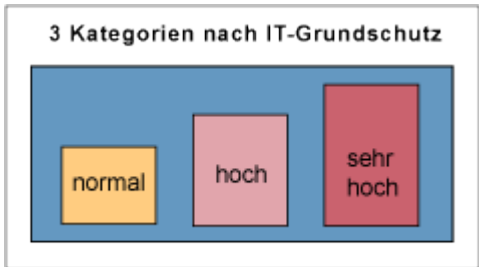
4.2 Schutzbedarfskategorien

4.2.1 Definition

Der Schutzbedarf eines Objekts orientiert sich an dem Ausmaß der **Schäden**, die entstehen können, wenn seine Funktionsweise beeinträchtigt ist. Da die Höhe eines Schadens häufig 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-Vorgehensweise empfiehlt **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.



Schutzziele und Grundwerte

Bei der Schutzbedarfsfeststellung ist danach zu fragen, welcher Schaden entstehen kann, wenn die **Grundwerte** Vertraulichkeit, Integrität oder Verfügbarkeit eines Objekts verletzt werden, wenn also

- 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**).

Schadensszenarien

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 Außenwirkung oder
- finanzielle Auswirkungen.

Ein Schadensfall kann mehr als ein Szenario betreffen. Wenn beispielsweise Bestelldaten in der Datenbank eines Unternehmens zerstört wurden und nicht wiederhergestellt werden können, drohen folgende Schadensszenarien:

- eingegangene Bestellungen können nicht bearbeitet werden (Beeinträchtigung der Aufgabenerfüllung),

- Verpflichtungen gegenüber den Kunden können nicht eingehalten werden (Verstoß gegen Verträge),
- beträchtliche Einnahmeausfälle für das Unternehmen (finanzielle Auswirkungen) und
- Ansehensverlust bei den Kunden (negative Außenwirkung).

Wie wichtig ein Szenario jeweils ist, unterscheidet sich von Institution zu Institution. Unternehmen schauen beispielsweise besonderes 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.

4.2.2 Abgrenzung der 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 4.3 des BSI-Standards 100-2. Die dort angeführten relativ allgemein gehaltenen Definitionen können Sie als Ausgangspunkt nehmen und an die besonderen Gegebenheiten Ihrer Organisation 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 IT-gestützten Verfahrens.

Beispiel

Für das Beispielunternehmen, die RECPLAST GmbH, wurde bezüglich der Schadensszenarien „finanzielle Auswirkungen“ und „Beeinträchtigung der Aufgabenerledigung“ 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."

4.2.3 Schutzbedarf und Schutzziele

Da der Schutzbedarf für die Grundwerte **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** unterschiedlich hoch sein kann und als Konsequenz unterschiedliche Sicherheitsmaßnahmen erforderlich sind, müssen Sie den Schutzbedarf für alle drei Ziele gesondert betrachten.

Der Schutzbedarf einer Firmendarstellung auf einem öffentlichen Webserver ist beispielsweise aus Sicht der **betreffenden Firma**

- bezüglich des Schutzziels Vertraulichkeit nicht relevant, da die Firmendarstellung ausschließlich Informationen enthält, die das Unternehmen sowieso an die Öffentlichkeit bringen will,
- bezüglich des Schutzziels Integrität in der Regel im normalen Bereich, da sich Integritätsverletzungen leicht erkennen und korrigieren lassen und der Image-Verlust, der sich z. B. aus einer gefälschten Homepage ergibt, meistens nicht nachhaltig ist,
- bezüglich des Schutzziels Verfügbarkeit ebenfalls als normal einzuschätzen, es sei denn, aus der fehlenden Verfügbarkeit resultieren gravierende wirtschaftliche Folgen, z. B. weil die Angebote der Firma nicht mehr von den Kunden wahrgenommen werden.

Sollte die Firmendarstellung auf dem Rechner eines **Providers** angesiedelt sein, könnte sich aus dessen Sicht bezüglich Integrität und Verfügbarkeit ein höherer Schutzbedarf ergeben, da er im Schadensfall seine Verpflichtungen nachweisbar nicht angemessen erfüllt hat und somit gravierende finanzielle Verluste befürchten muss, da zum Beispiel der Kunde den Vertrag kündigen könnte.

Wie dieses Beispiel zeigt, kann der Schutzbedarf für die Grundwerte unterschiedlich hoch sein. Für die gleiche Anwendung kann der Schutzbedarf auch unterschiedlich eingeschätzt werden, je nachdem aus welcher Sicht er betrachtet wird.

Fragen zu den Schadensszenarien

Um die Schäden zu betrachten, die aus Verletzungen der Integrität, Vertraulichkeit oder Verfügbarkeit bei den 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 100-2 finden Sie zu jedem Schadensszenario beispielhafte Fragestellungen, die Sie für Ihre Schutzbedarfsfeststellung anpassen und eventuell ergänzen können.

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 von den Mitarbeitern (und auch innerhalb der Projektgruppe) unterschiedlich eingeschätzt wird. Falls kein Konsens erzielt werden kann, muss das Management entscheiden.

4.3 Schutzbedarfsfeststellung für die Anwendungen

Wenn Sie die Schutzbedarfskategorien definiert haben, beantworten Sie im nächsten Schritt für alle Anwendungen, die Sie in der Strukturanalyse erfasst haben, die zu den Schadensszenarien entwickelten Fragen und schätzen Sie so den Schutzbedarf der Anwendungen im Hinblick auf die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit ein. Orientieren Sie sich dabei insbesondere auch an der **Bedeutung**, die eine Anwendung **für die Geschäftsprozesse** hat.

Wichtig ist, dass Sie die Schutzbedarfsfeststellungen begründen und zwar so ausführlich, dass die getroffenen Entscheidungen auch von anderen Personen (z. B. der Geschäftsführung) 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.

Schutzbedarfsfeststellung			
Nr.	**Bezeichnung**	**Schutzbedarf**	**Begründung**
A1	Personaldaten-verarbeitung	Vertraulichkeit: hoch	Personaldaten sind besonders schutzbedürftige Daten, deren Missbrauch die Betroffenen erheblich beeinträchtigen kann.
		Integrität: normal	Fehler werden rasch erkannt und können entweder aus der Datensicherung eingespielt oder durch Eingabe korrigiert werden.
		Verfügbarkeit: normal	Ausfälle bis zu einer Woche können mit manuellen Verfahren überbrückt werden.
A5	Benutzerauthen-tisierung	Vertraulichkeit: normal	Die Passwörter sind verschlüsselt gespeichert und damit praktisch nicht zugänglich.
		Integrität: hoch	Der hohe Schutzbedarf ergibt sich daraus, dass sich alle Mitarbeiter hierüber identifizieren.
		Verfügbarkeit: hoch	Bei Ausfall dieser Anwendung ist keine Identifizierung und damit keine Ausführung von IT-Verfahren möglich. Ein Ausfall ist allenfalls bis zu 24 Stunden tolerabel.
A12	Internet-Zugang	Vertraulichkeit: normal	Es werden keine vertraulichen Daten verarbeitet.
		Integrität: normal	Fehlerhafte Daten können in der Regel leicht erkannt werden.
		Verfügbarkeit: hoch	Die Recherche im Internet ist für einige Abteilungen wichtig (insbesondere die Einkaufsabteilung). Ein Ausfall ist höchstens 24 Stunden hinnehmbar.

4.4 Schutzbedarfsfeststellung für die 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 auf den Schutzbedarf des IT-Systems. Bei der Vererbung lassen sich folgende Fälle unterscheiden:

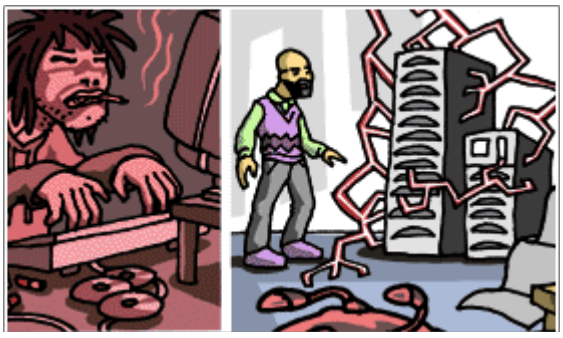
- In vielen Fällen lässt sich der höchste Schutzbedarf aller Anwendungen, die das IT-System benötigen, übernehmen (**Maximumprinzip**).
- Der Schutzbedarf des IT-Systems kann höher sein als der Schutzbedarf der einzelnen Anwendungen (**Kumulationseffekt**). Dies ist z. B. dann der Fall, wenn auf einem Server mehrere Anwendungen mit mittlerem Schutzbedarf in Betrieb sind. 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, in denen die Daten nur in pseudonymisierter Form verwendet werden, weniger kritisch.

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:

IT-System		**Schutzbedarfsfeststellung**	
Nr.	**Bezeichnung**	**Schutzbedarf**	**Begründung**
S1	Domänen-Controller	Vertraulichkeit: normal	Maximumprinzip gemäß Anwendung A5 (Benutzerauthentisierung)
		Integrität: hoch	Maximumprinzip gemäß Anwendung A5 (Benutzerauthentisierung)
		Verfügbarkeit: normal	Gemäß Anwendung A5 (Benutzerauthentisierung) wäre der Schutzbedarf hoch. Er wurde als normal festgelegt, weil die Benutzer aus Bad Godesberg sich auch über den Domänen-Controller S6 in Beuel anmelden können. Ein Ausfall bis zu drei Tagen ist hinnehmbar (Verteilungseffekt).
S2	Kommunikationsserver	Vertraulichkeit: hoch	Maximumprinzip gemäß Anwendung A7 (E-Mail)
		Integrität: hoch	Maximumprinzip gemäß Anwendung A7 (E-Mail)
		Verfügbarkeit: hoch	Maximumprinzip gemäß Anwendung A7 (E-Mail)
S5	DB-Server Finanzbuchhaltung	Vertraulichkeit: hoch	Maximumprinzip, da hohe Vertraulichkeit bei Anwendungen A1 (Personaldatenverarbeitung) und A3 (Finanzbuchhaltung)
		Integrität: hoch	Maximumprinzip von Anwendung A3 (Finanzbuchhaltung)
		Verfügbarkeit: normal	Ausfälle können mittels manueller Verfahren überbrückt werden.

4.5 Schutzbedarfsfeststellung für die Kommunikationsverbindungen

4.5.1 Kritische Verbindungen



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.

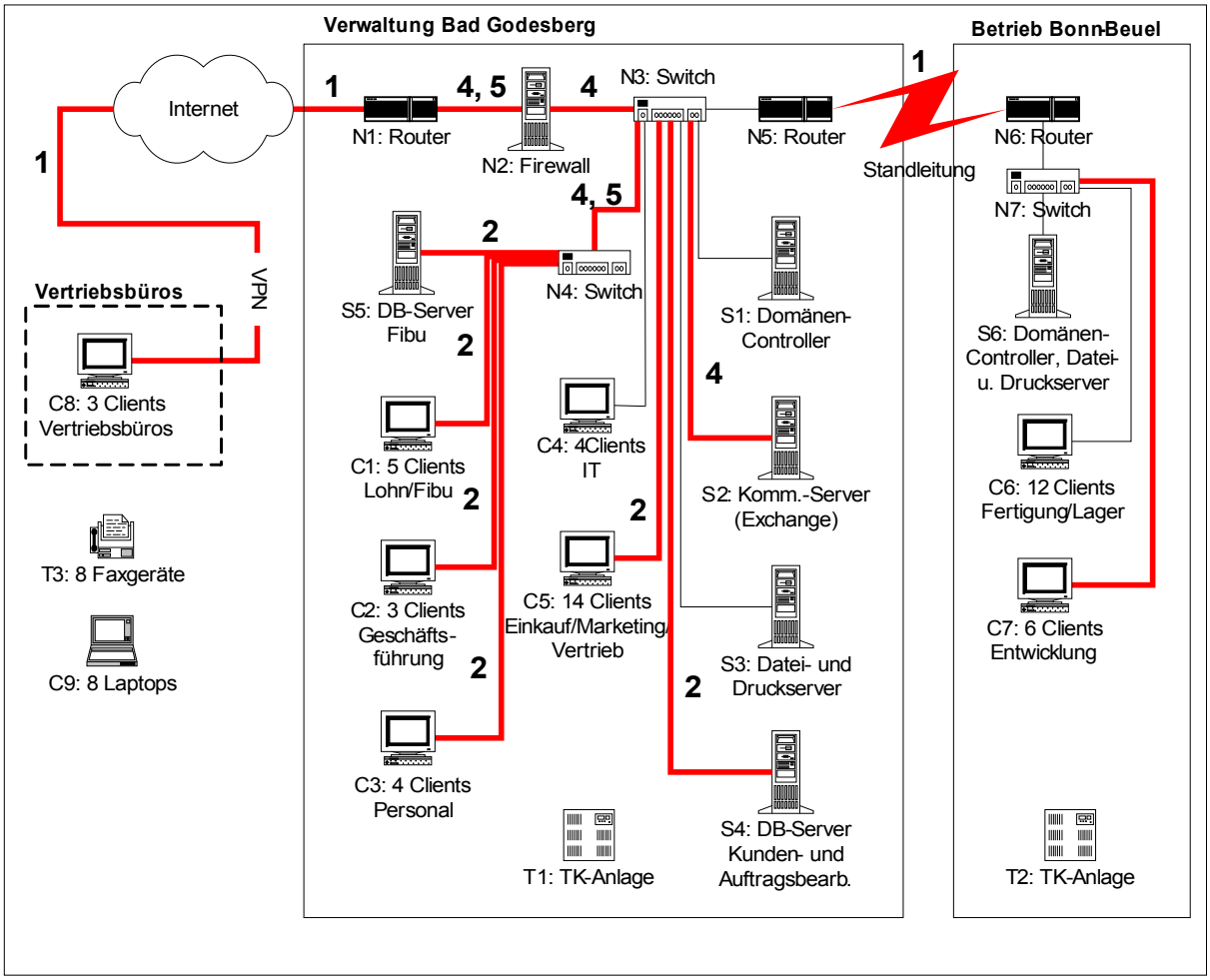
Sie sollten folgende **Verbindungen** als **kritisch** einstufen:

- Verbindungen, die aus dem Unternehmen **in ein öffentliches Netz** (z. B. Telefonnetz, Internet) oder **über ein öffentliches Gelände** reichen. Über solche Verbindungen können Schadprogramme in das Unternehmensnetz eingeschleust werden, Unternehmens-Server 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. Ein Beispiel finden Sie auf der nächsten Seite.

4.5.2 Beispiel für kritische Verbindungen

Nachfolgend sehen Sie nochmals den bereinigten Netzplan der RECPLAST GmbH. Die kritischen Verbindungen sind rot markiert.



Die kritischen Verbindungen sind zusätzlich mit Ziffern versehen, die als Kürzel für die Gründe für die vorgenommene Einstufung dienen. Die Ziffern bedeuten:

1: kritisch aufgrund Außenverbindung,

2: kritisch aufgrund hoher Vertraulichkeit,

3: kritisch aufgrund hoher Integritätsanforderungen,

4: kritisch aufgrund hoher Verfügbarkeitsanforderungen,

5: Informationen mit hoher Vertraulichkeit dürfen nicht übertragen werden,

6: Informationen mit hohen Integritätsanforderungen dürfen nicht übertragen werden,

7: Informationen mit hohen Verfügbarkeitsanforderungen dürfen nicht übertragen werden.

Beschreibung der Verbindung		**Kritisch aufgrund**				**Nicht übertragen werden dürfen Informationen mit**		
Nr.	Beschreibung	**1**	**2**	**3**	**4**	**5**	**6**	**7**
V1	N1<-> Internet	**X**			**X**			
V3	S5 <-> N4		**X**					
V4	S2 <-> N3				**X**			
V7	N4 <-> N3				**X**	**X**		

Um Ihre Entscheidungen für andere Personen nachvollziehbar zu machen, sollten Sie für jede Verbindung begründen, warum Sie diese als kritisch einschätzen. Mögliche Begründungen zeigt die folgende Tabelle:

Nr.	Begründung
V1	Alle Verbindungen nach außen sind als kritisch anzusehen.
V3	Die übertragenen Daten sind vertraulich und die Anwendungen, deren Daten über diese Verbindungen übertragen werden, haben einen hohen Schutzbedarf an Vertraulichkeit.
V4	Der Kommunikationsserver S3 weist hohen Schutzbedarf in Bezug auf Verfügbarkeit auf und es ist keine redundante Verbindung vorhanden. Den Schutzbedarf für die Grundwerte Vertraulichkeit und Verfügbarkeit erbt die Verbindung nicht, da die schutzbedürftigen Daten hauptsächlich durch Außenangriffe gefährdet sind.
V7	Die Kommunikationsverbindung ist kritisch, da hierüber keine vertraulichen Daten vom Server S2 in das hinter dem Switch N4 liegende Netz übertragen werden dürfen.

4.6 Schutzbedarfsfeststellung für die 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.

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

Raum				Schutzbedarf		
Bezeichnung	**Art**	**Lokation**	**IT-Systeme**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
BG, R. 1.01	Technikraum	Verwaltungsgebäude	TK-Anlage T1	normal	normal	hoch
BG, R. 1.02	Serverraum	Verwaltungsgebäude	S1 bis S5 N1 bis N5	hoch	hoch	hoch
Beuel, R. 2.01	Serverraum	Produktionshalle	S6, N6, N7	normal	normal	normal
Beuel, R. 2.10 – 2.13	Büroräume	Produktionshalle	C6, einige mit Faxgeräten	hoch	normal	normal

4.7 Abstimmung mit der Geschäftsleitung

Die Kategorien, mit deren Hilfe Sie den Schutzbedarf für die einzelnen Objekte des Informationsverbundes bestimmen, sollten Sie vorab mit der Behördenleitung oder Geschäftsführung abstimmen. Häufig kann auch nur diese entscheiden, bis zu welchen finanziellen Verlusten nur ein normaler Schaden und ab welchen Verlusten ein hoher oder sehr hoher Schaden anzunehmen ist. Der Geschäftsführung kommt außerdem auch eine entscheidende Rolle zu, falls in den Beratungen des IS-Management-Teams unterschiedliche Ansichten zum Schutzbedarf einzelner Objekte entstanden sind.

Bei einigen Fragestellungen, insbesondere zu solchen, die den rechtlich gebotenen Umgang mit personenbezogenen Daten betreffen, sollten Sie auch den Datenschutzbeauftragten einbeziehen. Er kann sicher wertvolle Hinweise über die Folgen von fahrlässigem Umgang mit solchen Informationen geben.

Die Schutzbedarfsfeststellung ist die Grundlage für die Auswahl der Sicherheitsmaßnahmen für die Bestandteile des Informationsverbundes, ihre Ergebnisse sollten daher von der Geschäftsleitung bestätigt werden. Je detaillierter und plausibler Ihre Begründungen sind, desto leichter sind sie auch für die Leitung nachvollziehbar, desto eher ist sie bereit, die erforderlichen Maßnahmen zu unterstützen.

Die Geschäftsführung kann Einschätzungen des Schutzbedarfs ändern. Solche Änderungen lassen Sie sich – am besten schriftlich – bestätigen, damit Sie bei höheren Kosten oder eventuell auftretenden Schadensfällen darauf verweisen können.

4.8 Test zur Schutzbedarfsfeststellung

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.

Gegebenenfalls können auch mehrere Antwortmöglichkeiten zutreffend sein.

1. **Welche Schutzziele werden bei der Schutzbedarfsfeststellung gemäß IT-Grundschutz betrachtet?**
   a) Authentizität
   b) Verfügbarkeit
   c) Vertraulichkeit
   d) Integrität

2. **In welchen Fällen können Sie gemäß IT-Grundschutz-Vorgehensweise 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, 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 der Anwendung

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 unwesentliche Teile der Anwendungen bedient

c) wenn ein redundant ausgelegtes weiteres IT-System vorhanden ist, das die Funktionen unterstützt, die für die betreffenden Anwendungen benötigt werden

d) wenn die Anwendungen innerhalb der nächsten 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 insgesamt höheren Gesamtschaden addieren.

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

c) … der für das IT-System bestimmte Schutzbedarf sich auch auf den Schutzbedarf anderer mit dem betreffenden IT-System vernetzter IT-Systeme auswirkt.

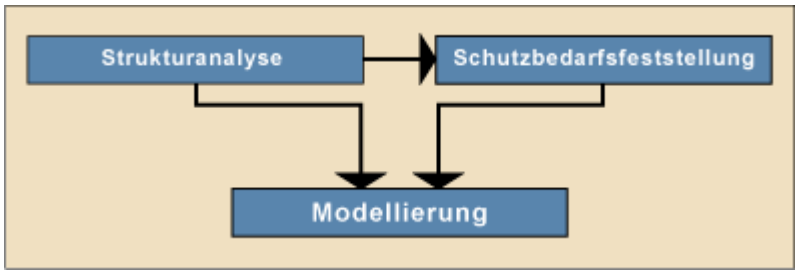
d) … der Schutzbedarf des IT-Systems erst bestimmt werden kann, wenn der Schutzbedarf der mit diesem vernetzten IT-Systeme bestimmt ist.

Kapitel 5: Modellierung nach IT-Grundschutz

5.1 Überblick

Wie in Kapitel 1 dargestellt, sind die IT-Grundschutz-Kataloge als Baukastensystem gestaltet. Sie enthalten Bausteine für Objekte, die in einem üblichen Informationsverbund anwendbar sind, beispielsweise Datenbanken, Client unter Windows Vista, Sicherheitsgateway (Firewall), Serverraum oder Sicherheitsmanagement, und beschreiben teils technische Komponenten (wie Verkabelung), teils organisatorische Verfahren (wie Notfallmanagement) und besondere Einsatzformen (wie häuslicher Arbeitsplatz).

Bei der **Modellierung** bilden Sie den Informationsverbund und seine einzelnen Komponenten mithilfe der Bausteine nach. Das Ergebnis ist ein **IT-Grundschutz-Modell**. Dafür greifen Sie auf die Ergebnisse der beiden vorangegangenen Schritte zurück:



- Bei der **Strukturanalyse** haben Sie Übersichten über die einzelnen Komponenten des betrachteten Informationsverbundes angefertigt.
- Ferner benötigen Sie die Ergebnisse der **Schutzbedarfsfeststellung**, denn es gibt Bausteine, deren Anwendung sich insbesondere für solche Komponenten empfiehlt, die einen höheren Schutzbedarf in einem der drei Grundwerte haben. Dies gilt etwa für den Baustein B 1.7 *Kryptokonzept*, der vor allem für solche Objekte wichtig ist, deren Bedarf an Vertraulichkeit hoch oder sehr hoch ist.

Dieses Modell können Sie für die bestehenden Teile Ihrer Informationstechnik als **Prüfplan** verwenden (siehe *Kapitel 6: Basis-Sicherheitscheck)* und für geplante Teile als **Entwicklungskonzept**.

Was machen Sie, wenn die IT-Grundschutz-Kataloge keinen passenden Baustein enthalten?

In solchen Fällen können Sie einen neuen („benutzerdefinierten“) Baustein anlegen. Die in *Kapitel 7: Risikoanalyse* beschriebene **Risikoanalyse auf Basis von IT-Grundschutz** kann die Auswahl zweckmäßiger Maßnahmen für einen solchen Baustein unterstützen.

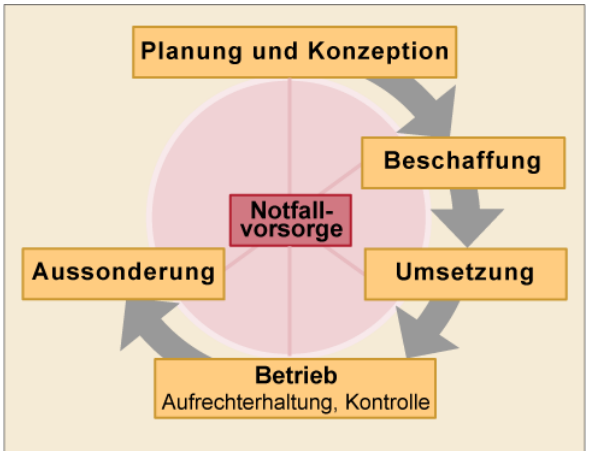
5.2 Bausteine

Gliederung

Den Kern der IT-Grundschutz-Kataloge bilden die Bausteine, über die sich die Gefährdungen, denen ein Objekt ausgesetzt ist, und die Maßnahmen, mit denen es gegen diese Gefährdungen geschützt werden kann, erschließen. Alle Bausteine sind gleichartig gegliedert. Schauen Sie sich als Beispiel einmal den Baustein B 3.203 *Laptop* an.

Sie finden dort den typischen Aufbau mit den folgenden Abschnitten:

- **Kurzbeschreibung**
  Jeder Baustein beginnt mit einer kurzen Beschreibung und Abgrenzung des betrachteten Gegenstands.
- **Gefährdungslage**
  Dieser Abschnitt zeigt auf, welchen Gefährdungen die im Baustein beschriebenen Objekte ausgesetzt sein können. Die Gefährdungslage wird pauschal betrachtet, also ohne Berücksichtigung von Eintrittswahrscheinlichkeiten. Die Gefährdungen werden als Referenzen auf ihre ausführliche Beschreibung in den Gefährdungskatalogen angeführt und sind gegliedert in die möglichen Ursachen „Höhere Gewalt“, „Organisatorische Mängel“, „Menschliche Fehlhandlungen“, „Technisches Versagen“ und „Vorsätzliche Handlungen“.
- **Maßnahmenempfehlungen**
  Danach folgen die Maßnahmenempfehlungen, die mit kurzen Erläuterungen zum jeweiligen Maßnahmenbündel eingeleitet werden, z. B. Hinweisen zu einer sinnvollen Umsetzungsreihenfolge. Die Maßnahmen sind als Referenzen auf die ausführliche Beschreibung in den Maßnahmenkatalogen angeführt und in Anlehnung an ein Lebenszyklusmodell gegliedert in die Rubriken „Planung und Konzeption“, „Beschaffung“, „Umsetzung“, „Betrieb“, „Aussonderung“ und die Querschnittsaufgabe „Notfallvorsorge“.



Die Lektüre der Gefährdungen ist zwar für die Umsetzung des IT-Grundschutzes nicht zwingend erforderlich, kann aber zu einem besseren Verständnis der Schutzwirkung der Maßnahmen beitragen und Argumente für deren Umsetzung liefern. Dies gilt auch für die Kreuzreferenztabellen, die Sie unter den Hilfsmitteln zu den IT-Grundschutz-Katalogen finden. Dort ist für jeden Baustein dargestellt, gegen welche Gefährdungen die zugeordneten Maßnahmen schützen.

Angabe der Siegelstufe

Zu jeder Maßnahme finden Sie in Klammern eine Angabe zur Siegelstufe. Diese gibt an, wie wichtig die Umsetzung der Maßnahme ist. Sie zeigt außerdem für die Qualifizierung und Zertifizierung nach IT-Grundschutz den Umsetzungsstatus von IT-Grundschutz an. (siehe dazu Kapitel 9: Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz). Die folgende Tabelle zeigt die Bedeutung dieser Kennzeichnungen:

Kennzeichnung	Bedeutung
A (Einstieg)	Unabdingbare Standardsicherheitsmaßnahmen; die Umsetzung ist für alle drei Stufen der IT-Grundschutz-Qualifizierung erforderlich.
B (Aufbau)	Wichtigste Standardsicherheitsmaßnahmen; die Umsetzung ist für die Aufbaustufe und für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz erforderlich.
C (Zertifikat)	Diese Maßnahmen sind für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz darüber hinaus erforderlich.
Z (zusätzlich)	Die Umsetzung dieser zusätzlichen Sicherheitsmaßnahmen sollte zur Steigerung der Informationssicherheit erfolgen (zum Beispiel bei hohem Schutzbedarf), ist jedoch zur Qualifizierung nach IT-Grundschutz nicht erforderlich.
W (Wissen)	Diese Maßnahmen dienen der Vermittlung von Grundlagen und Kenntnissen, die für das Verständnis und die Umsetzung der anderen Maßnahmen hilfreich sind. Sie müssen weder für ein Auditor-Testat noch für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz geprüft werden.

5.3 Schichtenmodell

Die Bausteine sind in den IT-Grundschutz-Katalogen in fünf Schichten gruppiert:

1. **Übergreifende Aspekte:** Die hier zugeordneten Bausteine betreffen grundsätzliche organisatorische Aspekte der Informationssicherheit und gelten in der Regel für den gesamten Informationsverbund. Dazu gehören beispielsweise die Bausteine B 1.0 *Sicherheitsmanagement*, B 1.1 *Organisation* und B 1.4 *Datensicherungskonzept*.
2. **Infrastruktur:** Diese Bausteine (z. B. B 2.1 *Gebäude* oder B 2.4 *Serverraum*) behandeln baulich-technische Fragen und dienen insbesondere dem physischen Schutz etwa vor Feuer, Wasser oder Diebstahl.
3. **IT-Systeme:** Diese Bausteine beschreiben die Sicherheitsaspekte von IT-Systemen (z. B. B 3.101 *Allgemeiner Server* oder B 3.201 *Allgemeiner Client*).
4. **Netze:** Hier finden Sie Bausteine für Netzaspekte (z. B. B 4.4 *VPN* oder B 4.6 *WLAN*).
5. **Anwendungen:** Zur Sicherheit ausgewählter Anwendungen gibt es hier Bausteine (z. B. B 5.7 *Datenbanken* oder B 5.8 *Telearbeit*).

Vorzüge des Schichtenmodells

Informationssicherheit ist eine komplexe Aufgabe, bei der viele Einflussfaktoren zu berücksichtigen sind. Die Sicherheit einer Anwendung hängt beispielsweise von den folgenden Faktoren ab:

- den besonderen Merkmalen der Anwendung selber (Welche Risiken ergeben sich durch die Anwendung? Welche Schutzvorkehrungen sind in sie integriert?),
- den Merkmalen und Sicherheitsmechanismen des IT-Systems, mit dem sie genutzt wird (Welche Schwachstellen hat das Betriebssystem? Wie sieht eine sichere Konfiguration aus?),
- der baulichen und räumlichen Umgebung des IT-Systems (Wie gut ist der Zugang geschützt? Wie anfällig ist das IT-System gegen Gefährdungen durch Feuer oder Wasser?),
- den Sicherheitsmerkmalen des Netzes, in das ein unterstützendes IT-System eingebunden ist (Sind unerlaubte Zugriffe über das Netz möglich? Wie geschützt sind die Informationen bei ihrer Übertragung?) sowie
- den organisatorischen Regelungen und Bedingungen für den Einsatz der Anwendung.

Wollte man alle diese Abhängigkeiten in einem Sicherheitskonzept für jede Komponente einzeln berücksichtigen, käme man zu umfangreichen und kaum handhabbaren Konzepten. Das Schichtenmodell soll diese Komplexität überschaubar machen und zu übersichtlichen Sicherheitskonzepten führen.

Im Einzelnen ergeben sich dabei die folgenden Vorteile:

- Die **Komplexität der Darstellung** wird durch eine sinnvolle Aufteilung der Einzelaspekte, z. B. organisatorische Bedingungen, infrastrukturelle Gegebenheiten und Besonderheiten der technischen Systeme, **reduziert**.
- Da übergeordnete Aspekte und gemeinsame infrastrukturelle Fragestellungen getrennt von den IT-Systemen betrachtet werden, werden **Redundanzen vermieden**, weil diese Aspekte nur einmal bearbeitet werden müssen und nicht wiederholt für jedes IT-System.
- Aufgrund der Aufteilung der Sicherheitsaspekte in Schichten können Einzelaspekte in den Sicherheitskonzepten **leichter aktualisiert und erweitert** werden, ohne dass andere Schichten umfangreich berührt werden.
- Die einzelnen Schichten sind so gewählt, dass auch die **Zuständigkeiten** für die betrachteten Aspekte **gebündelt** sind. Schicht 1 betrifft Grundsatzfragen, damit in erster Linie die Leitung einer Institution und das Informationssicherheitsmanagement, Schicht 2 den Bereich Haustechnik, Schicht 3 die Ebene der Administratoren und Benutzer, Schicht 4 die Netz- und Systemadministration und Schicht 5 schließlich die Anwendungsverantwortlichen und -betreiber.

Aktualisierung und Erweiterung der Bausteine

Die IT-Grundschutz-Kataloge werden 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).

5.4 Vorgehen bei der Modellierung

5.4.1 Schichten 1 und 2

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* der IT-Grundschutz-Kataloge. Dort ist auch beschrieben, welche Bausteine **Pflichtbausteine** sind, die immer angewendet werden müssen, und welche nur ausgewählt werden müssen, wenn spezielle Bedingungen vorliegen.

Im Folgenden werden die Bausteine der einzelnen Schichten und die Zuordnung zu den Bausteinen anhand des Beispielunternehmens näher beschrieben.

Zuordnung zu den Bausteinen der Schicht 1: Übergreifende Aspekte

Die in dieser Schicht beschriebenen übergreifenden Aspekte haben die Besonderheit, dass die vorgeschlagenen Konzepte und Regelungen für den ganzen Informationsverbund einheitlich gelten sollten und daher meistens nur einmal angewendet werden müssen. Dies gilt auch für unser Beispielunternehmen RECPLAST GmbH und Bausteine wie B 1.0 *Sicherheitsmanagement*, B 1.1 *Organisation* oder B 1.13 *Sensibilisierung und Schulung zur Informationssicherheit.*

Bei der Anwendung der Bausteine B 1.3 *Notfallmanagement* und B 1.8 *Behandlung von Sicherheitsvorfällen* ist insbesondere auf Komponenten mit hohen oder sehr hohen Verfügbarkeitsanforderungen zu achten (also z. B. auch auf den Kommunikationsserver).

Der Baustein B 1.7 *Kryptokonzept* ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf Vertraulichkeit oder Integrität haben, oder wenn bereits kryptographische Verfahren im Einsatz sind. Mögliche Einsatzfelder für Verschlüsselung sind im Beispielunternehmen der Austausch von

vertraulichen E-Mails zwischen den Vertriebsbüros und der Verwaltung oder im Unternehmen gespeicherte geschäftskritische Informationen.

Zuordnung zu den Bausteinen der Schicht 2: Infrastruktur

Während die Bausteine der Schicht 1 in der Regel für einen Informationsverbund nur einmal anzuwenden sind, sind die Bausteine der Schicht „Infrastruktur" differenzierter zu betrachten:

- Der Baustein B 2.1 *Gebäude* sollte immer dann gesondert für jedes Gebäude eines Informationsverbundes angewandt werden, wenn sich die Gebäude in wesentlichen Merkmalen unterscheiden. Zum Beispiel unterscheiden sich Verwaltungs- und Produktionsgebäude der RECPLAST GmbH in ihrer Struktur und in den dort erledigten Arbeiten so sehr, dass sie auch bezüglich Sicherheit gesondert betrachtet werden sollten.
- Außerdem muss der Baustein B 2.2 *Elektrotechnische Verkabelung* sowohl für das Verwaltungs- als auch das Produktionsgebäude zusätzlich zum Baustein B 2.1 *Gebäude* gesondert betrachtet werden.

Die IT-Grundschutz-Kataloge enthalten Bausteine für unterschiedliche Arten von Räumen: Büroraum, Serverraum, Raum für technische Infrastruktur sowie Besprechungs-, Veranstaltungs- und Schulungsräume. Dabei wird davon ausgegangen, dass die in den jeweiligen Räumen untergebrachte Informationstechnik einen unterschiedlichen Schutzbedarf hat und dementsprechend angepasste Sicherheitsvorkehrungen erforderlich sind.

Die Bausteine zu den Räumen wie B 2.3 *Büroraum* oder B 2.4 *Serverraum* erfordern immer eine Anwendung des Bausteins B 2.1 *Gebäude*, in dem wesentliche Informationen zur Umsetzung stehen, die in den speziellen Bausteinen zu Büro- und Serverräumen nur um weitere Maßnahmen ergänzt werden.

Aber wie verhält es sich mit den Vertriebsbüros der RECPLAST GmbH in den Außenstellen Berlin, Hamburg und München? Ist für diese Ihrer Meinung nach der Baustein B 2.1 *Gebäude* anzuwenden?

Da sich die Vertriebsbüros selbstverständlich in einem Gebäude befinden, ist der Gedanke naheliegend, dass für diese auch der Baustein B 2.1 *Gebäude* hinzuziehen ist. Allerdings sind die Büros lediglich angemietete Räume in nicht-firmeneigenen Gebäuden. Die Möglichkeiten, die Sicherheit solcher Gebäude zu beeinflussen, sind in der Regel eher gering. Zudem ist in diesen Räumen keine teure Technik mit hohem Schutzbedarf untergebracht, in jedem Vertriebsbüro nur ein PC und eventuell ein Laptop – wäre dies anders, würden sich die Empfehlungen des Bausteins B 2.1 *Gebäude* ggf. als Kriterien für die Auswahl angemieteter Büroräume anbieten. Auch der Baustein B 2.3 *Büroraum* passt nicht hinreichend zu den Vertriebsbüros, da dieser Baustein für Räume in Gebäuden des betrachteten Informationsverbundes entworfen ist. Geeigneter ist der Baustein B 2.8 *Häuslicher Arbeitsplatz*, der für solche Räume anwendbar ist, die sich nicht im direkten Einfluss des Unternehmens befinden. Es wäre in diesem Zusammenhang ebenfalls möglich, den Bausteins B 2.10 *Mobiler Arbeitsplatz* anzuwenden.

5.4.2 Vorgehen bei der Modellierung – Schichten 3 bis 5

Zuordnung zu den Bausteinen der Schicht 3: IT-Systeme

Die Bausteine der Schicht 3 sind für jedes IT-System oder jede Gruppe von IT-Systemen gesondert zu berücksichtigen. Für die im Netz der Firma RECPLAST vorhandenen Computer sind dies z. B. die Bausteine B 3.108 *Windows Server 2003*, B 3.203 *Laptop* und B 3.210 *Client unter Windows Vista*,

für jeden Server zusätzlich der Baustein B 3.101 *Allgemeiner Server* sowie für jede Gruppe von Clients der Baustein B 3.201 *Allgemeiner Client*.

Zuordnung zu den Bausteinen der Schicht 4: Netze

Die Bausteine dieser Schicht behandeln die Sicherheitsaspekte der Netzverbindungen und der Kommunikation zwischen den IT-Systemen.

Insbesondere bei großen Netzen, die sich über mehrere Standorte erstrecken, erleichtert es die Modellierung, wenn Sie das Netz abhängig vom jeweiligen Schutzbedarf aufteilen und die dadurch gebildeten Teilnetze gesondert betrachten. Grundsätzlich ist dies für alle Verbindungen zweckmäßig, die Sie bei der Schutzbedarfsfeststellung als kritisch identifiziert haben und über die bestimmte Daten auf keinen Fall übertragen werden dürfen. Teilnetze sollten sich nicht über mehrere Standorte oder Liegenschaften erstrecken.

Für das Unternehmen RECPLAST bietet sich eine Aufteilung des Gesamtnetzes in die Teile *Produktionsgebäude Bonn-Beuel* und *Verwaltungsgebäude Bad Godesberg* und innerhalb des letzteren noch eine weitere Unterteilung in ein Teilnetz *Personal, Buchhaltung und Geschäftsführung* sowie ein Teilnetz *Andere Verwaltungsabteilungen* an. Für diese Teilnetze ist der Baustein B 4.1 *Heterogene Netze* geeignet. Da die Teilnetze vergleichsweise klein sind und von denselben Administratoren verwaltet werden, reicht es aus, den Baustein einmal durchgängig anzuwenden.

Zuordnung zu den Bausteinen der Schicht 5: Anwendungen

Gefährdungen und Schutzmaßnahmen für einige typische Anwendungen sind in den Bausteinen der Schicht 5 beschrieben, z. B. in B 5.7 *Datenbanken*. Ein Baustein dieser Schicht ist zu berücksichtigen, wenn die in ihm behandelte Anwendung in einem Informationsverbund genutzt wird. Zum Beispiel können die Empfehlungen des Bausteins B 5.8 *Telearbeit* zur Sicherheit der Vertriebsbüros der RECPLAST GmbH beitragen.

5.5 Prüfung auf Vollständigkeit

Ziel der Modellierung ist eine möglichst vollständige Abbildung des betrachteten Informationsverbundes auf die Bausteine der IT-Grundschutz-Kataloge: Jeder Baustein sollte auf alle Zielobjekte (IT-Systeme, Räume usw.) angewandt werden, für die er relevant ist.

Um sicherzustellen, dass keine Komponenten des Informationsverbundes oder wesentliche Sicherheitsaspekte übersehen wurden, prüfen Sie abschließend, ob in Ihrem IT-Grundschutz-Modell

- alle übergeordneten Aspekte korrekt modelliert sind,
- alle beteiligten Gebäude, Räume, Schutzschränke und die Verkabelung im Hinblick auf die infrastrukturelle Sicherheit berücksichtigt sind,
- alle erfassten IT-Systeme abgedeckt sind,
- die netztechnischen Sicherheitsaspekte durch die zugehörigen Bausteine korrekt modelliert sind,
- diejenigen Anwendungen berücksichtigt sind, für die es IT-Grundschutz-Bausteine gibt, sowie
- diejenigen Objekte, für die keine unmittelbar passenden Bausteine vorhanden sind, angemessen durch andere geeignete Bausteine modelliert sind.

Bei dieser Prüfung auf Vollständigkeit ist ein Rückgriff auf die Dokumente der Strukturanalyse hilfreich, beispielsweise auf die Liste der IT-Systeme oder auf den Netzplan.

Dokumentation des IT-Grundschutz-Modells

Ein Beispiel dafür, wie Sie die vorgenommene Modellierung dokumentieren können, finden Sie in folgender Tabelle, die einen Auszug aus der Modellierung für die RECPLAST GmbH wiedergibt.

Baustein	Zielobjekt	Hinweise
B 1.4 *Datensicherungskonzept*	Gesamte Organisation	Gilt einheitlich für alle Betriebsteile.
B 2.1 *Gebäude*	Verwaltungsgebäude	Der Baustein muss auf beide Gebäude getrennt angewendet werden.
B 2.1 *Gebäude*	Produktionshalle	
B 2.4 *Serverraum*	Serverraum BG, R. 1.02	Der Baustein muss auf beide Serverräume getrennt angewendet werden.
B 2.4 *Serverraum*	Serverraum Beuel, R. 2.05	
B 3.203 *Laptop*	C9	Die Laptops in den Vertriebsbüros, in Bad Godesberg und in Beuel werden von den Vertriebsmitarbeitern benutzt und sind in einer Gruppe zusammengefasst.
B 5.7 *Datenbanken*	A3 Finanzbuchhaltung	Die Datenbanksysteme unterscheiden sich bezüglich ihrer Server, ihrer Benutzer und ihres Schutzbedarfs. Der Baustein ist daher getrennt auf beide Anwendungen anzuwenden.
B 5.7 *Datenbanken*	A4 Auftrags- und Kundenverwaltung	

5.6 Test zur Modellierung

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.

Gegebenenfalls können auch mehrere Antwortmöglichkeiten zutreffend sein.

1. Welche Aufgaben stellen sich 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 entwickeln zusätzliche Bausteine für solche Komponenten des Informationsverbundes, für die es keinen angemessenen Baustein in den IT-Grundschutz-Katalogen gibt.

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

2. **Welche der folgenden Änderungen an den IT-Grundschutz-Bausteinen sind gemäß IT-Grundschutz-Vorgehensweise unter bestimmten Umständen im Rahmen der Modellierung zulässig?**
   a) die Konkretisierung von Maßnahmen um technische Details
   b) die Streichung von allzu kostspieligen Maßnahmen
   c) die Anpassung von Bezeichnungen (etwa für Rollen) an die Konventionen der betrachteten Institution
   d) die Ergänzung eines Bausteins um zusätzliche Maßnahmen

3. **Worauf sollten Sie achten, wenn Sie einen eigenen IT-Grundschutz-Baustein anfertigen?**
   a) auf die Wirtschaftlichkeit der vorgeschlagenen Maßnahmen
   b) auf die Wirksamkeit der vorgeschlagenen Maßnahmen
   c) auf den Innovationsgrad der vorgeschlagenen Maßnahmen
   d) auf die Benutzerfreundlichkeit der vorgeschlagenen Maßnahmen

4. **Auf welche Arten von Zielobjekten ist der Baustein B 1.9 Hard- und Software-Management anzuwenden?**
   a) auf alle IT-Systeme oder Gruppen von IT-Systemen
   b) auf alle identifizieren Anwendungen
   c) auf alle Server oder Gruppen von Servern eines Informationsverbundes
   d) auf den gesamten Informationsverbund

5. **Welche Bausteine werden bei der Modellierung mit einem Server mit dem Betriebssystem Windows Server 2003 verknüpft?**
   a) B 1.9 *Hard- und Software-Management*
   b) B 1.14 *Patch- und Änderungsmanagement*
   c) B 3.101 *Allgemeiner Server*
   d) B 3.108 *Windows Server 2003*

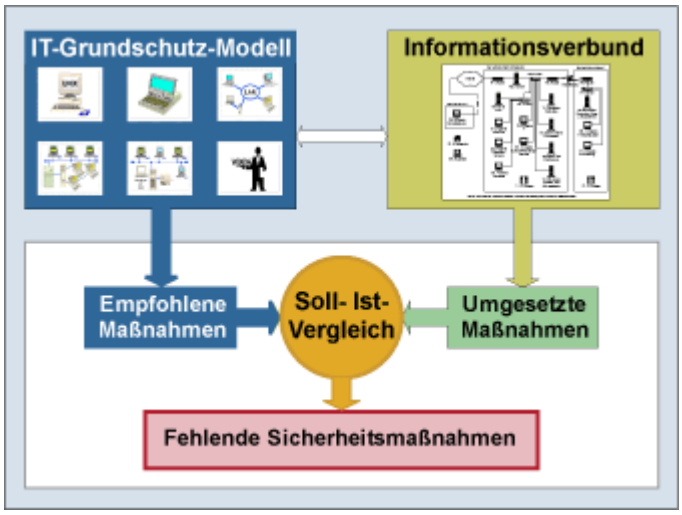
6. **Wann ist gemäß IT-Grundschutz-Vorgehensweise der Baustein B 1.7 *Kryptokonzept* für einen Informationsverbund anzuwenden?**
   a) immer
   b) sofern im Informationsverbund besondere Anforderungen an die Vertraulichkeit von Informationen gestellt werden
   c) wenn der zuständige IT-Sicherheitsbeauftragte dies befürwortet
   d) nur bei großen Informationsverbünden

Kapitel 6: Basis-Sicherheitscheck

6.1 Überblick

Sind meine Informationen und meine Informationstechnik hinreichend geschützt? Was bleibt noch zu tun?

Der Basis-Sicherheitscheck ist ein effizientes Instrument zur Beantwortung dieser Fragen. Das Vorgehen ist im Prinzip denkbar einfach: Die bereits umgesetzten Sicherheitsmaßnahmen werden mit den Empfehlungen der IT-Grundschutz-Kataloge 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 der anzuwendenden Bausteine einen **Prüfplan** (**„IT-Grundschutz-Modell“**) für die verschiedenen **Zielobjekte** (gesamter Informationsverbund, Räume, IT-Systeme, Kommunikationsverbindungen, Anwendungen) zusammengestellt.

Den Prüfplan wenden Sie beim Basis-Sicherheitscheck an, indem Sie für jedes Zielobjekt und für jede Maßnahme, die in den zugehörigen Bausteinen empfohlen wird, beurteilen,

- ob sie überhaupt auf das Zielobjekt anzuwenden ist, und falls ja,
- ob sie vollständig, teilweise oder überhaupt nicht umgesetzt ist.

Wie Sie beim Basis-Sicherheitscheck im Einzelnen vorgehen, worauf Sie achten sollten und wie Sie die Ergebnisse dokumentieren und auswerten können, erfahren Sie auf den nachfolgenden Seiten.

Basis-Sicherheitscheck und ergänzende Sicherheitsanalyse

Zuvor noch eine Anmerkung zum Stellenwert des Basis-Sicherheitschecks: Die IT-Grundschutz-Bausteine sind auf die üblicherweise eingesetzte Informationstechnik und ein Sicherheitsniveau ausgerichtet, das zumindest für den normalen Schutzbedarf angemessen und für den höheren Schutzbedarf ausbaufähig ist. Sollte der Basis-Sicherheitscheck ergeben, dass alle Standard-Sicherheitsmaßnahmen konsequent umgesetzt sind, so sind weitergehende Sicherheitsmaßnahmen damit zwar oft nicht mehr erforderlich, ihre Notwendigkeit kann aber – abhängig vom Schutzbedarf – nicht pauschal ausgeschlossen werden.

Die Frage, ob Sicherheitsmaßnahmen erforderlich sind, die über den Grundschutz hinausgehen, ist mit Hilfe zusätzlicher Sicherheitsanalysen zu klären. In Kapitel 7 ist beschrieben, wie Sie dazu vorgehen.

6.2 Hinweise zu den Maßnahmen

Um Ihnen die Durchführung eines Basis-Sicherheitschecks zu vereinfachen, werden auf den nächsten Seiten zunächst einige Besonderheiten der Maßnahmen-Empfehlungen der IT-Grundschutz-Kataloge beschrieben.

6.2.1 Zertifikatsrelevanz der Maßnahmen

In den Bausteinen ist zu jeder Maßnahme durch einen der drei Buchstaben „A“, „B“ und „C“ vermerkt, für welche Stufe der IT-Grundschutz-Qualifizierung sie umgesetzt sein sollte. Die Umsetzung aller derart gekennzeichneten Maßnahmen bietet für Komponenten mit einem normalen Schutzbedarf einen Grundschutz gegen die meisten relevanten Gefährdungen – und dies im Allgemeinen zu vergleichsweise geringen Kosten. Dieser Basisschutz soll gleichzeitig für Objekte mit höherem Schutzbedarf ausbaufähig sein. Daher enthalten die Bausteine auch Verweise auf Maßnahmen, mit denen sich das Sicherheitsniveau weiter verbessern lässt. Solche Maßnahmen sind durch ein **„Z“** als **zusätzlich** gekennzeichnet.

Als Beispiel ist nachfolgend das Maßnahmenbündel für den Baustein B 2.4 *Serverraum* abgebildet.

Planung und Konzeption

- M 1.3 (A) *Angepasste Aufteilung der Stromkreise*
- M 1.7 (A) *Handfeuerlöscher*
- M 1.10 (C) *Verwendung von Sicherheitstüren und -fenstern*
- M 1.18 (Z) *Gefahrenmeldeanlage*
- M 1.24 (B) *Vermeidung von wasserführenden Leitungen*
- M 1.26 (W) *Not-Aus-Schalter*
- M 1.27 (B) *Klimatisierung*
- M 1.28 (B) *Lokale unterbrechungsfreie Stromversorgung*
- M 1.31 (Z) *Fernanzeige von Störungen*
- M 1.52 (Z) *Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur*
- M 1.58 (A) *Technische und organisatorische Vorgaben für Serverräume*

- M 1.62 (C) *Brandschutz von Patchfeldern*

Umsetzung

- M 2.17 (A) *Zutrittsregelung und -kontrolle*
- M 2.21 (A) *Rauchverbot*

Betrieb

- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 1.23 (A) *Abgeschlossene Türen*

Wie Sie an der Maßnahme M 1.26 *Not-Aus-Schalter* erkennen können, gibt es eine weitere Kennzeichnung und zwar ein „W“ (= „Wissen“). Mit diesem Zeichen sind Maßnahmen gekennzeichnet, die Hintergrundwissen zu einem Sachverhalt liefern, nicht aber (beispielsweise im Rahmen eines Audits) zu überprüfende Maßnahmen.

Überprüfung zusätzlicher Maßnahmen

Für den normalen Schutzbedarf reichen die mit „A“, „B“ oder „C“ markierten Maßnahmen aus, für höheren Schutzbedarf sind zusätzliche Maßnahmen zu ergreifen, z. B. die mit „Z“ gekennzeichneten. Dies bedeutet jedoch nicht, dass bei einem Basis-Sicherheitscheck die Umsetzung dieser Maßnahmen nur dann geprüft werden sollte, wenn der Schutzbedarf eines Serverraums als hoch oder sehr hoch eingestuft ist. So könnte eine der zusätzlichen Maßnahmen bereits in einem Unternehmen umgesetzt sein, obwohl der Schutzbedarf des betreffenden Serverraums dies nicht unbedingt erfordern würde. In diesem Fall können Sie unter Umständen Umsetzungsfehler identifizieren, wenn Sie die betreffende Maßnahme überprüfen, beispielsweise den Verzicht auf regelmäßige Funktionstests einer installierten Gefahrenmeldeanlage.

Maßnahmen, die als zusätzlich gekennzeichnet sind, gehen häufig über den normalen Schutzbedarf hinaus und müssen geprüft werden, wenn sie umgesetzt sind.

6.2.2 Bestandteile einer Maßnahme

Im Allgemeinen enthält eine Maßnahme die folgenden drei Abschnitte:

- **Verantwortlichkeiten**
  Hier ist angegeben, welche Organisationseinheit oder Person üblicherweise jeweils für die Initiierung und die Umsetzung einer Maßnahme verantwortlich ist oder sein sollte. Sie können auf diese Angaben bei der Realisierungsplanung zurückgreifen, wenn es darum geht, die Verantwortung für die Umsetzung ausstehender Maßnahmen festzulegen.
- **Maßnahmentext**
  Dieser benennt und erläutert die einzelnen Empfehlungen zum jeweiligen Sachverhalt.
- **Prüffragen**
  Diese Fragen können als Checkliste für die Prüfung der Maßnahme etwa im Rahmen einer Revision oder eines Zertifizierungsaudits benutzt werden.

Einige Maßnahmen enthaltenen anstelle der Prüffragen noch den Punkt **Ergänzende Kontrollfragen**. Die dort aufgeführten Fragen betonen abschließend Aspekte, die für die Umsetzung der beschriebenen Maßnahme wesentlich sind, oder ergänzen den Maßnahmentext um noch nicht angesprochene Aspekte, sind aber, anders als die Prüffragen, nicht auf Vollständigkeit hin angelegt.

Eine Maßnahme umfasst in der Regel eine Reihe von verbindlichen Empfehlungen und zusätzlich solche, die ersatzweise oder ergänzend umgesetzt werden können. Nachfolgend sehen Sie als Beispiel die Maßnahme M 1.24 *Vermeidung von wasserführenden Leitungen*.

M 1.24 Vermeidung von wasserführenden Leitungen

Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT

Verantwortlich für Umsetzung: Haustechnik, Administrator

In Räumen oder Bereichen, in denen sich IT-Geräte mit zentralen Funktionen wie z. B. Server befinden, sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wasserführenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen, möglichst außerhalb des Raumes oder Bereiches, versehen werden. Außerhalb der Heizperiode sind diese Ventile zu schließen.

Sind wasserführende Leitungen unvermeidbar, müssen Vorkehrungen getroffen werden, einen Wasseraustritt möglichst frühzeitig zu erkennen bzw. die negativen Auswirkungen zu minimieren. Als Minimalschutz kann eine Wasserauffangwanne oder -rinne unter der Leitung angebracht werden, deren Ablauf außerhalb des Raumes führt. Günstig ist es, dazu den Flur zu nutzen, da so ein eventueller Leitungsschaden früher entdeckt wird. Zur frühzeitigen Erkennung von Wassereinbrüchen oder undichten Leitungen hat es sich bewährt, Decken hell zu streichen. Durch Sichtprüfungen müssen die vorhandenen Wasserleitungen regelmäßig auf ihre Dichtigkeit hin überprüft werden.

Es ist zu erwägen, wasserführende Leitung durch Wassermelder zu überwachen. Dafür können besondere Meldekabel unterhalb von Leitungen verlegt werden. Werden diese an eine Wassermeldeanlage angeschlossen, ist darüber eine schnelle und recht genaue Lokalisierung des Wasseraustritts möglich. Eine solche Anlage muss auf eine ständig besetzte Stelle aufgeschaltet werden, um in Verbindung mit entsprechenden Reaktionsplänen und einer aktuellen Dokumentation ein schnelles Eingreifen möglich zu machen. Optional können Wassermelder mit automatisch arbeitenden Magnetventilen eingebaut werden. Diese Magnetventile sind außerhalb des Raumes bzw. Bereiches einzubauen. Damit die Ventile auch bei Stromausfall ihre Schutzfunktion erfüllen, müssen sie im stromlosen Zustand geschlossen sein.

Als zusätzliche oder alternative Maßnahme empfiehlt sich ggf. eine selbsttätige Entwässerung (siehe M 1.14 Selbsttätige Entwässerung).

Alle Mitarbeiter im Bereich der IT und der Haustechnik sollten darüber informiert sein, dass in Gebäudeteilen mit IT-Systemen mit hohen Verfügbarkeitsanforderungen wasserführende Leitungen problematisch sind und was zu beachten ist. Es sollten Reaktionspläne vorhanden sein, in denen beschrieben ist, welche Maßnahmen bei Wasserleckagen zu ergreifen sind.

Prüffragen:

Werden eventuell vorhandene Wasserleitungen regelmäßig auf ihre Dichtigkeit hin überprüft (Sichtprüfung)?

Gibt es Reaktionspläne, die zielgerichtete Handlungen bei Meldung von Wasserleckagen vorgeben?

Beim Basis-Sicherheitscheck prüfen Sie, ob die **verbindlichen Empfehlungen** einer Maßnahme vollständig und wirksam umgesetzt sind oder nicht. So lautet die verbindliche Empfehlung im obigen Beispiel, auf wasserführende Leitungen möglichst zu verzichten. Falls diese unvermeidbar sind, sind ersatzweise Vorkehrungen zu treffen, um Wasseraustritt frühzeitig zu erkennen und dessen Auswirkungen zu begrenzen. Die Beispiele für Ersatzmaßnahmen (z. B. Auffangwanne,

Wassermelder) sind dagegen **optionale Empfehlungen**, aus denen Sie die für Ihren Einsatzbereich zweckmäßigsten Maßnahmen auswählen können.

Verbindliche Anforderungen werden in den IT-Grundschutz-Maßnahmen durch Formulierungen ausgedrückt wie „Es muss getan werden“, „Es sollte getan werden“ oder „Es ist zu tun“. Optionale Empfehlungen erkennen Sie dagegen an Formulierungen wie „Es kann getan werden“ oder „Es sollte überlegt werden, etwas zu tun“.

Wird in einer Maßnahme auf eine andere Maßnahme verwiesen, ...

... dann brauchen Sie die Umsetzung der Maßnahme, auf die verwiesen wird, im gegebenen Kontext nur dann zu überprüfen, wenn der Text der Maßnahme dies ausdrücklich verlangt. Im obigen Beispiel ist dies nicht der Fall: Der Hinweis auf die Maßnahme M 1.14 dient lediglich als Empfehlung.

Und welche Bedeutung haben die Prüffragen für den Basis-Sicherheitscheck?

Die Prüffragen ersetzen die bisherigen Kontrollfragen am Ende einer Maßnahmen. Sie sollen als letzte Checkliste dienen, um die Umsetzung der Maßnahme bei einem Basis-Sicherheitscheck, eine Revision oder einem Zertifizierungsaudit prüfen zu können. Die in einer Prüffrage angesprochenen Aspekte sollten folglich in dem betrachteten Informationsverbund angemessen berücksichtigt sein.

6.2.3 Konkrete und generische Maßnahmen

Abhängig vom jeweiligen Baustein sind die zugeordneten Maßnahmen unterschiedlich konkret formuliert. Dies bedeutet natürlich auch, dass ihre Umsetzung unterschiedlich einfach zu überprüfen ist.

Konkrete und techniknahe Maßnahmen

In Bausteinen, die sich auf ein bestimmtes technisches System beziehen, finden Sie Maßnahmen, die sehr detailliert beschreiben, welche Einstellungen an diesem System vorzunehmen sind. Ein Beispiel hierfür ist M 4.56 *Sicheres Löschen unter Windows-Betriebssystemen,* in der Empfehlungen dazu gegeben werden, wie verhindert werden kann, dass gelöschte Daten nachträglich rekonstruiert werden.

Die Umsetzung derart techniknaher Empfehlungen können Sie leicht anhand der Konfiguration eines gegebenen Rechners überprüfen.

Generische Maßnahmen

Meistens sind die Empfehlungen jedoch offener gehalten und damit auf eine Vielzahl von Einsatzbereichen anwendbar (generische Maßnahmen). Auch hierfür ein Beispiel, ein Ausschnitt aus M 4.2 *Bildschirmsperre*:

> „(...) Die Bildschirmsperre sollte sich sowohl manuell vom Benutzer aktivieren lassen, als auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch gestartet werden. Alle Benutzer sollten dafür sensibilisiert sein, dass sie die Bildschirmsperre aktivieren, wenn sie den Arbeitsplatz für eine kurze Zeit verlassen. Bei längeren Abwesenheiten sollten Benutzer sich abmelden.
> Der Zeitraum, nach dem sich eine Bildschirmsperre wegen fehlender Benutzereingaben aktiviert, sollte gewisse Grenzen weder unter- noch überschreiten. Der Zeitraum sollte nicht zu knapp gewählt werden, damit die Bildschirmsperre nicht bereits nach kurzen Denkpausen anspringt. Dieser Zeitraum darf aber auf keinen Fall zu lang sein, damit die Abwesenheit des Benutzers nicht von Dritten ausgenutzt werden kann. Eine sinnvolle Vorgabe ist eine Zeitspanne von 15 Minuten. (...)“

Es wird hier gefordert, durch technische und organisatorische Maßnahmen für einen lokalen Zugriffsschutz auf die Rechner zu sorgen. Wie diese Anforderung umgesetzt werden kann, hängt von den jeweils vorhandenen technischen Bedingungen ab, insbesondere dem eingesetzten Betriebssystem. An dieser Stelle detaillierte technische Anforderungen zu nennen, wäre daher angesichts der Vielzahl der vorhandenen Systeme und ihrer kontinuierlichen Weiterentwicklung kaum möglich.

Beim Basis-Sicherheitscheck sollten Sie bei generischen Maßnahmen danach fragen, ob und wie eine Maßnahme umgesetzt wurde. Zum Beispiel: Welche technischen Vorkehrungen wurden zur Aktivierung der Bildschirmsperre getroffen? Aufgrund der gegebenen Antwort entscheiden und dokumentieren Sie dann, ob die Maßnahme **sinngemäß umgesetzt** ist, also den beabsichtigten Schutzzweck wirksam erfüllt.

6.2.4 Maßnahmen für Planungsphasen

Beim Basis-Sicherheitscheck benutzen Sie die Maßnahmenempfehlungen der IT-Grundschutz-Kataloge als Kriterien für die Überprüfung des Sicherheitsniveaus eines bestehenden Informationsverbundes. Wie im letzten Kapitel („Modellierung“) erwähnt wurde, dienen die Bausteine allerdings nicht nur als **Prüfplan**: So haben sie auch eine Bedeutung als **Entwicklungskonzept**, mit dem Sie Sicherheitsaspekte bereits bei der Planung neuer Informationstechnik angemessen berücksichtigen können. Aus diesem Grund enthalten die IT-Grundschutz-Kataloge auch eine Reihe von Maßnahmen, die sich ausdrücklich auf Planungsphasen beziehen und für diese erforderliches Hintergrundwissen und Handlungsempfehlungen geben.

So gibt es Maßnahmen, die

- ausschließlich **Hintergrundwissen** enthalten, das Ihnen bei der Entscheidung über die einzusetzende Sicherheitstechnik helfen kann, z. B.
  M 4.90 *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells,*
- Sie bei der **Produktauswahl** unterstützen, z. B.
  M 2.75 *Geeignete Auswahl eines Application-Level-Gateways*,
  M 2.124 *Geeignete Auswahl einer Datenbank-Software*,
- Aspekte benennen, die in **Planungsphasen** zu berücksichtigen sind, z. B.
  M 2.315 *Planung des Server-Einsatzes*,
  M 4.250 *Auswahl eines zentralen, netzbasierten Authentisierungsdienstes*.

Bei einem Basis-Sicherheitscheck erübrigt es sich, die Umsetzung von Maßnahmen zu prüfen, die ausschließlich Hintergrundwissen enthalten. Solche Maßnahmen sind mit einem „W“ gekennzeichnet. Wenn das betreffende Zielobjekt bereits im Einsatz ist, gilt dies auch für viele Aspekte von Maßnahmen, die die Produktauswahl unterstützen oder Planungsphasen gewidmet sind. Prüfen Sie diejenigen Aspekte, die Auswirkungen auf den laufenden Betrieb haben können.

So enthält M 2.75 *Geeignete Auswahl eines Application-Level-Gateways* eine Vielzahl an Anforderungen, die an ein Application-Level-Gateway gestellt werden können, angefangen mit der Unterstützung aller wesentlichen Protokolle der Anwendungsschicht bis hin zur VPN-Fähigkeit. Im Rahmen des Basis-Sicherheitschecks müsste geprüft werden, ob das eingesetzte Produkt diesen Anforderungen entspricht oder nicht.

6.2.5 Zusammenfassung der Hinweise zu den Maßnahmen

Abschließend eine Zusammenfassung der wichtigsten Hinweise:

- Maßnahmen, die durch ein „Z“ als **zusätzlich** gekennzeichnet sind, geben Sicherheitsempfehlungen, die über den normalen Schutzbedarf oder typische Informationsverbünde hinausführen. Falls solche Maßnahmen umgesetzt wurden, sollten sie auch in Prüfungen einbezogen werden.
- Die Umsetzung **techniknaher Empfehlungen** kann unmittelbar anhand der Konfiguration eines IT-Systems überprüft werden.
- Bei **generischen Maßnahmen** prüfen Sie, ob diese sinngemäß umgesetzt sind, also die Art ihrer Umsetzung den beabsichtigten Schutzzweck wirksam unterstützt.
- Die Überprüfung der Umsetzung erübrigt sich bei mit „W“ gekennzeichneten Maßnahmen, die ausschließlich **Hintergrundwissen** enthalten.
- Bei Maßnahmen, die die Produktauswahl unterstützen oder **Planungsphasen** gewidmet sind, kann sich die Überprüfung auf die Aspekte beschränken, die offensichtliche Konsequenzen für den laufenden Betrieb haben, falls das betreffende Zielobjekt bereits im Einsatz ist.

6.3 Vorgehen beim Basis-Sicherheitscheck

6.3.1 Empfehlungen

Grundlage des Basis-Sicherheitschecks ist das in der Modellierung aufgrund der vorhandenen Informationstechnik und ihres Schutzbedarfs zusammengestellte IT-Grundschutz-Modell des Informationsverbundes. In diesem Modell ist festgelegt, welche Bausteine und damit Maßnahmenbündel für die verschiedenen Zielobjekte des Informationsverbundes anzuwenden sind.

Den Umsetzungsgrad der einzelnen Maßnahmen für das jeweilige Zielobjekt ermitteln und dokumentieren Sie beim Basis-Sicherheitscheck in Interviews mit den zuständigen Mitarbeitern und Überprü-

fungen vor Ort, z. B. der Begehung von Serverräumen oder der Kontrolle von Konfigurationseinstellungen.

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

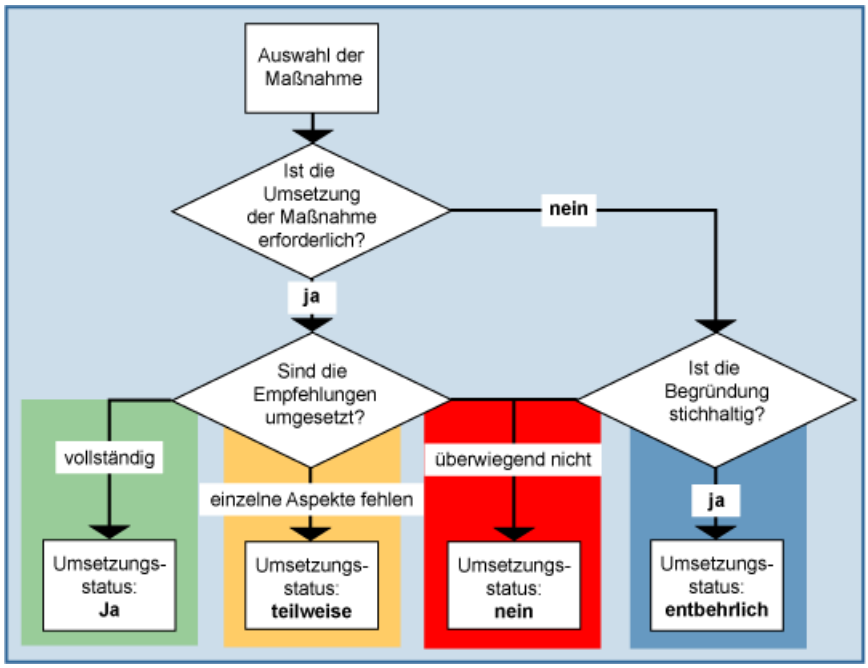
- Zunächst die wichtigste Regel:
  Die Informationstechnik ändert sich kontinuierlich, sodass regelmäßig geprüft werden muss, ob die eingeführten Sicherheitsmaßnahmen noch einen angemessenen Schutz bieten. Aus diesem Grund werden die IT-Grundschutz-Kataloge fortlaufend angepasst und um neue Bausteine ergänzt. Benutzen Sie bitte für den Basis-Sicherheitscheck die **aktuelle Version der IT-Grundschutz-Kataloge**, da nur diese einen dem Stand der Technik entsprechenden Grundschutz unterstützt.
- Die vorhandenen **Dokumente** über sicherheitsrelevante Abläufe, Regelungen und Sachverhalte enthalten bereits viele Informationen, die Ihnen bei der Ermittlung des Umsetzungsgrads der Maßnahmen helfen können. Sichten Sie diese Papiere daher 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 im Übrigen oft direkt aus dem sachlichen Zusammenhang der jeweiligen Bausteine: So können Mitarbeiter der Personalabteilung oder Benutzerbetreuer gute Ansprechpartner für den Baustein B 1.2 *Personal* sein, während es sich anbietet, für die Bausteine der Schichten IT-Systeme, Netze und 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 Maßnahmenbeschreibungen kennen, deren Umsetzungsstatus Sie überprüfen. Gegebenenfalls können stichpunktartige **Zusammenfassungen** zu einzelnen Maßnahmen nützlich sein.
- Zuletzt noch ein ebenso selbstverständlicher Hinweis: Der Basis-Sicherheitscheck 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.

6.3.2 Dokumentation

Den **Umsetzungsgrad** der IT-Grundschutz-Empfehlungen für die verschiedenen Komponenten des betrachteten Informationsverbundes dokumentieren Sie mit folgenden Kategorien:

- **„entbehrlich“**, wenn die Umsetzung der Empfehlungen nicht notwendig ist, da den möglichen Gefährdungen mit mindestens gleichwertigen Ersatzmaßnahmen entgegengewirkt wird (z. B. erübrigen sich Passwortregeln, wenn Chipkarten für die Authentisierung eingesetzt werden) oder wenn die Empfehlungen für den betrachteten Einsatzzweck nicht relevant sind (so ist M 5.33 *Absicherung von Fernwartung* nur dann bedeutsam, wenn tatsächlich auch Systeme von entfernten Standorten aus gewartet werden),
- **„ja“**, wenn alle Empfehlungen in der Maßnahme vollständig und wirksam umgesetzt sind,
- **„teilweise“**, wenn einige der Empfehlungen umgesetzt sind, andere noch nicht oder nur teilweise,
- **„nein“**, wenn die Empfehlungen der Maßnahme größtenteils noch nicht umgesetzt sind.

Die folgende Abbildung veranschaulicht den Entscheidungsprozess:



Damit die Ergebnisse des Basis-Sicherheitschecks später und auch von Dritten nachvollzogen und gegebenenfalls überprüft werden können, ist es wichtig, dass Sie diese sorgfältig dokumentieren. Vergessen Sie nicht, bei Maßnahmen, die Sie als entbehrlich, nur teilweise oder nicht umgesetzt eingestuft haben, in der Dokumentation Ihre **Begründung** 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 Basis-Sicherheitschecks mit **Hilfsmitteln** vereinfachen:

- So finden Sie unter den Hilfsmitteln zum IT-Grundschutz Formblätter für die IT-Grundschutz-Erhebung für alle Bausteine.
- Entsprechende Formulare bietet auch GSTOOL. Bei Verwendung des Tools haben Sie den zusätzlichen Vorteil, dass die Daten der Strukturanalyse für die Dokumentation des Basis-Sicherheitschecks konsistent übernommen werden.

Sowohl die Checklisten im Anhang der IT-Grundschutz-Kataloge als auch die Formulare des GSTOOLs enthalten weitere Felder, 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 Basis-Sicherheitscheck ist es noch nicht erforderlich, diese Felder auszufüllen.

6.4 Beispiel

Nachfolgend finden Sie einen Ausschnitt des Erhebungsformulars für den Serverraum der RECPLAST GmbH im Verwaltungsgebäude in Bad Godesberg.

Raum: BG, R. 1.02 Serverraum
erfasst am: 19. August erfasst durch: P. Muster
Baustein: B 2.4 *Serverraum*
Befragung am: 19. August
Leiter der Befragung: P. Muster
befragte Personen: A. Admin (Leiter IT), M. Wachsam (Haustechnik)

Maßnahmen

Maßnahme (erforderlich ab Siegelstufe)	**entbehrl.**	**ja**	**teilweise**	**nein**	**Bemerkung/Begründung bei Nicht-Umsetzung**
M 1.3 *Angepasste Aufteilung der Stromkreise* (A)				**X**	Bislang wurde die Elektroinstallation nicht geprüft.
M 1.7 *Handfeuerlöscher* (A)			**X**		Die betroffenen Mitarbeiter wurden nicht im Umgang mit den vorhandenen CO_2-Löschern geschult.
M 1.10 *Verwendung von Sicherheitstüren und -fenstern* (C)			**X**		Der Raum hat kein Sicherheitsfenster, nur eine Sicherheitstür.
M 1.15 *Geschlossene Fenster und Türen* (A)		**X**			Gemäß Dienstanweisung müssen Fenster und Türen bei Abwesenheit geschlossen sein.
M 1.18 *Gefahrenmeldeanlage* (Z)				**X**	Eine solche Anlage wurde bislang als unnötig und zu kostspielig eingestuft.
M 1.23 *Abgeschlossene Türen* (A)	**X**				Die Tür hat flurseitig einen Blindknauf.
M 1.24 *Vermeidung von wasserführenden Leitungen* (B)				**X**	Im Raum sind Heizkörper. Die Dichtigkeit der Leitungen wurde bislang nicht kontrolliert. Im Raum befindet sich ferner eine Klimaanlage mit Zuleitungen. Ein Rechner befindet sich direkt unter einer Zuleitung. Es fehlen Absperrventile außerhalb des Raums, mit denen die Wasserzufuhr zum Serverraum gezielt unterbrochen werden kann.
M 1.27 *Klimatisierung* (B)		**X**			
M 1.31 *Fernanzeige von Störungen* (Z)				**X**	Dies wurde bislang als unnötig teuer eingestuft.
M 1.52 *Redundanz,Modularität und Skalierbarkeit in der technischen Infrastruktur* (Z)	**X**				Es werden keine Ersatzgeräte vorrätig gehalten, da der IT-Lieferant vertraglich zugesichert hat, Ersatzgeräte innerhalb von 4 Stunden zu liefern.

6.5 Test zum Basis-Sicherheitscheck

Wenn Sie möchten, können Sie mit den nachfolgenden Fragen Ihre Kenntnisse zum Basis-Sicherheitscheck überprüfen. Die Auflösungen zu den Fragen finden Sie im Anhang.

Gegebenenfalls können auch mehrere Antwortmöglichkeiten zutreffend sein.

1. Welche Aussagen zum Basis-Sicherheitscheck sind zutreffend?

a) Ein Basis-Sicherheitscheck ermöglicht, Defizite bei der Umsetzung von Sicherheitsmaßnahmen zu ermitteln.

b) Bei einem Basis-Sicherheitscheck werden lediglich die als elementar gekennzeichneten IT-Grundschutz-Maßnahmen geprüft.

c) Ein Basis-Sicherheitscheck dient dazu, Sicherheitsprobleme zu identifizieren, die in einer Risikoanalyse genauer untersucht werden müssen.

d) Ein Basis-Sicherheitscheck ist ein Soll-Ist-Vergleich zwischen den erforderlichen und den tatsächlich umgesetzten Sicherheitsmaßnahmen.

2. Welche Vorarbeiten erfordert der Basis-Sicherheitscheck?

a) die Festlegung eines Zeitplans

b) die Auswahl von geeigneten Gesprächspartnern

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

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

3. Welche Verfahren nutzen Sie, um in einem Basis-Sicherheitscheck 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 beurteilen Sie eine Maßnahme zu Schutz eines IT-Systems in einem Basis-Sicherheitscheck als umgesetzt?

a) wenn alle wesentlichen Empfehlungen der zugehörigen Maßnahmenbeschreibung 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 Basis-Sicherheitscheck mit Maßnahmen, die durch ein „z“ als zusätzlich gekennzeichnet sind?

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

b) Sie streichen die Maßnahmen aus Ihrem Sollkonzept.

c) Sie überprüfen die Umsetzung dieser Maßnahmen nur dann, wenn das betreffende Objekt einen hohen oder sehr hohen Schutzbedarf hat.

d) Sie überprüfen diese Maßnahmen, sofern Sie in Ihrer Einrichtung umgesetzt sind.

6. Sie stellen fest, dass eine wichtige IT-Grundschutz-Maßnahme für ein IT-System nicht umgesetzt ist, das nur noch kurze Zeit in Betrieb ist. Wie behandeln Sie diese Maßnahme beim Basis-Sicherheitscheck?

a) Sie streichen die Maßnahme aus dem IT-Grundschutz-Modell.

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

c) Sie dokumentieren diese als nicht umgesetzt, und merken gegebenenfalls an, dass geprüft werden muss, ob eine nachträgliche Umsetzung angesichts der kurzen Einsatzzeit des IT-Systems noch angemessen ist.

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

Kapitel 7: Risikoanalyse

7.1 Überblick

Der IT-Grundschutz bietet für **typische Infrastrukturen** mit normalem Schutzbedarf ein **angemessenes und kostengünstiges Sicherheitsniveau**. Wie verfahren Sie aber, wenn

- eine Komponente einen **hohen oder sehr hohen Bedarf** an Vertraulichkeit, Integrität oder Verfügbarkeit hat,
- die IT-Grundschutz-Kataloge (noch) **keinen passenden Baustein** enthalten (Beispiel: Labormessgerät mit direkter Netzanbindung) oder aber
- ein solcher Baustein zwar vorhanden ist, die Komponente allerdings in einer für das Anwendungsgebiet des IT-Grundschutzes **untypischen Weise** oder Einsatzumgebung betrieben wird?

Zwei (rhetorische) Fragen:

Vergessen Sie in diesen Fällen den IT-Grundschutz, weil diese ja nicht dessen Anwendungsgebiet zu entsprechen scheinen?

Selbstverständlich nicht, denn die Umsetzung der IT-Grundschutz-Maßnahmen bietet meistens auch eine gute Basis für die Absicherung hochgradig schutzbedürftiger Systeme und Anwendungen. Unter Umständen erübrigen sich aufwändigere oder kostspieligere Maßnahmen.

Können Sie sich jedoch darauf verlassen, dass Sie hinreichend sicher sind, wenn Sie den IT-Grundschutz umgesetzt haben?

Umgekehrt können Sie sich aber auch nicht darauf verlassen, dass die IT-Grundschutz-Maßnahmen in den oben genannten Fällen eine ausreichende Sicherheit bieten. Ohne sorgfältige Prüfung, ob zusätzliche oder wirksamere Maßnahmen erforderlich sind oder nicht, gehen Sie in allen oben genannten Fällen möglicherweise unvertretbare Risiken ein.

Die Lösung:

In einer **ergänzenden Sicherheitsanalyse** prüfen Sie, wie diejenigen Zielobjekte zu behandeln sind, die eines der drei oben genannten Kriterien erfüllen. Diese Überlegungen können zu dem Ergebnis führen, dass die Umsetzung der IT-Grundschutz-Maßnahmen genügt und kein zusätzlicher Analysebedarf besteht. Sie können aber auch einen **Bedarf an zusätzlichen oder höherwertigen Maßnahmen** aufzeigen.

Für deren Auswahl sind unterschiedliche Verfahren möglich. So kann es für spezielle IT-Systeme genügen, die Sicherheitsempfehlungen der Hersteller umzusetzen. Andere Zielobjekte können intensivere Untersuchungen

zu den Risiken, die mit ihnen verbunden sind, und den Auswirkungen möglicher Gegenmaßnahmen erfordern. Ein übliches Verfahren dafür ist die sogenannte **Risikoanalyse**. Es gibt zahlreiche Varianten, die meisten sind recht aufwändig und verlangen ein sehr spezielles Expertenwissen.

Zur Erleichterung notwendiger zusätzlicher Sicherheitsanalysen hat das BSI eine eigene Methode für eine **Risikoanalyse auf der Basis von IT-Grundschutz** entwickelt. Auf den folgenden Seiten wird diese Methode mit Hilfe eines Beispiels veranschaulicht. Ausführlich dargestellt ist sie in BSI-Standard 100-3: *Risikoanalyse auf der Basis von IT-Grundschutz.*

7.2 Ergänzende Sicherheitsanalyse

Ausgangssituation

Voraussetzung für eine ergänzende Sicherheitsanalyse ist, dass Sie für den betrachteten Informationsverbund die Schritte Strukturanalyse, Schutzbedarfsfeststellung, Modellierung und Basis-Sicherheitscheck durchgeführt haben. Ferner hat sich gezeigt, dass für einzelne Zielobjekte die IT-Grundschutz-Maßnahmen unter Umständen keine hinreichende Sicherheit bieten, sei es,

- weil diese einen hohen oder sehr hohen Bedarf an Vertraulichkeit, Integrität oder Verfügbarkeit haben,
- es keinen hinreichend geeigneten IT-Grundschutz-Baustein gibt oder aber
- ein solcher zwar vorhanden ist, das Zielobjekt aber in einer für das Anwendungsgebiet des IT-Grundschutzes untypischen Weise oder Einsatzumgebung betrieben wird.

Die **ergänzende Sicherheitsanalyse** ist ein **Entscheidungsprozess**, aus dem sich ergibt, für welche dieser Zielobjekte weitergehende Untersuchungen erforderlich sind und für welche nicht.

Dazu zwei Beispiele aus der RECPLAST GmbH.

Beispiel 1: Risikoanalyse wird durchgeführt

Die Schutzbedarfsfeststellung bei der Beispielfirma RECPLAST GmbH ergab für mehrere Zielobjekte einen höheren Schutzbedarf in einem der drei Schutzziele. Auf den Clients der Entwicklungsabteilung werden beispielsweise hochgradig vertrauliche Daten bearbeitet und gespeichert, sodass man im IS-Management-Team darin übereinstimmte, für diese IT-Systeme eine Risikoanalyse durchzuführen. Bei dieser Untersuchung sollte ebenfalls die Sicherheit der Räume, in denen die Clients untergebracht sind, untersucht werden.

Beispiel 2: Zusätzliche IT-Grundschutz-Maßnahmen genügen

Auch für die beiden Anwendungen *Finanzbuchhaltung* und *Personaldatenverarbeitung* ergab die Schutzbedarfsfeststellung einen hohen Wert für Vertraulichkeit, der Schutzbedarf der Anwendung *Finanzbuchhaltung* bezüglich Integrität wurde ebenfalls mit hoch bewertet. Daraus wurde auch ein hoher Schutzbedarf abgeleitet bezüglich Integrität und Vertraulichkeit des Servers, auf dem die beiden Anwendungen betrieben werden (vgl. Kapitel 4.4 *Schutzbedarfsfeststellung für die IT-Systeme*).

Eine Diskussion dieses Befundes im IS-Management-Team ergab jedoch, dass für beide Anwendungen die Umsetzung der Maßnahme M 4.72 *Datenbank-Verschlüsselung* eine ausreichende Sicherheit für die Anwendungen und damit auch den Server bietet (diese Maßnahme ist im Baustein B 5.7 *Datenbanken* als zusätzlich gekennzeichnet).

Dokumentieren Sie die ergänzende Sicherheitsanalyse!

Ergebnis einer ergänzenden Sicherheitsanalyse sind Entscheidungen dazu, ob die IT-Grundschutz-Maßnahmen für die betrachteten Zielobjekte hinreichende Sicherheit bieten oder nicht und wie gegebenenfalls mit diesen weiter zu verfahren ist.

Für jedes Zielobjekt, das in der ergänzenden Sicherheitsanalyse betrachtet wird, sind die getroffenen Entscheidungen sorgfältig zu **begründen**, mit dem Management **abzustimmen** und nachvollziehbar in einem Managementreport zu **dokumentieren**. Eine solche Dokumentation ist auch Bestandteil der Dokumente, die für den Erwerb eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz erforderlich sind (siehe dazu *Kapitel 9: Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz*).

7.3 Risikoanalyse – traditionelles Vorgehen und Ansatz des BSI

Zur Beurteilung von Gefährdungsszenarien ist die Risikoanalyse ein weitverbreitetes und auf vielen Fachgebieten angewendetes Verfahren. Bei einer klassischen, quantitativen Risikoanalyse wird dabei das **Risiko**, dem ein Objekt ausgesetzt ist, in Abhängigkeit von der **Eintrittswahrscheinlichkeit** eines Schadensereignisses und der möglichen **Schadenshöhe** definiert. Es werden daher

- in einer **Bedrohungsanalyse** die Bedrohungen, denen ein System ausgesetzt ist, und
- in einer **Schwachstellenanalyse** die Angriffspunkte, aufgrund derer die Bedrohungen erst wirksam werden können,

eingeschätzt. Anschließend wird unter Berücksichtigung von vermuteten Eintrittswahrscheinlichkeiten und ebenso angenommenen Schadensausmaßen das individuelle Risiko eines Systems bestimmt und bewertet. Die mit Hilfe einer Risikoanalyse auszuwählenden Sicherheitsmaßnahmen sollen die Risiken verringern, also die Eintrittswahrscheinlichkeiten oder Schadensausmaße auf ein vertretbares Restrisiko senken. Gleichzeitig sollen sie in einem (insbesondere auch in finanzieller Hinsicht) angemessenen Verhältnis zur vermuteten Schadenshöhe stehen.

Probleme

Dieses auf den ersten Blick plausible Vorgehen hat allerdings einige Tücken:

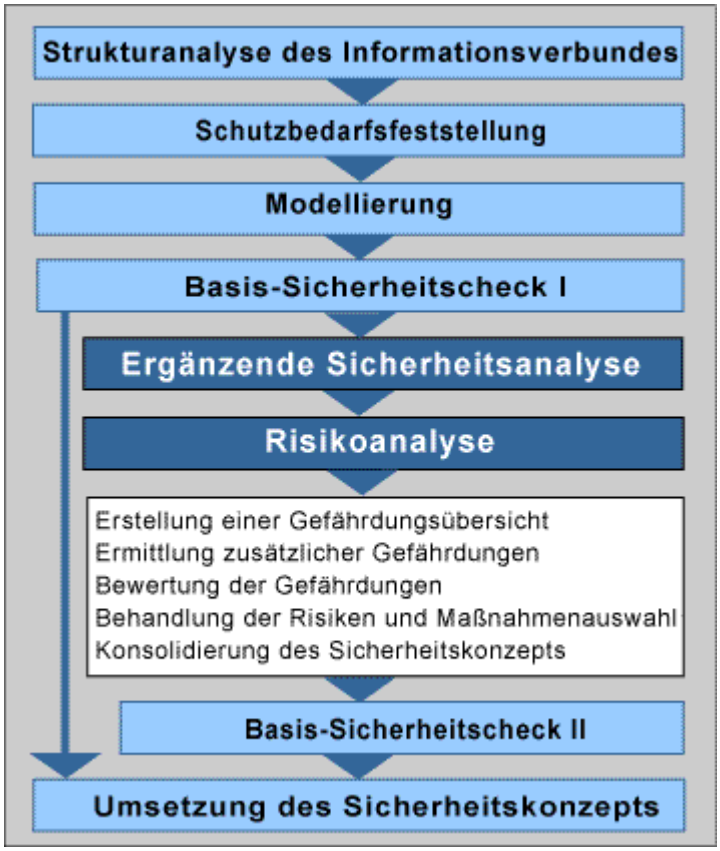
- So täuscht es eine Berechenbarkeit vor, die in der Praxis nicht gegeben ist. Für den Bereich der Informationssicherheit gibt es für die meisten Szenarien beispielsweise immer noch keine wirklich verlässlichen statistischen Daten über die Häufigkeit sicherheitsrelevanter Vorgänge und die Höhe der dabei entstandenen Schäden. Und selbst wenn diese ermittelt wären, blieben Projektionen auf zukünftige Ereignisse hochgradig spekulativ.
- Eine Risikoanalyse ist ein aufwändiges Verfahren und verlangt ein umfangreiches Expertenwissen, viel Sorgfalt und auch eine gewisse Unabhängigkeit des Durchführenden. Aber auch dann, wenn diese Voraussetzungen gegeben sind, bleibt das Verfahren fehleranfällig. Und dies nicht ohne Konsequenzen: Aus zu hoch eingeschätzten Eintrittswahrscheinlichkeiten kann ein unnötiger Sicherheitsaufwand resultieren, werden sie dagegen viel zu niedrig bemessen, so kann dies zum Verzicht auf notwendige Sicherheitsmaßnahmen führen – und dies mit möglicherweise gravierenden Folgen.

Lösungsvorschlag des BSI

Gemäß ISO 27001 enthält ein Managementsystem zur Gewährleistung von Informationssicherheit Verfahren zur Identifikation, Bewertung und Behandlung von Risiken. Diese Anforderung erfüllt die IT-Grundschutz-Vorgehensweise mit einem zweistufigen Verfahren:

1. Für übliche Informationstechnik und normalen Schutzbedarf greifen Sie auf die IT-Grundschutz-Bausteine (und die diesen zugrunde liegende qualitative Risikobewertung) zurück.
2. Für hochschutzbedürftige Objekte und beim Fehlen geeigneter IT-Grundschutz-Maßnahmen führen Sie zusätzliche Sicherheitsuntersuchungen durch.

Bei der Risikoanalyse auf der Basis von IT-Grundschutz verwenden Sie die Gefährdungskataloge als Ausgangspunkt dieser Untersuchungen und prüfen, ob gegebenenfalls weitere Gefährdungen zu berücksichtigen sind. Die folgende Abbildung zeigt die Einzelschritte des Verfahrens und wie es in die IT-Grundschutz-Vorgehensweise eingeordnet ist.



Anders als bei der traditionellen Risikoanalyse verzichten Sie bei dem auf den folgenden Seiten vorgestellten Verfahren auf eine explizite Berechnung von Eintrittswahrscheinlichkeiten und auf eigenständige Untersuchungen von Bedrohungen, Schwachstellen und Risiken.

Anstelle der Risikoanalyse auf der Basis von IT-Grundschutz können Sie selbstverständlich auch eine klassische Risikoanalyse anwenden.

Ein Hinweis zur Einordnung der Risikoanalyse in die IT-Grundschutz-Vorgehensweise:

Abweichend von der obigen Darstellung bietet es sich unter Umständen an, eine Risikoanalyse erst nach Umsetzung der IT-Grundschutz-Maßnahmen durchzuführen. Dies kann beispielsweise bei Zielobjekten, die bereits im Einsatz sind und die hinreichend durch IT-Grundschutz-Bausteine dargestellt werden können, sinnvoll sein. Als Entscheidungshilfe dazu, nach welchem Schritt eine Risikoanalyse sinnvoll ist, finden Sie eine Zusammenstellung der Vor- und Nachteile der möglichen Zeitpunkte neben weiteren Informationen zur Einordnung der ergänzenden Risikoanalyse in Kapitel 4.6.3 von BSI-Standard: *100-2: IT-Grundschutz-Vorgehensweise*.

7.4 Erstellung der Gefährdungsübersicht

Ausgangspunkt für die ergänzende Risikoanalyse ist eine Tabelle mit der für den Informationsverbund vorgenommenen Modellierung. Mit dieser Tabelle verfahren Sie wie folgt:

1. Reduzieren Sie den Informationsverbund auf diejenigen Zielobjekte, für die Sie in der ergänzenden Sicherheitsanalyse entschieden haben eine Risikoanalyse durchzuführen.
2. Streichen Sie anschließend alle Bausteine, für die keine Zielobjekte mehr vorhanden sind.

Die nachfolgende Tabelle zeigt einen Auszug der Tabelle, die sich nach diesen beiden Schritten für das Beispiel – die Räume der Entwicklungsabteilung und die in diesen befindlichen Clients – ergibt.

Nr.	Titel des Bausteins	Zielobjekt
B 1.0	Sicherheitsmanagement	Gesamte Organisation
B 1.1	Organisation	Gesamte Organisation
B 1.2	Personal	Gesamte Organisation
usw.	usw.	usw.
B 2.3	Büroraum	Räume 2.14 – 2.20 in Bonn-Beuel
B 3.201	Allgemeiner Client	C7 Clients in Entwicklungsabteilung
B 3.210	Client unter Windows Vista	C7 Clients in Entwicklungsabteilung

3. Stellen Sie anschließend für jedes betrachtete Zielobjekt eine Tabelle mit den Gefährdungen zusammen, auf die in den zugeordneten Bausteinen verwiesen wird.
4. Streichen Sie alle doppelt oder mehrfach genannten Gefährdungen.
5. Sortieren Sie die verbliebenen Gefährdungen thematisch, um die Tabellen übersichtlicher zu machen.
6. Vermerken Sie für jedes Zielobjekt und in allen drei Schutzzielen (Vertraulichkeit, Integrität, Verfügbarkeit) den ermittelten Schutzbedarf.

Nachfolgend sehen Sie einen Auszug der Tabelle, die sich als Ergebnis dieser Schritte für die Büroräume der Entwicklungsabteilung der Firma RECPLAST ergibt.

Zielobjekt:	Räume 2.14 – 2.20 in Bonn-Beuel
Vertraulichkeit: Integrität: Verfügbarkeit:	sehr hoch normal normal
G 2.1	Fehlende oder unzureichende Regelungen
G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal
usw.	usw.

Hinweise

Im Allgemeinen können Sie die Bausteine der Schicht 1 nicht streichen. Eine Ausnahme bilden Bausteine, die nur angewendet werden müssen, wenn spezielle Sachverhalte vorliegen. So können Sie häufig die Bausteine B 1.3 *Notfallmanagement* und B 1.8 *Behandlung von Sicherheitsvorfällen* vernachlässigen, wenn die in der Risikoanalyse betrachteten Zielobjekte nur normale Verfügbarkeitsanforderungen stellen, und den Baustein B 1.7 *Kryptokonzept*, wenn die betreffenden Zielobjekte keinen höheren Schutzbedarf bezüglich Vertraulichkeit oder Integrität haben.

7.5 Ermittlung zusätzlicher Gefährdungen

Auch wenn die Gefährdungskataloge vielfältige Bedrohungen berücksichtigen, denen Informationen und Informationstechnik ausgesetzt ist, und fortlaufend aktualisiert werden, so kann dennoch nicht ausgeschlossen werden, dass weitere Gefährdungen zu betrachten sind. Dies gilt insbesondere dann, wenn es für ein Zielobjekt keinen geeigneten Baustein gibt oder es in untypischen Einsatzszenarien betrieben wird.

Wie finden Sie zusätzliche Gefährdungen?

Ein bewährtes Mittel, diese Gefährdungen zu ermitteln, ist ein von einem IT-Sicherheitsbeauftragten 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, Publikationen im Internet und – selbstverständlich auch – die Gefährdungskataloge.

Worauf sollten Sie achten?

Unter Umständen können in dem Workshop zahlreiche und vielfältige Gefährdungen diskutiert werden. Um die sich anschließende Bewertung der Gefährdungen zu erleichtern, sollten Sie

- sich möglichst 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

In dem Workshop, der bei der RECPLAST GmbH zur Sicherheit der Entwicklungsabteilung stattfand, wurde Industriespionage als große Gefahr angesehen. Dabei wurde besonders lange über den Zutrittsschutz diskutiert, da die Räumlichkeiten bislang nicht anders gesichert waren als die anderen Büroräume der Firma. Da die sich daraus ergebenden Gefährdungen in den berücksichtigten Bausteinen bereits genannt sind, wurde die Gefährdungsübersicht zu den Räumen nicht erweitert. Hingegen wurde die Gefährdungsübersicht zu den IT-Systemen um die Gefährdung *Abhören der elektromagnetischen Abstrahlung von IT-Komponenten* ergänzt (siehe folgende Tabelle).

Zielobjekt: C 7 Clients in Entwicklungsabteilung	
Vertraulichkeit: Integrität: Verfügbarkeit:	sehr hoch normal normal
G 5.B1	Abhören der elektromagnetischen Abstrahlung von IT-Komponenten
	Die Informationen auf den Clients können das Ziel von Industriespionage sein. Die elektromagnetische Abstrahlung der Geräte kann für derartige Zwecke ausgespäht werden. Diese Gefährdung ist in den IT-Grundschutz-Katalogen nicht aufgeführt.

7.6 Bewertung der Gefährdungen

Aufgabe der Risikoanalyse ist es zu untersuchen, ob angesichts der Gefährdungslage ein **Bedarf an zusätzlichen Schutzmaßnahmen** besteht, und falls dem so ist, zweckmäßige Maßnahmen auszuwählen. Im nächsten Schritt prüfen Sie daher, ob auch nach Umsetzung der vorgesehenen Sicherheitsmaßnahmen noch Schwachstellen verbleiben. Dazu bewerten Sie für jede einzelne Gefährdung in der vervollständigten Gefährdungsübersicht, ob die bereits umgesetzten oder in Ihrem (bisherigen) Sicherheitskonzept enthaltenen Maßnahmen der Gefährdung vollständig, hinreichend stark und zuverlässig entgegenwirken.

- Bei der Prüfung auf **Vollständigkeit** prüfen Sie, ob die Maßnahmen Schutz gegen alle Aspekte der jeweiligen Gefährdung bieten (*Sind wirklich alle Türen geschlossen? Wurde auch an die Hintertür zum Gebäude gedacht?*).

- Bei der Prüfung auf **Mechanismenstärke** prüfen Sie, ob die Maßnahmen gegen die jeweilige Gefährdung hinreichend wirksam sind (*Wie einbruchssicher ist das Schließsystem? Wie sicher sind die verwendeten Schlüssel?*).
- Bei der Prüfung auf **Zuverlässigkeit** prüfen Sie, wie schwer es ist, die Maßnahmen zu umgehen (*Ist gewährleistet, dass nur Berechtigte Zugriff auf die Schlüssel haben? Wie sicherheitsbewusst gehen die Mitarbeiter mit den Schlüsseln um?*).

Dokumentation der Ergebnisse

Das Ergebnis dieser Prüfung dokumentieren Sie in einer eigenen Spalte OK der Gefährdungsübersicht wie folgt:

- Ein **„J“** tragen Sie ein, wenn
  - die vorhandenen oder geplanten Maßnahmen **ausreichenden Schutz** vor der jeweiligen Gefährdung bieten oder
  - die jeweilige Gefährdung nicht relevant ist (zum Beispiel, weil ein anderer Grundwert betroffen ist).
- Ein **„N“** tragen Sie ein, wenn die vorhandenen oder geplanten Maßnahmen **keinen ausreichenden Schutz** vor der jeweiligen Gefährdung bieten.

Als Ergebnis erhalten Sie eine Übersicht, aus der deutlich hervorgeht, bei welchen Gefährdungen noch Handlungsbedarf besteht und bei welchen nicht.

Beispiel

Die folgende Tabelle zeigt als Beispiel einen Ausschnitt der Gefährdungsbewertung für die Büroräume der Entwicklungsabteilung. Die Übersicht verdeutlicht, warum die vorhandenen Mechanismen zum Zugangsschutz zu den Räumen (und den IT-Systemen) als unzureichend eingestuft wurden.

Zielobjekt:	**Räume 2.14 – 2.20 in Bonn-Beuel**	
Vertraulichkeit: Integrität: Verfügbarkeit:	sehr hoch normal normal	
G 2.1	Fehlende oder unzureichende Regelungen	
	Der Zugang zu den Räumen ist bislang nicht ausreichend geregelt. Die bestehende Regelung reicht zwar für alle anderen Räumlichkeiten aus, wird aber den besonderen Anforderungen der Entwicklungsabteilung nicht gerecht.	OK=N
G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	
	Aufgrund der unzureichenden Regelungen kann ein unbefugter Zutritt nicht ausgeschlossen werden.	OK=N
G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen	
	Gefährdung ist für das Schutzziel Vertraulichkeit nicht relevant.	OK=J
G 3.6	Gefährdung durch Reinigungs- oder Fremdpersonal	
	Die bisherigen Regelungen für Reinigungs- und Fremdpersonal werden den besonderen Anforderungen dieser Räume nicht gerecht. Insbesondere sollte ein unbeaufsichtigter Zugang von Reinigungs- oder Wartungspersonal ausgeschlossen werden.	OK=N
usw.		

7.7 Behandlung der Risiken

7.7.1 Risikostrategien – Alternativen

In der Regel wird die Gefährdungsbewertung aufzeigen, dass nicht alle Gefährdungen durch das vorhandene Sicherheitskonzept ausreichend abgedeckt sind. Selbstverständlich sollten Sie es nicht bei einer solchen Erkenntnis belassen, sondern überlegen, wie angemessen mit den verbleibenden Gefährdungen umgegangen werden kann.

Grundsätzlich können vier Möglichkeiten unterschieden werden, mit Risiken umzugehen:

A: Risiko-Reduktion durch weitere Sicherheitsmaßnahmen

Die Risiken können durch zusätzliche, höherwertige Sicherheitsmaßnahmen verringert werden. Abhängig vom Typ des jeweiligen Zielobjekts finden Sie Hinweise auf geeignete Maßnahmen beispielsweise in Produktdokumentationen, in Standards zur Informationssicherheit oder in Fachveröffentlichungen. Vorschläge für höherwertige Sicherheitsmaßnahmen finden Sie auch in den IT-Grundschutz-Katalogen mit den als „zusätzlich“ gekennzeichneten Maßnahmen.

B: Risiko-Reduktion durch Umstrukturierung

Die Risiken können vermieden werden, indem der Informationsverbund so umstrukturiert wird, dass die Gefährdung nicht mehr wirksam werden kann.

C: Risiko-Übernahme

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.

D: Risiko-Transfer

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!

Auch für diese Entscheidung bietet sich ein Workshop an, bei der infrage kommende zusätzliche Sicherheitsmaßnahmen ermittelt und diskutiert werden. Die getroffenen Entscheidungen sollten Sie in der Gefährdungsübersicht dokumentieren.

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 untragbar sein werden. 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 und anstelle der Risiko-Übernahme (Option C) eine der drei anderen Risikostrategien zu wählen ist.

7.7.2 Dokumentation der gewählten Risikostrategie

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**.

Die folgenden Tabellen zeigen, welche Entscheidungen für das ausgewählte Beispiel getroffen wurden.

Zielobjekt:	**Räume 2.14 – 2.20 in Bonn-Beuel**
Vertraulichkeit: Integrität: Verfügbarkeit:	sehr hoch normal normal
G 2.1	Fehlende oder unzureichende Regelungen
„B“	Umstrukturierung: Die bestehenden Regelungen zum Zugangsschutz werden so geändert, dass auch Betriebsangehörige, Wartungsarbeiter und Reinigungskräfte die Räume der Entwicklungsabteilung nicht mehr unbeaufsichtigt betreten können. Für die Umsetzung der Regelung werden die entsprechenden Büroräume so verlegt, dass sie durch eine flurseitig mit einem Blindknauf versehene Zwischentür von den anderen Räumen abgetrennt sind.
G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen
	Siehe unter G 2.1.
usw.	

Zielobjekt:	**C7 Clients in Entwicklungsabteilung**
Vertraulichkeit: Integrität: Verfügbarkeit:	sehr hoch normal normal
G 5.B1	Abhören der elektromagnetischen Abstrahlung von IT-Komponenten
„A“ M 1.B1	Zusätzliche Sicherheitsmaßnahme Verringern der elektromagnetischen Abstrahlung von IT-Geräten Die elektromagnetische Abstrahlung der vorhandenen IT-Systeme wird von einer darauf spezialisierten Firma so weit reduziert, dass sie nicht mehr außerhalb der Büroräume wahrnehmbar ist.
usw.	

7.8 Abschließende Arbeiten

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

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 Sicherheitsmaßnahmen als auch zu Änderungen im bestehenden Konzept führen.

Weitere Informationen zur Konsolidierung von Sicherheitsmaßnahmen finden Sie in *Kapitel 8: Realisierungsplanung*.

Weitere Untersuchungen?

Sie können sich auch überlegen, ob neben der Risikoanalyse weitere Untersuchungen zur Verbesserung der Informationssicherheit sinnvoll sind – zum Beispiel Penetrationstests, mit denen Sie das Angriffsverhalten von Innen- und Außentätern simulieren. Auch die Ergebnisse dieser zusätzlichen Untersuchungen können das Sicherheitskonzept beeinflussen.

Fortführung des Sicherheitsprozesses

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

Ein zweiter Basis-Sicherheitscheck 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.

7.9 Test zur Risikoanalyse

Sie möchten, können Sie mit den nachfolgenden Fragen Ihre Kenntnisse zur ergänzenden heitsanalyse und zur Risikoanalyse überprüfen. Die Auflösungen zu den Fragen finden Sie im Anhang.

Gegebenenfalls können auch mehrere Antwortmöglichkeiten zutreffend sein.

1. **Was ist Aufgabe einer ergänzenden Sicherheitsanalyse?**
   a) Es wird entschieden, für welche Objekte eines Informationsverbundes eine Risikoanalyse durchgeführt wird.
   b) Es wird geprüft, ob die umgesetzten Sicherheitsmaßnahmen wirtschaftlich sind.
   c) Es wird entschieden, welche Risiken für einen Informationsverbund besonders relevant sind.
   d) Der Basis-Sicherheitscheck wird durch eine differenziertere Sicherheitsanalyse vertieft.

2. Die Verantwortung für die bei einer ergänzenden Sicherheitsanalyse getroffenen Entscheidungen trägt ...

a) … der für das jeweils betrachtete Objekt zuständige Mitarbeiter.

b) … die Leitung der Institution.

c) … der IT-Sicherheitsbeauftragte.

d) … das IS-Management-Team.

3. Welche Gefährdungen sind Ausgangspunkt bei einer Risikoanalyse auf Basis von IT-Grundschutz?

a) die im Anhang von BSI-Standard 100-3 enthaltenen Risikokataloge

b) die für die betrachteten Objekte relevanten Gefährdungen aus den IT-Grundschutz-Katalogen

c) die IT-bezogenen Gefährdungen aus den IT-Grundschutz-Katalogen

d) alle in den Gefährdungskatalogen enthaltenen übergreifenden Gefährdungen

4. Was prüfen Sie bei der Gefährdungsbewertung?

a) die Eintrittswahrscheinlichkeit einer Gefährdung

b) das mit einer Gefährdung verbundene Schadensausmaß

c) welches Schutzziel von einer Gefährdung betroffen ist

d) die Wirksamkeit der umgesetzten oder geplanten Maßnahmen gegen eine Gefährdung

5. 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 erforderlichen Finanzmittel dafür bereitstehen.

6. Wann ist es vertretbar, ein Risiko zu akzeptieren?

a) wenn der Aufwand für mögliche Schutzmaßnahmen unangemessen hoch ist

b) wenn vergleichbare Institutionen das Risiko auch akzeptieren

c) wenn die möglichen Schutzmaßnahmen verhindern, dass die Geschäftsprozesse hinreichend effizient durchgeführt werden können

d) wenn es bislang noch zu keinem nennenswerten Sicherheitsvorfall aufgrund der dem Risiko zugrunde liegenden Gefährdung gekommen ist

Kapitel 8: Realisierungsplanung

8.1 Überblick

In Ihrer Institution sind alle Standard-Sicherheitsmaßnahmen umgesetzt? Sie haben festgestellt, dass auch kein weiterer Schutz für diejenigen Zielobjekte erforderlich ist, die Sie in einer ergänzenden Sicherheitsanalyse oder zusätzlichen Risikoanalysen betrachtet haben? Dann können Sie sich vielleicht überlegen, ob Sie Ihr gutes Sicherheitsniveau durch ein Zertifikat bestätigen lassen, und direkt zur Lektüre des nächsten Kapitels übergehen.

Dies ist jedoch nicht die Regel: Irgendetwas fehlt 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.

Insbesondere dann, wenn viele Sicherheitsmaßnahmen umzusetzen sind, ist es hilfreich, wenn Sie sich bei der Umsetzungsplanung an die folgende Reihenfolge halten:

1. **Ergebnisse sichten**

   Sichten Sie zunächst die Ergebnisse des Basis-Sicherheitschecks und gegebenenfalls durchgeführter Risikoanalysen und stellen Sie die noch nicht oder nur teilweise umgesetzten Sicherheitsmaßnahmen tabellarisch zusammen.

2. **Maßnahmen konsolidieren**

   Prüfen und konkretisieren Sie die Maßnahmen im Zusammenhang. Dies reduziert gegebenenfalls die Anzahl der umzusetzenden Maßnahmen.

3. **Aufwand schätzen**

   Schätzen Sie den finanziellen und personellen Aufwand, der mit der Umsetzung der einzelnen Maßnahmen verbunden ist. Unterscheiden Sie dabei zwischen dem einmaligen Aufwand bei der Einführung einer Maßnahme und dem wiederkehrenden Aufwand im laufenden Betrieb.

4. **Umsetzungsreihenfolge festlegen**

   Legen Sie eine sinnvolle Umsetzungsreihenfolge fest. Berücksichtigen Sie dabei sowohl die sachlogischen Zusammenhänge der einzelnen Maßnahmen als auch deren Wirkung auf das Sicherheitsniveau des Informationsverbundes.

5. **Verantwortliche bestimmen**

   Entscheiden Sie, bis zu welchem Termin eine Maßnahme umzusetzen ist und wer für die Realisierung und deren Überwachung zuständig sein soll.

6. **Begleitende Maßnahmen festlegen**

   Die praktische Wirksamkeit der Sicherheitsmaßnahmen hängt von der Akzeptanz und dem Verhalten der betroffenen Mitarbeiter ab. Planen Sie daher Schritte zu ihrer Sensibilisierung und Schulung ein.

Die Schritte 1, 3 und 4 können entfallen, falls nur wenige Maßnahmen zu realisieren sind oder die Maßnahmen insgesamt nur geringe personelle und finanzielle Ressourcen benötigen.

8.2 Schritte 1 und 2

Auf dieser und den folgenden Seiten werden die einzelnen Schritte der Realisierungsplanung und die Aspekte, die bei diesen zu berücksichtigen sind, näher beschrieben.

Schritt 1: Ergebnisse sichten

Im ersten Schritt sind aus den Ergebnissen des Basis-Sicherheitschecks und eventuell durchgeführter Risikoanalysen diejenigen Maßnahmen herauszufiltern, die nicht oder nur teilweise umgesetzt sind.

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

Schritt 2: Maßnahmen konsolidieren

Anschließend betrachten Sie die Maßnahmen im Zusammenhang und prüfen,

- ob einzelne Maßnahmen überflüssig werden, weil andere umzusetzende Maßnahmen einen mindestens gleichwertigen Schutz für das jeweilige Zielobjekt bewirken,
- welche Maßnahmen noch konkretisiert und an die individuellen Gegebenheiten der Organisation 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 Umsetzungsaufwand auf das notwendige Maß zu begrenzen.

Das Ergebnis dieses Schritts ist eine auf die jeweilige Organisation 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 ergänzende Sicherheitsanalyse ergab, dass für eine Gruppe von Rechnern eine Authentisierung über ein chipkarten- oder token-basiertes Verfahren angewendet werden sollte, entfällt für diese IT-Systeme die Maßnahme M 4.48 *Passwortschutz unter NT-basierten Windows-Systemen* da durch die höherwertigen Maßnahmen der Funktionsumfang von M 4.48 vollständig abgedeckt wird.
- Fehler bei der Gebäudeplanung lassen sich nachträglich oft nur mit einem unverhältnismäßig hohen Aufwand korrigieren. Wenn die vollständige Umsetzung von Maßnahmen wie M 1.24 *Vermeidung von wasserführenden Leitungen* aufgrund der baulichen Gegebenheiten nicht

wirtschaftlich vertretbar ist, sollten zumindest Ersatzmaßnahmen getroffen werden, mit denen sich Wasserschäden frühzeitig erkennen und in den Auswirkungen begrenzen lassen. Beispielsweise können unter den vorhandenen Leitungen wasserableitende Bleche installiert werden, die von einem Wassermelder mit einer im ständig besetzten Pförtnerraum hörbaren Alarmsirene überwacht 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 unternehmenskritischer 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 ggf. 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.

8.3 Schritte 3 bis 5

Schritt 3: Kosten- und Aufwand 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 dritten Schritt, welcher einmalige und wiederkehrende finanzielle und personelle Aufwand durch die Umsetzung der einzelnen 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. Hierfür 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 Nicht-Umsetzung von Sicherheitsmaßnahmen entstehen, dem Management bewusst machen (als Argumentationshilfe können Sie die Kreuzreferenztabellen verwenden, die Sie unter den Hilfsmitteln zu den IT-Grundschutz-Katalogen finden und in denen dargestellt ist, gegen welche Gefährdungen eine Maßnahme hilft) und
- dafür sorgen, dass das Management bei der Entscheidung über das Budget durch Unterschrift dokumentiert, dass es bereit ist, die Restrisiken zu tragen.

Schritt 4: Umsetzungsreihenfolge festlegen

Wenn Budget oder Personal nicht ausreichen, alle wünschenswerten Sicherheitsmaßnahmen unmittelbar umzusetzen, ist eine sinnvolle Reihenfolge festzulegen. Diese ergibt sich teilweise aus sachlogischen Zusammenhängen der einzelnen Maßnahmen: So sind diejenigen Maßnahmen vorzuziehen, deren Umsetzung eine Voraussetzung für die Realisierung weiterer Maßnahmen ist.

Dazu ein Beispiel aus dem Baustein B 3.103 *Windows Server 2003*: Maßnahme M 2.364 *Planung der Administration für Windows Server 2003* ist vor Maßnahme M 4.281 *Sichere Installation und Bereitstellung von Windows Server 2003* umzusetzen.

Hinweis: Wie in B 3.103 finden Sie in allen Bausteinen an einem Lebenszyklus-Modell orientierte Erläuterungen zur folgerichtigen Umsetzung der zugehörigen Maßnahmen. Diese Darstellungen berücksichtigen die folgenden Phasen:

- Planung und Konzeption,
- Beschaffung (wo sinnvoll),
- Umsetzung,
- Betrieb,
- Aussonderung (soweit erforderlich) sowie
- Notfallvorsorge (als in allen Phasen zu berücksichtigende Querschnittsaufgabe).

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 vorrangig 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.

Einen Hinweis auf die Dringlichkeit, mit der einzelne Maßnahmen umzusetzen sind, bieten die Angaben zur Siegelstufe (A, B, C, Z oder W – siehe dazu die Tabelle in Kapitel *5.2 Bausteine*).

Schritt 5: Verantwortlichkeiten bestimmen

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 gegebenenfalls auch Fortbildungsmaßnahmen ein.

Als Orientierungshilfe für die Bestimmung der Verantwortlichkeiten enthalten die Maßnahmen Empfehlungen dazu, wer typischerweise für die Umsetzung und deren Initiierung zuständig sein sollte.

Die Kontrolle der Umsetzung sollte üblicherweise dem IT-Sicherheitsbeauftragte obliegen.

8.4 Schritt 6

Der Erfolg der Sicherheitsmaßnahmen hängt in einem entscheidenden Umfang davon ab, wie diese von den Mitarbeitern akzeptiert werden. Berücksichtigen Sie daher bei der Umsetzungsplanung Schulungs- und Sensibilisierungsmaßnahmen.

Planen Sie Schulungsmaßnahmen ein

Die Einführung neuer Sicherheitsmaßnahmen erfordert immer auch aufgaben- und produktbezogene Schulungsmaßnahmen für die betroffenen Mitarbeiter. Einige Beispiele:

- Wenn die Schnittstelle zum Internet durch ein Sicherheitsgateway geschützt werden soll, benötigt der zuständige Netzadministrator Kenntnisse über dessen sichere Installation, Konfiguration und Administration.
- Was nützt ein neu angeschaffter Feuerlöscher, wenn die Mitarbeiter im Brandfall nicht sachgerecht mit ihm umgehen können?
- Der Einsatz von Verschlüsselungssoftware zum Schutz der Vertraulichkeit personenbezogener oder unternehmenskritischer 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 wird gesichert, 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 Maßnahmen 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 Keilen 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 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 gegebenenfalls zusätzliche Sensibilisierungsmaßnahmen ein.

8.5 Beispiel für einen Realisierungsplan

Im **Realisierungsplan** sind für jede Maßnahme die folgenden Angaben festzuhalten:

- Spezifikation der Maßnahme (Nummer und Titel der Maßnahme, zugehöriger Baustein, Zielobjekt),
- spätester Umsetzungstermin,
- bereitgestellte finanzielle und personelle Ressourcen für die Einführung und den laufenden Betrieb der Maßnahme,
- Verantwortlicher für die Umsetzung und
- Verantwortlicher für die Kontrolle der Umsetzung.

Nachfolgend sehen Sie einen Ausschnitt aus der Liste der umzusetzenden Maßnahmen bei der LAST GmbH. Die Tabelle gibt den Stand der Umsetzungsplanung für den zentralen Serverraum in Bad Godesberg nach **Schritt 3, Konsolidierung der Maßnahmen,** wieder.

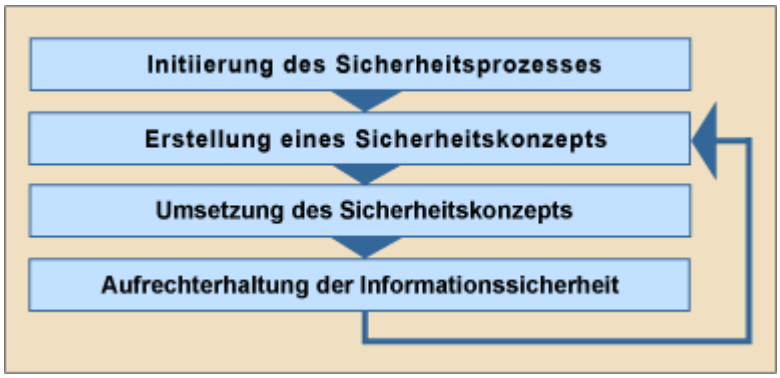
Legende: Z = Zusatzmaßnahme, PT = Personentage, KW = Kalenderwoche
a) Einmalige Investitionskosten b) Einmaliger Personalaufwand
c) Wiederkehrende Kosten d) Wiederkehrender Personalaufwand

Zielobjekt: BG R. 1.02 Serverraum		
Baustein: B 2.4 *Serverraum*		
Maßnahme (erforderlich ab Siegelstufe)	**Aufwand**	**Bemerkungen**
M 1.3 (A) *Angepasste Aufteilung der Stromkreise*	a) 0,- € b) 0,3 PT c) 0,- € d) 0,3 PT/Jahr	Die Elektro-Installation wird von der Haustechnik geprüft. Eine mindestens jährliche Überprüfung wird festgelegt.
M 1.7 (A) *Handfeuerlöscher*	a) 0,- € b) 0,3 PT c) 0,- € d) 0 PT/Jahr	Alle Mitarbeiter mit Zugangsberechtigung zum Serverraum sollen in die Handhabung der vorhandenen CO2-Löscher eingewiesen werden.
M 1.24 (C) *Vermeidung von wasserführenden Leitungen*	a) 20.000,- € b) 12 PT c) 0,- € d) 0 PT/Jahr	Die Maßnahme übersteigt das derzeit vorhandene Budget. Ersatzweise wird die Zusatzmaßnahme Z1 realisiert.
Z1: Einbau von Wasser ableitenden Blechen und Installation eines Wassermelders mit Sirene	a) 500,- € b) 1 PT c) 0,- € d) 0 PT/Jahr	Diese Maßnahme ersetzt Maßnahme M 1.24.

Die folgende Tabelle enthält den mit der Unternehmensleitung **abgestimmten Realisierungsplan** mit eingetragenen **Verantwortlichen** und **Umsetzungsterminen** für den Serverraum.

Zielobjekt: BG R. 1.02 Serverraum				
Baustein: B 2.4 Serverraum				
Maßnahme (erforderlich ab Siegelstufe)	**Umsetzung bis**	**Verantwortlich**	**Budget**	**Bemerkungen**
M 1.3 (A) *Angepasste Aufteilung der Stromkreise*	38. KW	Umsetzung: M. Wachsam Kontrolle: P. Muster	a) 0,- € b) 0,3 PT c) 0,- € d) 0 PT/Jahr	Die Elektro-Installation wird von der Haustechnik geprüft. Eine mindestens jährliche Überprüfung wird festgelegt.
M 1.7 (A) *Handfeuerlöscher*	38. KW	Umsetzung: M. Wachsam Kontrolle: P. Muster	a) 0,- € b) 0,3 PT c) 0,- € d) 0 PT/Jahr	Alle Mitarbeiter mit Zugangsberechtigung zum Serverraum sollen in die Handhabung der vorhandenen CO2-Löscher eingewiesen werden.
Z1: Einbau von Wasser ableitenden Blechen und Installation eines Wassermelders mit Sirene	39. KW	Umsetzung: M. Wachsam Kontrolle: P. Muster	a) 500,- € b) 1 PT c) 0,- € d) 0 PT/Jahr	Diese Maßnahme ersetzt Maßnahme M 1.24.

8.6 Aufrechterhaltung und Verbesserung der Informationssicherheit



Sie haben alle beschlossenen Sicherheitsmaßnahmen umgesetzt – ist damit Informationssicherheit dauerhaft gewährleistet?

Eine (nahezu) rhetorische Frage, denn Sicherheit lässt sich nur dann aufrechterhalten, wenn regelmäßig kontrolliert wird, ob die eingeführten organisatorischen Vorkehrungen und die umgesetzten Sicherheitsmaßnahmen noch angemessen und aktuell sind. Sie sollten daher regelmäßig prüfen, ob die im Sicherheitskonzept festgelegten Maßnahmen

- wie geplant umgesetzt sind und sie so funktionieren, wie es beabsichtigt war (= **Sicherheitsrevision**), sowie
- ob sie noch hinreichenden Schutz bieten und die Sicherheitsziele, die mit ihnen verfolgt werden, noch mit den aktuellen Gegebenheiten übereinstimmen (= **Vollständigkeits- oder Aktualisierungsprüfung**).

Sie sollten Ihr Sicherheitskonzept zu festgelegten Zeitpunkten mindestens alle zwei Jahre überprüfen, bei Bedarf aber auch vorzeitig – zum Beispiel nach Sicherheitsvorfällen.

Voraussetzung für die Aufrechterhaltung und Verbesserung der Informationssicherheit ist, dass geregelt ist, wer dafür zuständig ist, die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen zu überprüfen. Der Tätigkeit des IT-Sicherheitsbeauftragten und des IS-Management-Teams kommt hier besondere Bedeutung zu.

Zur Sicherheitsrevision und zu Aktualisierungsprüfungen siehe Maßnahme M 2.199 *Aufrechterhaltung der Informationssicherheit* der IT-Grundschutz-Kataloge. Eine ausführliche Darstellung zu den Aufgaben bei einer Revision der Informationssicherheit bietet der Leitfaden IS-Revision. Download unter bsi.bund.de → Themen → IS-Revision → Leitfaden.

8.7 Test zur Realisierungsplanung

Wenn Sie möchten, können Sie mit den nachfolgenden Fragen Ihre Kenntnisse zur Realisierungsplanung und zur Umsetzung von Sicherheitskonzepten überprüfen. Die Auflösungen zu den Fragen finden Sie im Anhang.

Gegebenenfalls können auch mehrere Antwortmöglichkeiten zutreffend sein.

1. **Wenn Sie die Umsetzung von Sicherheitsmaßnahmen planen, müssen Sie prüfen, ...**
   a) … welche begleitenden Maßnahmen erforderlich sind, damit die Maßnahme erfolgreich eingeführt werden kann.
   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. **Wer sollte in der Regel dafür zuständig sein, technische Maßnahmen zur Absicherung eines bestimmten IT-Systems umzusetzen?**
   a) die Leitung der IT-Abteilung
   b) der IT-Sicherheitsbeauftragte
   c) der zuständige Systemadministrator
   d) der Benutzer des IT-Systems

3. **Wer sollte üblicherweise prüfen, ob eine Sicherheitsmaßnahme wie geplant umgesetzt ist?**
   a) die Geschäftsführung
   b) der IT-Sicherheitsbeauftragte
   c) der zuständige IT-Administrator
   d) die Leitung der IT-Abteilung

4. **Welche Angaben aus den IT-Grundschutz-Katalogen unterstützen Sie bei der Planung der Umsetzungsreihenfolge von Maßnahmen?**
   a) die Verweise auf die Gefährdungslage am Beginn der Beschreibung einer Maßnahme
   b) die Einordnung der Maßnahme in einen Lebenszyklus
   c) die Kontrollfragen am Ende der Beschreibung einer Maßnahme
   d) die Angabe einer Priorität bei dem Verweis auf eine Maßnahme

5. 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

6. 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 des Institutionen

d) die Vollständigkeit des Sicherheitskonzepts

Kapitel 9: Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

9.1 Warum 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.

Seit dem Jahr 2005 gibt es mit der Norm **ISO 27001** einen international anerkannten Standard, mit dem Managementsysteme für Informationssicherheit zertifiziert werden können. Das **ISO 27001-Zertifikat auf Basis von IT-Grundschutz** ist an dieser Norm ausgerichtet. Es belegt in besonderer Weise das Bemühen um Informationssicherheit, da Grundlage für die Vergabe dieses Zertifikats nicht nur die Erfüllung der allgemeinen Anforderungen von ISO 27001 an das Sicherheitsmanagement ist, sondern auch die nachgewiesene Umsetzung der konkreten IT-Grundschutz-Maßnahmen.

Zielgruppen und Einsatzbereiche

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

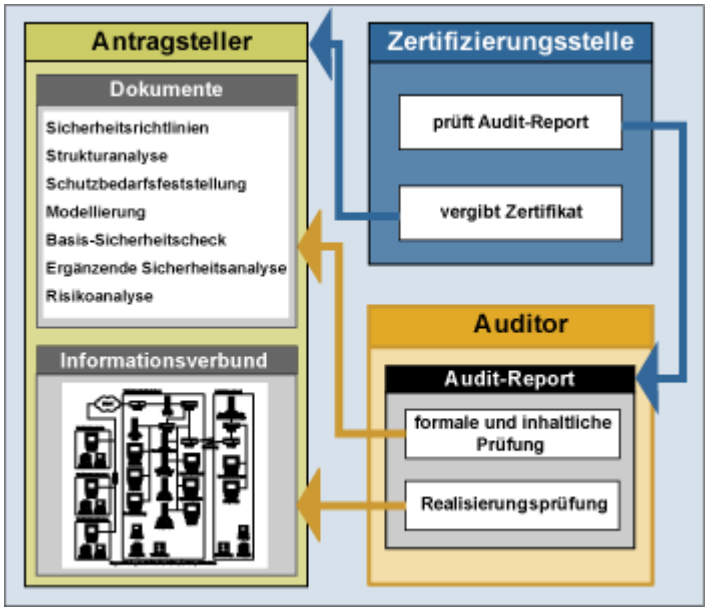
- Anbieter im E-Commerce oder E-Government, die verdeutlichen wollen, dass sie sorgfältig und sicherheitsbewusst mit den Daten der Kunden und Bürger umgehen,
- IT-Dienstleister, die mit einem allgemein anerkannten Maßstab die Sicherheit ihrer Dienstleistungen belegen wollen,
- Unternehmen und Behörden,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

Ein Zertifizierungsverfahren wirkt aber **auch nach innen**: Es sorgt für einen Grundschutz und trägt dazu bei, das Bewusstsein der Mitarbeiter für die Notwendigkeit von Informationssicherheit zu stärken.

9.2 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-Maßnahmen wirksam umgesetzt** sind. Gegenstand der Zertifizierung muss dabei nicht die gesamte Organisation 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**:



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

Phase 1 umfasst eine **Dokumentenprüfung** der so genanten Referenzdokumente des Antragstellers. Zu diesen Dokumenten gehören:

- Sicherheitsrichtlinien (zumindest: Leitlinie zur Informationssicherheit, Richtlinien zur Risikoanalyse, zur Lenkung von Dokumenten und Aufzeichnungen, zur internen Auditierung des Informationssicherheitsmanagements, zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen),
- Strukturanalyse,
- Schutzbedarfsfeststellung,
- Modellierung des Informationsverbundes,
- Basis-Sicherheitscheck,
- Ergänzende Sicherheitsanalyse sowie
- Risikoanalyse.

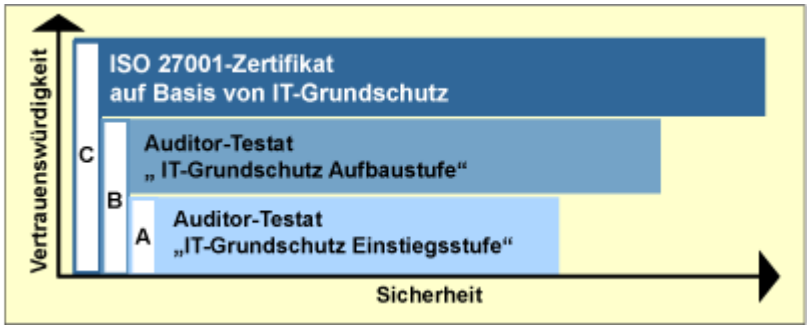
In **Phase 2** schließt sich eine Vor-Ort-Prüfung des Informationsverbundes durch den Auditor an, in der im realen Informationsverbund die praktische Umsetzung der in den Referenzdokumenten dokumentierten Sicherheitsmaßnahmen bezüglich ISO 27001 und IT-Grundschutz auf ihre Vollständigkeit, Korrektheit und Wirksamkeit hin überprüft wird (**Umsetzungsprüfung**).

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 durch ein jährlich zu wiederholendes Überwachungsaudit bestätigt werden.

Auditor-Testate zur Qualifizierung für die ISO 27001-Zertifizierung

Kosten und Aufwand für den Erwerb eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz sind vergleichsweise gering. Unter Umständen kann es allerdings für ein Unternehmen oder eine Behörde recht aufwändig sein, den IT-Grundschutz im erforderlichen Umfang umzusetzen. Daher gibt es als Vorstufe zum Zertifikat **zwei Qualifizierungsstufen**:

- ein **Auditor-Testat „IT-Grundschutz Einstiegsstufe“**, mit dem dokumentiert wird, dass die unabdingbaren Standard-Sicherheitsmaßnahmen wirksam umgesetzt sind, und
- ein **Auditor-Testat „IT-Grundschutz Aufbaustufe“**, mit dem dokumentiert wird, dass die wichtigsten Standard-Sicherheitsmaßnahmen wirksam umgesetzt sind.



Beide Testate werden nach vorangegangener Prüfung durch einen vom BSI zertifizierten Auditor erteilt. Sie bleiben zwei Jahre gültig und können nicht wiederholt werden.

9.3 Zusammenfassung

Die folgende Tabelle fasst die wesentlichen Informationen zur ISO 27001-Zertifizierung und zu den Auditor-Testaten zusammen:

	Auditor-Testat IT-Grundschutz Einstiegsstufe	**Auditor-Testat IT-Grundschutz Aufbaustufe**	**ISO 27001-Zertifikat auf der Basis von IT-Grundschutz**
Anforderungen an den Prüfer	ISO 27001-Grundschutz-Auditor	ISO 27001-Grundschutz-Auditor	ISO 27001-Grundschutz-Auditor
umzusetzende Maßnahmen	ca. 55 % (A)	ca. 72 % (A + B)	ca. 82 % (A + B + C)
Prüfung des Auditberichts	keine	keine	vertrauliche Prüfung durch das BSI
Kosten beim BSI	45,- €	45,- €	2.500,- €
Gültigkeit	2 Jahre	2 Jahre	3 Jahre (jährliches Überwachungsaudit)
wiederholbar	nein	nein	ja

Legende: A: unabdingbare Standardsicherheitsmaßnahmen; B: wichtigste Standardsicherheitsmaßnahmen; C: für das Zertifikat darüber hinaus erforderliche Maßnahmen

Die Honorarkosten des Auditors sind nicht in der Tabelle enthalten, da sie Verhandlungssache sind.

Umfassende Informationen zur ISO 27001-Zertifizierung auf Basis von IT-Grundschutz (z. B. Zertifizierungsschema, lizenzierte Auditoren, ausgestellte Zertifikate und Testate) finden Sie im Internet-Angebot des BSI unter dem Stichwort „IT-Grundschutz-Zertifikat“ und insbesondere in den folgenden beiden Dokumenten:

- Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz. (PDF)
  Dieses Dokument enthält das Prüfschema für ISO 27001-Audits.
- IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten (PDF)
  Dieses Dokument beschreibt die Anforderungen für die Zertifizierung ausgelagerter Bestandteile eines Informationsverbundes.

Ein Wort zum Schluss

Sie sind jetzt am Ende des Webkurses IT-Grundschutz angelangt. Schön, dass Sie es geschafft haben!

Wenn Sie zur Anwendung der IT-Grundschutz-Vorgehensweise oder der IT-Grundschutz-Kataloge noch Fragen, Anregungen oder Probleme haben, können Sie sich gerne mit uns in Verbindung setzen.

Tel.:0228 99 9582-5369
E-Mail: grundschutz@bsi.bund.de

Anhang 1: Auflösungen zu den Tests

Nachfolgend finden Sie die Auflösungen zu den Testfragen aus den Kapiteln 2 bis 7. Die richtigen Antworten sind **fett hervorgehoben** und mit einem Haken (✔) versehen.

Lösungen zu Kapitel 2: Sicherheitsmanagement

1. **Welches Modell liegt dem in BSI-Standard 100-1 beschriebenen Sicherheitsprozess zugrunde?**
   - **a) ein Zyklus aus den Schritten Plan, Do, Check und Act (✔)**
   - b) ein auf stetige Weiterentwicklung angelegtes Spiralmodell
   - c) das IT-Grundschutz-Modell
   - d) das Informationssicherheitsmodell

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 IT-Sicherheitsbeauftragte?**
   - a) **Sicherheitsvorfälle zu untersuchen (✔)**
   - b) **die Entwicklung von Sicherheitskonzepten zu koordinieren (✔)**
   - c) die eingesetzte Sicherheitstechnik zu konfigurieren
   - d) **der Leitungsebene über den Stand der Informationssicherheit zu berichten (✔)**

4. **Wie wird zweckmäßig ein IS-Management-Team gebildet?**
   - a) Alle Personen werden in das Team aufgenommen, die sich für die Aufgabe interessieren und sich freiwillig melden.
   - **b) Die Geschäftsleitung setzt ein IS-Management-Team aus Verantwortlichen für bestimmte IT-Systeme, Anwendungen, Datenschutz und IT-Service zusammen. (✔)**
   - c) Der IT-Leiter beauftragt fachkundige Mitarbeiter aus der IT-Abteilung.
   - d) Alle Abteilungs- oder Bereichsleitungen entsenden einen Vertreter aus ihrem jeweiligen Zuständigkeitsbereich in das Team.

5. Wer ist für die Bekanntgabe der Leitlinie zur Informationssicherheit verantwortlich?

a) das IS-Management-Team

b) der Sicherheitsbeauftragte

c) die Unternehmens- oder Behördenleitung (✔)

d) die Öffentlichkeitsabteilung eines Unternehmens oder einer Behörde

6. Welche Aufgabe obliegt dem Informationssicherheitsmanagement?

a) die Arbeitssicherheit

b) der Schutz der für die Geschäftsprozesse und Fachaufgaben einer Institution wichtigen Informationen (✔)

c) der Datenschutz

d) der Schutz der Informationstechnik

Lösungen zu Kapitel 3: Strukturanalyse

1. Bei der Festlegung des Informationsverbundes sollten Sie darauf achten, dass dieser ...

a) … möglichst viele Bereiche einer Institution umfasst.

b) … eindeutig und einfach gegen Bereiche innerhalb der Institution, die nicht einbezogen sind, abgegrenzt werden kann. (✔)

c) … eine sinnvolle Mindestgröße hat. (✔)

d) … vollständig mit allen externen Schnittstellen beschrieben wird. (✔)

2. Welche Ziele verfolgt die Strukturanalyse im Rahmen der IT-Grundschutz-Vorgehensweise?

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 IT-Grundschutz-Bausteine gibt

3. 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

4. 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 etc.) haben (✔)

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

c) wenn diese in denselben Räumlichkeiten untergebracht sind

d) wenn der Umfang der insgesamt erfassten Objekte zu groß zu werden droht

5. Welche der folgenden Aufgaben gehören gemäß BSI-Standard 100-2 zur Strukturanalyse?

a) die angemessene Gruppierung der Objekte, die in einem Sicherheitskonzept unterschieden werden müssen (✔)

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 (✔)

6. Welche der folgenden Aussagen für die Behandlung von Datenträgern bei der Strukturanalyse sind zutreffend?

a) Datenträger dienen lediglich als Backup-Medium und zu Übertragungszwecken und brauchen deswegen bei der Strukturanalyse nicht berücksichtigt zu werden.

b) Datenträger sollten in der Strukturanalyse berücksichtigt werden, wenn sie schutzbedürftige Informationen enthalten. (✔)

c) Datenträger, die fest mit einem IT-System verknüpft sind, werden bei der Strukturanalyse nicht erfasst. (✔)

d) Sie sollten auf eine angemessene Gruppierung der Datenträger achten, die Sie bei der Strukturanalyse erfassen. (✔)

Lösungen zu Kapitel 4: Schutzbedarfsfeststellung

1. Welche Schutzziele werden bei der Schutzbedarfsfeststellung gemäß IT-Grundschutz betrachtet?

a) Authentizität

b) **Verfügbarkeit (✔)**

c) **Vertraulichkeit (✔)**

d) **Integrität (✔)**

2. In welchen Fällen können Sie gemäß IT-Grundschutz-Vorgehensweise 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, 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 der Anwendung

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 unwesentliche Teile der Anwendungen bedient (✔)

c) wenn ein redundant ausgelegtes weiteres IT-System vorhanden ist, das die Funktionen unterstützt, die für die betreffenden Anwendungen benötigt werden (✔)

d) wenn die Anwendungen innerhalb der nächsten 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 insgesamt höheren Gesamtschaden addieren. (✔)

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

c) … der für das IT-System bestimmte Schutzbedarf sich auch auf den Schutzbedarf anderer mit dem betreffenden IT-System vernetzter IT-Systeme auswirkt.

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

Lösungen zu Kapitel 5: Modellierung gemäß IT-Grundschutz

1. **Welche Aufgaben stellen sich bei der Modellierung gemäß IT-Grundschutz?**
   - **a) Sie bilden den in der Strukturanalyse dokumentierten Informationsverbund mit Hilfe der IT-Grundschutz-Bausteine ab. (✔)**
   - b) Sie entwerfen die Sicherheitsarchitektur des betrachteten Informationsverbundes.
   - **c) Sie entwickeln zusätzliche Bausteine für solche Komponenten des Informationsverbundes, für die es keinen angemessenen Baustein in den IT-Grundschutz-Katalogen gibt. (✔)**
   - **d) Sie prüfen, welche IT-Grundschutz-Bausteine für den betrachteten Informationsverbund relevant sind. (✔)**

2. **Welche der folgenden Änderungen an den IT-Grundschutz-Bausteinen sind gemäß IT-Grundschutz-Vorgehensweise unter bestimmten Umständen im Rahmen der Modellierung zulässig?**
   - **a) die Konkretisierung von Maßnahmen um technische Details (✔)**
   - b) die Streichung von allzu kostspieligen Maßnahmen
   - **c) die Anpassung von Bezeichnungen (etwa für Rollen) an die Konventionen der betrachteten Institution (✔)**
   - **d) die Ergänzung eines Bausteins um zusätzliche Maßnahmen (✔)**

3. **Worauf sollten Sie achten, wenn Sie einen eigenen IT-Grundschutz-Baustein anfertigen?**
   - **a) auf die Wirtschaftlichkeit der vorgeschlagenen Maßnahmen (✔)**
   - **b) auf die Wirksamkeit der vorgeschlagenen Maßnahmen (✔)**
   - c) auf den Innovationsgrad der vorgeschlagenen Maßnahmen
   - **d) auf die Benutzerfreundlichkeit der vorgeschlagenen Maßnahmen (✔)**

4. **Auf welche Arten von Zielobjekten ist der Baustein B 1.9 Hard- und Software-Management anzuwenden?**
   - a) auf alle IT-Systeme oder Gruppen von IT-Systemen
   - b) auf alle identifizieren Anwendungen
   - c) auf alle Server oder Gruppen von Servern eines Informationsverbundes
   - **d) auf den gesamten Informationsverbund (✔)**

5. **Welche Bausteine werden bei der Modellierung mit einem Server mit dem Betriebssystem Windows Server 2003 verknüpft?**
   - a) B 1.9 *Hard- und Software-Management*
   - b) B 1.14 *Patch- und Änderungsmanagement*
   - **c) B 3.101 *Allgemeiner Server* (✔)**
   - **d) B 3.108 *Windows Server 2003* (✔)**

6. Wann ist gemäß IT-Grundschutz-Vorgehensweise der Baustein B 1.7 *Kryptokonzept* für einen Informationsverbund anzuwenden?

a) immer

b) sofern im Informationsverbund besondere Anforderungen an die Vertraulichkeit von Informationen gestellt werden (✔)

c) wenn der zuständige IT-Sicherheitsbeauftragte dies befürwortet

d) nur bei großen Informationsverbünden

Lösungen zu Kapitel 6: Basis-Sicherheitscheck

1. **Welche Aussagen zum Basis-Sicherheitscheck sind zutreffend?**
   - **a) Ein Basis-Sicherheitscheck ermöglicht, Defizite bei der Umsetzung von Sicherheitsmaßnahmen zu ermitteln. (✔)**
   - b) Bei einem Basis-Sicherheitscheck werden lediglich die als elementar gekennzeichneten IT-Grundschutz-Maßnahmen geprüft.
   - c) Ein Basis-Sicherheitscheck dient dazu, Sicherheitsprobleme zu identifizieren, die in einer Risikoanalyse genauer untersucht werden müssen.
   - **d) Ein Basis-Sicherheitscheck ist ein Soll-Ist-Vergleich zwischen den erforderlichen und den tatsächlich umgesetzten Sicherheitsmaßnahmen. (✔)**

2. **Welche Vorarbeiten erfordert der Basis-Sicherheitscheck?**
   - **a) die Festlegung eines Zeitplans (✔)**
   - **b) die Auswahl von geeigneten Gesprächspartnern (✔)**
   - c) einen Penetrationstest, um Schwachstellen zu identifizieren, die mit den ausgewählten Gesprächspartner erörtert werden
   - **d) die Zusammenstellung und Lektüre der vorhandenen Dokumente zur Informationssicherheit in dem betrachteten Informationsverbund (✔)**

3. **Welche Verfahren nutzen Sie, um in einem Basis-Sicherheitscheck 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 beurteilen Sie eine Maßnahme zu Schutz eines IT-Systems in einem Basis-Sicherheitscheck als umgesetzt?**
   - **a) wenn alle wesentlichen Empfehlungen der zugehörigen Maßnahmenbeschreibung 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 Basis-Sicherheitscheck mit Maßnahmen, die durch ein „z“ als zusätzlich gekennzeichnet sind?

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

b) Sie streichen die Maßnahmen aus Ihrem Sollkonzept.

c) Sie überprüfen die Umsetzung dieser Maßnahmen nur dann, wenn das betreffende Objekt einen hohen oder sehr hohen Schutzbedarf hat.

d) Sie überprüfen diese Maßnahmen, sofern Sie in Ihrer Einrichtung umgesetzt sind. (✔)

6. Sie stellen fest, dass eine wichtige IT-Grundschutz-Maßnahme für ein IT-System nicht umgesetzt ist, das nur noch kurze Zeit in Betrieb ist. Wie behandeln Sie diese Maßnahme beim Basis-Sicherheitscheck?

a) Sie streichen die Maßnahme aus dem IT-Grundschutz-Modell.

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

c) Sie dokumentieren diese als nicht umgesetzt, und merken gegebenenfalls an, dass geprüft werden muss, ob eine nachträgliche Umsetzung angesichts der kurzen Einsatzzeit des IT-Systems noch angemessen ist. (✔)

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

Lösungen zu Kapitel 7: Risikoanalyse

1. **Was ist Aufgabe einer ergänzenden Sicherheitsanalyse?**
   - **a) Es wird entschieden, für welche Objekte eines Informationsverbundes eine Risikoanalyse durchgeführt wird. (✔)**
   - b) Es wird geprüft, ob die umgesetzten Sicherheitsmaßnahmen wirtschaftlich sind.
   - c) Es wird entschieden, welche Risiken für einen Informationsverbund besonders relevant sind.
   - d) Der Basis-Sicherheitscheck wird durch eine differenziertere Sicherheitsanalyse vertieft.

2. **Die Verantwortung für die bei einer ergänzenden Sicherheitsanalyse getroffenen Entscheidungen trägt ...**
   - a) … der für das jeweils betrachtete Objekt zuständige Mitarbeiter.
   - **b) … die Leitung der Institution. (✔)**
   - c) … der IT-Sicherheitsbeauftragte
   - d) … das IS-Management-Team.

3. **Welche Gefährdungen sind Ausgangspunkt bei einer Risikoanalyse auf Basis von IT-Grundschutz?**
   - a) die im Anhang von BSI-Standard 100-3 enthaltenen Risikokataloge
   - **b) die für die betrachteten Objekte relevanten Gefährdungen aus den IT-Grundschutz-Katalogen (✔)**
   - c) die IT-bezogenen Gefährdungen aus den IT-Grundschutz-Katalogen
   - d) alle in den Gefährdungskatalogen enthaltenen übergreifenden Gefährdungen

4. **Was prüfen Sie bei der Gefährdungsbewertung?**
   - a) die Eintrittswahrscheinlichkeit einer Gefährdung
   - b) das mit einer Gefährdung verbundene Schadensausmaß
   - c) welches Schutzziel von einer Gefährdung betroffen ist
   - **d) die Wirksamkeit der umgesetzten oder geplanten Maßnahmen gegen eine Gefährdung (✔)**

5. **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 erforderlichen Finanzmittel dafür bereitstehen.

6. Wann ist es vertretbar, ein Risiko zu akzeptieren?

a) wenn der Aufwand für mögliche Schutzmaßnahmen unangemessen hoch ist (✔)

b) wenn vergleichbare Institutionen das Risiko auch akzeptieren

c) wenn die möglichen Schutzmaßnahmen verhindern, dass die Geschäftsprozesse hinreichend effizient durchgeführt werden können (✔)

d) wenn es bislang noch zu keinem nennenswerten Sicherheitsvorfall aufgrund der dem Risiko zugrunde liegenden Gefährdung gekommen ist

Lösungen zu Kapitel 8: Realisierungsplanung

1. **Wenn Sie die Umsetzung von Sicherheitsmaßnahmen planen, müssen Sie prüfen, ...**
   - **a) … welche begleitenden Maßnahmen erforderlich sind, damit die Maßnahme erfolgreich eingeführt werden kann. (✔)**
   - 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. **Wer sollte in der Regel dafür zuständig sein, technische Maßnahmen zur Absicherung eines bestimmten IT-Systems umzusetzen?**
   - a) die Leitung der IT-Abteilung
   - b) der IT-Sicherheitsbeauftragte
   - **c) der zuständige Systemadministrator (✔)**
   - d) der Benutzer des IT-Systems

3. **Wer sollte üblicherweise prüfen, ob eine Sicherheitsmaßnahme wie geplant umgesetzt ist?**
   - a) die Geschäftsführung
   - **b) der IT-Sicherheitsbeauftragte (✔)**
   - c) der zuständige IT-Administrator
   - d) die Leitung der IT-Abteilung

4. **Welche Angaben aus den IT-Grundschutz-Katalogen unterstützen Sie bei der Planung der Umsetzungsreihenfolge von Maßnahmen?**
   - a) die Verweise auf die Gefährdungslage am Beginn der Beschreibung einer Maßnahme
   - **b) die Einordnung der Maßnahme in einen Lebenszyklus (✔)**
   - c) die Kontrollfragen am Ende der Beschreibung einer Maßnahme
   - d) die Angabe einer Priorität bei dem Verweis auf eine Maßnahme

5. **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

6. 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 des Institutionen

d) die Vollständigkeit des Sicherheitskonzepts (✔)

Anhang 2: Kontakte

Herausgeber dieses Kurses

Bundesamt für Sicherheit in der Informationstechnik (BSI),
Referat 114 – IT-Sicherheitsmanagement und IT-Grundschutz
Postfach 20 03 63
53133 Bonn
Telefon: +49 (0) 228 99 9582-5369
Telefax: +49 (0) 228 99 9582-5405
E-Mail: grundschutz@bsi.bund.de

Entwickler dieses Kurses

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Bereich Anwendungs- und Prozesssicherheit (APS)
Schloss Birlinghoven
53754 Sankt Augustin
Telefon: +49 (0) 2241 14-3272
Telefax: +49 (0) 2241 14-3007