Bundesamt
für Sicherheit in der
Informationstechnik

IT-Grundschutz-Profile
– Strukturbeschreibung –

Version 1.0

Änderungshistorie

Version	Datum	Name	Beschreibung
0.1	22.01.18	BSI	Community Draft
1.0	28.09.18	BSI	Finale Version

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

Inhaltsverzeichnis

1 Einleitung

Diese Strukturbeschreibung gibt einen Überblick, wie ein IT-Grundschutz-Profil aufgebaut ist. Zur Verdeutlichung wird in jedem Kapitel ein Beispiel (in Blau) aufgeführt, das in dieser Form auch in einem IT-Grundschutz-Profil für eCommerce-Anbieter verwendet werden könnte.

Motivation

Die Cyber-Bedrohungslage stellt durch die immer professionelleren und ausgefeilteren Angriffe neue Anforderungen an die Informationssicherheit. Jede Institution muss ein individuelles Sicherheitskonzept für die internen Anforderungen erstellen, um die entstehenden Risiken zu minimieren. Je nachdem, welche Vorgehensweise des IT-Grundschutzes eine Institution ausgewählt hat, muss sie als nächstes diverse Rahmenbedingungen ermitteln, um in den eigentlichen Sicherheitsprozess einsteigen zu können. Dazu gehört zum Beispiel, die vorhandenen Geschäftsprozesse und Fachaufgaben, IT-Systeme, Anwendungen, Räume und Kommunikationsverbindungen zu identifizieren und den Schutzbedarf zu ermitteln. Außerdem gilt es, Bausteine zu modellieren, einen IT-Grundschutz-Check und unter Umständen eine Risikoanalyse durchzuführen. Über die IT-Grundschutz-Profile können diese Schritte für spezifische Anwendungsfelder vorab systematisiert angegangen werden. So können Institutionen mit diesen Mustern weiterarbeiten und viel Arbeit und Zeit sparen.

Zielsetzung IT-Grundschutz-Profile

Ziel der IT-Grundschutz-Profile ist es, für bestimmte Anwendungsfelder Musterszenarien anzubieten. Diese Szenarien sollen es den einzelnen Anwendern aus diesen Bereichen erleichtern, den Sicherheitsprozess nach IT-Grundschutz an ihre individuellen Rahmenbedingungen anzupassen. Ein IT-Grundschutz-Profil ist eine Schablone für einen ausgewählten Informationsverbund oder Geschäftsprozess, mit dem die IT-Grundschutz-Umsetzung für diesen Bereich konkretisiert wird. Über ein IT-Grundschutz-Profil werden verschiedene Schritte des Informationssicherheitsprozesses für einen definierten Anwendungsbereich so aufbereitet, dass es als Rahmen für Sicherheitskonzepte adaptiert werden kann. Dazu gehören:

- Festlegung des Anwendungsbereichs
- Durchführung einer verallgemeinerten Strukturanalyse, Schutzbedarfsfeststellung und Modellierung für diesen Bereich
- Auswahl und Anpassung von umzusetzenden IT-Grundschutz-Bausteinen
- Beschreibung spezifischer Sicherheitsanforderungen und Maßnahmen sowie
- gegebenenfalls eine Risikoanalyse und Risikobehandlung.

Um für ein spezifisches Anwendungsfeld die jeweiligen Anforderungen und passenden Sicherheitsempfehlungen zu identifizieren und in einem IT-Grundschutz-Profil abzubilden, sollten diese zusammen mit Vertretern der zukünftigen Anwender erstellt werden. Daher sollten IT-Grundschutz-Profile durch Gremien oder Anwendergruppen einer Branche

beziehungsweise durch Vertreter eines Themenbereichs erstellt werden. Unterstützt werden sie dabei durch das IT-Grundschutz-Team des BSI.

IT-Grundschutz-Profile sollten im Nachgang der interessierten Community zur Verfügung gestellt werden. Dadurch können Erfahrungen und Know-how geteilt und Synergieeffekte genutzt werden. In einer einzelnen Institution können sich die Verantwortlichen für Informationssicherheit dann künftig auf die Umsetzung von konkreten Sicherheitsempfehlungen konzentrieren. Von der Zeitersparnis sowie den geschonten personellen und finanziellen Ressourcen können alle beteiligten Institutionen profitieren. Mögliche Anwendungsbereiche für diese neuen IT-Grundschutz-Profile sind zum Beispiel:

- Kommunalverwaltungen,
- Krankenhäuser oder
- Wasserwerke als Kritische Infrastruktur.

Die von einer oder mehreren Institutionen einer bestimmten Branche oder durch einen Verband erstellten IT-Grundschutz-Profile können von weiteren Anwendern in ihre Sicherheitskonzepte integriert werden.

Auf Basis der IT-Grundschutz-Profile können neben Sicherheitskonzepten für Informationsverbünde auch einzelne Geschäftsprozesse oder Fachaufgaben abgebildet werden. Beispiele für den Bereich der öffentlichen Verwaltung sind Verfahren wie das Nationale Waffenregister (NWR) oder die "E-Akte".

Vorteile

IT-Grundschutz-Profile bieten den Vorteil, dass darüber Gremien ihren Anwendern künftig einen Werkzeugkasten zur Verfügung stellen können, der bereits auf ihre Spezifika, ihren Sprachgebrauch und ihr Hintergrundwissen angepasst wurde. Je nach den Sicherheitsanforderungen für den betrachteten Bereich, können die notwendigen Bestandteile des IT-Grundschutzes modular zusammengestellt werden. Dadurch sind Sicherheitskonzepte einer Branche nicht nur einfacher zu erstellen, sondern auch vergleichbarer.

Zielsetzung dieses Dokuments

Im vorliegenden Dokument wird der grundsätzliche Aufbau von IT-Grundschutz-Profilen beschrieben. Zusätzlich wird an einer beispielhaft dargestellten Referenzarchitektur von e-Commerce-Anbietern gezeigt, wie einzelne Strukturelemente eines IT-Grundschutz-Profils in der Praxis aussehen könnten. Beispiele innerhalb des Dokuments sind durch eine blaue Schrift hervorgehoben.

2 Struktur von IT-Grundschutz-Profilen

Im Folgenden wird dargestellt, wie ein IT-Grundschutz-Profil aufgebaut werden sollte. Der gezeigte Aufbau ist sinnvoll, denn damit werden keine Aspekte vergessen. Außerdem erleichtert ein einheitlicher Aufbau den Vergleich und die Anerkennung durch das BSI und die Aufnahme in das IT-Grundschutz-Profil Register. Je nach Einsatzszenario oder Anwendungszweck kann die Struktur eines IT-Grundschutz-Profils aber auch hiervon abweichen.

IT-Grundschutz-Profile sollten folgenden Aufbau aufweisen:

- Formale Aspekte (Herausgeber, Registrierungsnummer, Version, Laufzeit)
- Management Summary
- Geltungsbereich (Scope)
- Relevante Bausteine, Anforderungen und Maßnahmen
- Restrisikobetrachtung/Risikobehandlung
- Anwendungshinweise
- Unterstützende Informationen
- Anhang

2.1 Formale Aspekte

Der erste Abschnitt der IT-Grundschutz-Profile gibt einen Überblick über grundlegende formale Aspekte. Folgende Punkte sollten mindestens beschrieben werden:

- Titel (Kurztitel):

  Vollständiger Titel des IT-Grundschutz-Profils. Ein einprägsamer Kurztitel kann in Klammern angefügt werden.

- Autor:

  Personen bzw. Institutionen, die das IT-Grundschutz-Profil erstellt haben. Dies können z. B. Berater sein, die mit der Erstellung des IT-Grundschutz-Profils beauftragt wurden. Hier können auch einzelne Projekteilnehmer namentlich genannt werden.

- Herausgeber:

  Nennung der Branche, des Gremiums oder des Arbeitskreises

- IT-Grundschutz-Profil Registrierungsnummer:

  Eindeutiger Bezeichner für das IT-Grundschutz-Profil, der nach Überprüfung des IT-Grundschutz-Profils vom BSI vergeben wird.

- Versionsstand:

  Neben einer Registrierungsnummer wird jedes IT-Grundschutz-Profil auch mit einem Versionsstand versehen. So können die Anwender erkennen, wann das IT-Grundschutz-

Profil generiert beziehungsweise aktualisiert wurde und wann es das letzte Mal geprüft wurde.

Mindestens: Veröffentlichungsstatus, Versionsnummer, Datum der Erstellung. Bei etablierten und bereits veröffentlichten Dokumenten: Datum der letzten Änderung, Datum der letzten Prüfung.

- Revisionszyklus:

  Angabe, nach welcher Zeitspanne die Aktualität des Dokuments geprüft werden sollte.

- Vertraulichkeit:

  Hier kann auch eingetragen werden, ob das IT-Grundschutz-Profil offen oder vertraulich, und damit nur bestimmten Anwendern zugänglich ist.

  Eine Einstufung, beispielsweise nach TLP (Traffic Light Protocol) oder VSA (Verschlusssachenanweisung), ist hier möglich.

Beispiel: Formale Aspekte

Titel:	Elektronischer Handel über das Internet (eCommerce)
Autor:	BSG
Herausgeber:	AK eCom
Registrierungsnummer:	GS-PRO_2017-0001
Versionsstand:	Working Draft, Version 1 vom 07.02.2017
Revisionszyklus:	jährlich
Vertraulichkeit:	öffentlich

2.2 Management Summary

Der eigentliche Einstieg in ein IT-Grundschutz-Profil beginnt mit einem kurzen Überblick für das Management der Institution. Eilige Leser sollen in wenigen Zeilen über das Ziel und die Kernaussagen des IT-Grundschutz-Profils informiert werden. Hier wird außerdem die Zielgruppe beschrieben, die angesprochen werden soll. Zusätzlich können in diesem Überblick auch erste Handlungs- und Entscheidungsempfehlungen, etwa basierend auf der Risikobehandlung, integriert werden. Auch die wichtigsten Restrisiken sollten auf den ersten Blick erkennbar sein.

Folgende Aspekte sollten in einem Managementüberblick zusammengefasst werden:

- Kurzbeschreibung der adressierten Zielgruppe
- Kurzbeschreibung der Zielsetzung
- Aufgaben der Leitungsebene (Kurzbeschreibung von Handlungs- und Entscheidungsempfehlungen z. B. basierend auf den Ergebnissen der Risikobehandlung).

Beispiel: Management Summary

Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an eCommerce-Anbieter, die über das Internet Produkte und/oder Dienstleistungen anbieten und demzufolge regelmäßig mit Kundendaten operieren.

Zielsetzung

Es definiert einen Mindest-Schutzbedarf für die dabei verarbeiteten personenbezogenen Daten, die Zahlungsverkehrsdaten sowie für das eCommerce-Angebot. Neben den anzuwendenden Bausteinen gemäß der IT-Grundschutz-Vorgehensweise "Standardabsicherung", umfasst das IT-Grundschutz-Profil einen spezifischen Baustein "ePayment" sowie zusätzliche Einzelanforderungen.

Das BSI empfiehlt die Anwendung dieses IT-Grundschutz-Profils für eCommerce-Anbieter als Grundlage für die Sicherheitskonzeption.

2.3 Festlegung des Geltungsbereichs

Im Geltungsbereich wird beschrieben, was genau das IT-Grundschutz-Profil abdeckt, also für welche Art von Geschäftsprozessen und Informationsverbünden das IT-Grundschutz-Profil geeignet ist. Dazu gehört:

- eine Beschreibung der Zielgruppe, an die sich das vorliegende IT-Grundschutz-Profil richtet.
- eine Beschreibung des zugrunde gelegten Schutzbedarfs einschließlich einer Erläuterung.
- eine Beschreibung, welche der IT-Grundschutz-Vorgehensweisen Basis-, Standard- oder Kern-Absicherung bei der Erstellung des IT-Grundschutz-Profils zugrunde gelegt worden ist.

Zusätzlich sollten noch folgende Punkte aufgeführt werden:

- Abdeckung Vorgehensweise:

  Aussage darüber, welches Schutzniveau im Vergleich zu den Vorgehensweisen des IT-Grundschutzes mit dem IT-Grundschutz-Profil erreicht wird.

- ISO 27001-Kompatibilität:

  Zusätzlich sollte noch ein Überblick über die Kompatibilität zu anderen Standards der Informationssicherheit (z. B. ISO/IEC 27001:2013) gegeben werden. Wird mindestens die IT-Grundschutz-Vorgehensweise "Standardabsicherung" umgesetzt, ist diese zu der ISO 27001 kompatibel. Werden die Anforderungen gegenüber der "Standardabsicherung" nur zu einem geringeren Anteil erfüllt, ist zu prüfen, ob Kompatibilität zur ISO 27001 besteht, sofern eine solche Absicherung nötig ist.

- Rahmenbedingungen:

Aufführung von Rahmenbedingungen (z. B. Rechtsgrundlagen) oder Compliance-Anforderungen, die dem IT-Grundschutz-Profil zugrunde liegen.

- Verpflichtung zur Erfüllung (optional):

  Es kann beschrieben werden, ob das IT-Grundschutz-Profil für die Zielgruppe verpflichtenden oder empfehlenden Charakter hat.

Beispiel: Festlegung des Geltungsbereichs

Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an eCommerce-Anbieter, die über das Internet Produkte oder Dienstleistungen anbieten und demzufolge regelmäßig mit Kundendaten operieren.

Schutzbedarf

Im vorliegenden IT-Grundschutz-Profil ist ein Schutzniveau beschrieben, das über der Standard-Absicherung der IT-Grundschutz-Vorgehensweise liegt. Das ist deshalb der Fall, weil im Rahmen von eCommerce-Dienstleistungen in der Regel große Mengen an personenbezogenen Kundendaten verarbeitet werden, auf deren Vertraulichkeit großer Wert gelegt wird. Darüber hinaus besteht meist ein erhöhter Schutzbedarf hinsichtlich der Verfügbarkeit der angebotenen Services seitens des eCommerce-Anbieters. Daher ist für personenbezogene Kundendaten und Zahlungsverkehrsdaten ein hoher Schutzbedarf bezüglich Vertraulichkeit und Integrität anzunehmen. Für das eCommerce-Angebot im Internet bestehen außerdem hohe Verfügbarkeitsanforderungen. Dieser erhöhte Schutzbedarf ist bei der Anwendung des IT-Grundschutz-Profils zu berücksichtigen.

IT-Grundschutz-Vorgehensweise

Die in diesem IT-Grundschutz-Profil aufgeführten Anforderungen sind Empfehlungen des AK eCom für eCommerce-Anbieter. Sie decken mindestens die Anforderungen der "Standard-Absicherung" des BSI-Standards 200-2 ab, teilweise müssen außerdem Anforderungen aus dem Bereich des hohen Schutzbedarfs umgesetzt werden.

Abdeckung Vorgehensweise: mindestens Standard, teilweise hoch

ISO 27001-Kompatibilität: ja

Rahmenbedingungen: Die in diesem IT-Grundschutz-Profil dargestellten Anforderungen berücksichtigen die Vorgaben des BDSG und TMG § 13.

2.4 Abgrenzung des Informationsverbunds

Der betrachtete Informationsverbund oder Geschäftsprozess muss klar abgegrenzt werden. Hierzu gehören Aussagen darüber, was Gegenstand des IT-Grundschutz-Profils ist und was nicht. Konkret sollten folgende Aspekte beschrieben werden:

- Bestandteile des Informationsverbunds beziehungsweise des Geschäftsprozesses/der Fachaufgaben

- Nicht berücksichtigte Objekte: Wurden Zielobjekte, die zum Informationsverbund gehören im IT-Grundschutz-Profil nicht berücksichtigt, ist das zu begründen.
- Verbindung zu anderen IT-Grundschutz-Profilen

Beispiel: Abgrenzung des Informationsverbunds

Bestandteile des Informationsverbunds

Zum Informationsverbund "eCommerce" gehören alle Prozesse und Verfahren bei einem eCommerce-Anbieter, die für die Abwicklung der Geschäfte im Internet notwendig sind. Auf technischer Ebene sind hierfür in der Regel der Web-Auftritt, die Datenbanken, die E-Mail- und sonstigen Kommunikationsserver sowie die entsprechende Netzinfrastruktur einzubeziehen. Außerdem gehören weitere IT-Systeme dazu, die für das eCommerce-Angebot wesentlich sind.

Nicht berücksichtigte Objekte

Die Clients, die für die Bürokommunikation des eCommerce-Anbieters genutzt werden, werden vom IT-Grundschutz-Profil nicht berücksichtigt, da sie für das eCommerce-Angebot nicht wesentlich sind.

eCommerce-Anbieter, die große Teile ihrer technischen Infrastruktur durch Dritte betreiben lassen, sollten das vorliegende IT-Grundschutz-Profil als Grundlage für die Auswahl entsprechender Dienstleister verwenden. Die hier formulierten Anforderungen sollten in den Vertragsbedingungen enthalten sein.

Verweis auf andere IT-Grundschutz-Profile: entfällt

2.5 Referenzarchitektur

Die Referenzarchitektur, also der Untersuchungsgegenstand, legt fest, auf welche Objekte die Anforderungen des IT-Grundschutzes im Kontext des IT-Grundschutz-Profils angewendet werden müssen. Hierzu können neben Geschäftsprozessen auch Infrastrukturelemente, wie Gebäude und Räume, sowie die beteiligten IT-Systeme mit den installierten Anwendungen zählen. Diese können in einer Übersicht und einem Netzplan dargestellt werden (siehe Abbildung 1). Bei komplexen Informationsverbünden kann es zielführend sein, mit dem IT-Grundschutz-Profil nur einen Teilbereich des Informationsverbunds zu betrachten. Mit weiteren separaten IT-Grundschutz-Profilen für einzelne Teilverbünde kann dann der gesamte Informationsverbund abgebildet werden.

Folgende relevante Objekte sollten mit einem eindeutigen Identifikator und einer kurzen Beschreibung aufgeführt werden. Diese sollten im Idealfall in Objektgruppen oder in Abhängigkeit der identifizierten Geschäftsprozesse zusammengefasst sein:

- Infrastruktur: Gebäude und Räume
- Netze und Kommunikation: Netze, Netzkomponenten und Kommunikationsverbindungen
- IT-Systeme (Server, Desktop-Systeme, Mobile Devices etc.)
- Geschäftsprozesse/Anwendungen

Um die Komplexität zu reduzieren, sollten ähnliche Zielobjekte zu Gruppen zusammengefasst werden.

Zusätzlich sollte, wenn notwendig, beschrieben werden, wie mit Abweichungen und Erweiterungen gegenüber der Referenzarchitektur umgegangen werden kann. Dies ist wichtig, wenn die tatsächlich vorhandenen Infrastruktur-Elemente, IT-Systeme und Anwendungen beziehungsweise die Geschäftsprozesse oder Fachaufgaben sich von der Referenzarchitektur unterscheiden. Diese Abweichungen sollten nicht zu groß sein, da es sonst zielführender wäre, ein eigenes IT-Grundschutz-Profil zu erstellen, beispielsweise auf Basis des vorliegenden IT-Grundschutz-Profils.

Beispiel: Referenzarchitektur

Der vom IT-Grundschutz-Profil betrachtete Informationsverbund fokussiert alle essentiellen Objekte des eCommerce-Anbieters. Die relevanten Objekte werden im folgenden Unterkapitel "Untersuchungsgegenstand" beschrieben.

Untersuchungsgegenstand

Infrastruktur:

- [R1] Gebäude
- [R2] Serverraum
- [R3] Arbeitsplatz zur Administration und Konfiguration

Netze und Kommunikation

- [K1] Verbindung zum ISP
- [N1] separiertes LAN
- [N2] aktive Netzkomponenten (Router, Switches)
- [N3] Sicherheitskomponenten (Firewall, mehrere Paketfilter)
- [N4] Managementnetz (Out-of-Band)

IT-Systeme:

- Kommunikationsserver:
  - [S2] E-Mail-Server
- Drei-Schicht-Architektur des Web-Angebots bestehend aus
  - [S3] Webserver zur Darstellung des eCommerce-Angebots
  - [S4] Applikationsserver zur Ausführung der eCommerce-Applikation
  - [S5] Datenbankserver zur Vorhaltung der persistenten eCommerce-Daten, einschließlich Kundendaten
- Zahlungssystem
  - [K2] VPN-Verbindung zum Zahlungsverkehrsdienstleister
  - [S1] VPN-Server
- [S6] Payment-Server für Zahlungssystem

- [C1] IT-System zur Administration und Konfiguration von Netzen und IT-Systemen

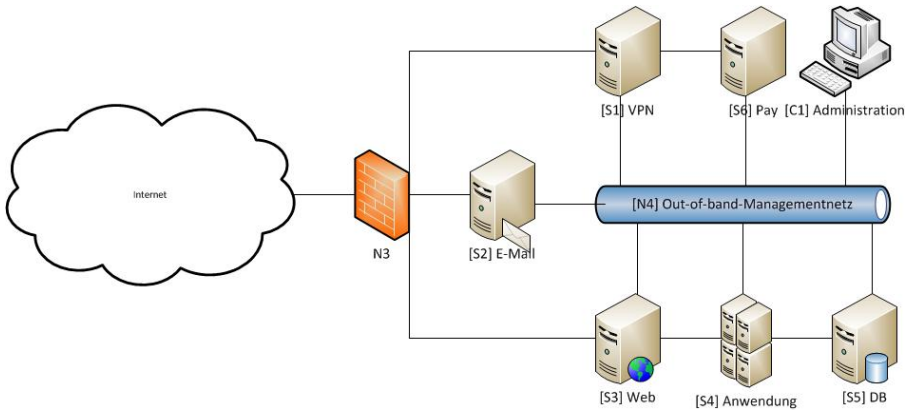

Abbildung 1: Netzplan eCommerce

Umgang mit Abweichungen

Weicht der zu schützende Informationsverbund von der Referenzarchitektur ab, sind die zusätzlichen oder nicht vorhandenen Objekte zu dokumentieren. Diesen Objekten sind geeignete Bausteine des IT-Grundschutz-Kompendiums zuzuordnen. Die aus den Bausteinen abgeleiteten Anforderungen müssen in Abhängigkeit des Schutzbedarfs angepasst werden.

2.6 Zu erfüllende Anforderungen und umzusetzende Maßnahmen

In einem IT-Grundschutz-Profil kann vorgegeben werden, ob alle Anforderungen eines Bausteins oder lediglich eine Auswahl relevant sind, wie z. B. nur die Basis-Anforderungen oder zusätzlich ausgewählte Standard-Anforderungen. Außerdem können und sollten die ausgewählten Anforderungen konkretisiert werden. Nicht nur vorhandene Anforderungen aus den IT-Grundschutz-Bausteinen können dem IT-Grundschutz-Profil zugeordnet werden, sondern auch bisher im IT-Grundschutz noch nicht vorhandene Anforderungen. Auf diese Weise kann mit Hilfe der IT-Grundschutz-Profile ein Sicherheitsniveau erreicht werden, das exakt dem Schutzbedarf des betrachteten Anwendungsbereiches entspricht. Dieses kann dann Basis-Sicherheit, Standard-Sicherheit oder erhöhten Schutzbedarf abdecken.

Zuordnung der relevanten Bausteine

Nachdem die Referenzarchitektur festgelegt und die relevanten Zielobjekte identifiziert worden sind, besteht die nächste Aufgabe darin, den betrachteten Informationsverbund (Untersuchungsgegenstand) mit Hilfe des IT-Grundschutz-Modells nachzubilden. Dafür werden im IT-Grundschutz-Kompendium vorhandene Bausteine ausgewählt und umgesetzt (siehe auch BSI-Standard 200-2, Kapitel 8.3 Modellierung eines Informationsverbunds oder Kapitel 2 des IT-Grundschutz-Kompendiums). Um die Auswahl zu erleichtern, sind die Bausteine des IT-Grundschutz-Kompendiums in Prozessbausteine und Systembausteine aufgeteilt. Prozessbausteine behandeln übergreifende Sicherheitsaspekte, die für sämtliche oder große Teile des Informationsverbunds gleichermaßen gelten, z. B. ORP.1 *Organisation* oder ORP.2 *Personal*. Systembausteine hingegen adressieren Sicherheitsaspekte von spezifischen Komponenten, z. B. IT-Systeme (SYS.1.3 *Unix-Server*) oder Anwendungen (APP.3.2

Webserver). Die einzelnen Bausteine können dann auf relevante Objekte der Referenzarchitektur modelliert werden.

Das IT-Grundschutz-Kompendium enthält Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen und Komponenten. Unter Umständen kann ein Zielobjekt nicht oder nicht hinreichend mit den bestehenden Bausteinen aus dem IT-Grundschutz-Kompendium abgebildet werden. In solchen Fällen muss das betrachtete Zielobjekt einer Risikoanalyse unterzogen werden (siehe auch BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz).

Als Ergebnis liegt nach diesem Schritt eine Liste oder eine Tabelle vor, in der alle relevanten Bausteine für die zugrunde gelegte Referenzarchitektur aufgeführt sind. Die Prozessbausteine sind dabei, wie weiter oben beschrieben, für viele Zielobjekte wichtig. Die Bausteine in den übrigen Schichten (siehe Schichtenmodell des IT-Grundschutz-Kompendiums) beziehen sich dagegen auf spezielle Zielobjekte oder Gruppen von Zielobjekten, die in der Referenzarchitektur enthalten sind.

Relevanz der Anforderungen

Nachdem die relevanten Bausteine des IT-Grundschutz-Kompendiums identifiziert worden sind, wird bei der Erstellung von IT-Grundschutz-Profilen im nächsten Schritt eine zielgruppengerechte Anpassung der Anforderungen vorgenommen. In den Bausteinen werden Anforderungen vorgeschlagen, die typischerweise für diese Komponenten geeignet und angemessen sind. Für die Erstellung eines IT-Grundschutz-Profils müssen die einzelnen Anforderungen durchgearbeitet werden und, wenn nötig, an die Rahmenbedingungen des IT-Grundschutz- Profils angepasst werden.

Es kann beispielsweise sinnvoll sein:

- alle Anforderungen eines Bausteins als relevant zu identifizieren,
- nur bestimmte Anforderungen als relevant zu identifizieren (z. B. nur Basis-Anforderungen),
- Anforderungen zu konkretisieren, also zum Beispiel, um weitere Aspekte zu ergänzen, oder
- Anforderungen komplett zu streichen.

Nicht nur vorhandene Anforderungen aus den IT-Grundschutz-Bausteinen können dem IT-Grundschutz-Profil zugeordnet werden. In der Praxis wird es häufig erforderlich sein, zusätzliche Anforderungen zu identifizieren die für den betrachteten Informationsverbund von Bedeutung sind. Dies ist beispielsweise dann der Fall, wenn erhöhter Schutzbedarf vorliegt. Auch wenn einzelne Zielobjekte der Referenzarchitektur nicht oder nicht hinreichend mit bestehenden Bausteinen aus dem IT-Grundschutz-Kompendium abgebildet werden können, müssen weitere Anforderungen ergänzt werden.

Auf diese Weise kann mit Hilfe der IT-Grundschutz-Profile ein Sicherheitsniveau erreicht werden, das exakt dem Schutzbedarf des betrachteten Anwendungsbereiches entspricht.

Als Ergebnis liegt nach diesem Schritt eine Liste oder eine Tabelle vor, in der alle relevanten Anforderungen für die zugrunde gelegte Referenzarchitektur aufgeführt sind. Es ist dabei zu

beachten, dass diese Liste auch die ergänzenden Sicherheitsanforderungen enthält, die sich aus der Risikoanalyse ergeben haben und die über das IT-Grundschutz-Modell hinausgehen, wie z. B. Anforderungen bei erhöhtem Schutzbedarf oder Anforderungen aus benutzerdefinierten Bausteinen.

Relevanz der Maßnahmen

Die in den IT-Grundschutz-Bausteinen enthaltenen Anforderungen beschreiben, was getan werden sollte. Die Anwender können verschiedene Möglichkeiten wählen, um diese Anforderungen zu erfüllen. Hilfe gibt es z. B. in den konkreten Umsetzungshinweisen zu den einzelnen Bausteinen. Durch die IT-Grundschutz-Profile kann wiederum festgelegt werden, auf welche Weise die Anforderungen im Kontext des IT-Grundschutz-Profils erfüllt werden müssen. Um die einzelnen Anforderungen entsprechend erfüllen zu können, sollte eine Umsetzungsvorgabe formuliert werden. Folgende Formulierungen sind denkbar (<**Umsetzungsvorgabe**>):

- "**auf geeignete Weise**": Es liegt im Ermessen der Anwender, wie die Anforderungen erfüllt werden können.
- "**Durch Umsetzung der zugehörigen Maßnahmen der Umsetzungshinweise**": Die Maßnahmen aus den Umsetzungshinweisen sind für die Erfüllung der Anforderungen umzusetzen.
- "**Durch Umsetzung von** [...]": Die umzusetzenden Maßnahmen können sich in weiteren Quellen befinden, auf die verwiesen werden kann. Es kann auch direkt eine Maßnahme vorgegeben werden.

Eine konkrete Vorgabe, wie die Anforderungen umgesetzt werden müssen, ermöglicht es, die Anforderungen einheitlich zu erfüllen. Dennoch kann es im Rahmen eines IT-Grundschutz-Profils zielführender sein, auf eine entsprechende Umsetzungsvorgabe zu verzichten.

Umsetzungsvorgaben einzelner Bausteine

Nachdem alle relevanten Bausteine sowie die generellen Anforderungen und Maßnahmen identifiziert worden sind, können für jeden einzelnen Baustein die Anforderungen und eine Vorgabe zur Umsetzung festgelegt werden:

- Verzicht auf (einzelne) Standard-Anforderungen:
  Alle Basis-Anforderungen müssen <Umsetzungsvorgabe> erfüllt werden.

  Bis auf folgende Standardanforderung müssen alle Standard-Anforderungen <Umsetzungsvorgabe> erfüllt werden:

  - Nennung entsprechender Standard-Anforderungen des Bausteins, die im Kontext des IT-Grundschutz-Profils nicht erfüllt werden müssen, mit stichhaltiger Begründung (Risiko-Übernahme, Risiko-Reduktion durch Erfüllung alternativer Anforderungen, Risiko-Transfer)

- Verbindliche Erfüllung von Anforderungen bei erhöhtem Schutzbedarf
  Folgende Anforderungen bei erhöhtem Schutzbedarf sollten <Umsetzungsvorgabe> zusätzlich erfüllt werden:
  - Nennung entsprechender Anforderungen bei erhöhtem Schutzbedarf des Bausteins durch optionale <Umsetzungsvorgabe>
- Zusätzliche Anforderung:
  Folgende Anforderungen müssen <Umsetzungsvorgabe> zusätzlich zu den Anforderungen des Bausteins erfüllt werden:
  - Zusätzliche Anforderung und Beschreibung durch optionale <Umsetzungsvorgabe>
- Verbindliche Vorgabe einer Maßnahme zur Erfüllung einer Anforderung:
  Die Anforderungen des Bausteins sind durch folgende Maßnahmen zu erfüllen, beziehungsweise zu ergänzen:
  - Nennung der Anforderung durch Umsetzung von [...]
- Bedingte Einschränkung für Anwendung eines Bausteins:
  Auf die Erfüllung der Anforderungen des Bausteins kann verzichtet werden, wenn [...]

Beispiel: Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Die folgenden obligatorischen **Prozess-Bausteine** sind auf den gesamten Informationsverbund anzuwenden. Wenn nicht anders angegeben, müssen alle Basis- und Standard-Anforderungen der Bausteine *auf geeignete Weise* erfüllt werden:

- ISMS.1 ISMS (Sicherheitsmanagement)
  - Folgende Anforderungen bei erhöhtem Schutzbedarf müssen durch Umsetzung der zugehörigen Maßnahme der Umsetzungshinweise zusätzlich erfüllt werden:
    - ISMS.1.A15 Erstellung von zielgruppengerechten Sicherheitsrichtlinien
    - ISMS.1.A17 Abschließen von Versicherungen
- ORP.1 Organisation
- ORP.2 Personal
  - Alle Basis-Anforderungen des Bausteins müssen geeignet erfüllt werden.
  - Bis auf folgende Standardanforderung müssen alle Standard-Anforderungen geeignet erfüllt werden:
    - ORP.2.A10 Vermeidung von Störungen des Betriebsklimas.

      Begründung:
      - Durch eine nahezu familiäre und freundschaftliche Betriebsstruktur müssen keine zusätzlichen Anforderungen für ein positives Betriebsklima erfüllt werden.
- ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
- ORP.4 Identitäts- und Berechtigungsmanagement

- ORP.5 Anforderungsmanagement (Compliance)
- CON.1 Kryptokonzept
  - Die Anforderung "CON.1.A9 Auswahl kryptografischer Produkte" des Bausteins sind durch folgende Maßnahme zu erfüllen, beziehungsweise zu ergänzen:
    - "Einsatz von Hardware-Sicherheitsmodulen":
      Es sollten Hardware-Sicherheitsmodule eingesetzt werden, um personenbezogene Daten, Kreditkarten-Daten und andere Zahlungsdaten zu verschlüsseln.
  - Die Anforderung "CON.1.A19 Verschlüsselung von Datenträgern" des Bausteins sind durch folgende Maßnahme zu erfüllen, beziehungsweise zu ergänzen:
    - "Vollverschlüsselung geschäftskritischer Datenträger":
      Alle Datenträger, auf denen sich geschäftskritische, personenbezogene oder finanzrelevante Daten befinden, sollten vollverschlüsselt werden, mindestens mit AES-256.
- CON.2 Datenschutz
- CON.6 Löschen und Vernichten
- OPS.1.2.1 Änderungsmanagement
- OPS.1.2.2 Archivierung
- OPS.1.2.7 Verkauf/Aussonderung von IT
- DER.1 Detektion von Sicherheitsvorfällen in der IT
- DER.2.1 Behandlung von Sicherheitsvorfällen
- DER.3 Sicherheitsprüfungen
- DER.4 BCM/Notfallmanagement
- OPS.1.1 Kern-IT-Betrieb/Kernaufgaben
  - Die Anforderungen aus dem Baustein müssen nicht erfüllt werden, wenn die IT-Infrastruktur von Dritten betrieben wird.
- OPS.2.1 Outsourcing-Nutzung
  - Auf die Erfüllung der Anforderungen des Bausteins kann verzichtet werden, wenn die IT-Infrastruktur selbst betrieben wird.
- OPS.2.5 SLA/SSLA
  - Auf die Erfüllung der Anforderungen des Bausteins kann verzichtet werden, wenn die IT-Infrastruktur selbst betrieben wird.

Zusätzliche Anforderungen, die für den gesamten Informationsverbund erfüllt werden müssen:

- Die Anforderungen der BSI-Publikation "Absicherung von Telemediendiensten nach Stand der Technik" müssen durch die in der Publikation genannten Empfehlungen erfüllt werden.

Darüber hinaus sind alle Bausteine umzusetzen, die sich im Rahmen der Anwendung der IT-Grundschutz-Vorgehensweise, insbesondere bei der Modellierung des Informationsverbunds, ergeben.

Die folgenden obligatorischen **System-Bausteine** sind auf die in eckigen Klammern genannten Zielobjekte (siehe Referenzarchitektur) anzuwenden. Wenn nicht anders angegeben, müssen alle Basis- und Standard-Anforderungen der Bausteine *durch Umsetzung der zugehörigen Maßnahmen der Umsetzungshinweise* erfüllt werden.

Infrastruktur

- [R1] Gebäude
  - INF.1 Allgemeines Gebäude
  - INF.4 IT-Verkabelung
- [R2] Serverraum/Technikraum
  - INF.5 Serverraum/Technikraum
- [R3] Arbeitsplatz zur Administration und Konfiguration
  - INF.8b Büroarbeitsplatz

Netze und Kommunikation

- [K1] Verbindung zum ISP
  - NET.1.1 Netz-Architektur und -design
  - NET.1.2 Netz-Management
- [N1] separiertes LAN
  - NET.1.1 Netz-Architektur und -design
  - NET.1.2 Netz-Management
- [N2] Aktive Netzkomponenten (Router, Switches)
  - NET.3.1 Router/Switches
- [N3] Sicherheitskomponenten (Sicherheitsgateway, mehrere Paketfilter)
  - NET.3.2 Firewall
  - NET 3.4 IDS/IPS
- [N4] Managementnetz
  - NET.1.1 Netz-Architektur und -design
  - NET.1.2 Netz-Management

IT-Systeme:

- Kommunikationsserver:
  - [S2] E-Mail-Server
    - SYS.1.1 Allgemeiner Server
    - SYS.1.3 Unix-Server (oder vergleichbarer Baustein)

- APP.5.1 E-Mail/Groupware

- Drei-Schicht-Architektur des Web-Angebots bestehend aus
  - [S3] Webserver zur Darstellung des eCommerce-Angebots
    - SYS.1.1 Allgemeiner Server
    - SYS.1.3 Unix-Server (oder vergleichbarer Baustein)
    - APP.3.2 Web-Server
  - [S4] Applikationsserver zur Ausführung der eCommerce-Applikation
    - SYS.1.1 Allgemeiner Server
      - Folgende Anforderungen müssen zusätzlich zu den Anforderungen des Bausteins erfüllt werden:
        - Speicherung von Passwörtern nur als Hash mit Salt
        - Regelmäßige Integritätsprüfungen
    - SYS.1.3 Unix-Server (oder vergleichbarer Baustein)
    - APP.3.1 Web-Anwendungen
      - Folgende Anforderung muss zusätzlich zu den Anforderungen des Bausteins erfüllt werden:
        - Verschlüsselte Übertragung personenbezogener Daten und Daten zur Abwicklung des Zahlungsverkehrs: Geschäftskritische, personenbezogene oder finanzrelevante Daten müssen bei der Übertragung gemäß Richtlinie 4711 verschlüsselt werden. Dabei sind folgende Algorithmen und Schlüssellängen zulässig [....]
  - [S5] Datenbankserver zur Vorhaltung der persistenten eCommerce-Daten, einschließlich Kundendaten
    - SYS.1.1 Allgemeiner Server
      - Folgende Anforderungen müssen zusätzlich zu den Anforderungen des Bausteins erfüllt werden:
        - Regelmäßige Integritätsprüfungen
        - Zusätzlich sind alle Abfragen der Kundendatenbank zu protokollieren.
    - SYS.1.3 Unix-Server (oder vergleichbarer Baustein)
    - APP.4.3 Datenbank
      - Folgende Anforderungen müssen zusätzlich zu den Anforderungen des Bausteins erfüllt werden:
        - Verschlüsselte Speicherung von Kundendaten/Zahlungsverkehrsdaten
- Zahlungssystem

- [K2] VPN-Verbindung zum Zahlungsverkehrsdienstleister
  - NET.3.3 VPN
- [S1] VPN-Server
  - SYS.1.1 Allgemeiner Server
  - SYS.1.3 Unix-Server (oder vergleichbarer Baustein)
  - NET.3.3 VPN
- [S6] Payment-Server für Zahlungssystem
  - SYS.1.1 Allgemeiner Server
  - SYS.1.3 Unix-Server (oder vergleichbarer Baustein)
  - NET.3.3 VPN
  - ePayment (siehe Anlage)
- [C1] IT-System zur Administration und Konfiguration von Netzen und IT-Systemen
  - SYS.2.1 Allgemeiner Client
    - Folgende Anforderungen müssen zusätzlich zu den Anforderungen des Bausteins erfüllt werden:
      - Vier-Augen-Prinzip für kritische Administrationstätigkeiten
  - SYS.2.2.2 Client unter Windows 8 (oder vergleichbarer Baustein)
  - CON.4 Standard-Software

2.7 Restrisikobetrachtung/Risikobehandlung

Bei der Erstellung von IT-Grundschutz-Profilen werden im Rahmen von Risikoanalysen in der Regel ergänzende Sicherheitsanforderungen identifiziert, die über das IT-Grundschutz-Modell hinausgehen. Dabei werden typischerweise auch Risiken gefunden, die nicht alle durch vorgegebene Anforderungen bzw. dazugehörige Maßnahmen abgedeckt werden können. Solche Restrisiken müssen bewertet und dokumentiert werden. So sollte unter anderem aufgenommen werden, wenn vorhandene (Standard-)Anforderungen eines Bausteins nicht erfüllt werden oder wenn mit zusätzlichen Maßnahmen mehr Risiken abgedeckt werden könnten.

Darüber hinaus können sich im Einzelfall zusätzliche Risiken ergeben, die im Rahmen des Informationssicherheitsmanagements behandelt werden müssen.

Beispiel: Restrisikobetrachtung/Risikobehandlung

In der Regel werden bei der Authentisierung der Kunden nur einfache passwortbasierte Verfahren angewendet. Soweit die damit verbundenen Risiken nicht getragen werden können, müssen stärkere Verfahren wie etwa eine Mehrfaktor-Authentisierung angewendet werden.

Hochprofessionelle, zielgerichtete Angriffe lassen sich nach aktuellem Stand nicht vollständig präventiv beherrschen. Daher ist es wichtig, Sicherheitsvorfälle möglichst umgehend zu

erkennen und angemessen darauf zu reagieren. Das entsprechende Risiko muss getragen werden.

Verteilte Denial-of-Service-Angriffe haben in letzter Zeit enorm an Durchschlagskraft gewonnen. Ein hochwertiger Schutz vor solchen Angriffen lässt sich nur in Zusammenarbeit mit den Internet-Providern erreichen. Ein Restrisiko, dass das eCommerce-Angebot von solchen Angriffen beeinträchtigt wird, muss getragen werden.

2.8 Anwendungshinweise

Die Anwendungshinweise beschreiben, wie mit den aufgezeigten Anforderungen innerhalb des Managementsystems für Informationssicherheit (ISMS) umgegangen werden kann. In der Regel sollen die Anwendungshinweise im Gesamtsicherheitskonzept integriert und im Betrieb umgesetzt werden.

Beispiel Anwendungshinweise:

Die ermittelten Anforderungen sind in das Gesamtsicherheitskonzept zu integrieren und im Zuge der geplanten Realisierung umzusetzen.

2.9 Unterstützende Informationen

In diesem Kapitel erhalten die Anwender ergänzende Informationen für die weitere Recherche. Dies können beispielsweise Verweise auf andere IT-Grundschutz-Bausteine, weitere BSI-Publikationen oder andere Quellen sein.

Beispiel: Unterstützende Informationen

Detailliertere Informationen zu den einzelnen Anforderungen finden sich in den Umsetzungshinweisen der einzelnen Bausteine des IT-Grundschutzes.

Spezielle Informationen zur Umsetzung der Anforderungen des § 13 TMG finden sich in der BSI-Publikation "Absicherung von Telemediendiensten nach Stand der Technik".

2.10 Anhang

Bei der Erstellung eines IT-Grundschutz-Profils werden in der Regel fast alle Schritte, also Strukturanalyse, Schutzbedarfsfeststellung, Modellierung und Risikoanalyse, durchlaufen, die für die Erstellung eines Sicherheitskonzepts nach IT-Grundschutz erforderlich sind. Im Anhang können weitere detailliertere Informationen dazu ausführlich dargestellt werden.

Unter Umständen kann der im IT-Grundschutz-Profil betrachtete Informationsverbund oder Geschäftsprozess nicht vollständig mit den vorhandenen IT-Grundschutz-Bausteinen abgebildet werden. In diesem Fall ist es zielführend, benutzerdefinierte Bausteine zu erstellen und diese in den Anhang des IT-Grundschutz-Profils aufzunehmen. Zusätzlich hilft den Anwendern oft ein Abkürzungs- oder ein Literaturverzeichnis, beziehungsweise ein Glossar, das in den Anhang integriert werden kann.

Beispiel: Anhang:

- Abkürzungen

  [...]
- Literatur

  [...]
- Glossar

  [...]
- Baustein ePayment

  [...]
- Schutzbedarfsfeststellung, Risikobewertung etc.

  [...]

3 Ausblick: Zeit, Kosten und Ressourcen sparen mit den IT-Grundschutz-Profilen

IT-Grundschutz-Profile sind als praktikable Schablonen zu verstehen, mit denen verschiedene Anwendergruppen den IT-Grundschutz an ihre Bedürfnisse anpassen können. Die Erarbeitung von IT-Grundschutz-Profilen kann durch Anwender in der Praxis selbst erfolgen, mit dem klaren Fokus auf branchen- und zielgruppenspezifische Anpassungen. Der enge Praxisbezug und der Modellcharakter helfen Institutionen jeder Größenordnung, Aufwand, Zeit und Kosten bei der individuellen Umsetzung des IT-Grundschutzes zu sparen.

IT-Grundschutz-Profile sollten allen Interessierten zur Verfügung gestellt werden. Dadurch können Erfahrungen und Know-how geteilt und Synergieeffekte genutzt werden. Damit die Anwender einen Überblick über die vorhandenen IT-Grundschutz-Profile erhalten, arbeitet das BSI an dem Aufbau eines öffentlichen IT-Grundschutz-Profil Registers. IT-Grundschutz-Profile können dann zukünftig zur Registrierung beim BSI eingereicht werden. Das BSI nimmt eine formale und stichprobenartige inhaltliche Prüfung vor. Bei positiven Abschluss der Prüfung wird eine Registernummer erteilt und das IT-Grundschutz-Profil im IT-Grundschutz-Profil Register gelistet.