3 Sicherheitsmanagement nach IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit der Vorgehensweise nach IT-Grundschutz eine Methodik für ein effektives IS-Management entwickelt, die einfach auf die Gegebenheiten einer konkreten Institution angepasst werden kann. Diese vom BSI seit 1994 eingeführte und weiterentwickelte Methode bietet sowohl eine Vorgehensweise für den Aufbau eines Managementsystems für Informationssicherheit als auch eine umfassende Basis für die Risikobewertung, die Überprüfung des vorhandenen Informationssicherheitsniveaus und die Implementierung der angemessenen Informationssicherheit.
Die Beschreibung der IT-Grundschutz-Methodik ist im BSI-Standard 200-2 zu finden, Sicherheitsanforderungen für die verschiedenen Bereiche eines Informationsverbundes in den Bausteinen des IT-Grundschutz-Kompendiums (siehe https://www.bsi.bund.de/grundschutz).

Der IT-Grundschutz wurde 2017 einer grundlegenden Modernisierung unterzogen. Hierbei wurde die klassische Vorgehensweise, jetzt „Standard-Absicherung", um die „Basis-Absicherung" und die „Kern-Absicherung" ergänzt. Mit der „Standard-Absicherung" wird durch die Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen ein Sicherheitsniveau für die betrachteten Geschäftsprozesse erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Bei der Umsetzung der Vorgehensweise „Basis-Absicherung" wird ein Sicherheitsniveau erreicht, das zwar deutlich unter dem der Standard-Absicherung liegt, aber eine gute Grundlage für ISMS-Einsteiger bietet. Mit der Vorgehensweise „Kern-Absicherung" können besonders schützenswerte Informationen und Geschäftsprozesse vorrangig abgesichert werden.

Einer der großen Vorteile des IT-Grundschutzes liegt in der umfangreichen Wissenssammlung im Bereich der IT-Grundschutz-Bausteine, die kostenfrei verfügbar ist. Diese ständig wachsende Wissenssammlung führte aber auch dazu, dass die IT-Grundschutz-Kataloge mit ihrer Vielzahl von konkreten Maßnahmenempfehlungen für verschiedene typische IT-Umgebungen immer umfangreicher wurden. Bei der Modernisierung des IT-Grundschutzes wurden die Bausteine deutlich verschlankt und stärker strukturiert, um Inhalte künftig schneller bereitstellen können.

Das neue IT-Grundschutz-Kompendium als Nachfolger der IT-Grundschutz-Kataloge wurde 2017 als Draft vorgestellt und wird erstmalig im Februar 2018

veröffentlicht. Es enthält die modernisierten Bausteine und ist Prüfgrundlage für Zertifizierungen nach ISO 27001 auf Basis von IT-Grundschutz.

Auf den Webseiten des BSI finden sich zahlreiche weitere Werkzeuge rund um den IT-Grundschutz, wie z.B. der „Leitfaden zur Basis-Absicherung“, um den Unternehmen einen schnellen Einstieg zu geben, die sich zum ersten Mal mit der Absicherung ihrer IT-Systeme und Daten befassen wollen. Es lohnt sich immer, regelmäßig unter https://www.bsi.bund.de/grundschutz nach neuen Informationen zu suchen.

In der BSI-Schriftenreihe mit Standards zu verschiedenen Bereichen der Informationssicherheit finden sich die folgenden BSI-Standards zum Thema IS-Management:

BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)

BSI-Standard 200-2: IT-Grundschutz-Methodik

BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz

BSI-Standard 100-4: Notfallmanagement (Business Continuity)

Die BSI-Standards enthalten generelle Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit. Das BSI greift dabei Themenbereiche auf, die von grundsätzlicher Bedeutung für die Informationssicherheit in Behörden oder Unternehmen sind und für die sich national oder international sinnvolle und zweckmäßige Herangehensweisen etabliert haben.

BSI-Standard 200-1

Im BSI-Standard 200-1 wird beschrieben, wie ein IS-Managementsystem aufgebaut werden kann und welche Aufgaben der Unternehmensleitung dabei zukommen. Er stellt übersichtlich die wichtigsten Aufgaben des Sicherheitsmanagements dar und wie der Sicherheitsprozess und die notwendige Sicherheitsorganisation etabliert werden können. Der 200-2 ist vollständig kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der ISO-Standards 27000 und 27002. Er bietet eine leicht verständliche und systematische Anleitung, unabhängig davon, mit welcher Methode eine Institution die Anforderungen umsetzen möchte.

Das BSI stellt den Inhalt dieser ISO-Standards in einem eigenen BSI-Standard dar, um einige Themen ausführlicher beschreiben zu können und so eine didaktischere Darstellung der Inhalte zu ermöglichen. Zudem wurde die Gliederung so gestaltet, dass sie zur IT-Grundschutz-Methodik kompatibel ist. Durch die einheitlichen Überschriften in den zuvor genannten ISO-Standards ist eine Orientierung für die Leser sehr einfach möglich.

BSI-Standard 200-2

In BSI-Standard 200-2 zur IT-Grundschutz-Methodik wird aufgezeigt, wie der im BSI-Standard 200-1 vorgestellte grundlegende Rahmen für ein IS-Managementsystem durch IT-Grundschutz konkretisiert wird. Zu den Zielen des IT-Grundschutzes gehört es, den Aufwand im Informationssicherheitsprozess zu reduzieren und für Institutionen jeder Größe und Sparte eine kosteneffektive und zielführende Methode zum Aufbau und zur Umsetzung der für sie angemessenen Informationssicherheit zur Verfügung zu stellen. Um den IT-Grundschutz an die Anforderungen von Institutionen verschiedener Größe und unterschiedlichem Schutzbedarf anpassen zu können, werden im 200-2 die drei Vorgehensweisen „Standard-Absicherung", „Basis-Absicherung" und „Kern-Absicherung" vorgestellt.

Die Basis-Absicherung verfolgt das Ziel, Institutionen, die noch am Anfang des Sicherheitsprozesses stehen, zu ermöglichen, schnell eine breite, grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Institution zu erzielen. Entsprechend konzentriert sich diese Vorgehensweise auf die Essenz eines ISMS. Die Basis-Absicherung versteht sich als Einstieg und kann für ein komplettes Unternehmen oder einzelne Bereiche, beispielsweise neue hinzugekommene Geschäftsprozesse, umgesetzt werden.

Die Kern-Absicherung dient als weitere Einstiegsvorgehensweise dem Schutz der essentiellen Geschäftsprozesse und Ressourcen einer Institution. Bei dieser Vorgehensweise wird sich auf einige herausragende, besonders geschäftskritische Assets (sogenannte Kronjuwelen) konzentriert. Es wird also ein sehr eingegrenzter Geltungsbereich betrachtet. Die Kern-Absicherung ist vor allem für Institutionen geeignet, die einige wenige Geschäftsprozesse identifiziert haben, die wesentlich für den Fortbestand der Institution sind und vorrangig abgesichert werden müssen. Die Vorgehensweise orientiert sich dabei stark an den Schritten der Vorgehensweise zur Standard-Absicherung.

Die dritte Vorgehensweise, die ein gleichmäßiges und umfassendes Sicherheitsniveau liefert, ist die Standard-Absicherung.

Die Vorgehensweisen nach dem 200-2 in Kombination mit dem IT-Grundschutz-Kompendium bieten eine systematische Methodik zur Erarbeitung von Sicherheitskonzepten und praxiserprobten Sicherheitsmaßnahmen.

Im 200-2 wird Schritt für Schritt beschrieben, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des IS-Managements und der Aufbau einer Organisationsstruktur für Informationssicherheit sind dabei wichtige Themen. Die Einrichtung eines funktionierenden IS-Managements ist unabdingbar, um ein angemessenes Sicherheitsniveau innerhalb einer Institution zu erreichen und aufrechtzuerhalten.

Der BSI-Standard 200-2 geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt werden kann, wie angemessene Sicherheitsmaßnahmen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzeptes zu beachten ist. Auch die Frage, wie die Informationssicherheit im laufenden Betrieb aufrechterhalten und verbessert werden kann, wird beantwortet.

IT-Grundschutz interpretiert damit die sehr allgemein gehaltenen Anforderungen der oben genannten ISO-Standards 27000, 27001 und 27002 und hilft den Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrund-Know-how und Beispielen. Über die Bausteines des IT-Grundschutz-Kompendiums werden die Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, Systeme, Kommunikationsverbindungen und Räume aufgezeigt, aus denen Sicherheitsmaßnahmen für die jeweilige Institution abgeleitet werden können. Ein Vorgehen nach IT-Grundschutz ist somit eine erprobte und effiziente Möglichkeit, allen Anforderungen dieser ISO-Standards nachzukommen.

BSI-Standard 200-3

Im BSI-Standard 200-3 wird eine Methodik zur Risikoanalyse auf der Basis des IT-Grundschutzes vorgestellt. Diese Vorgehensweise bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit dem IT-Grundschutz arbeiten und möglichst nahtlos eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten.

BSI-Standard 100-4

Im BSI-Standard 100-4 wird eine Methodik zur Etablierung und Aufrechterhaltung eines behörden- bzw. unternehmensweiten Notfallmanagements erläutert. Die beschriebene Methodik baut dabei auf der im BSI-Standard 200-2 beschriebenen IT-Grundschutz-Methodik auf und ergänzt diese sinnvoll.

IT-Grundschutz-Kompendium

Eines der wichtigsten Ziele des IT-Grundschutzes ist es, den Aufwand im Informationssicherheitsprozess zu reduzieren, indem bekannte Vorgehensweisen zur Verbesserung der Informationssicherheit gebündelt und zur Wiederverwendung angeboten werden.

Um die Innovationsschübe und häufigen Änderungen in Geschäftsprozessen und vor allem im IT-Bereich berücksichtigen zu können, ist das IT-Grundschutz-Kompendium mit Hilfe der Baustein-Struktur modular aufgebaut und konzentriert sich auf die Darstellung der wesentlichen Sicherheitsanforderungen für die jeweiligen Bausteine. Damit ist es leicht erweiterbar und aktualisierbar.

Das IT-Grundschutz-Kompendium enthält Prozess- und Systembausteine für typische Geschäftsprozesse, Anwendungen, Systeme, Kommunikationsverbindungen und Räume. Aus diesen sollten die für die eigene Institution relevanten Bausteine ausgewählt werden. Im IT-Grundschutz werden alle Bereiche

betrachtet, die sich in Institutionen finden können. Dazu gehören neben Organisation und Personal auch IT-Betrieb, aber auch Produktion und Fertigung mit Industrial Control Systems (ICS), ebenso wie Komponenten aus dem Bereich Internet of Things (IoT).

Die Bausteine des IT-Grundschutz-Kompendiums sind in prozess- und systemorientierte Bausteine aufgeteilt und nach zusammengehörigen Themen in ein Schichtenmodell einsortiert.

Die prozessorientierten Bausteine sind in die folgenden Schichten gruppiert:

- ISMS (Managementsysteme für Informationssicherheit)
- ORP (Organisation und Personal)
- CON (Konzepte)
- OPS (Betrieb)
- DER (Detektion und Reaktion)

Die systemorientierten Bausteine sind in die folgenden Schichten gruppiert:

- INF (Infrastruktur)
- NET (Netze und Kommunikation)
- SYS (IT-Systeme)
- APP (Anwendungen)
- IND (Industrielle IT)

Jeder Baustein enthält eine kurze Beschreibung der Thematik und des Ziels, das mit der Umsetzung des Bausteins erreicht werden soll, sowie eine Abgrenzung zu anderen Bausteinen, die einen thematischen Bezug haben. Weiterhin gibt es einen Überblick über die spezifischen Gefährdungen des betrachteten Themengebietes. Die Sicherheitsanforderungen für die Basis-, Standard- und Kern-Absicherung bilden den Schwerpunkt eines jeden Bausteins. Sie beschreiben, *was* für den Schutz des betrachteten Zielobjektes zu tun ist.

- **Basis-Anforderungen** müssen vorrangig erfüllt werden, da bei diesen Empfehlungen mit (relativ) geringem Aufwand der größtmögliche Nutzen erzielt werden kann. Es handelt sich um uneingeschränkte Anforderungen. Die Basis-Anforderungen sind ebenfalls die Grundlage für die Vorgehensweise „Basis-Absicherung".
- **Standard-Anforderungen** bauen auf den Basis-Anforderungen auf und adressieren den normalen Schutzbedarf. Sie sollten grundsätzlich erfüllt werden, aber nicht vorrangig. Die Ziele der Standard-Anforderungen müssen erreicht werden, um eine Standard-Absicherung zu erzielen.

- **Anforderungen für einen hohen Schutzbedarf** sind eine Auswahl von Vorschlägen für eine weitergehende Absicherung, die bei erhöhten Sicherheitsanforderungen oder unter bestimmten Rahmenbedingungen als Grundlage für die Erarbeitung geeigneter Anforderungen und Maßnahmen berücksichtigt werden können.

IT-Grundschutz richtet sich primär an die Verantwortlichen für Informationssicherheit in Behörden und Unternehmen aller Größenordnungen. Dies können Informationssicherheitsbeauftragte, Administratoren und auch Manager verschiedener Bereiche sein. Um die gezielte Verteilung der jeweiligen Sicherheitsmaßnahmen an die zuständigen Akteure zu erleichtern, wird in jedem Baustein erläutert, wer für dessen Umsetzung verantwortlich ist. Der Informationssicherheitsbeauftragte (ISB) ist grundsätzlich bei allen strategischen Entscheidungen, die die Informationssicherheit berühren, einzubeziehen.

Zusätzlich kann es zu den Bausteinen des IT-Grundschutz-Kompendiums Umsetzungshinweise geben. Diese beschreiben, wie die Anforderungen der Bausteine in der Praxis erfüllt werden können, und enthalten dafür passende Sicherheitsmaßnahmen mit detaillierten Beschreibungen, die auf dem Erfahrungsschatz und „Best Practices“ von BSI und IT-Grundschutz-Anwendern basieren.

Die Bausteine des IT-Grundschutz-Kompendiums und die Umsetzungshinweise werden regelmäßig aktualisiert und erweitert. Sie werden als Printversion und außerdem kostenfrei im Internet veröffentlicht.

Zusammenfassung der Anwendungsweise

Im BSI-Standard 200-2 „IT-Grundschutz-Methodik“ wird dargestellt, wie ein effizientes Managementsystem für die Informationssicherheit aufgebaut, Sicherheitskonzepte erstellt und wie das IT-Grundschutz-Kompendium im Rahmen dieser Aufgabe verwendet werden kann. Die Vorgehensweisen Basis-, Standard- und Kern-Absicherung bieten Hilfestellung beim Aufbau und bei der Aufrechterhaltung des Prozesses Informationssicherheit in einer Institution, indem Wege und Methoden für das generelle Vorgehen, aber auch für die Lösung spezieller Probleme aufgezeigt werden.

In der nachfolgenden Abbildung wird die prinzipielle Vorgehensweise schematisch dargestellt:

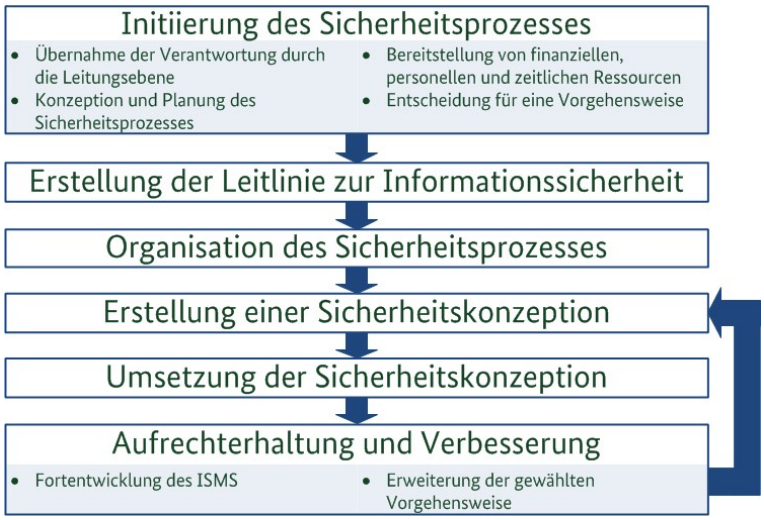

Abb. 3.1: Phasen des Sicherheitsprozesses mit IT-Grundschutz

Die Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren. Hierzu gehören strategische Leitaussagen zur Informationssicherheit ebenso wie die Entscheidung, mit welcher Vorgehensweise die verschiedenen Bereiche der Institution abgesichert werden sollen.

Als wesentliche Grundlage für die weitere Ausgestaltung des Sicherheitsprozesses dient die Leitlinie zur Informationssicherheit. In dieser wird beschrieben, welche Sicherheitsziele und welches Sicherheitsniveau die Institution anstrebt, was die Motivation hierfür ist und mit welchen Maßnahmen und mit welchen Strukturen dies erreicht werden soll.

Für das Informationssicherheitsmanagement muss eine für Größe und Art der Institution geeignete Organisationsstruktur aufgebaut werden. Außerdem muss eine Sicherheitskonzeption für die Institution erstellt und in die Praxis umgesetzt werden.

Damit das einmal erreichte Sicherheitsniveau dauerhaft aufrecht erhalten und verbessert werden kann, müssen der Sicherheitsprozess, die Organisationsstrukturen für Informationssicherheit und das Sicherheitskonzept regelmäßig daraufhin überprüft werden, ob sie angemessen, wirksam und effizient sind.

3.1 Sicherheitsprozess und -organisation

Die Komplexität und Vernetzung der Informations- und Kommunikationstechnik wird weiter zunehmen, immer mehr Geschäftsprozesse werden durch diese miteinander verknüpft und sind von deren korrektem Funktionieren