



Vorgehensweisen zum IT-Grundschutz

Der IT-Grundschutz ist eine umfangreiche Dokumentensammlung, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben wird. Das Werk soll Behörden und Unternehmen ein Verfahren bieten, ihre Informationen und digitalen Systeme zu schützen. Der IT-Grundschutz wird laufend aktualisiert, um auf neue Techniken und neue Bedrohungen reagieren zu können.

Elemente des IT-Grundschutz

Der IT-Grundschutz besteht aus mehreren Dokumenten. In den **vier BSI-Standards** (200-1, 200-2, 200-3 und 100-4) wird das Verfahren erläutert, wie der IT-Grundschutz anzuwenden ist.

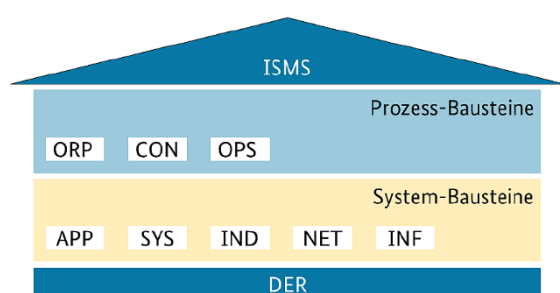
Das **IT-Grundschutz-Kompodium** enthält die konkreten Sicherheitsanforderungen und Umsetzungshinweise zum sicheren Umgang mit Informationen in unterschiedlichen Einsatzumgebungen.

Mit dem IT-Grundschutz-Kompodium kann folgende Frage beantwortet werden:

Welche Infrastruktur in meiner Institution ist auf welche Art gefährdet und wie kann ich sie schützen?

IT-Grundschutz-Kompodium

Das IT-Grundschutz-Kompodium enthält die sog. *Bausteine*, die alle Bereiche der Informationssicherheit abdecken (z.B. Anwendungen, Systeme, Kommunikationsverbindungen und Räume).



Um die Auswahl zu erleichtern, sind die Bausteine im IT-Grundschutz-Kompodium zunächst in prozess- und systemorientierte Bausteine aufgeteilt und diese jeweils in einzelne Baustein-Gruppen untergliedert.

(ISMS, ORP, ... , INF, DER). Jede Gruppe deckt einen Teilbereich der Informationssicherheit ab.

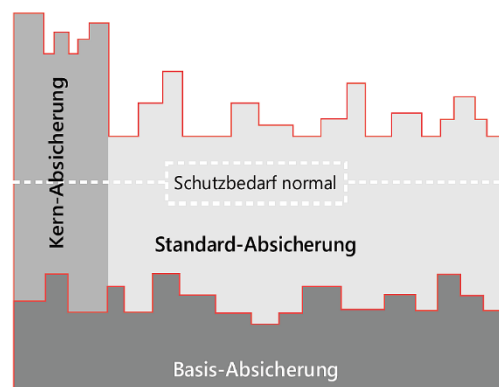
IT-Grundschutz-Bausteine

Um die Anwendung der Bausteine zu vereinfachen, sind diese immer gleich aufgebaut:

- kurze Beschreibung des Themengebiets und Überblick über die Gefährdungen mit Beispielen
- konkrete Sicherheitsanforderungen, abhängig vom Schutzbedarf (Basis, Standard, erhöhter SB)
- genaue beschriebene Sicherheitsmaßnahmen, wie diese Anforderungen erfüllt werden können

Basis-, Kern- und Standardabsicherung

Das IT-Grundschutz-Verfahren sieht drei Varianten vor: Basis-, Kern- und Standardabsicherung



Die **Basisabsicherung** sorgt für eine grundlegende Erst-Absicherung und soll schnell die größten Risiken senken, um dann eine gründlichere Absicherung darauf aufzubauen. Sie ist für kleinere Institutionen gedacht, die noch am Anfang ihres Sicherheitsprozesses stehen.

Die **Kernabsicherung** konzentriert sich zunächst auf einen kleinen, aber sehr wichtigen Teil eines Unternehmens (*Kronjuwelen*) und sichert diese Schutzobjekte schon so-

fort gründlich ab, bevor später der Schutz auf andere Unternehmensbereiche ausgedehnt wird.

Die Basis- und Kern-Absicherung sind mögliche Einstiegsvarianten mit dem Ziel, mittelfristig ein vollständiges Sicherheitskonzept gemäß der Standard-Absicherung zu erstellen und umzusetzen.

Die **Standard-Absicherung** ist die empfohlene IT-Grundschutz-Vorgehensweise. Sie hat eine angemessene und ausreichende Absicherung für alle Prozesse und Bereiche des Unternehmens mit normalem Schutzbedarf als Ziel. Durch eine geeignete Umsetzung wird ein Sicherheitsniveau erreicht, das angemessen ist und ausreicht, um geschäftsrelevante Informationen zu schützen.

Aufgabenstellung:

- 1.) Beschreiben Sie, was unter dem IT-Grundschutz zu verstehen ist!

Umfangreiche Dokumentensammlung, die ein Verfahren bieten soll Informationen und digitale Systeme zu schützen

- 2.) Welche Bestandteile bilden den Kern des BSI-Grundschutzes?

BSI-Standard 200-1 - 200-3 (200-1 ISMS WICHTIG!!!)
BSI-Standard 100-4
IT-Grundschutz-Kompendium mit Umsetzbeispielen

- 3.) Was ist ein "BSI-Grundschutz Baustein"?

- alle Bereiche des ISMS sind in Bausteine untergliedert
- beinhalten konkrete Maßnahmen und Umsetzungen
- prozessorientiert: (ORP, CON, OPS)
- systemorientiert: (DER, APP, SYS, IND, NET, INF)

- 4.) Beschreiben Sie kurz die drei Varianten der Absicherung nach dem BSI IT-Grundschutz-Verfahren.

Basisabsicherung: grundlegende Erstabsicherung um schnell die größten Risiken zu senken

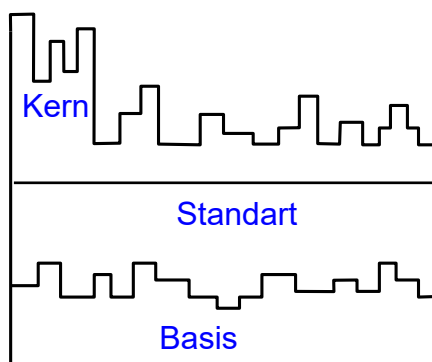
Kernabsicherung: Absicherung der wichtigsten Teile eines Unternehmens

Standardabsicherung: Angemessene und ausreichende Absicherung für alle Prozesse und Bereiche

- 5.) Im Rahmen der Kernabsicherung wird von "Kronjuwelen" gesprochen. Was heißt das?

Kronjuwelen sind die wichtigsten Teile eines Unternehmens

- 6.) Die folgende Grafik taucht häufig auf, wenn es um das Thema BSI IT-Grundschutz geht.



a) Zeigen Sie daran die drei Absicherungs-Varianten

b) Skizzieren Sie die Linie für den normalen Schutzbedarf hinein.

c) Markieren Sie die Assets der Kronjuwelen.