Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

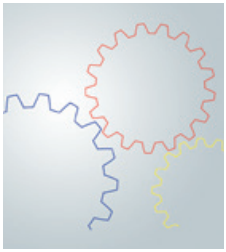
Informationssicherheit mit System

Der IT-Grundschutz des BSI

Inhaltsverzeichnis

Seite 4

Seite 11



Seite 10

Kurz und knapp: Der IT-Grundschutz des BSI

» **aktuell:** kontinuierliche Weiterentwicklung der Inhalte auf dem Stand der Technik

» **branchenspezifisch:** IT-Grundschutz-Profile als Muster-Sicherheitskonzepte für diverse Branchen

» **bewährt:** seit über 25 Jahren DIE Methodik für Informationssicherheit

» **international:** kompatibel zum internationalen Standard ISO/IEC 27001

» **modular:** flexible Verwendung einzelner Inhalte je nach individuellen Sicherheitsbedürfnissen

» **praxiserprobt:** kompakte und praktikable Methodik für eine angemessene Informationssicherheit

» **systematisch:** strukturiert aufgebaut für eine effiziente Bearbeitung von Themen

» **umfassend:** rund 100 IT-Grundschutz-Bausteine zu den relevanten Themen der Informationssicherheit

» **überschaubar:** Basis-Absicherung für eine grundlegende Erstabsicherung – auch für kleinere und mittelgroße Betriebe

» **zertifizierbar:** anerkannter Nachweis der Informationssicherheit

Informationssicherheit mit System

Die Digitalisierung gehört zu den zentralen Themen der Gegenwart für Wirtschaft und Verwaltung. Die Herausforderungen bezüglich Informations- und Cyber-Sicherheit nehmen dabei stetig zu – sei es durch Vernetzung und mobiles Arbeiten auf der einen Seite oder immer ausgefeiltere Cyber-Angriffe auf der anderen Seite. Die Anforderungen sind zahlreich und vielfältig: Sind die IT-Systeme gut gegen Cyber-Angriffe gewappnet? Können Beschäftigte im Bedarfsfall sicher auf das Unternehmensnetz und Kommunikationsanwendungen zugreifen? Sind Tablets zur Steuerung von Anlagen in der Produktion robust gegen Angriffe von außen? Können Behörden sichere digitale Anwendungen für Bürgerinnen und Bürger anbieten?

Nicht nur für diese Herausforderungen benötigen Institutionen ein starkes Fundament, um Informationen und IT bestmöglich schützen zu können. Der Schlüssel zur Informationssicherheit ist ein ganzheitliches und systematisches Managementsystem für Informationssicherheit (ISMS). Um ein solches System aufzubauen, stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) kostenfrei den IT-Grundschutz zur Verfügung. Darüber hinaus behandelt der IT-Grundschutz auch das Thema Notfallmanagement. Informationssicherheit und Notfallmanagement erhöhen zusammen die Widerstandsfähigkeit von Institutionen gegenüber den unterschiedlichsten Risiken und Bedrohungen.

In dieser Broschüre werden die verschiedenen Bestandteile des IT-Grundschutzes vorgestellt. Sie erfahren, welche Angebote sich für Ihren Arbeitsalltag zum Thema Informationssicherheit eignen und wie Ihre Institution von den praxiserprobten Empfehlungen aus dem IT-Grundschutz profitieren kann.

IT-Grundschutz – der bewährte Begleiter für Informationssicherheit

Das macht den IT-Grundschutz so einmalig

Der IT-Grundschutz ist seit über 25 Jahren die bewährte Methodik im Arbeitsalltag von Verantwortlichen in Behörden und Unternehmen: Welche Anforderungen an Informationssicherheit sind wichtig, welche Regelungen müssen definiert werden? Mit dem IT-Grundschutz können Verantwortliche ein passgenaues ISMS aufbauen und langfristig in ihrer Institution etablieren.

Ein ISMS beinhaltet diverse Aspekte, die in der IT-Grundschutz-Methodik berücksichtigt werden:

- den Sicherheitsbedarf definieren
- tragfähige Sicherheitskonzepte entwickeln

- passende Sicherheitsmaßnahmen festlegen
- bestehende Schutzmaßnahmen auf ihre Effektivität überprüfen

Der IT-Grundschutz ist in Deutschland DER Maßstab, wenn es um die Absicherung von Informationen und den Aufbau eines Managementsystems für Informationssicherheit geht.

Systematisches Vorgehen führt zum Ziel

Die BSI-Standards und das IT-Grundschutz-Kompendium bilden die Hauptwerke im IT-Grundschutz. Die BSI-Standards 200-1 bis 200-3 erläutern, wie ein ISMS in einer Institution aufgebaut werden kann und Geschäftsprozesse bzw. Fachaufgaben abgesichert werden können. Im IT-Grundschutz-Kompendium beschreiben Fachtexte, die sogenannten IT-Grundschutz-Bausteine, was ein Anwender tun muss, um einen bestimmten Bereich besser abzusichern. In Kombination angewandt, bilden diese beiden Komponenten des IT-Grundschutzes die Grundlage für eine solide Informationssicherheit.

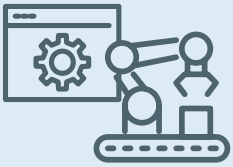
IT-Grundschutz bietet mehr als nur technische Hilfe

Die rund 100 IT-Grundschutz-Bausteine erläutern neben technischen Aspekten auch solche, die Infrastruktur, Organisation und Personal betreffen. Anwender können sich gezielt die IT-Grundschutz-Bausteine heraussuchen, die für ihre aktuellen Sicherheitsfragen relevant sind.

Gut gewappnet: Ganzheitliche Informationsicherheit mit IT-Grundschutz

Legende

- Beispielhafte Gefährdungen
- IT-Grundschutz-Bausteine zum Thema



Produktion

Zerstörung,
Produktionsunterbrechung

- IND.1 Prozessleit- und Automatisierungstechnik
- IND.2.2 Speicherprogrammierbare Steuerung
- IND.2.3 Sensoren und Aktoren

Internet

Hacker (Spionage, Zerstörung),
Schädlinge, Datenverlust,
Offenlegung von Daten

- APP.1.2 Web-Browser
- APP.3.1 Webanwendungen
- NET.3.2 Firewall

Hard- und Software

Bedienfehler, Datenverlust

- APP.1.4 Mobile Anwendungen
- NET.3.1 Router und Switches
- SYS.2.2.3 Clients unter Windows 10

Home Office

Fehlverhalten, Diebstahl, Manipulation, Offenlegung von Interna

- INF.8 Häuslicher Arbeitsplatz
- NET.3.3 VPN
- OPS.1.2.3 Telearbeit

Reisen

Datenverlust, Manipulation, Spionage

- CON.7 Informationssicherheit auf Auslandsreisen
- INF.9 Mobiler Arbeitsplatz
- SYS.3.3 Mobiltelefon

Menschen

Fehlverhalten, Manipulation, Spionage, Unwissenheit

- ORP.2 Personal
- ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
- ORP.4 Identitäts- und Berechtigungsmanagement

Infrastruktur

Fehlplanung, Feuer, unbefugtes Eindringen

- INF.2 Rechenzentrum sowie Serverraum
- INF.7 Büroarbeitsplatz
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume

Das Fundament: Die BSI-Standards

Die BSI-Standards erläutern, wie ein ISMS bestmöglich organisatorisch und systematisch aufgebaut werden kann.

Was macht ein ISMS aus?

Der **BSI-Standard 200-1: Managementsysteme für Informationssicherheit** beschreibt verständlich, welche grundlegenden Anforderungen ein Managementsystem für Informationssicherheit erfüllen muss. Er erläutert, welche Komponenten ein ISMS enthalten sollte und welche Aufgaben die Leitungsebene übernehmen muss.

Basis-, Standard- oder Kern-Absicherung?

Der **BSI-Standard 200-2: IT-Grundschutz-Methodik** beschreibt, wie ein ISMS schrittweise in einer Institution aufgebaut und aufrechterhalten werden kann. Hierfür erläutert er drei effiziente Vorgehensweisen. Die Basis-Absicherung kann bereits mit einem relativ geringen finanziellen, personellen und zeitlichen Aufwand realisiert werden. Darauf aufbauend ist das Ziel einer Standard-Absicherung ein vollumfängliches ISMS. Bei der Kern-Absicherung werden ausgewählte, besonders wichtige Bereiche abgesichert.

Welches Risiko besteht im Einzelfall?

Der **BSI-Standard 200-3: Risikomanagement** stellt ein vereinfachtes Verfahren zur Risikoanalyse dar und beinhaltet gebündelt alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes. Der Vorteil für die Anwender ist ein deutlich reduzierter Aufwand, um ein angestrebtes Sicherheitsniveau zu erreichen.

Was unternehme ich im Notfall?

Der **BSI-Standard 100-4: Notfallmanagement** zeigt einen systematischen Weg, um ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen. Damit können die zeitkritischen Geschäftsprozesse nach einem Ausfall schnell wieder aufgenommen werden. Dieser Standard wird derzeit aktualisiert. Zukünftig wird der **BSI-Standard 200-4: Business Continuity Management** den 100-4 ablösen. Bis zum Erscheinen des neuen Standards gelten die Empfehlungen zum Notfallmanagement aus dem BSI-Standard 100-4.

Die BSI-Standards

» Aufbau und Etablierung eines ISMS

» drei Vorgehensweisen für unterschiedliche Anwendungsfälle

» abgestimmt auf das IT-Grundschutz-Kompendium

» umfassen auch Risikomanagement und Notfallmanagement

» ISO/IEC 27001- bzw. ISO/IEC 22301-kompatibel

» ISO 27001-Zertifizierung auf Basis von IT-Grundschutz möglich

Weitere Informationen finden Sie hier: www.bsi.bund.de/standards

Das IT-Grundschutz-Kompendium

» DAS zentrale Arbeitswerkzeug für Informationssicherheit

» praxisnahe IT-Grundschutz-Bausteine zu allen relevanten Themen

» konkrete Sicherheitsanforderungen

» jährlich aktualisiert gemäß dem Stand der Technik

» kontinuierliche Fortschreibung zu neuen Themen

Weitere Informationen finden Sie hier: www.bsi.bund.de/gs-kompendium

Das Werkzeug: Das IT-Grundschutz-Kompendium

Das IT-Grundschutz-Kompendium besteht aus den IT-Grundschutz-Bausteinen und einer Einführung in die Thematik. Es enthält jährlich aktualisiert praxisorientiertes Fachwissen zu den wichtigsten Themen der Informationssicherheit. Ergänzend zu den IT-Grundschutz-Bausteinen erläutern Umsetzungshinweise, wie geeignete Sicherheitsmaßnahmen im jeweiligen Kontext realisiert werden können.

Gefährdungen und Anforderungen

Die IT-Grundschutz-Bausteine sind zehn verschiedenen Themenbereichen zugeordnet, den sogenannten Schichten. Dazu zählen etwa „Organisation und Personal", „IT-Systeme", „Anwendungen" oder „Detektion und Reaktion". Neben technischen Aspekten werden auch Sicherheitsaspekte zu Infrastruktur, Organisation und Personal berücksichtigt. Der Aufbau ist stets gleich: Nach einer Einführung in die jeweilige Thematik werden exemplarische Gefährdungen benannt und danach die Sicherheitsanforderungen erläutert. Die Anforderungen gliedern sich in Basis- und Standard-Anforderungen sowie in Anforderungen bei erhöhtem Schutzbedarf.

Umsetzungshinweise

Die IT-Grundschutz-Bausteine beschreiben detailliert, was für ein angemessenes Sicherheitsniveau erforderlich ist. Die Umsetzungshinweise geben für viele Bausteine konkrete Tipps, wie die Anforderungen umgesetzt werden können. Hier erfahren Anwender, wie geeignete Sicherheitsmaßnahmen zu realisieren sind und können einzelne Schritte nachvollziehen.

Leichter Einstieg über die Online-Kurse

Der Online-Kurs IT-Grundschutz richtet sich an Anwender, die sich zum ersten Mal mit den Inhalten des IT-Grundschutzes befassen möchten. Sie erfahren zum Beispiel, wie sie bei der Einführung eines ISMS strategisch vorgehen sollten, welche Aufgaben ein Informationssicherheitsbeauftragter (ISB) hat oder welche Aspekte in einer Informationssicherheitsleitlinie erfasst sein sollten. Der Online-Kurs eignet sich für Anwender aus Wirtschaft und Verwaltung, auch KMU sind eingeladen, den Kurs für erste Sicherheitsbetrachtungen zu nutzen. Der Online-Kurs zum IT-Grundschutz basiert auf Bausteinen des IT-Grundschutz-Kompendiums und den BSI-Standards 200-1, -2 und -3.

Ein weiterer Online-Kurs beschäftigt sich – basierend auf dem BSI-Standard 100-4 – mit dem Thema Notfallmanagement. Der Kurs wird nach der Veröffentlichung des neuen BSI-Standards 200-4 modernisiert. Beide Kurse sind auf der Website des BSI kostenfrei verfügbar. Sie sind allgemeinverständlich und bilden jeweils einen sehr guten Einstieg in die IT-Grundschutz-Methodik.

Weitere Informationen finden Sie hier: www.bsi.bund.de/grundschutzkurs

IT-Grundschutz-Profile: Informationssicherheit nach Branche

In einem IT-Grundschutz-Profil werden die einzelnen Schritte eines Sicherheitsprozesses für einen definierten Anwendungsbereich dokumentiert. Diese Schablonen für Informationssicherheit werden in der Regel von mehreren Institutionen einer Branche gemeinsam erstellt – meist mit Beteiligung von Branchenverbänden. Anwender, die ähnliche Sicherheitsanforderungen haben, können auf der Basis eines IT-Grundschutz-Profils mit deutlich reduziertem Aufwand ihre Geschäftsprozesse absichern. IT-Grundschutz-Profile sind unter anderem für Handwerksbetriebe, Kommunalverwaltungen oder Papierfabriken veröffentlicht. Gemeinsam mit der Allianz für Cyber-Sicherheit, der Wirtschaftsinitiative des BSI, unterstützt das IT-Grundschutz-Team interessierte Anwender mit einer Workshop-Reihe bei der Erstellung von IT-Grundschutz-Profilen. Eine Anleitung auf der Website des BSI führt Anwender durch den Erstellungsprozess für ein IT-Grundschutz-Profil.

Weitere Informationen finden Sie hier: https://www.bsi.bund.de/profile

Zertifizierung nach IT-Grundschutz: Nachgewiesene Informationssicherheit

Ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz ist sowohl für Behörden als auch für Unternehmen sinnvoll. Eine erfolgreiche Zertifizierung belegt, dass die technischen und organisatorischen Maßnahmen rund um die Informationssicherheit anerkannten internationalen Standards entsprechen – und schafft dadurch zusätzliches Vertrauen bei Kunden und Partnern. Zertifizierungsverfahren werden von einem externen Auditor durchgeführt.

Personenzertifizierung zum IT-Grundschutz-Berater: Nachgewiesene Expertise

Das BSI hat ein zweistufiges Schulungsangebot entwickelt, um die Ausbildung im Bereich IT-Grundschutz auf ein einheitlich hohes Niveau zu bringen. Interessierte Personen können sich zunächst zum IT-Grundschutz-Praktiker und im nächsten Schritt zum IT-Grundschutz-Berater qualifizieren. Mit dem Abschluss zum IT-Grundschutz-Berater ist eine gleichnamige Personenzertifizierung möglich. Auf der Website des BSI gibt es eine Übersicht von Fortbildungsinstituten, die Schulungen zum IT-Grundschutz-Praktiker und -Berater anbieten.

Weitere Informationen finden Sie hier: https://www.bsi.bund.de/gsberater

Ausführliche Infos auf der Website des BSI

Weitere Informationen zu allen Angeboten und Veröffentlichungen rund um den IT-Grundschutz gibt es auf der BSI-Website unter www.bsi.bund.de/grundschutz.

Mehr erfahren?

Kontakt zum IT-Grundschutz

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

Twitter

Alle aktuellen Neuigkeiten rund um den IT-Grundschutz gibt es auch bei Twitter unter @BSI_Bund, #ITGrundschutz.

https://www.bsi.bund.de/SozialeNetzwerke

Newsletter

Der IT-Grundschutz-Newsletter informiert Anwender und Interessierte regelmäßig per E-Mail. Die Registrierung erfolgt über die BSI-Website.

https://www.bsi.bund.de/newsletter

Xing

Für Anwender und Interessierte hat das BSI bei Xing die Gruppe „IT-Grundschutz" eingerichtet. Sie bietet Informationen, Neuigkeiten und Erfahrungsaustausch zum Thema.

https://www.bsi.bund.de/SozialeNetzwerke

IT-Grundschutz-Tage

Das BSI veranstaltet regelmäßig IT-Grundschutz-Tage. In Kooperation mit einem Unternehmen oder einer Behörde wird dabei die konkrete Umsetzung des IT-Grundschutzes erläutert – themenorientiert und praxisnah.

www.bsi.bund.de/grundschutz

Allianz für Cyber-Sicherheit

Allianz für Cyber-Sicherheit

Mit der 2012 gegründeten Allianz für Cyber-Sicherheit (ACS) verfolgt das BSI das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Hierfür realisiert die größte Cyber-Sicherheits-Public-Private-Partnership der Bundesrepublik zahlreiche Formate, die das nötige Know-how in Organisationen fördern. Best-Practices und aktuelle Warnmeldungen zählen ebenso zu den Angeboten, wie Cyber-Sicherheits-Tage oder Workshops zur Erstellung von IT-Grundschutz-Profilen, die in Kooperation mit dem IT-Grundschutz-Team organisiert werden.

Weitere Informationen: https://www.allianz-fuer-cybersicherheit.de

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185 – 189
53175 Bonn
Tel.: +49 228 99 9582-0
E-Mail: bsi@bsi.bund.de

Text und Redaktion
PRESSTO GmbH, Köln

Layout und Gestaltung
artwork factory, Köln

Druck
Appel und Klinger Druck & Medien GmbH
Bahnhofstraße 39
96277 Schneckenlohe
www.ak-druck-medien.de

Bildnachweis
Titelbild: Adobe Stock / Photocreo Bednarek, istockphoto / nadla,
S. 4: Adobe Stock / sdecoret, S. 5: Adobe Stock / NicoElNino,
S. 6: Adobe Stock / Graf Vishenka, S. 7: Adobe Stock / sdecoret,
S. 11: Adobe Stock / Elnur, S. 12: Adobe Stock / Thitiphat,
S. 14: Adobe Stock / sepy, S. 15: Adobe Stock / NDABCREATIVITY,
S. 16: Adobe Stock / jackfrog, S. 17: Adobe Stock / panitan,
S. 3 und 13: Bundesamt für Sicherheit in der Informationstechnik - BSI

Stand
11/2020

Artikelnummer
BSI-Bro20/333

www.bsi.bund.de

www.bsi.bund.de