# 

# Überblick

Februar **2018** erschien die **erste Edition** des **IT-Grundschutz-Kompendiums** und definierte die Anforderungen des BSI an die IT-Sicherheit. Das IT-Grundschutz-Kompendium ist seitdem elementarer Bestandteil und **grundlegendes Instrument** aller IT-Sicherheitsbetrachtungen in Deutschland.

Das BSI wird nun jährlich jeweils zum 01.02. eine aktualisierte Version des IT-Grundschutz-Kompendiums veröffentlichen.

Die Version 2021 enthält **achthundertzehn Seiten und ist grob wie folgt gegliedert:**

1. Vorwort, Verzeichnis, Einleitung, Rollen (definiert die beteiligen Personen) und Glossar
2. Auflistung der „**elementaren Gefährdungen**“ (49 Seiten)
3. Auflistung aller **Prozess- und System-Bausteine** (97 Stück auf 710 Seiten!)

# BSI - Elementare Gefährdungen

Das BSI hat aus den vielen spezifischen Einzelgefährdungen der Bausteine der früheren IT-Grundschutz-Kataloge die generellen Aspekte herausgearbeitet und in **47 sogenannte elementare Gefährdungen** überführt. Diese sind **im IT-Grundschutz-Kompendium** aufgeführt. Bei der Erstellung der Übersicht der elementaren Gefährdungen wurden die im Folgenden beschriebenen Ziele verfolgt. Elementare Gefährdungen sind

* für die Verwendung bei der **Risikoanalyse** optimiert (wie heißt noch das Lernfeld? Richtig: „**Schutzbedarfsanalyse**“, aha!),
* **produktneutral** (immer), **technikneutral** (möglichst, bestimmte Techniken prägen so stark den Markt, dass sie auch die abstrahierten Gefährdungen beeinflussen),
* kompatibel mit vergleichbaren internationalen Katalogen und Standards und
* nahtlos in den **IT-Grundschutz** (wichtigster Begriff „ever“) integriert.

Quelle: Nach <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html> ,abg. am 20.9.2021

# Auftrag:

1. Verschaffen Sie sich einen **Überblick** über die 47 elementaren Gefährdungen! Nutzen Sie dazu die PDF des BSI und clustern Sie die 47 Punkte in beispielsweise 5 Abschnitte!

**Natur und Umwelt**:

G 0.1 Feuer

G 0.2 Ungünstige klimatische Bedingungen

G 0.3 Wasser

G 0.4 Verschmutzung, Staub, Korrosion

G 0.5 Naturkatastrophen

G 0.10 Ausfall oder Störung von Versorgungsnetzen

**Technische Ausfälle und Störungen**:

G 0.8 Ausfall oder Störung der Stromversorgung

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.12 Elektromagnetische Störstrahlung

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

**Menschliches Fehlverhalten**:

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.24 Zerstörung von Geräten oder Datenträgern

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

**Vorsätzliche Handlungen**:

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.34 Anschlag

G 0.35 Nötigung, Erpressung oder Korruption

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

**IT-spezifische Bedrohungen**:

G 0.13 Abfangen kompromittierender Strahlung

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

1. **Lesen** Sie den Text zum Vorfall „Hackerangriff erschüttert USA“. **Kreuzen** Sie dann unten die elementaren Gefährdungen an, die in dem Artikel als **Schaden** erwähnt werden!
2. **Unterstreichen** Sie anschließend die elementaren Gefährdungen, die von den Angreifern bei ihrer Vorgehensweise (fette Absätze) als **Sicherheitslücken** ausgenutzt worden sind!

**Elementare Gefährdungen nach BSI**

* G 0.1 Feuer
* G 0.2 Ungünstige klimatische Bedingungen
* G 0.3 Wasser
* G 0.4 Verschmutzung, Staub, Korrosion
* G 0.5 Naturkatastrophen
* G 0.6 Katastrophen im Umfeld
* G 0.7 Großereignisse im Umfeld
* G 0.8 Ausfall oder Störung der Stromversorgung
* G 0.9 Ausfall oder Störung von Kommunikationsnetzen
* G 0.10 Ausfall oder Störung von Versorgungsnetzen



* G 0.11 Ausfall oder Störung von Dienstleistern
* G 0.12 Elektromagnetische Störstrahlung
* G 0.13 Abfangen kompromittierender Strahlung
* G 0.14 Ausspähen von Informationen (Spionage)
* G 0.15 Abhören



* G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
* G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten
* G 0.18 Fehlplanung oder fehlende Anpassung
* G 0.19 Offenlegung schützenswerter Informationen



* G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle



* G 0.21 Manipulation von Hard- oder Software
* G 0.22 Manipulation von Informationen



* G 0.23 Unbefugtes Eindringen in IT-Systeme



* G 0.24 Zerstörung von Geräten oder Datenträgern
* G 0.25 Ausfall von Geräten oder Systemen
* G 0.26 Fehlfunktion von Geräten oder Systemen
* G 0.27 Ressourcenmangel
* G 0.28 Software-Schwachstellen oder -Fehler



* G 0.29 Verstoß gegen Gesetze oder Regelungen
* G 0.30 Unberechtigte Nutzung/Administr. von Geräten und Systemen



* G 0.31 Fehlerhafte Nutzung/Administr. von Geräten und Systemen
* G 0.32 Missbrauch von Berechtigungen
* G 0.33 Personalausfall
* G 0.34 Anschlag
* G 0.35 Nötigung, Erpressung oder Korruption
* G 0.36 Identitätsdiebstahl
* G 0.37 Abstreiten von Handlungen
* G 0.38 Missbrauch personenbezogener Daten



* G 0.39 Schadprogramme



* G 0.40 Verhinderung von Diensten (Denial of Service)
* G 0.41 Sabotage
* G 0.42 Social Engineering
* G 0.43 Einspielen von Nachrichten



* G 0.44 Unbefugtes Eindringen in Räumlichkeiten



* G 0.45 Datenverlust
* G 0.46 Integritätsverlust schützenswerter Informationen
* G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe