

---

# **BSI**

# **Grundschutzhandbuch**

**Andre Böhringer,  
Benjamin Bratkus,  
Thomas Steinhart,  
Tobias Satzger**

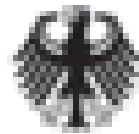
---

# BSI-Grundschriftzhandbuch!?!?

## was ist denn das?



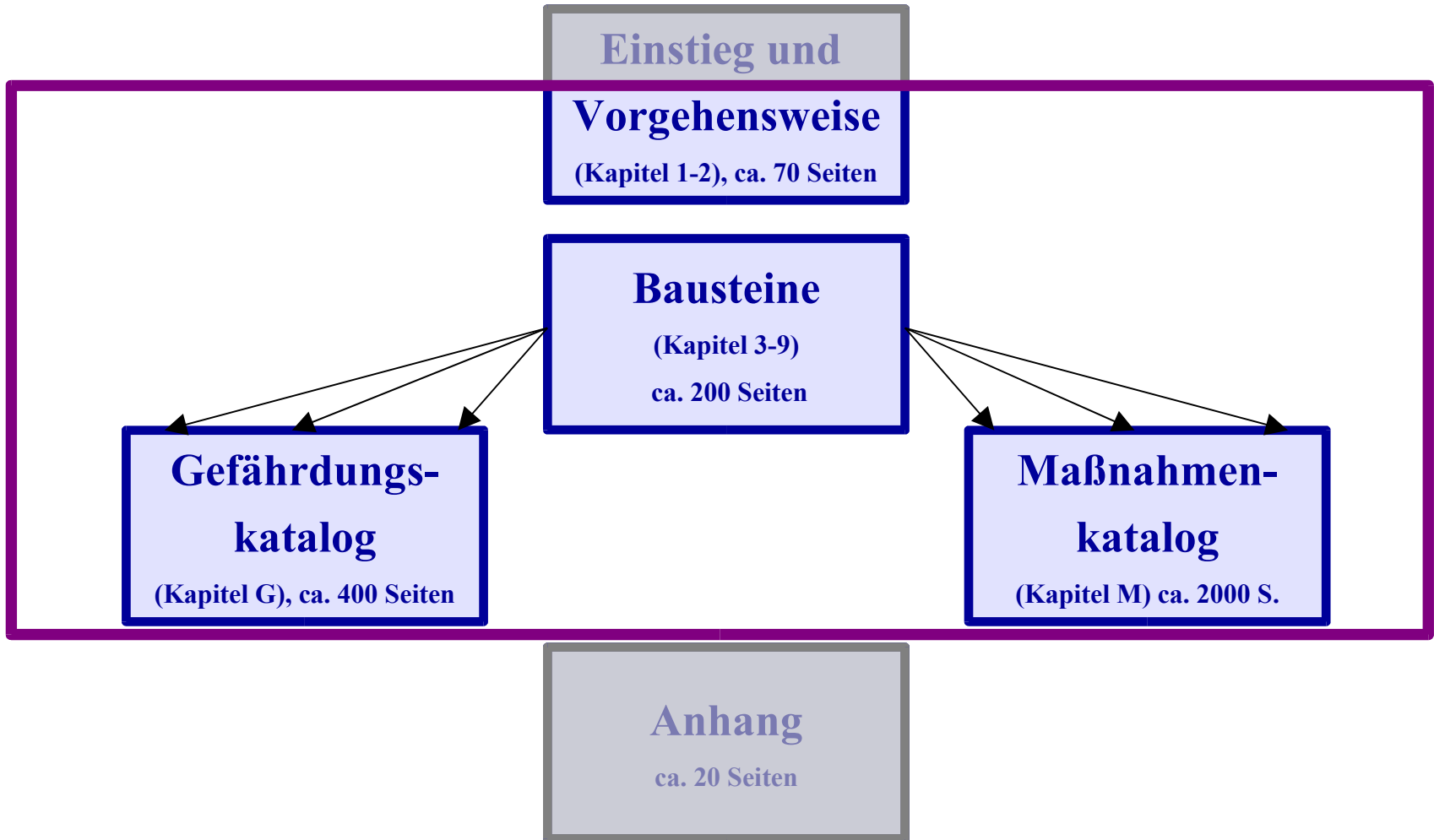
- 
- **Nachschlagewerk**
  - **detaillierte Beschreibung der Vorgehensweise zur Umsetzung von Sicherheitslösungen**



Bundesamt  
für Sicherheit in der  
Informationstechnik

[www.bsi.de](http://www.bsi.de)

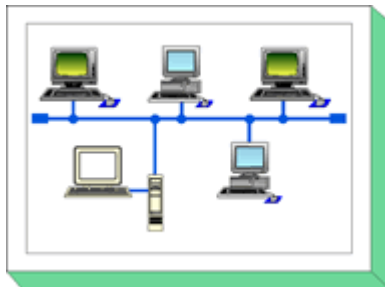
# Aufbau



# Aufbau Bausteine

---

- **Beschreibung**
- **Gefährdungslage**
- **Maßnahmenempfehlungen**

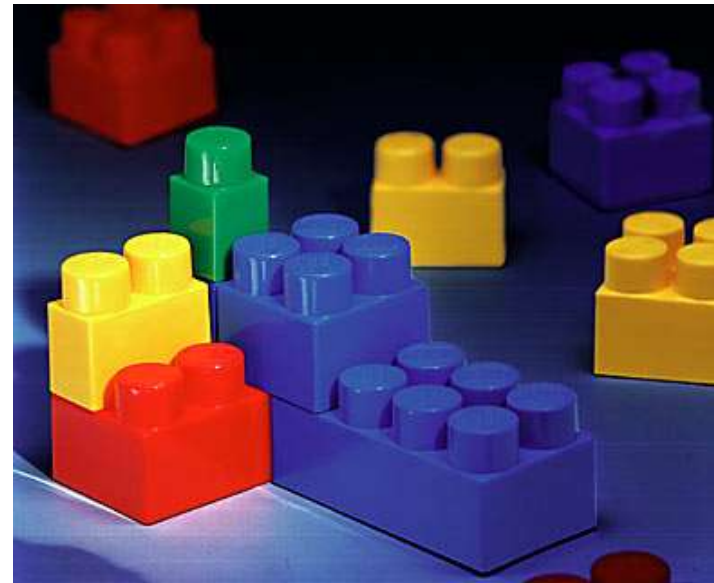


Beispiel: Baustein 6.2 Unix-Server

# weitere Beispiele Bausteine

---

- Notfallvorsorge-Konzept
- Schutzschranke
- Rechenzentrum
- PC mit Windows NT
- Tragbarer PC
- UNIX-Server
- Firewall
- Apache-Webserver
- Mobiltelefon
- Datenbanken



# Beispiele Gefahren

---

- Ausfall des IT-Systems
- Feuer
- Mangelhafte Beschreibung von Dateien
- Unerlaubte Ausübung von Rechten
- Vandalismus
- DNS-Spoofing
- Hijacking von Netz-Verbindungen

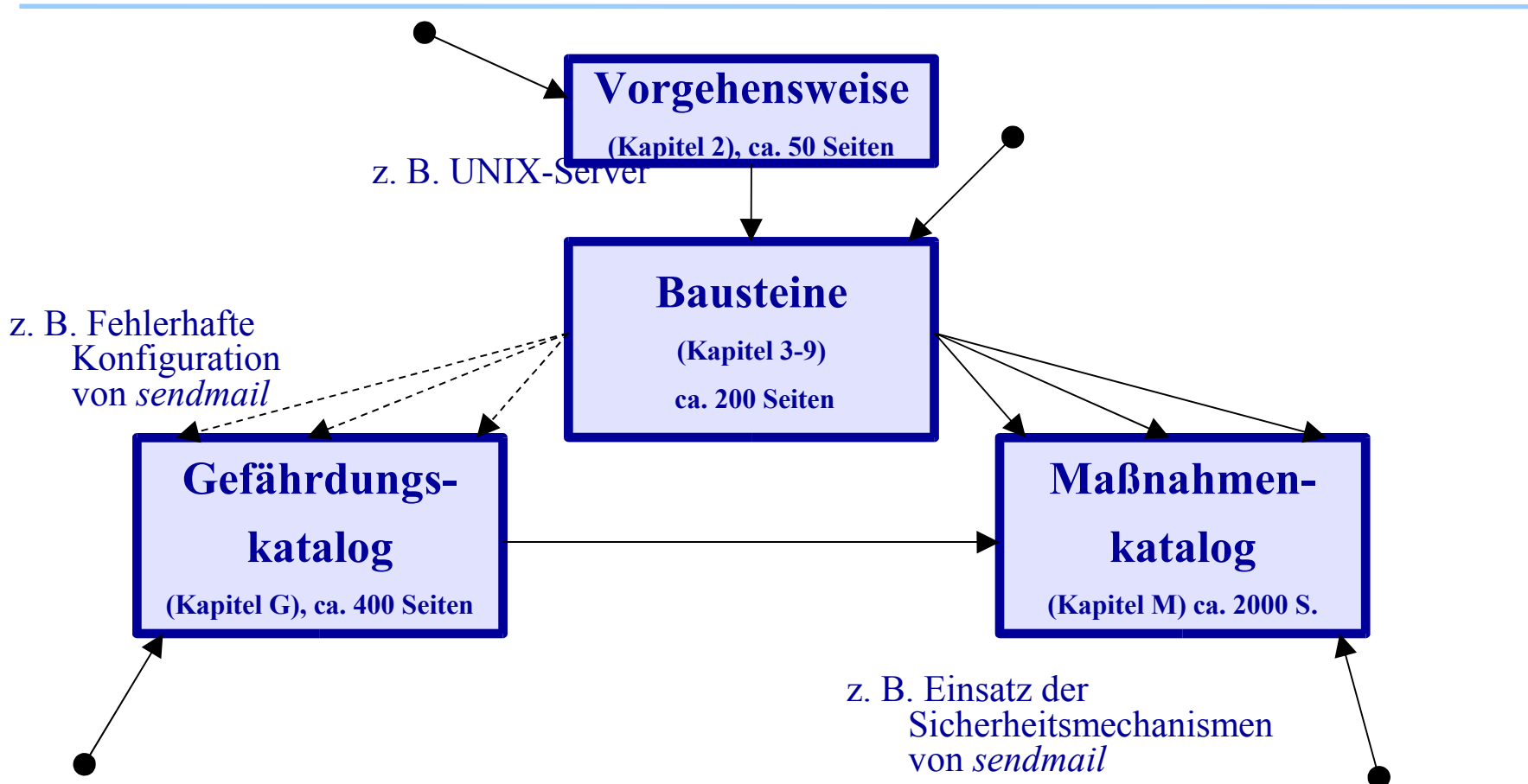


# Beispiele Maßnahmen

---

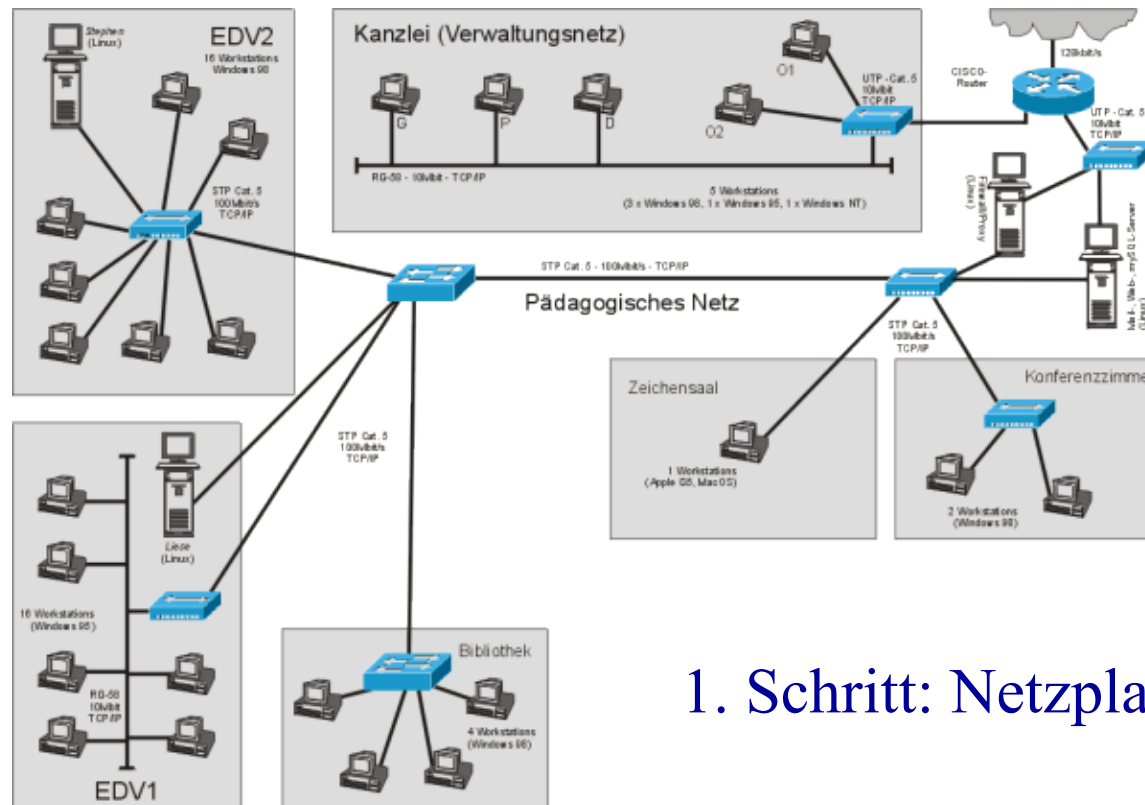
- Handfeuerlöscher
- Videoüberwachung
- Geeignetes Schlüsselmanagement
- Sperren nicht benötigter Leistungsmerkmale
- Einrichten des LDAP-Zugriffs auf Novell eDirectory
- Absicherung von E-Mail mit SPHINX (S/MIME)
- Verwendung eines Zeitstempel-Dienstes





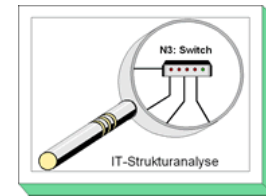
# Anwendung des Handbuchs

- detaillierte Beschreibung der einzelnen Schritte



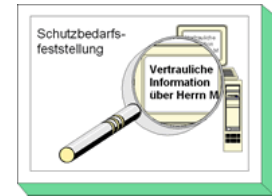
## 1. Schritt: Netzplanerhebung

# Strukturanalyse



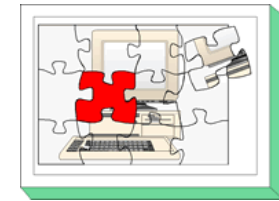
Nr.	Beschreibung	Plattform	Anz.	Aufstellungsort	Status	Anwender/Admin.
S1	Server für Personalverwaltung	Windows NT-Server	1	Bonn, R 1.01	in Betrieb	Personalreferat
S2	Primärer Domänen-Controller	Windows NT-Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
C1	Gruppe von Clients der Personaldatenverarbeitung	Windows NT-Workstation	5	Bonn, R 1.02 - R 1.06	in Betrieb	Personalreferat
C6	Gruppe der Laptops für den Standort Berlin	Laptop unter Windows 95	2	Berlin, R 2.01	in Betrieb	alle IT-Anwender in der Außenstelle Berlin
N2	Firewall	Application Gateway auf Unix	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N3	Switch	Switch	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
T1	TK-Anlage für Bonn	ISDN-TK-Anlage	1	Bonn, B.02	in Betrieb	alle Mitarbeiter in der Hauptstelle Bonn

# Schutzbedarfsfeststellung



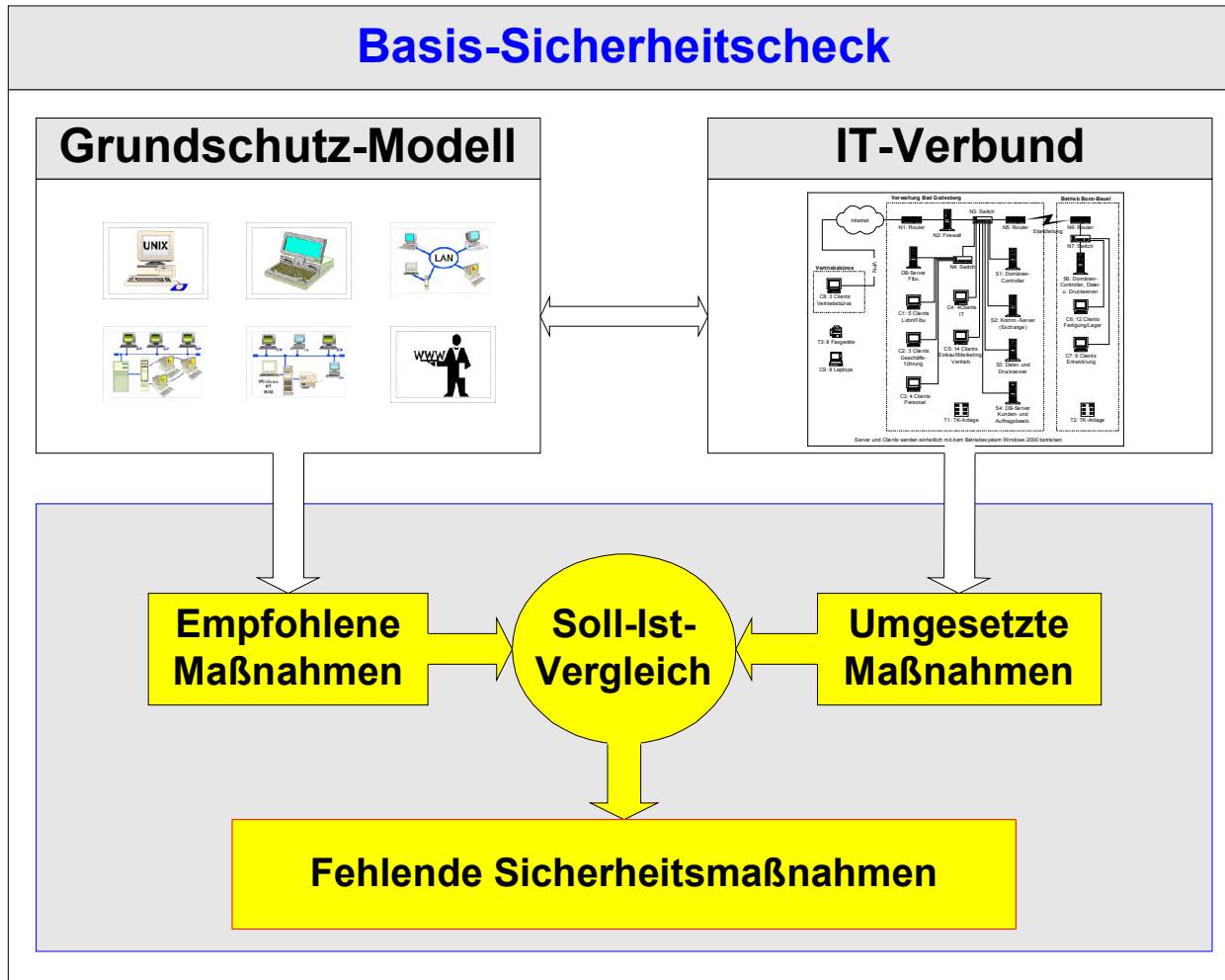
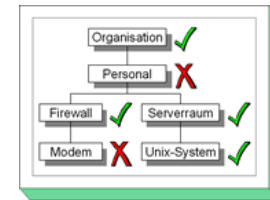
Bezeichnung	Art	Lokation	IT Systeme / Datenträger	Vertraulichkeit	Integrität	Verfügbarkeit
R U.02	Datenträgerarchiv	Gebäude Bonn	Backup-Datenträger (Wochensicherung der Server S1 bis S5)	hoch	hoch	mittel
R B.02	Technikraum	Gebäude Bonn	TK Anlage	mittel	mittel	hoch
R 1.01	Serverraum	Gebäude Bonn	S1, N4	hoch	hoch	mittel
R 1.02 – R 1.06	Büroräume	Gebäude Bonn	C1	hoch	mittel	mittel
R 3.11	Schutzschrank in Raum R 3.11	Gebäude Bonn	Backup-Datenträger (Tagessicherung der Server S1 bis S5)	hoch	hoch	mittel
R E.03	Serverraum	Gebäude Berlin	S6, N6, N7	mittel	hoch	hoch
R 2.01 – R 2.40	Büroräume	Gebäude Berlin	C4, einige mit Faxgeräten	mittel	mittel	mittel

# Modellierung mittels der Bausteine



Nr.	Titel des Bausteins	Zielobjekt/ Zielgruppe	Ansprech- partner	Hinweise
3.1	Organisation	Standort Bonn		Der Baustein Organisation muss für die Standorte Bonn und Berlin separat bearbeitet werden, da in Berlin eigene organisatorische Regelungen gelten.
3.1	Organisation	Standort Berlin		
3.2	Personal	gesamtes BOV		Die Personalverwaltung des BOV erfolgt zentral in Bonn.
4.3.3	Datenträgerarchiv	R U.02 (Bonn)		In diesem Raum werden die Backup-Datenträger aufbewahrt
5.3	Tragbarer PC	C5		Die Laptops in Bonn bzw. Berlin werden jeweils in eine Gruppe zusammengefasst.
5.3	Tragbarer PC	C6		
7.5	WWW-Server	S5		S5 dient als Server für das Intranet.
9.2	Datenbanken	S5		Auf dem Server S5 kommt eine Datenbank zum Einsatz

# Soll-Ist-Vergleich



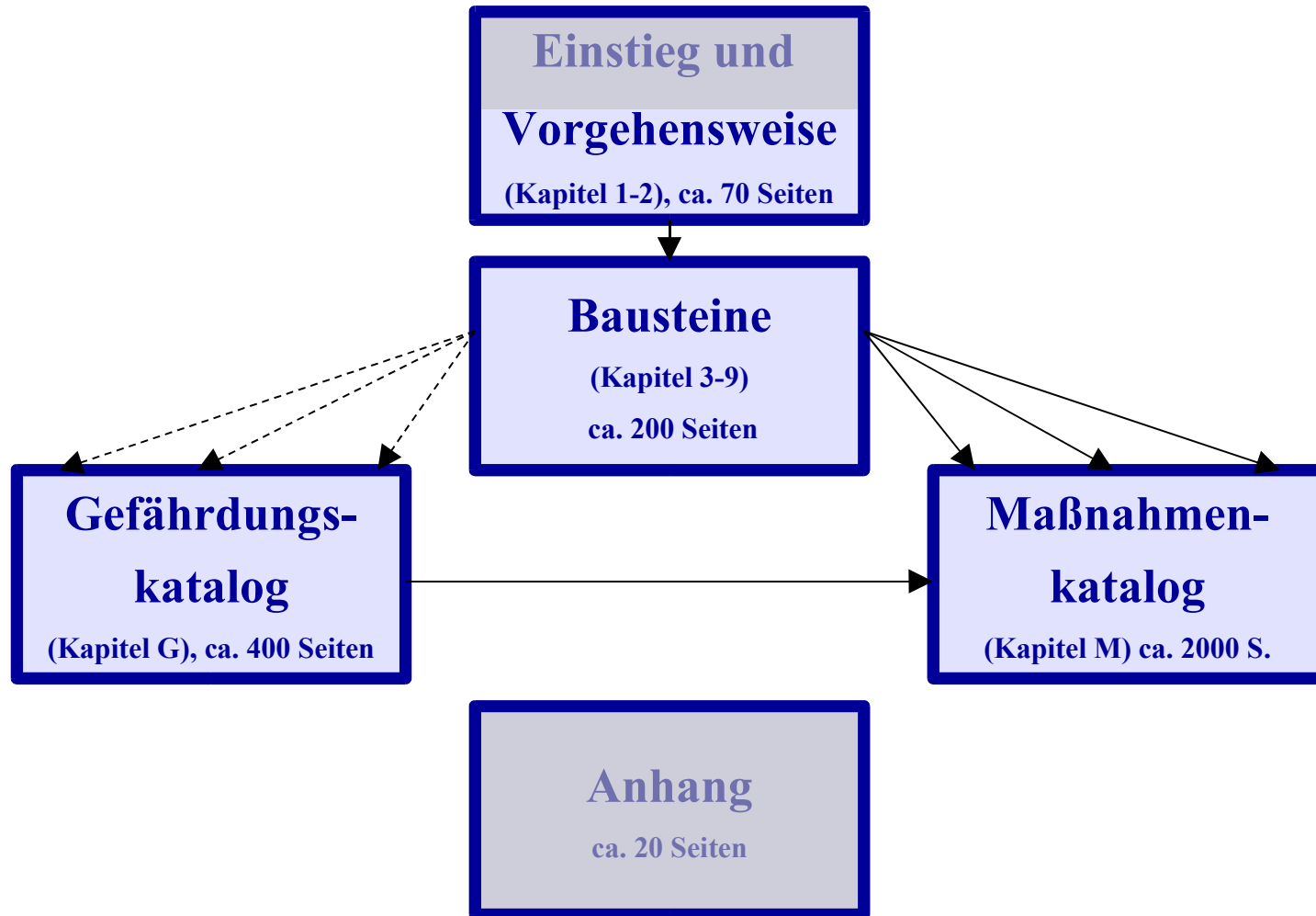
# Zertifikat

---



# Übersicht

---



# Gefahrenkatalog Übersicht

---

## Katalog gegliedert in fünf Kapitel

- G1 „Höhere Gewalt“
- G2 „Organisatorische Mängel“
- G3 „Menschliche Fehlhandlungen“
- G4 „Technisches Versagen“
- G5 „Vorsätzliche Handlungen“

# Gefährdungskatalog G1

---

- Keinen direkten Einfluss auf das Auftreten der Gefährdungen
- Präventive Massnahmen
- Beispiele:
  - Naturkatastrophen
  - Personalausfälle
  - Veranstaltungen

# Gefährdungskatalog G2

---

- Gefahren treten durch Disorganisation auf
- Behandelt die Planung des IT-Systems
- Beispiele:
  - Fehlende und unzureichende Regelungen
  - Unzureichende Kenntnis über Regelungen
  - Fehlende, ungeeignete und inkompatible Betriebsmittel

# Gefährdungskatalog G3

---

- Gefahren treten durch fahrlässiges Handeln auf
- Behandelt den Betrieb und Alltag des IT-System
- Beispiele:
  - Fahrlässige Zerstörung von Gerät oder Daten
  - Kein ordnungsgemäßer PC-Benutzerwechsel
  - Unbeabsichtigte Datenmanipulation

# Gefährdungskatalog G4

---

- Gefahren entstehen durch Hard- und Software
- Gefahren treten während des Betriebs auf
- Beispiele:
  - Verlust gespeicherter Daten
  - Defekte Datenträger
  - Ausfall der Stromversorgung

# Gefährdungskatalog G5

---

- Durch Absicht und Willen entstehen Gefahren
- Schädigung des IT-Systems durch den Menschen
- Beispiele:
  - Manipulation von Daten oder Software
  - Diebstahl
  - Vandalismus
  - Gebührenbetrug

# Maßnahmenkatalog Übersicht

---

Katalog gegliedert in sechs Kapitel

- M1 „Infrastruktur“
- M2 „Organisation“
- M3 „Personal“
- M4 „Hardware/Software“
- M5 „Kommunikation“
- M6 „Notfallvorsorge“

# Maßnahmenkataloge

---

- M1 „Infrastruktur“
  - Hauptsächlich Gebäudemaßnahmen
  - Aufbewahrung und Lagerung von Geräten
- M2 „Organisation“
  - Allgemeine organisatorische Maßnahmen
  - Spezielle Maßnahmen z.B. für
    - Firewall
    - Datenbanken

# Maßnahmenkataloge

---

- M3 „Personal“
  - Allgemeine Verfahrensvorschläge beim
    - Einlernen
    - Vertreten
    - Ausscheiden eines Mitarbeiters
  - Schulungen
- M4 „Hardware/Software“
  - Allgemeine Maßnahmen, z.B.
  - Maßnahmen für spezielle Software, z.B.
    - Windows NT/2000
    - Unix
    - Novell
    - Lotus Notes

# Maßnahmenkataloge

---

- M5 „Kommunikation“
  - Schutz für
    - Email
    - Telefonie
  - Allgemeiner Netzwerkschutz
- M6 „Notfallvorsorge“
  - Was kann getan werden, wenn ein Notfall eingetreten ist
  - Wie kann der Betrieb weitergehen, wenn ein Notfall eingetreten ist

# Beispiel

---

Die Gefährdungen und  
Maßnahmen des  
Grundschutzhandbuches am  
Beispiel von  
Datenbanken

# Höhere Gewalt

---

- **Gefährdung:**
  - Personalausfall
    - Krankheit
    - Tod
    - Urlaub
    - Kündigung
    - Abteilungswechsel

# Höhere Gewalt

---

- **Maßnahmen:**

- Hinterlegen des Passwortes
- Dokumentation der Systemkonfiguration
- Dokumentation der Veränderungen an einem bestehenden System
- Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
- Erstellung eines Anforderungskataloges für Standardsoftware

# Organisatorische Mängel

---

- **Gefährdung:**

Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen

- **Maßnahmen:**

- Regelmäßiger Sicherheitscheck der Datenbank
- Geeignete Auswahl einer Datenbank - Software
- Erstellung eines Datenbank - Sicherheitskonzeptes

# Menschliche Fehlhandlung

---

- **Gefährdung:**

Durch Reinigungs- oder Fremdpersonal  
(Betriebsspionage)

- **Maßnahme:**

Verpflichtung der PC-Benutzer zum  
Abmelden nach Aufgabenerfüllung

# Menschliche Fehlhandlung

---

- **Gefährdung:**

Fehlerhafte Administration von Zugangs- und Zugriffsrechten

- **Maßnahme:**

Sperren und Löschen nicht benötigter Datenbank- Accounts

# Menschliche Fehlhandlung

---

- **Gefährdung:**

Fehlerhafte Administration eines DBMS

- **Maßnahmen:**

- Auswahl eines vertrauenswürdigen Administrators und Vertreters
- Schulung des Wartungs- und Administrationspersonals

# Technisches Versagen

---

- **Gefährdung:**  
Ausfall einer Datenbank
- **Maßnahmen:**
  - Durchführung einer Datenbanküberwachung
  - Wiederherstellung einer Datenbank

# Technisches Versagen

---

- **Gefährdung:**

Verlust der Datenbankintegrität/-konsistenz

- **Maßnahmen:**

- Sicherstellung einer konsistenten Datenbankverwaltung
- Verhaltensregeln nach Verlust der Datenbankintegrität

# Vorsätzliche Handlungen

---

- **Gefährdung:**

- Unberechtigte IT-Nutzung
- Systematisches Ausprobieren von Passwörtern

- **Maßnahmen:**

- Passwortschutz für IT-Systeme
- Änderung voreingestellter Passwörter

# GSTOOL

---

- Zur Überprüfung des eigenen Grundschutzes
- Zur Dokumentation des Grundschutzes
- Keine Analyse

# Quellen

---

- Grundschriftzhandbuch
  - <http://www.bsi.bund.de/gshb/deutsch/index.html>