TÜV Informationstechnik GmbH
Langemarckstraße 20
45141 Essen, Germany
Phone: +49-201-8999-401
Fax: +49-201-8999-888
Email: A.sommer@tuvit.de
Web: www.tuvit.de

Sicherheit als strategische Herausforderung

Antonius Sommer
Geschäftsführer

TÜV Informationstechnik GmbH

The Trust Provider

IT-Sicherheit als strategische Herausforderung

Die Nutzung neuer Informationstechnologien, insbesondere das Internet mit allen seinen e-Disziplinen, vom e-Business über e-Commerce und e-Government bis hin zu e-Procurement und e-Services, eröffnet allen Organisationen, ob privatwirtschaftlicher oder staatlicher Natur neue Möglichkeiten zur Effizienzsteigerung und Kostensenkung. Dies ist die eine Seite der Medaille. Auf der Kehrseite finden sich die Risiken durch Hacker, Viren und Würmer, elektronischer Spionage, CyberWar und CyberTerrorismus.

Quelle: HP

Was sieht für die Realität aus?

•Verbraucher und Bürger haben kein Vertrauen in Nutzung der e-Angebote

•Organisationen sehen IT-Sicherheit häufig noch als nice to have an

•Die Sensibilisierung und Aufklärung in der Gesellschaft ist noch unzureichend

Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)

Drei Strategische Ziele:

1. **Prävention: Informationsinfrastrukturen angemessen schützen**
2. **Reaktion: Wirkungsvoll bei IT-Sicherheitsvorfällen handeln**
3. **Nachhaltigkeit: Deutsche IT-Sicherheitskompetenz stärken – internationale Standards setzen**

Quelle: NPSI

Nationale Plan zum Schutz der Informationsinfrastrukturen (NPSI)

Drei strategische Ziele:

1. **Prävention: Informationsinfrastrukturen angemessen schützen**
2. **Reaktion: Wirkungsvoll bei IT-Sicherheitsvorfällen handeln**
3. **Nachhaltigkeit: Deutsche IT-Sicherheitskompetenz stärken – internationale Standards setzen**

Gewährleistung der IT-Sicherheit auf hohem Niveau

Quelle: NPSI

Nationale Plan zum Schutz der Informationsinfrastrukturen (NPSI)

Was bedeutet dies in der Umsetzung:

1. **Prävention: Informationsinfrastrukturen angemessen schützen**
   - **Einsatz von zertifizierten Produkten**
   - **Betrieb von Zertifizierten IT-Systemen / IT-Installationen**
   - **Nachvollziehbares Sicherheitsniveau durch zertifiziertes Sicherheitsmanagementsystem nach IT-Grundschutz oder ISO 17799**

Quelle: NPSI

Nationale Plan zum Schutz der Informationsinfrastrukturen (NPSI)

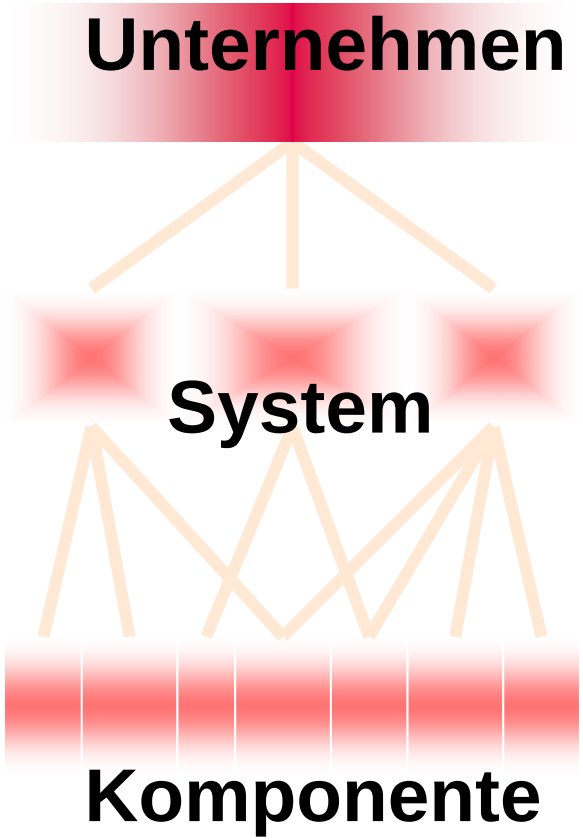
Was bedeutet dies in der Umsetzung:

2. **Reaktion: Wirkungsvoll bei IT-Sicherheitsvorfällen handeln**
   - **Nutzung der vorhandenen CERT z.B. CERT-Bund (CERT: Computer Emergency Response Team)**

Quelle: NPSI

Informationssicherheit

auf **allen** Ebenen



Sicherheitsmanagement

IT-Grundschutz

ISO 17799

Netzwerke

Verteilte Systeme
verteilte Applikationen
physikalische Sicherheit

lokale Applikationen
Softwarekomponenten
Hardwarekomponenten

IT-Grundschutz: Ziel

Ziel des IT-Grundschutzes:

Durch Anwendung von

- organisatorischen
- personellen
- infrastrukturellen
- technischen

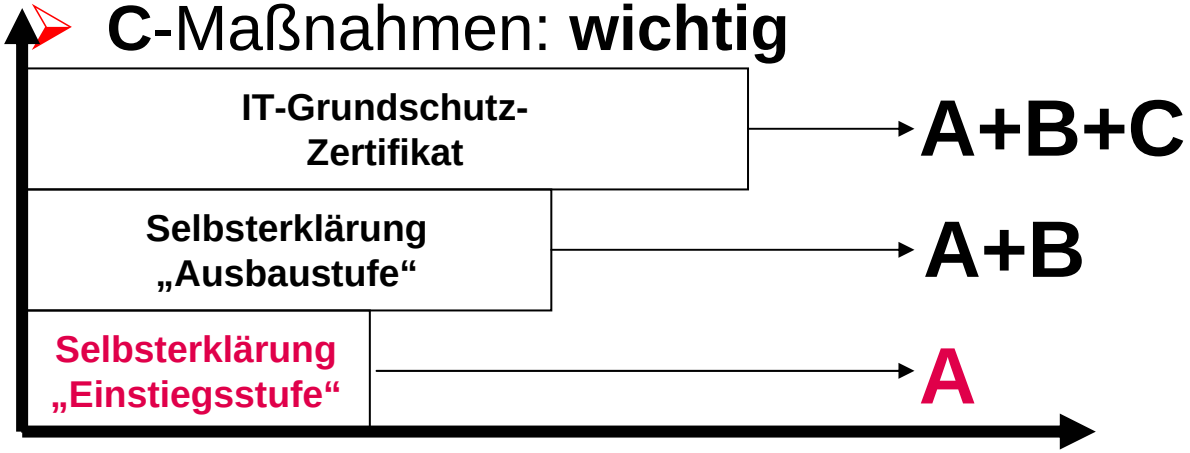
Standard-Sicherheitsmaßnahmen

ein **Sicherheitsniveau** zu erreichen, das

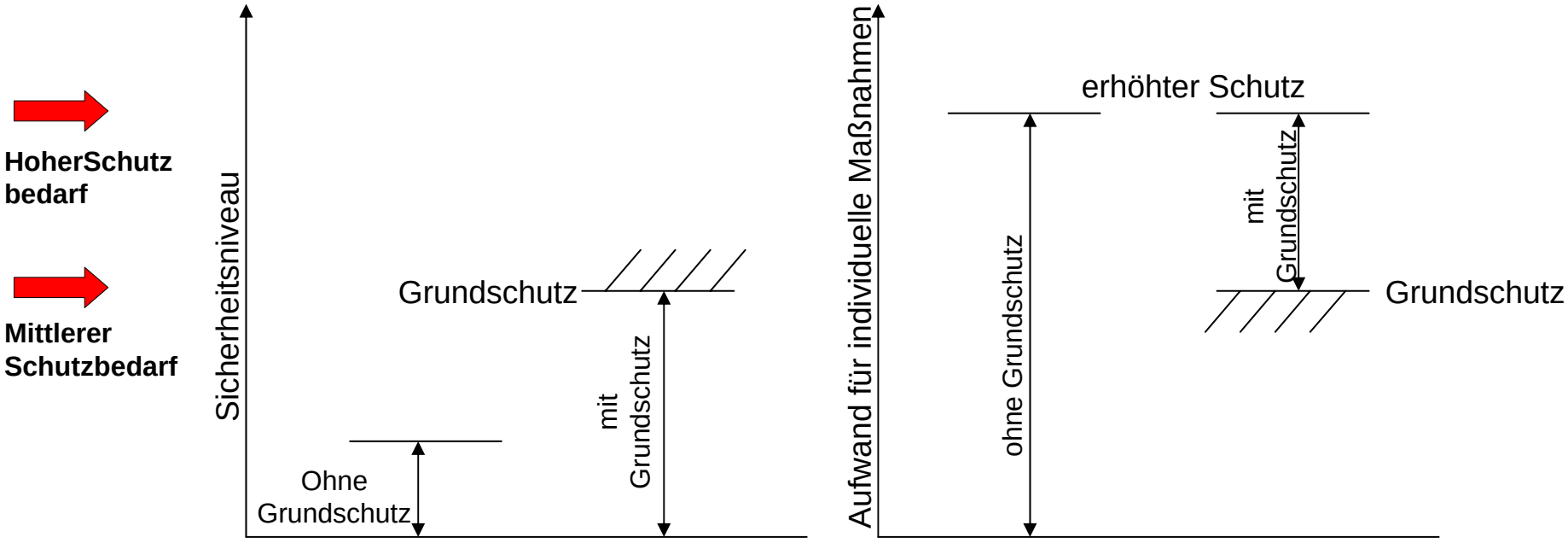
- **für den mittleren Schutzbedarf** angemessen und ausreichend ist und
- als **Basis** für hochschutzbedürftige IT-Anwendungen dienen kann

IT-Grundschutz: Zertifizierung

- **Vertrauen gegen Nachweis**
- stufenweise **erreichbar über die Erfüllung der drei Kategorien von ITGS-Maßnahmen:**
  - **A**-Maßnahmen: **unabdingbar**
  - **B**-Maßnahmen: **wesentlich**
  - **C**-Maßnahmen: **wichtig**

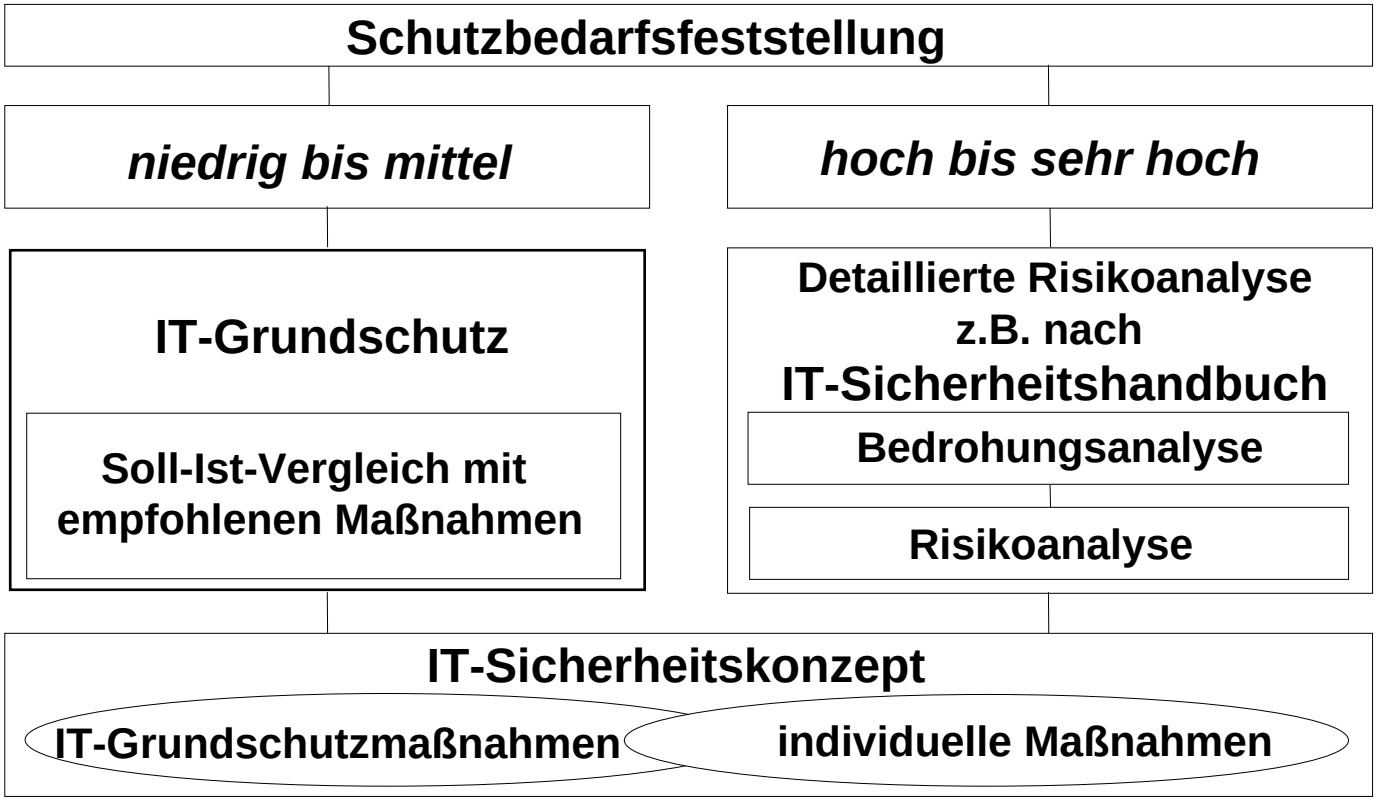


Erhöhung der IT-Sicherheit durch IT-Grundschutz (GSHB)



Grundschutz

IT-Sicherheitshandbuch



TÜViT Assessmentansatz

Wie kann man die strategische Herausforderung praktisch angehen?

Der

TÜViT Assessmentansatz

Assessmentansatz (1)
Ziele der Untersuchung

- Schwachstellen **in der IT-Sicherheit** schnell **und** effektiv aufdecken
- **erhebliche** Hindernisse **zur Realisierung eines auf Dauer gerichteten IT-Grundschutzes** frühzeitig erkennen
- Sicherheitsprobleme **im** Vorfeld **der Anwendung der IT-Grundschutzmethode erkennen und Vorschläge zur Behebung unterbreiten**
- Aufwand **für die** Realisierung **eines technischen, infrastrukturellen, organisatorischen und personellen Grundschutzes nach** BSI-Vorgabe **erheblich** reduzieren
- Weg **zur** IT-Grundschutz-Zertifizierung ebnen

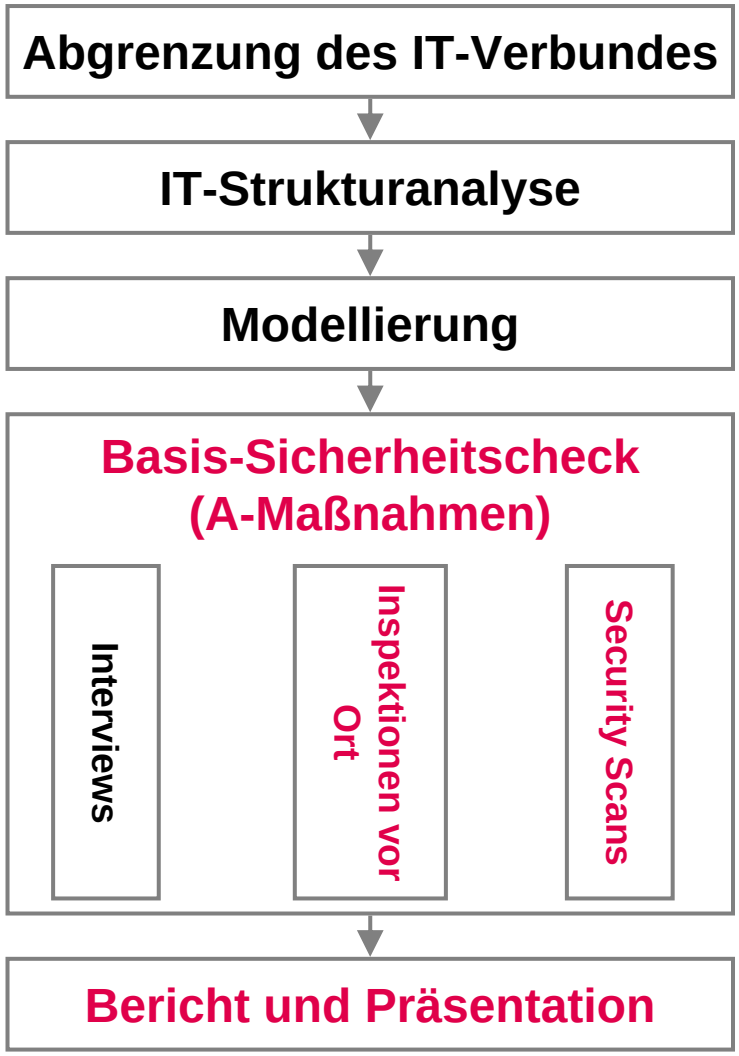
Assessmentansatz (2)
Umfeld der Untersuchung

- **Das Assessment konzentriert sich auf** sicherheitskritische Teilbereiche**:**
  - z.B. Serverfarm, Internetanbindung und/oder IT-Systeme, die zur Erbringung bestimmter Dienstleistungen kritisch sind
- **Der** Untersuchungsgegenstand
  - wird im Vorfeld des Assessments als **IT-Verbund** (d.h. als Untermenge der Informationstechnik einer Organisation, die betrachtet werden soll) abgegrenzt
  - ist **überschaubar**
  - ist im **Rahmen** des Assessments prüfbar

Assessmentansatz (3)
Gegenstand der Untersuchung

- **wichtige** Komponenten der eingesetzten Technik
  - Webserver- und Firewallkonfiguration
  - Verzeichnisdienste
  - Authentisierungs- und Berechtigungskonzept
  - Netzwerkkomponenten
  - Windows 2000 Server / Client,...
- **wichtige** Infrastrukturaspekte
  - Gebäude
  - Verkabelung
  - Rechenzentrum usw.
- **entscheidende** allgemeine Aspekte**:**
  - IT-Sicherheitsmanagement
  - Organisation
  - Personal
  - spezifische Sicherheitskonzepte usw.

Ablauf des Assessments (2)
Durchführung der Untersuchung



Festlegung des Untersuchungsgegenstandes

Erfassung der Information für das weitere Vorgehen

Ermittlung der relevanten Bausteine

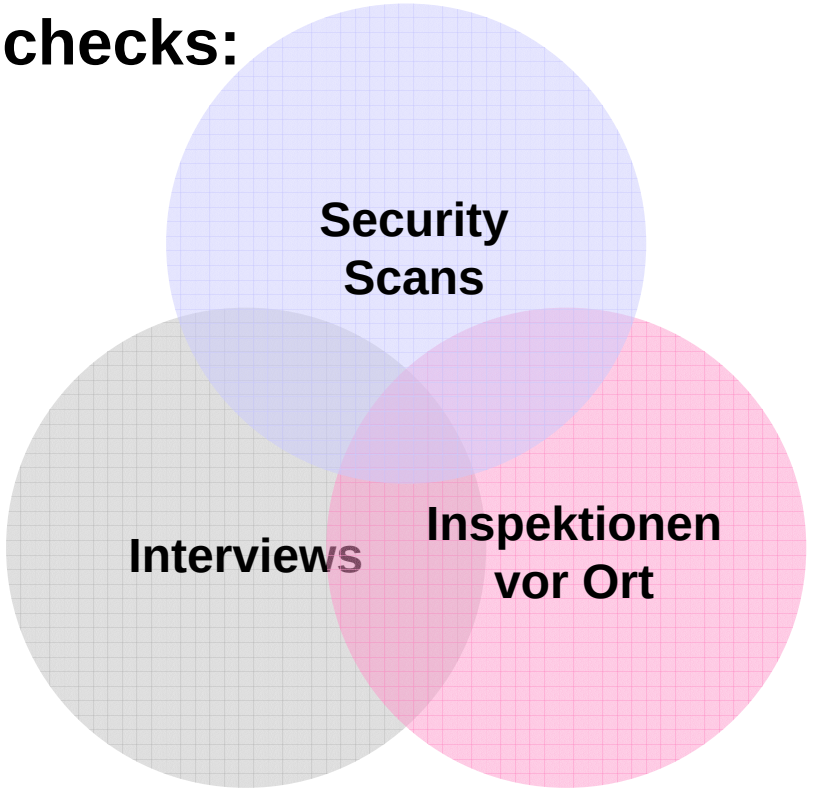
Soll-Ist Vergleich

Statistiken, Gefährdungen, technischen Schwachstellen, Maßnahmen-empfehlungen, weiteres Vorgehen

Sicherheitscheck (1)
Überblick

Typische Kombinationen von Techniken zur Durchführung von Sicherheitschecks:

Einsatzbeispiel
„klassische“ Auditierung



Einsatzbeispiel
TÜViT-Assessment

Sicherheitscheck (2)
Interviews

- Durchführung von **Interviews** (Fachgesprächen) über definierte Themen mit den jeweiligen Ansprechpartner der Institution:
  - Verantwortliche für IT-Sicherheit in leitenden Positionen (OE-Leiter)
  - Fachkräfte für die administrative und technische Umsetzung der IT-Sicherheitsmaßnahmen
  - Anwender der IT-Hard- und Software

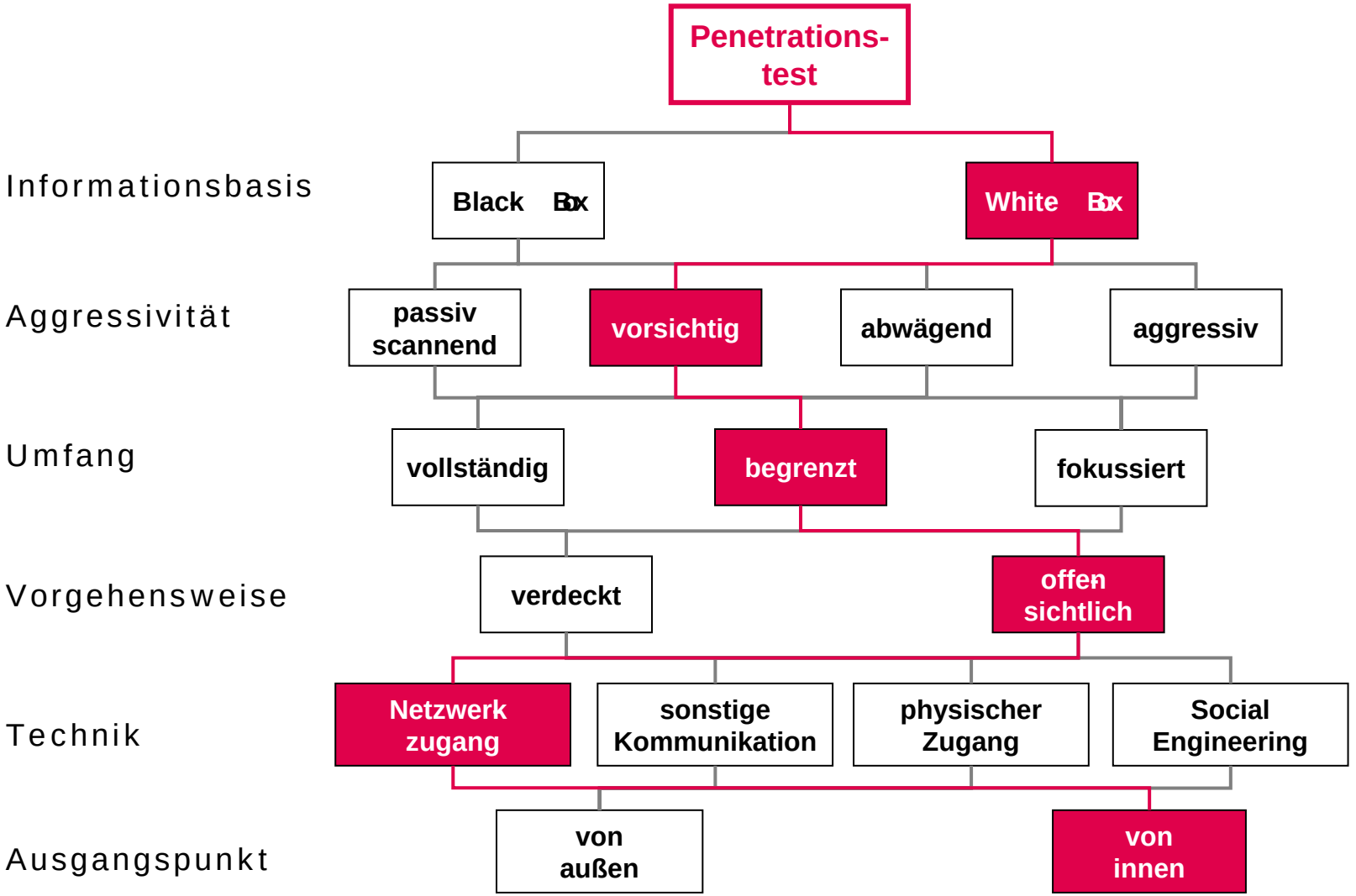
Sicherheitscheck (3)
Inspektionen

- **Inspektionen** von Gebäuden, IT- und Infrastruktur-Räumen
  - Stromversorgung, USV, Brandschutz, Gebäudeschutz, Klimatisierung, Gefahrenmeldeanlagen usw.
- **Konfigurationsanalysen** an IT-Systemen, in folgenden Fällen:
  - in Bereichen, die von den Security Scans nicht erfasst werden
  - wenn die Ergebnisse der Security Scans weitere Schwachstellen vermuten lassen
  - zur stichprobenartigen Verifikation der Ergebnisse der Security Scans
  - wenn die individuellen Gegebenheiten dies erfordern

Sicherheitscheck (4a)
Security Scans

- Durchführung von **automatisierten**
  - Portscans
  - Netzwerk-Schwachstellen-Scans
  - System-Schwachstellen-Scans
- Einschätzung der **tatsächlichen** Bedrohungslage
- Entwicklung von **Angriffszenarien**, die auf die potentiellen Risiken basieren
- Erbringung von **Nachweisen**, dass Schwachstellen durch als realistisch eingeschätzte Bedrohungen tatsächlich ausgenutzt werden könn(t)en

Sicherheitscheck (4b)
Security Scans



IT-Sicherheit als strategische Herausforderung

Die Gewährleistung der IT-Sicherheit stellt tatsächlich eine strategische Herausforderung dar, weil

1. **Weil sie für die Nutzung der IT von gravierender Bedeutung ist**
2. **Weil sie nicht einfach und trivial, sondern hoch komplex und heterogen ist**
3. **Weil sie Geld und Zeit kostet und Ressourcen braucht**
4. **Weil die negativen Folgen der Verletzung der IT-Sicherheit weit reichende Auswirkungen national und international haben kann**