

# IT-Sicherheit

## Methoden der Identitätsdiebstahl

- Phishing
- Vishing
- Pharming
- Spoofing
- Nicknapping

## Schadprogramme & Maleware

- Spam
- Spyware
- Adware
- Virus
- Trojaner
- Wurm
- Ransomware

## Andere Schädliche Dinge

- DDos
- Botnetzte
- APT-Angriffe
- Mining Software

## Maßnahmen gegen Phishing

- Virens Scanner aktuell halten
- Niemals TAN's und Kennwörter weitergeben
- Verdächtige Emails erkennen (Schlechte Rechtschreibung, Schlechtes Vornat)

## Maßnahmen gegen Ransomware

- Alle Netzwerkverbindungen Lösen
- Keine Anmeldung von Admin Accounts
- Backups einspielen oder System neuinstallieren

## Maßnahmen gegen DDos

- Gute Passwörter bei Netzwerkgeräten
- Deaktivieren von Universal Plug and Play
- Erstellen eines Honeypots

## BSI

Bundesamt für Sicherheit in der Informatik

# IT-Grundschutz

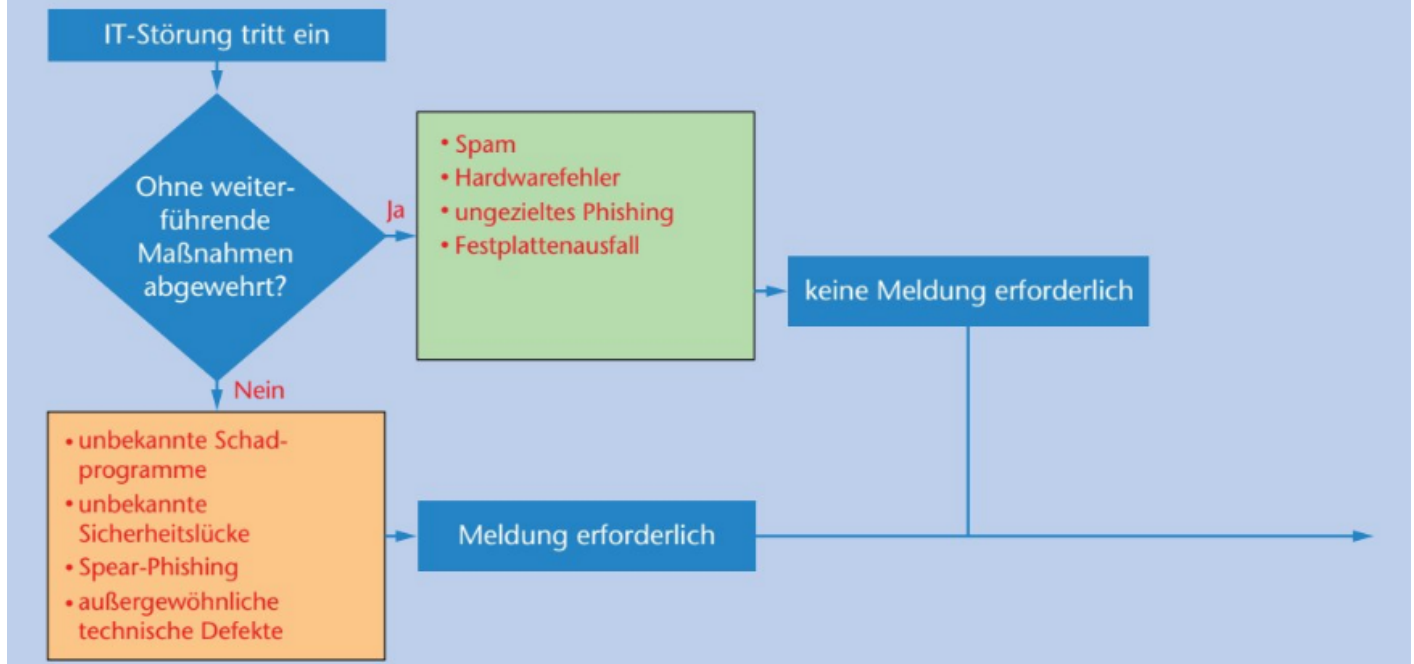


## Sektoren der Kritischen Infrastruktur

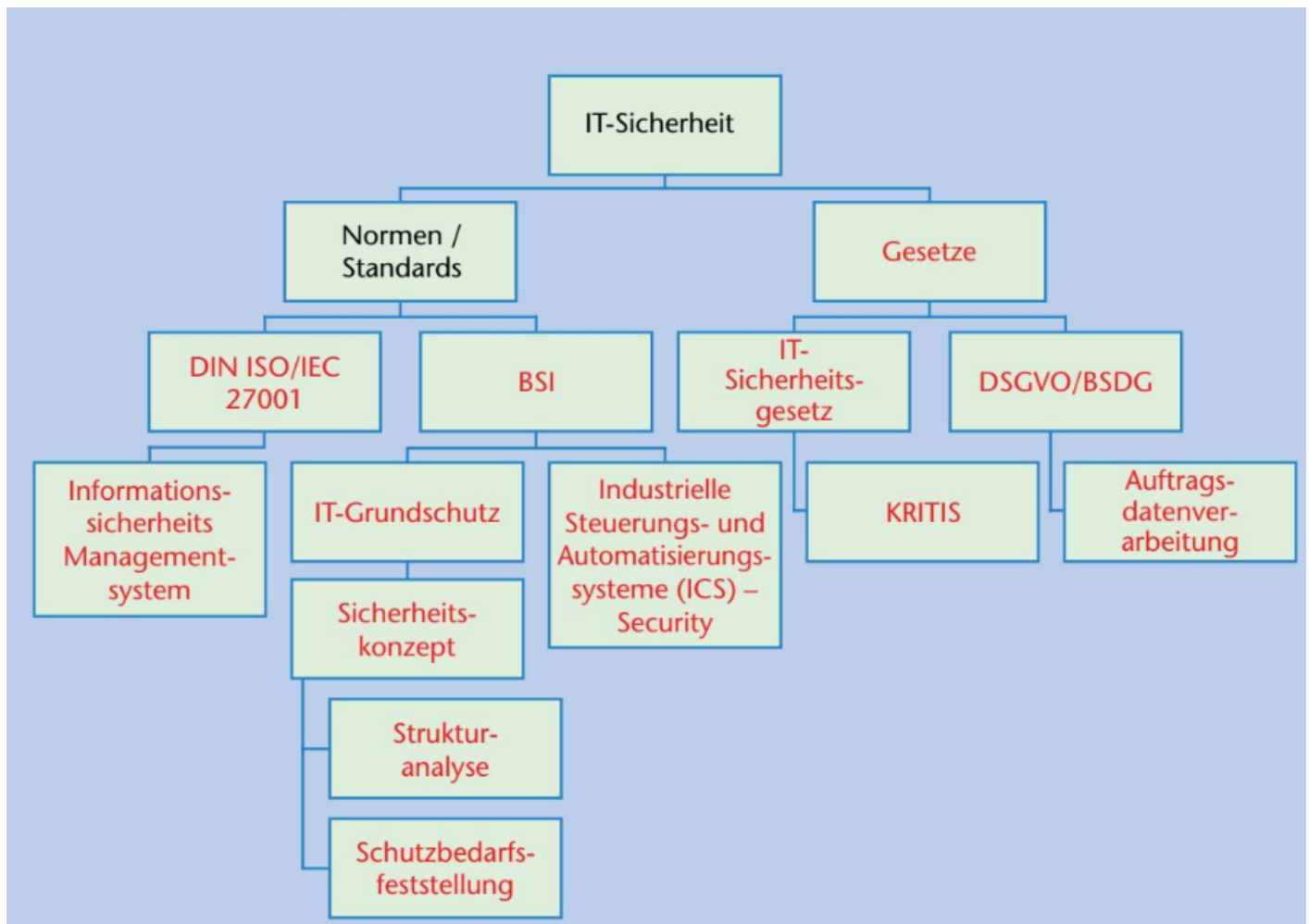
- Transport
- Finanz / Versicherungswesen
- Gesundheit
- IT / Telekommunikation
- Ernährung
- Wasser
- Energie

## Ablauf bei IT-Störungen

### Ablaufplan der Meldung einer IT-Störung:



## IT-Sicherheit Mindmap





# Verschlüsselung

## Symmetrische Verschlüsselung:

Der gleiche Schlüssel wird von beiden Seiten gleichzeitig zur Ver- und Entschlüsselung von Daten verwendet.

## Asymmetrische Verschlüsselung

Es wird ein Geheimer und Öffentlicher Schlüssel verwendet. Dabei wird der Öffentliche Schlüssel nur mit den zu kommunizierenden Personen gegeben.

# Verschlüsselungsverfahren

## Modern:

- AES
- Diffie Hellman
- Blowfish
- PGP

## Veraltet:

- DES
- Trippel DES
- RSA-OAEP