

1 Einführung in Grundbegriffe

IT-Compliance: IT Compliance beschreibt in der Unternehmensführung die Kenntnis und die Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft.

IT-Governance: Liegt der Verantwortung des Vorstands und des Managements und ist wesentlicher Bestandteil der Unternehmensführung. IT-Governance besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die IT die Unternehmenstrategie und Ziele unterstützt.

ISMS = Informationssicherheitsmanagementsystem: Beschreibt das allgemeine Sicherheitsmanagement speziell im Bereich der Informationssicherheit. ISMS ist ein komplexer Prozess der Steuerung von materiellen, konzeptionellen und menschlichen Ressourcen mit dem Ziel, den Anforderungen an die Aspekte -Auftragserfüllung, Vertraulichkeit, Integrität und Verfügbarkeit einer Organisation angemessen zu entsprechen.

Bedrohung: Ereignisse oder Begebenheiten aus denen ein Schaden entstehen kann.

Bedrohungskategorie
höhere Gewalt
elementare Bedrohung
technisches Versagen
vorsätzliches Handeln
menschliche Fehlentscheidung

Schwachstelle: Sicherheitsrelevanter Fehler eines IT-Systems oder eines Prozesses.

Schutzmaßnahmen: Maßnahmen um einen Zustand von Sicherheit zu erreichen oder zu verbessern.
nach BSI:

Infrastruktur: Verschlussene Türen + Videokameras

Hardware und Software: Firewall, Malwareschutz, IDS (Analysiert und schlägt Alarm wenn Angriff stattfindet) - IPS (leitet sogar noch Gegenmaßnahmen ein)

Organisation: Verantwortlichkeiten regeln, Nutzungsverbot nicht freigebender Hardware/Software

Kommunikation: Dokumentation der Verabelung, Regelmäßiger Sicherheitscheck der Netze, restriktive Rechtvergabe

Notfallvorsorge: Regelmäßige Datensicherung, TKA-Basisanschluss für Notrufe, Übersichert über Verfügbarkeitsanforderungen

Personal: Vertretungsregelung, Awarenessmaßnahmen, Einarbeitung von Mitarbeitern