IT-Grundschutz für große IT-Dienstleister

Schutzbedarf „NORMAL“

Zielgruppen:
- Einen erwirtschafteten Jahresumsatz von mindestens 50 Millionen Euro Brutto
- Einen Mitarbeiterstamm von mindestens 250 Mitarbeitern
- Eine Verteilung über mindestens 5 verschiedene Standorte

Zielsetzung:
- Ziel ist eine Basisabsicherung unter Realisierung der Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität im Rahmen eines stabilen und nachhaltigen Informationssicherheitsmanagement

ISMS.1 Sicherheitsmanagement

Prozessschicht

ORP.1 Organisation
ORP.2 Personal
ORP.3 Sensibilisierung und Schulung
ORP.4 Identitäts- und Berechtigungsmanagement
ORP.5 Compliance Management

CON.1 Kryptokonzept
CON.2 Datenschutz
CON.3 Datensicherungskonzept
CON.4 Auswahl und Einsatz von Standardsoftware
CON.5 Entwicklung und Einsatz von Fachanwendungen
CON.6 Löschen und Vernichten

OPS.1.1.2 Ordnungsgemäße IT-Administration
OPS.1.1.3 Patch- und Änderungsmanagement
OPS.1.1.4 Schutz vor Schadprogrammen
OPS.3.1 Outsourcing für Dienstleister

Systemschicht

INF.1 Allgemeines Gebäude
INF.2 Rechenzentrum sowie Serverraum
INF.3 Elektrotechnische Verkabelung
INF.4 IT-Verkabelung
INF.7 Büroarbeitsplatz

NET.1.1 Netzarchitektur und –design
NET.1.2 Netzmanagement
NET.3.1 Router und Switches
NET.3.2 Firewall
NET.3.3 VPN

DER

DER.1 Detektion von sicherheitsrelevanten Ereignissen
DER.2.1 Behandlung von Sicherheitsvorfällen
DER.4 Notfallmanagement

Prozessschicht

ORP.2 Personal
- Ziel: Mitarbeitende sollen verantwortungsbewusst mit Daten umgehen
- Gefahr: Sorglosigkeit und unzureichende Kenntnis über Regeln

CON.3 Datensicherungskonzept
- Ziel: Datensicherungskonzept für Institutionen, damit diese gegen Datenverlust gesichert sind
- Anmerkung: Es sollen automatische Prozesse sein
- Gefahr: Fehlende Tests/Dokumentation / Unzureichendes Datensicherungskonzept

OPS.1.1.4 Schutz vor Schadprogrammen
- Ziel: Effektives Schützen gegen Schadprogramme
- Gefahr: Social Engineering / Botnetze / Softwareschwachstellen

Systemschicht

INF.2 Rechenzentren sowie Serverraum
- Ziel: Gewährleisten des sicheren Betriebes eines Rechenzentrums
- Gefahr: Fehlende Überwachung / Zutrittskontrollen / Elementare Gefahren

NET.1.2 Netzmanagement
- Ziel: Etablieren der Informationssicherheit innerhalb des Netzmanagements
- Gefahr: Unberechtigter Zugriff auf Komponenten des Netzes / Eingriff in die Kommunikation des Netzmanagements

DER

DER.1 Detektion von sicherheitsrelevanten Ereignissen
- Ziel: Systematischer Weg, wie Informationen gesammelt, korreliert und ausgewertet werden können, um sicherheitsrelevante Ereignisse zeitnah zu detektieren
- Gefahr: Unzureichende Qualifikation und Missachtung der Vorschriften