IT-**Grundschutz** nach BSI 100-1/-4

Marko Rogge

www.marko-rogge.de
www.leiner-denzer.com

100-1, 100-2, 100-3, 100-4

- 100-1
  - Managementsysteme für Informationssicherheit (ISMS, Information Security Management System)
- 100-2
  - Vorgehensweise nach Grundschutz
- 100-3
  - Risikoanalyse nach Grundschutz
- 100-4
  - Notfallmanagement

100-1

Aufbau eines ISMS nach Grundschutz

100-1

- Definition der allgemeinen Anforderungen an ein ISMS
- Kompatibel zu ISO/IEC 27001
- Kompatibel mit Grundschutz nach BSI
- BSI stellt mit 100-1 einen eigenen Standard

ISMS

- Versteht sich als Schutz von Daten in jeder Herkunft und Form, ob Papier oder elektronisch. (Notizen, Gedanken, E-Mails)

- Basis ist hierbei:
  - Verfügbarkeit, Integrität, Vertraulichkeit
  - Authentizität, Verbindlichkeit, Zuverlässigkeit

- Informationssicherheit vs. IT-Sicherheit

Bedrohungen

- Bedrohungen für Informationssicherheit
  - Schadcode: Viren, Trojaner, Rootkits …
  - Geheimdienste, Wettbewerb, Mitarbeiter …
  - Feuer, Wasser, Strom
  - Diebstahl, Beschädigung

Bedrohungen

- Durch Menschen initiiert:
  - Beeinträchtigungen technisch
    - Mutwillig, unwissentlich
  - Wirtschaftsspionage – gezielt
  - Know-How Abfluss – neuer Arbeitgeber
  - Korruption
  - Geheimnissverrat

ISMS Standard

- ISO/IEC 2700x
  - Internationale Organisation für Standards
  - Internationales Elektronische Kommission
- Zusammenführung:
  - z.B. ISO 17799:2005 wurde ISO/IEC 27002 (Das Rahmenwerk für ein Informationssicherheitsmanagement)

Vorgehensweise nach Grundschutz BSI

Grundschutz: Vorgehensweise

- Schritt für Schritt die Umsetzung von ISMS
- Aufbau und Betrieb von ISMS / 2700x
- Aufbau des ISMS und die Struktur
- Aufgaben des ISMS

- Verinice - Sercon

ISMS

- Definition des ISMS – steuern & lenken
- Ressourcen, Management, Mitarbeiter, Prozesse
  - Erstellung eines Sicherheitskonzeptes
  - Organisation
  - Ziele und Strategien

Prozesse

- Veränderlicher Prozess
  - Daher Lebenszyklen definieren
  - Notwendig für die Umsetzung:
    - Planung
    - Beschaffung (kaufm.)
    - Betrieb
    - Notfallvorsorge
    - Aussonderung

Beschreibung der Prozesse

- Planung
- Umsetzung der Planung, Durchführung
- Kontrolle und Überwachung
- Schwachstellen beseitigen
  - Verbessern
  - Beseitigen

- PDCA: Plan – Do – Check – Act
  (Grundsatz - Einsatz)

Management

- Verantwortung
- Integration der Informationssicherheit
- Steuern – aufrechterhalten
- Ziele setzen, Ziele verfolgen
- Kosten – Nutzen
- Vorbildfunktion – Vorleben
- Kommunikation

Planung und Ressourcen

- Geltungsbereich definieren, planen
- Datenschutz, Anforderungen, Ziele des ISMS
- Anforderungen von Kunden
- Risikomanagement / Krisenmanagement berücksichtigen
- Mitarbeiter

Kontrolle

- Kontrolle über Erfolg
- Veränderungen der Prozesse
- Ziele noch angemessen?
- Leitlinien und Strategien angemessen?
- Konzept noch zur Zielsetzung angemessen?
- Verbindung von Aufwand und Kosten

Risikobewertung

- Bewertung von Schäden
- Bewertung von Bedrohungen
- Erstellen von Wertigkeiten
- Risikobewertung nach ISO 27005
- Betrachtung von Organisation, Branche, Anforderungen, Sicherheitsniveau
  - Risiko berechnet sich aus der Schadenshöhe multipliziert mit der Eintrittswahrscheinlichkeit

Risikobewertung

- Aufwendig
- Kostenintensiv
- Individuell
- Wahrscheinlichkeiten abwägen
- Schutzbedarfsermittlung
- Klassifizieren, orientieren
  - Bekannte Vorfälle?
  - Verstöße gegen Gesetze?
  - Finanzielle Auswirkungen?
  - Wirkung innen und außen?

Grundschutz & Maßnahmen

- Bausteine (B)
- Maßnahmen (M)

- Kombination und Anpassung aus den Vorgehensweisen 100-1/4
- Anpassung an ISO 2700x

Notfallmanagement

- Begriffsdefinitionen:
  - Störung
  - Notfall
  - Krise
  - Katastrophe
- Krisenmanagement

Störung

- Leichte Beeinträchtigung
- Kaum messbarer Schaden
- Kein Ausfall

- Wird im Tagesablauf beseitigt

Notfall

- Beeinträchtigung der Geschäftsprozesse
- Zeitnahe Behebung nicht möglich

  (nach Anforderungen)
- Hohe Schäden sind zu erwarten

- Notfallbehebung nur durch Organisation möglich

Katastrophe

- Großereignis
- Auswirkungen weder örtlich noch zeitlich begrenzt; Menschen, Sachwerte, Produktion
- Gefährdungen für Leben von Menschen
- Gefährdung des Unternehmens gänzlich

- Katastrophenschutz

Krise

- Abweichend eintretend, trotz Maßnahmen
- Ablauf kann nicht eingehalten werden
- Einmaligkeit einer Krise
- Ereignisse gehen voran
- Eskalation möglich
- Starke Beeinträchtigung

Krisen

- Finanzkrisen
- Erpressungen
- Bombendrohungen
- Entführungen
- Know-How Abfluss
  - ...

Krisenmanagement

- Systematisches Vorgehen
- Koordinierte Abläufe
- Krisenstab
- Kommunikation
- Gegenmaßnahmen

- Krisenmanagement gesondert behandeln
- Erstellung eines Krisenplanes

Notfallmanagement

- Umsetzung nach BCM nach BS 25999-1/2

  (Business Continuity Management)

  - Verstehen der Organisation
  - Entwicklung von Plänen
  - Implementieren von Reaktionsmaßnahmen
  - Übungen, Überprüfungen
  - ...

Notfallmanagement

- Weitere Standards:
  - GPG Good Practice Guidlines
  - PAS77 Public Available Specification
  - NIST SP 800-34 National Institute of Standards and Technology
  - ITIL IT Infrastructure Libary
  - ISO 20000 – IT Service Management
  - ISO 27001/27002

Notfallmanagement - Ablauf

- Initiieren eines Notfallmanagement
- Konzeption
- Umsetzung des Konzept
- Notfallbewältigung
- Übung – Test
- Überprüfung und Verbesserung der Prozesse

- Dokumentation

Fragen?

Danke für die Aufmerksamkeit!