2024-07-08#IT-SEC

Dozent:

IT-SEC

Datenschutz oder Datensicherheit

Datenschutz und Datensicherheit

Was ist Datenschutz?

- Schutz vor der missbräuchlichen Verarbeitung personenbezogener Daten
- Schutz des Rechts auf informationelle Selbstbestimmung.
- durch die Datenschutz-Grundverordnung (DSGVO), Bundesdatenschutzgesetz (BDSG) sowie der Landesdatenschutzgesetzte (LDSG) geregelt
- Für die rechtmäßige Verarbeitung personenbezogener Daten ist eine Rechtsgrundlage gemäß DSGVO oder eine Einwilligungserklärung der betroffenen Personen notwendig.
- **Leitfrage Datenschutz:**
  Darf ich diese personenbezogenen Daten erheben und verarbeiten?
- Verstöße gegen den Datenschutz werden mit Bußgeldern von bis zu 20 Mio. EUR oder 4 % des weltweiten Jahresumsatzes der verantwortlichen Stelle bestraft. Auch eine Freiheitsstrafe von bis zu 3 Jahren ist möglich.

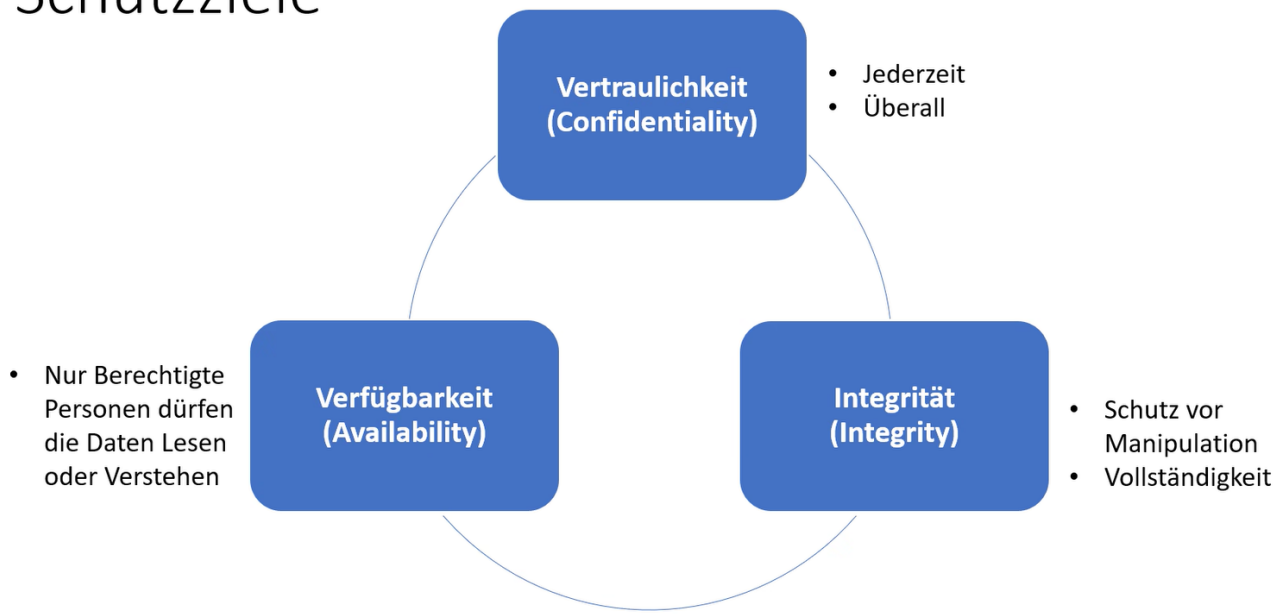
Was ist Datensicherheit

- Schutz sämtlicher Daten, egal ob Personenbezogen oder nicht
- Datensicherheit bezieht alle Formen von Daten/Informationen ein, egal ob analog, digital oder in denn Köpfen der Menschen
- durch das Handelsgesetzbuch (HGB), IT-Sicherheitsgesetz nach BSI-Gesetz, Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) aber auch Strafgesetzbuch (StGB) und Gesetz gegen unlauteren Wettbewerb (UWG) geregelt
- **Leitfrage Datensicherheit:**
  Wie schütze ich Daten vor einem Zugriff durch Unbefugte?
- Unternehmen- /Wirtschaftsspionage werden mit Bußgeldern von bis zu 300.000 EUR bestraft. Auch eine Freiheitsstrafe von bis zu 5 Jahren ist möglich.

Schutz -Ziele

- Ziele liegen Hand-In-Hand

IT/Informations-Sicherheit
Schutzziele



Datensicherheit

Vertraulichkeit

- Jederzeit
- Überall

Integrität

- Schutz vor Manipulation
- Vollständigkeit

Verfügbarkeit

- Nur Berechtigte Personen dürfen die Daten Lesen oder Verstehen

Informationssicherheit gefährdet durch

- Höhere Gewalt
  - Feuer
  - Wasser
  - Blitzschlag
  - Krankheit
- Organisatorische Mängel
  - Fehlende Konzepte
  - Fehlende Unklare Regelungen
- Menschliche Fehlhandlung

    - Öffnen oder Weiterleiten von Spam-Mails
    - Weitertragen von Firmen Interna "PW Erneuerung usw."
    - Weitergabe von Daten über unsichere Medien
- Technisches Versagen
    - Falsch konfigurierte Software
    - nicht konfigurierte Schutzmechanismen wie Firewall oder USV
    - keine Segmentierung des LAN
- Vorsätzliche Handlungen
    - Hacker
    - Viren
    - Trojaner

IT Grundschutz Kompendium

- stellt eine Zusammenfassung von Gefährdungen und
- Prozess Bausteinen in 900 Seiten zusammen

ISMS

Bedeutung ISMS

Ein Information Security Management System (ISMS) ist ein **Managementsystem**,

- das Regeln,
- Verfahren,
- Maßnahmen und
- Tools definiert,

um die Informationssicherheit in einem Unternehmen sicherstellen, steuern, kontrollieren und kontinuierlich verbessern zu lassen. Durch die IT verursachte Risiken sollen identifizierbar und beherrschbar werden.

Ein ISMS gibt Unternehmen Klarheit über die wichtigen Assets und dient als Notfallfahrplan für den Ernstfall. Es ist ein systematisches und strukturiertes Framework zur Verwaltung von Informationen und Werten, das dazu dient, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Durch die Implementierung eines ISMS können Unternehmen die Gefahren und Risiken für ihre Daten und Systeme besser erkennen und minimieren, um die Verfügbarkeit, Vertraulichkeit und Integrität ihrer Daten zu gewährleisten.

8 Phasenmodell

“Pasted image 20240708103235.png” could not be found.

Iso Cert Referenz

- ISO/IEC 27001:2013

“Pasted image 20240708110426.png” could not be found.