IT-Sicherheit: Einführung

Themenplan

Verschlüsselung / Kryptographie

- Wie kann sichergestellt werden, dass Vertrauliches vertraulich bleibt?

Signaturen und Zertifikate

- Gewährleisten, dass Daten nicht manipuliert wurden und die Quelle echt ist

Backup, USV etc.

- Sicherstellen, dass Daten und Ressourcen zuverlässig zur Verfügung stehen

Zugangskontrolle

- Den unbefugten Zugang zu Räumen / Zugriff auf Daten unterbinden

Angriffsszenarien & Schutzmaßnahmen

- Typische Angriffe und wie man sich davor schützt

Datenschutz

- Welche Auswirkungen hat die DSGVO, worauf muss man achten?

Sonstiges

- Cloud, Tracking im Internet, E-Mail-Sicherheit, Social Media, Blockchain …

Grundbegriffe

Datensicherheit

- Schutz *aller* Daten vor Verlust, Manipulation, Ausspähen. Liegt im Ermessen des Einzelnen

Datenschutz

- Schutz *personenbezogener* Daten vor Verlust, Manipulation, Ausspähen. Gesetzliche Vorschrift: „Recht auf informationelle Selbstbestimmung“; DSGVO

Datensicherung

- Regelmäßige Sicherung wichtiger / relevanter / aller Daten

Risiken *ohne* menschliches Eingreifen

Schäden, die auftreten können, ohne dass sie absichtlich oder versehentlich ausgelöst werden, z.B.:

- Defekte Hardware
- Fehler in der Software (Bugs)
- Stromausfall
- Feuer- / Brandschäden
- Wasserschäden
- Naturkatastrophen

Risiken *mit* menschlichem Eingreifen

Schäden, die versehentlich oder absichtlich herbeigeführt werden, durch, z.B.:

Unachtsamkeit, Fahrlässigkeit, fehlendes Problembewusstsein

- Fehlerhafte Eingaben, ungeschützte Systeme, einsehbare Passwörter, „Stecker ziehen“, versehentliches Löschen/Überschreiben, Öffnen von Mail-Anhängen, Benutzung ungesicherter Geräte, offenes Speichern sensibler Daten …

Gezielte Angriffe

- Angriff auf Server & Systeme, Schadsoftware, Diebstahl, Sabotage …

Fehler in der Organisation

- Keine Ablaufpläne für einen Schadensfall, keine Kontrolle, fehlende Verantwortlichkeiten …

Sicherheit ist kein Zustand

IT-Sicherheit ist ein dynamischer *Prozess*, kein einmal erreichter Zustand, bei dem man verharren kann

IT-Sicherheit ist auch immer ein Kompromiss:

- Sicherheitsmaßnahmen
- Bedienbarkeit
- Akzeptanz
- Kosten

VIVA – Die Schutzziele

Vertraulichkeit

- Schutz der Daten & Ressourcen vor unbefugtem Zugriff

Integrität

- Schutz der Daten vor Manipulation (nicht zuverlässig realisierbar, aber man kann Manipulationen erkennen)

Verfügbarkeit

- Sicherstellen, dass Daten & Ressourcen zuverlässig zur Verfügung stehen

Authentizität

- Sicherstellen, dass die Quelle der Daten verifizierbar ist (Daten müssen „echt“, „authentisch“ sein)

Weitere mögliche Schutzziele sind z.B. Nichtabstreitbarkeit, Verlässlichkeit, Anonymität …

VIVA – Die Maßnahmen

Vertraulichkeit

- Verschlüsselung, Zugangskontrollen

Integrität

- Digitale Signaturen lassen erkennen, ob die Daten manipuliert wurden

Verfügbarkeit

- Backup, Wartung, USV, NSV, RAID, Brandschutz ...

Authentizität

- Digitale Zertifikate

CIA – Die Schutzziele

Im angelsächsischen Sprachraum ist für die Schutzziele das Kürzel **CIA** üblich

Das Kürzel steht für:

- **C**onfidentiality: Vertraulichkeit
- **I**ntegrity: Integrität
- **A**vailability: Verfügbarkeit

Das Schutzziel **Authentizität** wird nicht explizit aufgeführt

Grund: Die Maßnahmen (*Digitale Signaturen* und *Digitale Zertifikate*) sind technisch praktisch identisch, Authentizität wird hier als Sonderfall der Integrität behandelt

Die Konzentration auf drei (statt vier) Schutzziele findet sich auch in manchen deutschen Texten, hier wird Authentizität dann als erweitertes Schutzziel definiert