1 Vorlesung

1.1 IT-System

1.1.1 IT-System

technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen

1.1.2 Information

wird durch Daten repräsentiert und ergibt sich durch eine festgelegte Interpretation der Daten

1.1.3 Objekte

- **passive** Objekte (z.B. Dateien): Fähigkeit zur **Speicherung** von Information
- **aktive** Objekte (z.B. Prozesse): Fähigkeit zur **Speicherung und Verarbeitung** von Informationen
- **Assets**: Informationen und Objekte, die repräsentiert, sind die schützenswerten Güter (asset) eines Systems

1.1.4 Subjekte

Benutzer oder aktive Objekte, die im Auftrag von Benutzern aktiv sind (z.B. Prozesse, Server, Prozeduren)

1.1.5 Zugriffe

Interaktionen zwischen einem Subjekt und einem Objekt durch die Informationsfluss auftritt

- Zugriff auf Datenobjekt ist gleichzeitig Zugriff auf die dadurch repräsentierte Information

1.2 Sicherheit

1.2.1 Funktionssicherheit (engl. safety)

- Ist-Funktionalität == Soll-Funktionalität
- Das System funktioniert unter allen (normalen) Betriebsbedingungen
- z.B. technische Fehlverhalten des Systems durch Programmierfehler ⇒ Programmvalidierung oder -verifikation können es lösen

1.2.2 Informationssicherheit (security)

Informationssicherheit ist gegeben, wenn "ein funktionssicheres System nur solche Systemzustände annimmt, die zu keiner **unautorisierten Informationsverändeurng oder -gewinnung** führen"

1.2.3 Datensicherheit

- Datensicherheit ist gegeben, wenn "ein funktionssicheres System nur solche Systemzustände annimmt, die zu keinem **unatuorisierten Zugriff** auf Systemressourcen und insbesondere auf Daten führen"
- Umfasst Datensicherung (backup): "Schutz vor Datenverlust durch Erstellung von Sicherungskopien"

1.2.4 Privatheit, Datenschutz

natürliche Person kontrolliert Erhebung und Verarbeitung ihrer persönlichen Daten

- Informationelle Selbstbestimmung

1.2.5 Verlässlichkeit

Funktionssicherheit + Funktion wird zuverlässig erbracht

1.3 Schutzziele

Welche Funktionen können wir implementieren, um ein informationssicheres bzw. datensicheres System zu haben?

- Identifikation und Verifikation der Identität der zugreifenden Subjekte
- Zugriffseinschränkung und -kontrolle
- Zuordung von Aktionen und Zugriffen zu zugreifenden Subjekten

1.4 Authentizität

1.4.1 Authentizität

- "Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand einer **eindeutigen Identität und charakteristischen Eigenschaft** überprüfbar ist"

1.4.2 Authentifikationen

- **Nachweis**, dass eine behauptete Identität eines Objekts bzw Subjekts mit dessen charakterisierenden Eigenschaften übereinstimmt
- z.B Benutzererkennungen, Benutzernamen mit Passwörtern, biometrische Merkmale als Eigenschaften

1.5 Datenintegrität

1.5.1 Datenintegrität

ist "[...] ist gewährleistet, wenn es Subjekten nicht möglich ist, die zu schützenden Daten **unautorisiert und unbemerkt** zu manipulieren"

- Unautorisiert ⇒ **Rechtefestlegung** z.B. Lese- oder Schreiberechtigungen für Dateien
- Unbemerkt ⇒ **Manipulationserkennung**. Manipulationen sind nicht vermeidbar, aber müssen erkannt werden (z.B. Hashfunktionen)

1.6 Vertraulichkeit

"[ist] gewährleistet, wenn [...] **keine unautorisierte Informationsgewinnung** [möglich ist]"

- Unautorisiert ⇒ **Berichtigungen, Zugriffsrechte, und Kontrolle**
- Unautorisiert ⇒ **Verschlüsselung**

1.7 Verfügbarkeit

- .[ist] gewährleistet, wenn **authentifizierte und autorisierte** Subjekte in der Wahrnehmung ihrer Berechtigungen **nicht** unautorisiert **beeinträchtigt** werden können"
- d.h. "Normale" Nutzer verfügen unter normalen Bedingungen über die Ressourcen des Systems
- z.B. Einführung von Quoten für CPU-Zeit oder Speicher

1.8 Verbindlichkeit

1.8.1 Verbindlichkeit bzw. Zuordbarkeit

- "[ist] gewährleistet, wenn es nicht möglich ist, dass ein Subjekt im Nachhinein die **Durchführung einer solchen Aktion abstreiten** kann"
- D.h. Die Aktionen eines Nutzers können zu seiner Person zugeordnet werden
- z.B. **Digitale Signaturen**

1.9 Inhärente Zielkonflikte

Um die **Vertraulichkeit** von Informationen zu schützen kann die Löschung der Information (Selbstzerstörung) angebracht sein ⇒ Verlust der **Verfügbarkeit**
Um die **Verfügbarkeit** von Informationen zu schützen, können Backup-Kopien von vertraulichen Informationen (z.B. Passwörter PINS) angebracht sein ⇒ Erhöhtes Risiko des Verlusts der **Vertraulichkeit**