1 Einführung in Begrifflichkeiten

1.1 Daten und Information

- **Defintion Information :** Information besitzt für den Empfänger einen Neugkeitsgehalt und kann unterschiedlich übertragen werden
- **Daten** Repräsentieren Informationen (Bytefolge, Netzwerkpaket) ⇒ Interpretation ergibt die Information

1.2 Sicherheit

- **Definition Sicherheit:** Zustand oder subjektiver Eindruck frei von Gefahr
- **Definition Informationssicherheit:** Schutz der Information unabhängig von der Repräsentation
- **IT-Sicherheit:** Schutz
- **Zwei Formen der Sicherheit:** security (Angriff), safety(Betrieb)

1.3 Kommunikationskanäle

- **Kommunikation:** Nachrichtenaustausch zwischen mindestens zwei Partnern oder Gegenstellen
- **Kommunikationskanal:** Notwendig für den Informationsfluss zwischen Sender und Empfänger
- **Legitime Kanäle:** Vorgesehen für den Informationsaustausch z.B Sprache über Telefon
- **Verdeckte Kanäle:** Kanal der absichtlich aber unabsichtlich zur Kommunikation missbraucht wird. Z.B. versteckte Botschaften in Bildern (Stenographie)

1.4 Bedrohung

- **Gefährdungsfaktoren nach BSI := Bundesamt für Sicherheit in der Informationstechnik:** Höhere Gewalt, Vorsätzliche Handlung, Technische Fehler, Fahrlässigkeit, Organisatorische Mängel
- **Verwundbarkeit:** Schwachstelle beziehungsweise eine Sicherheitslücke des Systems, mittels derer die vorhandenen Sicherheitsmechanismen umgangen oder getäuscht werden können.
- **Bedrohung:** Ereignis aus dem Schaden entstehen kann.

1.5 Angriff

- **Angriff:** bezeichnet einen nicht autorisierten Zugriff(sversuch) auf ein It-Sytem oder Information.
- **aktiver Angriff:** nicht autorisierte Informationsveränderung, richtet sich typischerweise gegen die Integrität oder Verfügbarkeit des Systems
- **passiver Angriff:** nicht autorisierten Informationsgewinne: zuschauen, mithören, aufzeichnen

1.6 Risiko

- **Risiko** Risiko = Eintrittswahrscheinlichkeit * Schadenshöhe

1.7 Schutzziele

- **Schutzziel** Ziel der Sicherheitsmaßnahmen, um ein System gegen bestimmte Angriffe zu schützen
- **Vertraulichkeit** Informationen nur für diejenigen Personen oder Ressourcen zugänglich sind, welche für einen Zugriff berechtigt sind (Zugriffskontrolle, Verbergen der Information(Stenographie), Verschlüsselung)
- **Integrität** Unversertheit der Daten (Zugriffskontrolle, elektronische Signatur)
- **Authentizität** Authentizität bedeutet, dass der Urheber einer Information bekannt ist (Authentizitätsverfahren)
- **Zurechenbarkeit** beschreibt die Eigenschaft, dass es nicht möglich ist, eine Aktion gegenüber unbeteiligten Dritten abzustreiten. (Sicherstellen über Integrität und Authentizität)
- **Verfügbarkeit** bedeute das es autorisierten Subjekt möglich ist, die Funktionalität der Ressource zu nutzen, wenn diese benötigt wird (Sicherstellen durch reduntante Systeme)

1.8 Anonymisierung und Pseudonymisierung

- **Anonymität**beschreibt die Eigenschaft, dass es nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, die Identität eines Subjekts zu bestimmen. (Stärker als Pseudonymisierung)(nur möglich bei großer Menge Individuen)
- **Pseudonymität** hingegen versteht man das Verändern einer Identität anhand einer Zuordnungsvorschrift, die die echte Identität auf ein zugehöriges Pseudonym abbildet. Kommunikationspartner sehen nur das Pseudonym.

1.9 Zussammenfassung

Schutzziel	**Maßnahme**
Vertraulichkeit	Zugriffskontrolle, Verschlüsselung
Integrität	Zugriffskontrolle, elektronische Signatur
Authentizität	Zugangskontrolle, elektronische Signatur
Zurechenbarkeit	Zugangskontrolle, elektronische Signatur, Audit Trail/Log
Verfügbarkeit	Maßnahmen der Netzwerksicherheit
Anonymisierung, Pseudonymisierung	Proxies samt Verschlüsselung

Proxies weil sie andere IP zur Verfügung stellen - deswegen gut für Pseudonymisierung geeignet