IX. Netzwerksicherheit

IX.1. CIA-Paradigma

- Confidentiality
- Integrity
- Availability

(das ist noch keine vollständige Spezifikation, aber ein „Template“)

IX.2. Sicherheitsbegriff

- Vertraulichkeit
- Integrität
- Data origin authentification
- Peer entity authentification
- Non repudiation (Nichtabstreitbarkeit)
  - proof of origin
  - proof of delivery/submission
  - proof of receipt

IX.3. Das ISO/OSI-Referenzmodell

7 Anwendungsschicht
6 Präsentationsschicht
5 Sitzungsschicht
4 Transportschicht
3 Netzwerkschicht
2 Verbindungsschicht
1 Physikalische Schicht

Sicherheitseigenschaften sollen/können durch darunterliegende Schichten nicht gefährdet werden. (Ausnahme: Anonymität)

IX.4. IPsec

Protokollsuite, die Authentifikation und Verschlüsselung von IP-Paketen sowie entity authentification und key exchange erlaubt (bringt Sicherheit schon auf Ebene 3).

Schneier, Ferguson: „IPsec was a great disappointment to us.“

Im Wesentlichen: zu komplex.

IX.5. Bedrohungen für Rechner in Netzwerken

(Liste nicht vollständig)

- Belauschen, Unterdrücken, Verfälschen von Daten
- Portscan (automatisches Scannen von Schwachstellen)
- Fingerprinting (z.B. Ermitteln der OS-Version)
- Angriffe auf das Routing
- Schwachstellen in anderen Protokollen (z.B. DNS)
- Denial-of-Service-Attacken (DoS)
- Angriffe von innen
- Viren, Würmer, Trojaner
- Backdoors

IX.6. Schutzmaßnahmen

IX.6.1. Firewalls

- Paketfilter (Aussortieren nach Adressen/Diensten)
- Stateful Inspection (berücksichtigt zusätzliche Verbindungsinformationen)

FIXME: Bilder Firewall, S. 34

Firewalls sind eine Präventivmaßnahme, die ergänzt werden sollten durch Monitoring.

IX.6.2. Monitoring

Intrusion Detection Systems

IX.6.3. Honeypots

IX.6.4. Datendiode

Datenversand nur in eine Richtung möglich

FIXME: Bild Datendiode, S. 35