II. Einleitung

II.1. Was ist Sicherheit?

Was soll geschützt werden?

- Geheimnisse
- Daten/Wissen
- Dienste/Ressourcen/Infrastruktur
- Kommunikation
- Ansehen
- Rechte (informelle Selbstbestimmung)/Souveränität
- Hardware, Maschinen, (Versorgungs)Anlagen
- Vermögen, Besitz
- Urheberschaft/-recht
- Gesundheit/Leben

Vor wem?

- einzelne (Gelegenheits)Kriminelle
- Laien/"Kinder", unerfahrene Benutzer
- Spionage, Geheimdienste
- organisierte Kriminalität
- Saboteure
- interessengesteuerte, nicht-böswilligeÖrganisationen (Staat, Firmen)
- interne Angreifer (Bekannte, Verwandte, Mitarbeiter)
- Trojaner
- Vandalismus (Skript-Kiddies)
- private Feinde/Konkurrenten

Wie?

- Obscurity, Steganographie
- Kryptographie (Verschlüsselung, Signaturen)
- physikalische Sicherheit (Bunker, Tresor)
- Security Awareness (Mitarbeiterschulung)
- Policies, vorgeschriebene Abläufe
- Honey Pots, Intrusion Detection

ganzheitliche Sicherheit (Vermeidung von Schwachstellen):

- Angriffe auf Algorithmenebene (Verschlüsselung brechen, Signatur fälschen)
- Angriffe auf Protokollebene (z.B. Replay-, Man-in-the-Middle-Attacken)
- Angriffe auf Implementierungsebene (z.B. Bugs ausnutzen, Overflows, Injections)
- Angriffe aus Betriebsumgebung (z.B. Power Analysis, Timingattacken)
- Angriffe über ëxterne Komponenten"(z.B. Social Engineering, Phishing)

II.2. Wichtigste Sicherheitsziele

- Confidentiality (Schutz vor unbefugten Lesezugriffen)
- Integrity (Schutz vor unbefugten Schreibzugriffen (Veränderung/Verfälschung)
- Availability (Möglichkeit, Ressourcen/Dienste in der vorgesehenen Form zu nutzen)

II.3. Praxisprobleme

- Abwägung Kosten/Nutzen
- gesetzliche Regelungen
- ethische/soziale Probleme
- Grunddilemma unterschiedlicher Begriffe und Definitionen
- Snake Oil (z.B. Enigma, Quantenkryptographie + One-Time-Pad)