

Gefahren im Internet

- Kompromittierung des eigenen Systems
 - ◆ **Ausspähen von Daten**
 - ◆ **Mißbrauch von Ressourcen**
 - ◆ **Zerstörung des Systems**
- Gefährdung fremder Systeme
 - ◆ **„Hacken“ fremder Systeme**
 - ◆ **Denial-of-Service-Attacken (DDOS)**
- Rufschädigung durch Domain-Mißbrauch

Systemkonfiguration

- Software aktualisieren (Sicherheitsupdates)
- Paßwörter (BIOS, Windows, Shares) benutzen
- Freigaben nicht anzeigen, Paßwortverschlüsselung
- Bildschirmschoner mit Paßwort aktivieren
- Makro-Schutz bei Office-Programmen einschalten
- Fremdsoftware (vor allem Spiele!) überprüfen
- **System-Sicherung (Image-Backup)**
- Antivirenprogramm
- Persönliches Firewall

E-Mail

■ Konfigurieren:

- ◆ Automatische Vorschau abschalten
- ◆ Sicherheit für eingeschränkte Sites
- ◆ Nur Text (quoted printable) beim Senden
- ◆ Digitale Signatur und Verschlüsselung

■ Gefahren:

- ◆ HTML-Mail (bereits Vorschau)
- ◆ Hoaxes (falsche Virenwarnung)
- ◆ Anhänge (ausführbare Dateien, .exe, .vbs)
- ◆ Dokumente mit Macros (.doc, .xls)

Surfen im Web nur mit Eingabeaufforderung

- ActiveX (Plugins) nur mit Eingabeaufforderung
- Download von Dateien und ActiveX dto...
(Vorsicht vor 190-Dialern und Spyware)
- Aktive Inhalte nur von vertrauenswürdigen Sites
- Vorsicht bei Domains (Statuszeile beobachten)
- Formulare, Paßwörter und persönliche Informationen nicht abspeichern

Human (social) engineering

- Zugangssicherung
 - ◆ System, Drucker, Netze
 - ◆ Datenträger sichern
- Risikobewußtsein im Netz
 - ◆ Domains, Mailadressen
- Vertrauensprüfung