Sicherheit im Internet

- Was ist ‚Sicherheit‘ - das Vokabular
- Angriff und Verteidigung
  - Zugriff verweigert - drei ‚A‘s
  - Lücken und Löcher - man kommt doch rein
  - Lauschangriff und Verschluesselung
  - DoS - nichts geht mehr
  - Firewalls - die Rettung?
- Ein Sicherheitskonzept
- Tips für den Alltag

Was ist ‚Sicherheit‘

- Mehrere ‚Arten von Sicherheit‘
  - was soll geschützt werden:
    - Geheimhaltung - Confidentiality
    - ‚wer und was‘ - Integrity and Authenticity
    - Verfügbarkeit - Availability
- Schwächen und Angriffspunkte
  - Zugang zur Hardware, Naturkatastrophen, Abstrahlung, Kommunikationswege (inkl. Netzwerk), Softwarefehler, Benutzer
- Das Internet ist ‚nur ein‘ Sicherheitsaspekt!

Zugriff verweigert - drei ‚A‘s

- Am meisten kann der Angreifer bewirken wenn er den eigentlichen Rechner kontrolliert. Also:
- Zugriffskontrolle - AAA:

  Authentication - Authorization - Accounting

  Identität feststellen - Zugriffsrechte prüfen - Aufzeichnen
- Welche Dienste sind verfügbar?

- Wie sind die Passwörter gewählt?
- Sind die ‚Nutzerprivilegien‘ richtig? Dateirechte!
- Werden Logdaten gesichert und gesichtet?

Lücken und Löcher

- Niemand kann sich sicher sein, daß die Software nur tut was er möchte
  - Konfigurationsfehler öffnen Lücken
  - Softwarefehler. Berühmt: Buffer overflow
    - für fast jeden Dienst gab es schon (populäre) Server mit schweren Fehlern. Und es gibt sie weiterhin.
  - Viren, Würmer, Trojaner und anderes Getier.
    - Viren sind nicht neu, das Netz bietet nur einen hervorragenden Verteilungsweg
    - Trojaner können das System zum Netz hin öffnen
  - Wer ein ‚Loch' hat, ist schnell entdeckt - selbst dialup-nutzer sind nicht sicher vor ‚Scannern'

Lauschangriff und Verschlüsselung

- Hier geht es um die Daten selbst
  - Jeder Knoten auf dem Pfad eines Pakets im Internet kann sich dessen Inhalt anschauen!

  -> wer seine Daten vor Fremden verbergen will, muß verschlüsseln.
- Public-Key Verfahren bieten nicht nur Daten-verschlüsselung sondern auch Unterschriften
  - PGP und S/MIME für Email.
  - SSL/TLS für Web und viele TCP-Dienste
  - SSH als Ersatz fuer rlogin, rcp und rsh
  - IPSEC als Hoffnung für die Zukunft?

DoS - nichts geht mehr

- Sabotage - ‚Denial of Service‘
  - Steigender ‚Wert‘ von Netzdienstleistungen führt zu mehr Motiven für Angreifer.
  - Da es nur ums ‚Kaputtmachen‘ geht, gibt es viel mehr Angriffspunkte - Verteidigung ist sehr schwer.
- Haeufig wird Resourcenmangel ‚erzeugt‘:
  - smurf - Bandbreitenfresser
  - Ping-of-death - IP Layer
  - SYN-attack - TCP Layer
  - „CGI-Benchmarks“ - Applikations-Überlast

Firewalls - die Rettung?

- Zonen des eigenen Netzes werden von der Aussenwelt abgeschottet
- Für jede Zone wird nur Verkehr zu genau definierten Diensten zugelassen.
- Firewall muss selbst stark geschützt sein und
- Guter Schutz auf IP- und TCP-Ebene
- Wenig Hilfe auf Netz- und Applikationlayer
- Firewall kann Ziel von DoS Angriffen werden

Und wenn es doch passiert?

- Intrusion Detection
  - Schon herauszufinden ob jemand eingedrungen ist, ist meisst sehr schwer.
  - Analog zu Firewalls entwickelt sich langsam eine Gruppe von ‚Jagdprogrammen‘ (IDs)
- Reaktionen
  - Daten (Beweise!) sammeln
  - Löcher schliessen
  - Zurückgelassene Hintertüren entfernen
  - Anzeige erstatten

Ein Sicherheitskonzept

- Was soll vor wem geschützt werden?
- Kosten / Risiko - wieviel Aufwand darf es sein?
- Was soll erlaubt sein?
- Wie wird im Ernstfall vorgegangen?
- „Sicherheitsvorschriften“ für Rechner, Netz und Nutzer

- Ideal: Auch der Ernstfall wird geübt

Tips für den Alltag

- Für den Heimbedarf:
  - nicht benötigte Dienste ausschalten, bei allen anderen die Konfiguration überprüfen und updates einspielen
  - Logfiles regelmässig kontrollieren und archivieren
  - Virenchecker nutzen
  - Backups machen
- Leseliste
  - Computer Security Basics (Russel & Gangemi, O'Reilly)
  - Building Internet Firewalls (Chapman & Zwicky, O'Reilly)
  - System Security; A Management Perspective
    Aus ‚Short Topics in System Administration', Editor Dan Green, SAGE