„Internet Security“ — was unseren PC bedroht und wie wir uns davor schützen können

Torsten Neck
FTU
18.07.2002

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck

Kommunikationsplattform Internet

- Zugriff auf Informationen:
  - WorldWideWeb
  - Filetransfer
  - News
- Bereitstellung von Informationen:
  - WorldWideWeb
  - Filetransfer
  - News
- Kommunikation:
  - eMail
  - ICQ — IRC
- Anbindung externer Personen
  - Mitarbeiter
  - Wartungspersonal
- Electronic Commerce

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck

Bedrohungen und Schäden

- Natürliche und technische Vorfälle
  - Naturgewalten, Feuer, Wasser
  - Klima (Hitze!)
  - Ermüdung, Verschleiß
- Angriffe
  - auf die Verfügbarkeit von Daten
  - auf die Integrität von Daten
  - auf die Vertraulichkeit von Daten

- Schaden
  - Beeinträchtigung der Aufgabenerfüllung
  - Dauer der Verzichtbarkeit
  - Außenwirkung und Innenwirkung
  - finanzieller Verlust — direkt und indirekt

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck

Statistik

Das amerikanische Verteidigungsministerium
hat vor einigen Jahren seine eigene Sicherheit getestet:

▼ Angriffe:	8932 Systeme	100,0 %
▼ erfolgreich bei:	7860 Systemen	88,0 %
▼ entdeckt:	390 Einbrüche	4,4 %
▼ gemeldet:	19 Einbrüche	0,2 %

Quelle: Internet Security Systems Inc.

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck

CERT Statistik 1988 bis 1998

Jahr	gemeldete Angriffe	gemeldete Systemfehler
1988	6	—
1989	132	—
1990	252	—
1991	406	—
1992	773	—
1993	1334	—
1994	2340	—
1995	2412	171
1996	2573	345
1997	2134	311
1998	3734	262

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck

Angreifer

- Identität von Angreifern:
  - Mitarbeiter des eigenen Unternehmens — 70 % der Angriffe!
  - Studenten und Schüler — jugendliches „Austesten“
  - Konkurrenz und Wettbewerber
  - Hacker aus der Computer-Untergrundszene
  - professionelle Hacker und Industriespione

- Expertise von Hackern:
  - detaillierte Informationen frei im Internet verfügbar
  - Umnutzung von Standardprogrammen
  - Software Werkzeuge für Jedermann verfügbar:
    - Sniffit (mitlesen) und Spoofit (mitlesen und verändern)
    - cRACK
    - ISS und S.A.T.A.N (Security-Checker)
    - Wardialer
    - ...

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck

Angriffsnutzen

- Beschaffung von Informationen
- Manipulation von Informationen
- Denial of Service
  Verfügbarkeit von Diensten oder Systemen einschränken oder blockieren
- Kontrolle über ein System
- Benutzung als „Sprungbrett“
- Spaß und Zeitvertreib

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck

Angriffsweisen

- passive Gefährdung
  - Spamming — Erhalt von unerwünschten Informationen
  - Mailbombing und Flooding
  - maligne Attachments
    - Scripts und Executables
    - umfunktionierte Bilder und Animationen, Multimediafiles
  - Viren und Würmer
  - Trojaner
  - Port-Scan
  - Broadcast-Storming und DDOS
- (re-)aktive Gefährdung:
  - Autentifizierung — Passwordeingabe, -übertragung
  - Cookies
  - dynamisches HTML, browserseitige Scripts
  - Link Flooding und Spamming

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck

Werkzeuge der Internet-Security

- Autentifizierung
- Verschlüsselung
- Firewalls
- Content-Security
- Sicherheitsüberprüfung und regelmäßige Kontrolle

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck

funktionale und technische Angriffsziele

- Workstation
  - Hardwarekomponenten
    - Zugangskontrolle
    - Systemmonitoring
    - Virencheck
  - Dateisystem
    - NTFS mit wohldefinierter Rechtevergabe
    - minimale Freigaben mit wohldefinierten Berechtigungen
    - Logging
    - Virencheck
  - Benutzerinformationen
    - beschränkte Benutzer
    - sichere Passwörter
  - Kommunikationsklienten
    - gesundes Mistrauen
    - Virencheck
    - digitale Signatur und Verschlüsselung
    - zentrale Entrypoints und Proxies
    - zentrale Firewall
  - Software
    - nur Notwendiges
    - Virencheck

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck

funktionale und technische Angriffsziele

- Server
  - Hardwarekomponenten
    - Zugangskontrolle
    - Systemmonitoring
    - Virencheck
  - Dateisystem
    - NTFS mit wohldefinierter Rechtevergabe
    - minimale Freigaben mit wohldefinierten Berechtigungen
    - Logging
    - Virencheck
  - Benutzerinformationen
    - Domainkonzept, zentrale Verwaltung
    - sichere Passwörter
  - Kommunikationsdienste
    - Beschränkung auf das Notwendige
    - Logging, Monitoring und Virencheck
    - Verschlüsselung
    - Zentralisierung und Redundanz
    - zentrale Firewall
  - Software
    - nur Notwendiges
    - Virencheck

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft
Fortbildungszentrum f. Technik u. Umwelt
Dipl.-Inform. Torsten E. Neck