

---

# Sicherheit

Bedeutung

Gefahren

---

---

# Sicherheitsbegriff

- n Unversehrtheit und Vertraulichkeit persönlicher Daten
- n Datenschutzgesetz 2000
- n Bedrohungen
  - q Dialer, Spam, Spyware, Viren, Würmer, Trojaner
  - q Hackerattacken, Passwortschutz
- n IT-Fachmann haftbar

---

# Gefahren für Benutzer

- n Programmfehler – Sicherheitsupdates
- n Windows (Sicherheitscenter)
  - q Manuelle und automatische Updates, Patches, Hotfixes, Service Packs
  - q Systemsteuerung/Software
- n Office
  - q Gefahr durch VBA (Makros...)
  - q Updates und Service Packs

---

# Viren

- n Über 60.000 Computer-Viren (2005)
- n *"We define a computer-'virus' as a program that can infect other programs by modifying them to include as possibly evolved copy of itself....."*  
(Fred Cohen, Diss. 1984)
- n Schleusen Code in andere Programme oder Bereiche des Betriebssystems ein und reproduzieren sich

---

# Viren - Funktionsweise

- n Bootsektor-Viren
- n Datei-Viren (Link-Viren) - häufigster
- n Polymorphe Viren
- n Speicherresidente Viren
- n Tarnkappen-Viren (Stealth Viren)
- n Scriptviren (PHP, JavaScript, VBScript)
- n Makro-Viren (VBA)

---

# Würmer - Funktionsweise

- n In Netzwerken – aktiv, selbständig
- n Nützen Sicherheitslücken
- n Schaden oder Ressourcen binden
- n Attacken auf Server (Denial of Service – DoS)
- n Verbreitung
  - q E-Mail (oft eigener mailservers dabei), HTTP (VBS)
  - q IRC-Systeme, File-Sharing-Systeme

---

# Viren

## n Trojaner

- q Oft über kostenlose Programme, Spiele, Raubkopien (Bedrohung im Hintergrund)

## n Bomben

- q Funktionen in Programmen, die später Schaden anrichten

## n Trap doors (Backdoor)

- q Zugang verschaffen

---

# Viren - Bedrohungen

- n Versand persönlicher Daten
- n Protokollierung von Eingaben
  - q Mitlesen sensibler Daten
- n Versand manipulierte Mails
- n Protokollierung Suchvorgänge
  - q Browser lädt unerwünschte Seiten
- n "Denial of Service"-Attacken

---

# Viren Info (Beispiele)

- n Hersteller von Anti-Viren-Programmen à Warnungen und Info über Risiken, Entfernung etc.
- n Symantec – Norton Antivirus
- n Network Associates – McAfee
- n Ikarus Software
- n Trend Micro
- n Kaspersky Software
- n U.a.

---

# Viren – Vermeidung und Abwehr

## n Basissicherheit

- q Betriebssystem updaten und patchen
- q Aktuelle Virens Scanner
- q Programmeinstellungen (Mail!)

## n Weitere Maßnahmen

- q Firewall (à Würmer)
- q Passwörter
- q Keine Raubkopien
- q Datensicherung
- q Verantwortungsbewusstsein

## n HOAX à falscher Alarm per E-Mail

# Passwörter

## Passwortstärke

- n Keine Benutzernamen
- n Keine Personen, Tiere, Orte
- n Keine Abkürzungen, nicht aus Wörterbuch
- n Keine persönlichen Daten
- n Keine Varianten (rückwärts, groß/klein)
- n Buchstaben und Ziffern kombinieren
- n Mind. 8 Zeichen (groß, klein, Sonderzeichen)
- n Hilfe: Eselsbrücken (Anf.Buchst. Eines Satzes)

---

# Passwörter

## n Hackermethoden

### q Wörterbuch-Attacke

- n Wörter aus täglichem Sprachgebrauch

### q Brute-Force-Technik

- n Alle möglichen Kombinationen probieren
- n Mehrere Rechner einsetzen

### q Passwörter löschen

## n IDS (Intruder Detection)

- q Sperre des Kontos nach mehrmaliger falscher Passworteingabe

## n Phishing (meist per E-Mail)



---

# Firewall

- n Verhindert Zugriffe von anderen Computern
- n Hardware, Software oder Kombi zum Schutz des LAN
- n Desktop-Firewall schützt einzelnen Rechner selbst (Würmer, Viren)
- n Packet Filter Firewall (Transportschicht) prüft Dienste (Ports)
- n Application Level Firewall (Anwendungsschicht) → Berechtigung

---

# Firewalls

- n XP – Windows-Firewall
  - q Einstellung für best. Verbindungen
  - q Ausnahmen möglich....
- n ZoneAlarm
  - q Jedes Programm muss fragen bei TCP/IP-Kommunikation
  - q Zugriffsteuerung für jedes Programm
  - q Not-Stopp
- n Websites (auch kostenlose Versionen)
  - q [www.zonelabs.de](http://www.zonelabs.de)
  - q [www.sygate.de](http://www.sygate.de)

---

# Schutz der Privatsphäre

- n Achtung auf "Spuren"
- n Spuren verwischen
- n Sicherheitscenter – Internetoptionen
- n Spyware – Surfverhalten ausspionieren
  - q Durch Freeware und Adware
  - q Schutz durch AntiSpy-Programme
- n Spuren
  - q Verlauf (History) im Browser
  - q Cookies
  - q Temporäre Dateien

---

# Verlauf / History

- n Verlauf (Internet Explorer)
- n Chronik (Firefox)
  
- n Optionen
  - q Löschen
  - q Wie viele Tage aufbewahren?

# Brute-Force-Technik: Übung

Passwort	Länge	Anzahl der verwendeten Zeichen
U	1 Stelle	256 (gesamter Zeichensatz)
Abcd	4 Stellen	52 (nur Groß- und Kleinbuchstaben)
Aö8d	4 Stellen	256
AbdideiE	8 Stellen	52
uidDiä8w	8 Stellen	256

**Wie lange braucht ein Hacker zum "Erraten" des Passwortes bei 100.000 Versuchen pro Sekunde?**



# Passwortstärke prüfen

- n Prüfe folgende Passwörter online
- n [www.securitystats.com/tools/password.php](http://www.securitystats.com/tools/password.php)

<b><i>Passwort</i></b>	<b><i>Schwach/Mittel/Stark</i></b>
Susi	
Susanne	
Susanne1999	
lfgmdFidS	
lfgmdFidS1986	

