Sicherheitsbedrohungen in Netzen

Einführung in die Praxis des betrieblichen Datenschutzbeauftragten

Dirk Fox
fox@secorvo.de

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455
E-Mail: info@secorvo.de
http://www.secorvo.de

Anhang zu §9 des BDSG

Anforderungen des Datenschutzes an die Verarbeitung öffentlicher und nicht-öffentlicher personenbezogener Daten:

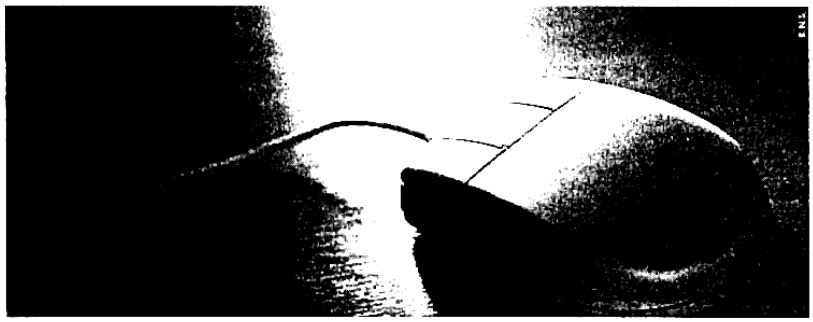
- **Zutrittskontrolle**
- **Zugangskontrolle**
- **Zugriffskontrolle**
- **Weitergabekontrolle**
- **Eingabekontrolle**
- **Auftragskontrolle**
- **Verfügbarkeitskontrolle**
- **Getrennte Verarbeitung**

Maßnahmen sind *erforderlich*, wenn ihr Aufwand in angemessenem Verhältnis zum angestrebten Schutzzweck steht.

secorvo security consulting

Notizen:

Der Dieb von heute benutzt keinen Dietrich, sondern eine Maus.



secorvo security consulting

Notizen:

Übersicht

- **Gefährdung von Daten in Netzen**
  - Klassifikation und Überblick
- **Maskeradeangriffe**
  - Password Guessing und Password Scanning
- **Integritäts- und Authentizitätsangriffe**
  - Connection Highjacking
  - DNS Spoofing, ARP Spoofing
- **Malicious Code**
  - ActiveX Controls, Scriptsprachen
  - Trojanische Pferde

secorvo security consulting

Notizen:

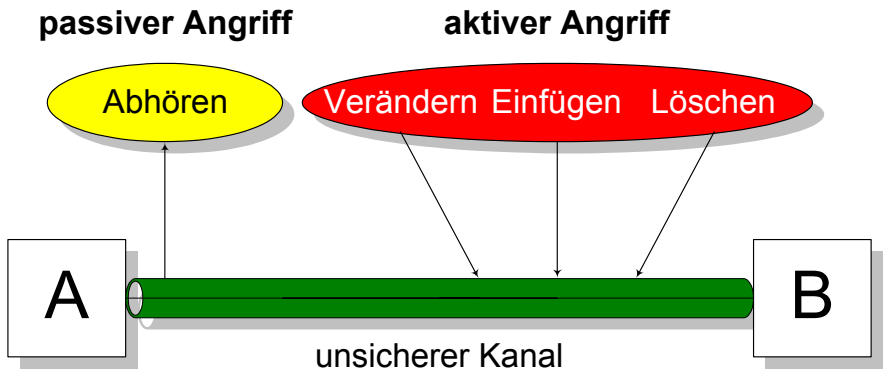
Übersicht

- **Gefährdung von Daten in Netzen**
  - **Klassifikation und Überblick**
- Maskeradeangriffe
  - Password Guessing und Password Scanning
- Integritäts- und Authentizitätsangriffe
  - Connection Highjacking
  - DNS Spoofing, ARP Spoofing
- Malicious Code
  - ActiveX Controls, Scriptsprachen
  - Trojanische Pferde

Notizen:

Gefährdung von Daten in Netzen

- **Angriffe auf das Übertragungsmedium**



Notizen:

Gefährdung von Daten in Netzen

Klassifikation nach Schutzobjekten:

- **Zentrale Ressourcen**
  - Verfälschung, Kenntnisnahme zentral gespeicherter Daten
  - Missbrauch von Plattenspeicher, Kommunikationsdiensten
- **Arbeitsstationen**
  - Kopieren oder Verfälschen lokal gespeicherter Daten
  - Unberechtigter Netzzugang
- **Übertragungsmedium**
  - Abhören und Protokollieren übertragener Daten
  - Einspielen oder Modifizieren von Daten

secorvo security consulting

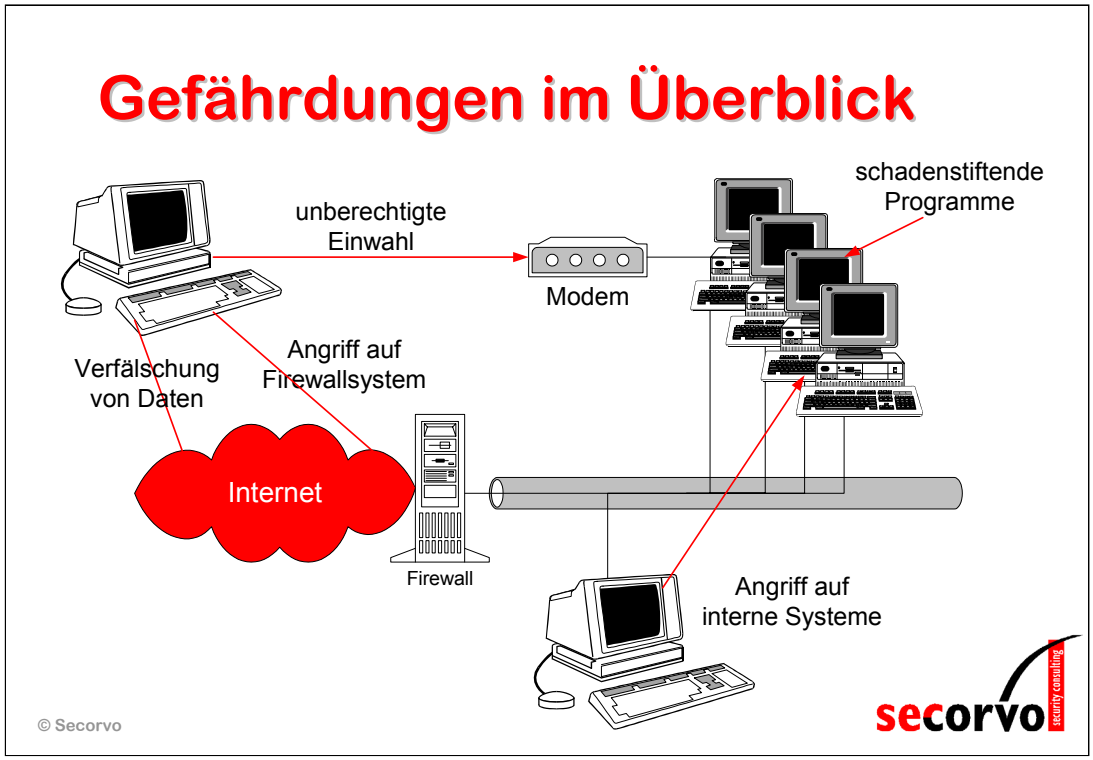
Notizen:

Gefährdungen im Überblick

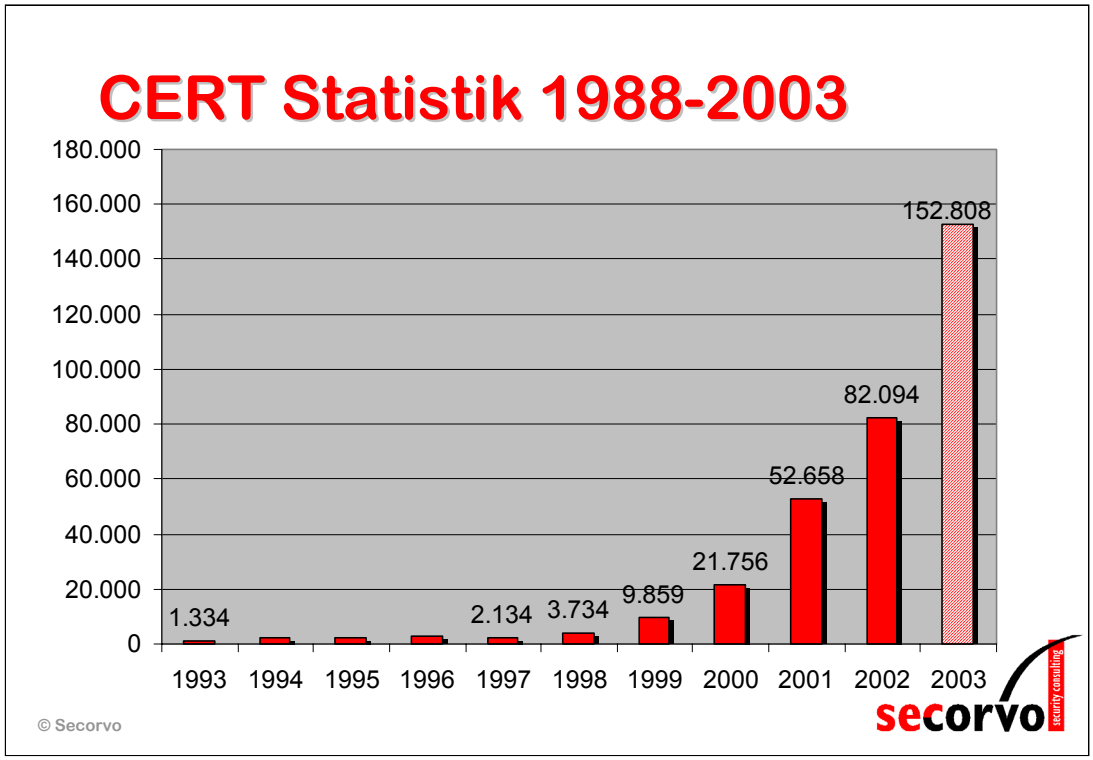
- **Abhören (Vertraulichkeit)**
  - Abhören des Übertragungsmediums (Kabel, Richtfunk)
- **Unberechtigter Systemzugriff (Autorisierung)**
  - Ausnutzung von Programm-/Betriebssystemfehlern
  - Missbrauch von Rechten
- **Maskerade (Authentizität)**
  - Ausspähen von Passworten (z. B. social engineering)
  - IP-Spoofing (Fälschung der Senderadresse)
- **Connection Highjacking (Datenauthentizität)**
  - Übernahme bestehender Verbindungen nach Authentifikation
  - Einspielen gefälschter Daten (z. B. gefälschte E-Mails)
- **Malicious Code (Integrität)**
  - Einschleusen von Trojanischen Pferden

secorvo security consulting

Notizen:

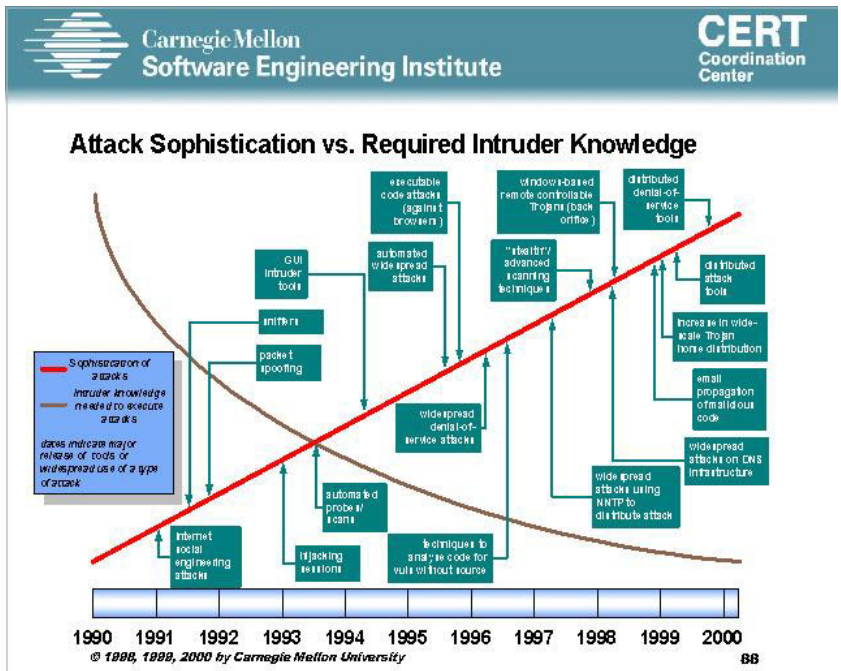

Gefährdungen im Überblick
unberechtigte Einwahl
Modem
schadenstiftende Programme
Verfälschung von Daten
Angriff auf Firewallsystem
Internet
Firewall
Angriff auf interne Systeme
© Secorvo
secorvo
security consulting

Notizen:



CERT: Computer Emergency Response Team

Notizen:



CERT/CC: CERT Coordination Center

Notizen:

Übersicht

- Gefährdung von Daten in Netzen
  - Klassifikation und Überblick
- **Maskeradeangriffe**
  - **Password Guessing und Password Scanning**
- Integritäts- und Authentizitätsangriffe
  - Connection Highjacking
  - DNS Spoofing, ARP Spoofing
- Malicious Code
  - ActiveX Controls, Scriptsprachen
  - Trojanische Pferde

secorvo security consulting

Notizen:

Password Guessing

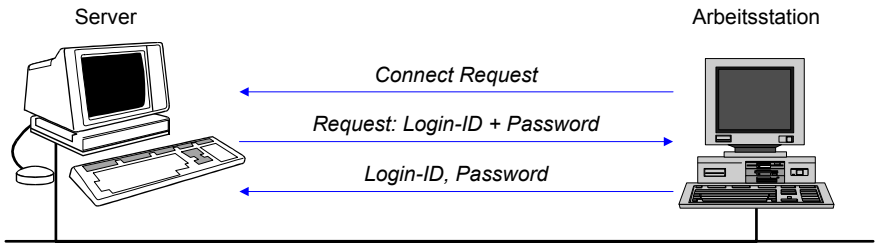
- **Passwortwahl**
  - Passwort aus „persönlichen“ Daten (Geburtsdatum, Namen von Angehörigen etc.): „Social Engineering“ möglich
  - Keine Sonderzeichen, Ziffern: Verkleinerung des Suchraums
  - Lexikalische Begriffe: Informationsgehalt ca. 1 bit je Zeichen
- **Passwortwechsel**
  - Selten
  - Häufig identische oder ähnliche Passworte
  - Passwort oft notiert
- **Identische Passworte**
  - Verschieden sichere Systeme
  - Größerer Schaden bei Passwortverlust
  - Passwortwechsel aufwendig

secorvo security consulting

Notizen:

Password Scanning

- **Passwort-„Authentifikation“ in Internet-Protokollen (Telnet, FTP, POP3, ...)**



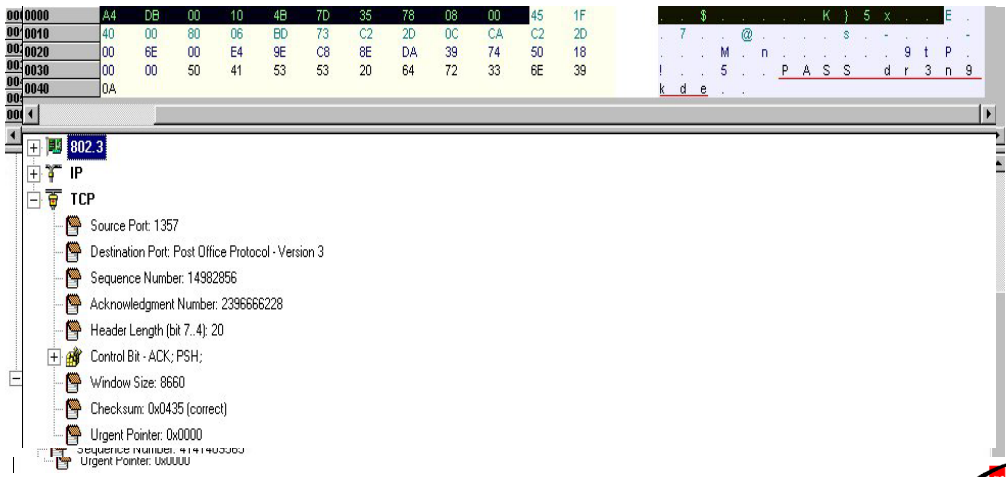
- **Probleme:**
  - **Login-ID und Passwort im Klartext übertragen**
  - **Password Guessing-Angriffe sind möglich**

FTP: File Transfer Protocol

POP3: Post Office Protocol v3

Notizen:

Password Scanning



Notizen:

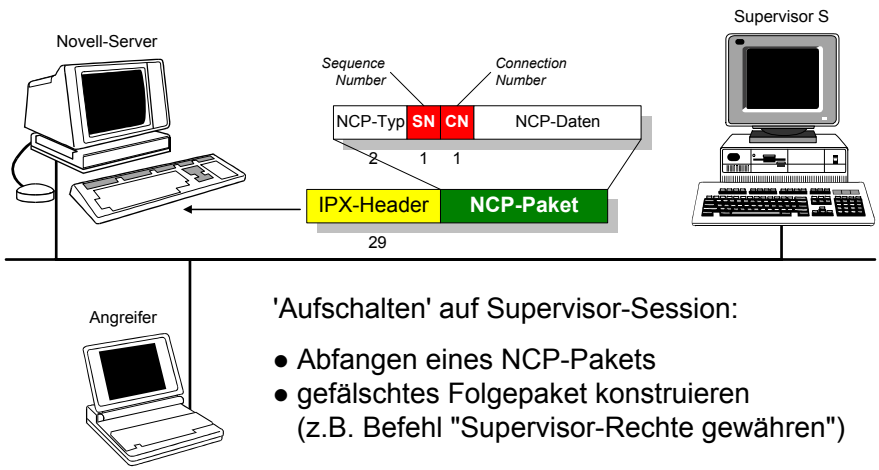
Übersicht

- Gefährdung von Daten in Netzen
  - Klassifikation und Überblick
- Maskeradeangriffe
  - Password Guessing und Password Scanning
- **Integritäts- und Authentizitätsangriffe**
  - **Connection Highjacking**
  - **DNS Spoofing, ARP Spoofing**
- Malicious Code
  - ActiveX Controls, Scriptsprachen
  - Trojanische Pferde

Notizen:

Connection Highjacking

- **Connection Hijacking (z. B.: Novell-Netware)**



'Aufschalten' auf Supervisor-Session:

- Abfangen eines NCP-Pakets
- gefälschtes Folgepaket konstruieren (z.B. Befehl "Supervisor-Rechte gewähren")

secorvo security consulting

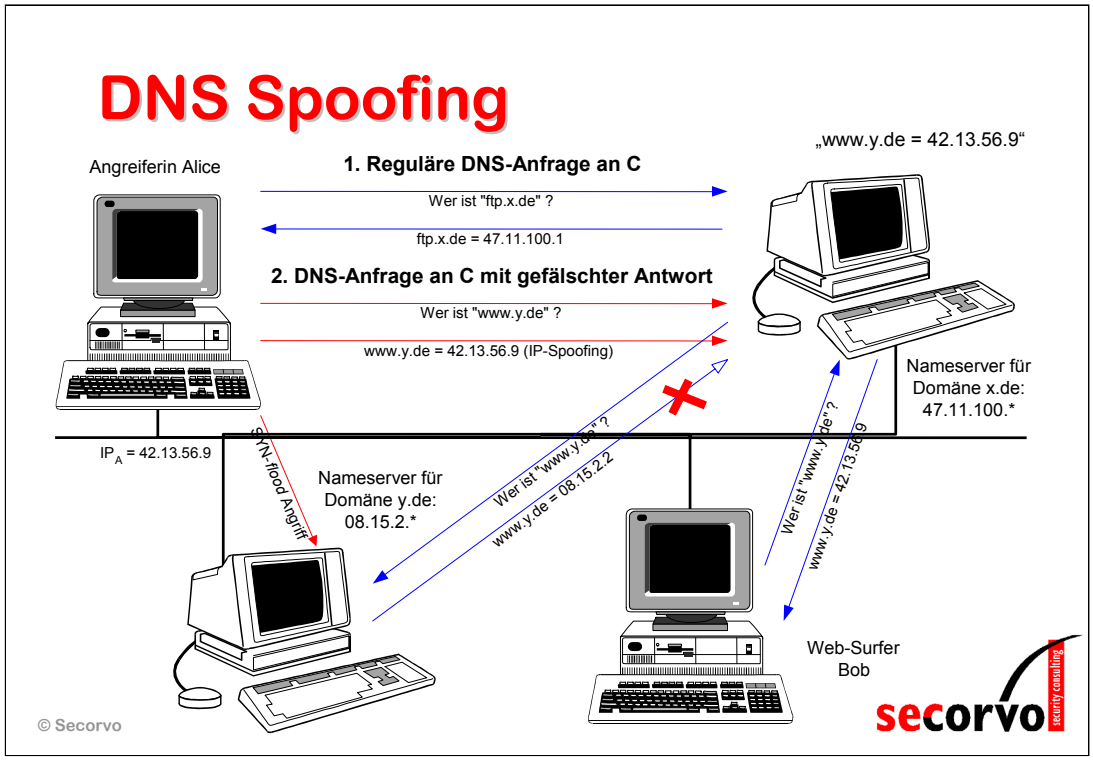
CN: Connection Number

IPX: Internetwork Packet Exchange

NCP: Netware Core Protocol

SN: Serial Number

Notizen:

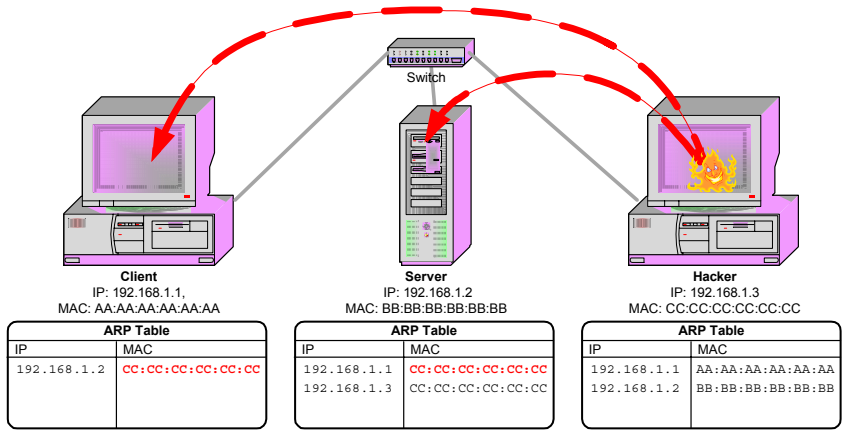


DNS: Domain Name Service

Notizen:

ARP Spoofing

- **Angreifer fälscht ARP-Pakete und damit ARP-Tabellen**
- **Pakete werden über Angreiferrechner „umgeleitet“**



ARP Table

IP	MAC
192.168.1.2	CC:CC:CC:CC:CC:CC

ARP Table

IP	MAC
192.168.1.1	CC:CC:CC:CC:CC:CC
192.168.1.3	CC:CC:CC:CC:CC:CC

ARP Table

IP	MAC
192.168.1.1	AA:AA:AA:AA:AA:AA
192.168.1.2	BB:BB:BB:BB:BB:BB

secorvo security consulting

ARP: Address Resolution Protocol

IP: Internet Protocol (Protokollschicht 3)

MAC: Medium Access Control (Protokollschicht 2)

Notizen:

Übersicht

- Gefährdung von Daten in Netzen
  - Klassifikation und Überblick
- Maskeradeangriffe
  - Password Guessing und Password Scanning
- Integritäts- und Authentizitätsangriffe
  - Connection Highjacking
  - DNS Spoofing , ARP Spoofing
- **Malicious Code**
  - **ActiveX Controls, Scriptsprachen**
  - **Trojanische Pferde**

Notizen:

Angriffe von Webseiten

- **ActiveX-Controls (Microsoft)**
  - **ActiveX-Berechtigungen**
    - **Voller Zugriff auf Betriebssystem-APIs**
    - **Keine Sicherheitsmechanismen**
    - **“Offenes Scheunentor” für Angreifer**
  - **AuthentiCode-Mechanismus**
    - **Digitale Signatur unter ActiveX-Control**
    - **Authentizitäts- und Integritätsnachweis**
    - **Keine Garantie für “sauberen” Code**

secorvo security consulting

Notizen:

Angriffe mit Script-Sprachen

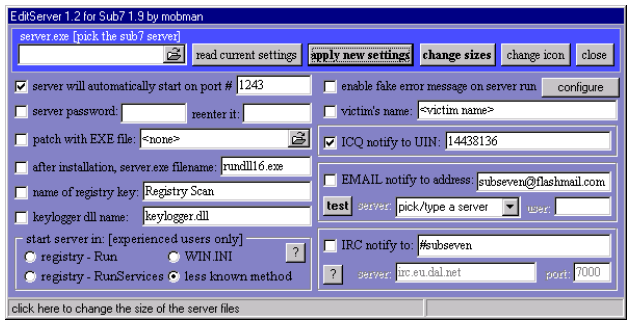
- **Arten von Script-Sprachen:**
  - **Integration von Betriebssystem-Befehlen in Dokumente**
  - **Makro-Sprachen für Tabellenkalkulation, Textverarbeitung**
  - **Script-Kommandos in WWW-Dokumenten (JavaScript, VBScript)**
- **Beispiel: VisualBasicScript v3.x**

```
<HTML>
<HEAD></HEAD>
<BODY>

<SCRIPT LANGUAGE="VBSCRIPT">

Set fs = CreateObject("Scripting.FileSystemObject")
Set a = fs.CreateTextFile("c:\autoexec.bat", True)
a.WriteLine("@echo off")
a.WriteLine("cd c:\windows")
a.WriteLine("delete *.*")
a.Close

</SCRIPT>

</BODY>
</HTML>
```


Notizen:

Trojanische Pferde

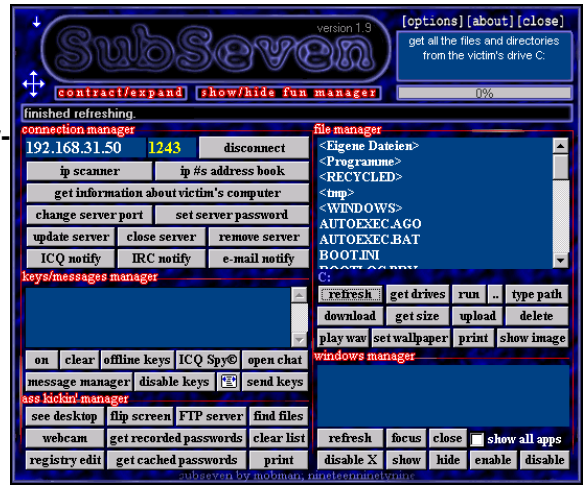
- **Angriffe mit „Trojanischen Pferden“**
  - **Trojaner über das Internet laden**
  - **Konfigurieren des Trojaners (Port, Name, Autostart-Methode)**
  - **„Patchen“ auf Wirtsprogramm**
  - **Versendung des Wirtsprogramms via CD, E-Mail, Download)**
  - **Trojaner meldet sich nach Start (E-Mail, IRC)**



Notizen:

Trojanische Pferde

- „Leistungsumfang“
  - Dateien laden
  - Änderung der Rechnerkonfiguration
  - Auslesen zwischengespeicherter Passworte
  - Kopie des Bildschirminhalts
  - Raumüberwachung (Mikrofon, Webcam)
  - Fernsteuerung des „Opfers“



Notizen:

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455
E-Mail info@secorvo.de
http://www.secorvo.de