RRZN-Basiskurs:

Sicherheit für Anwender

Birgit Gersbeck-Schierholz



Sicherheit für Anwender

R|R|Z|N

- Zielsetzung des Kurses
- Sicherheitsrisiken
- Hacker und Cracker
- Grundlagen zur Internet-Kommunikation
- Unsichere Einstellungen im Betriebssystem
- Gefahrenquelle: Surfen im Internet
- Viren, Würmer und Trojaner
- E-Mail: Einstellungen und gefährliche Anhänge
- Passwörter
- Installieren einer Personal Firewall



Sicherheit für Anwender

R|R|Z|N

<u>Zielgruppe</u>: PC-Anwender, die sich nicht hauptberuflich um die Technik ihres Arbeitsgerätes kümmern

<u>Zielsetzung des Kurses</u>: Die Sensibilisierung der Anwender für das Thema Computersicherheit durch eine zusammenfassende Darstellung der wesentlichen Sicherheitsmaßnahmen für Nutzer

Es sollte deutlich werden, dass es sich auszahlt, ein **geschärftes Sicherheitsbewusstsein** zu entwickeln, denn

- **Sicherheit macht Arbeit** (Überlegungen zu sicheren Einstellungen in der Software anstellen, Pflegen und Warten von Betriebssystemen und Virenscannern, Informationen über Sicherheitslücken sammeln …)
- **ein kompromittierter oder virenverseuchter Rechner macht noch mehr Arbeit, unabhängig vom Schaden** (Säubern von Viren, Neuinstallation des Rechners, Ausfallzeiten …)



Sicherheitsrisiken

R|R|Z|N

- **Im Zusammenhang mit Computer-Sicherheit stehen zwei Bedürftnisse im Gegensatz zueinander:**
  - **der Wunsch nach komfortabler Bedienung**
  - **die Forderung nach Verfügbarkeit, Vertraulichkeit und Integrität der Daten**

Beispiele für Arten des Missbrauchs (1)

Ein unsicheres Computersystem läßt den **unberechtigten Zugriff auf vertrauliche Daten** zu.

– Wissenschaftsspionage, Ausspähen von Online-Banking-Daten und Passwortdateien -

Beispiele für Arten des Missbrauchs (2)

- Das **Löschen** und/oder **Modifizieren** Ihrer Daten ist möglich.

  - Verlust der Verfügbarkeit bzw. der Integrität -

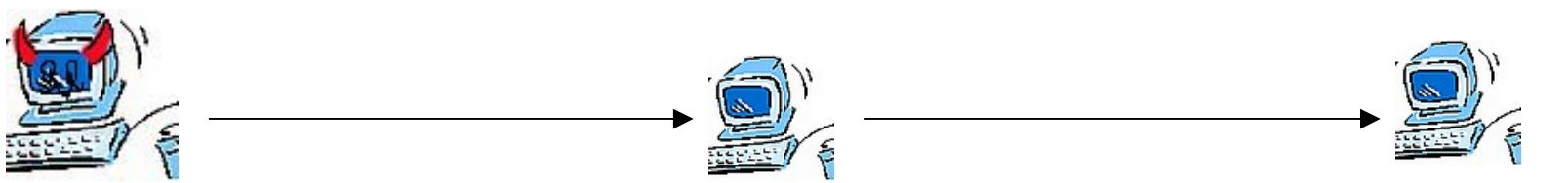


Beispiele für Arten des Missbrauchs (3)

- Eine von Ihnen unbemerkte Tauschbörse für **illegales Datenmaterial** wird auf Ihrem PC eingerichtet.

Beispiele für Arten des Missbrauchs (4)

- Der Hacker „borgt“ sich Ihre Identität und unternimmt damit weltweite Angriffe.
  - **Dabei werden Sie als Verursacher angesehen** …

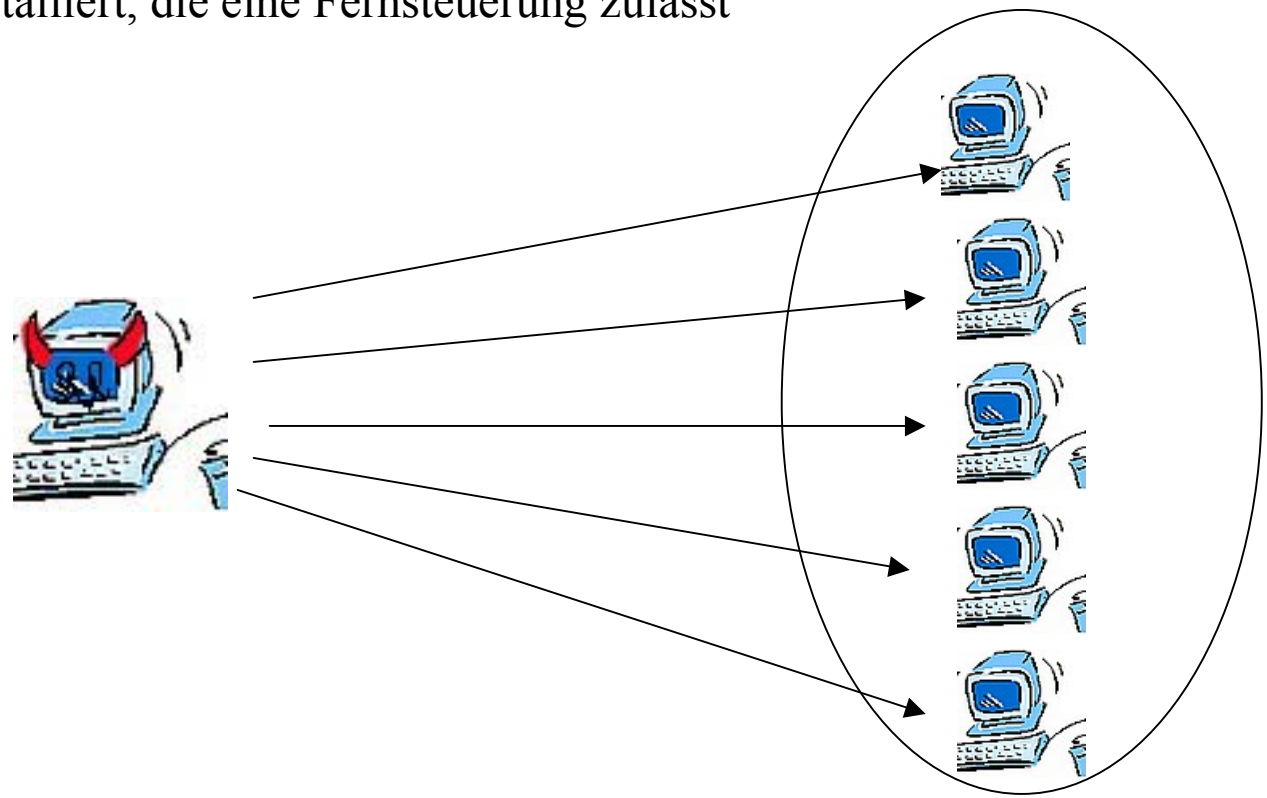


Beispiele für Arten des Missbrauchs (5)

- **Unfreiwillige Beteiligung** Ihres Computers an einem verteilten Denial-of-Service-Angriff (DDoS), der zur Überlastung des Netzes und zum „Crash“ des Ziel-Servers führen soll.

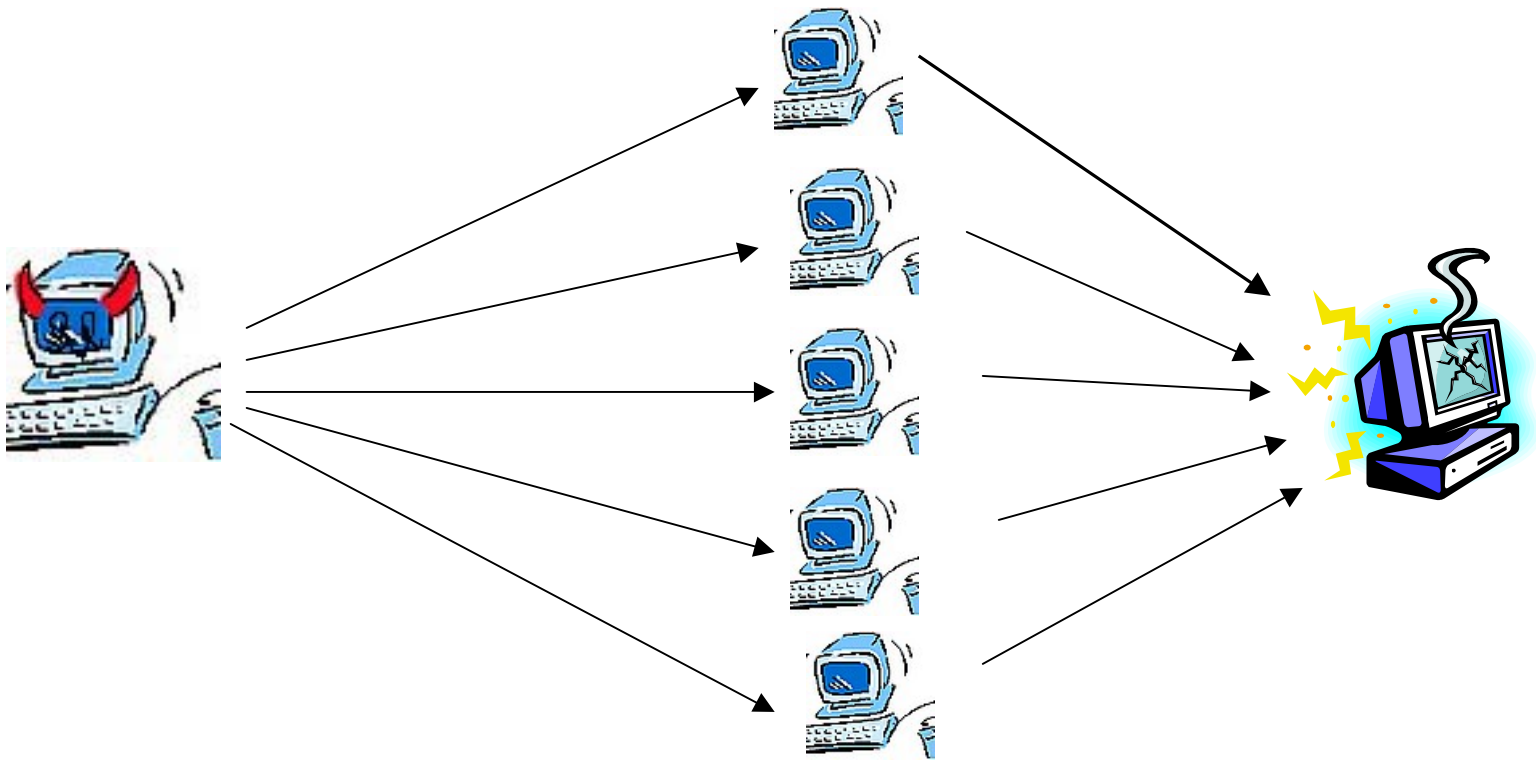
Beispiel: verteilter Denial-of-Service-Angriff (DDoS)(1)

1. Schritt: Auf vielen ungeschützten Internetrechnern wird eine Software installiert, die eine Fernsteuerung zulässt



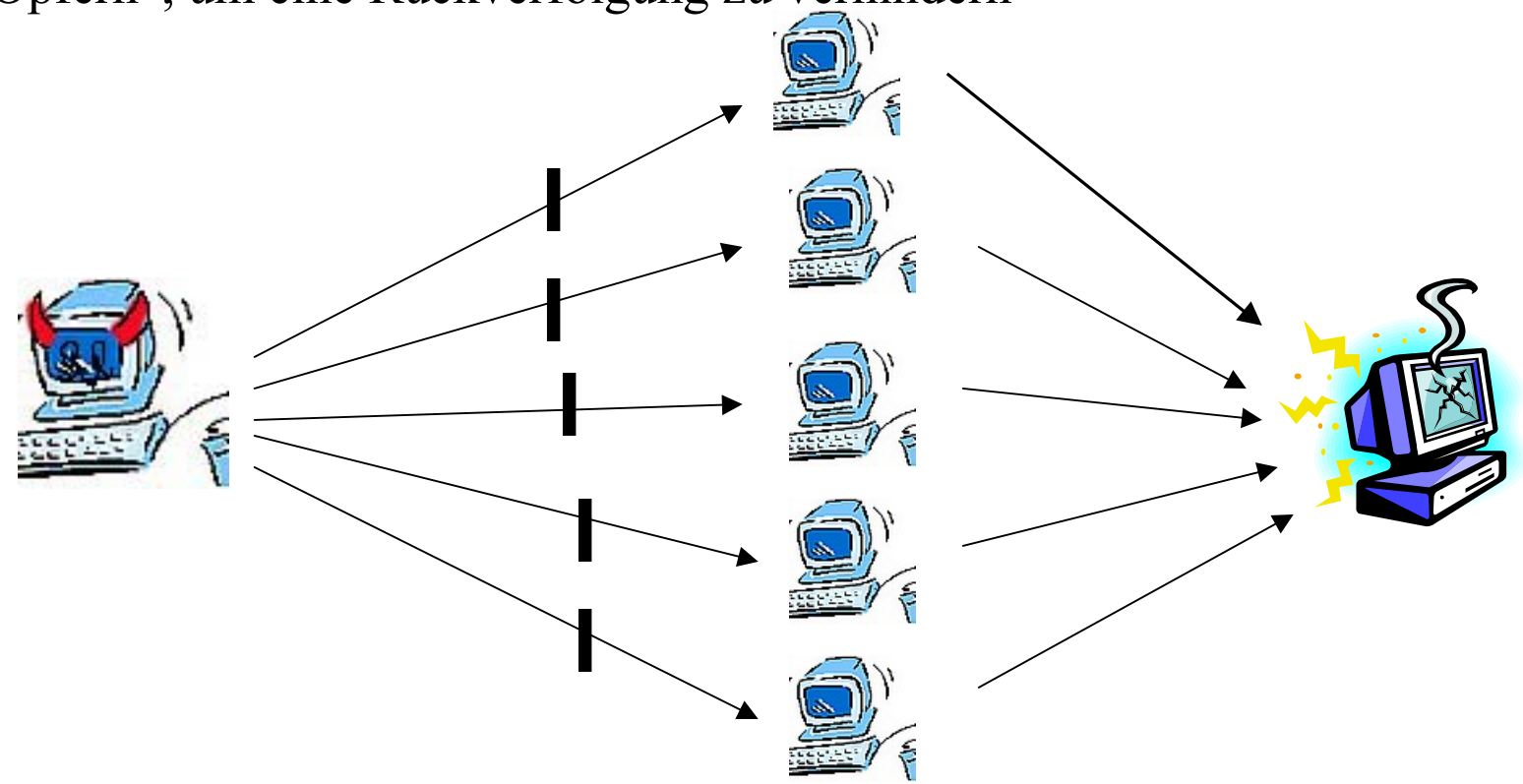
Beispiel: verteilter Denial-of-Service-Angriff (DDoS)(2)

2. Schritt: Der Angreifer veranlasst ein synchrones Aussenden von Anfragen an ein Zielsystem, was zur Überlastung führt



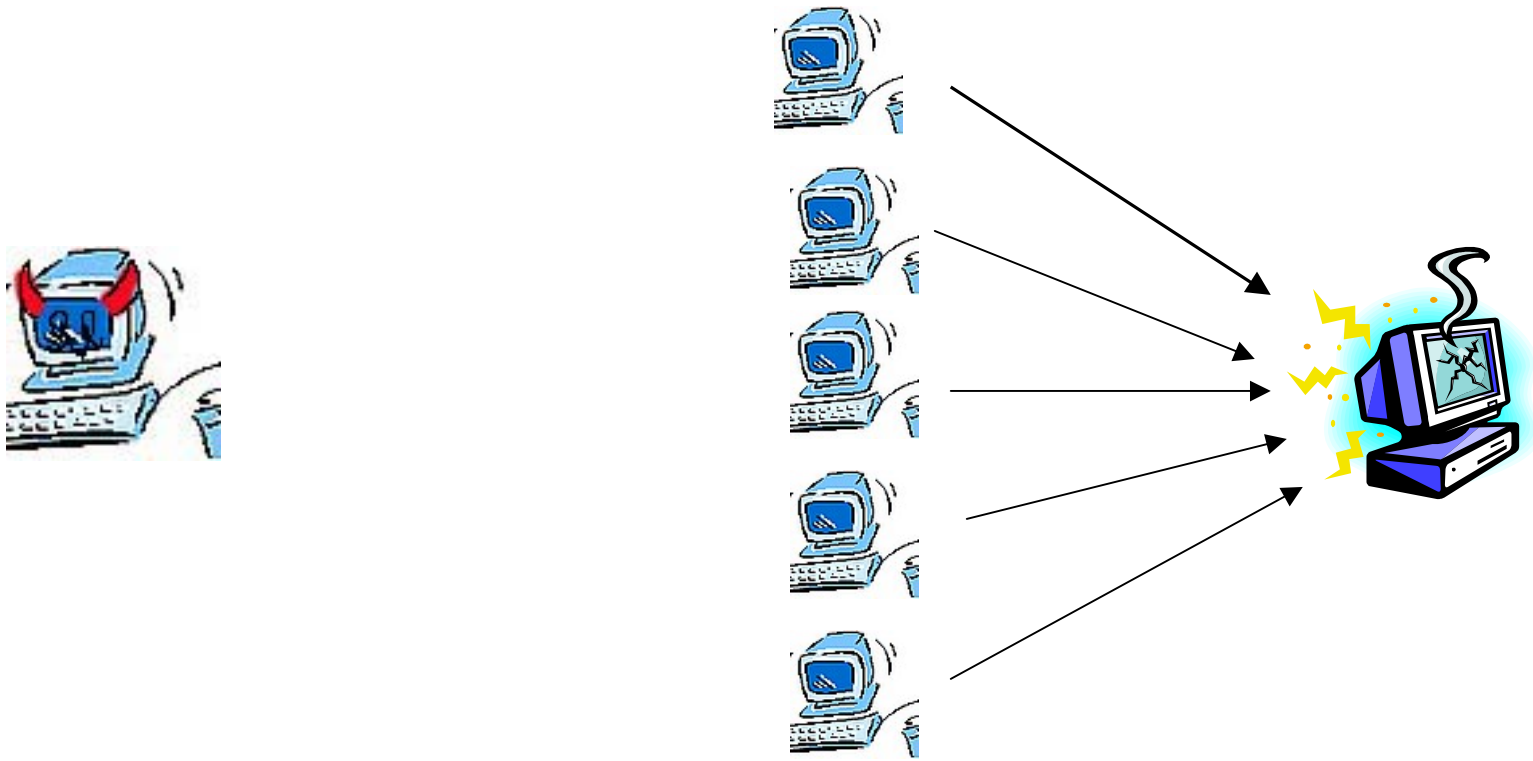
Beispiel: verteilter Denial-of-Service-Angriff (DDoS)(3)

3. Schritt: Der Angreifer trennt die Verbindung zu den ferngesteuerten „Opfern“, um eine Rückverfolgung zu verhindern



Beispiel: verteilter Denial-of-Service-Angriff (DDoS)(4)

3. Schritt: der Angreifer trennt die Verbindung zu den ferngesteuerten „Opfern“, um eine Rückverfolgung zu verhindern



Beispiel: verteilter Denial-of-Service-Angriff (DDoS)(5)

Bruce Schneier stellte folgenden „alltäglichen“ Vergleich an:

- Alice kann Bob nicht leiden



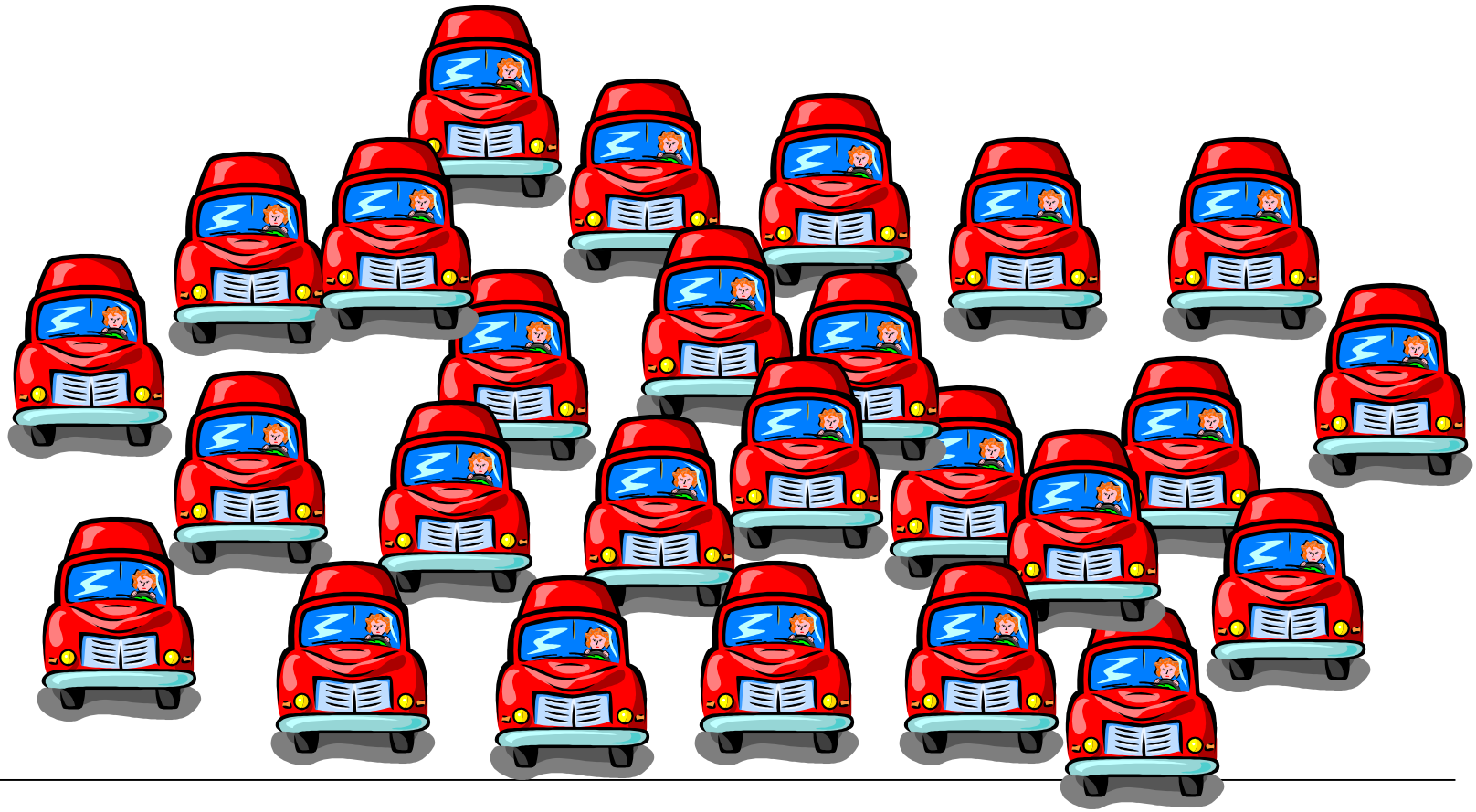


- Sie ruft bei 100 Pizza-Bringdiensten an und bestellt je eine Pizza „Salami“ für 20:00 Uhr



- Lieferadresse: **Bob´s Haus**

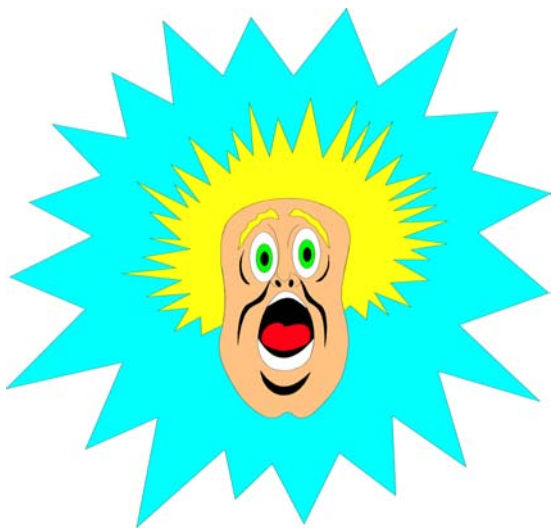
Um 20:00 Uhr fahren 100 Pizzaautos vor Bob´s Haus vor



100 Pizzas werden gleichzeitig bei Bob abgeliefert und 100 Pizzafahrer wollen ihr Geld



Bob dreht durch und „gibt den Geist auf“!





Hacker und Cracker

Wie gehen die Angreifer vor?

- **Passwort Angriffe** - Wörterbuchattacken, Brute force Attacken
- **Viren, Trojanische Pferde, Backdoors**
- **Sniffing** - Abhören der Leitung (unverschlüsselt übertragene Passwörter ermitteln)
- **IP-Spoofing** - Unterwandern einer adressbasierten Authentifizierung (u.a. Fälschen der IP-Adresse) => sehr komplexer Angriff
- **Wardriving (1)** - Systematische Suche nach ungeschützten Access Points, Abhören von Funk-LANs
  - Voraussetzungen sind leicht erschwinglich und schnell aufgebaut: Funk-LAN-Netzwerkkarten, Access Point

Wie gehen die Angreifer vor?

➢ Wardriving (2)

- Abhörsicherheit muss erst konfiguriert werden
- **WEP:** Mindestsanforderung an Verschlüsselung der übertragenen Daten, hält aber etwas hartnäckigeren Krackversuchen nicht stand!





Hacker und Cracker

- **Was motiviert Hacker, Cracker und Scriptkids?**

- Hacker, Cracker und Scriptkids haben gemeinsam, dass Sie sich für die Computer fremder Leute, samt Inhalt, interessieren:
- **Hacker** aus Sportsgeist, **Cracker** weil sie sich bereichern wollen,
  - sind auf ihrem Gebiet Spezialisten, beide verfügen über sehr viel technisches Know-how.
- **Scriptkids** probieren fertige Hackprogramme (Scripts) aus, sie sind nur bedingt Spezialisten.
- Wer zu wem gehört ist in der Szene heiß umstritten...

Legendäre Hacks und Cracks

3 Beispiele:

- **Kevin Mitnick (Condor)**
  Er besaß Tausende von Kreditkartennummern, hat sich trotzdem nie persönlich bereichert. Er wurde zu 35 Jahren Haft verurteilt, kam aber im Jahre 2000 wieder frei und arbeitet jetzt als Sicherheitsexperte.
- **Ehud Tenebaum**
  Hackte sich in 1000 Computer ein und nutzte sie für seine Zwecke. Er wurde vom FBI gefasst und nach Israel ausgeliefert. Anstatt bestraft zu werden, arbeitet er jetzt für den Mossad.
- **Vladimir Levin**
  beging 1994 den ersten elektronischen Banküberfall. Er drang in das Netz der US-Bank Swift ein und hob bei der First City Bank 15 Millionen Dollar ab. Allerdings buchte er das Geld auf sein eigenes Konto und wurde sofort gefunden.



Warum geht Sicherheit jeden an?

R|R|Z|N

- **Internet-Boom**
  - Heute sind ungleich mehr Nutzer im Internet als noch vor 10 Jahren
  - Standardmäßig ist ein Internet-Zugang für jeden Arbeitsplatzrechner vorhanden
- **Leistungsfähige Betriebssysteme**
  - Ein älteres Betriebssystem wie Windows 3.x bietet so gut wie keine Angriffspunkte
  - Windows XP dagegen hat alles, um es als Hacker-Plattform attraktiv werden zu lassen
- **Trends in der Software-Industrie**
  - Komfort kommt vor der Sicherheit!
  - Der Nutzer muss mittlerweile selbst dafür sorgen, dass seine Systeme sicher sind



Allgemeine Sicherheitsmaßnahmen

1. **Ausbildung der Anwender**
   - Entwicklung des Bewusstseins in Bezug auf die technischen Risiken
   - Zusammenschluss der Internet-Gemeinde (Diskussionslisten)

2. **Nutzung möglichst sicherer Systeme**
   - Behebung der aufgedeckten Schwachstellen in den Betriebssystemen und Programmen (Browser, E-Mail-Klienten, etc.)

3. **Überwachung der eigenen Systeme bezügl. Auffälligkeiten**



Warum geht Sicherheit jeden an?

Ziel ist die Erkennung und Vermeidung von unberechtigten Zugriffen auf den eigenen Computer

- Eindringlinge sollen von dem eigenen System und den eigenen Daten ferngehalten werden
- Erfolgte Einbrüche sollen erkannt und in ihrem Ausmaß beurteilt werden können
- Auch wenn keine extrem sicherheitsrelevanten Daten verarbeitet werden, schätzen wir es dennoch nicht, von Fremden ausgespäht zu werden, oder dass unser Rechner von Fremden für andere Tätigkeiten missbraucht wird

Grundlagen zur Internet-Kommunikation

Internet (1)

- **Kommunikationssystem ohne zentrale Steuerung und Kontrolle**
- **Paketvermittelte Verbindung:**
  - **Zerlegung einer Nachricht in Pakete, die unabhängig voneinander das Ziel erreichen**
  - **Verteilung der gesamten Leitungskapazität auf mehrere Benutzer**

- ***1979-83* Entwicklung des CSNET (Computer Science Research Network) für die amerik. Universitäten**
- **Ab *1982* Einführung des TCP/IP Protokolls**
- ***1984* der erste deutsche Anschluss - Uni Dortmund**

Internet (2)

- **Protokoll**
  - **Regeln und Konventionen über den Austausch von Informationen zwischen den Kommunikationspartnern mit dem Ziel einer vollständigen, fehlerfreien und effektiven Übertragung**
- **Firmeneigene Protokolle: z.B. DECnet, IPX, SNA**
- **Unabhängige Protokolle: TCP/IP**
  - **Zur Abwicklung der Datenübertragung im Internet**
  - **Ursprünglich zwei eigenständige Protokolle: TCP = Transmission Control Protocol und IP = Internet Protocol, mittlerweile eine ganze Protokollfamilie**
  - **„De-facto-Standard“, auf allen gängigen Plattformen implementiert**



Internet (3)

Das Internet ist die Gesamtheit aller Netzwerke und Computer, die über TCP/IP-Verbindungen erreichbar sind

Internet (4)

Internet-Adressen

Beispiel: Webserver des RRZN

Symbol. Name	www.rrzn.uni-hannover.de
Dezimale Notation mit Punkten zwischen den Bytes	**130 . 75 . 2 . 23**
Binär	10000010 1001011 10 10111

Jeder im Internet erreichbare Rechner ist durch eine numerische Adresse eindeutig identifizierbar = IP-Adresse

Ports (1)

- **Ohne Ports wäre eine Kommunikation über TCP/IP nicht möglich. Die „Nebenstellen“ erlauben es, dass mehrere Anwendungsprozesse über eine Internet-Verbindung gleichzeitig Daten austauschen können (vergleichbar mit Wohnungstüren in einem Mietshaus).**
  - Wenn sich eine Anwendung wie z.B. FTP an TCP/IP wendet, um eine Funktion auszuführen, sieht TCP/IP nicht den Namen der Anwendung sondern nur Zahlen:
    1. die Internet-Adresse des Servers, der den Dienst anbietet
    2. **Die Port-Nummer, über welche die Anwendung kommunizieren möchte**

Ports (2)

- **Um Konflikte zu vermeiden müssen die verschiedenen Applikationen (Services) unterschiedliche Ports verwenden**
- **Ein Port ist eine 16-Bit-Adresse (0 bis 65535)**
- **Für Standarddienste (WWW, Mail, FTP, ..) sind Portnummern vordefiniert**
- **Beispiel: ein Webserver wartet am Port 80 darauf, von einem Webbrowser angesprochen zu werden**

Ports (3)

Bekannte Portnummern:

20, 21 FTP
22 SSH
25 SMTP - Mail versenden
80 HTTP - WWW
53 DNS
79 Finger
110 POP3 - Mail empfangen
119 NNTP
143 IMAP4 - Mail empfangen

443 HTTPS
6667-8 IRC
137 Netbios Name Service
138 Netbios Datagram Service
139 Netbios Session Service
445 Microsoft DS

Ports (4)

- **Ports sind beliebte Angriffsziele, denn sie eignen sich hervorragend als Einfalltore.**
- **Aufspüren offener Ports:**
  - Der Angreifer setzt einen Portscanner ein, um geeignete Zielrechner-Adressen zu ermitteln und Informationen über das Zielsystem sammeln
  - Ein bestimmter Adressraum wird nach unsicheren Rechnern (z.B.:130.75.5.1 - 130.75.5.254)durchsucht
  - Der Portscanner stellt Anfragen an typische Portnummern und aktive Netzwerkdienste antworten
- **So werden gezielt unsichere Computersysteme ausgespäht, in die anschließend mittels bekannter Vorgehensweisen eingebrochen wird.**

Ports (5)

Portscanner LANguard (GFI)

Ports (6)

Weitere Vorgehensweise des Angreifers nachdem er mit einem automatisierten Portscanner Systeme mit Sicherheitslücken ermittelt hat:

- **Die bekannte Sicherheitslücke wird ausgenutzt.**
- **Der Angreifer verfügt über eine Eingabeaufforderung auf dem System, mit dem er den angegriffenen Rechner für seine Zwecke einsetzen kann.**

Unsichere Einstellungen im Betriebssystem

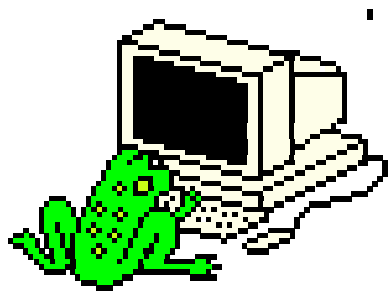
Allgemeine Risiken (1) - großes Angebot an offenen Ports

- Der Angriff auf ein Computersystem ist nur möglich, wenn Anwendungen gestartet sind, die eine Kontaktaufnahme von außen akzeptieren.
  - Unix, Novell Netware, Windows 95, 98, ME oder Windows NT/2000/XP bieten eigene **Netzdienste** an, z. B. die Freigabe der Platte oder auch Fax-, Modem- oder Druckerserverprogramme.

- Bei der Installation von Betriebssystemen werden oft Standarddienste aktiviert. (z.B.: Internet Information Webserver bei Windows 2000, FTP-Server oder Apache-Webserver bei Linux).
  - **80% der Anwender nutzen nur 20% der Möglichkeiten eines Programms**

Allgemeine Risiken (1) - großes Angebot an offenen Ports

Alle diese Dienste bieten offene Ports für die Kontaktaufnahme von außen an!



Allgemeine Risiken (1) - großes Angebot an offenen Ports

Schutzmaßnahmen:

- Generell gilt: nur das installieren, und nur die Dienste aktivieren, die auch wirklich benötigt werden
- Alle noch offenen nicht benötigten Ports schließen

Allgemeine Risiken (2) - mit Admin-Rechten ins Internet

- Der Benutzer hat auf seinem Rechner *Administrator*-Rechte
  - ➢ auch der Eindringling hat nun *Administrator*-Rechte
  - ➢ das hat fatale Folgen: dem Angreifer steht Tür und Tor für alle Gemeinheiten offen

Schutzmaßnahmen:

- Mehrere Benutzerkonten anlegen
  - ➢ für normales Arbeiten eingeschränkte Rechte für Systemzugriffe
- Kein Betriebssystem ohne Benutzerverwaltung einsetzen
  - ➢ der Angreifer hat in jedem Fall volles Zugriffsrecht auf dem Rechner

Allgemeine Risiken (3) - keine Sicherheitsupdates (Patches) eingefahren

- Auch Computersysteme, die von Experten mit Sorgfalt installiert wurden, benötigen regelmäßige Zuwendung.
- Die Produkte der Software- und Hardware-Hersteller sind nicht frei von Fehlern (Bugs).
- Hacker und Cracker suchen aus unterschiedlichsten Motiven nach diesen Sicherheitslücken, nutzen sie aus oder melden sie dem Hersteller.
- Irgendwie und irgendwann erfährt der Hersteller von der Lücke.
- Er behebt das Problem und verteilt eine Programmkorrektur (Patch).
- Sie installieren den Patch und sind auf der sicheren Seite.

Allgemeine Risiken (3) - keine Sicherheitsupdates (Patches) eingefahren

Schutzmaßnahmen:

- Vorsicht bei Installationen **Out-of-the-Box**: schon während der Installation sollten die notwendigen Aktualisierungen eingespielt werden.
- Überprüfen Sie in regelmäßigen Abständen ob neue Service Packs und Hot fixes (Patches) zur Verfügung stehen z.B.
  - **Windows:** ***http://www.microsoft.de/security/***,
  - **Windows 2000/XP**: automatischer Updateservice
  - **Linux :**von der Webseite für die jeweilige Distribution ist meist ein automatisches Sicherheits-Update möglich

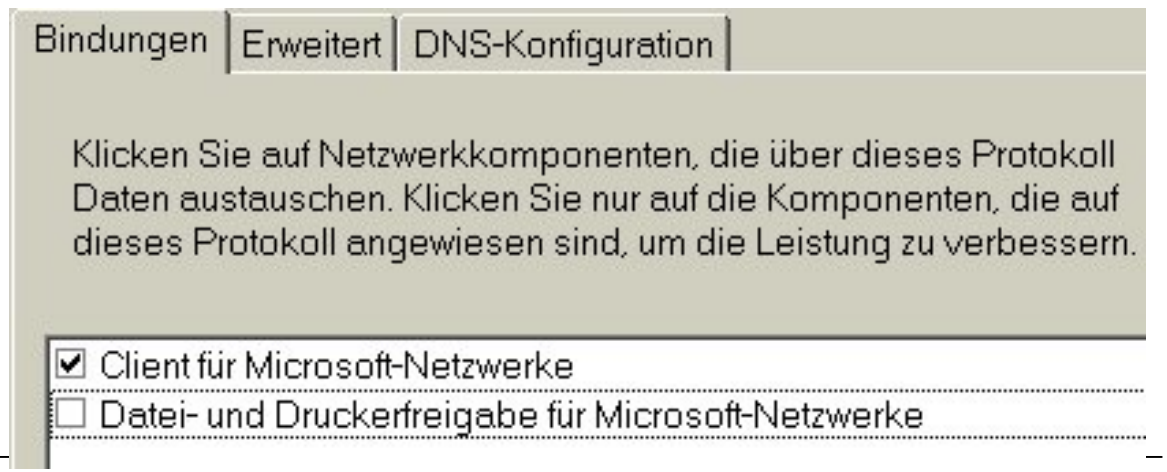
Allgemeine Risiken (4) – Datei und Druckerfreigabe

- Sinn und Zweck der "Datei- und Druckerfreigabe für Microsoft-Netzwerke" ist es, Daten zwischen Rechnern in einem lokalen Netz auszutauschen und Drucker gemeinsam zu benutzen
  - SMB-Protokoll = Server Message Block
- Sobald eine Verbindung zum Internet besteht, sollten über das entsprechende Interface keine Freigaben vorhanden sein
- Freigaben lassen sich leicht ermitteln
  - Portscanner: Freigabedienste melden sich auf TCP-Port 135-139!! unter Windows 2000, XP auch unter 445

Allgemeine Risiken (4) – Datei und Druckerfreigabe

Abhilfe:

- Die Bindung des Netzwerkadapters, mit dem man ins Internet geht (z. B. DFÜ-Adapter), an die Datei- und Druckerfreigabe muss unbedingt aufgehoben sein
  - **<u>Beispiel</u>: Win9x im DFÜ-Netz: Unter TCP/IP -> DFÜ-Adapter > Bindungen, den Haken bei "Datei- und Druckerfreigabe für Microsoft-Netzwerke" entfernen**



Gefahrenquelle: Surfen im Internet



Gefahrenquelle: Surfen im Internet

- In seinen Anfängen bestand das Web im Wesentlichen aus formatiertem Text mit eingebundenen Bildern
  - ➢ geringes Sicherheits-Risiko beim Betrachten der Seiten

- Mittlerweile kommen jedoch immer weniger Web-Sites ohne eingebaute Skripte, menügesteuerte Java-Applets oder gar multimedial aufbereitete Präsentationen aus, dazu benötigen sie erweiterte Browser-Funktionen wie
  - ➢ **JavaScript**
  - ➢ **Java**
  - ➢ **ActiveX**



Gefahrenquelle: Surfen im Internet

R|R|Z|N

- **JavaScript, Java, ActiveX** erfordern es, dass fremder Code auf dem Rechner der Besucher ausgeführt wird. Sicherheitsmechanismen, die verhindern sollen, dass solcher Code auf dem Rechner Schaden anrichtet sind zwar vorhanden, aber:

  Es gibt immer wieder Sicherheitslücken durch **Programmierfehler**, die diese Einschränkungen aushebeln

  - Beeinträchtigung der Funktionstüchtigkeit, z.B. Absturz beim Aufruf bestimmter Seiten
  - **Sicherheitsrisiko** => über speziell präparierte Web-Seiten lassen sich dann **Dateien auf der Festplatte lesen und manipulieren** oder **Viren einschleusen**
    - **Programmierfehler lassen sich durch Installation der aktuellen Browser-Patches beseitigen**
    - **Risiken prinzipieller Natur lassen sich nur durch Deaktivieren der zugehörigen Optionen vermeiden**

Java

- Java ist eine plattformübergreifende Programmiersprache (Sun)
- Java wird auf Webseiten in Form kleiner Applets, die auf dem Rechner ablaufen ausgeführt
- Die Browser bieten hierfür eine Laufzeitumgebung (=JVM, Java Virtual Machine) an, die wie eine abgeschlossene Sandbox wirken soll
  - es sind keine Zugriffe auf lokale Ressourcen wie Dateien oder Programme erlaubt und
  - die Applets dürfen grundsätzlich keine Betriebssystemfunktionen aufrufen
  - Sicherheitslücken entstehen durch mögliche Fehler bei der Implementierung in ein Produkt
    - z.B. wird das Aufzeichnen von Sitzungsinformationen ermöglicht

Javascript

- Javascript ist eine von Netscape für das WWW entwickelte Scriptsprache (bei Microsoft wird sie aus lizenzrechtlichen Gründen JScript genannt)
- Es dient dazu dynamische Effekte zu erzeugen, die Navigation zu erleichtern etc.
- Es ist in der Vergangenheit häufig die Quelle diverser Sicherheitslücken gewesen, die zum Ausspähen lokaler Daten benutzt wurden (z.B. durch Implementierungsfehler)

ActiveX (1)

- Von Microsoft eingeführte sprachunabhängige Software-Technologie, die unter anderem ermöglicht, dass Webbrowser Office-Dateien und interaktive Inhalte anzeigen können

- Sie beschränken sich auf MS Windows-Systeme und vorwiegend auf den Internet Explorer
  - ➢ ActiveX sorgt dafür, dass Windows-Anwendungen mit dem Internet zusammenarbeiten

ActiveX (2)

Gefahrenquelle ActiveX:

1. Automatischer Download eines neuen ActiveX-Controls beim Aufruf einer Webseite
   - Läuft das ActiveX-Programm erst einmal, dann ist sein Funktionsumfang in keiner Weise eingeschränkt oder kontrollierbar. Das ActiveX-Programm läuft mit allen Rechten des angemeldeten Benutzers - ohne jede Einschränkung! Es ist demnach ein leichtes, private oder sicherheitsrelevante Daten auszulesen, zu löschen, zu manipulieren, den Rechner umzukonfigurieren, einen Virus oder ein Trojanisches Pferd zu installieren.

2. Aktivierung bestehender ActiveX-Controls durch geschickt programmierte Webseiten meistens via Jscript oder VBS

Der Browser

- Internetsurfen ohne Browser ist wie Autofahren ohne Auto
  - » es funktioniert einfach nicht

- Mit Hilfe eines Web-Browsers können Sie Daten aus dem weltweiten Netz abrufen und auf Ihrem PC anzeigen und verarbeiten
- Die bekanntesten Browser sind
  - » **Netscape Navigator**
  - » **Microsoft Internet Explorer**
  - » **Opera**
  - » **Mozilla**

Netscape 7.1

- Nachfolgeversion des Netscape Communicators, hervorgegangen aus dem Mozilla-Projekt
- Leider hoher Arbeitsspeicherverbrauch (beruht auf enger Anbindung an AOL), besonders in der Ladephase, dadurch relativ langsames Arbeitsverhalten

Sicherheit:

- Detaillierte Anleitung für eine sichere Konfiguration von Netscape findet man bei Heise Security
  - **c't-Browsercheck**

  http://www.heise.de/security/dienste/browsercheck/anpassen/nc70/

Microsoft Internet Explorer

- Derzeit mit über 80% Marktführer
- Aktuelle Version: 6.0 SP1

Sicherheit:

- Da der IE immer wieder Ziel von Virusattacken aufgrund auftretender Sicherheitsmängel wird, gilt:

  Unbedingt stets die neueste Version mit den neuesten Korrekturen (Patches) einsetzen!

- Ermöglicht Sicherheitseinstellungen über das Zonenkonzept
- **ActiveScripting** sollte deaktiviert werden
  - damit wird leider auch Javascript abgeschaltet. Kompromiss: entsprechende Server in die vertrauenswürdige Zone eintragen oder **c´t-IE Controller** einsetzen
- Detaillierte Anleitung für sichere Einstellungen im IE findet man bei Heise Security => **c't-Browsercheck**

  http://www.heise.de/security/dienste/browsercheck/demos/ie/

Viren, Würmer und Trojaner



Viren, Würmer und Trojaner

R|R|Z|N

Viren:

- Sind zumeist sehr kleine Programme, die in der Lage sind sich an andere Programme zu hängen, sich so zu reproduzieren und zeitgesteuert Schäden zu verursachen
- Verbreitet sind besonders die **Macroviren**, die in den sehr leistungsfähigen Macrosprachen von hochentwickelten Anwendungsprogrammen (MS Office) verfasst sind und sich in den Dokumenten (.doc, .xls) verbergen

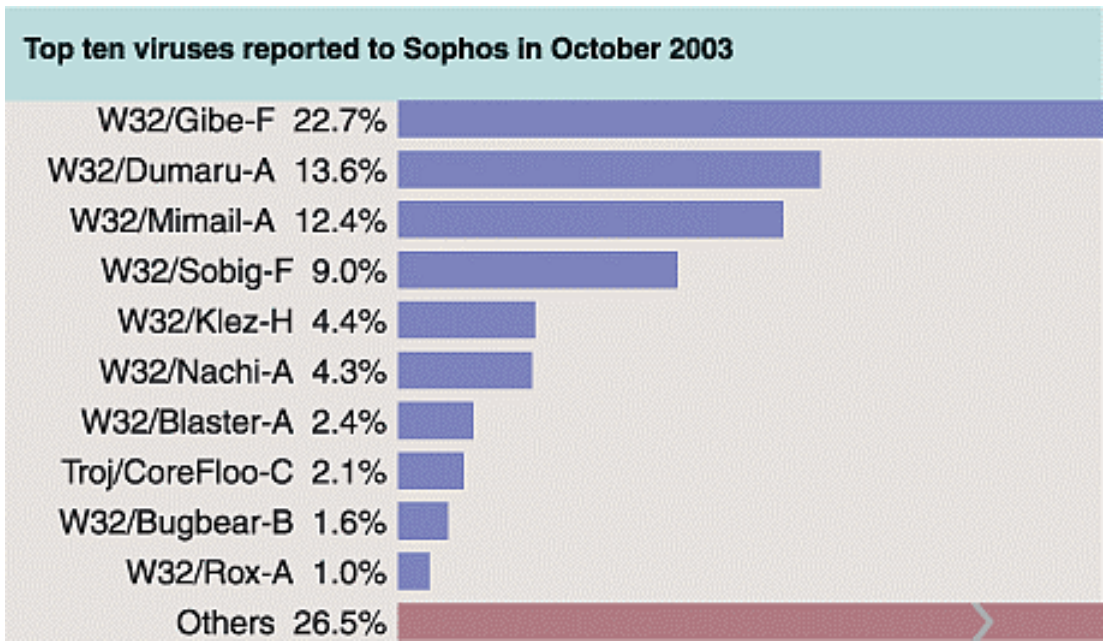
Würmer:

- Ein Wurm braucht im Gegensatz zum Virus keinen Wirt! Denn er besteht aus einem eigenständigem Programm, welches auf dem Rechner selbstständig Prozesse startet – er repliziert (kopiert) sich auf andere Rechner, z.B. über E-Mail, um dort sein Unwesen weiter zu treiben

Trojanische Pferde:

- Scheinbar harmlose Programme, die sich nicht reproduzieren, sondern sich in ein Rechnersystem einschleusen, es kompromittieren und dort Daten ausspähen oder den Rechner fernsteuern

Virenstatistik der Fa. Sophos (Oktober 2003)





(Juni 2003) Bugbear-B:

- **verbreitet sich über E-Mail-Anhänge und Netzwerkfreigaben**
- **Die Attachments haben doppelte Erweiterungen, wobei die zweite Erweiterung EXE, SCR oder PIF ist (z.B. .txt.pif)**
- **lässt ein Programm im Hintergrund laufen, das versucht, Antiviren- und Sicherheitsprogramme zu beenden**
- **eine Komponente zum Mitschneiden von Tasteneingaben zeichnet die Tastenfolgen im Speicher auf**
- **W32/Bugbear-B öffnet Port 1080 und wartet auf Befehle von einem Remote-Rechner. Je nach den gesendeten Anweisungen kann ein Remote-Benutzer folgendes auf dem Computer des Opfers versuchen:**
  - **Ausspionieren von Kennwörtern**
  - **Download und Start einer Datei**
  - **Suchen, Löschen, Ausführen, Kopieren von Dateien**
  - **Ausspionieren von Informationen, wie Benutzername, Prozessortyp, Windows Version, Speicherdaten**

(August 2003) W32/Blaster alias Lovsan

- Nutzt zur Verbreitung eine Schwachstelle in Windows Systemen (hauptsächlich Win 2000/XP)
- Bei Windows XP Rechnern führt die Blaster-Infektion häufig zu einem wiederholten Reboot des Systems
- Der Wurm sucht nach offenen Ports (135), wird er bei einem System fündig, wird der Rechner infiziert
- Die Scan-Aktivitäten belasten im hohen Maße das Netzwerk
- Zur nachhaltigen Beseitigung des Wurms benötigt man
  1. Virenscanner (Removal-Tool)
  2. Microsoft Patch zum Schließen der Sicherheitslücke

(August 2003) W32/Nachi

- versucht auf Windows 2000 und Windows XP-Rechnern den Microsoft-Patch, welcher die DCOM RPC-Schwachstelle behebt, zu installieren
- versucht außerdem den Blaster-Wurm zu entfernen, diese Funktion ist aber teilweise fehlerhaft, so dass bei einem Befall allgemeine Probleme bei der Rechnerbedienung auftreten können
- verursacht sehr viel Netzverkehr und verlangsamt dadurch den Rechner und insbesondere die Netzverbindungen

(August 2003) W32/Dumaru-A

- verbreitet sich über E-Mail
- hat als angebliche Absender-Adresse "security@microsoft.com" und behauptet, in seinem Anhang einen wichtigen Microsoft-Patch zu beinhalten
- Das Ausführen des Anhangs liefert nicht wie erwartet den Patch, sondern den Wurm
- Verbreitung des Wurms ist sehr hoch, da viele Anwender, die durch den Blaster-Wurm verunsichert sind, den Anhang ausführen.
- Microsoft verschickt grundsätzlich keine ausführbaren Dateien oder Patches per E-Mail



Viren, Würmer und Trojaner

(August 2003) Sobig-F

- verbreitet sich über E-Mail und Netzwerkfreigaben unter Windows
- es muss explizit das Attachment ausgeführt werden. Die Namen der Attachments und Betreffszeilen variieren
- Fälscht sowohl Absender- also auch Empfängeradressen (installiert eigene SMTP-Engine)
- Besonders E-Mails mit Attachments, die von vermeintlich bekannten Adressen kommen, sind also mit Vorsicht zu genießen.
- Mail-Server von Institutionen werden durch das hohe Mailaufkommen stark belastet

Viren – Bekämpfung und Schutzmaßnahmen

- Einsatz eines möglichst aktuellen Virenscanners mit Hintergrundwächter
- Regelmäßige Aktualisierung der Virendatenbank

Viren – Bekämpfung und Schutzmaßnahmen

Sophos Downloadseiten des RRZN:

- **Infos und Download zu Virenschutz in der UH**
- **Antiviren-Software: Sophos Antivirus**

http://www.rrzn.uni-hannover.de/security/tools/Sophos1.html

- **für Mitglieder der UH kostenlos**

- **Wichtig**: immer gleich nach dem Download die heruntergeladene Version aktualisieren, damit der Scanner stets die aktuellsten Virensignaturen hat
- **Sophos-Abonnenten** erhalten bei besonders gravierenden Virenattacken eine Nachricht vom RRZN, mit dem Hinweis ihren Virenscanner umgehend zu aktualisieren. Der angegebene Link verweist direkt auf eine Download-Seite der Fa. Sophos

Infiziert - und nun?



Infiziert - und nun?

Trotz aller Vorsichtsmaßnahmen kann es passieren, dass es Sie trotzdem erwischt. Und dann?

- Administrator benachrichtigen, der über eine saubere Notfalldiskette mit Virenscanner verfügt
- Virenscanner aktualisieren

  1. Neueste Monatsversion =>

  http://www.rrzn.uni-hannover.de/Security/Tools/sophos/Sophos1.html

  2. Neueste Virenkennungen =>

  http://www.sophos.de/support/faqs/usingides.html
- Aktuelle Virenwarnungen der RRZN-Security lesen

  http://www.rrzn.uni-hannover.de/Security/

Was ist ein Trojaner?

- Trojaner sind eigenständige Programme mit mehr oder weniger destruktiver Energie
- Die Bezeichnung Trojanisches Pferd geht zurück auf die Homer´sche Odyssee
- Mit ihrer Hilfe gelingt es, die vollständige Kontrolle über einen infizierten PC zu erhalten und diverse Funktionen auszuführen – eine Art Fernsteuerung:
  - Kontrolle über das Dateisystem und die Peripherie des Rechners
  - Keylogger-Funktion zum Ausspähen von gerade eingegebenen Kennwörtern
- Der Trojaner lausch auf einem bestimmten Port auf Verbindungsaufnahme
- Er besitzt eine Autostart-Funktion, falls der Rechner gebootet wird

Wie kommt man zu einem Trojaner?

- Durch versteckte, aktive Inhalte von WWW-Seiten, die aufgrund nicht sicher eingestellter Internet-Browser, Dateien auf Ihre Festplatte kopieren,
- durch kostenlose Software, die zum Download im Internet angeboten wird und nicht nur das ausführt, was sie verspricht,
- durch E-Mail Anhänge, die nach Ausführung ein Trojanisches Pferd auf Ihrem Rechner installieren
- durch versteckte, aktive Inhalte in HTML-E-Mails.

Trojaner erkennen und abwehren

- **Virenscanner:** gute Virenjäger erkennen die meistenTrojaner (Voraussetzung: ein regelmäßiges Aktualisieren der Virendatenbank)

- **Anti-Trojan Tool**: funktioniert ähnlich wie ein Virenscanner. Da die Autostart-Mechanismen vieler Trojaner bekannt sind, werden die verdächtigen Schlüssel in der Registrierungsdatei gescannt und nach modifizierten Dateien gesucht
  - Ants 2.1, http://www.ants-online.de (kostenfreier Scanner)

- **Personal Firewall**: verhindert den bzw. warnt vor dem Verbindungsaufbau des Trojaners zum Internet

Was ist ein Hoax?

- Scherz-Mails“ mit Warnungen vor vermeintlichen Viren
- Treffen im Allgemeinen unaufgefordert ein
- Fordern dazu auf, die Mail an alle Freunde und Bekannte weiter zu schicken
- Einige fordern den Nutzer dazu auf bestimmte Dateien zu löschen, weil sie angeblich virenverseucht sind, z.B.:
  - Sulfnbk.exe und
  - Jdbmgr.exe
- Wenn man sich nicht sicher ist:

  => Hoax-Info-Service der TU Berlin

  http://www.tu-berlin.de/www/software/hoaxlist.shtml



Viren, Würmer und Trojaner

Auszug aus einer Hoax-Warnmeldung des BSI:

Name: ACE-HoaxAlias: Mobile Phone Virus Hoax, Cell Phone hoax

----

Betreff: Handy-Virus

Wenn jemand einen Anruf bekommt wo man auf dem Display "ACE-?" sieht, NICHT ABHEBEN, SONDERN SOFORT ABWEISEN!
Es ist ein Virus, welcher alle IMEI und IMSI Daten im Telefon und von der SIM Karte löscht. So kann das Gerät nicht mehr zum Netz eine Verbindung aufnehmen und ist nicht mehr verwendbar. Diese Information hat Motorola und Nokia bestätigt und ist auch auf der Homepage von CNN nachzulesen. 3 Millionen Geräte sind auf diesem Weg schon zerstört worden. Bitte schicken Sie dieses Mail an alle Bekannten weiter.
Viele Grüße

- Die Warn-E-Mail taucht in mehreren Varianten und Sprachen auf.
- Anmerkung: Es existiert kein Virus, der Mobiltelefone zerstören kann.

E-Mail: Einstellungen und gefährliche Anhänge

Die häufigste Art und Weise der Virenverbreitung ist die E-Mail:

1. als **E-Mail-Anhang** (engl. = Attachment), der vom Benutzer mit Doppelklick gestartet werden muss,

2. als speziell formatierte **HTML-E-Mail**, wobei der Virus bereits beim Lesen der Mail aktiv werden kann.

E-Mail-Anhänge (Attachments)

- Anhänge sind nicht der eigentliche Text der E-Mail, sondern Dateien mit noch mehr Text, Bildern oder Ton.
- Sobald der Anhang geöffnet wird, verbreiten sich die Viren und richten Schaden auf dem Computer an.
- Solange man ihn nicht öffnet, passiert auch nichts.

Gefahren:

- Geschickte Formulierungen und schillernde Namen im E-Mail-Text wecken die Neugierde (z.B. Clinton_Lewinsky_SpyCam.avi).
- Der Absender der Mail ist vermeintlich ein Bekannter, dadurch wird ein trügerisches Vertrauen erzeugt.
- Unsichere Einstellungen im E-Mail-Programm veranlassen ein automatisches Öffnen der E-Mail-Anhänge.

Wie erkenne ich schädliche Anhänge?

- Anhänge haben eine Dateinamenerweiterung (Teil des Dateinamens nach dem Punkt).
- Daran lässt sich erkennen, welcher Dateityp im Anhang steckt.
- Viren verstecken sich vornehmlich in Dateien der Typen

  .**VBS, .EXE, .COM, .SCR, .BAT, .PIF** .

Problem:

- **Ausblenden bekannter Dateiendungen bei Windows** (Standard nach Installation)

- **Beispiel**: anna-kournikova**.jpg.vbs**-Virus
  - nutzte aus, dass viele die Dateinamen- Erweiterungen nicht anzeigen lassen
  - als Anhang der E-Mail erschien dann anna-kournikova.**jpg** **(**harmloses Bild) - viele betrachteten den Anhang als harmlos und konnten nicht widerstehen - der Virus schlug zu:
    - verschickte sich an alle Einträge im Adressbuch
    - richtete Schaden auf der Festplatte an

Schutzmaßnahmen:

- **Dateienamen-Erweiterungen bei Windows anzeigen**

  - Wenn Windows so eingestellt ist, dass es keine Dateierweiterungen anzeigt, sollte das folgendermaßen geändert werden:
    - Windows-**Explorer** öffnen
    - dort unter **Ansicht/Extras** den Punkt **Ordneroptionen** auswählen
    - unter **Ansicht** das Häkchen bei **"Dateinamenerweiterungen bei bekannten Dateitypen ausblenden"** entfernen

Dateinamenerweiterungen .doc, xls, ppt, ...

- In Microsoft Office Dateien versteckte **Macros** sind oft Träger von Computerviren.

  - Erhalten sie eine E-Mail mit einem solchen Attachment, öffnen Sie es nicht vor einem Viren-Check.
  - Selbst sollten Sie die Office-Dokumente z.B im .pdf-Format verschicken (kann keinen ausführbaren Programm-Code enthalten).

Kein Garant für ein sauberes E-Mail-Attachment: der Absender ist ein/e Bekannte/r ...

- denn er/sie könnte schon auf den Virus reingefallen sein:

  der Virus benutzt dessen E-Mail Adressbuch und verschickt sich automatisch in dessen Namen.

  - Beispiele: Sircam-A, Klez-h, Bugbear-A, ..,Sober-A,..

Schutzmaßnahmen:

1. Kein unüberlegtes Doppelklicken auf das Attachment, auch bei bekannter Absender-Adresse

2. Mail-Programm so einstellen, dass Anhänge nicht automatisch geöffnet werden

3. Die Dateienamen-Erweiterungen einblenden und die wichtigsten Erweiterungen kennen

Outlook Express 6.0 SP1 sicher konfigurieren

- Bei der Einrichtung der Mailkonten sollte niemals das Zugangspasswort mitgespeichert werden – dies verhindert den automatischen Zugriff auf den Mailer
  - ➢ Automatismen bieten Komfort, dienen aber oft den Viren
- Einstellungen unter Extras | Optionen | Registermenü Sicherheit
  - ➢ Auswahl auf *„Eingeschränkte Sites“*
    - schließt AktiveX-Controls aus, Active Scripting ist noch aktiv
    - Bislang benötigen alle Viren und Würmer **ActiveX-Unterstützung**
  - ➢ *„Warnung anzeigen, wenn andere Anwendungen versuchen, E-Mail unter meinem Namen zu versenden“*
    - schützt vor missbräuchlicher Verwendung durch Mass-Mail-Viren
- Im Registermenü *Allgemein*: alle Häkchen entfernen
- Im Registermenü *Lesen*: deaktivieren von *“Nachrichten im Vorschaufenster automatisch downloaden“*

Anhänge vor dem Öffnen speichern und auf Viren prüfen

HTML-E-Mail

- HTML ist die Programmier-Sprache, in der Inhalte für das World Wide Web geschrieben werden.

- HTML kann nicht sichtbare ausführbare Bestandteile enthalten, die erhebliche Gefahren und Sicherheitsrisiken für den Empfänger bergen.

Gefahren:

- schon beim Lesen der E-Mail wird über den HTML-Code eine Web-Adresse kontaktiert und Viren-Code von dort nachgeladen:
  - Infizierung des Rechners mit Viren und Trojanern ohne E-Mail-Anhänge,
  - eigener Virenscanner ist wirkungslos, da der Virus immer wieder neu übertragen wird.

Außerdem: HTML wird oft in unerwünschten Werbesendungen benutzt

- Dem Leser werden unsichtbare Bilder der Größe eines einzelnen Bildpunktes untergeschoben, die erst beim Lesen der E-Mail von einer Webseite nachgeladen werden.
- mit Hilfe solcher Ein-Pixel-Bilder ist es möglich, festzustellen ob und wann die E-Mail gelesen wurde und Informationen zum Surfverhalten der Leser zu übertragen.

Schutzmaßnahmen:

- Wenn möglich, keine HTML Mail empfangen
  - Ausschalten des Empfangs von HTML-Mails gelingt in **Pine**, **Outlook XP**, **Outlook Express 6.0 SP1**
- Vorschau im E-Mail-Programm ausschalten
- selbst keine HTML-Mail verschicken
  - HTML wird immer häufiger als Kriterium zum automatischen Ablehnen von E-Mail eingesetzt
  - Bei HTML-Mail müssen größere Datenmengen übertragen werden

Outlook Express 6.0 SP1 sicher konfigurieren

- nur noch Mails im Textformat versenden:
  - ➢ Extras > Optionen > Senden
    - Sende-Format auf *„Nur-Text“* umstellen.
- Automatisch empfangene HTML-Mails in reines ASCII-Format umwandeln:
  - ➢ Extras > Optionen > Lesen
    - Menüpunkt *„Alle Nachrichten als Nur-Text lesen“*
- Verzicht auf Briefpapier und Visitenkarte:
  - ➢ Extras > Optionen > Erstellen

Versenden vertraulicher Informationen:

- **Frage: könnten Sie den Inhalt der E-Mail auch getrost per Postkarte verschicken?**



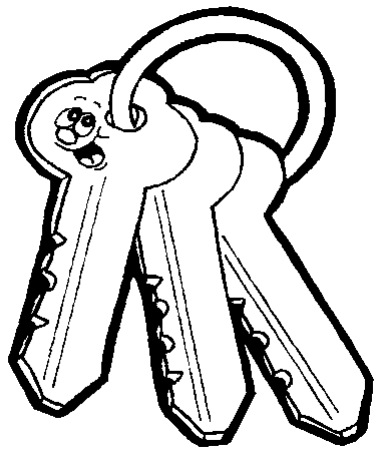
- Wenn **nein**, sollten Sie eine Verschlüsselungssoftware verwenden, z.B. GnuPG.

Passwörter

Passwörter

- **Als Zugangskontrolle zu Systemressourcen unerlässlich, wie der Schlüssel zu Ihrer Wohnung**
  - **Sorgfältiger Umgang mit Passwörtern**
  - **Auswahl eines „sicheren“ Passwortes**

  => Sind knackbar (Wörterbuchattacken, Brute-force Methode)





Passwörter-Tipps

R|R|Z|N

- Passwortlänge: 8 - 10 Zeichen
- Möglichst viele verschiedene Zeichen, auch Zahlen, Sonderzeichen, sowie Groß- und Kleinschrift verwenden
- Sollte keine persönlichen Daten enthalten
- Sollte nicht in einem Wörterbuch zu finden sein, auch keine Fremdsprachen
- Sind schnell einzutippen, damit sie nicht ausgespäht werden können
- Aber trotzdem muss das Passwort leicht zu merken sein, damit es nicht aufgeschrieben werden muss
- Tipp: Anfangsbuchstaben der Wörter eines Satzes, Liedes oder Mottos:
  Von einem der auszog das Fürchten zu lernen = V1dadF-l
  (einem=1, zu= -)
- Eigennamen in umgekehrter Reichenfolge oder Permutationen mit vorangestellter oder angehängter Zahl ist keine gute Idee => Crack-Programme wie **John the Ripper** lösen so etwas in Sekunden auf



Umgang mit Passwörtern

- Passwörter sollten alle 6 Monate oder früher geändert werden
- Initialpasswörter sind unbedingt bei der ersten Benutzung zu ändern
- Keine alten Passwörter wieder verwenden
- Passwörter nicht abspeichern, z.B. Windows
- Passwörter geheim halten, nicht in Web-Formularen oder in E-Mails verbreiten
- Passwörter sollten nicht aufgeschrieben werden

  Ausnahme: Hinterlegung in einem verschlossenen Couvert im feuersicheren Safe
- Sie gehören weder unter die Tastatur noch in die oberste Schreibtischschublade
- Passwörter sind zu schützen gegenüber Methoden des social engineering und des trashing (Durchsuchen des Mülls eines Instituts)



Passwörter - SSH

- SSH = Secure Shell dient als Ersatz für telnet, rsh, rlogin zum Einloggen auf entfernte Unix-Rechner
- Passwort wird beim Anmeldevorgang verschlüsselt übertragen => verhindert das einfache Auslesen (Sniffing) des Passwortes
- Genauere Informationen im Vortrag: ssh, e-mail etc
  (Marquard/Obendorf, RRZN)

Installieren einer Personal Firewall

Was ist eine Firewall:

- Sie kontrolliert die Internetverbindung indem sie die Netzwerkströme anhand von Zugriffsregeln filtert.
- Die Schutzfunktion ist in 2 Richtungen wirksam:
  - von Außen nach Innen (verhindert unkontrollierten Zugriff aus dem Internet und blockt die Sicht auf die zu schützenden Rechner)
  - von Innen nach Außen (versperrt z.B. Trojanern die Kontaktaufnahme ins Internet)
- Die Firewall regelt welche Anwendungen über das Internet kommunizieren dürfen.

Wogegen schützt eine Firewall nicht?

- **Mail-Würmer** und **Computerviren**
  - ➢ werden über zugelassene Wege transportiert
    - E-Mail, WWW, ...

Personal (Desktop) Firewall:

- Software, die ähnliche Funktionen wie eine „große“ Firewall erfüllt, aber auf der Hardware, die sie schützen soll installiert wird.
- für den privaten Gebrauch kostenlos sind z.B. die Produkte
  - Kerio Personal Firewall
  - Zone Alarm
  - Outpost
- Beispiele für kostenpflichtige Software:
  - Norton Personal Firewall 2003 (Symantec)
  - Norman Personal Firewall
  - Zone Alarm Pro



Installieren einer Personal Firewall

Einsatzaspekte für eine Personal Firewall (Abwehrleistung)

- **Schutz gegen Portscanning?**
  - Wenn das System keine nennenswerten Sicherheitslücken aufweist, unproblematisch => per se nicht gefährlich, nur lästig ..
  - Allerdings blockiert die PFW das Ausspähen unsicherer Computersysteme
- **Schutz vor Trojanern?**
  - Wenn ein Trojaner (trotz Virenscanner?) auf das System gelangt ist, erfolgt eine Warnmeldung wenn er eine Verbindung nach außen eröffnet
  - Aber **Achtung**: Viele Trojaner können bereits eine Personal Firewall deaktivieren
- **Schutz vor vergessenen Laufwerks-Freigaben?**
  - Ja, aber warum werden diese nicht gleich abgestellt?
- **Schutz vor Sicherheitsproblemen der Software und des Betriebssystems?**
  - Die Personal Firewall bringt hier Schutz, enthebt aber den Anwender nicht von der Aufgabe, Korrekturen für sein System einzufahren

LanGuard security Scanner (GFI)

Vorgehensweise nach Installation einer Personal Firewall

- Die Firewall muss lernen, was erlaubt ist und was nicht
- Besteht hinsichtlich der angeforderten Ports Unklarheit, sollte zunächst blockiert werden
- Gerade im Lernmodus sind die vermehrten Rückfragen oftmals lästig und beeinträchtigen den Komfort
- **Hier ist Sorgfalt geboten!** Andernfalls besteht die Gefahr, dass in der Hektik des Alltags vorschnell alles durchgelassen wird, nur um von der ständigen Fragerei der Personal Firewall nicht behelligt zu werden



Installieren einer Personal Firewall

R|R|Z|N

Eine kleine Auswahl empfehlenswerter Personal Firewall Lösungen (für den Privatgebrauch kostenfrei):

Outpost, aktuelle Version 1.0.1817 – www.agnitum.com

- verfügbar in einer freien und in einer kostenpflichtigen Professional-Version
- Einfache Bedienung mit deutscher Oberfläche

ZoneAlarm 3.7 – www.zonelabs.com

- Weite Verbreitung => man findet im Internet viele Informationen hierzu
- Einsteigerfreundlich

Kerio Personal Firewall 2.1.5 (ehem. Tiny Personal Firewall) – www.kerio.com

- Setzt gewisse Grundkenntnisse über Netzwerk-Kommunikation voraus
- Weniger geeignet für normale Anwender
- Vorteil für den fortgeschrittenen Internet-Nutzer: individuelle Filtereinstellungen ermöglichen Feinabstimmung



Installieren einer Personal Firewall

R|R|Z|N

Wie kann ich die Funktionalität der Personal Firewall testen?

- Selbsttest: http://www.grc.com (ShieldsUp)



Checkliste: Computer-Sicherheit für Anwender

R | R | Z | N

- **Einsatz eines Virenscanners**, der regelmäßig mit neuen Virenkennungen auf den neuesten Stand gebracht wird (besser: permanente automatische Aktualisierung) zur Abwehr von *Viren, Würmern und Trojanern*
- **Ein generell umsichtiges und wachsames Verhalten im Umgang mit E-Mail-Anlagen** zur Abwehr von *Viren, Würmern und Trojanern*
  - E-Mail Anhänge nur durch Doppelklick öffnen, wenn sicher ist, dass der Anhang keine Viren enthält
  - Dateinamenerweiterungen einblenden
  - Anhänge nicht automatisch öffnen
  - Vorsicht bei Office-Dokumenten als E-Mail-Anhang
- **Einsatz der jeweils neuesten Web-Browser mit sicherer Konfiguration und mit den aktuellsten Sicherheits-Korrekturen,** denn *aktive Elemente und Softwarefehler bieten Schlupflöcher für Eindringlinge und Viren*
- **Ein generell umsichtiges und wachsames Verhalten im Umgang mit dem Internet** zur Abwehr von *Viren und Trojanern*
  - Downloads nur durchführen, wenn die Website absolut vertrauenswürdig ist
- **HTML-Mail vermeiden** zur Abwehr von *Viren, Würmern und Trojanern*
- **Sorgfältiger Umgang mit Passwörtern,** denn *Missbrauch ermöglicht vollen Zugriff*
- **Regelmäßiges Einfahren von Sicherheits-Korrekturen für die Betriebssysteme,** denn *Betriebssystemfehler bieten Schlupflöcher für Eindringlinge und Viren*
- **Was nicht benötigt wird, sollte deinstalliert oder zumindest deaktiviert werden,** denn *offene Ports sind offene Türen für Angreifer und Viren*
- **Keine Datei- und Drucker-Freigaben,** solange eine Verbindung mit dem Internet besteht, denn *offene Standard-Ports sind offene Scheunentore für Eindringlinge und Viren*

Informationen zur Sicherheit:

RRZN-Security Webseiten

http://www.rrzn.uni-hannover.de/Security

Literatur

- **Handbücher des RRZN:**
  - **Computersicherheit im Internet**
  - **Internetworking: Sicherheit**
  - **Windows 2000 – Sicherheit im Netzwerk**