Wie sichere ich meinen PC gegen Spyware, Viren, Rootkids, Botnets etc.

In diesem Vortrag soll aufgezeigt werden, „Welche Gefahren drohen einem PC?“.

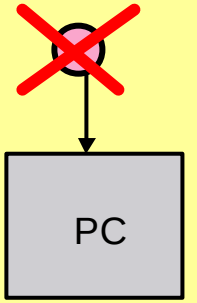
Es wird erklärt, was sind Viren, Trojaner, Rootkids, Botnets usw. und wie kann man diese möglichst verhindern den eigenen PC zu befallen. Welche Maßnahmen sollte man treffen, um möglichst viele Gefahren abzuwenden oder zu umgehen. Was sollte man möglichst nicht tun! Wie immer Bescheid wissen ist sehr wichtig!

Ein gut geschützter Rechner ist nur ein Rechner ohne Netz, und ohne Datenträgeraustausch!

1995 Ausspruch eines Arbeitskollegen, der für die Sicherheit der Abteilungsrechner zuständig war.

Aber ist dann dieser Rechner heute noch interessant?
Er ist dann nur ein besserer Taschenrechner.

Wie sichere ich meinen PC gegen Spyware, Viren, etc.



Datenträger
CD, DVD
USB-Sticks
USB-Platten
usw.

= besserer Taschenrechner

Heute ist diese Gefahr nicht mehr besonders gross, es sei denn die Herkunft des Datenträgers ist nicht ganz einwandfrei. Z.B. Sonderprogramme aus irgendwelchen Zeitschriften.

100% Schutz gibt es nicht!!

Jedoch den Schaden so klein wie möglich halten!

Wofür schliessen Sie eine Versicherung ab?

Die technische Versicherung für den PC heisst „IT-Security“

IT-Security (englisch)

Informationssicherheit (deutsch)

Sicherheit für den PC

Schutz gegen

Daten Verlust

Daten Spionage = Heutiges Thema

Rechnerausfall

Schutzware und Malware

Antivirenprogramme

Firewallprogramme

Blocking Programme (Registry)

Viren

Trojaner

Würmer

Rootkids

usw.

Was sind: (Malware)

- **Spyware** — Spionage Software
- **Trojaner** — Spionage Software
- **Adware** — Zusatzsoftware (Werbung usw.)
- **Viren** — Software, die Dateien löscht oder den Rechner stört.
- **Würmer** — Software, die sich von Rechner zu Rechner verbreitet.
- **Rootkits** — Software, die sich Administratorrechte erobert
- **Botnets** — Netze aus gekaperten Rechnern
- **BHO‘s** — Browser Help Objects (Aufgabe Erweiterungen des Browsers)
- **Hoax** — Unsinnige Mail, die verbreitet wird, weil man glaubt anderen Helfen zu müssen.
  Hoax (engl. für Jux, Scherz, Schabernack; auch Schwindel)
- **Phishing** — Fischen, in der Hoffnung, dass Sie anbeissen.
- Im Unterschied zu einem Computervirus fehlt dem Trojanischen Pferd die Eigenschaft, sich selbständig zu verbreiten.

Weitere Begriffe

Sniffer	Schnüffler für Tastatureingaben
Keylogger	Tastatureingaben Schüffler
Passwort Grabber	Programme, die Passwörter aufzeichnen
Backdoor programme	Sind Programme (auch Standard Programme), in die der Entwickler Hintertüren eingebaut hat, über die er in den Rechner kann.
Dialer	Programme, die selbst Telefonverbindungen aufbauen sind nicht mehr so interssant.
Plugin Trojaner	Trojaner welche als Plugin zu einem Programm oder Browser installiert wurden
Exploit	Programme, welche Sicherheitslücken und Verwundbaren Code ausnutzen um Unheil anzurichten.
Web-Exploit	Schwachstellen in Websites, welche Hackern die Möglichkeit bieten mit Malcode Rechner zu kapern.
Browser-Hijacking	Umleitung von Browser-Anfragen
BHO	Browser Help Objects
DoS	Denial of Service (Dienstverweigerung, Angriff auf einen Host)

Ein Virus ist ein Programm oder Code, der sich repliziert, indem er sich an ein anderes Programm, einen Boot-Sektor, einen Partitionssektor oder ein Dokument, das Makros unterstützt, anhängt. Viele Viren vermehren sich einfach nur, andere fügen jedoch Schaden zu. Ein Virus kann über ein Dokument, das Sie per E-Mail empfangen, auf Ihren Computer gelangen.

Quelle: Norton Internet Security 2003 Seite 263

Ein Virus kann durch alle Aktivitäten eingeschleppt werden, der Code ausführen z.B. auch HTML-Seiten.

Ein Wurm ist ein Programm, das Kopien von sich selbst erstellt, beispielweise von einem Laufwerk zu einem anderen oder indem es sich per E-Mail versendet. Es kann u.U. Schaden zufügen oder die Sicherheit eines Computers verletzen. Ein Wurm kann als Anlage zu einer E-Mail, deren Betreff Sie in Versuchung bringt, die Anlage zu öffnen, auf Ihren Computer gelangen.

Quelle: Norton Internet Security 2003 Seite 264

Meist durchsucht ein Wurm das Mailadressbuch und verschickt sich selbst an alle gefundenen Adressen, so schlängelt sich der Wurm schnell durch sehr viele Computer.

Ein Zombie-Programm ist ein "schlummerndes" Programm, das heimlich auf einem Computer angelegt wurde. Es kann zu einem späteren Zeitpunkt per Fernsteuerung aktiviert werden, um bei einem Kollektivangriff auf ein anderes System zu helfen. Zombie-Programme fügen dem Computer, auf dem sie gespeichert sind, normalerweise keinen Schaden zu, sondern werden für Angriffe auf andere Computer verwendet. Ein Zombie-Programm kann als E-Mail-Anlage empfangen werden. .

Quelle: Norton Internet Security 2003 Seite 264

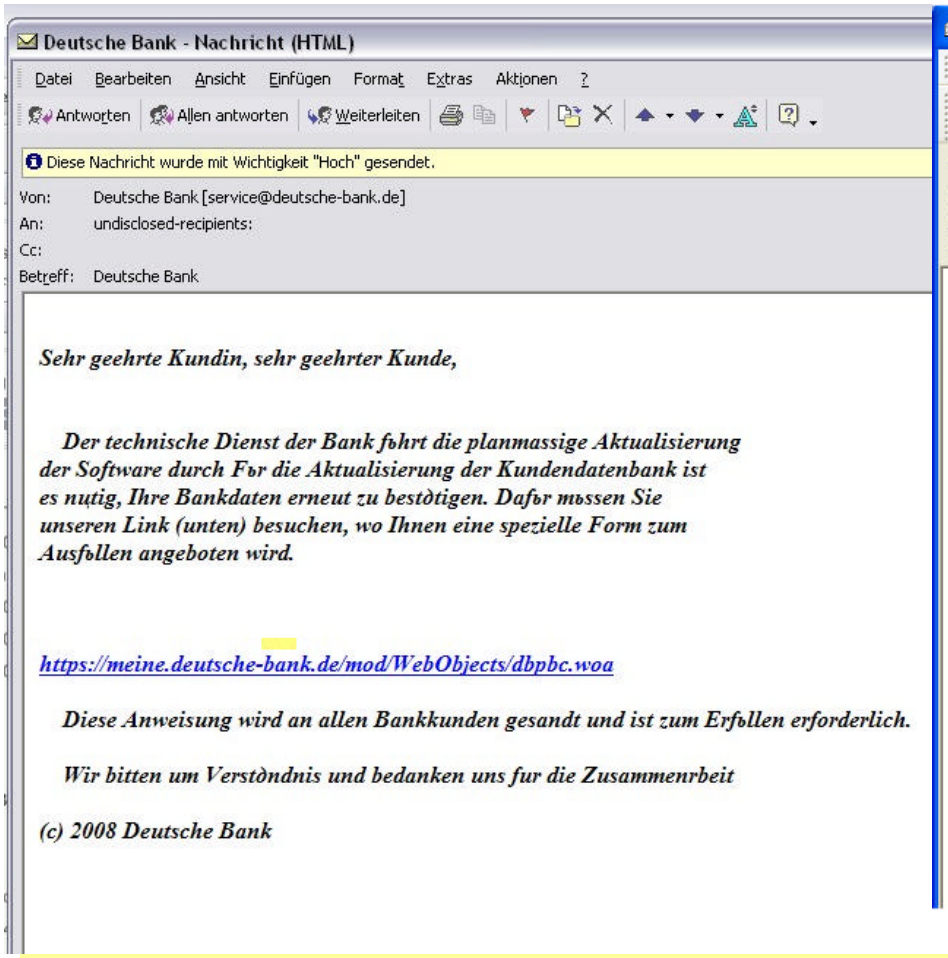
Ein Trojanisches Pferd ist ein Programm, das sich nicht replizieren kann, jodoch dem Computer Schaden zufügt oder seine Sicherheit verletzt. Normalerweise ist das Programm darauf angewiesen, dass ein Benutzer es per E-Mail an Sie schickt; es kann sich nicht selbst per E-Mail versenden. Oft wird ein Trojanisches Pferd als nützliche Software ausgegeben. Manche Trojaner-Programme führen destruktive Aktionen auf dem Computer durch, auf dem sie ausgeführt werden, andere hingegen, wie z.B. Back Orifice, bieten Hackern die Möglichkeit des ferngesteuerten Zugriffs auf Ihren Computer.

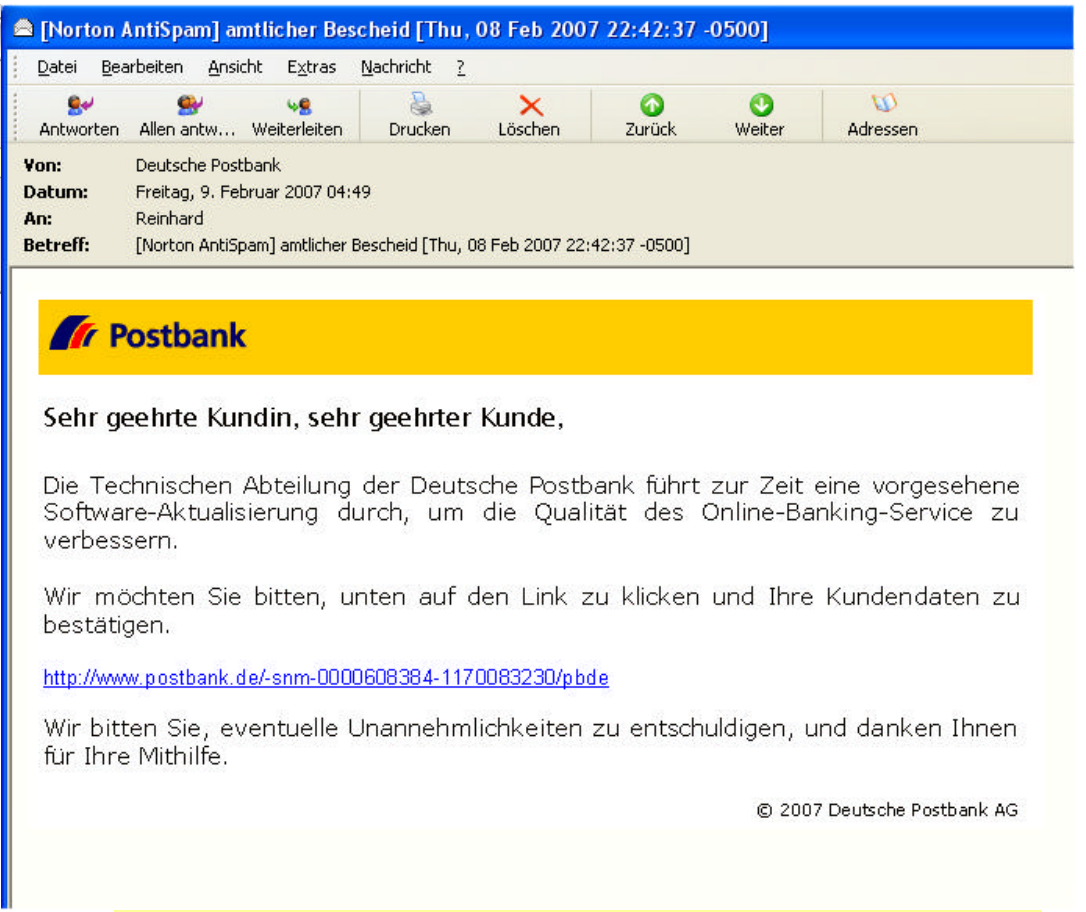
Quelle: Norton Internet Security 2003 Seite 263

Ein Programm-Download kann auch einen Trojaner enthalten.

- Ein Virenscanner prüft alle Programme und ausführbaren Codeteile auf ganz eindeutige Bitmuster, die den Virus von anderen Programmen unterscheiden (Fingerprints).
- Die typischen Viren-Bitmuster müssen deshalb gepflegt werden, das heisst vom Vertragspartner downgeladen werden.
- Der Vertragspartner erstellt stets neue eindeutige Bitmuster sobald ein neuer Virus aufgetaucht ist und festgestellt wurde.
- Deshalb sollte man wöchentlich (heute alle 2 h) die neuen Muster herunterladen und einen erneuten Scan durchführen.
- Durch die Zeitverzögerung kann man sich also trotz Virenscanner einen neuen Virus einfangen. Wie im richtigen Leben!
- Sie können ihn nachträglich dann jedoch eliminieren, wenn er hoffentlich noch keinen Schaden angerichtet hat.

Wie sichere ich meinen PC gegen Spyware, Viren, etc.



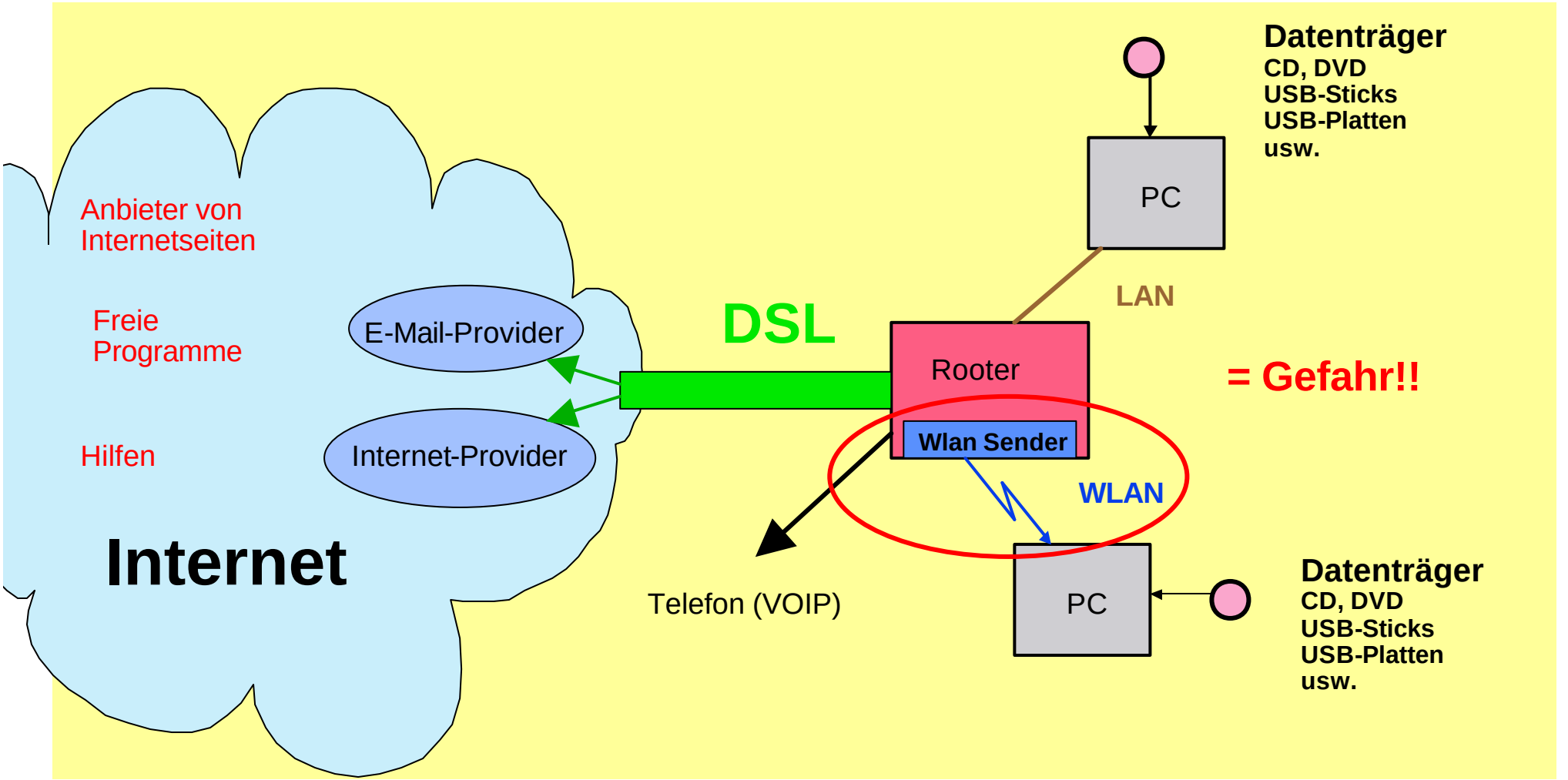



Sperrung Ihrer E-Mail reinhard@reinhardschmitt.de
Datei Bearbeiten Ansicht Extras Nachricht ?
Antworten Allen antw... Weiterleiten Drucken Löschen Zurück Weiter Adressen
Von: Blaine Wolf
Datum: Dienstag, 2. Dezember 2008 10:19
An: reinhard@reinhardschmitt.de
Betreff: Sperrung Ihrer E-Mail reinhard@reinhardschmitt.de
Einfügen: Hinweis.zip (25 Byte)
Sehr geehrte Damen und Herren,
Ihre Email "reinhard@reinhardschmitt.de" wird wegen Missbrauch innerhalb der naechsten 24 Stunden gesperrt. Es sind 48 Beschwerden wegen Spamversand bei uns eingegangen.
Details und moegliche Schritte zur Entsperrung finden Sie im Anhang.

Prüfungen der Antivirenprogramme

1. Quersumme
2. Spezifische Fingerabdrücke (Fingerprints)
3. Fingerprints & Heuristik & aktive Programme & Zusätzliches

Wie sichere ich meinen PC gegen Spyware, Viren, etc.



WLAN

Wireless Local Area Network

Lokales Funk Netz

Folgendes Video wurde am 10.11.2008 in der ZDF-Sendung

Wiso

gesendet.

http://www.youtube.com/watch?v=MJaJ6a4jRnM

http://www.zdf.de/ZDFmediathek/content/1342

Video extra aufrufen!

Wiso Wlan-Video

1. **Betreiber Rooter ungeschützt**
   Nach Betrieb Funknetz extra ausschalten, Rechner alleine nützt nichts
   Missbrauch IP wird hinterlassen
   Wenn Fremde über diese IP illegal Daten (z.B. Musik) herunterladen
   ist Strafrechtlich unbedenklich aber
   zivilrechtlich sind wegen Störungshaftung Regressansprüche möglich, die sind meist hoch.
2. **Betreiber Telefon über VOIP**
   Nachbarn haben den Internetzugang mitbenutzt
   Achtung Telefon ist ggf. auch möglich, kann teuer werden.
3. **Betreiber**
   zusätzlich: Ordner im PC ungeschützt (freigegeben)
   Datenklau möglich
   Urlaubsfotos & Sexfilme
4. **Betreiber**
   zusätzlich:
   Bankdaten freigegeben zur Einsicht
   Kontonr. ! Kontostände, sämtliche Buchungen
   Missbrauch möglich

Antiviren-Programmtests in der Zeitschrift c‘t

Wie sichere ich meinen PC gegen Spyware, Viren, etc.

Antiviren-Software für Windows XP und Vista aus c't 23/08

Programmname	Avira AntiVir Premium	G Data AntiVirus 2009	Kaspersky Anti-Virus 2009	Norton AntiVirus 2009	McAfee VirusScan Plus 2009
Hersteller	Avira	G Data	Kaspersky Lab	Symantec	McAfee
Homepage	www.avira.de	www.G Data.de	www.kaspersky.de	www.symantec.de	www.mcafee.com/de/default.asp
Programmversion	8.1.0.367	19.0.0.49	8.0.0.454	16.0.0.125	13.0 Build 218
unterstützte Windows-Versionen (Herstellerangaben)	2000/XP (+ 64 Bit)/Vista (+ 64 Bit)	XP (+ 64 Bit)/Vista (+ 64 Bit)	XP (+ 64 Bit)/Vista (+ 64 Bit)	XP/Vista (+ 64 Bit)	2000/XP/Vista(+64Bit)
Updates pro Woche / durchschnittliche Größe	35 / 95 KByte	160 / 110 KByte	160 / 85 KByte	1750 / 10 KByte	8 / 125 KByte
mittlere Reaktionszeit bei Ausbrüchen	0 bis 2 Stunden	0 bis 2 Stunden	2 bis 4 Stunden	0 bis 2 Stunden	0 bis 2 Stunden[6]
Bewertung					
Signatur-Erkennung Schadsoftware / Ad- und Spyware	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕	⊕⊕ / ⊕	⊕⊕ / ⊕⊕
Erkennung Heuristik / verhaltensbasiert	⊕⊕ / ⊖⊖	⊕⊕ / ○	⊕ / ○	⊕ / ⊕⊕	⊕ / ⊖⊖
Erkennung Rootkits / Web-Exploits	⊕ / ⊕⊕	⊕ / ○	○ / ⊖	⊕⊕ / ○	○ / ⊖⊖
Signatur-Updates und Reaktionszeiten	⊕⊕	⊕⊕	⊕	⊕⊕	⊕⊕[6]
Bedienung	⊕	⊕	○	⊕	⊖
Geschwindigkeit	⊕	⊖	⊕⊕	⊕	○
Preis für drei PCs (neu / Verlängerung)	50 € / 50 €[5]	40 € / 35 €	50 € / 35 €	40 € / 30 €	25 € / 25 €

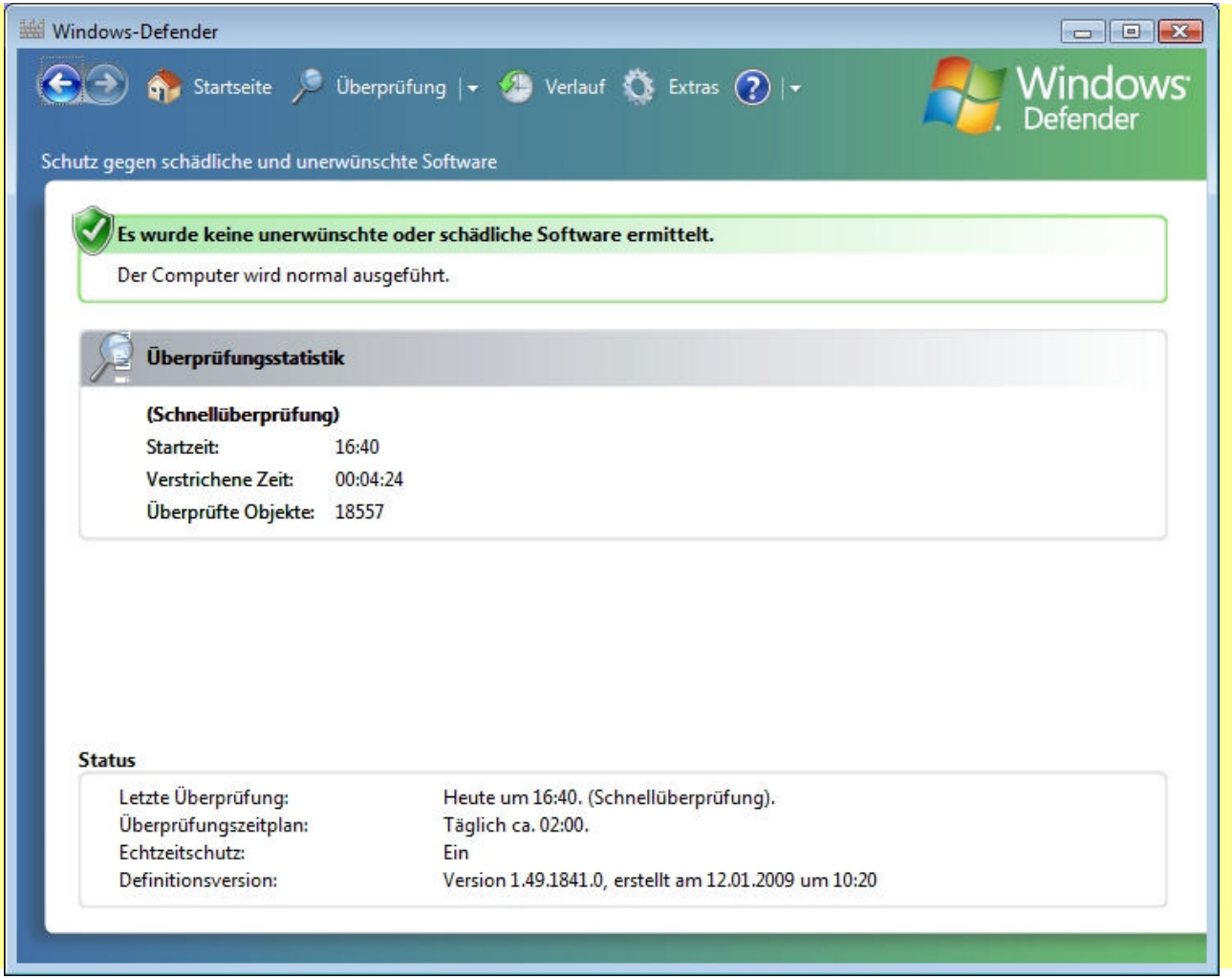
[1] standardmäßig werden ausgehende Mails nicht gescannt
[2] standardmäßig wird HTTP-Verkehr nicht gescannt
[3] meldet nur 3 von 4 passwortgeschützten Archiven
[4] trotz Meldung, dass die verschickte E-Mail einen infizierten Anhang enthält, nicht geblockt, Hersteller hat nachgebessert

⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden – nicht vorhanden k. A. keine Angabe

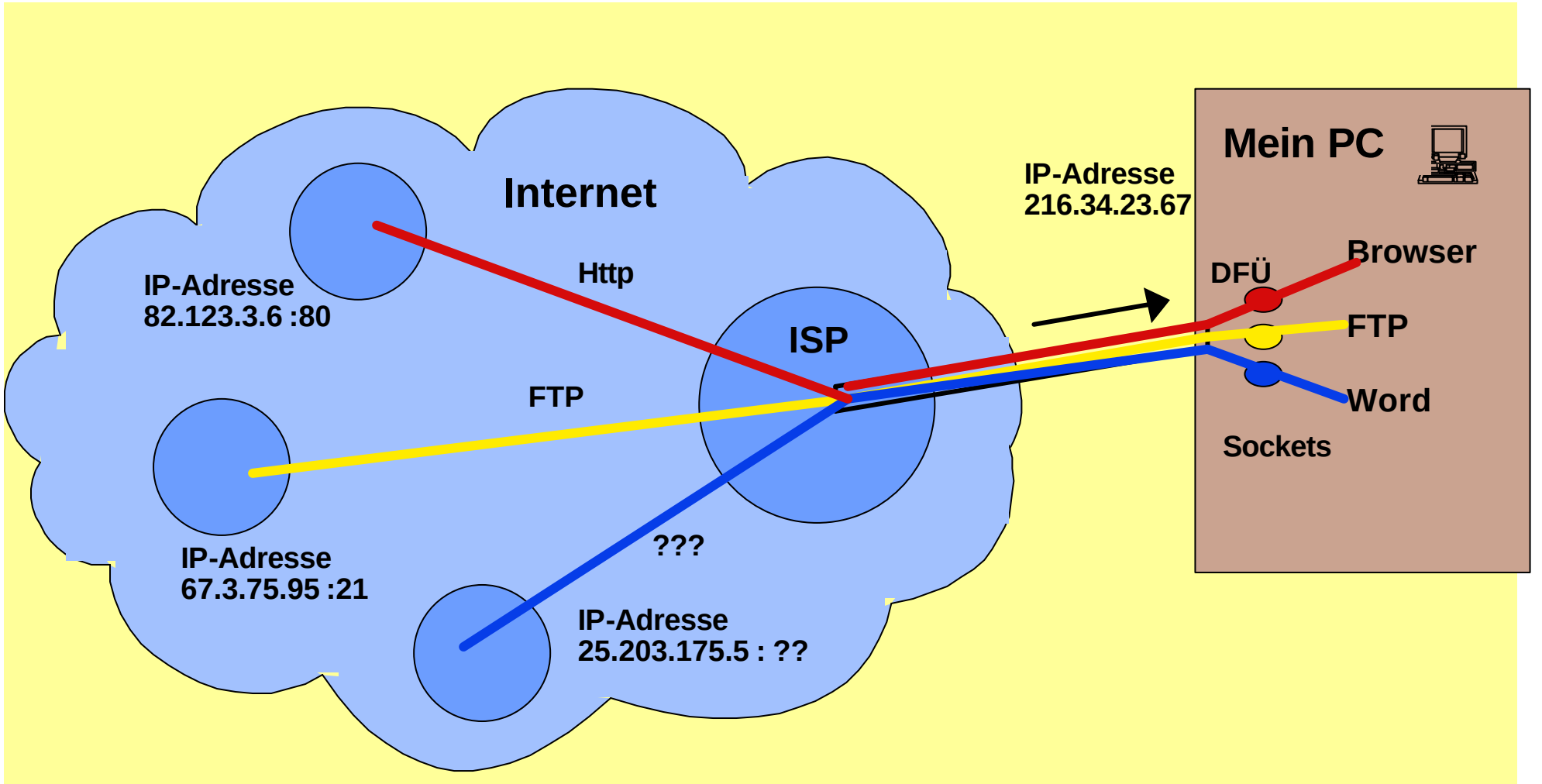
Testergebnisse der wichtigsten Antivirenprogramme

12.01.2009 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

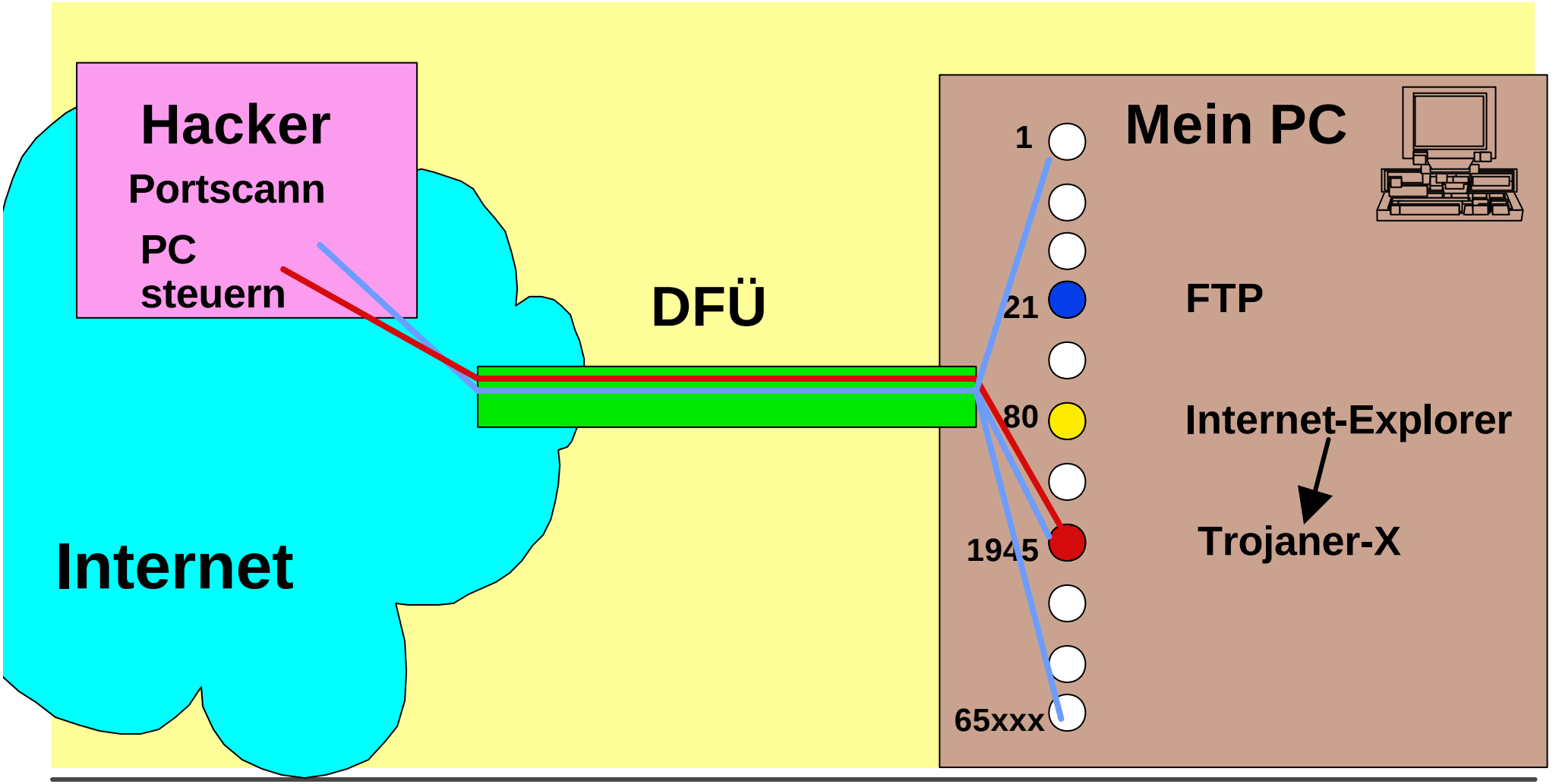
Wie sichere ich meinen PC gegen Spyware, Viren, etc.

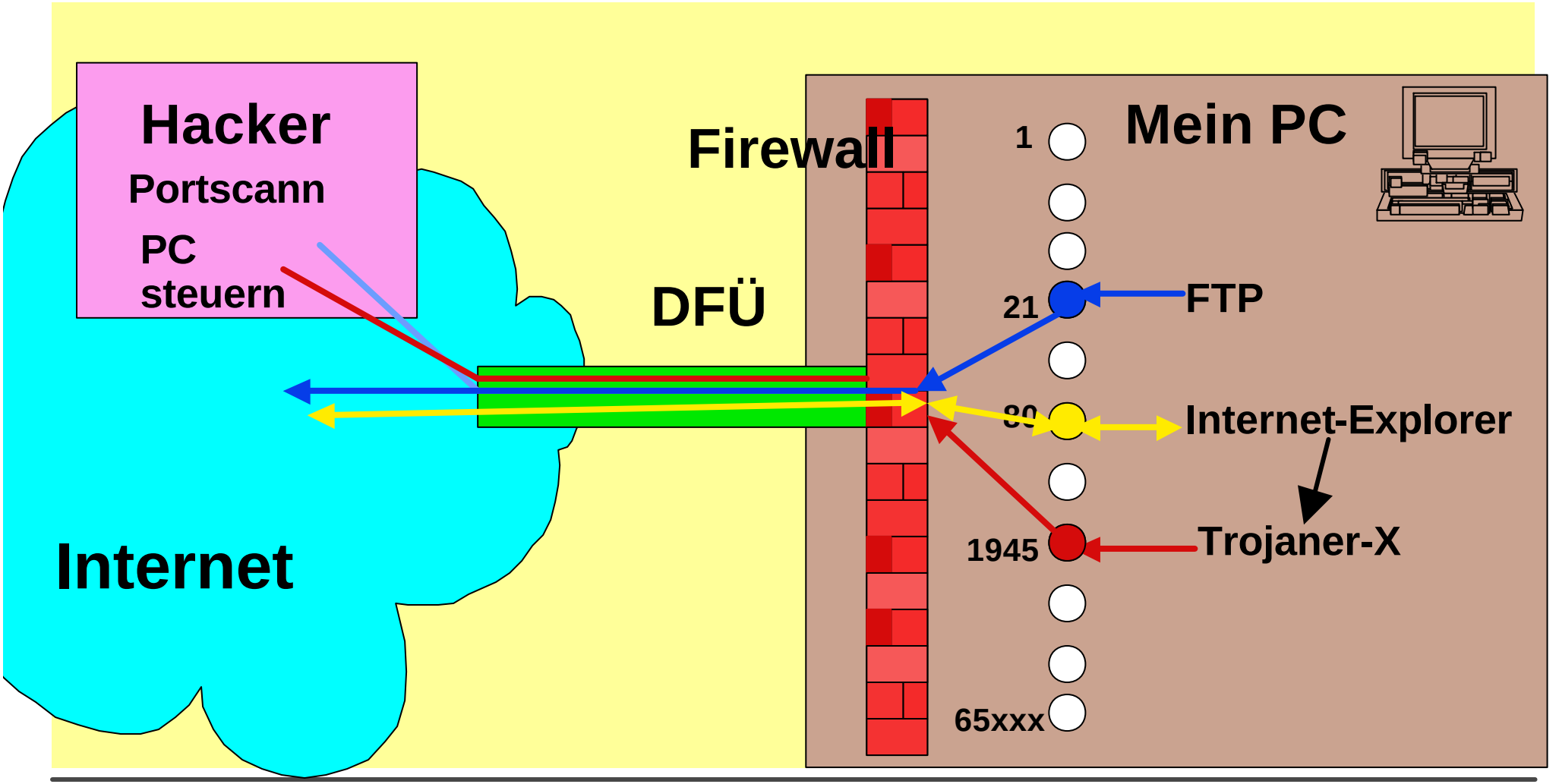


Wie sichere ich meinen PC gegen Spyware, Viren, etc.



Wie sichere ich meinen PC gegen Spyware, Viren, etc.




Hacker
Portscann
PC
steuern
Internet
DFÜ
Firewall
Mein PC
1
21
80
1945
65xxx
FTP
Internet-Explorer
Trojaner-X

Standardanschluss (Sockets)	Dienstname	Programm
20	ftp-data	FTP-Daten (File Transfer Protocol)
21	ftp	FTP-Steuerung (File Transfer Protocol)
23	telnet	Telnet Terrminal Handler
25	smtp	SMTP (Simple Mail Transfer Protocol
53	Domäne	DNS-Suche (Domain Name Service)
79	Finger	Finger
80	http	HUP (Hypertext Transfer Protocol)
110	Pop3	POP3 (Post Office Protocol 3)
113	auth	Ident Authentication Service
119	nntp	NNTP (Network News Transfer Protocol)
137	nbname	NetBIOS-Name \Microsoft-Netzwerk)
138	nbdatagram	NetBIOS-Datagram (Microsoft Netzwerk)
139	nbsession	NetBIOS-Sitzung (Microsoft- Netzwerk)
143	imap	IMAP (Intemet Message Acces Protocol)
194	irc	IRC (Internet Relay Chat)
389	ldap	LDAP (Lightweight Directory Access Protocol)
443	https	HTTPS (Sicheres HTTP)

Aufgaben von Firewalls

1. Portsscanns unterbinden
2. Verbindungen von innen
3. Verbiegen von URL-Zeigern verhindern

Informationssicherheit (Auszug)

http://de.wikipedia.org/wiki/Informationssicherheit

Operative Maßnahmen

Zu den Sicherheitsmaßnahmen, die von jedem Verantwortlichen für die vor allem von jedem privaten Nutzer von Computern und Netzwerken in Privathaushalten für die Informationssicherheit getroffen werden können, gehören unter anderem die folgenden Punkte.

Software aktualisieren

Für viele Programme werden Aktualisierungen angeboten. Diese beheben häufig auch schwere Sicherheitslücken. Besonders betroffen sind alle Programme, die Daten mit dem Internet austauschen, wie zum Beispiel Betriebssysteme, Browser, Schutzprogramme oder E-Mail-Programme. Die Aktualisierungen sollten so schnell wie möglich auf den entsprechenden Rechnersystemen installiert werden.

Antiviren-Software verwenden

Wenn Daten aus dem Internet oder von Mailservern heruntergeladen oder von Datenträgern kopiert werden, besteht immer die Möglichkeit, dass sich darunter auch schädliche Dateien befinden. Um dies zu vermeiden, muss ein sogenanntes Antivirenprogramm installiert werden.

Diversifikation

Eine weitere Maßnahme zur Reduktion der Gefahren besteht in der Diversifizierung von Software, also darin, Software von verschiedenen, auch nicht marktführenden Anbietern zu verwenden. Die Angriffe von Crackern zielen oftmals auf Produkte von großen Anbietern, Insofern kann es ratsam sein, auf Produkte von kleineren und weniger bekannten Unternehmen oder zum Beispiel auf Open-Source-Software zurückzugreifen.

Firewalls verwenden

Für Angriffe, die ohne das aktive Zutun des Nutzers drohen, ist es unerlässlich eine Netzwerk-Firewall oder Personal Firewall zu installieren. Die Konfiguration einer Firewall ist nicht trivial und erfordert eine gewisse Kenntnis der Vorgänge und Gefahren.

Informationssicherheit (Auszug)

Eingeschränkte Benutzerrechte verwenden

Es ist für normale Benutzer alles andere als ratsam, mit den Rechten eines Administrators im Internet zu surfen, Dateien oder E-Mails herunterzuladen. Moderne Betriebssysteme verfügen daher über die Möglichkeit, die Benutzerrechte einzuschränken, so dass zum Beispiel Systemdateien nicht verändert werden können. Von diesen Möglichkeiten ist unbedingt Gebrauch zu machen!

Aktive Inhalte deaktivieren

Es sollten aktive Inhalte, wie zum Beispiel ActiveX, Java oder JavaScript, soweit wie möglich deaktiviert werden.

Sensible Daten verschlüsseln

Daten, die nicht in die Hände Dritter geraten sollen, müssen durch geeignete Maßnahmen, wie zum Beispiel PGP oder Device-Encryption-Software verschlüsselt werden (siehe auch Kryptographie). Passwörter, persönliche Identifikationsnummern (PIN) und Transaktionsnummern (TAN) sollten nicht unverschlüsselt gespeichert oder übertragen werden.

Sicherungskopien erstellen

Von jeder Datei, die wichtig ist, muss mindestens eine Sicherungskopie auf einem separaten Speichermedium angefertigt werden

Protokollierung

Automatisch erstellte Protokolle oder Logdateien können dabei helfen, zu einem späteren Zeitpunkt zu ermitteln, wie es zu Schäden an einem Rechnersystem gekommen ist.

Was muss ich tun?

- Antivirenprogramm installieren
- Einen Firewall einrichten
- Ein Blockingprogramm installieren (z.B. Spybot)

- WLAN Verschlüsseln (abschalten wenn nicht benötigt)
- LAN (DSL) (abschalten wenn nicht benötigt)
- Das Betriebssystem stets aktuell halten (Updates)
- Die neuesten Virenmuster downloaden (Rechner testen lassen)
- Verbindungsprotokolle des Firewall sichten
- Nicht unnötige Programme installieren
- Vorsicht bei unsicheren Quellen (DVD‘s & Web)
- Mein Wissen auf dem Laufenden halten

„Internet Links“

- **BSI Bundesamt für Sicherheit in der Informationstechnik**
  http://www.bsi-fuer-buerger.de/
- **Test von Anti Spyware-Programmen (90 Tage – 6 Monate)**
  http://www.microsoft.com/germany/athome/security/downloads/default.mspx
- **Literatur des Bundesamtes für Sicherheit in der Informationstechnik (BSI)**
  http://www.bsi.bund.de/literat/index.htm
- **BSI Informationen „Trojanische Pferde“**
  http://www.bsi.bund.de/literat/trojaner.htm
- **PC-Professionell So funktionieren 0190-Fallen**
  http://www.vnunet.de/testticker/internet/article.asp?ArticleID=988&Ref=testticker
- **BSI Informationen zu 0190-Dialern**
  http://www.bsi.bund.de/av/dialer.htm

- ARP = Adress Resolution Protocol
- DNS = Domain Name System (Server)
- HTTP = Hypertext Transfer Protocol
- HTTPS = Secure HTTP
- ICMP = Internet Control Message Protocol
- IGMP = Internet Group Membership Protocol
- IP = Internet Protocol
- IRC = Internet Relay Chat
- ISP = Internet Service Provider
- MAEs = Metropolitain Area Exchanges
- NAPs = Network Access Points
- MIME = Multipurpose Internet Mail Extension
- NNTP = Network News Transfer Protocol
- POP = Post Office Protocol
- RFC = Request for Comments
- TCP = Transmission Control Protocol
- URL = Uniform Resource Locator
- UDP = User Datagram Protocol

Fragen und Diskussion

Internet Recherchen zu:
Wie sichere ich meinen PC gegen Spyware, Viren, Rootkids, Botnets etc.

Maleware
http://de.wikipedia.org/wiki/Malware

Alternate Data Streams
http://de.wikipedia.org/wiki/Alternate_Data_Streams

Botnet
http://de.wikipedia.org/wiki/Botnet

Bot (Robot)
http://de.wikipedia.org/wiki/Bot

Contentfilter
http://de.wikipedia.org/wiki/Contentfilter

Crimeware
http://de.wikipedia.org/wiki/Crimeware

Drive-by-Download
http://de.wikipedia.org/wiki/Drive-by-Download

Informationssicherheit
http://de.wikipedia.org/wiki/Informationssicherheit

Spyware
http://de.wikipedia.org/wiki/Spyware
http://www.bsi-fuer-buerger.de/abzocker/05_05.htm
http://www.zdnet.de/specials/spyware-center/
http://www.virenschutz.info/spyware.html
http://www.microsoft.com/germany/athome/security/spyware/spywarewhat.mspx
http://www.microsoft.com/germany/athome/security/spyware/spywaresigns.mspx
http://www.microsoft.com/germany/athome/security/spyware/spywareremove.mspx
http://www.safer-networking.org/de/spybotsd/index.html

Viren
http://de.wikipedia.org/wiki/Computervirus

Würmer
http://de.wikipedia.org/wiki/Computerwurm

Trojaner
http://de.wikipedia.org/wiki/Trojaner
http://de.wikipedia.org/wiki/Trojanisches_Pferd_(Computerprogramm)
http://www.trojaner-info.de/

Keylogger
http://de.wikipedia.org/wiki/Keylogger

Logikbombe
http://de.wikipedia.org/wiki/Logikbombe

Pharming
http://de.wikipedia.org/wiki/Pharming

Phishing

http://de.wikipedia.org/wiki/Phishing

Ransomware

http://de.wikipedia.org/wiki/Ransomware

Riskware

http://de.wikipedia.org/wiki/Riskware

Rogue-Software

http://de.wikipedia.org/wiki/Rogue-Software

Rootkit

http://de.wikipedia.org/wiki/Rootkit

Spam

http://de.wikipedia.org/wiki/Spam

Vishing

http://de.wikipedia.org/wiki/Vishing

BHO's

Download BHODemon 2.0.0.23
http://www.pcworld.com/downloads/file_download/fid,23611-order,4-page,1-c,security/download.html
http://www.bsi.bund.de/av/hijack/browserhj.htm
http://de.wikipedia.org/wiki/Browser_Helper_Object

Exploit

http://de.wikipedia.org/wiki/Exploit

DoS Denial of Service

http://de.wikipedia.org/wiki/Denial_of_Service

Backdoor

http://de.wikipedia.org/wiki/Backdoor

Adware

http://de.wikipedia.org/wiki/Adware

BSI Bundesamt für Sicherheit in der Informationstechnik

http://www.bsi-fuer-buerger.de/

Test von Anti Spyware-Programmen (90 Tage – 6 Monate)

http://www.microsoft.com/germany/athome/security/downloads/default.mspx