Hochschule
Augsburg University of
Applied Sciences

Fakultät für
Elektrotechnik

Rechnersicherheit

Vortrag im Rahmen des Seminars

Stand: 12/2009

Prof. Dr.-Ing. Dr. h.c. Alfred Eder

alfred.eder@hs-augsburg.de

Dieser Vortrag beschreibt die üblichen Gefährdungen eines Rechners und die notwendigen Gegenmaßnahmen basierend auf eigenen und fremden Erfahrungen. Er erhebt keinen Anspruch auf Vollständigkeit. Für den Betrieb von Servern und Firmennetzwerken reichen die dargestellten Maßnahmen definitiv nicht aus.

Inhalt:

- Datensicherung, Backup
  - Beispiel: Acronis
- Wiederherstellung von Daten (Dateien), Data Recovery
- Endgültiges Löschen von Dateien, Erase, Wipe)
  - Beispiele: FileShredder, Erase
- Verschlüsselung von Dateien, File Encryption
  - Beispiel: Blowfish
- Wahl von Passwörtern, Password Selection, Schutz von Passwörtern
- "Malicious Software", "Malware", Viren, Würmer etc.
- Virenscanner
  - Beispiel: SOPHOS
- Firewall
  - Beipiel: Comodo

Datensicherung (Backup)

Warum Datensicherung? Was kann passieren?

- Plattendefekt (Head Crash), bei PCs und Marken-HDD inzwischen recht selten, bei Notebooks recht häufig, da diese im Betrieb nicht unbedingt ruhig und sicher stehen. Nur gegen diesen Fehler helfen RAID-Systeme.
- Softwarefehler, insbesondere beim Installieren von Software, oder beim Update
- "Malicious Software", Viren etc.
- Stromausfall, während kritische Prozesse laufen, ziehen von USB-Sticks vor Ende der letzten Datenübertragung
- Alterung von Datenträgern, besonders kritisch sind DVD±R (Haltbarkeit z. T. unter 3 Monaten, deutlich besser sind DVD±RW), magnetische Datenträger mit flexiblem Trägermaterial (Haltbarkeit < 10 Jahre), heikel sind auch Flash-Memories (USB-Sticks, SD-Card, CF-Card)
- Änderung des Speicherformats bei Software-Update, Daten sind physikalisch noch vorhanden, können aber nicht mehr gelesen (genauer: interpretiert) werden
- Eigene Dummheit

Strategien für die Datensicherung

- Sicherung der Files: Sichert nicht das Betriebssystem, hilft bei unbeabsichtigtem Löschen, nicht bei HDD-Ausfall, leicht zu machen mit Copy oder NERO etc., ausreichend für eigene Dateien
- Sicherung der Partitions: Sichert u.U. auch das Betriebssystem, nicht den Bootsektor und die Partitiontables
- System Wiederherstellung (System Recovery) von Windows, kritisch, hilft nicht bei HDD-Ausfall, malicious Software, Reparatur von Windows ist immer heikel
- Sicherung der ganzen Platte mit allen Partitions, Bootsektor und Partitiontables als Disk Image-File mit einem passenden Tool (nicht in Windows enthalten, Tools: Acronis True Image, Symantec Ghost)
    - Sichert alles, hilft auch bei HDD-Ausfall, notfalls Start des Programms von der Notfall-CD
    - Erlaubt bei infiziertem oder unbrauchbarem Betriebssystem die Rückkehr zum letzten Zustand. Man repariert nicht, sondern geht zurück.
    - Mit der richtigen Strategie lassen sich u.U. auch noch nicht gesicherte Files retten, siehe unten.
    - Auch einzelne Files oder Folders lassen sich gezielt wieder herstellen
    - Rechner, Betriebssysteme und Platten lassen sich klonen.
    - Man kann die System Wiederherstellung abschalten und vergessen

Datenträger für Sicherungsdateien

- 2. HDD, nicht ganz billig, <100 € für 1 TB, schnellste Sicherungsmethode, 10 GB sichern in < 5 Minuten (SATA ohne RAID), es gibt allerdings Szenarien, bei denen beide Platten verloren gehen. Es lassen sich auch bei NTFS einzelne Files leicht restaurieren. Disk Image File ist komprimiert, eins der sichersten Medien

- Externe Platte, USB, Firewire oder eSATA, 10 GB sichern in < 10 Minuten (USB 2.0), < 5 Minuten (eSATA ohne RAID)

- DVDs, max. 4.35 GB pro DVD (Single Layer), die Tools splitten das Image File selbsttätig, relativ langsam, üblicherweise werden mehrere DVDs gebraucht, lassen sich leicht in einem feuersicheren Safe lagern, es lassen sich aber einzelne Files bei NTFS nur über Umwege restaurieren. Als Medium kommen nur DVD±RW oder DVD-RAM in Frage (beide Technologien sind leider langsam und Single Layer, aber 30 Jahre), DVD±R sind zu unsicher, altern zu schnell und unvorhersehbar. Blu-ray ist immer noch zu teuer.

- Bänder, u. U. mit Roboter zum Wechseln der Bänder, Methode für Rechenzentren, die Bänder müssen regelmäßig erneuert werden, es lassen sich einzelne Files bei NTFS nur über Umwege restaurieren.

- Netzlaufwerke, für kleinere Netzwerke, stopfen wegen des hohen Datenaufkommens leicht das Netz zu.

Sicherungsstrategien bei Sicherung der ganzen Platte

- Mehrere Sicherungen aufheben, z. B. 5, immer die älteste Sicherung löschen und dann die neue aufspielen, niemals die letzte Sicherung überschreiben
- Es gibt drei Modi, in denen die Sicherung laufen kann:
    - Full Backup: Die ganze Platte wird gesichert
    - Differential Backup: Es werden nur die Änderungen zwischen dem letzten Full Backup und dem aktuellen Stand aufgezeichnet, braucht weniger Platz geht schneller
    - Incremental Backup: Es werden nur die Änderungen zwischen dem letzten Backup und dem aktuellen Stand aufgezeichnet, braucht noch weniger Platz geht noch schneller. Der erste Incremental Backup und der erste Diffential Backup sind gleich.
- Man macht für gewöhnlich gelegentlich einen Full Backup (Rechenzentren jedes Wochenende) und deutlich öfter einen Incremental Backup (Rechenzentren mindestens einmal täglich)
- Ist das Betriebssystem unrettbar infiziert oder startet nicht mehr, zieht man mit Hilfe der Boot-CD einen Backup, spielt den letzten guten Backup zurück und holt dann die ungesicherten Benutzer-Files vom Image des kaputten Systems

Beispiel für ein Werkzeug:

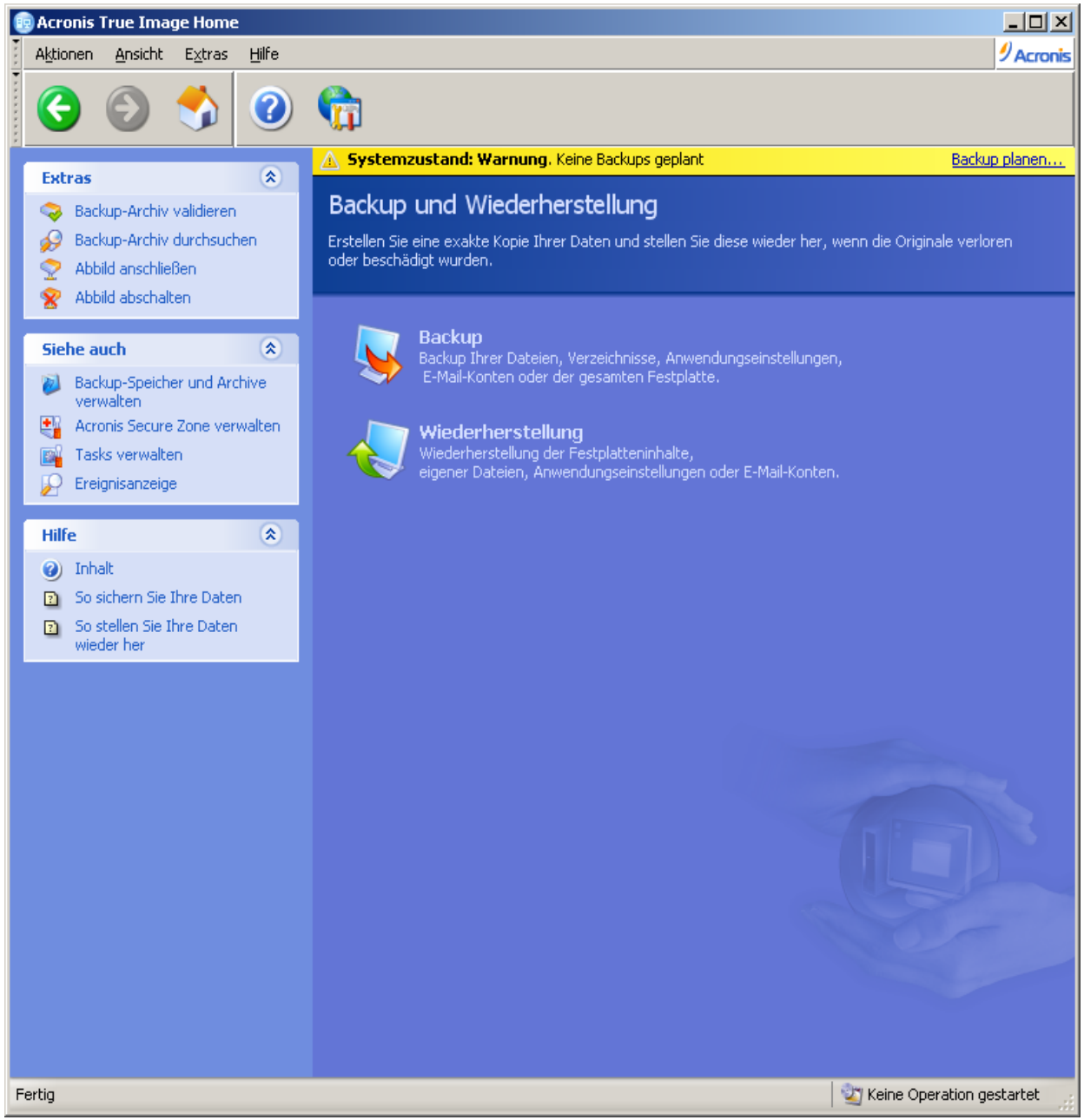
Acronis True Image

ca. 50 €

Freeware (noch nicht probiert):

Comodo Backup

Areca Backup



Wiederherstellung von Daten (Data Recovery)

Data Recovery wird normalerweise nicht gebraucht, wenn ausreichend oft die Daten gesichert wurden. Dies ist nur die allerletzte Methode und die hier vorgestellten Tools helfen auch nur bei Flash-Speichern aller Art. Die Wiederherstellung zerstörter Dateisysteme auf Festplatten ist die Aufgabe von Fachleuten (ca. € 1500).

Gelöschte Dateien landen zunächst im Papierkorb und werden erst gelöscht, wenn der Papierkorb geleert wird. Auch dann sind die Daten noch nicht vom Träger verschwunden, es wird lediglich der Datei-Header für ungültig erklärt und der belegte Platz auf dem Datenträger freigegeben. Die Daten selbst und auch der Header werden erst überschrieben, wenn der Platz für neue Dateien gebraucht wird.

Tools:

- **PC Inspector File Recovery** (Freeware, Download z.B. www.chip.de)
  recht ordentlich, kann bei Formatierung mit FAT16 und FAT32 (z. B. USB-Sticks, SD-Cards etc.) Files ganz ordentlich wieder herstellen, hat manchmal Probleme mit stark fragmentierten Dateien, hat deutliche Schwächen, wenn die Allocation Tables zerstört sind, Verwendung bei NTFS möglich, aber kaum sinnvoll
- **recuva** (wie recover gesprochen) (Freeware, Download z.B. www.chip.de)
  sehr ordentlich, kommt auch mit NTFS zurecht, die Restaurierung von Files auf den derzeit üblichen HDD-Platten ist eine eher theoretische Möglichkeit.

Alle diese Tools brauchen Administratorrechte und außer dem zu rettenden Datenträger noch einen weiteren.

Endgültiges Löschen von Dateien (Erase, Wipe)

Da Dateien auch nach dem Leeren des Papierkorbs noch da sind, müssen kritische Dateien gezielt zerstört d. h. überschrieben werden. Auch einfaches Formatieren der Platte hilft nicht. Nicht vergessen, wenn ein Rechner verkauft oder entsorgt wird.

Strategien:

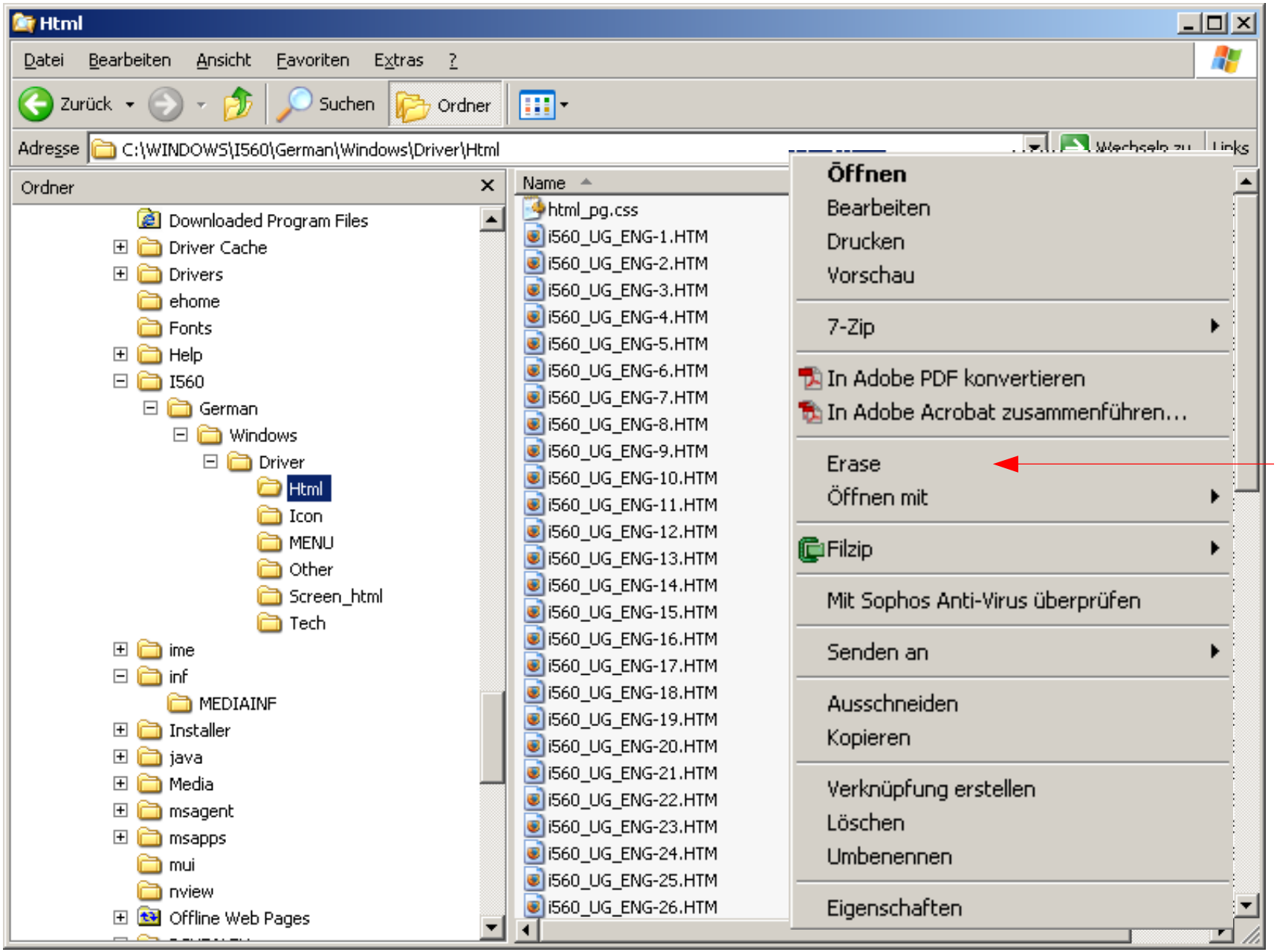
- Überschreiben mit Nullen oder Einsen
- Überschreiben mit Pseudo-Random-Zahlen (reicht für normale Zwecke, insbesondere Flash-Speicher)
- Überschreiben mit echten Zufallszahlen
- Mehrfaches Überschreiben mit verschiedenen Strategien
- Überschreiben mit seitlicher Verstellung der Schreib/Leseköpfe (erfordert spezielle Software)

Für Privatanwender reicht eine relativ einfache Strategie, wirkliche Sicherheit ist nur schwer erreichbar.

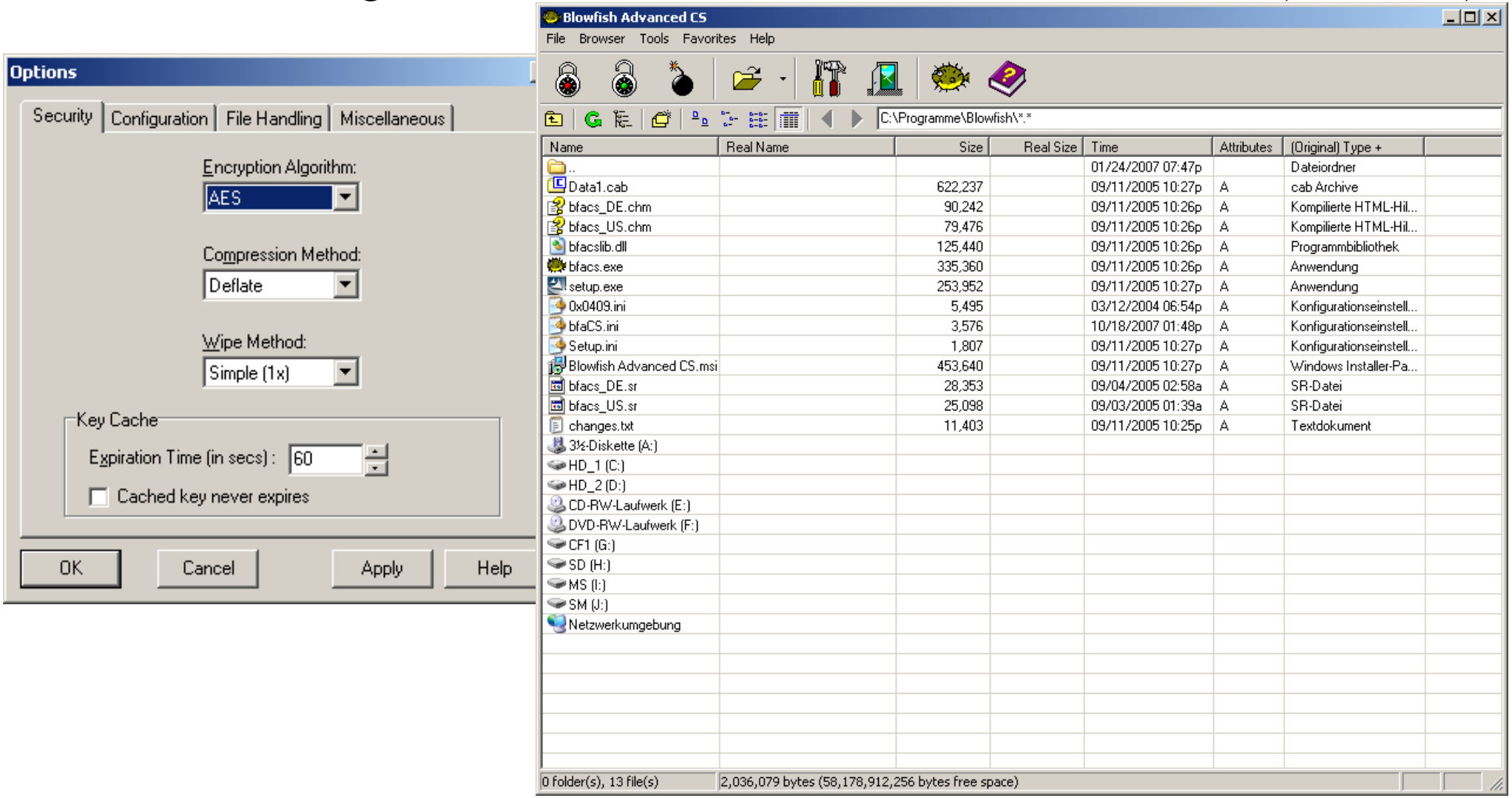
Vorsicht: Die Dateien können noch auf Backups vorhanden sein. Abhilfe: Backup verschlüsseln.

Tools (kleine Auswahl)

- Fileshredder (Freeware) Download z. B. www.chip.de (gibt es auch für Pocket-PC)
- Erase (Freeware) Download z. B. www.chip.de
  lässt sich in das Kontext-Menü des File-Explorers einbinden


Html
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Ordner
Adresse C:\WINDOWS\I560\German\Windows\Driver\Html
Ordner
Downloaded Program Files
Driver Cache
Drivers
ehome
Fonts
Help
I560
German
Windows
Driver
Html
Icon
MENU
Other
Screen_html
Tech
ime
inf
MEDIAINF
Installer
java
Media
msagent
msapps
mui
nview
Offline Web Pages
Name
html_pg.css
i560_UG_ENG-1.HTM
i560_UG_ENG-2.HTM
i560_UG_ENG-3.HTM
i560_UG_ENG-4.HTM
i560_UG_ENG-5.HTM
i560_UG_ENG-6.HTM
i560_UG_ENG-7.HTM
i560_UG_ENG-8.HTM
i560_UG_ENG-9.HTM
i560_UG_ENG-10.HTM
i560_UG_ENG-11.HTM
i560_UG_ENG-12.HTM
i560_UG_ENG-13.HTM
i560_UG_ENG-14.HTM
i560_UG_ENG-15.HTM
i560_UG_ENG-16.HTM
i560_UG_ENG-17.HTM
i560_UG_ENG-18.HTM
i560_UG_ENG-19.HTM
i560_UG_ENG-20.HTM
i560_UG_ENG-21.HTM
i560_UG_ENG-22.HTM
i560_UG_ENG-23.HTM
i560_UG_ENG-24.HTM
i560_UG_ENG-25.HTM
i560_UG_ENG-26.HTM
Öffnen
Bearbeiten
Drucken
Vorschau
7-Zip
In Adobe PDF konvertieren
In Adobe Acrobat zusammenführen...
Erase
Öffnen mit
Filzip
Mit Sophos Anti-Virus überprüfen
Senden an
Ausschneiden
Kopieren
Verknüpfung erstellen
Löschen
Umbenennen
Eigenschaften
Erase

Verschlüsselung von einzelnen Dateien, z. B. mit Blowfish CS (Freeware)



Download-Quelle z.B. http://www.chip.de/downloads Blowfish Advanced CS

Empfehlenswerte Algorithmen: Blowfish, Twofish, Advanced Encryption Standard (AES), Serpent

Viele andere Verfahren, z. B. DES, Triple-DES gelten als veraltet.

Verschlüsselung von Dateien über das Dateisystem z. B. EFS bei NTFS

Blowfish und andere Werkzeuge eignen sich dann, wenn ein File oder ein Ordner verschlüsselt werden soll und nur selten von nur einem oder wenigen Menschen zugegriffen werden soll. Sobald ein File z. B. in einer Firmenumgebung ständig von mehreren Mitarbeitern benutzt wird, ist es besser, auf ein automatisches Verschlüsselungs/Entschlüsselungssystem überzugehen.

Die Implementierung von EFS in Windows hat einige Schwachpunkte, z. B. den, dass die Verschlüsselung im Dateisystem erfolgt, d. h. auf den Intranets ist das File ungeschützt. Ein anderer Schwachpunkt sind die Recovery Agents. Mehr Information:

http://www4.informatik.uni-erlangen.de/Lehre/SS03/PS_KVBK/talks/Folien-NTFS_EFS.pdf

Es gibt deutlich sicherere Systeme, bei diesen sind nur die benötigten Teile der Files im RAM entschlüsselt z. B.

- **TrueCrypt** (Freeware, bewährt, für Privatzwecke völlig ausreichend; es gibt inzwischen einen bekannten Angriffspunkt, der aber eine Manipulation am Rechner voraussetzt; braucht einmal Administratorrechte)
- **FreeOTFE** "on the fly encryption" (Freeware), es gibt eine Version für Pocket-PC, kompatibel mit der PC-Version, sonst wie TrueCrypt
- **RSA** (kommerziell, bewährt, für Firmen, insbesondere, wenn mehrere Mitarbeiter an den gleichen Files arbeiten)
- USB-Sticks mit eingebautem **Chip**, Fingerabdrucksensor (z.B. Jetflash) oder kleiner Tastatur

Wahl von Passwörtern

Normalerweise erfolgt der Angriff auf verschlüsselte Daten nicht als Angriff auf den Algorithmus (gilt beim Stand der Technik als aussichtslos) sondern über Schwächen der Implementierung oder die Passwörter oder über das Ausspähen des Rechners durch Keylogger oder "Social Engineering" oder "Phishing" oder .....

Regeln:

- Passwörter dürfen nicht in Wörterbüchern zu finden sein, insbesondere nicht in englischen, besonders schlecht sind die Vornamen der Freundin etc.
- Kurze Passwörter (manchmal ist die Beschränkung 8 Zeichen) müssen sicher gegen einen Silbenangriff sein, d. h. Sonderzeichen enthalten und keine Silben der eigenen oder einer weit verbreiteten Sprache, damit nur der "Brute Force" Angriff zum Ziel führt.
- Lange Passphrases (ab 15 Zeichen) gelten derzeit auch dann noch als sicher, wenn Silben der eigenen oder der englischen Sprache verwendet werden, trotzdem machen Rechtschreibfehler das Passwort sicherer.
- Es lohnt nicht, sich ein komplexes Passwort für die Anmeldung am PC auszudenken, das verwendete Verfahren ist als solches unsicher.
- Im industriellen Bereich ist der Schutz mit Passwörtern nicht ausreichend. Passwörter können verraten oder erpresst werden. Dort braucht man Kombinationen von Passwörtern mit Fingerabdruck oder Hardware zur Erzeugung von "Session Keys" (z. B. RSA-Token)

Schutz von Passwörtern gegen Ausspähen

Passwörter sind ziemlich kritische Informationen und es gibt tausende Möglichkeiten, sie sich von unvorsichtigen Benutzern zu beschaffen.

- "Phishing", "Social Engineering", mit trickreichen Geschichten den Benutzer überreden, dass er seine Passwörter (Kreditkartennummern etc.) verrät
- Internet, LAN und WLAN abhören
- Keylogger, Trojaner und andere Malware
- Erpressung

Vorsichtsmaßregeln

- Gesunden Menschenverstand einschalten, dies ist die einzige Maßnahme gegen Phishing
- Mehrere Passwörter für verschiedene Anwendungen wählen, damit bei einem erfolgreichen Ausspähversuch nicht alle Anwendungen ungeschützt sind. Z. B. eines für Online-Banking, eines für die Verschlüsselung, eines für Mails, eines für den Rechnerzugang, eines für alle unkritischen Fälle.
- Kritische Passwörter öfter wechseln
- Email nur zusammen mit TLS-Verschlüsselung benutzen, z. B. Thunderbird, TLS wird praktisch von allen Mailservern unterstützt, auch GMX, web.de und anderen
- Zugriff auf Online-Daten mindestens mit SSL verschlüsseln, z. B. SSH, WinSCP, FileZilla
- WLAN nur mit WPA2 benutzen oder VPN-Channel
- Bei Online-Banking auf das Verschlüsselungssymbol und VeriSign achten
- Rechner auf Trojaner und Keylogger prüfen (SOPHOS, SpyBot, Protokolle der Firewall)
- Auf Reisen Portable Firefox und Portable Thunderbird auf einem USB-Stick mitnehmen
- Passwörter nicht auf Papier notieren, sondern in einem File speichern und verschlüsseln

"Malicious Software" "Malware"

Viren, Worms, Spys, Key-Loggers, Root-Kits, Dialers, Browser-Hijackers, Backdoors ....

Cartoon aus "Dilbert" von Scott Adams, © Scott Adams, Inc.

Personen: Evil H.R. Director Mr. Catbert, The Boss

Malicious Software kommt nicht von irgend woher, man holt sie sich.

Infektionswege:

- infizierte Datenträger mit Autostart starten (USB-Sticks, CDs, ...), > 65% aller Ansteckungen
- Chatrooms (IP-Adresse ist bekannt)
- infizierte Mails öffnen ("I love you") oder die Anhänge anklicken
- infizierte Software laden
- infizierte oder bösartige Sites besuchen (Sex umsonst ....)
- Angriff aus dem Internet
- ...

Abhilfe:

- gesunden Menschenverstand einschalten, nicht auf alles klicken
- Virenscanner einsetzen
- gute Firewall im "Expert Mode" oder "Learning Mode" einsetzen
- Chatrooms, wenn überhaupt, dann nur über Proxies besuchen oder Virtual PC benutzen
- möglichst mit DHCP (Dynamic Host Configuration Protocol) arbeiten
- nur Mailserver benutzen, die alle Mails auf Viren und Worms prüfen (z. B. RZ der FHA)
- Anhänge nicht "inline" anzeigen lassen, sondern als getrennte Files
- keine Dateien von Leuten laden, denen man nicht zutraut, ihren Rechner in Ordnung zu halten
- Autoplay komplett abschalten, ohnehin mehr ärgerlich als nützlich Tool: Registry System Wizard

Wichtigste Maßnahmen:

Normalerweise nicht mit Administratorrechten arbeiten

Benutzer haben nicht das Recht, Software zu installieren und damit auch keine Möglichkeit, Malware zu laden.

Diskussion siehe http://www.ntsvcfg.de/

Adminstratoren sollten nicht im Internet surfen und keine Mails abrufen.

Betriebssystem, Browser und Email-Tool: Sicherheitsupdates regelmäßig laden

Virenscanner

Alle Studenten und Mitarbeiter haben die Möglichkeit, sich den Virenscanner SOPHOS zu laden und mehrmals täglich neue Updates zu holen. Zum Laden der Updates von außerhalb der Hochschule ist eine VPN-Verbindung zum Rechenzentrum nötig, schlecht automatisierbar. Ein Virenscanner ist nur dann eine Hilfe, wenn er auf dem neuesten Stand ist, alte Viren sind kaum im Umlauf. Neue Viren und Worms brauchen etwa 24 bis 36 Stunden, um jeden Winkel der Erde zu erreichen. Es ist derzeit nicht nötig, den Scanner ständig im Hintergrund laufen zu lassen, es reicht nach einmaliger und gelegentlicher Prüfung der Platte, Files beim Schreiben zu prüfen. SOPHOS bietet eine entsprechende Konfiguration an.

SpyBot, AdAware , a-squared (alle Freeware)

Diese drei Tools finden Malicious Software, die nicht als klassische Viren gelten, z. B. Dialers, kritische Cookies, Spies etc. SpyBot ist etwas effizienter und aggressiver als AdAware, a-squared ist relativ neu.

ClearProg (Freeware)

Löscht temporäre Files, Verläufe, Papierkorb, Cookies und anderen Schrott, der sich in Windows sammelt.

Firewall

Vorbemerkung: Beim Stand der Technik hat eine Firewall bei weitem nicht mehr die Bedeutung wie noch vor zwei, drei Jahren. Mittlerweile sind die kritischen Teile, über die die so genannten "Exploits" angreifen, z. B. der IP-Stack, schon sehr ausgreift. Es gibt durchaus ernst zu nehmende Argumentationen, man könne auf eine Firewall verzichten, wenn

- stets die aktuellen Updates mindestens für das Betriebssystem, Browser und Email-Client gezogen werden
- und sichergestellt ist, dass das System frei von Trojanern und anderer Malware ist.

Eine Firewall kann u. U. auch ein Gigabit-LAN ganz ordentlich bremsen, insbesondere, wenn mit kleinen Files auf eine Netzwerkplatte (z.B. Samba-Server) zugegriffen wird.

Eine Firewall muss 4 Funktionen erfüllen können

- Angriffe von außen abwehren, schafft auch die Windows Firewall.
- Ungewollte Zugriffe von Software des eigenen Rechners auf das Internet verhindern bzw. melden "Heimtelefonieren" z. B. das Abschicken von Protokolldateien.
  Die meisten derartige Zugriffe sind harmlos, Software sucht nach Updates, kann trotzdem sehr lästig sein.
- Verdächtige Pakete oder Zugriffe von innen oder außen protokollieren, damit findet man auch Software, die ungewollt startet (manche verstecken sich sehr gekonnt, z. B. Root Kits).
- In besonders kritischen Fällen Alarm schlagen.

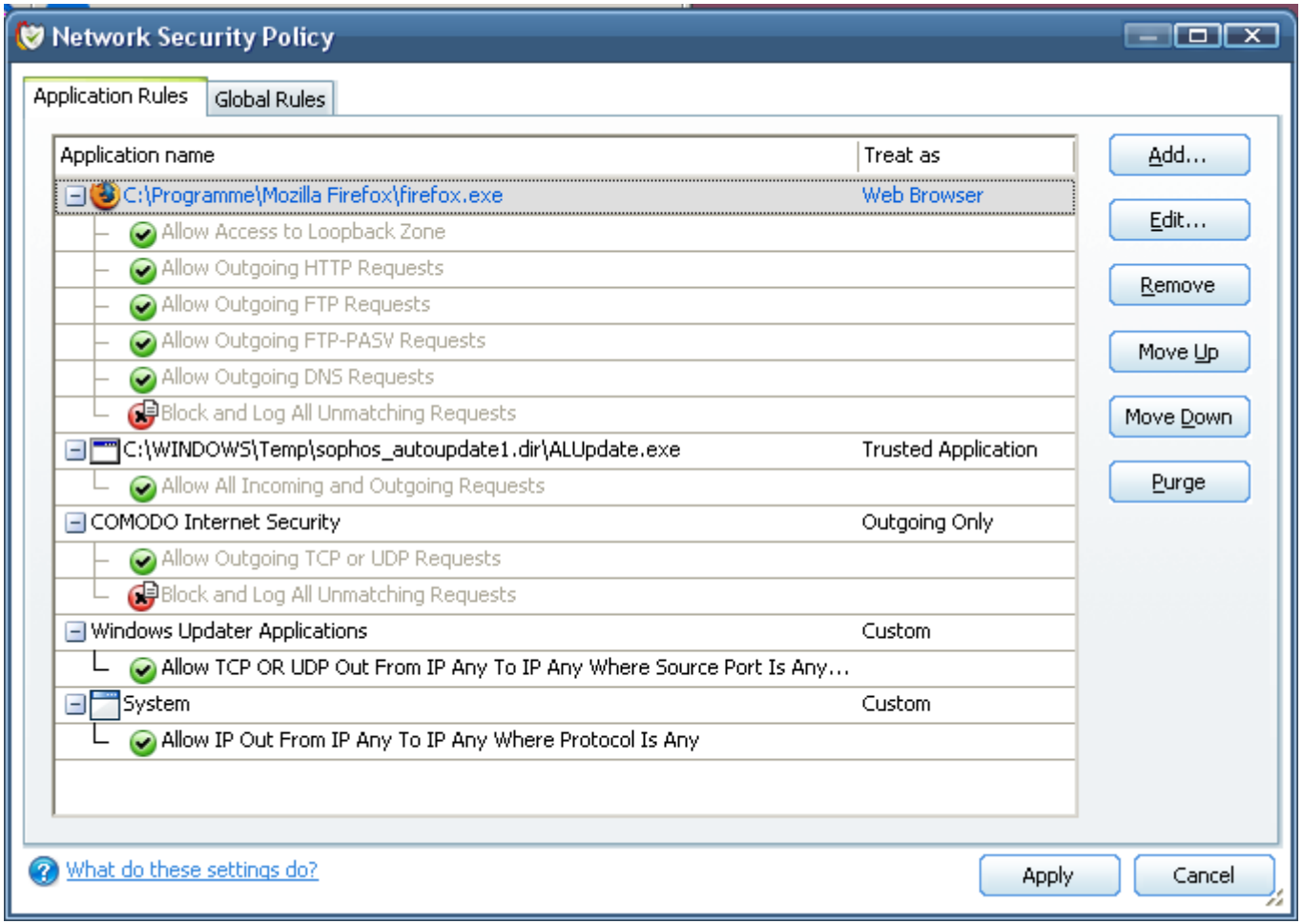
Beispiele für Firewalls (ein Vergleichstest von Freeware Firewalls findet sich in CHIP 10/2008):

- Windows ab XP SP2, Vista (Stateful Packet Inspection, SPI), keine editierbaren Regeln, kein vernünftiges Protokoll, keine Prüfung ungewollter Zugriffe, hat möglicherweise Backdoors
- Comodo Firewall Pro (enthalten in Comodo Internet Security), Freeware, deutlicher Testsieger des o. g. Tests., relativ leicht zu administrieren, bremst Zugriffe auf Netzlaufwerke, kein Problem bei DSL
- ZoneAlarm, Freeware, weit verbreitet, hat manchmal Kollisionen mit Installationen

Firewalls müssen sorgfältig administriert werden, sonst sind sie kaum wirkungsvoller als die Windows-Firewall. Sie setzen dabei stets ein Mindestmaß an Fachwissen voraus, nichts für Anfänger.

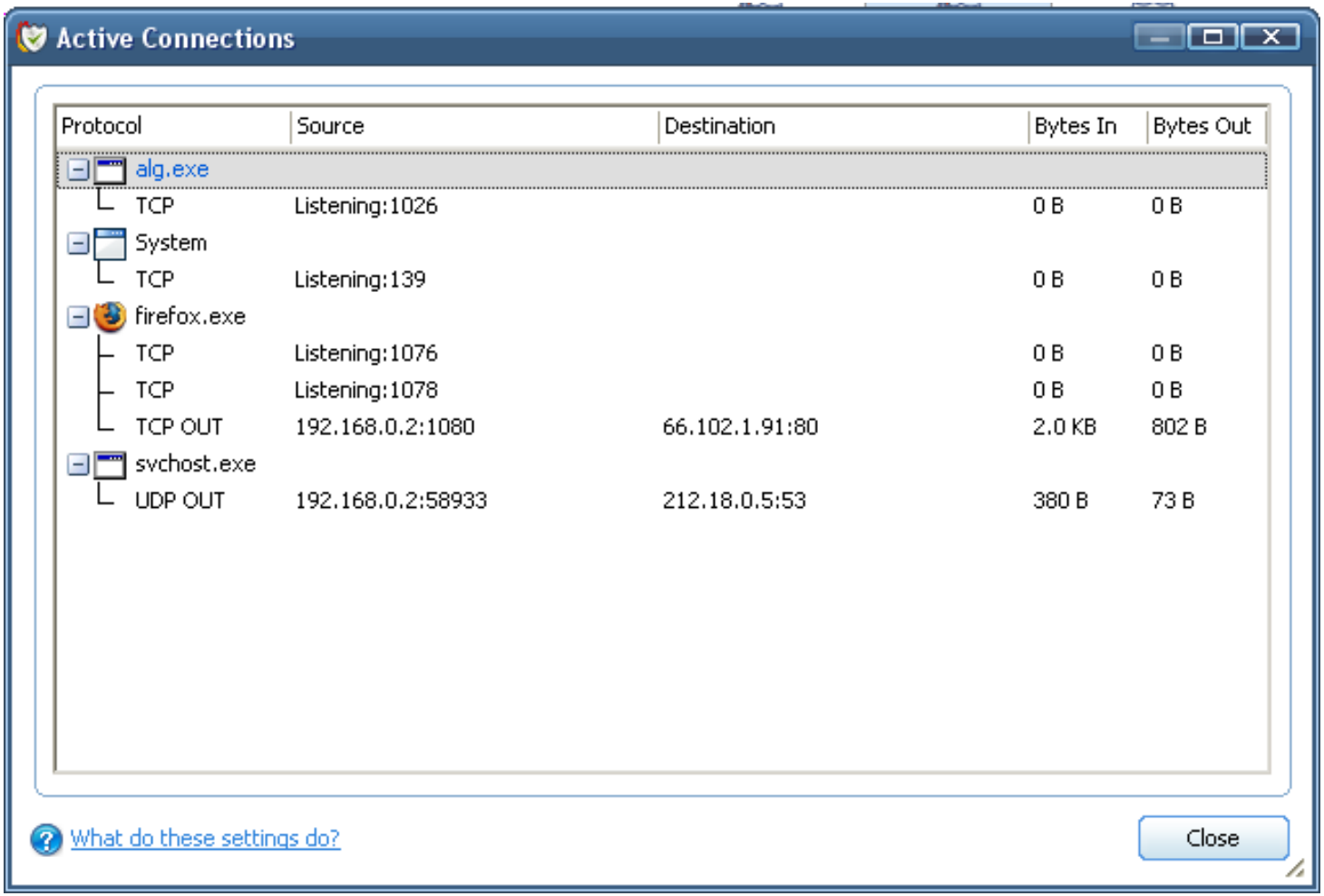
Ein Sonderfall ist die NAT-Firewall (eigentlich nur Network Address Translation, wirkt aber wie eine Firewall) im Router, sehr sicherer Schutz, keine Prüfung ungewollter Zugriffe nach draußen

Beispiel: Regeln von Comodo

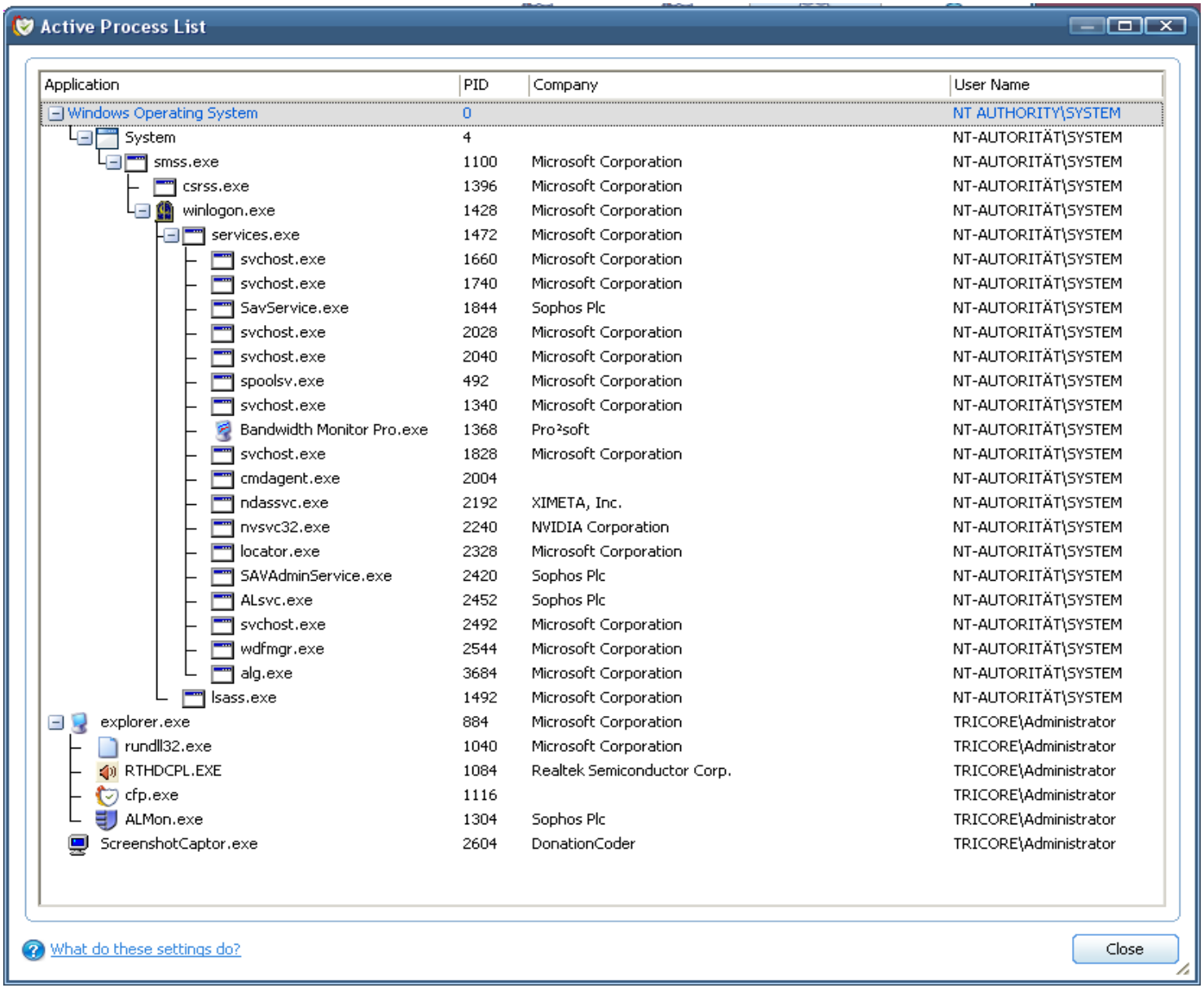


Beispiel: Vorgefertigte Regeln von Comodo für FTP

Beispiel: Offene Ports von Comodo



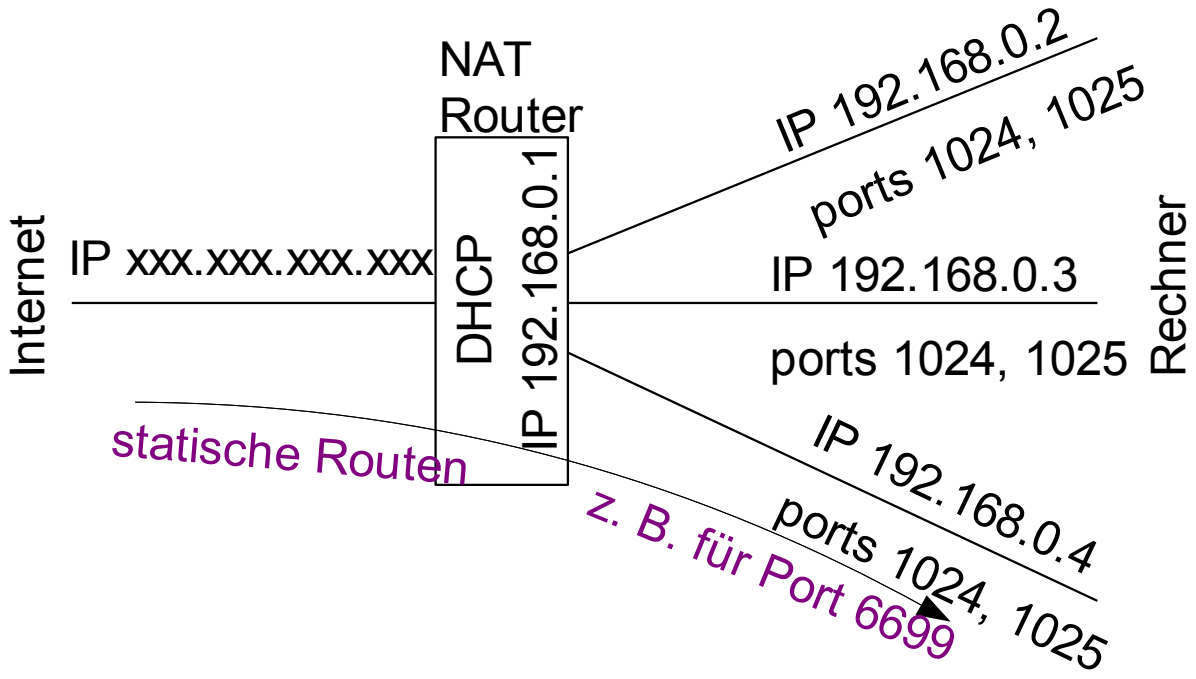
Beispiel: Prozessliste von Comodo (Zusatzfunktion)



Application	PID	Company	User Name
Windows Operating System	0		NT AUTHORITY\SYSTEM
System	4		NT-AUTORITÄT\SYSTEM
smss.exe	1100	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
csrss.exe	1396	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
winlogon.exe	1428	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
services.exe	1472	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
svchost.exe	1660	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
svchost.exe	1740	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
SavService.exe	1844	Sophos Plc	NT-AUTORITÄT\SYSTEM
svchost.exe	2028	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
svchost.exe	2040	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
spoolsv.exe	492	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
svchost.exe	1340	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
Bandwidth Monitor Pro.exe	1368	Pro²soft	NT-AUTORITÄT\SYSTEM
svchost.exe	1828	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
cmdagent.exe	2004		NT-AUTORITÄT\SYSTEM
ndassvc.exe	2192	XIMETA, Inc.	NT-AUTORITÄT\SYSTEM
nvsvc32.exe	2240	NVIDIA Corporation	NT-AUTORITÄT\SYSTEM
locator.exe	2328	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
SAVAdminService.exe	2420	Sophos Plc	NT-AUTORITÄT\SYSTEM
ALsvc.exe	2452	Sophos Plc	NT-AUTORITÄT\SYSTEM
svchost.exe	2492	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
wdfmgr.exe	2544	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
alg.exe	3684	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
lsass.exe	1492	Microsoft Corporation	NT-AUTORITÄT\SYSTEM
explorer.exe	884	Microsoft Corporation	TRICORE\Administrator
rundll32.exe	1040	Microsoft Corporation	TRICORE\Administrator
RTHDCPL.EXE	1084	Realtek Semiconductor Corp.	TRICORE\Administrator
cfp.exe	1116		TRICORE\Administrator
ALMon.exe	1304	Sophos Plc	TRICORE\Administrator
ScreenshotCaptor.exe	2604	DonationCoder	TRICORE\Administrator

NAT-Firewall (im Router)

In Routern ist eine NAT-Firewall mit SPI zwangsläufig eingebaut, sie ist bei der Abwehr von außen fast unschlagbar, da nicht zugänglich (Fernsteuerung abschalten, Passwort einstellen). Sie ist auch von gängigen Root-Kits kaum auszuhebeln.



NAT schützt ziemlich zuverlässig vor Angriffen von außen, da für Ports, für die keine Daten erwartet werden, auch keine Pfade existieren. Wenn keine statischen Routen eingerichtet wurden und keine Pakete erwartet werden, herrscht hinter der NAT-Firewall absolute Ruhe.

NAT verhindert nicht ungewollte Zugriffe von innen, deshalb wird trotz allem eine interne Firewall gebraucht.
Für Peer-to-Peer Anwendungen müssen statische Routen (port forwards) eingerichtet werden, die natürlich ein Sicherheitsloch darstellen. Typische Ports sind, je nach Protokoll, z. B. 1214, 4662, 4665, 6346, 6699.

Zusatzmaßnahmen

- nicht benötigte Ports schließen und die dazugehörenden Dienste deaktivieren oder auf manuell setzen, erfordert aber etwas erweiterte Kenntnisse der Diensteverwaltung; nichts für Anfänger. Diese Maßnahme beschleunigt auch den Start des Betriebssystems. In jedem Fall vorher die nachfolgend angegebenen Quellen anschauen.

  ausführliche Anleitung und kleines Tool in: http://www.ntsvcfg.de/

  oder (neuer): http://free.pages.at/bios01/dienste_wxp.htm

  Für den Virenscanner SOPHOS muss der Dienst DCOM-Server-Prozess auf "automatisch" stehen.

  Für Vista siehe http://www.speedyvista.com/

Test von Firewalls: Diese beiden Server starten einen (Schein-) Angriffsversuch und melden das Ergebnis:

PC-Flank:	http://www.pcflank.com/welcome.htm
Anti Hacker:	http://www.hackerwhacker.com/freetools.php

Verschlüsselung von Emails mit "Pretty Good Privacy" PGP oder GnuPG

Emails am Internet sind in etwa so sicher wie der Text auf Postkarten.

Sorry, ab hier ist immer noch eine Baustelle, aber hier sind wenigstens die gesammelten Links:

http://www.cryptool.de/ (Theorie)

http://www.gnupp.de/start.html

http://www.gpg4win.de/

http://www.erweiterungen.de/detail/Enigmail/

https://www.bsi.bund.de/cln_183/ContentBSI/Themen/sinet/EMail/EMailClient/Dokumente/isi-mail-client-doc.html

Nicht angesprochene Themen

- Verschlüsselung am Internet: Pretty Good Privacy
- Sicherheit von Online Banking
- WLAN (WEP, WPA-PSK, WPA-802.1x)
- Cookies
- Junk Filters
- ...