



# Nach Hause telefonieren ...

## Spyware - ein neues Problem aus dem Internet

Bert Schöneich

September 2003

## Inhalt (I)

- “Immer ich”
- Spyware - allgemein
  - Definition
  - Infektionsweg
  - Aufgaben
  - Beharrungsvermögen
  - „Spyware“ versus „Adware“
  - Böse oder Gut ?
  - Spyware - Viren - Trojaner - Dialer – Spam

## Inhalt (II)

- Historie
  - Anfänge
  - Statistik
- Entdecken
- Schützen und Beseitigen
  - summarisch
  - persönliches Schutzverhalten
  - Anti – Spyware – Tools
  - Firewalls



## Inhalt (II)

- reales Beispiel
  - „befallener“ PC: hardware , software
  - Wirtsprogramm
  - Entdeckung
  - Sofortmaßnahmen
  - Beseitigung
  - Erfolg



## Inhalt (IV)

- Spyware - ein Problem für DESY?
- Erfahrungen
  - persönliche Erfahrungen
  - Installation von Ad-Aware
- Literaturhinweise, Webseiten
- Erklärung zur genutzten Literatur
- Autor und Quellfiles



# 0. „Immer ich“

oder das  
„Postamt Niederbörnische“ - Syndrom



## 0. “Immer ich”

Dieser Vortrag will kein paranoides Horrorszenario zeichnen.

Er warnt vor einer Gefahr und nennt Verhaltensweisen und Möglichkeiten, sich vor dieser Gefahr zu schützen.

Der eigene PC ist einer von Millionen PCs im Internet.  
Angriffe auf ihn und die damit verbundene Verletzung der Privatsphäre sind in den seltensten Fällen persönlich gemeint.

Erkenntnisse aus derartigen Angriffen können allerdings Folgen nach sich ziehen, die mit persönlichen Konsequenzen verbunden sind.

## 1. Spyware – allgemein

# 1.1 Definition

## Was ist Spyware?

Spyware ist **JEDE SOFTWARE**, die die Internetverbindung eines Nutzers im Hintergrund (den sogenannten "backchannel") ohne dessen Wissen und ausdrücklicher Zustimmung nutzt.

Die "stille" Verwendung einer Internet "backchannel" Verbindung **MUSS EINGELEITET WERDEN** durch eine komplette und wahre Offenlegung der beabsichtigten Nutzung des backchannels, gefolgt von einer quittierten, ausdrücklichen Einverständniserklärung für eine solche Verwendung.

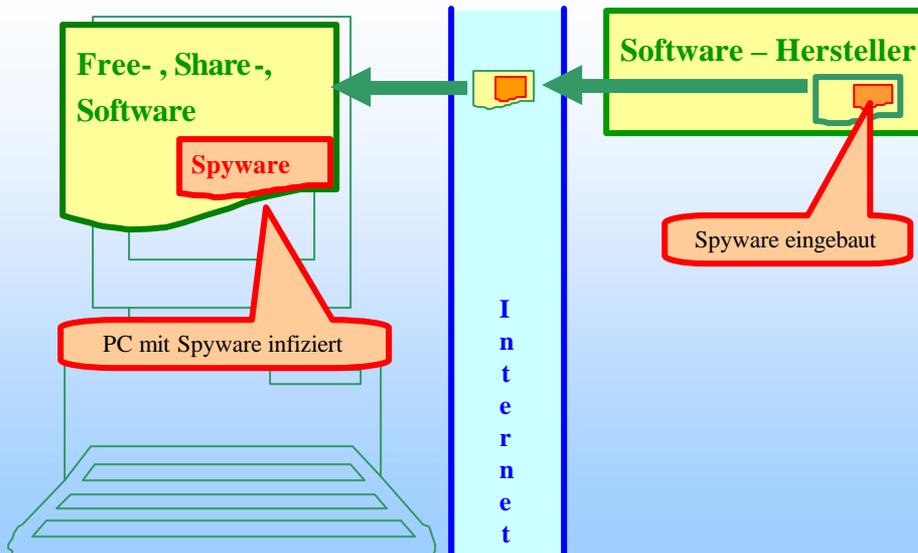
**JEDE Software** Kommunikation über das Internet, die diese Elemente nicht enthält, ist verdächtig, Informationen zu stehlen und wird deshalb zurecht

## Spyware

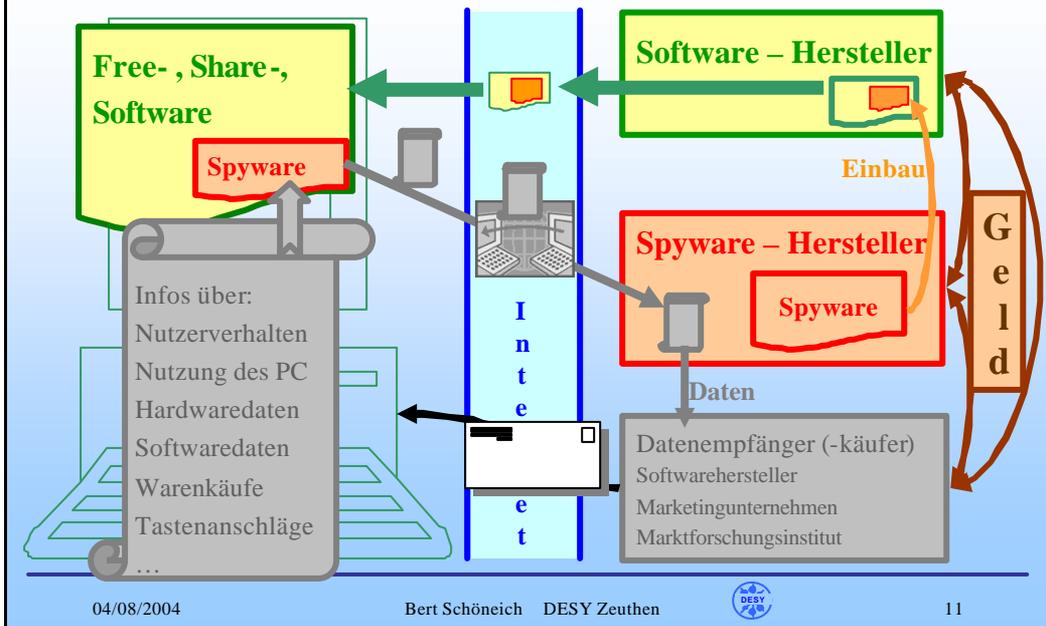
genannt.

(<http://grc.com/optout.htm>)

## 1.2 Infektionsweg



## 1.3 Aufgaben



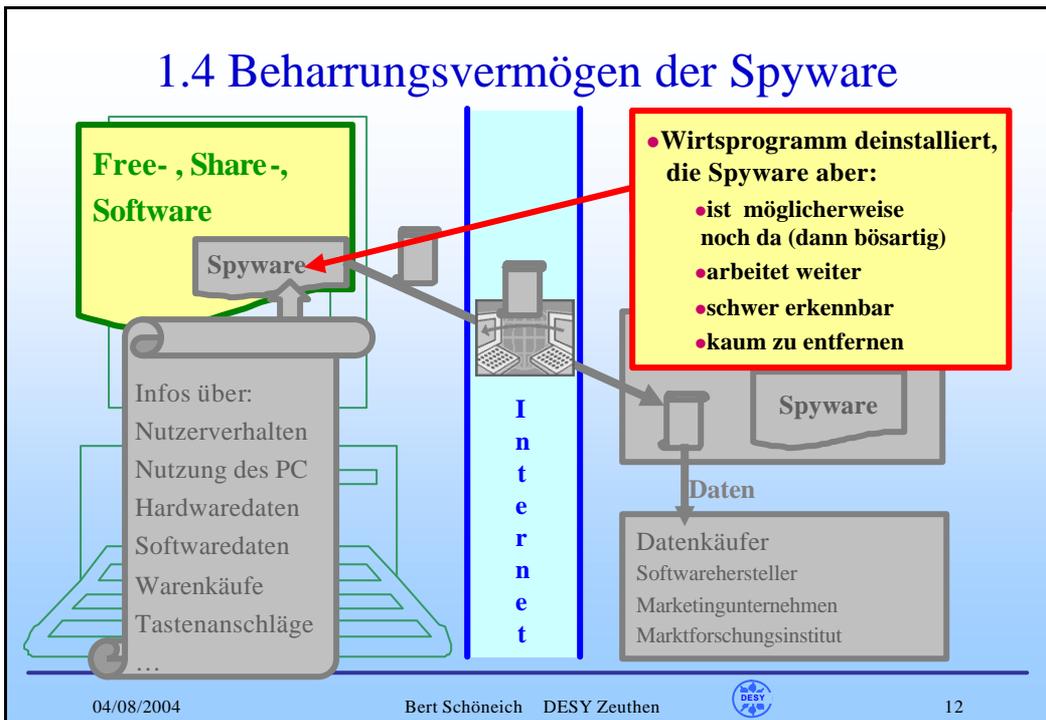
04/08/2004

Bert Schöneich DESY Zeuthen



11

## 1.4 Beharrungsvermögen der Spyware



04/08/2004

Bert Schöneich DESY Zeuthen



12

## 1.5 „Spyware“ versus „Adware“

### Spyware

- Spyware kommt huckepack mit anderer, eigentlich gewünschter Software
- ohne Kenntnis des Nutzers
- zeichnet Informationen auf:
  - Internet-Gewohnheiten
  - Namen, E-Mail-Adresse
  - Passwörter, sensible Daten
  - genutzte Software
- diese Informationen werden zurück an den Hersteller der Software geschickt
- der setzt sie für seine eigenen Zwecke ein oder verkauft sie an Dritte

### Adware

- Adware kommt huckepack mit anderer, eigentlich gewünschter Software
- wahrscheinlich mit Einverständnis des Nutzers (Lizenzbedingungen!)
- überwacht die Surf-Gewohnheiten des Users (besuchte Websites)
- sendet spezifische, den Surfgewohnheiten angepasste Pop-Up-Werbung an den PC des Nutzers
- dabei gewonnene Daten über diesen Nutzer können an ein Marketingunternehmen oder ein Marktforschungsinstitut verkauft werden.

## 1.6 Böse oder Gut?

**Spyware** oder **Adware** ?

**Gefahr** oder **Problem** ?

**Bedrohung** oder **Hilfe** ?

?

**Goethe: “Ich möchte das nicht!”**

(Ich möchte nicht, daß ohne mein Wissen und ohne meine ausdrückliche Zustimmung irgendwelche Informationen von meinem PC aus versandt werden.)

## 1.7 Spyware - Viren - Trojaner - Dialer - Spam

- **Spyware:**  
Auspionieren und Versenden sensibler Daten, Verletzen der Privatsphäre
- **Viren:**  
Verfälschen oder Zerstören dem Nutzer gehörender Informationen
- **Trojaner:**  
scheinbar sinnvolle und gutmütige Programme haben noch eine andere Aufgabe, z.B. das Öffnen des Rechners für unbemerkte Zugänge von außen
- **Dialer:**  
unbemerktes Installieren einer teuren Internet-Zugangssoftware
- **Spam:**  
massenhaftes Zusenden unerwünschter Werbeinformationen

### allen gemeinsam:

**teuer; unerwünscht; illegaler** Eingriff in die Privatsphäre des Nutzers;  
be- oder **verhindern**, bzw. **zerstören** die Arbeit des Nutzers



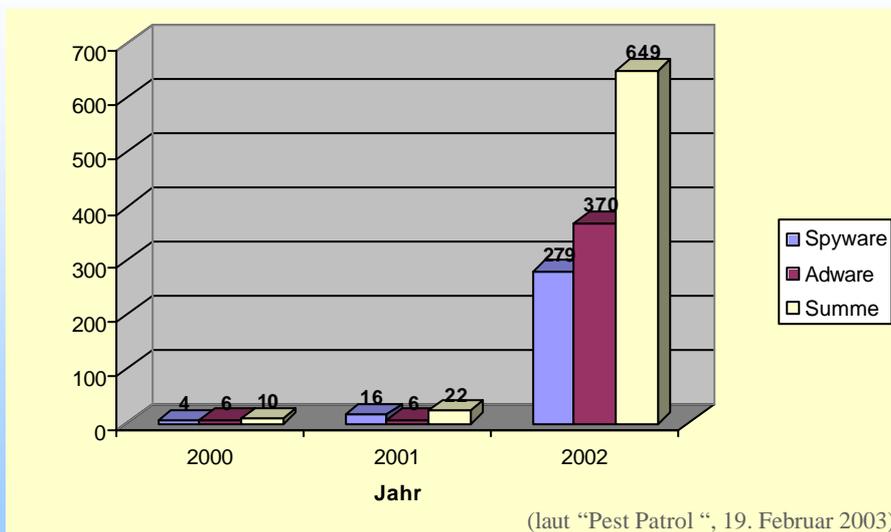
## 2. Historie



## 2.1 Anfänge

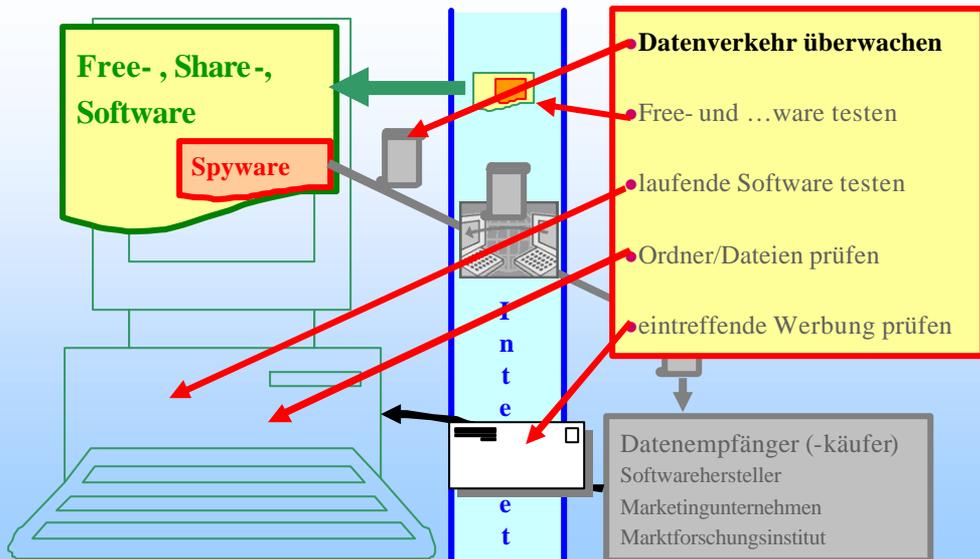
- 1996 Gründung der Firma „Aureate Media“ von drei Studenten
  - Philosophie: Bannerwerbung in normale Software plazieren
  - Entwicklung eines Codes (= Spyware), den Entwickler in ihre Programme einbauen, so dass beim Starten immer ein Banner auf dem Bildschirm des Anwenders erscheint
  - beim ersten Aufruf des Programmes werden auch einige Informationen über den Anwender abgefragt
  - gleichzeitig werden Daten über die Gewohnheiten in eine Datenbank übertragen
- mittlerweile viele weitere Anbieter
- Spyware gibt es schon seit Jahren
- weite Verbreitung, seitdem:
  - kostenlose File-Sharing-Programme wie Kazaa, Limewire und Imesh begannen, diese Spyware mit ihren eigenen Programmen zu integrieren, um die gesammelten Daten zu verkaufen und so Einnahmen zu erzielen
- Boom seit ca. einem Jahr (2002/2003)
  - große Zahl von Wirtsprogramme
  - große Zahl von Spyware

## 2.2 Statistik



# 3. Enttarnen

## 3.1 Entdecken

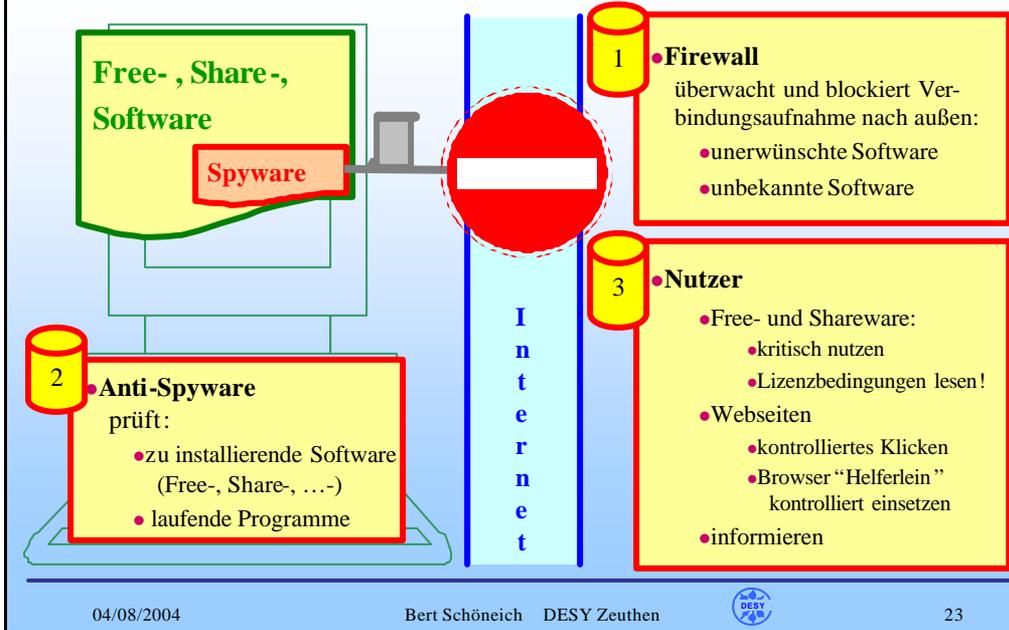


## 3.2 Entdecken

- **Datenverkehr überwachen**
  - Firewall meldet unbekannte Programme, die “nach Hause telefonieren” wollen
- **laufende Software testen**
  - läuft unbekannte Software?
  - Anti-Spyware findet Spyware
- **Free-, Share- und Software testen**
  - Internetlisten verseuchter Wirts-Software
  - Anti-Spyware findet Spyware
- **Ordner/Dateien prüfen**
  - unbekannte Ordner/Dateien auf dem Rechner (Hersteller?, Zweck?)
  - nicht deinstallierbare Software
- **eintreffende Werbung prüfen**
  - Post, Email, Messages/Nachrichtendienst:  
(Wieso bekomme ich seit kurzem viel unerwünschte Werbung aus Flensburg?)

# 4. Schützen und Beseitigen

## 4.1 Überblick



## 4.2 persönliches Schutzverhalten

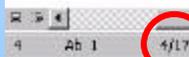
- Free-, Share- und Software:
  - kritisch nutzen, vorher (!) informieren:
    - Ist der Hersteller und/oder Vertreiber vertrauenswürdig?
    - Was sagt das Internet/Zeitschriften dazu?
  - Lizenzbedingungen und Copyrights immer bis unten (oder mindestens unten) lesen. Nicht ohne Scrollen nach dem Überfliegen der ersten Zeilen die Bedingungen akzeptieren ...

aber

## 4.2.1 Exkurs zu Lizenzbedingungen

**RealOne Player (Win 32, Version 2.0,  
download: RealOnePlayerV2GOLD\_de.exe):**

c) AutoUpdate: Der RealOne Player kommuniziert über die AutoUpdate-Funktion automatisch mit den Servern von RN im Internet und prüft so, ob Aktualisierungen der Software von RN oder den Partnern von RN (Bug-Fixes, Patches, erweiterte Funktionen, fehlende Plug-Ins und neue Versionen) zur Verfügung stehen. AutoUpdate kann auch unabhängig vom RealOne ablaufen und im Hintergrund prüfen, ob Updates vorliegen. RN kann Updates bei den Hintergrundprüfungen herunterladen, wenn der RealOne Player automatisch mit den Servern von RN kommuniziert, wenn Sie manuell nach Updates suchen oder wenn der RealOne Player eine Datei entdeckt, die er nicht unterstützt. AutoUpdate übermittelt Informationen über die installierten Produkte und Komponenten von RealNetworks an die Server, um die Verfügbarkeit von Upgrades zu bestimmen. Wenn Sie von der Durchführung eines AutoUpdate benachrichtigt werden möchten, führen Sie folgende Schritte durch: Wählen Sie im Menü 'Extras' die Option 'Einstellungen', 'Automatische Dienste', 'AutoUpdate', und deaktivieren Sie dort 'Wichtige Updates automatisch herunterladen und installieren'. Wie oben beschrieben, werden allerdings gewisse Aktualisierungen der Funktion des RealOne Player automatisch und ohne Benachrichtigung ablaufen.

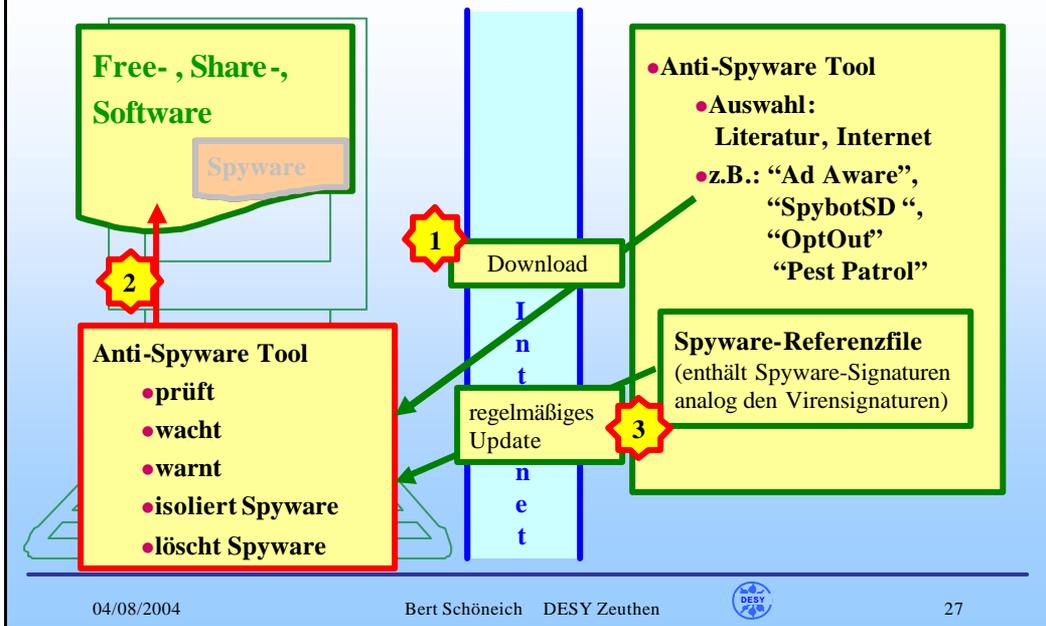


17 Seiten Lizenzbedingungen !  
Diese müssen "verstanden und akzeptiert" werden,  
bevor der RealOne Player genutzt werden darf.

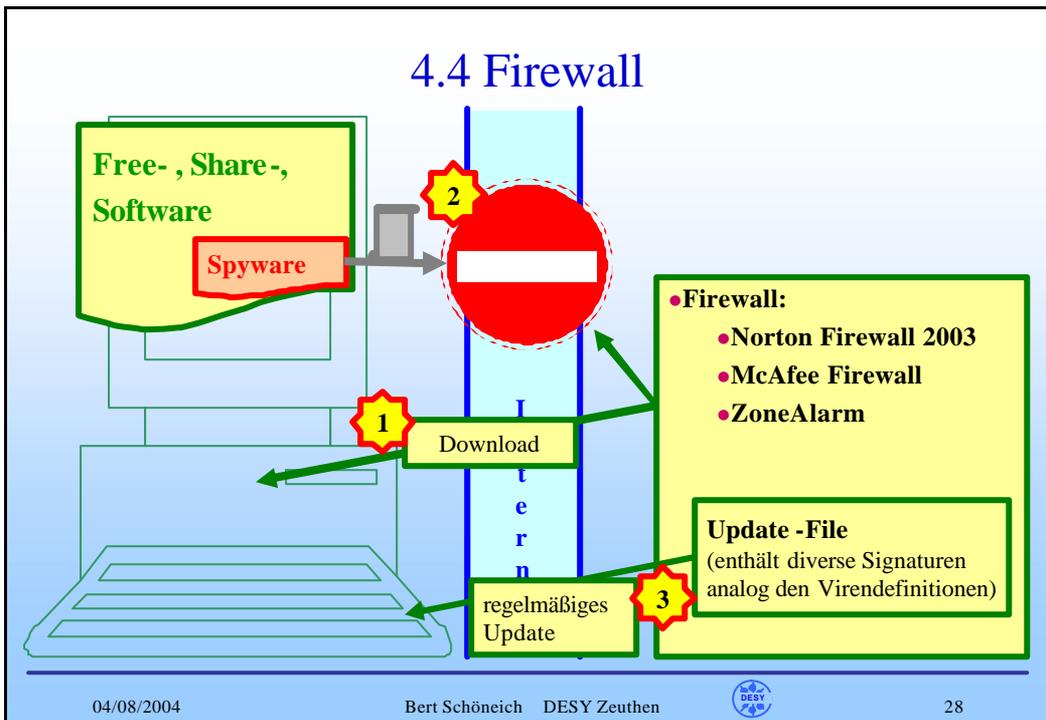
## 4.2 persönliches Schutzverhalten

- Free-, Share- und Software:
  - kritisch nutzen, vorher (!) informieren:
    - Ist der Hersteller und/oder Vertreiber vertrauenswürdig?
    - Was sagt das Internet/Zeitschriften dazu?
  - Lizenzbedingungen und Copyrights immer bis unten (oder mindestens unten) lesen. Nicht ohne Scrollen nach dem Überfliegen der ersten Zeilen die Bedingungen akzeptieren.
- Webseiten
  - kontrolliertes Klicken
    - informieren und wissen, was passiert, wenn gerade dieser Button gedrückt wird
    - ansonsten Gefahr des beiläufigen downloads von Spyware ("drive by download")
  - Browser "Helferlein" kontrolliert einsetzen
    - Bowser Helper Objects (BHO): Toolbars, Browser Plugins
- informieren, lesen
  - Internet, Zeitschriften, ...
  - kritisch lesen

## 4.3 Anti-Spyware Tool



## 4.4 Firewall



# 5. reales Beispiel



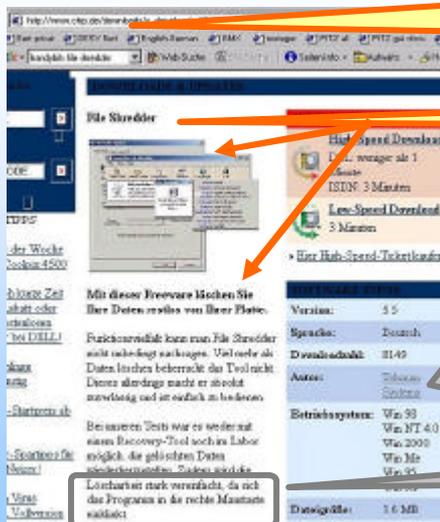
## 5.1 befallener PC, hardware, software

PC: Sony VAIO Notebook

- hardware:
  - Model : Mobile Intel(R) Celeron(tm)
  - Speed : 597MHz
  - Total Memory: 126MB SDRAM
  - Logical Storage Devices
    - ▣ Removable Drive (A:) : N/A
    - ▣ Vaionote (C:) : 5.0GB (2.5GB, 51% Free) (FAT32)
    - ▣ Hard Disk (D:) : 4.4GB (3.8GB, 86% Free) (FAT32)
    - ▣ CD-ROM/DVD (E:) : N/A
- software:
  - Windows ME



## 5.2.1 Wirtsprogramm



renommierter Anbieter von Downloads von Free- und Shareware ([www.chip.de](http://www.chip.de) und viele andere)

nettes, kleines, hilfreiches Programm

etwas überraschend (im nachhinein):

- Firma "teknum" erscheint zunächst
- Allerdings erscheint sie nach der Installation nicht mehr deutlich als Hersteller
- dann wird der Eindruck erweckt, die Firma "HandyBits" sei der Hersteller
- HandyBits bietet noch weitere gute Free- und Shareware an

Nicht nur dort!

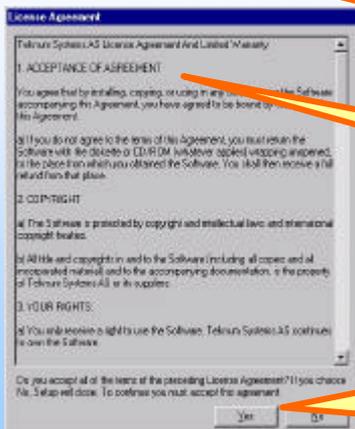
## 5.2.2 Wirtsprogramm



Installation mit dem Downloadfile, es erscheint ...

die übliche Lizenzvereinbarung die niemand liest und ...

jeder sofort bestätigt ...  
(Die Lizenzvereinbarung enthält allerdings bis zum Ende auch keinen beunruhigenden Hinweis auf Spyware-Funktionalität.)



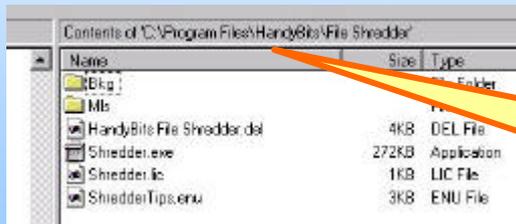
## 5.2.3 Wirtsprogramm



die Freeware ist da und erfüllt ihren Zweck

Nur den einen?

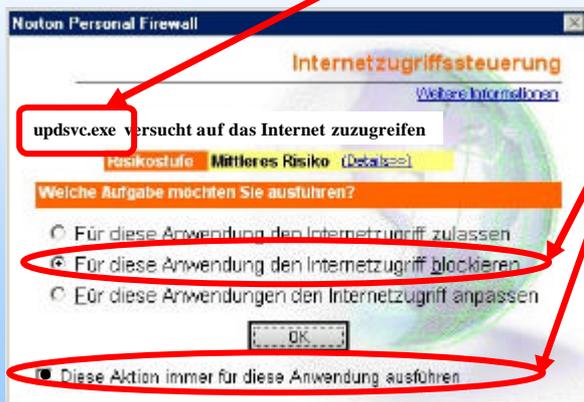
Steht wirklich alles hier?



In einem "vernünftigen" Ordner, an "vernünftiger" Stelle steht unter klarem Namen alles, was zum HandyBits File Shredder gehört.

## 5.3.1 Entdeckung, Firewall meldet sich

Ein unbekanntes Programm "updsvc.exe" versucht erstmalig auf das Internet zuzugreifen.



• (Standardreaktion bei unbekanntem Programm:

**Zugriff zunächst für immer (!) blockieren)**

danach:

• Woher kommt das Programm?

• Was will es?

• Programmname bekannt oder unbekannt?

• entscheiden, ob und wie lange der Zugriff erlaubt wird

## 5.3.2 Entdeckung, was wurde installiert?

Gruppen	Autor	Software	Alter
Installierte Software	<input type="checkbox"/>	Teknum Systeme	Neu
Autostart-Programme	<input type="checkbox"/>	Uninstall Icons	Neu
Deinstallationsmenü	<input type="checkbox"/>	HandyBits	Neu
Registrierte Dateitypen	<input type="checkbox"/>	HandyBits	Neu
Shell-Env. "Neu"	<input type="checkbox"/>	File Shredder	Neu
Shell-Erweiterungen	<input type="checkbox"/>	Yakoy Software	Alt
	<input type="checkbox"/>	WinZip Computing	Alt

Alles klar, das ist die Freeware.

Deinstallatinsroutinen

Was aber ist das?

(Keine Deinstallationsroutinen?)

Gruppen	Software	Alter	
Installierte Software	<input type="checkbox"/>	HandyBits File Shredder	Neu
Autostart-Programme	<input type="checkbox"/>	workgroup Manager 1.45	
Deinstallationsmenü	<input type="checkbox"/>	WISO Sparsbuch 2002	Alt
Registrierte Dateitypen	<input type="checkbox"/>	WinFaxio Mobile	Alt

04/08/2004

Bert Schöneich DESY Zeuthen



35

## 5.3.3 Entdeckung, Spyware "teknum"

Suche nach "\*teknum\*" - Files in einem ein wenig verstecktem Ordner steht unter fremden Namen etwas, was bei der Installation des HandyBits File Shredders ebenfalls installiert wurde.

"SendMail.exe"

"update.exe"

"updsvc.exe"

updsvc.exe ist das Programm, das durch die Firewall am "nach Hause telefonieren" gehindert wurde!

Name	Size	Type
File Delete Caution.txt	1KB	Text Document
InfoViewerV2.ocx	103KB	OCX File
SendMail.exe	14KB	Application
tsnkDiag.dll	10KB	Application Extension
tsSetup.exe	228KB	Application
tsUninst.exe	70KB	Application
update.dat	1KB	DAT File
update.exe	30KB	Application
update3.exe	34KB	Application

File mit nettem Hinweis ...

This folder contains files shared by different programs installed on your machine.

**CAUTION!**

=====

If you delete any of files in this folder, your computer or one of your programs may no longer work correctly.

04/08/2004

Bert Schöneich DESY Zeuthen



36

## 5.3.4 Entdeckung, Test auf Spyware

**Systemprüfung beendet.** Test auf Spyware erfolgreich!

Momentane Operation  
Scan beendet. Objekte geprüft: **62679**  
D:\ZEUHA2000\Runtime\

Zusammenfassung

31 Geladene Prozesse	0 Prozesse identifiziert
2 Objekte identifiziert	0 Reg. Schlüssel identifiziert
0 Objekte ignoriert	0 Reg. Daten identifiziert
2 Neue Objekte	1 Dateien identifiziert
	1 Verzeichnisse identifiziert

2 Objekte

Log zeigen Weiter

Ad-aware 6 Personal, Build 102

## 5.3.5 Entdeckung, Welche Spyware?

**Ergebnisse der Systemprüfung**

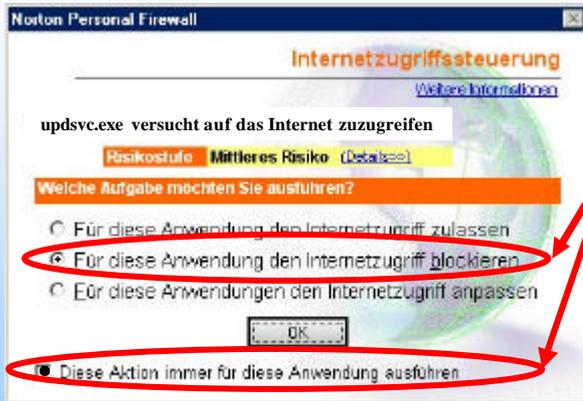
Nr.	Hersteller	Typ	Kategorie	Objekt	Komm...
<input type="checkbox"/>	Teknum Up...	Datei	Data Miner	c:\program files\common files...	
<input type="checkbox"/>	Teknum Up...	Verzeichnis	Data Miner	C:\Program Files\Common File...	

2 Objekte

Sichern Log zeigen Weiter

Ad-aware 6 Personal, Build 102

## 5.4.1 Sofortmaßnahmen, Spyware blockieren



Mit Hilfe der Firewall Zugriff auf das Internet für **immer (!)** blockieren.

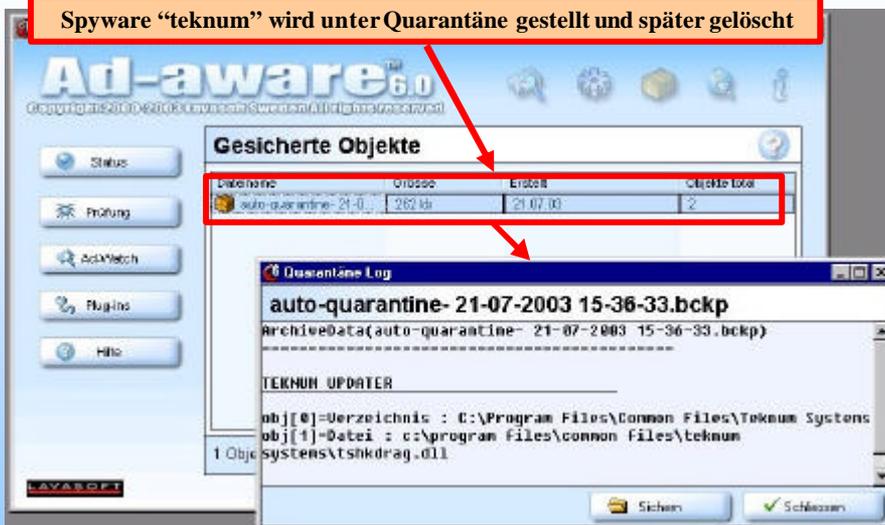
Im Zweifelsfall immer blockieren und warten, ob etwas nicht mehr funktioniert.

## 5.3.5 Entdeckung, Welche Spyware?



## 5.4.2 Sofortmaßnahmen, Anti-Spyware agiert

Spyware "teknum" wird unter Quarantäne gestellt und später gelöscht



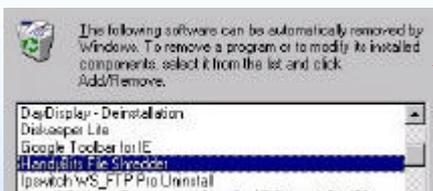
04/08/2004

Bert Schöneich DESY Zeuthen



41

## 5.5.1 Beseitigung, Deinstallation



- normale Deinstallation der Freeware HandyBits
- streichen der stehengebliebenen Dateien in C:\Program Files\HandyBits\...
- *Ausschalten des "teknum"-Updateservice mit dem Programm des Herstellers*
- Deinstallation der "teknum"-Software und streichen der unter C:\Program Files\CommonFiles\... stehengebliebenen Dateien
- Spyware weg?

**NEIN !**

04/08/2004

Bert Schöneich DESY Zeuthen



42



## 5.5.4 Beseitigung

- Löschen von:
  - allen verbliebenen 29 Registryeinträge von “HandyBits” und ”teknum” mit Hilfe eines guten Registryeditors (ACHTUNG, Löschen in der Registry kann problematisch werden!)
  - der “System”-Datei ssmenu.dll:
    - ▢ Windows ME und Windows XP: PC im abgesicherten Modes starten (Taste F8 beim Booten)
    - ▢ Windows NT: Verwenden eines Notfallsystems auf Diskette, um den Rechner zu booten
- danach Suchen nach “teknum” und “handybits”
  - Files (*Explorer-Suchfunktion*)
  - Registryeinträge (*guter Registryeditor*)
  - Spyware (*Anti-Spyware*)
- PC rebooten
  - ohne Fehlermitteilung
  - Firewall meldet keine versuchten Kontaktaufnahmen nach außen



## 5.6 Erfolg

Erst nach

- dem Blockieren durch eine Firewall
- dem Isolieren der Spyware durch eine Anti-Spyware
- dem Deinstallieren der Fre- und Spyware
- dem Löschen der verbliebenen Dateien
- dem Löschen der verbliebenen Registryeinträge
- dem Ausschalten der Systemdatei ssmenu.dll
- dem Testen des Ergebnisses

war diese relativ harmlose Spyware komplett vom Rechner beseitigt.



# 6. Spyware - ein Problem für DESY?



## 6.1 Spyware – ein Problem für DESY?

- ZDNet.de: “Inakzeptables Risiko für Großunternehmen”
  - “Da viele dieser Programme, die von ... Mitarbeitern unbewusst heruntergeladen werden, ... **Daten an ihre Herstellerfirmen zurücksenden**, sind auch Großunternehmen von diesem Problem betroffen.”
- Problem für DESY ja :
  - Kein bewußtes oder vorsätzlich falsches (nicht gestattetes) Handeln notwendig, um einen Rechner mit Spyware zu infizieren (“drive by download”).
  - Daten des DESY jeder Art (Physik?, Personal?) können betroffen sein.
- Lösungsansatz
  - vorgegebene, getestete Standardinstallationen (Netinstall)
  - nur kontrollierte downloads von Free- und Shareware
  - Anti-Spyware?
  - Firewall?



# 7. Erfahrungen



## 7.1.1 persönliche Erfahrungen

- Software, die “nach Hause telefonieren” wollte
  - Freeware
  - Shareware
  - Software
  - File-Sharing-Programme (Limewire)
  - Multimediasoftware
  - Player (Real- und diverse andere Player)
  - Handy-Bits Software (z.B. File Shredder)
  - div. Microsoftprodukte
  - Acrobat Reader (auch, nachdem alle update-“Angebote ausgeklickt wurden”!)
  - ...
  
- Hardware, die “nach Hause telefonieren” wollte
  - Fotodrucker HP Photosmart 7345



## 7.1.2 persönliche Erfahrungen

- Free- und Software aus dem deutschsprachigen Raumen hielt bisher (bei mir!) keine Spyware
- in einem Fall infizierte Freeware aus den USA meinen privaten PC mit Spyware (siehe “reales Beispiel”)
- vor allem auf PCs mit installierten File-Sharing-Programmen (Limewire) viel Spyware gefunden
- Firewall
  - **auch auf privaten PCs einsetzen!**
  - Vor allem, um Programme dauerhaft daran zu hindern, ins Internet zu gelangen.
  - wichtig bei einem Internetzugang über DSL (da lang offene Verbindung ins Netz)
  - wenn möglich, für kritische Daten (Kontoverbindung, Kreditkarte, PIN) sensibilisieren
  - von mir genutzt: [Norton Firewall 2003](#)
- Anti-Spyware Tool einsetzen
  - von mir genutzt: [Ad-Aware 6.0](#) unter Windows ME, Windows XP, Windows NT



## 7.1.3 persönliche Erfahrungen

- Schritte zur Nutzung der Anti-Spyware
  - download und installieren des Tools
  - update der Signaturfiles (Freeware-CD's beinhalten u.U. veraltete Versionen)
  - testen des PCs
- regelmäßiges Update der Signaturfiles notwendig
- wann PC testen
  - immer, nachdem Free-, Share- oder andere Software installiert wurde
  - rhythmisch, z.B. jeden Monat einmal
- Spyware entdecken
  - ist stark vom Zufall abhängig
  - als erstes meldet sich eine gut konfigurierte Firewall
  - danach bei Routinetests die Anti-Spyware



## 7. 1.4 persönliche Erfahrungen

- Spyware entfernen:
  - Anti-Spyware einsetzen
  - Anti-Spyware allein reicht nicht, sondern auch
    - Filesuche nach Namensbestandteilen
    - guter Registryeditor notwendig
  - entfernen erfordert u.U. detaillierte Systemkenntnisse
  - Vorsicht! Notwendige Systemfiles (\*.dll) könnten betroffen sein!
  - Vorsicht bei Arbeiten in der Registry!
  - Zunächst nichts löschen!
    - erst isolieren (umkopieren, macht u.U. Anti-Spyware)
    - PC einige Tage laufen lassen
    - wenn ok, dann endgültig entfernen



## 7. 1.5 persönliche Erfahrungen

- Freeware (Wirtssoftware) prüfen
  - Ist diese wirklich notwendig?
  - Läuft diese auch ohne die mit ihr gekommene Spyware?
  - nach Deinstallation der Freeware PC auf Spyware und –reste prüfen
- Spyware – Freeware
  - üblicherweise keine namentliche Verbindung Spyware heißt anders
  - Spyware liegt in anderem Ordner
  - Spyware liegt u.U. nicht in C:\programme\... , sondern in common-directories, so daß sie beim Einloggen beliebiger Nutzer gestartet wird
- Spyware triggert Systemprogramme, für sie “nach Hause zu telefonieren”
  - Drucker Photosmart: rundll32.exe (ist von Microsoft, nicht von HP)



## 7. 1.6 persönliche Erfahrungen

- Internet zur Information nutzen
  - Internet kritisch nutzen
  - Ist diese Software Spyware?
  - Enthält diese Software Spyware?
  - Welche Files/Registry Keys sind betroffen?
  - Welche Files/Registry Keys sind wie zu entfernen?
- detailliert und kontrovers diskutiertes Beispiel für die Funktion einer Spyware:
  - Aureate der Firma Aureate Media Corporation
  - Analyse von Aureate und Gegendarstellung der Firma  
[http://home.t-online.de/home/tschitschi/spyware\\_hints.htm](http://home.t-online.de/home/tschitschi/spyware_hints.htm)

Vielen Dank für Ihre  
Aufmerksamkeit.

## 7.2 Installation von Ad-Aware

- Ad-Aware installieren:
  - downloaden von <http://www.lavasoft.de/german/>
    - aaw\*.exe (Anti-Spysoftware)
    - aaw-lang-pack.exe (Sprachpaket dafür)
  - installieren von *aaw\*.exe*
  - installieren von *aaw-lang-pack.exe*
  - Ad-Aware starten
  - Sprachmodul “deutsch” einstellen (Zahnrad in Symbolleiste anklicken)
  - “Nach Updates suchen” anklicken, damit letzte Referenzdatei laden
  - “Prüfen” rechts unten anklicken
  - “Benutzereinstellungen verwenden” markieren
  - “Editieren” anklicken, zu scannende Laufwerke festlegen
  - mit “Weiter” Scan starten



# 12. Literatur Webseiten



## 12.1 Literatur, Webseiten

- Bundesamt für Sicherheit in der Informationstechnik - BSI  
[http://www.bsi-fuer-buerger.de/05/05\\_05.htm](http://www.bsi-fuer-buerger.de/05/05_05.htm)

### Spyware Listen:

- Schwarze Liste bei Cybers Palace - DIE Liste von Spionagesoftware !  
<http://www.cyberspalace.de/htm/sicher1.htm>
- Cybers Palace - DIE Liste von Spywarekit verseuchter Software  
<http://www.cyberspalace.de/htm/aured.htm>
- Spychecker - Online-Datenbank zur Suche nach suspekten Programmen  
<http://www.spychecker.com/>
- Your online guide to Spy- and Antispy-Software  
<http://www.spywareguide.com/>



## 12.2 Literatur, Webseiten

### Anti - Spyware:

- Ad-aware  
<http://www.lavasoft.de/german/>
- SpybotSD  
<http://security.kolla.de/>
- OptOut  
<http://grc.com/optout.htm>
- Pest Patrol  
<http://www.pestpatrol.com/>

### Informationen rund um Aureate/Radiate:

- Internetprofi Gerhard Glaser mit vielen Infos und weiteren links  
<http://home.t-online.de/home/tschitschi/spyware.htm>
- Analyse von Aureate und Gegendarstellung der Firma  
[http://home.t-online.de/home/tschitschi/spyware\\_hints.htm](http://home.t-online.de/home/tschitschi/spyware_hints.htm)
- Truth About Computer Virus Myths & Hoaxes: "Aureate DLLs Trojan"  
<http://www.Vmyths.com/hoax.cfm?id=36&page=3>
- McAfee Eintragung zu Aureate  
[http://vil.mcafee.com/dispVirus.asp?virus\\_k=98516&](http://vil.mcafee.com/dispVirus.asp?virus_k=98516&)



## 12.3 Literatur, Webseiten

### Foren, Diskussionsbeiträge, ... :

- ZDNet : Spyware Der rasante Verlust der Privatsphäre  
<http://techupdate.zdnet.de/story/0,,t419-s2131656,00.html>
- ZDNet: Spyware - Inakzeptables Risiko für Großunternehmen  
<http://techupdate.zdnet.de/story/0,,t419-s2131656-p2,00.html>
- ZDNet: Spyware - 'Drive-By Downloads' verhindern  
<http://techupdate.zdnet.de/story/0,,t419-s2131656-p3,00.html>
- CHIP: Forum zu "teknum" und "Handy Bits"  
<http://www.chip.de/forum/thread.html?bwthreadid=428745>
- Computing.Net - About Handy Bits Software  
<http://computing.net/security/wwwboard/forum/2620.html>
- Spyware entfernen - PCtip-Kummerkasten  
<http://www.pctip.ch/helpdesk/kummerkasten/archiv/internet/21033.asp>
- heise.de: Spyware und unsterbliche Cookies  
<http://www.heise.de/tp/deutsch/inhalt/te/14425/1.html>
- CHIP: "Vorsicht! Spioniert Ihr Chef Sie aus?"  
CHIP, November 2003, S.238 ff.



## 12.4 Literatur, Webseiten

### diverses:

- ET-Titelbild  
[http://www.cinezone.de/zone/2/html/index\\_link.html#/zone/2/2002/2803/et\\_kritik.html](http://www.cinezone.de/zone/2/html/index_link.html#/zone/2/2002/2803/et_kritik.html)

### UNIX:

- Spyware in OPEN SOURCE Software gefunden:  
<http://news.zdnet.de/story/0,,t101-s2125989,00.html>
- Anti-Spyware (?)  
<http://www.chkrootkit.org/> (mit vielen weiterführenden links)

### Macintosh:

- Überblick über Sicherheitssoftware  
<http://www.securemac.com/>
- Anti-Spyware  
<http://macscan.securemac.com/>



## 13 Erklärung

### Quellen:

Für die Erarbeitung dieses Vortrages wurden nur die unter dem Punkt „Literatur, Webseiten“ angegebenen Quellen verwendet.

### Haftungshinweis:

Trotz sorgfältiger inhaltlicher Kontrolle übernehme ich keine Haftung für die Inhalte externer Links. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreiber verantwortlich.



## 14 Autor und Quellfiles

### Autor:

Bert Schöneich

DESY Zeuthen  
Platanenallee 6  
D-15738 Zeuthen  
Germany

Tel.: +49 (33762) 77373

FAX: +49 (33762) 77216

e-mail: [bert.schoeneich@desy.de](mailto:bert.schoeneich@desy.de)

<http://www-zeuthen.desy.de/~schoene>

### Quellfiles:

powerpoint: [http://www.ifh.de/~schoene/unter\\_texte/texte/spyware-Dateien/spyware.ppt](http://www.ifh.de/~schoene/unter_texte/texte/spyware-Dateien/spyware.ppt)

pdf: [http://www.ifh.de/~schoene/unter\\_texte/texte/spyware-Dateien/spyware.pdf](http://www.ifh.de/~schoene/unter_texte/texte/spyware-Dateien/spyware.pdf)

