

microsoft.public.de.security.heimanwender FAQ

Autor: Ralf Schroth
feedback@faq.underflow.de

Stand: 28. Juli 2005

Inhaltsverzeichnis

1. **Worum geht's hier eigentlich?** – 2
2. **Warum werde ich hier nur blöde angemacht und bekomme keine Antworten?** – 2
3. **Wichtige Grundbegriffe** – 4
4. **Bei mir tauchen immer seltsame Fenster mit Werbung oder Aufforderungen zu Updates auf. Was kann ich dagegen tun?** – 6
5. **Ich habe eine Nachricht bekommen, dass ich jdbgmgr.exe (die Datei mit dem Teddybär Symbol) oder sulfnbk.exe löschen soll, da dies Viren seien. Stimmt das?** – 7
6. **Ich habe eine Mail mit einem Sicherheitsupdate von Microsoft bekommen. Kann ich dieser Mail trauen?** – 8
7. **Outlook Express blendet alle Dateianhänge aus. Wie kann ich sie wieder anzeigen lassen?** – 9
8. **Meine Personal Firewall macht Probleme / meldet Angriffe. Was kann ich tun?** – 10
9. **Wie kann ich denn nun mein System vernünftig absichern?** – 11

10. Ich habe einen Virus / Dialer / "Trojaner" / wurde "gehackt". Was soll ich tun? – 17

11. Ich habe eine Datei / einen Ordner verschlüsselt und nun Probleme damit. Was muß ich beachten? – 19

12. Die Startseite meines Internet Explorers wurde verändert. Was kann ich dagegen tun? – 20

13. Dank an ... – 22

1. Worum geht's hier eigentlich?

In der Newsgroup microsoft.public.de.security.heimanwender treten bestimmte Fragen zum Thema Sicherheit sehr häufig auf. Dieses Dokument versucht die häufigsten und wichtigsten Fragen zu beantworten. Natürlich erhebt dieses Dokument keinerlei Anspruch auf Vollständigkeit, da es bewußt verständlich formuliert wurde und deshalb nicht auf alle Details eingeht. Es werden jedoch zumeist am Ende eines jeden Abschnitts eine große Zahl von Links zu weiterführenden Informationen angegeben, auf die teilweise auch im Text Bezug genommen wird, damit sich der interessierte Leser ein genaueres Bild machen kann.

Hier werden Links auf einige Programme und Skripte externer Anbieter verlinkt, die von der Gemeinde in microsoft.public.de.security.heimanwender und vom Autor der FAQ für empfehlenswert erachtet werden. Dies soll aber nicht heißen, dass diesen Angeboten blind vertraut werden soll. Vielmehr ist es die Entscheidung jedes Einzelnen, ob er diesen Angeboten vertrauen möchte oder nicht.

2. Warum werde ich hier nur blöde angemacht und bekomme keine Antworten?

Wie überall im Leben gibt es auch in den Newsgroups bestimmte Regeln des Umgangs miteinander. Diese sind in der sog. Netikette niedergelegt. Für die Newsgroups der microsoft.public.de.* Hierarchie findet sich diese unter <http://support.microsoft.com/default.aspx?scid=fh;DE;NGNetikette>.

Diese Regeln wurde nicht willkürlich oder als Selbstzweck aufgestellt, es gab (und gibt immer noch) gute Gründe für diese Regeln, auch wenn sie einem Neueinsteiger nicht gleich ersichtlich werden. Für regelmäßige Leser der Newsgroup sind Postings, die diese Regeln nicht einhalten sehr ärgerlich, da sie sehr schwer lesbar sind (also viel Zeit kosten), weshalb es teilweise zu sehr heftigen Reaktionen kommen kann. Viele der sog. "Regulars" (das sind meist sehr kompetente Menschen, die schon seit längerem regelmäßig in der Newsgroup

posten) filtern deshalb ganz einfach Postings, die nicht den Regeln entsprechen (z. B. keinen Realname enthalten) einfach weg, werden also die Fragen nie zu Gesicht bekommen.

Wenn man also eine vernünftige Antwort auf seine Frage erhalten möchte sollte man es den potentiellen Helfern so einfach wie möglich machen:

- Erst die Postings der letzten paar Tage lesen, da bestimmte Fragen sehr häufig gestellt und beantwortet werden
- Diese FAQ und die hier verlinkten Seiten lesen
- Bei einer Suchmaschine wie z. B. <http://www.google.de> suchen. Es gibt auch sehr empfehlenswerte Suchmaschinen speziell für Newsgroups, mit denen man alte Postings durchsuchen kann (die meisten Fragen wurden bestimmt schon mehrmals beantwortet): <http://groups.google.de>
- Klare Problembeschreibungen verfassen (Welche Versionen werden verwendet, Wortlaut der Meldungen etc.)
- Vernünftige Zitierweise
- Groß- und Kleinschreibung beachten
- Realname angeben
- Ratschläge annehmen und Lernbereitschaft zeigen
- Keine allgemeinen Fragen zu Windows stellen, die nicht sicherheitsrelevant sind.

Diese FAQ soll gerade dazu beitragen häufig aufkommende Fragen zu beantworten und einige harsche Reaktionen zu vermeiden.

Weiterführende Informationen zum Thema:

Der erfolgreiche Einstieg in die Newsgroups:

<http://www.kirchwitz.de/~amk/dni/erst-lesen-dann-schreiben>

Richtig zitieren:

<http://learn.to/quote>

<http://got.to/quote>

Outlook Express richtig konfigurieren:

<http://www.oe-faq.de>

Intelligente Fragen stellen:

http://www.lugbz.org/documents/smart-questions_de.html

Allgemeine FAQ zu Windows:

<http://www.winfaq.de>

3. Wichtige Grundbegriffe

Die folgenden Begriffe tauchen in diesem Dokument immer wieder auf:

Virus Ein Virus ist ein Stück ausführbaren Programmcodes, das mit der primären Absicht geschrieben wurde, sich selbst verbreiten zu können. Wie beim biologischen Vorbild auch ist ein Computervirus nicht in der Lage, eigenständig zu existieren, sondern ist auf ein Wirtsprogramm angewiesen, mit dem er zusammen ausgeführt wird. Üblicherweise hängt sich ein Virus an den Wirt an oder überschreibt diesen teilweise mit seinem eigenen Code. Einige Viren enthalten neben der Fähigkeit, sich zu vermehren (die teilweise auch schon allein erheblichen Schaden verursachen kann) eine sog. Payload (Nutzlast) in Form einer Schadensroutine.

Trojanisches Pferd Ein Trojanisches Pferd ist ein Programm, das neben der eigentlichen (oftmals nützlich erscheinenden) Funktion eine weitere, potentiell schädliche, dem Benutzer unbekannt Funktion enthält. Beispiele hierfür sind Programme, die eingegebene Passworte stehlen oder eine Backdoor enthalten. Häufig ist auch der Begriff "Trojaner", dieser ist aber insofern inkorrekt, da er mit den historischen Wurzeln des Begriffs in Homers Ilias nicht übereinstimmt.

Backdoor Eine in einem Programm versteckte Funktion, die es, sofern man Kenntnis von ihrer Existenz hat, erlaubt, Zugriff auf ein fremdes System zu erlangen. Häufig geschieht dies durch Eingabe eines bestimmten Passworts. Heutzutage bieten die meisten Backdoorprogramme Funktionen an um sich als Server auf einen bestimmten Port zu binden und auf eingehende Verbindungen zu warten. Viele Backdoorprogramme lassen sich auch völlig normal zur Fernwartung eines Systems einsetzen, sind also nicht unbedingt "böse".

Wurm Ein Wurm ist ein Programm, das sich über Netzwerkverbindungen verbreitet. Es nutzt zu diesem Zweck Sicherheitslücken (z. B. Buffer-Overflows) in häufig eingesetzter Software aus. Im Gegensatz zum Virus ist ein Wurm auch allein ausführbar und braucht die Wirtssoftware nur um Zugriff auf ein anderes System zu erlangen. Heutzutage sind die meisten Würmer für die e-Mail Programme Outlook und Outlook Express von Microsoft geschrieben, da diese sehr weit verbreitet sind und viele Angriffspunkte bieten.

In jüngerer Zeit sind auch sehr häufig Würmer anzutreffen, die sich alleine durch die Mithilfe des Nutzers verbreiten. Diese Würmer spiegeln eine glaubwürdig klingende Nachricht vor (z. B. ein Liebesbrief, ein Sicherheitsupdate von Microsoft oder der

neueste Bildschirmschoner mit Nacktfotos irgendwelcher weiblicher Prominenten zu sein) um so den Nutzer dazu zu bewegen das Wurmprogramm auszuführen.

Hoax Ein Hoax ist eine Art Kettenbrief. Meist enthalten Hoaxes interessant klingende Nachrichten (z. B. Virenwarnung, Microsoft verschenkt Geld usw.) und fordern den Empfänger dazu auf, die Nachricht so schnell wie möglich weiter zu verbreiten. Die Inhalte der Nachrichten sind i. d. R. völlig frei erfunden. Wenn man einen Hoax als solchen erkannt hat, sollte man seinem Inhalt keinen Glauben schenken und ihn natürlich auch nicht mehr weiter verbreiten.

Patch Ein Patch ist eine Korrektur für einen aufgetretenen Fehler in einem Softwaresystem. Dabei wird keine komplett neue Version verteilt, sondern nur der schadhafte Teil ersetzt. Man kann einen Patch also mit einem Flicker auf einem kaputten Fahrradschlauch vergleichen.

Buffer-Overflow Ein Buffer-Overflow ist ein Fehler in einem Programm, der dazu führen kann, dass ein Teil des Hauptspeichers überschrieben wird und so beliebiger anderer Code ausgeführt werden kann. Fehler dieser Art treten u. a. häufig dann auf, wenn Programmierer in ihren Programmen für bestimmte Aktionen (z. B. Benutzereingaben) einen zu kleinen Speicherbereich (Puffer) vorgesehen haben und nicht überprüfen ob, die Eingabe auch in diesen paßt. Durch überlange Eingaben kann es also geschehen, dass der Puffer überläuft und Teile des eigentlichen Programms überschreibt. Besonders gefährlich wird dies, wenn der Puffer über eine Netzwerkverbindung zum Überlaufen gebracht werden kann. Häufig nutzen dies Würmer zur Verbreitung aus.

Dienst Unter einem Dienst versteht man eine Anwendung oder einen Systemprozess, der eine bestimmte Funktionalität anbietet. Meist geschieht dies über ein Netzwerk. Zum Beispiel ist ein Webserver ein Dienst, der auf einem bestimmten Port (i. d. R. TCP-Port 80) erreichbar ist. Solch ein Dienst stellt aber immer auch ein Einfallstor für Angriffe dar, weshalb man nur die Dienste anbieten sollte, die man auch anbieten will, d. h., dass ein PC, mit dem man sich bei einem Internetprovider einwählt um zu surfen, keinerlei Dienste anbieten sollte.

Bindung Über eine Bindung wird ein bestimmter Dienst mit einem bestimmten Netzwerkgerät (Modem, ISDN-Karte, Netzwerkkarte usw.) so verbunden, dass Datenpakete, die über dieses Gerät kommen, den Dienst erreichen können. Häufig spricht man im Zusammenhang auch von Interfaces, wenn man ein solches Netzwerkgerät meint. Man kann also über die Bindungen steuern, welche Dienste aus dem Internet und welche nur aus dem lokalen Netzwerk erreichbar sind. Beispielsweise sollte man die "Datei- und Druckerfreigabe" nur an das lokale Netzwerk binden und nicht an das externe Interface, das z. B. in's Internet geht, außer man möchte seine Dateien mit der ganzen Welt teilen.

Port Ein Port dient dazu, über das Internet Protokoll IP übermittelte Daten den richtigen Anwendungen/Diensten zuzuordnen. Man kann sich einen Port also als eine Art Buchse vorstellen, in die eine Datenverbindung hineingeht. Es gibt ██████ zustandsbehaftete

Ports (TCP) und ebenso viele zustandslose Ports (UDP). Ein Port kann zwei Zustände haben (offen, geschlossen). Von Haus aus ist ein Port geschlossen, erst wenn ein Dienst diesen Port öffnet um auf diesen Anfragen entgegen zu nehmen, können über den Port Daten in den Rechner gelangen. Anfragen, die an einen geschlossenen Port gesendet wurden, werden vom Betriebssystem einfach weggeworfen und durch eine entsprechende Antwort quittiert.

Portscan Bei einem Portscan wird versucht herauszufinden, ob ein bestimmter Rechner einen bestimmten Dienst anbietet. Dazu werden ein oder mehrere Datenpakete an diesen Rechner gesendet. Aus dessen Antworten (übrigens auch aus der Tatsache, dass er nicht antwortet) kann man dann schließen, ob bestimmte Ports offen sind, d. h. dass dort ein Dienst erreichbar ist. Häufig werden Portscans als Angriffe gewertet, dies sind sie aber keinesfalls. Jede Verbindungsaufnahme zu einer Gegenstelle ist schon ein Portscan, es wird zwar nur ein einzelner Port auf einem einzelnen Rechner gescannt, aber es ist und bleibt ein Portscan.

Eine ganz gute Analogie ist es, wenn man sich vorstellt mit vielen Personen in einem großen und absolut dunklen Raum (das Internet) zu sein. Man kann sich allein durch tasten mit den Händen (Senden von Paketen) orientieren. Natürlich kann es sein, dass man dabei versehentlich mit anderen Personen (die "Gescannten") in Berührung kommt und diese sich belästigt fühlen. Es kann auch sein, dass jemand diese Situation ausnutzt und ihnen die Brieftasche stiehlt (Angriff nach einem Portscan), aber an sich ist an einer solchen Berührung nichts verwerfliches, da sie die einzige Möglichkeit ist sich zu orientieren.

Firewall Eine Firewall ist ein Konzept um zwei Netzwerke voneinander zu trennen und den Datenverkehr über diese Verbindung zu kontrollieren und zu steuern. Eine solche Firewall setzt bestimmte Regeln (Policies genannt) um, die festlegen welche Kommunikation stattfinden darf und welche verboten ist. Bestandteile der technischen Umsetzung einer Firewall sind beispielsweise Paketfilter (Einrichtungen, die bestimmte Datenpakete aufgrund ihrer Herkunft, ihres Ziels usw. durchlassen oder verwerfen) oder Proxies (Einrichtungen, die den Datenverkehr bündeln und als Vermittler zwischen den Endpunkten auftreten, wobei auch hier anhand des Inhalts und des Ziels gefiltert werden kann).

4. Bei mir tauchen immer seltsame Fenster mit Werbung oder Aufforderungen zu Updates auf. Was kann ich dagegen tun?

In jüngster Zeit treten bei Nutzern von Windows 2000 und XP verstärkt unerwünschte Dialogfenster auf, die sie vor vermeintlichen Sicherheitslücken warnen oder zu zwielichtigen Sex-Angeboten locken wollen. Hinter den angegebenen URLs stehen zumeist Downloads von sog. Dialern, die durch anwählen von ■■■■ / ■■■■-Nummern erhebliche Kosten verursachen können.

Diese Nachrichten nutzen einen von Windows NT/2000/XP angebotenen Dienst um über das Netzwerk Benachrichtigungen zu versenden. Dieser Dienst heißt „*Nachrichtendienst*“. Dieser war ursprünglich dazu gedacht Mitteilungen über erledigte Druckaufträge auf Abteilungsdruckern oder Warnungen des Systemadministrators auf die Bildschirme der Anwender zu bringen. Mit der zunehmenden Verbreitung von Windows XP auf Heimrechnern wurde dieses Medium von Spammern entdeckt und genutzt, um die unerwünschte Werbung direkt auf den Bildschirm des Anwenders zu schicken, mit dem "angenehmen" Nebeneffekt, dass diese wie eine Systemmeldung aussieht.

Um sich von diesen unerwünschten Pop-Up-Nachrichten zu befreien gibt es zwei Möglichkeiten:

- Den Nachrichtendienst abstellen.
- Den zugrundeliegenden Dienst vom externen Interface entfernen.

Die erste Alternative ist schneller erledigt, sie beseitigt jedoch nur die Symptome. Wie man den Nachrichtendienst abschaltet wird hier beschrieben:

<http://www.kachold.de/winxp.html#Nach>.

Die zweite Alternative ist wesentlich empfehlenswerter, da hierdurch nicht nur die Pop-Ups verhindert, sondern auch noch andere Sicherheitslücken geschlossen werden. Wie das geht wird in den folgenden Links beschrieben:

Windows 2000: <http://www.computer-security.ch/ids/default.asp?TopicID=165>

Windows XP: <http://www.computer-security.ch/ids/default.asp?TopicID=164>

Weiterführende Informationen zum Thema:

<http://www.mynetwatchman.com/kb/security/articles/popupspam/netsend.htm>

5. Ich habe eine Nachricht bekommen, dass ich jdbgmgr.exe (die Datei mit dem Teddybär Symbol) oder sulfnbk.exe löschen soll, da dies Viren seien. Stimmt das?

Nein das stimmt nicht. Diese Mitteilungen sind Hoaxes, also schlechte Scherze. Diese Dateien sind wichtige Bestandteile des Windows Betriebssystems und sollten *auf keinen Fall gelöscht* werden. Die Datei jdbgmgr.exe gehört zum Java-System des Internet Explorer und besitzt wirklich das Teddybär-Icon. Die Datei sulfnbk.exe gehört auch zu Windows und

dient(e) dazu, lange Dateinamen vor der Zerstörung durch bestimmte ältere Datenträger-tools zu sichern.

Bevor man solchen oder ähnlichen Warnungen vor Viren glauben schenkt sollte man sich vorher bei folgender Adresse schlau machen:

<http://www.tu-berlin.de/www/software/hoax/>

Hier werden alle derzeit bekannten Hoaxes aufgelistet. Ebenfalls ist es zu empfehlen, einfach mal den Namen der Datei, vor der gewarnt wird, in eine Suchmaschine wie z. B.

<http://www.google.de> einzutippen.

6. Ich habe eine Mail mit einem Sicherheitsupdate von Microsoft bekommen. Kann ich dieser Mail trauen?

Nein! Dies ist mit sehr hoher Sicherheit eine Mail, die den Wurm "Gibe.B" (oder einen seiner mittlerweile unzähligen Nachfolger, die die selbe Legende verwenden, zu denen Dumaru.A und Swen.A gehören) enthält. Diese Familie von Würmern ist zum ersten Mal im März ■■■■ aufgetaucht, hat seit Beginn ■■■■ epidemische Ausmaße angenommen, die größte Welle wurde bisher Mitte September ■■■■ beobachtet. Er tarnt sich als vorgebliches Sicherheitsupdate von Microsoft, das angeblich bestimmte Sicherheitslücken schließen soll. Durch diese, zumindest glaubwürdig scheinende, Geschichte versucht der Wurm den Anwender dazu zu verleiten, die angehängte Programmdatei auszuführen. In Wahrheit installiert sich der Wurm (und in einigen Versionen zusätzlich noch ein Trojanisches Pferd, das eine Backdoor zum System anbietet) und versendet sich an alle eMail-Adressen, die er auf der Festplatte finden kann. Wenn man versehentlich doch den Wurm installiert hat, so sollte man den unten genannten Ratschlägen für kompromittierte Systeme (Abschnitt 10) folgen.

Generell verschickt kein Softwarehersteller unaufgefordert irgendwelche Sicherheitsupdates per eMail (man denke allein schon an die Kosten für die gewaltigen Datenmengen), statt dessen geben die Hersteller in ihren sog. Advisories (Sicherheitshinweise) immer eine Adresse an, wo die entsprechenden Patches zum Download stehen (meist wird dort auch nochmal der Wortlaut der eMail wiederholt). Zusätzlich sind alle Mails, die Microsoft mit Sicherheitshinweisen verschickt, durch eine digitale Signatur (PGP) unterzeichnet, so dass der Ursprung verifiziert werden kann.

Falls man also von einem Softwarehersteller unaufgefordert "Sicherheitsupdates" oder Ähnliches zugesandt bekommt, sollte man keinesfalls die Dateien ausführen, auch wenn diese eine noch so glaubwürdig klingende Botschaft enthalten.

Weiterführende Informationen zum Thema:

Informationen von Microsoft zu dem Thema:

<http://www.microsoft.com/germany/technet/sicherheit/bulletins/>

bogusmails.mspix

Informationen des BSI zu Gibe.A:

<http://www.bsi.de/av/vb/gibe.htm>

Informationen des BSI zu Dumaru.A / Mimapil.A:

<http://www.bsi.de/av/vb/dumaru.htm>

Informationen des BSI zu Swen.A:

<http://www.bsi.de/av/vb/swena.htm>

7. Outlook Express blendet alle Dateianhänge aus. Wie kann ich sie wieder anzeigen lassen?

Seit Outlook Express 6 SP1 (im Service Pack 1 für den Internet Explorer 6 enthalten) enthält Outlook Express eine neue "Virenschutzfunktion", die standardmäßig aktiviert ist. . .

Ein Auszug aus der entsprechenden Readme-Datei:

Der Virenschutz ist die Antwort auf die anhaltende Bedrohung durch E-Mail-Viren. Damit werden programmgestützte Sendevorgänge blockiert und Benutzer können angeben, ob Anlagen geöffnet oder gespeichert werden sollen. Auf diese Option zum Blockieren der vordefinierten Listen von Dateitypen kann zugegriffen werden, indem Sie im Menü "Extras" auf "Optionen" klicken und auf der Registerkarte "Sicherheit" das Kontrollkästchen "Speichern oder Öffnen von Anlagen, die möglicherweise einen Virus enthalten könnten, nicht zulassen" aktivieren. Diese Option ist bei Neuinstallationen und Updates standardmäßig aktiviert.

Die von OE teilweise verwendete Meldung "folgende unsichere Attachments wurden gelöscht" ist dabei irreführend: OE löscht keine Attachments, sondern verwehrt nur den Zugriff darauf, indem es sie ausblendet. Nach dem Deaktivieren der o.a. Option (Extras - Optionen - Sicherheit - Speichern oder Öffnen von Anlagen, die möglicherweise einen Virus enthalten könnten, nicht zulassen) sind alle Attachments wieder verfügbar.

Weiterführende Informationen zum Thema:

Artikel der Microsoft Knowledge Base zum Thema:

<http://support.microsoft.com/?kbid=329570>

<http://support.microsoft.com/?kbid=291387>

Allgemeine Fragen zu Outlook Express:

<http://www.oe-faq.de>

FAQ-Artikel zum Thema:

<http://oe-faq.de/?56FAQ:2.11>

<http://insideoe.tomsterdam.com/faqs/why.htm#oe6attach>

Newsgroup zum Thema:

<news:microsoft.public.de.german.inetexplorer.ie6.outlookexpress>

8. Meine Personal Firewall macht Probleme / meldet Angriffe. Was kann ich tun?

Sog. *Personal Firewalls* oder auch *Desktop Firewalls* sind heute sehr in Mode und werden von einigen "Fachzeitschriften" und selbsternannten "Fachleuten" sehr propagiert. Diese Programme sind keine richtigen Firewalls, da eine Firewall ein Sicherheitskonzept und dessen technische Realisierung ist. Personal Firewalls enthalten kein Konzept, denn sie melden nur Anhand bestimmter Regeln „verdächtige“ Datenpakete. Diese Meldungen werden von einem mit der Materie nicht vertrauten Anwender meist fehlinterpretiert und sind somit nutzlos.

Die gemeldeten "Angriffe" sind in über █% der Fälle harmlose Portscans, Anfragen von Filesharingprogrammen (wie z. B. eDonkey) oder schlicht Antworten auf vom eigenen Rechner versandte Datenpakete, also einfach das völlig normale und harmlose Hintergrundrauschen des Internet.

Die Verfechter der Personal Firewalls führen einige gut klingende Argumente an, die für die Nutzung eines solchen Produkts sprechen sollen. Bei genauerem Hinsehen halten diese jedoch einer objektiven Betrachtung nicht stand. Eine ausführliche Auseinandersetzung mit diesen Argumenten findet sich unter <http://faq.underflow.de/pfargumente/>

Aufgrund dieser konzeptionellen Schwächen kann man von Personal Firewalls als Sicherheitsmaßnahme nur abraten. Solche Programme taugen allenfalls dazu, mehr über das eigene System zu lernen, doch selbst dazu gibt es passendere Werkzeuge.

Weiterführende Informationen zum Thema:

de.comp.security.misc-FAQ:

<http://www.stud.tu-ilmenau.de/~traenk/dcsm.htm#Firewall>

de.comp.security.firewall-FAQ:

<http://www.iks-jena.de/mitarb/lutz/usenet/Firewall.html>

Felix von Leitners Papers zum Thema (sehr deutlich!):

<http://www.fefe.de/pffaq/halbesicherheit.txt>

<http://www.fefe.de/pffaq/>

FAQ des Rechenzentrums der Universität Heidelberg:

<http://www.urz.uni-heidelberg.de/Netzdienste/firewall/pers-firewall.shtml>

Eine weitere FAQ zu dem Thema:

<http://www.nabooisland.com/publications/pffaq/>

Wie Personal Firewalls umgangen werden:

<http://home.arcor.de/nhb/pf-umgehen.html>

<http://www.stud.tu-ilmenau.de/~traenk/zaweg.htm>

<http://my-forum.netfirms.com/zone/zcode.htm>

<http://www.pcflank.com/art21.htm>

<http://www.computerbetrug.de/firewalls-umgehung.php>

Warum Personal Firewalls auch in Zukunft nicht sicher sein werden (englisch):

<http://www.freefire.org/grc-letter.html>

Ein Tool zum Testen der Lücken der eigenen Personal-Firewall:

<http://www.atelierweb.com/awft/>

IPSec-Policies:

<http://cert.uni-stuttgart.de/os/ms/ipsec-paketfilter.php>

Firewall-Konzepte:

<http://www.oreilly.de/catalog/fire2ger/chapter/>

Sicherheit in Netzen: <http://www.netzmafia.de/skripten/sicherheit/index.html>

TCP/IP Grundlagen:

<http://kris.koehntopp.de/artikel/tcpip-technik/>

<http://www.netzmafia.de/skripten/netze/netz8.html>

http://www.lug-sw.de/tcp_ip.html

<http://people.ee.ethz.ch/~strub/tcp-ip/tcp-ip.html>

9. Wie kann ich denn nun mein System vernünftig absichern?

Um ein System sicher zu machen muß man sich erst über einige Dinge klar werden:

- Welche Bedrohungen können auftreten?
- Welchen Sicherheitsgrad benötige ich?
- Welche Schäden / Folgen können auftreten, wenn mein System kompromittiert wird?
- Auch wenn ich keine wichtigen Daten habe, kann mein Rechner trotzdem als Ausgangspunkt für Angriffe auf weitere Rechner dienen
- ■■■%ige Sicherheit gibt es nicht!
- Sicherheit gibt es nicht umsonst, d. h. es kostet Zeit und/oder Geld ein System abzusichern!

Eine viel tiefgehendere Einführung in die Thematik der Sicherheitskonzepte und ihrer Realisierung findet sich im "Site Security Handbook" der IETF (RFC ■■■■). Das Dokument richtet sich zwar primär an professionelle Systemadministratoren, jedoch ist es auch für erfahrenere Heimanwender als Überblick zu empfehlen. Im "User' Security Handbook" der IETF (RFC ■■■■) findet sich eine sehr empfehlenswerte allgemeine Zusammenfassung von möglichen Bedrohungen und entsprechenden Gegenmaßnahmen, die ganz speziell auf Anwender zugeschnitten ist.

Wenn man sich über die eigenen Anforderungen an ein Sicherheitskonzept klar geworden ist, kann man beginnen solch ein Konzept aufzustellen und es dann zu realisieren.

Für den typischen Heimanwender (Rechner mit Dial-Up-Zugang ins Internet, evtl. noch ein kleines Heimnetzwerk) sollten folgende Maßnahmen eine vernünftige Grundlage, auf der man ein entsprechendes Konzept aufbauen kann, sein:

- Keine nicht vertrauenswürdige Software (z. B. aus dubiosen Quellen) nutzen, nur Original-Software einsetzen.
- Ein Betriebssystem verwenden, das verschiedene Benutzerrechte anbietet (z. B. Windows NT/2000/XP).
- Ein Dateisystem, das ACLs (Zugangsberechtigungen) anbietet einsetzen (z. B. NTFS) und natürlich auch entsprechende ACLs setzen.
- Nie als Administrator arbeiten. Vor administrativen Arbeiten genau nachdenken was man tut. Achtung: unter Windows 9x und Windows ME ist jeder Nutzer automatisch Administrator!

Einige (schlecht programmierte) Anwendungen erfordern für den Betrieb Zugriff auf Dateien oder Registry-Einträge, für die ein normaler Anwender keine ausreichende Berechtigungen besitzt. Ein fortgeschrittener Anwender kann solche Dateien und

Registry-Einträge mit Werkzeugen wie FileMon und RegMon identifizieren und die Berechtigungen entsprechend anpassen. Eine weitere Möglichkeit ist es solchen Programmen administrative Rechte zu geben, indem man mittels Werkzeugen wie runas (Bestandteil von Windows) oder SUperiorSU ausführt, was jedoch ein Sicherheitsrisiko darstellt, da der Anwender so auf Dateien (und evtl. auch Anwendungen) zugreifen kann, für die er selbst keine Berechtigungen besitzt.

- Für jeden Benutzer sichere Passwörter verwenden, d. h. mindestens ■ Zeichen lang, Kombinationen aus Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen. Vor allem sollten keine Begriffe aus dem privaten Umfeld (Name der Freundin, des Hundes, Autokennzeichen o.Ä.) oder aus irgendwelchen Wörterbüchern verwendet werden. Die Passwörter sollte man regelmäßig (mindestens einmal im Jahr) wechseln und keinesfalls notieren (außer vielleicht auf einem Zettel, der im Safe liegt).
- Alle unnötigen Dienste abschalten, die benötigten Dienste nur an die Interfaces binden, auf denen sie benötigt werden. Wegen grober Fehler in der Architektur von Windows können manche Dienste nur global für alle Interfaces gesteuert werden, was zur Folge haben kann, dass z. B. die "Netzwerkumgebung" nicht mehr im vollen Umfang funktioniert, wenn man einen solchen Dienst beendet. Für diese Aufgabe gibt es im Netz entsprechende Anleitungen und automatisierte Skripte, die es auch Laien ermöglichen, eine sichere Konfiguration zu erreichen.

Sollte man also auf die entsprechenden Dienste im LAN angewiesen sein, so ist zu empfehlen einen externen Paketfilter für den Internetzugang zu verwenden. Keinesfalls sollte man auf hostbasierte Paketfilter wie die sog. "Personal Firewalls" zurückgreifen, da dieser Ansatz keine Sicherheit bringen kann. Eine Alternative zur Paketfilterung auf dem Host selbst können in begrenztem Maße die IPSec-Policies sein, wobei diese als kleinen Schönheitsfehler keine standardkonformen "Reject"-Regeln erlauben, sondern Pakete nur vollständig blocken können, d. h. ohne Fehlermeldung an die Gegenstelle verwerfen.

- Inhärent unsichere Software, die in der Vergangenheit schon oft durch Sicherheitslücken aufgefallen ist (z. B. Internet Explorer, Outlook / Outlook Express, Internet Information Server, Filesharing-Tools, ICQ & Co.), durch bessere Alternativen (z. B. Mozilla Firefox, Opera, Apache usw.) ersetzen bzw. wenn möglich ganz darauf verzichten.
- Die genutzte Software sicher konfigurieren. Z.B. ActiveX und Active Scripting / Java Script deaktivieren, Makro-Funktionalitäten in den Office Produkten einschränken (wenn man sie nicht benötigt, einfach ganz deaktivieren) etc.
- Sicherheitsupdates zeitnah nach dem Erscheinen einspielen. Dies kann z. B. durch regelmäßige, d. h. mindestens einmal wöchentliche, Nutzung von Windows Update (zwar nicht optimal, aber für den Heimanwender immer noch die beste Lösung) geschehen.

Für alle, die Windows-Update aus verschiedensten Gründen nicht nutzen wollen oder können, existieren Quellen, die Skripte zum Download und zur Offline-Installation der Patches für MS Windows anbieten, die ohne Windows Update auskommen. Diese Skripte erlauben es auch, sich die Patches einmal herunterzuladen und auf vielen verschiedenen Rechnern offline einzuspielen.

- Sicherheits-Mailinglisten abonnieren, um über neue Schwachstellen und Patches informiert zu sein. Beispiele sind Bugtraq (englisch, relativ hohes Nachrichtenaufkommen) oder RUS-CERT-Ticker (deutsch, umfassende Bewertungen, leider momentan nur eingeschränkter Betrieb). Auch einzelne Softwarehersteller wie z. B. Microsoft bieten solche Dienste per e-Mail an, die auf Probleme mit den Programmen des jeweiligen Herstellers beschränkt sind.
- Bei fremden Dateien (z. B. aus Downloads oder eMail-Anhängen) lieber zweimal nachdenken bevor man sie ausführt. Bei unverlangten Attachments lieber beim Absender nachfragen, ob diese auch von ihm stammen. Achtung: auch scheinbare Datendateien (wie z. B. von diversen Office-Programmen) können ausführbare Inhalte besitzen und damit gefährlich sein!

Als ganz einfache Regel kann man sagen, dass man nur die Attachments oder Downloads öffnen sollte, bei denen man keinerlei Zweifel an deren Ursprung und Vertrauenswürdigkeit hat. Sobald man auch nur ein bißchen zweifelt, sollte man lieber zuerst beim Absender nachfragen, oder ganz auf das Öffnen verzichten und die Mail löschen. Keine Angst, man "blamiert" sich durch das Nachfragen keineswegs, im Gegenteil, es ist ein Zeichen für sichere Beherrschung des Mediums (natürlich nur, wenn man dem Gegenüber den Grund der Nachfrage erklärt). Das Einzige, was wirklich peinlich werden kann, ist, wenn man den gesamten Bekanntenkreis mit Viren/Würmern überschüttet, und eben dies wird so verhindert.

- Evtl. einen Virenschanner einsetzen (nicht den sog. „residenten“ Teil, der ständig im Hintergrund nach Schadprogrammen sucht, da dieser so gut wie keinen Sicherheitsgewinn bringt und zudem immens Rechenleistung verbraucht). Wenn man stets alle Sicherheitsupdates rechtzeitig einspielt, vernünftige und korrekt konfigurierte Software einsetzt und die nötige Vorsicht mit fremden Dateien walten läßt, sollte aber ein Virenschanner unnötig sein.

Man muß sich, falls man sich doch für ein solches Programm entscheidet, aber sehr genau im klaren darüber sein, dass Virenschanner ausschließlich bekannte, unmodifizierte Viren erkennen können (und das auch nur mit Erfolgsquoten von maximal 95%). Bei allen neu auftretenden Viren / Würmern ist man auch mit Scanner schutzlos, da ein Wurm sich heutzutage in ■■ Tagen weltweit verbreiten kann und i. d. R. einige Stunden bis etwa ■ Tage (dies hängt vom Hersteller und dem gewählten Update-Service ab) vergehen bis erste Signaturupdates für die Scanner verfügbar sind. Teilweise werden Bestandteile eines Schadprogramms von den Herstellern der Virenschanner überhaupt nicht als solche erkannt, wie es z. B. lange Zeit bei einem Teil der "Nutzlast" des Sobig.A Wurms der Fall war. Deshalb sollte man, wenn man einen Scanner

einsetzt trotzdem mindestens genauso vorsichtig sein wie ohne und zudem regelmäßig (wöchentlich dürfte ein guter Kompromiß sein) Signaturupdates einspielen um ein einigermaßen vernünftiges Maß an Sicherheitsgewinn aus einem Virens Scanner ziehen zu können.

Wenn man diese Einschränkungen nicht kennt, oder nicht beachtet, kann sich, wegen der Mängel des Konzepts und des Effekts der Risikokompensation, durch die Nutzung eines Virens Scanners das Sicherheitsniveau sogar verschlechtern.

- Regelmäßige Backups der Daten (nicht der Programme, denn diese verbrauchen nur unnötig Zeit und Platz auf den Backupmedien und können von den Original Datenträgern schneller neu installiert werden) durchführen und die Backupmedien vom Rechner getrennt aufbewahren. Man sollte sich aber auch regelmäßig vergewissern, dass die Backups auch wieder zurückgespielt werden können.
- Ein Konzept für den Fall einer Kompromittierung des Systems griffbereit haben.

Weiterführende Informationen zum Thema:

Dienste abstellen:

Windows 2000: <http://www.computer-security.ch/ids/default.asp?TopicID=165>

Windows XP: <http://www.computer-security.ch/ids/default.asp?TopicID=164>

Dienste abstellen mit einem automatischen Skript, das die empfohlene Konfiguration der vorgehenden

<http://www.ntsvcfg.de/>

Das ganze als "one-click" Lösung für absolute Laien:

<http://www.dingens.org/>

Windows Updates offline installieren:

<http://winpatches.freewww.info/>

RUS-CERT:

<http://cert.uni-stuttgart.de>

Bugtraq:

<http://www.securityfocus.com/archive/1>

Microsoft Sicherheitsbenachrichtigungsdienst:

<http://www.microsoft.com/germany/technet/datenbank/articles/430926.aspx>

"Users' Security Handbook" / RFC 2504 (engl.):

<ftp://ftp.rfc-editor.org/in-notes/rfc2504.txt>

"Site Security Handbook" / RFC 2196 (engl.):

<ftp://ftp.rfc-editor.org/in-notes/rfc2196.txt>

Unbeobachtete Sicherheitslücken im Internet Explorer:

<http://www.safecenter.net/UMBRELLAWEBV4/DirSvc/security/trie/index.html>
<http://www.pivx.com/larholm/unpatched/>

Browser sicher konfigurieren:

<http://www.heise.de/security/dienste/browsercheck/anpassen/>

Grundlegende Tipps zur Absicherung einer neuen Windows 2000 Installation:

<http://www.microsoft.com/germany/technet/datenbank/articles/600237.msp>

Grundlegende Tipps zur Absicherung einer bestehenden Windows 2000 Installation:

<http://www.microsoft.com/germany/technet/datenbank/articles/600236.msp>

Beschreibung der Dienste von Windows 2000:

http://www.different-thinking.de/windows_2000_dienste.php

IPSec-Policies:

<http://cert.uni-stuttgart.de/os/ms/ipsec-paketfilter.php>

Online Sicherheitscheck des niedersächsischen Datenschutzbeauftragten:

<http://check.lfd.niedersachsen.de/start.php>

Sicherheitslücken des Browsers testen:

<http://www.heise.de/ct/browsercheck/>

Sicherheitsmaßnahmen im Überblick:

<http://www.enyo.de/hweimer/security/massnahmen.html>

Sicherheitsratgeber des Bundesamt für Sicherheit in der Informationstechnik (BSI):

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

Gefahren durch Aktive Inhalte:

<http://www.bsi.bund.de/fachthem/sinet/aktiveinhalte/index.htm>

Sicherheit in Netzen: <http://www.netzmafia.de/skripten/sicherheit/index.html>

Wie Virens Scanner von Schadprogrammen umgangen werden:

<http://members.lycos.co.uk/scheinsicherheit/>

Warum Kompromittierungen nicht unvermeidbar sind:

<http://www.mathematik.uni-marburg.de/~wetz/mj/index.php?viewPage=sec-compromise.html>

Häufige Missverständnisse in der Computersicherheit (engl.):

<http://plastictree.net/articles/securitymisconcept/index.html>

Regmon und Filemon:

<http://sysinternals.com/Utilities/Filemon.html>

<http://sysinternals.com/Utilities/Regmon.html>

SUperior SU:

<http://www.stefan-kuhr.de/supsu/main.php3>

10. Ich habe einen Virus / Dialer / "Trojaner" / wurde "gehackt". Was soll ich tun?

Wenn ein System kompromittiert wurde, sollte man genau wissen wie man zu verfahren hat, um den Schaden einzudämmen. Virens Scanner bieten zwar als einfache Lösung an, das System zu "säubern", dies kann aber nicht erfolgreich sein, da ein Angreifer (Virus / Wurm / Dialer / Cracker etc.) längst beliebige Systemdateien ersetzt haben könnte (und vermutlich auch hat) und sich so im System festgesetzt hat. Solch einer Reinigung durch einen Virens Scanner kann man nur dann vertrauen, wenn man Prüfsummen aller (System-)Dateien hat und diese auch von einem Nachweisbar sauberen Datenträger aus verifizieren kann. Dies ist jedoch sehr selten der Fall, da ein solches Verfahren auf einem Desktop-System kaum zu realisieren ist.

Deshalb sollte man folgendes Vorgehen wählen:

1. System sofort von allen Netzwerkverbindungen (LAN, Internet etc.) trennen.
2. Evtl. den gesamten Inhalt der Systemdatenträger sichern, um im Falle eines straf-/ zivilrechtlichen Vorgehens Beweise zu haben. Für die meisten Heimanwender dürfte dies aber nicht nötig sein. Eine Ausnahme bildet der Fall, dass man einen sog. "Dialer" installiert hat. Hier sollte man auf jeden Fall eine Vollsicherung durchführen. Falls man vermutet, dass auch schon Kosten angefallen sind, sollte man evtl. sogar den gesamten Rechner als Beweismittel zur nächsten Polizeidienststelle bringen und Anzeige erstatten.
3. Feststellen welcher Art die Kompromittierung war und auf welchem Wege das System

kompromittiert wurde.

4. Alle evtl. betroffenen Dritten informieren.
5. Evtl. nötige Patches und Updates herunterladen. Hierzu ist ein sauberer Rechner notwendig, wie z. B. ein anderes System, oder ein Rettungssystem, wie z. B. Knoppix, das von CD lauffähig ist. Die Patches und Updates sollten wenn möglich auf einem schreibgeschützten Datenträger (CD-ROM, Diskette etc.) gespeichert werden, damit sie nicht kompromittiert werden können.
6. Alle Passwörter, die auf dem kompromittierten System verwendet wurden (also z. B. Login-, Mail- oder Website-Passwörter, aber auch die PIN für das Online-Banking) sofort ändern oder sperren lassen, da ein Angreifer die Passwörter z. B. verwenden kann, um erneut in das abgesicherte System einzudringen oder mit der Identität des Nutzers Transaktionen im Internet auszuführen.
7. Alle Datenträger neu formatieren und sämtliche Software von den Originaldatenträgern neu einspielen.
8. Das letzte, vor der Kompromittierung erstellte, Backup der Daten (nicht die Vollsicherung, die zu Beweis Zwecken erstellt wurde!) zurückspielen.
9. Die genutzte Sicherheitslücke (z. B. durch Einspielen der nötigen Patches) schließen und prüfen, ob es evtl. weitere, ähnliche Lücken gibt und diese ebenfalls schließen.
10. Erst jetzt das System wieder an die Netzwerke anbinden.
11. Konsequenzen aus dem Vorfall ziehen und ggf. das eigene Sicherheitskonzept entsprechend anpassen.

Dieses Verfahren wird auch von Microsoft, CERT und den entsprechenden Abschnitten des "Users' Security Handbook" der IETF (RFC ■■■■, Abschnitt ■.■) als Maßnahme zur Beseitigung einer Kompromittierung empfohlen.

Dass es wirklich nicht ausreichend ist, nur das Schadprogramm allein durch einen Virens scanner entfernen zu lassen, hat der Wurm Sobig – in all seinen Varianten – gezeigt. Er installierte unbemerkt (auch von Antivirus-Herstellern) ein Trojanisches Pferd und zusätzlich eine modifizierte Version des WinGate Proxies, der u. a. von Spam-Versendern zur Verschleierung ihrer Identität oder als quasi anonyme Ausgangsbasis für Angriffe auf andere Systeme mißbraucht wird. Nähere Informationen zu diesem Vorfall finden sich unter <http://www.lurhq.com/sobig.html> und <http://www.lurhq.com/sobig-e.html> (englisch).

Weiterführende Informationen zum Thema:

Empfehlungen von Microsoft:

<http://www.microsoft.com/technet/community/columns/secgmt/sm0504.aspx>
<http://www.microsoft.com/germany/technet/datenbank/articles/600230.aspx>

Warum nach einer Kompromittierung der Rechner nicht mehr dir gehört:

<http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.aspx>

Empfehlungen des CERT (engl.):

<http://www.cert.org/security-improvement/practices/p051.html>

"Users' Security Handbook" / RFC 2504 (engl.):

<ftp://ftp.rfc-editor.org/in-notes/rfc2504.txt>

Warum Kompromittierungen nicht unvermeidbar sind:

<http://www.mathematik.uni-marburg.de/~wetz/mj/index.php?viewPage=sec-compromise.html>

Knoppix Live-CD:

<http://www.knopper.net/knoppix/>

11. Ich habe eine Datei / einen Ordner verschlüsselt und nun Probleme damit. Was muß ich beachten?

Die neueren Windows-Varianten bieten eine Erweiterung des NTFS-Dateisystems namens EFS (Encrypting File System) an, mittels derer man einzelne Dateien oder ganze Verzeichnisse verschlüsseln kann. Dabei kommt auch ein sog. Public-Key Verfahren zum Einsatz. Bei diesem existiert ein öffentlicher (d. h. frei zugänglicher) Schlüssel und ein privater (geheimer) Schlüssel. Der private Schlüssel wird im Profil des jeweiligen Benutzers als sog. Zertifikat gespeichert und wird zum Entschlüsseln der verschlüsselten Daten benötigt.

Hierbei gibt es einige Probleme, die dazu führen können, dass der Schlüssel verloren geht und die Daten nicht mehr zugänglich sind. Bei folgenden Gelegenheiten kann dies geschehen:

- Bei der Neuinstallation (auch beim sog. "Überinstallieren") von Windows
- Beim Löschen und der anschließenden Neu-Anlage eines Benutzers unter dem selben Namen
- Teilweise beim Import eines zuvor gesicherten Schlüssels

- Beim Ändern eines Passworts durch den Administrator (nur unter Windows 2000)

Die ersten beiden Probleme beruhen darauf, dass der Schlüssel fest mit der SID (einer eindeutigen Kennnummer) des Benutzers verbunden ist. Bei diesen beiden Aktionen ändert sich diese SID und der Schlüssel wird unbenutzbar. Im dritten Fall, der vor allem bei Windows 2000 auftritt, ist noch nicht genau geklärt, woran es liegt, man sollte aber äußerst vorsichtig beim Import/Export seiner Zertifikate sein. Der letzte Fall tritt auf, da unter Windows 2000 der Schlüssel mit dem Anmeldekennwort des Nutzers gesichert wird.

Für den Fall des Verlustes eines Schlüssels wird für jeden Benutzer ein "Nachschlüssel" beim sog. "Recovery Agent" des Systems (meist ist dies der Administrator) hinterlegt, mit dem man wieder an die Daten gelangen kann.

Vom Sicherheitsstandpunkt her muß man anmerken, dass das Zertifikat allein durch das Anmeldekennwort des Benutzers geschützt ist. Wenn dieses also gebrochen wird, sind automatisch auch die Dateien lesbar.

Wenn man die Sicherheitsrisiken und den möglichen Datenverlust in Betracht zieht, kann man EFS nur eingeschränkt empfehlen. Andere (teilweise frei verfügbare) Programme wie z. B. Scramdisk, PGPDisc, DriveCrypt (der kommerzielle Nachfolger von Scramdisk), SafeGuard Easy, Controlbreak SafeBoot Solo und GPG sind hier eher zu empfehlen, da sie weniger Gefahren bei mindestens gleichwertigem Sicherheitsniveau bieten.

Weiterführende Informationen zum Thema:

Anleitungen zur Einrichtung und zum Gebrauch von EFS:

<http://www.kire.ch/datenschutz/efs.htm>

<http://www24.brinkster.com/thorsten123/faq/partitionieren/win2000/enc.htm>

Drive-Crypt:

<http://www.drivecrypt.com/>

GPG:

<http://www.gnupg.de/>

PGPDisk:

<http://www.pgpi.org/products/pgpdisk/>

Scramdisk:

<http://www.scramdisk.clara.net/>

Utimaco SafeGuard Easy:

<http://www.utimaco.de>

Controlbreak SafeBoot Solo:

<http://www.safeboot.com>

12. Die Startseite meines Internet Explorers wurde verändert. Was kann ich dagegen tun?

In jüngerer Zeit tritt massiv das Phänomen auf, dass die Startseite des Internet Explorers nach dem Surfen im WWW verändert ist oder unerwünschte Toolbars im Internet Explorer auftauchen. Meistens tritt dieses Verhalten erst nach dem nächsten Start des Internet Explorers auf, so dass der genaue Grund kaum nachvollziehbar ist, und ist auch nicht durch manuelles Einstellen der Startseite dauerhaft zu beheben. Zumeist wird dabei die Startseite auf ein Erotikangebot, eine bestimmte Suchmaschine oder eine sog. Bannerseite umgeleitet. All diesen Angeboten ist gemein, dass die Anbieter, wie z. B. Xupiter oder Lop.com, damit Geld verdienen möchten. Dieses Phänomen wird häufig "Hijacking" genannt, die Software die dahinter steckt wird als "Spyware" bezeichnet. Dabei wird die Tatsache, dass sehr viele Nutzer mit viel zu laxen Sicherheitseinstellungen für den Internet Explorer "unterwegs" sind, keine Sicherheitsupdates einspielen, oder leichtfertig Sicherheitsabfragen bestätigen, ausgenutzt, um entsprechende ActiveX-Controls, Erweiterungen für den Internet Explorer (auch Browser Helper Objects genannt), Scripte oder Plugins in das System des Anwenders einzuschleusen, die dafür sorgen, dass sich diese Einstellungen im Internet Explorer "festsetzen". Schlimmer noch, eine Vielzahl der Spyware-Programme zeichnet detailliert das Surf-Verhalten (und evtl. noch wesentlich persönlichere Daten, wie z. B. Passwörter) des Benutzers auf und übermittelt es an den Ersteller dieser zweifelhaften Software. Über die Gefährdung der Privatsphäre des Nutzers hinaus haben diese Programme teilweise auch massive Auswirkungen auf die Stabilität und die Geschwindigkeit des Systems, so dass häufig Abstürze oder langsame Reaktionen auf Eingaben zu beobachten sind.

Wie kann man denn nun mit solch einer Veränderung umgehen? Zunächst muss man sich klarmachen, dass durch die eingeschleusten Programme beliebige Veränderungen am System, neben den offensichtlichen häufig auch versteckte, vorgenommen worden sein können. Deshalb ist auch hier das im obigen Abschnitt zum Umgang mit Kompromittierungen (Abschnitt 10) angegebene Verfahren dringend zu empfehlen.

Wem dieses Verfahren zu aufwändig ist, der kann sich für den Einsatz eines der sog. "Spyware-Cleaner" Programme, wie z. B. AdAware, Spybot etc. entscheiden. Diese Programme können i. d. R. die meisten bekannten und harmloseren Schadprogramme beseitigen. Dabei muss man sich allerdings darüber im Klaren sein, dass diese Programme gegen neue oder unbekannte Varianten keine Chance haben können und auch keine weitergehenden Änderungen am System, die evtl. vorgenommen wurden, beheben können. Vielfach decken diese Spyware-Cleaner nur einen Teil der in Umlauf befindlichen Spyware-Varianten ab, so dass es oft erforderlich ist, mehrere solcher Reinigungsprogramme zu verwenden. Aggressive Varianten der Spyware graben sich teilweise sehr tief in das System ein und können so sogar die Reinigungsprogramme blenden und ihre Existenz so verschleiern. Deshalb muss hier nochmal darauf hingewiesen werden, dass nur das im obigen Abschnitt zum Umgang

mit Kompromittierungen (Abschnitt 10) angegebene Verfahren diese Programme wirklich zuverlässig beseitigen kann.

Wie kann man sich in Zukunft vor solchen Programmen schützen? Da diese Programme (bisher) ganz gezielt die Möglichkeiten des Internet Explorers ausnutzen, die von keinem anderen Browser in dieser Form geboten werden, ist die einfachste Lösung, vom Internet Explorer auf einen sichereren Web-Browser wie z. B. Mozilla Firefox oder Opera umzusteigen. Alle Nutzer, die zu einem Wechsel nicht bereit sind, sollten die Sicherheitseinstellungen des Internet Explorer auf wesentlich striktere Einstellungen ändern und regelmässig Sicherheitsupdates für ihren Browser einspielen (was natürlich auch für die alternativen Web-Browser gilt). Generell sollte man aber auf jeden Fall die im obigen Abschnitt über die Absicherung des Systems (Abschnitt 9) gegebenen Ratschläge beachten.

Weiterführende Informationen zum Thema:

Mozilla Firefox <http://www.mozilla.org/products/firefox/>

Opera <http://www.opera.com/>

Spybot Search&Destroy:

<http://www.safer-networking.org/de/spybot/d/index.html>

AdAware:

<http://www.lavasoft.de/german/software/adaware/>

HijackThis (für erfahrene Nutzer):

<http://www.tomcoyote.org/hjt/>

<http://www.spywareinfo.com/~merijn/>

13. Dank an ...

In alphabetischer Reihenfolge:

- Wolfgang Ewert
- Carsten Krueger
- Arno Luppold
- Paul Muster
- Bernd H. Steiner

- Urs Tränkner
- uvm.