Spyware und Hijacker

Spyware schnüffelt in Ihrem Privatleben, Hijacker entführen Ihren Webbrowser. Schützen Sie sich vor Befall und fegen Sie die Parasiten von der Platte.

ILLUSTRATION RICHARD TUSCHMAN

von Christian Bütikofer

Hilfe, mein Computer hat Bock auf Sex!» Die Kummerkasten-Anfrage von PCtipp-Leser Peter Hauser (Name geändert) war kein Witz: Sein Computer lädt bei jedem Start ein eindeutiges Hintergrundbild, der Media Player startet einen Porno, im Balken des Internet Explorers leuchtet ihm die Botschaft «Sex is great!» entgegen und die Startseite des Browsers landet auf einer Porno-Seite. Peter Hauser versuchte die unerwünschten Einträge zu löschen – ohne Erfolg. Porno-Magie? Keineswegs.

Seit Mitte 2003 verbreitet sich eine neue Computer-Seuche rasant im Internet: so genannte Hijacker. Hijacker (engl. to hijack/highjack = entführen) leiten Ihren Browser auf Internetseiten um, die Sie nicht wollen. Plötzlich nisten sich fremde Webseiten im Favoritenordner des Internetbrowsers ein. Wenn Sie im Browser eine WWW-Adresse eintippen, landen Sie auf einer völlig anderen Webseite, die Standardseite des Browsers wurde ausgetauscht. Von Ihnen ungewollt fummeln die Übeltäter in Ihrem System herum und halten Sie zum Narren.

Internetabzocker machen sich Sicherheitslücken des Internet Explorers zu Nutze, statten Webseiten oder Programme (meist Browser-Erweiterungen, so genannte Browser Helper Objects, BHO) mit Funktionen aus, um Sie auf ihre luschen Internetangebote zu locken oder mit Spyware Ihr Konsum- und Surfverhalten auszuspionieren. Manchmal macht sich diese so genannte Malware nach dem erfolgreichen Eindringen ins System ausserdem an der → Registry zu schaffen. Doch damit nicht genug. Oft werden zusätzlich noch Trojaner installiert: Programme, die Ihren PC zu einem offenen Tor für Angriffe aus dem Netz machen.

Falsche oder zu schwache Sicherheitseinstellungen des Internet Explorers sind der Hauptgrund für den Erfolg von Hijackern und Spyware. Wie Sie das ändern können, lesen Sie zum Thema Hijacker im nächsten Abschnitt und zum Thema Spyware ab S. 25.

→ FACHCHINESISCH

Registry

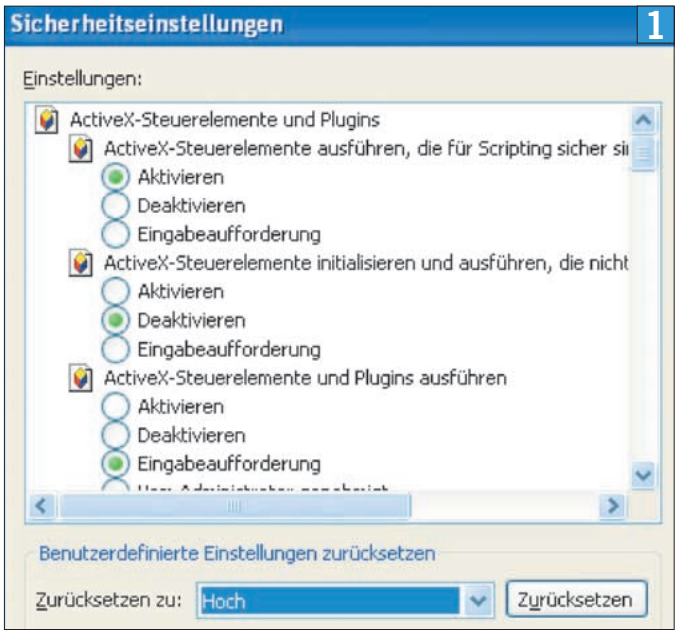
Die Registry ist seit Windows 95 das Herz des Betriebssystems. Es handelt sich dabei um eine spezielle Datenbank, die von Windows verwaltet wird. Auf Grund der Registry weiss Windows, wie gewisse Dateitypen (Dokumente, Kalkulationstabellen etc.) bearbeitet werden müssen oder wie das Einbetten von Objekten (OLE) in Dokumente abgehandelt werden muss.

Script

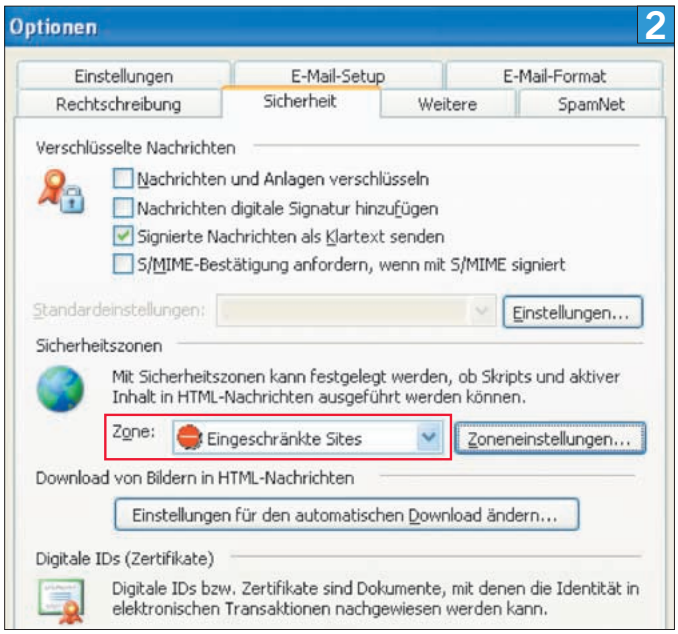
Script-Sprachen werden oft eingesetzt, um Internetseiten interaktiv zu gestalten. Beispiel: Verändert sich auf einer Website ein Button, wenn Sie mit der Maus darüber fahren, ist meist JavaScript im Spiel.

HTML

HyperText Markup Language; Datenformat von Webseiten.



Internet Explorer: Sicherheitsstufe anpassen



Outlook Express/Outlook: In die Zone EINGESCHRÄNKTE SITES platzieren

Hijacker

Prävention ist das effektivste Mittel gegen Hijacker. Vorbeugen beginnt mit der Browser-Konfiguration und hört bei den Windows-Updates auf. Befolgen Sie unsere sieben Vorschläge, ersparen Sie sich viel Ungemach.

1. Internet Explorer abdichten

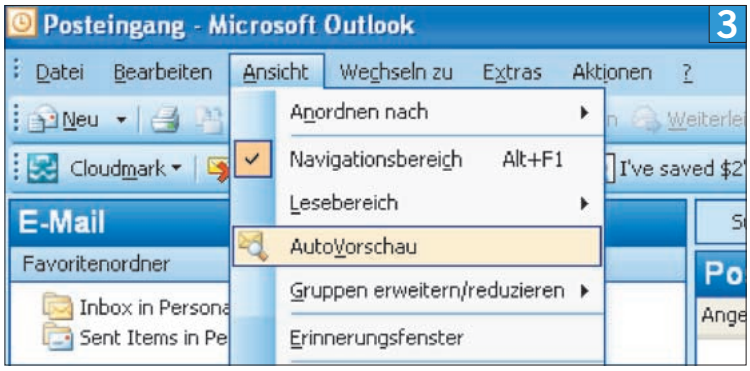
Im Internet Explorer stellen Sie unter EXTRAS/INTERNETOPTIONEN/SICHERHEIT/STUFE ANPASSEN die Sicherheitsstufe für die Zone «Internet» ein. Setzen Sie die benutzerdefinierten Einstellungen auf HOCH. Die Optionen in «Einstellungen» sollten Sie folgendermassen einstellen, Screen 1:

- «ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind»: Deaktivieren
- «ActiveX-Steuerelemente und Plugins ausführen»: Eingabeaufforderung
- «Download von unsignierten ActiveX-Steuerelementen»: Deaktivieren
- «Java-Einstellungen»: Hohe Sicherheit (falls vorhanden)

Übernehmen Sie die Änderungen mit einem Klick auf OK.

Binden Sie das → Script **IE-Spyads** in den Browser ein. Sie finden es unter www.pctipp.ch mit WEBCODE **27634**. Dieses Script legt zahlreiche unseriöse Webseiten direkt in die Zone für EINGESCHRÄNKTE SITES des Internet Explorers. Für Webseiten, die in dieser Zone liegen, gelten automatisch die Sicherheitsbestimmungen «Hoch».

Und so gehts: Downloaden Sie die Datei «ie-spyad.exe» und starten Sie sie mit einem Doppelklick. Nun entpacken Sie die Datei in einen Ordner Ihrer Wahl. In diesem Ordner befindet sich jetzt unter anderem die Datei «install.bat». Starten Sie diese per Doppelklick. Im DOS-Fenster wählen Sie die Option 2 «Install the New IE-Spyad List» mit der Taste *2*. Danach bestätigen Sie nochmals mit der Taste *1* «Yes – install IE-Spyad». Das Script schreibt nun hunderte von bekannten, unseriösen Webseiten in die «Zone für Eingeschränkte Sites» der Internetoptionen. Damit können diese Seiten mit Ihrem System keinen Unfug mehr treiben. Haben Sie in Windows mehrere Benutzer angelegt, muss das Script für jedes Benutzerkonto ausgeführt werden.



Outlook Express/Outlook: AutoVorschau ausschalten

2. Verhalten in E-Mail-Programmen

Neben dem Internetbrowser müssen Sie auch Ihr E-Mail-Programm auf Sicherheit trimmen. In Outlook 2003 stellen Sie über EXTRAS/OPTIONEN/SICHERHEIT die «Sicherheitszone» auf EINGESCHRÄNKTE SITES ein. In Outlook Express 6 finden Sie diese Einstellung in denselben Registern, Screen 2. Auch hier wählen Sie als «Zone» EINGESCHRÄNKTE SITES.

FACHCHINESISCH

Java

Programmiersprache der Firma Sun Microsystems. Java-Programme werden in einen rechnerunabhängigen Code übersetzt (kompiliert), der auf beinahe jedem System ausgeführt werden kann.

Patch

Wörtlich übersetzt: ausbessern oder flicken. Ein Patch repariert Fehler in der Software.

Öffnen Sie grundsätzlich keine Internetlinks in Ihrem E-Mail-Programm. Lassen Sie sich alle ankommenden E-Mails nur im Text-Format anzeigen und nicht im → HTML-Format. Dies stellen Sie in Outlook Express 6 unter OPTIONEN/LESEN mit der Konfiguration «Alle Nachrichten als Nur-Text lesen» ein. Für Outlook und Outlook Express 5.x gibts diesbezüglich keine Einstellung.

Deaktivieren Sie die automatische E-Mail-Vorschau. In Outlook Express 6 geht das folgendermassen: Klicken Sie auf den Posteingang. Wählen Sie ANSICHT/LAYOUT. In der Option «Vorschaufenster» deaktivieren Sie VORSCHAUFENSTER ANZEIGEN. In Outlook 2003 gehen Sie sicher, dass es unter ANSICHT bei «AutoVorschau» kein Häkchen hat, Screen 3.

3. Microsoft Java rausschmeissen

Da Microsoft → Java nicht mehr unterstützt, wird die alte MS-Java-Version auch nicht mehr mit → Patches gegen Sicherheitslücken versorgt. Höchste Zeit zum Umsteigen auf die Original-Java-Version von Sun Microsystems. Sie finden die aktuelle Java-Version auf der PCtipp-Homepage mit WEBCODE **17345**. Java bindet sich automatisch in die Systemsteuerung ein.

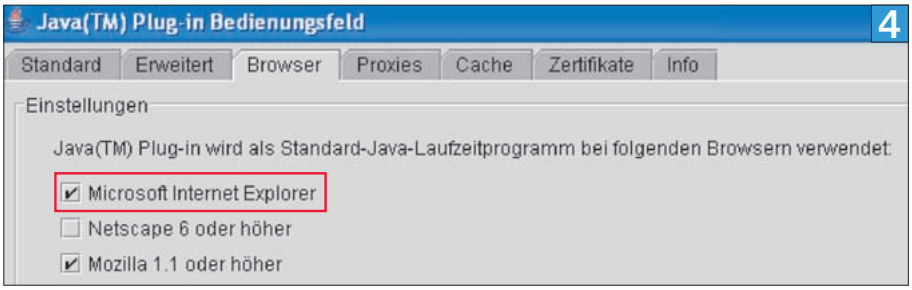
So stellen Sie sicher, dass Suns Java für Ihren Browser Standard ist: Doppelklicken Sie in der ▶

Systemsteuerung (START/SYSTEMSTEUERUNG) aufs Java-Icon – das sieht aus wie eine Kaffeetasse –, lässt sich Suns Java im Register BROWSER für Ihren Browser als Standard definieren, Screen 4. Falls Sie also den Internet Explorer verwenden, müssten Sie dort ein Häkchen machen.

4. Überwachungsprogramm installieren

Gegen ungebetene Gäste helfen Programme, die alle Aktivitäten im Hintergrund von Windows überwachen. Versucht sich eine Software zu installieren, werden Sie vom Überwachungsprogramm gefragt, ob Sie der jeweiligen Installation zustimmen wollen. Die Shareware **Geek Superhero**, WEBCODE 27629, sowie die Freeware **SpywareGuard**, WEBCODE 27630, erledigen diese Arbeit. Geek Superhero kann im Vergleich zu SpywareGuard einiges mehr – z. B. Pop-ups und WebBugs abklemmen –, dafür kostet das Programm 25 Dollar.

So funktioniert SpywareGuard: Laden Sie sich das Programm von der PCtipp-Homepage herunter. Installieren Sie es mit einem Doppelklick auf die Datei «spywareguardsetupmin.exe». SpywareGuard sorgt mit den Voreinstellungen, Screen 5, nun für Sicherheit. Er meldet sich, wenn irgendein Programm im Hintergrund versucht, ein neues Browser Helper Object (BHO) zu installieren oder die Standardseite, die Suchseite oder die Start-Homepage zu ändern. Sie haben so volle Kontrolle über Ihren Browser.



Definieren Sie Sun Java für Ihren Browser – hier der Internet Explorer und Mozilla – als Standard

SpywareGuard: Wehrt Spione ab

5. Rechte einschränken

Arbeiten Sie in Windows NT/2000/XP nie mit Administratorrechten, sondern verwenden Sie ein Benutzerkonto, das nur eingeschränkte Rechte besitzt. In der Praxis ist dies ganz einfach zu realisieren: Für Programminstallationen, Backups und System-Updates verwenden Sie das Administratorprofil, für die tägliche Arbeit das eingeschränkte Benutzerprofil. Gerade bei Surftouren ist dies von Vorteil: Hijacker haben im limitierten Benutzerprofil viel weniger Möglichkeiten, Windows Schaden zuzufügen. Wie Sie die verschiedenen Profiltypen einrichten, steht im Artikel «Chefsache», PCtipp 12/2003, S. 36, oder online unter WEBCODE **pdf031236**.

6. Radikalkur: Browser- und E-Mail-Wechsel

Internet Explorer und Outlook Express sind die meistverbreiteten Internetprogramme. Sie werden von Crackern am häufigsten auf Sicherheitslücken abgeklopft und sind leider nicht sonderlich auf Sicherheit getrimmt. Wer sicherer browsen will, steigt auf andere Software um. Als Browser empfehlen sich:

- **Opera** WEBCODE **16391**
- **Mozilla** WEBCODE **20935**
- **Firefox** WEBCODE **25897**

Als E-Mail-Alternativen bieten sich ebenfalls Opera oder Mozilla an, des Weiteren:

- **PMMail** WEBCODE **20201**
- **Thunderbird** WEBCODE **27440**
- **AK-Mail** WEBCODE **16390**
- **GeMail** WEBCODE **26287**
- **Pegasus Mail** WEBCODE **15647**

7. Wöchentliche Windows-Updates

Tragen Sie Sorge zu Ihrem System. Kontrollieren Sie unter Windows XP wöchentlich über START/ALLE PROGRAMME/WINDOWS UPDATE oder im Internet Explorer unter EXTRAS/WINDOWS UPDATE bei Microsoft, welche neuen Patches bereitstehen. So werden die bekannten Sicherheitslöcher in Windows gestopft. Eine weiterführende Anleitung für Windows-Updates finden Sie im Artikel «Sicher mit Microsoft», PCtipp 4/2004, S. 23, oder mit WEBCODE **pdf040423**.

Hijacker entfernen

Sie haben alle Anti-Hijacker-Tipps gelesen und werden sie in Zukunft auch befolgen? Prima! Doch was ist, wenn Ihr System bereits von Hijackern befallen ist? Der Kampf gegen ein verseuchtes System ist nicht aussichtslos. Es gibt brauchbare Programme, die Ihnen die Kontrolle über Windows zurückgeben. Wie bei Virenscannern gilt auch hier: Nicht jedes Programm findet garantiert jeden Hijacker. Wir empfehlen, die Programme **Ad-aware**, WEBCODE **17579**, **Spybot Search & Destroy**, WEBCODE **25550**, und **CWShredder** (siehe nächster Absatz) einzusetzen. Da Ad-aware und Spybot auch gleich Spyware abwürgen, lesen Sie die Anleitungen zu diesen Tools im Abschnitt «System offline überprüfen», S. 27.

So funktioniert **CWShredder**, WEBCODE **27631**: Laden Sie das Programm von der PCtipp-Webseite herunter. Ein Doppelklick auf die Datei CWShredder.exe startet den Schredder. Ein simpler Klick auf FIX schneidet die dem Schredder bekannten Pestbeulen aus Windows heraus.

Spyware

Wie der Name nahe legt, schnüffelt Spyware in Ihrem Konsum- und Surfverhalten herum. Spyware versteckt sich immer in Software, die vermeintlich gratis ist. Spyware ist nicht nur aus Sicht des Datenschutzes fragwürdig, vielfach schadet sie sogar Windows erheblich. Spyware ist mühsam zu deinstallieren und schiesst unter Umständen sogar reguläre Programme ab.

Für Spyware sind – im Gegensatz zu den Hijackern – keine Sicherheitslücken in Windows verantwortlich. An Spyware ist letztlich das Konsumverhalten der Mehrheit der Anwender schuld. Da der durchschnittliche Computer-User immer alles gratis will, gingen diverse Shareware-Programmierer vom kostenpflichtigen Shareware- zum vermeintlich kostenlosen Spyware-Modell über: Sie bieten ihre Software gratis an, bekommen aber von dubiosen Werbe-Füchsen Geld für Informationen über die Software-Nutzer. Seit Windows 2000 übt sich auch Microsoft im ungefragten Datensammeln: Der Media Player lässt z. B. eine eindeutige Identifizierung des Surfenden zu, oder bei Systemabstürzen möchte Microsoft das Speicherabbild erhalten.

Wie können Sie sich gegen Spyware schützen? Wie wissen Sie, ob in Ihrem System bereits fleissig Daten gesammelt werden? Die Internetgemeinschaft hatte über zwei Jahre Zeit, Abwehrmassnahmen gegen Spyware zu entwickeln. Entsprechend vielfältig sind die zur Verfügung stehenden Programme und Massnahmen.

1. Windows 2000/XP abdichten

Für Windows 2000 und XP brauchts grundsätzlich einen Kammerjägereinsatz, da diese Windows-Versionen einfach zu mitteilungsfreudig sind. Laden Sie sich das Tool **XP-AntiSpy**, WEBCODE **19905**, herunter. Entpacken Sie die Datei XP-AntiSpy_de.zip in einen Ordner Ihrer Wahl. Danach starten Sie XP-AntiSpy per Doppelklick. Deaktivieren Sie (grünes Häkchen) sämtliche Sammeleigenschaften des Windows Media Players, der Fehlerberichterstattung und des Internet Explorers. Die Optionen KEINE ÜBERPRÜFUNG AUF UPDATES und KEINE GEPLANTEN UPDATES sollten Sie aktiviert (rotes Ausrufezeichen) lassen. Bei angewählter Funktion erklärt das Programm im unteren Teil des Fensters, was die Aktivierung bedeutet. XP-AntiSpy muss in einem Profil mit Administratorrechten ausgeführt werden.

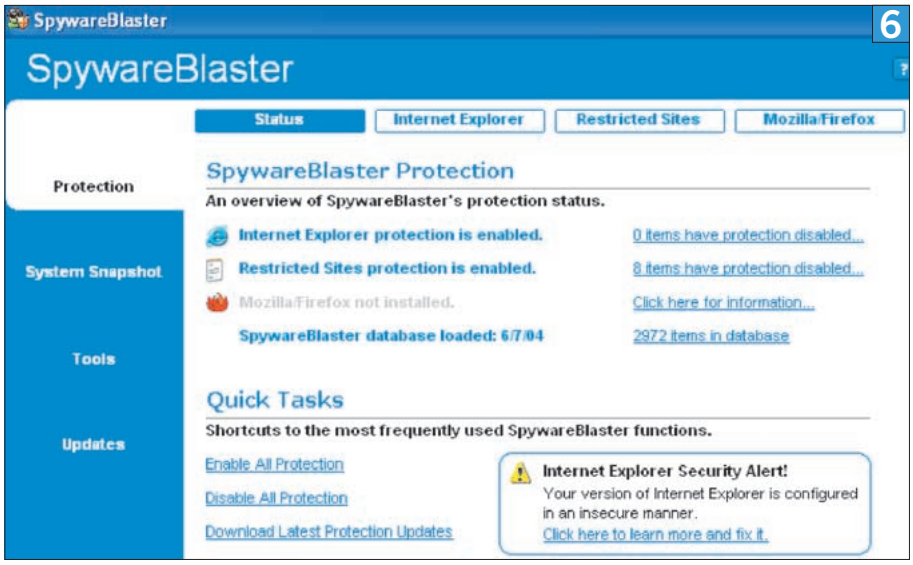
2. Spyware-Programme erkennen

Werden Sie schon zu Beginn einer Programminstallation nach demografischen Daten gefragt, besteht höchste Alarmstufe. Kein normaler Shareware-Autor interessiert sich für Ihr Alter, Ihre Einkaufsgewohnheiten oder sonstige Marketingdaten. Besonders bekannte Spyware-Beispiele sind die Download-Manager Download Accelerator Plus (DAP) und Go!Zilla. Auch die Tauschbörsenprogramme Kazaa und BearShare setzen in der Gratisversion auf Spyware. Überlegen Sie sich in einem solchen Fall sehr genau, ob Sie nicht besser auf die fragliche Software verzichten bzw. die kostenpflichtige Version anschaffen wollen.

3. Befall verhindern

Der **SpywareBlaster**, WEBCODE **27637**, schützt Ihr System vor Schnüffelbefall. Laden Sie sich das Programm von der PCtipp-Homepage herunter. Mit einem Doppelklick auf die Datei «spywareblastersetup.exe» installieren Sie den Wegpuster. Starten Sie SpywareBlaster. Vielleicht stellt das Programm gleich nach dem ersten Start fest, dass Ihre Internet-Explorer-Einstellungen unsicher sind. In diesem Fall erscheint der «Internet Explorer Security Alert!», **Screen 6**. Befolgen Sie die Vorschläge von SpywareBlaster. Wählen Sie CLICK HERE TO LEARN MORE AND FIX IT. Danach klicken Sie SET RECOMMENDED VALUES. Nun aktivieren Sie im Hauptmenü unter «Protection» den Schutz für die eingesetzten Browser mit CLICK HERE TO ENABLE PROTECTION.

RESTRICTED SITES PROTECTION schliesst Schmuddelwebseiten aus. Auch diese Option sollten Sie aktivieren. Zu guter Letzt holen Sie sich im Reiter UPDATES mit einem Klick auf CHECK FOR UPDATES die neusten Spyware-Erkennungsmuster aus dem Internet. SpywareBlaster muss für jedes Benutzerprofil einzeln angewendet werden. ▶



SpywareBlaster: Bemerkt unsichere Internet-Explorer-Einstellungen

4. Genügsamkeit ist eine Zier

Spyware vermeiden Sie am wirkungsvollsten, wenn Sie wirklich nur jene Programme aus dem Internet herunterladen und installieren, die Sie wirklich brauchen. Für jede Art von Anwendung findet sich garantiert ein Programm, das frei von Spyware ist. Vielleicht bekommen Sie es aber nicht zum Nulltarif.

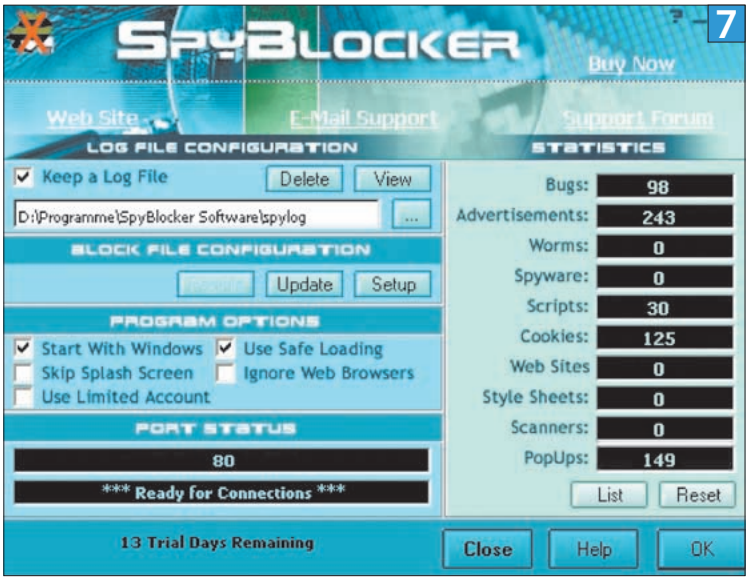
5. Eine Frage des Vertrauens

Laden Sie nur bei jenen Webseiten Software herunter, denen Sie vertrauen. Eine seriöse Homepage verweist im Beschreibungstext auf allenfalls verwendete Spyware.

Übrigens: Sollte ein Programm auf der PCtipp-Download-Seite Spyware verwenden, wird ausdrücklich darauf hingewiesen.

6. Spyware-Blocker

Sie wollen partout nicht auf Spyware-Programme verzichten, weil sie nichts kosten? Auch das ist möglich, ohne ausspioniert zu werden. Allerdings ist die Lösung nicht gratis. Damit Sie nicht Hauptdarsteller eines miesen Big-Brother-Films werden, hindert das Programm **SpyBlocker**, WEBCODE **18691**, zwar die Spyware nicht daran, sich zu installieren, macht sie jedoch für die Hersteller gänzlich unbrauchbar, **Screen 7**. SpyBlocker ändert keine Dateien der Spyware-Software, es blockt Spyware-Server, indem es ihnen einen eigenen Server vorsetzt. Somit behalten alle diese Programme die volle Funktionsfähigkeit, Sie brechen keinerlei Lizenzvereinbarungen, aber die Spyware verfehlt völlig ihr Ziel. Wenn Sie eine Firewall wie z. B. ZoneAlarm nutzen, müssen Sie SpyBlocker in der Firewall-Software den Zugang zu einigen → **Ports** (z. B. Port 80) gewähren.



SpyBlocker: Trickst Spyware aus

Spyware loswerden

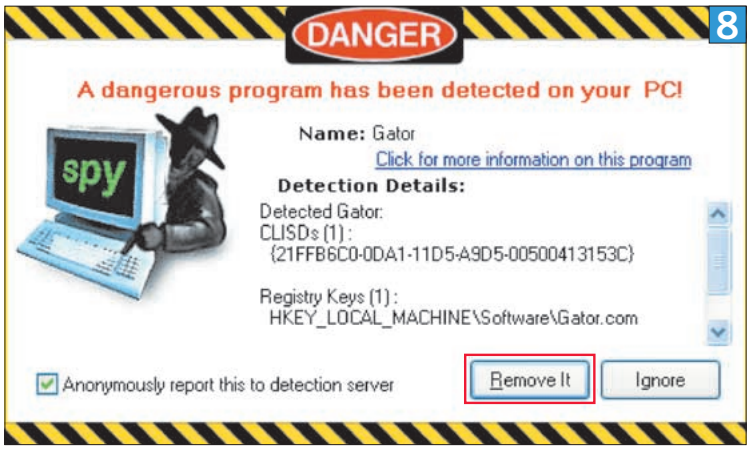
Sie sind der Meinung, alles erdenklich Mögliche gegen Spyware und Hijacker unternommen zu haben? Machen Sie den Test. Wetten, der eine oder andere Spion labt sich seit Monaten an Ihren Dateien? Die Testprogramme sind aber zum Glück fähig, entdeckte Spyware sofort zu eliminieren.

1. System online überprüfen

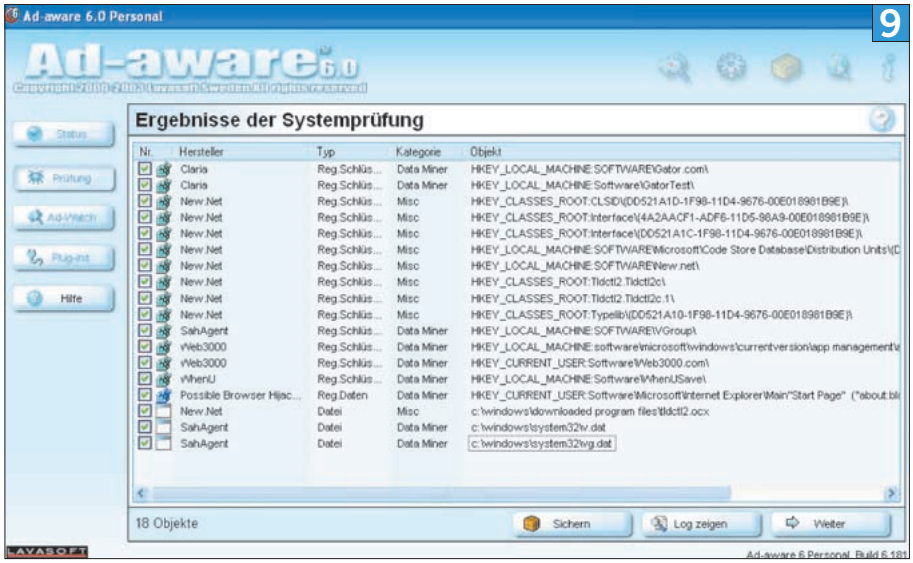
Die Internetseite Spyware-Guide.com stellt gratis einen Online-Spyware-Scanner zur Verfügung. Geben Sie die URL www.spywareguide.com/txt_onlinescan.html ein. Gegebenenfalls müssen Sie Ihren Download-Manager wie z. B. GetRight temporär deaktivieren, damit der Scan automatisch startet. Der Online-Scanner ist ein ActiveX-Objekt. Der Internet Explorer lädt die ActiveX-Control-Datei herunter. Sobald dies geschieht, erscheint ein Warndialogfeld: Der Online-Scanner bittet um Erlaubnis, starten zu können. Erlauben Sie es ihm mit YES. Sobald der Scanner Spyware, Trojaner, Keylogger, Adware oder sonstige Malware entdeckt, fragt er nach, ob Sie den Schädling ausradieren wollen. Klicken Sie auf REMOVE IT, **Screen 8**.

Findet der Online-Scanner nichts, schliesst er sich nach der Überprüfung automatisch.

Benutzen Sie einen anderen Browser als den Internet Explorer, geben Sie die URL www.xblock.com/download/xclean_micro.exe ein. Nun möchte der Browser die Datei lokal auf der Festplatte speichern. Tun Sie dies und starten Sie dann die genannte Datei mit einem Doppelklick.



8 **Der Online-Scanner von Spyware-Guide.com findet und entfernt Spyware**



9 **Ad-aware: Gefundene Spyware geben Sie manuell zum Löschen frei**

2. System offline überprüfen

Nach dem Online-Scanner-Test starten Sie den PC neu. Jetzt kommen die auf S. 25 bereits erwähnten Ad-aware und Spybot zum Einsatz. Denn was für Virenscanner gilt, ist auch hier der Fall: Nicht jedes Anti-Spyware-Tool erkennt alle Übeltäter. Dreifach genäht hält besser. Starten Sie in freier Reihenfolge die beiden Anti-Malware-Tools. Nach jedem Einsatz fahren Sie den Rechner runter und wieder hoch. So gehts:

■ **Ad-aware**, WEBCODE 17579, ist der Klassiker der Hijacker-, Spyware- und Adware-Bekämpfer. Adaware Personal ist gratis und macht dem lästigen Treiben diverser Malware ein Ende. Installieren Sie das Programm mit einem Doppelklick auf «aaw6181.exe» in einen Ordner Ihrer Wahl. Starten Sie Ad-aware und wählen Sie unter OPTIONS die Sprache Deutsch. Danach schliessen Sie Adaware, damit beim erneuten Start die Benutzeroberfläche in Deutsch erscheint.

Nun wählen Sie im Hauptfenster REFUPDATE ÖFFNEN. Laden Sie sich die neuste Referenz-Datei herunter. Ist dies erledigt, klicken Sie auf PRÜFUNG. Als Scanmodus nehmen Sie LAUFWERK\VERZEICHNISSE WÄHLEN und selektionieren jene Laufwerke, die Windows (Laufwerk C:) enthalten, sowie die verwendeten Programme (z. B. Laufwerk D:). Ein Klick auf WEITER startet die Spyware-Hatz. Hat Ad-aware alle angegebenen Laufwerke gescannt, müssen Sie manuell jene Dateien angeben, die gelöscht werden sollen, **Screen 9**.

Ad-aware findet bestimmt viele so genannte Tracking-→ **Cookies**, die Sie löschen können. Entfernen Sie alle von Ad-aware als Spyware entlarvten EXE-Dateien. Ein schneller Systemcheck über PRÜFUNG/SCHNELLER SYSTEMCHECK kontrolliert unter anderem in der Registry.

■ **Spybot Search & Destroy**, WEBCODE 25550: Beim ersten Start schlägt das Programm eine Sicherung der Windows-Registry vor. Tun Sie das. Danach laden Sie sich mit einem Klick auf ALLE UPDATES HERUNTERLADEN die neusten Updates für Spybot herunter. Dann gehts WEITER. Klicken Sie auf IMMUNISIEREN (IMMUNIZE THIS SYSTEM), worauf bedrohliche Produkte blockiert werden. Nach WEITER wählen Sie PROGRAMM BENUTZEN. Schliessen Sie Spybot Search & Destroy nochmals, um es umgehend wieder zu starten. Klicken Sie im Hauptfenster auf ÜBERPRÜFEN. Nach dem Scan sehen Sie die Ergebnisse. Ein Klick auf MARKIERTE PROBLEME BEHEBEN vertreibt die Übeltäter aus dem System.

Damit dieses Prozedere garantiert nicht in die Hose geht, legt Spybot vor dem Entfernen der Schädlinge einen Restore-Point in Windows an. Kann Spybot einige Dateien nicht sofort löschen, muss er dies beim nächsten Windows-Start durchführen. Erlauben Sie Spybot daher, sich beim nächsten Computer-Start automatisch mitzuladen.

→ FACHCHINESISCH

Port

Jeder Netzwerkdienst verfügt über einen eindeutig zugewiesenen Port (Verbindung), so auch das World Wide Web (Port 80).

Cookie

Englisch für «Keks»: Kleine Datei mit Textinformationen, die vom Webserver auf dem Benutzer-PC abgelegt und bei jedem Besuch abgerufen werden. Cookies enthalten Informationen, die beim nächsten Besuch das Wiedererkennen des Surfers ermöglichen.

System sichern

Windows ist jetzt von sämtlichen Malware-Rückständen befreit. Zeit also für eine Sicherung der Systeminnereien. Mit **SpywareBlaster** (siehe «3. Befall verhindern», S. 25) geht das am schnellsten. Nach dem Start des Programms wählen Sie im Hauptfenster die Option SYSTEM SNAPSHOT.

Wählen Sie «Create New System Snapshot» und klicken auf GO. Nun benennen Sie das Projekt und klicken auf CREATE SNAPSHOT! Voilà! Nach einigen Sekunden ist der Snapshot gemacht. Das Backup muss unter Windows NT/2000/XP für jeden Benutzer einzeln vorgenommen werden.

Sollte in Zukunft wieder mal eine Malware durch das nun aufgezogene engmaschige Anti-Malware-Netz schlüpfen, starten Sie einfach SpywareBlaster. Unter SYSTEM SNAPSHOT wählen Sie dann RESTORE SYSTEM TO SAVED SNAPSHOT POINT und klicken auf GO. Im nächsten Fenster wählen Sie die Sicherung Ihrer Wahl aus und starten die Wiederherstellung mit NEXT. ■