ILLUSTRATION GREG CLARKE

Gib Schnüfflern KEINE CHANCE

Beim Surfen, beim Mailen, im Betriebssystem und beim Provider – überall hinterlassen Sie ungewollt Spuren. So wehren Sie sich.

von Bruno Habegger

Kaum blinkt das Modemlämpchen, sind Sie nicht nur drin, sondern auch dran: Sie werden von Spammern belästigt, von Hackern belauscht und vom Staat registriert. Mit jedem Klick verraten Surferinnen und Surfer – ob sie es wollen oder nicht – im besten Fall etwas über ihre Lebensgewohnheiten und im schlimmsten Fall Geheimnisse, die ins finanzielle Desaster führen können.

Ein fremder Handy-Anschluss lässt sich bei einigen Telefonfirmen leicht sperren, sofern man das Geburtsdatum des Opfers kennt. Dessen Adresse beliefern Versandfirmen auf gut Glück mit Waren. Und fischt ein Hacker Ihre Kreditkartennummer vom Server, kann er mit Ihrem guten Namen einkaufen.

Harmlosere Formen des Datenklaus sind gang und gäbe: So grasen etwa Harvesting-Programme («Ernte-Programme») Webseiten und Newsgroups nach E-Mail-Adressen ab und füttern fremde Mailboxen mit Spam. Ihr Internetbrowser verrät Marketingfirmen mit Hilfe von Cookies, kleinen Textdateien, die vom Besuch einer Website herrühren, viel über Ihre Konsum- und

Sehgewohnheiten. (Mehr zu Cookies, siehe Abschnitt «Browser», rechts unten auf dieser Seite.) Oder Firmen führen Bonitäts-Datenbanken, die falsche Daten enthalten können – vielleicht weil jemand mal Produkte unter einem fremden Namen bestellt und nicht bezahlt hat. Die Folge kann eine Weigerung sein, den angeblich nicht kreditwürdigen Kunden mit Waren zu beliefern.

Sich anonym im Netz bewegen zu können, mag sich da manch einer angesichts solcher Gefahren wünschen. Doch das ist umstritten. Polizei, Justiz und die Industrie – allen voran die Musikfirmen – würden gern jeden Surfer mit einem Namensschild versehen. Ihre Bemühungen sind bereits weit vorangeschritten. So wird etwa seit kurzem verstärkt gegen Nutzer von Tauschbörsen vorgegangen und Provider werden gezwungen, die Identität ihrer Kunden offen zu legen.

Doch eine Aufhebung der Anonymität kollidiert nach Ansicht von Datenschutzexperten mit den demokratischen Grundrechten jedes Menschen auf die Kontrolle über seine eigene Privatsphäre. Jeder kauft anonym am Kiosk Zigaretten und Heftli, ohne sich vorher mit Namen und Adresse bei der Kioskfrau registrieren zu müssen.

Werden Daten laufend gesammelt, können diese zwar zur Verbrechensbekämpfung eingesetzt werden; andererseits steigt die Gefahr des Missbrauchs. Online-Karten und -Datenbanken verraten zum Beispiel, wo Surfer wohnen; Suchmaschinen, etwa der Newsgroup-Sucher von Google, etwas über die Lebensgewohnheiten von Diskussionsteilnehmern.

So wehren Sie sich

Aus all diesen Gründen sollten Sie sich die Kontrolle über Ihre Daten zurückholen. An diesen Stellen setzen Sie den Hebel an:

Ansprechpartner: Bevor Sie Ihren Namen, Ihre Adresse, Telefonnummer und andere Daten via Internet übermitteln, sollten Sie den Empfänger unter die Lupe nehmen. Wie vertrauenswürdig ist er? Sind Kontaktangaben und die allgemeinen Geschäftsbedingungen vorhanden, verständlich und klar? Legt er offen, wie er mit den gesammelten Daten umgeht?

Massnahmen:

- Wenn eine Website die Registrierung verlangt, ist es oft möglich, fiktive Daten einzugeben – der Dienst ist trotzdem nutzbar. Sie benötigen lediglich eine gültige E-Mail-Adresse. Eröffnen Sie für solche Zwecke bei einem anonymen Anbieter wie Hotmail oder GMX eine Adresse als «Spam-Fänger».
- Suchen Sie auf der Site nach einer Kontakttelefonnummer und rufen Sie an, um sicher zu gehen, dass die Firma auch tatsächlich existiert.
- Checken Sie unter **http://www.zefix.admin.ch/**, ob die hinter der Website stehende Firma im Handelsregister eingetragen ist. Das funktioniert natürlich nur bei Schweizer Firmen.

Deutliche Worte: Wer bei www.mywinsite.com an einem Wettbewerb teilnimmt, erlaubt, dass seine Daten für Werbung genutzt werden.

- Lesen Sie die Datenschutzregelung des Anbieters. Ist keine vorhanden oder nimmt er sich das Recht heraus, die Daten zu verkaufen, **Screen 1**, sollten Sie sich eine Nutzung des Angebotes zweimal überlegen.

Betriebssystem: Windows XP ist nicht gerade eine Quelle der Diskretion. Im Betriebssystem stecken einige Funktionen, die eigenmächtig Microsoft kontaktieren. So etwa gleich nach dem Windows-Start: Die Produkteaktivierung verletzt zwar nach dem derzeitigen Wissensstand und einem ausführlichen Microsoft-Paper die Privatsphäre nicht – trotzdem haben viele Anwender ein ungutes Gefühl.

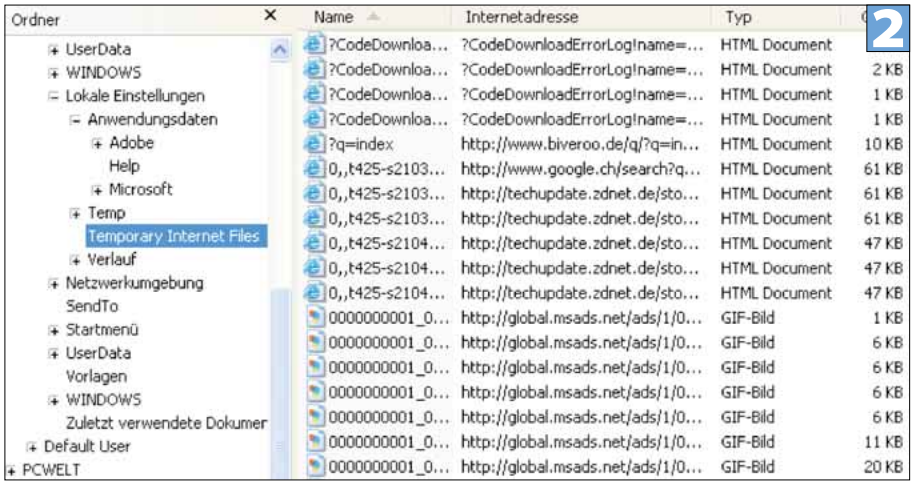
Die Musik- und Videoabspiel-Software Windows Media Player registriert, welche CDs und DVDs abgespielt werden, und meldet dies einem Microsoft-Server. Zwar liegt mit der neusten Version 9 die Kontrolle über dieses Verhalten wieder in der Hand der Anwender, doch bleiben viele misstrauisch.

Windows ist zudem ein Nährboden für Viren und Würmer aller Art. Durch diese Schwachstellen können Hacker das System infiltrieren.

Massnahmen:

- Halten Sie Ihr System mit der Windows-Update-Funktion (START-Menü oder mit dem Browser unter **http://www.windowsupdate.com/**) immer auf dem neusten Stand. Viele Sicherheitslöcher werden mit diesen Updates kurz nach ihrer Entdeckung gestopft.
- Ebenso ist der Einsatz einer Antiviren-Software Pflicht (siehe dazu auch «Doppelt schützt besser», S. 66). Auch diese müssen Sie regelmässig (mindestens einmal wöchentlich, besser täglich) updaten und so mit den neusten Virensignaturen bekannt machen.
- Windows XP können Sie von Hand zu mehr Diskretion verpflichten. Das ist aber aufwändig und heikel: Sie müssen an verschiedenen Stellen in das System und in die Windows-Registry, der zentralen Einstellungsdatenbank, eingreifen. Viel schneller und sicherer erledigt dies die Gratis-Software XP AntiSpy (WEBCODE 19905).
- Durchforsten Sie Ihren PC nach Spyware. Das erledigt die Freeware Ad-aware (WEBCODE 17579).
- Die Installation einer Desktop-Firewall wie ZoneAlarm (WEBCODE 16670) bietet zwar keine absolute Sicherheit, aber immerhin die Kontrolle darüber, welche Software vom PC aus Kontakt ins Internet aufnimmt und wer von aussen auf Ihren PC zugreifen will. Mehr über Firewalls lesen Sie ebenfalls ab Seite 66.
- Prüfen Sie die Qualität Ihrer Passwörter. Sie sollten mindestens acht beliebige Zeichen enthalten, Gross- und Kleinschreibung gemischt sowie mit Zahlen oder Sonderzeichen versetzt sein. Tipps für sichere Passwörter finden Sie im Artikel «Geheime Schlüssel», PCtip 3/2003, S. 42 (**http://www.pctip.ch/library/pdf/2003/03/0342Pass.pdf**).

Browser: Die Programme, die Internetseiten darstellen, sind die grössten Verräter. Der Internet Explorer hinterlässt seine Spuren an vielen Stellen des Systems. Die bekanntesten Surfspuren sind die temporären Dateien im Ordner «Temporary Internet Files», **Screen 2**, und die Cookies. Das sind kleine Textdateien, die einem von den angesurften Webservern angedreht werden, um gewisse Dienste beanspruchen zu können. So ▶



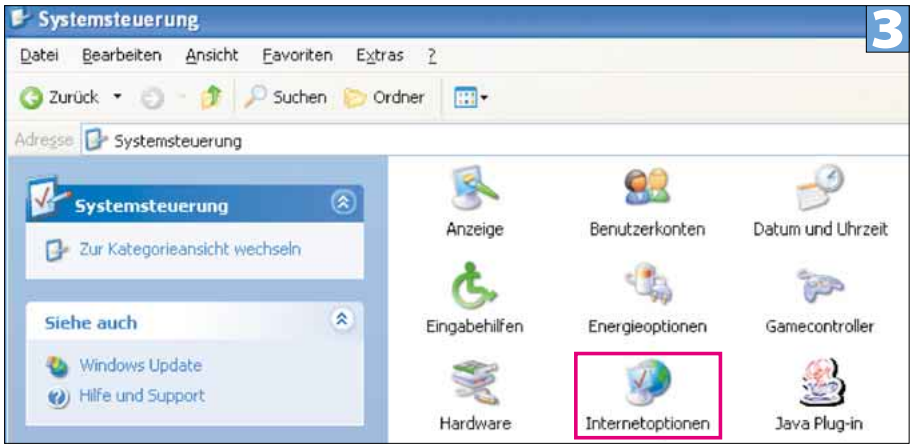
Verräterisches Archiv: In den «Temporary Internet Files» ist alles über Ihre Surftour gespeichert.

▶ erinnert sich der Server an einen früheren Besuch und bietet auf den Benutzer zugeschnittene Navigationsmöglichkeiten und Informationen. Dank Cookies diskutieren Forumsteilnehmer nicht anonym und finden Firmen heraus, welche Produkte Sie konsumieren oder welche Inhalte Ihnen am besten entsprechen.

Eine besonders raffinierte Methode, Benutzerprofile zu erstellen, sind WebBugs. Diese 1x1 Pixel kleinen GIF-Dateien rufen via Internet ein Programm ab, das aktuelle Benutzerdaten sammelt. WebBugs werden meist verwendet, um Zugriffe auf Internetwerbung zu protokollieren.

Andere Stellen sind nicht so bekannt. Etwa die Datei «index.dat». In dieser und in anderen DAT-Dateien speichert der Browser unter anderem Kennwörter, Webadressen und Formulardaten. Diese Dateien lassen sich nicht so einfach löschen, da Windows sie schützt.

Und weil im Internet Explorer auch andere Programme laufen – etwa der Media Player –, sammeln sich über diese weitere Protokolle an. Noch mehr Spuren erzeugen Sie, wenn Sie Dateien herunterladen und danach öffnen. Dann finden sich etwa Einträge im Dokumentenmenü und temporäre Dateien. Die Software, mit der Sie eine Datei betrachtet haben, führt häufig ebenfalls Protokoll.



Hinter dem Icon INTERNETOPTIONEN finden Sie diverse Sicherheitseinstellungen.

Massnahmen:

■ Löschen Sie nach jeder Sitzung den Inhalt des Ordners «Temporary Internet Files» (den so genannten Internetcache). Dort sind die Elemente aller besuchten Websites zwischengespeichert. Sie finden diesen Ordner im Verzeichnis C:\Windows oder unter Windows 2000 bzw. XP Pro in C:\Dokumente und Einstellungen\Ihr Name\Lokale Einstellungen.

An derselben Stelle leeren Sie den «Verlauf»-Ordner, der die Links zu Seiten enthält, die Sie besucht haben. Hier sind auch die Cookies dran. Die kleinen Textdateien sind zwar an sich harmlos, doch sie dienen Internetwerbefirmen zum Erstellen von Nutzerprofilen.

Starten Sie Ihre Säuberungsaktion in der SYSTEMSTEUERUNG. Klicken Sie auf INTERNETOPTIONEN, **Screen 3**.

Privatsphäre

Die entscheidenden Funktionen «Temporäre Internetdateien» und «Verlauf» sehen Sie nun vor sich, **Screen 4**.

Ein Klick auf DATEIEN LÖSCHEN..., **A**, leert den Ordner «Temporary Internet Files» und beseitigt einen Teil der Surfspuren. Anschliessend klicken Sie auf COOKIES LÖSCHEN..., **B** – und schon sind die Krümelmonster weg. Ein abschliessender Klick auf «VERLAUF» LEEREN, **C**, befreit Sie auch von gespeicherten Internetadressen. Sie können daneben auch die Anzahl Tage einstellen, nach denen der Verlaufsordner geleert werden soll.

Wechseln Sie zum Register ERWEITERT, haben Sie unter dem Punkt «Sicherheit» die Möglichkeit, die temporären Internetdateien nach dem Schliessen des Browsers automatisch zu löschen, **Screen 5**.

Damit ist es aber leider noch nicht getan, denn gemeinerweise liegen in den «Temporary Internet Files» auch viele versteckte Ordner, beispielsweise «Content.IE5». Darin finden Sie wie bereits angesprochen die Datei «index.dat», **Screen 6**. Sie ist nicht löschbar, weil sie bei jedem Start des PCs neu angelegt und sofort gesperrt wird.

Spezielle Internet-Spurenvernichter (s. Box «Wichtige Links», S. 31) kümmern sich um diese Datei. Von Hand wirds kompliziert. Sie müssen den ganzen Ordner von der DOS-Ebene aus löschen. Der Befehl lautet «deltree tempor~1», gefolgt von einem Druck auf die *Enter*-Taste.

Für Windows XP können Sie den Löschbefehl automatisieren, indem Sie ein Skript anlegen. So gehts: Erstellen Sie mit Notepad eine leere Datei und schreiben Sie genau folgende vier Zeilen hinein:

REM Loeschen der Temporaeren Internet Files inkl. index.dat

RD /s /q "c:\dokumente und einstellungen\username\Lokale Einstellungen\Temporary Internet Files"

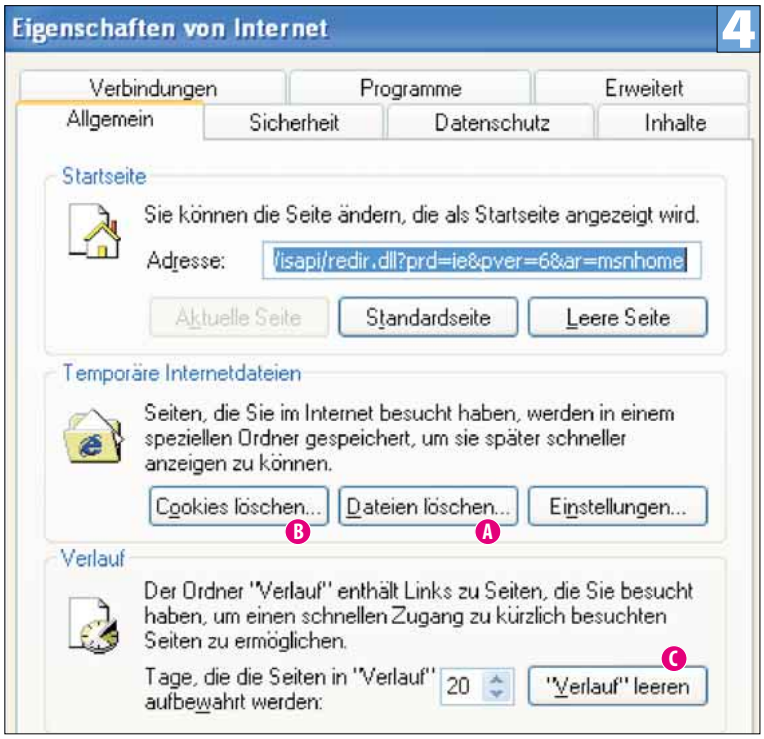
RD /s /q "c:\dokumente und einstellungen\username\Cookies"

RD /s /q "c:\dokumente und einstellungen\username\Lokale Einstellungen\Verlauf"

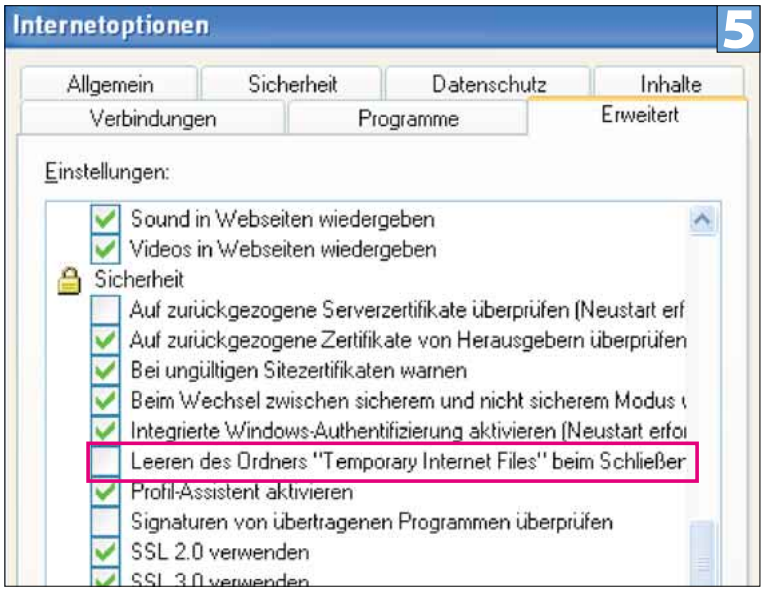
Liegt Ihre Windows-Installation auf einer anderen Festplatte mit einem anderen Laufwerksbuchstaben als auf C:, müssen Sie die Zeilen entsprechend anpassen. Ebenfalls müssen Sie statt username jenen Namen einsetzen, den Sie bei Ihrer Windows-Anmeldung verwenden.

Speichern Sie anschliessend das Skript unter einem beliebigen Namen mit der Endung .cmd oder .bat ab. Dann erstellen Sie unter «C:\Dokumente und Einstellungen\username\Startmenü\Programme\Autostart» eine Verknüpfung mit der Datei, so dass diese jeweils beim Systemstart automatisch ausgeführt wird. Der Befehl RD löscht das ganze Verzeichnis und somit auch die Datei index.dat. Windows erstellt dann eine neue, leere index.dat.

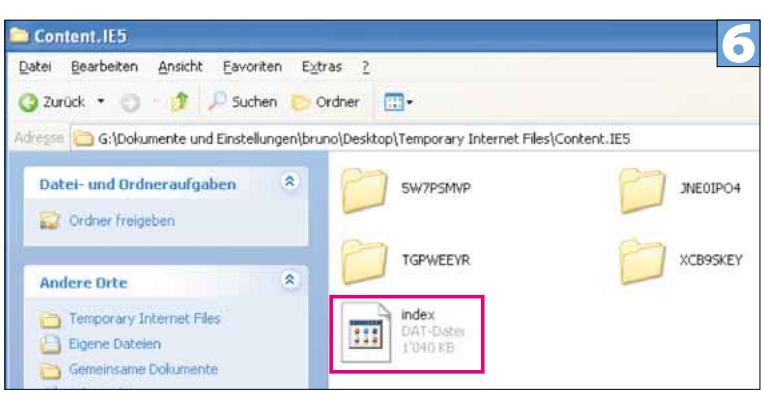
Das Skript wurde getestet, trotzdem erfolgt eine Verwendung auf eigene Gefahr.



Hier beseitigen Sie Surfspuren von Ihrem PC.



Mit der Aktivierung dieses Befehls leert sich der Verlaufsordner nach jedem Schliessen des Browsers automatisch.



Die Datei index.dat können Sie nicht einfach so löschen, denn sie ist geschützt.

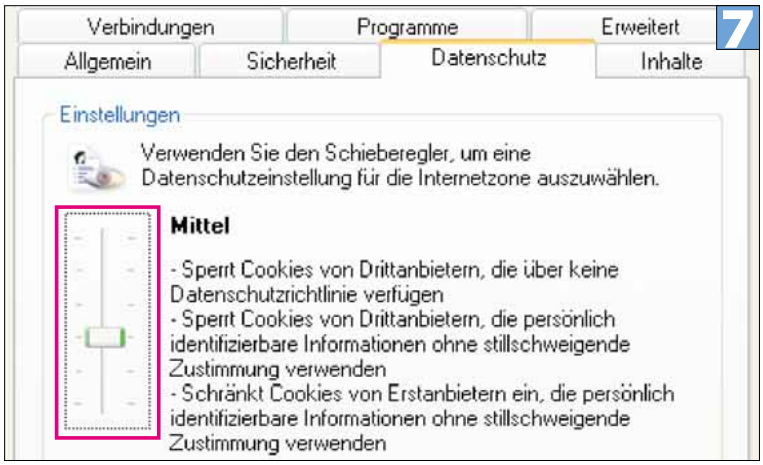
▶ ■ Weitere Anpassungen an den Voreinstellungen des Internet Explorers 6.0 nehmen Sie im Reiter DATENSCHUTZ vor. Hier stellen Sie ein, wie der Internet Explorer mit Cookies umgeht, **Screen 7**.

Die Einstellung «Mittel» hat sich für ein relativ sicheres, aber noch ungehindertes Surfen bewährt. Testen Sie die verschiedenen Einstellungen ruhig mal aus.

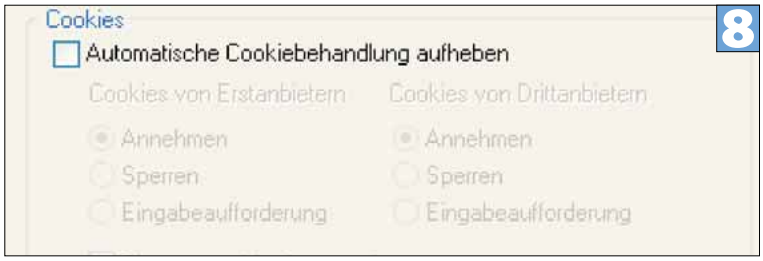
Der Button ERWEITERT bringt Sie zu einem Fenster, in dem Sie die automatische Cookiebehandlung abschalten können. Sie haben die Wahl, die Annahme von Cookies generell zu sperren oder bei jedem einzeln zu entscheiden, ob Sie es akzeptieren wollen, **Screen 8**.

Diese Abfrage verfeinern Sie im Reiter DATENSCHUTZ unter dem Punkt «Websites». Hier klicken Sie auf BEARBEITEN und legen anschliessend für jede einzelne Website fest, ob sie Cookies bei Ihnen ablegen darf.

■ Wechseln Sie abschliessend noch zum Register INHALTE. Wichtig ist hier der Button AUTOVERVOLLSTÄNDIGEN. Wenn Sie nicht wollen, dass bekannte Internetadressen beim Eintippen oben in der Adressleiste des Browsers automatisch nach wenigen Buchstaben ergänzt werden, entfernen Sie alle Häkchen in diesem Fenster und löschen alle Formulare und Kennwörter, **Screen 9**.



7 **Mit dem Schieberegler stellen Sie den Sicherheitsgrad ein.**



8 **Heben Sie die automatische Cookiebehandlung auf.**

Privatsphäre

■ Der Internet Explorer kennt verschiedene Sicherheitszonen. Jede kann mit eigenen Sicherheitseinstellungen betrieben werden. Mit einem Schieberegler stellen Sie unter EXTRAS/INTERNETOPTIONEN in der Registerkarte SICHERHEIT den gewünschten Grad der Sicherheit ein. Mit einem Klick auf ANGEPASST und EINSTELLUNGEN verfeinern Sie die vordefinierten Sicherheitsstufen. Hier sollten Sie mindestens Active-X abschalten.

E-Mail: Telefonieren ist diskreter als das Versenden einer E-Mail. Im Prinzip ist jeder einigermassen versierte Netzwerk- und Internetkenner in der Lage, den E-Mail-Verkehr im Klartext mitzuschneiden und sogar Passwörter für Mailboxen auszuspionieren. Mailprogramme wie Outlook (Express) sind zudem häufig Einfallstore für Trojaner und Viren, die Passwörter und andere vertrauliche Daten stehlen. Jüngstes Beispiel ist der Wurm Bugbear (mehr dazu: **WEBCODE 22174**).

Massnahmen:

■ Vertrauliches sollten Sie nie per E-Mail kommunizieren. Oder wenn, dann nur per verschlüsselter Kommunikation mit Pretty Good Privacy (**http://www.pgp.com/**) oder GnuPG (**http://www.gnupg.org/**). Wie Sie diese Software einsetzen, steht im Artikel «Sicher ist sicher», PCtip 2/2003, ab Seite 40 (**http://www.pctip.ch/library/pdf/2003/02/0240_PGP.pdf**).

Die Häkchen bei «AutoVervollständigen verwenden für» entfernen Sie am besten gleich alle.

■ Schützen Sie nicht nur den Inhalt, sondern auch die E-Mail-Adresse selbst: Wenn Sie sie auf Ihrer Homepage publizieren wollen, dann nur als Grafik, nicht als Text. So verunmöglichen Sie Suchrobotern von Spammern das Erfassen Ihrer Mailadresse. So gehts: Fügen Sie in einer beliebigen Bildbearbeitungs-Software – z. B. Windows Paint aus dem Zubehör-Ordner – Ihre Adresse als Text ein und speichern Sie das Ganze als Grafik.

Tauschbörsen: KaZaA, eDonkey und andere Programme zum direkten Austausch von Musik und Videos unter den Nutzern der Software enthalten oft zweifelhafte Software, die Anwender ausspionieren und ihre Gewohnheiten erfassen. Ausserdem ist in einem solchen «Netz im Netz» niemand anonym unterwegs. Die Polizei ist in Zusammenarbeit mit Providern in der Lage herauszufinden, wer Tauschnetze nutzt. So erhielten im vergangenen Jahr viele Kunden der Deutschen Telekom unmissverständliche Warnun- ▶

Privatsphäre

gen. Auch in der Schweiz leben Tauschbörsennutzer gefährlich: Bereits wurde der Betreiber eines Tauschservers, der randvoll mit illegal heruntergeladenen MP3-Dateien gefüllt war, verhaftet.

Massnahmen:

■ Am besten verzichten Sie auf den Einsatz einer Tauschbörsen-Software. Nicht nur, weil die Gefahr gross ist, sich Viren oder Spyware einzufangen, sondern auch, weil der Dateitausch rechtlich umstritten ist. Meist werden Raubkopien von Musik, Filmen oder Software gehandelt, was illegal ist.

Provider: Sie können sich noch so unauffällig verhalten, Sie sind trotzdem nicht anonym unterwegs. Ihr PC erhält nämlich vom Provider eine so genannte IP-Nummer. Sie identifiziert Ihren PC eindeutig, ist also gewissermassen seine «Telefonnummer». Modem-Surfer erhalten bei jedem Zugang eine neue Nummer aus dem IP-Nummernvorrat ihres Providers nach dem Muster 131.107.137.47. Breitband-Anwender sind über lange Zeit mit ein und derselben IP-Adresse im Netz unterwegs.

Wenn Sie im Browser eine Webseite betrachten, die von einem Webserver geliefert wird, fliessen im Hintergrund Daten zwischen Ihrem PC und dem Webserver hin und her. Alle diese Datenpakete sind mit der IP-Adresse von Absender und Empfänger versehen, damit sie auch wirklich ihr Ziel erreichen. Ohne IP-Adresse kein Internet. Der Provider führt in einem «Logfile» Buch darüber, wer zu welcher Zeit mit welcher IP-Nummer unterwegs war – Anonymität im Internet ist deshalb nur ein frommer Wunsch.

Dieses Logfile ist für den Betreiber einer Website ein wichtiges Hilfsmittel, um Anwenderprofile zu erstellen. Darin werden automatisch Besucherdaten eingetragen. Die Protokolldatei enthält zu jeder Anfrage die IP-Nummer des zugreifenden Rechners, Datum und Uhrzeit des Zugriffs, die angeforderten Dateien und das Ergebnis der Anfrage. Auch die zuvor besuchte Adresse sowie Betriebssystem und Browser des Benutzers werden erfasst.

Massnahmen:

■ Das Problem lässt sich mit Hilfe von anonymen Proxy-Servern umgehen. Dabei handelt es sich um zwischengeschaltete Webserver, welche die Anfragen Ihres Browsers entgegennehmen und an den eigentlich gewünschten Webserver weiterreichen. Dieser sieht natürlich nur noch die IP-Adresse des Proxy-Servers und nicht mehr die Ihnen zugeteilte.

Die Tarnkappen-Server sind aber nicht ständig im Netz präsent oder gehen öfter mal unter der Last der Anfragen in die Knie. Listen öffentlich zugänglicher Server finden Sie z. B. unter **http://atomintersoft.com/products/alive-proxy/proxy-list/**, unter **http://www.samair.ru/proxy/** oder unter **http://www.antiproxy.com/proxysearch.php**. Die dort aufgelisteten IP-Adressen und Port-Nummern tragen Sie in die Proxy-Einstellungen Ihres Webbrowsers (Internet Explorer: Extras/Internet-Optionen/Einstellungen/Proxy-Server) oder einer anderen Internetsoftware ein, die Proxy-Server unterstützt.

Die Sache hat einen Haken: Natürlich verfügt mindestens der Betreiber des Proxy-Servers immer noch über Ihre Daten. Er kann genau wie der Provider verpflichtet werden, diese preiszugeben. Oder er sammelt im schlimmsten Fall Ihre Daten ganz gezielt, z. B. für Werbung oder andere Zwecke. Gerüchten zufolge soll es Proxy-Server geben, die vom US-Geheimdienst CIA betrieben werden.

■ Lokal installierte Software ist um einiges sicherer und bequemer als der ständige Neueintrag der aktuellsten Proxy-Server im Browser. Ausserdem verschlüsselt sie auch die Verbindung zwischen PC und Proxy-Server und wechselt die Proxys automatisch in rascher Folge, um die Spuren weiter zu verwischen. Rewebber (**http://www.rewebber.de/**) ist ein kostenpflichtiger Online-Dienst, der automatisch alle persönlichen Daten entfernt und sogar eingegebene Internetadressen (URL) verschlüsselt.

Als besonders sicher gilt JAP, ein Projekt der Uni Dresden (**http://anon.inf.tu-dresden.de/**). Die Java-Software verschlüsselt die Daten mehrfach und verwendet mehrere Zwischenstationen. Die Folge: Internetverbindungen jedes einzelnen Anwenders werden unter denen der anderen, gleichzeitig surfenden Anwendern versteckt. Aussenstehende können nicht mehr ausmachen, wer auf welchen Seiten unterwegs ist.

Ein Albtraum für Justiz und Polizei, mehr Freiheit für die Surfer. Die können so im Internet einen Koffer einkaufen, ohne gleich Gefahr zu laufen, als potenzieller Bombenleger verdächtigt zu werden.

Tipp

Die goldenen Surfregeln

Wenn ich meine IP-Adresse verheimlichen möchte,	**dann** muss ich einen anonymen Proxy oder einen Dienst wie JAP verwenden, siehe «Massnahmen» unten auf dieser Seite.
Wenn niemand meine E-Mails mitlesen darf,	**dann** muss ich eine Verschlüsselungs-Software wie PGP oder GnuPG verwenden.
Wenn niemand sich an meinen Daten auf meinem PC vergreifen darf,	**dann** muss ich Firewall-Software einsetzen und diese korrekt konfigurieren, also die Bedienungsanleitung der Software genau befolgen.
Wenn ich mich vor Bespitzelung der Marketingfirmen schützen will,	**dann** verwende ich eine Software, die Werbebanner und Web-Bugs filtert, z. B. Webwasher (http://www.webwasher.de/).
Wenn ich nicht will, dass Informationen über mich auf Webseiten auftauchen,	**dann** muss ich zurückhaltend sein im Umgang mit Gästebüchern, Diskussionsforen oder im Usenet und nur ein Minimum über meine Person veröffentlichen. Als E-Mail-Adresse gebe ich nie meine private Adresse an, sondern eine, die ich bei einem Gratisanbieter extra für solche Zwecke eingerichtet habe.

Tipp

Wichtige Links

Privatsphäre und Datenschutz

- Eidg. Datenschutzbeauftragter: http://www.edsb.ch/
- Anonym surfen: http://www.anonymsurfen.com/
- Was Ihr Browser verrät: http://privacy.net/
- Funktioniert der anonyme Proxy-Server? http://www.leader.ru/secure/who.html
- Anonym surfen – Webdienst http://www.anonymizer.com/
- Englische und deutsche Anleitungen http://www.astalavista.com/privacy/
- Allgemeiner Datenschutz http://www.allgemeiner-datenschutz.de/

Anonyme Surf-Software

- Multi Proxy: http://www.multiproxy.org/
- Anonymizer: http://www.anonymizer.com/
- Internet Anonym 5: http://www.steganos.de/
- PTS Super Stealther 3.0: http://www.bhv.net/
- Anonymizer II http://scifi.pages.at/bdsx/prg_anonymizer.htm

Spurenverwischer

- TraXEx: http://www.almisoft.de/
- WinSweep: http://www.winsweep.de/
- WindowWasher: http://www.webroot.com/
- Internet-Spurenvernichter 6.0 http://www.steganos.de/
- Paranoia 2002: http://winutil.de/
- CookieCooker: http://cookie.inf.tu-dresden.de/
- SaferSurf (Online-Dienst) http://www.safersurf.com/
- Historykill http://www.swanksoft.com/historykill/