ILLUSTRATION RICHARD TUSCHMAN

Sicher surfen

Das Internet ist ein Tummelfeld für Viren, Datensammler, Betrüger und Abzocker. Wer um die Bedrohungen weiss, kann sich schützen.

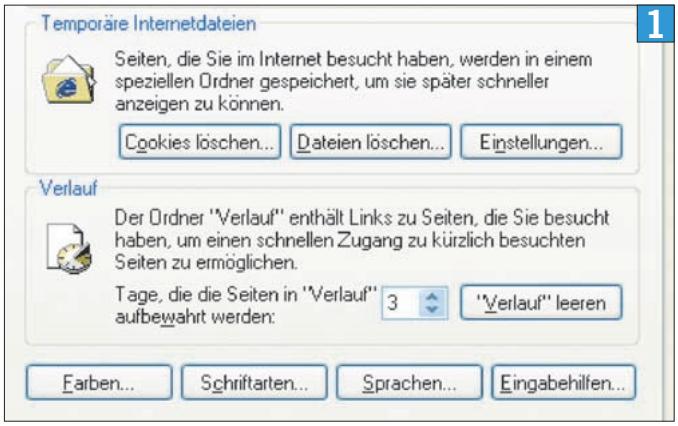
von Sascha Zäch

Heutzutage vergeht einem schnell einmal die Lust am Internet. Hinter jedem Bit scheinen Gefahren zu lauern. Die Medien sind voll mit Berichten über Computerviren, Hackerangriffe und Massenmails. Regelmässig wird vor Spyware, Dialern, Cookies und WebBugs gewarnt. Nicht zu vergessen: Der besonders fiese Blaster-Wurm, der sich im Sommer 2003 auf unzähligen Rechnern breit machte. Die meisten Opfer waren ratlos, hatten sie doch weder einen unbekannten Mailanhang geöffnet, noch wissentlich eine Datei auf den Rechner kopiert. Schon der Aufbau einer Internetverbindung reichte für diese Infektion. Wie soll der Anwender sich da noch schützen? Das Modem in der Mottenkiste verstauen und wieder in der internetlosen Informatiksteinzeit leben?

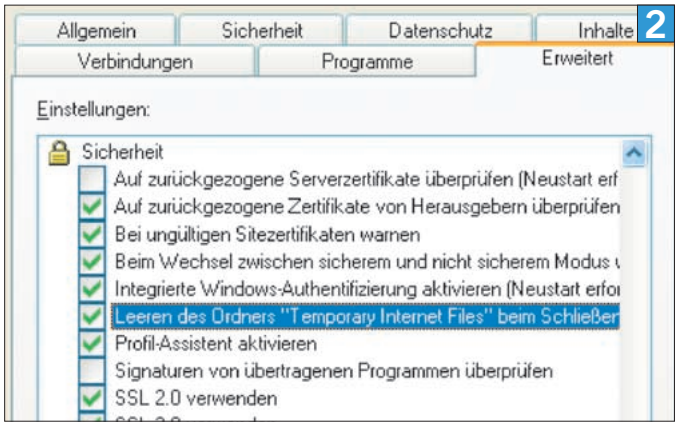
Nun, so weit müssen Sie glücklicherweise nicht gehen. Die erwähnten Gefahren sind zwar real, aber doch nicht unvermeidbar. Eine grosse Hilfe ist es bereits, wenn Sie wissen, wo sich die Bedrohungen verbergen und wie sie auf Ihren Rechner gelangen können. Frei nach der fernöstlichen Weisheit: «Nur wer den Feind kennt, kann ihn auch besiegen.» Der folgende Artikel klärt auf, mit welchen Gefahren Sie im Internet und speziell beim Surfen und Mailen rechnen müssen. Lösungsvorschläge helfen Ihnen, sich effizient zu schützen. Die Bezugsquellen aller empfohlenen Programme finden Sie in der Box «Empfohlene Schutz-Programme», S. 29.

Grundschutz

Der anfangs erwähnte Blaster-Wurm demonstrierte es letzten Sommer wieder einmal deutlich: Schädliche Software kann sich nicht nur per



Der Puffer gibt Auskunft über Ihre Surfgewohnheiten. Löschen Sie deshalb regelmässig seinen Inhalt



Wahren Sie Ihre Privatsphäre, indem Sie den Ordner «Temporary Internet Files» nach jeder Internetsitzung automatisch leeren

E-Mail oder über Websites verbreiten. Beliebte Schlupflöcher sind auch Sicherheitslücken im Betriebssystem und offene Ports. Neben einer Antiviren-Software zählen deshalb regelmässige Windows-Updates und eine Firewall zu den probatesten Mitteln, um ein System sicherzuhalten. Näheres zu diesen drei wichtigen Schutzwällen finden Sie im Artikel «Schon Windows schützt», Seite 58. Dort wird Ihnen auch genau erklärt, wie Sie die in Windows XP integrierte Firewall einschalten und konfigurieren.

Als Alternative zur Microsoft-Firewall empfiehlt sich der Einsatz einer Desktop-Firewall. Diese ist bequemer und einfacher zu handhaben als ihr Windows-XP-Pendant – und muss nicht einmal etwas kosten. ZoneAlarm bekommen Sie z. B. gratis im DOWNLOAD-Bereich der PCtipp-Website unter www.pctipp.ch. Einen noch besseren Schutz bieten Hardware-Firewalls, die zwischen Rechner und Internetzugang geschaltet werden. Mit ihnen lassen sich mehrere PCs gleichzeitig abschirmen. Zudem arbeiten sie unabhängig vom Betriebssystem und warten mit nützlichen Zusatzfunktionen auf. Leider sind Hardware-Firewalls sehr teuer und komplizierter zu bedienen als die Software-Varianten.

Hinweis: Vermehrt finden sich auch ADSL-Modems mit Firewall-Funktionen auf dem Markt. Achten Sie darauf, wenn Sie sich für einen ADSL-Zugang entscheiden.

Sicher surfen

Die scheinbare Anonymität im World Wide Web bringt leider viele Anwender dazu, sich beim Surfen allzu sorglos zu verhalten. Eine jüngere Studie des deutschen Bundesamtes für Sicherheit (BSI) zeigte, dass gerade Jugendliche schlecht über Gefahrenquellen im Internet informiert sind oder diese nicht genügend ernst nehmen (siehe News Seite 17). Mit einem unbedachten Klick kann schnell eine teure Einwahl-Software auf der Festplatte landen. Zahlreiche Webseiten verwenden Cookies und WebBugs (mehr dazu S. 30), die das Verhalten der Benutzer dokumentieren. Wer mit seiner E-Mail-Adresse zu lasch umgeht, hat in Windeseile ein lebenslanges «Abo» für Brust- und Penisvergrösserungswerbung am Hals. Mit ein paar wenigen Massnahmen lassen sich all diese Bedrohungen fast vollständig abwehren.

Verlauf und Puffer: Die meisten Browser speichern besuchte Webseiten in einem speziellen Ordner ab. Dadurch werden sie bei einem erneuten Besuch schneller geladen. Diese Pufferfunktion hat aber einen gravierenden Nachteil: Es lässt sich relativ einfach in Erfahrung bringen, welche Webseiten Sie sich angesehen haben. Dazu muss nur der entsprechende Ordner geöffnet werden. Im Internet Explorer nennt sich der verräterische Ordner «Temporäre Internetdateien». Sie können mit der Option EXTRAS/INTERNETOPTIONEN/ALLGEMEIN/EINSTELLUNGEN/DATEIEN ANZEIGEN auf seinen Inhalt zugreifen. Schützen Sie Ihre Privatsphäre, indem Sie nach dem Surfen unter EXTRAS/INTERNETOPTIONEN/ALLGEMEIN/DATEIEN LÖSCHEN den Inhalt von «Temporäre Internetdateien» ins Nirvana befördern, Screen 1.

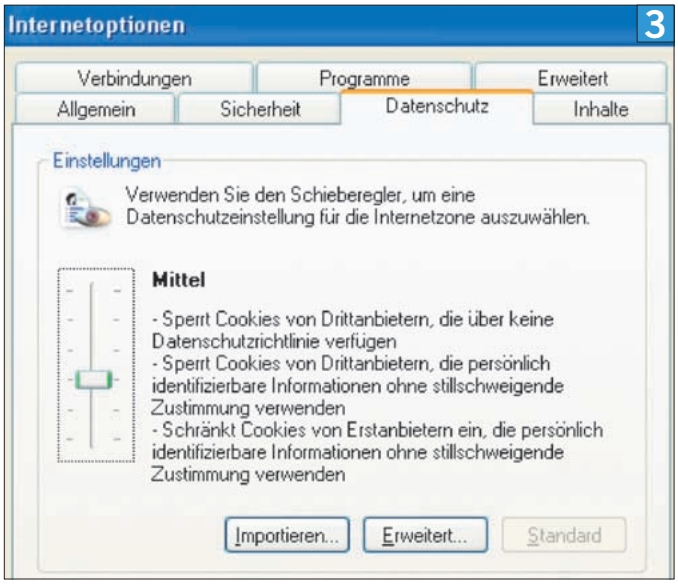
Im gleichen Fenster sollten Sie ausserdem den VERLAUF LEEREN. Der Verlauf speichert Internetadressen, die Sie während der Sitzung besucht haben. Einen Teil der Arbeit können Sie übrigens automatisch vom Browser erledigen lassen. Kreuzen Sie dazu das Feld «Leeren des Ordners "Temporary Internet Files" beim Schliessen des Browsers» im Register EXTRAS/INTERNETOPTIONEN/ERWEITERT an, Screen 2. ▶

SOFTWARE

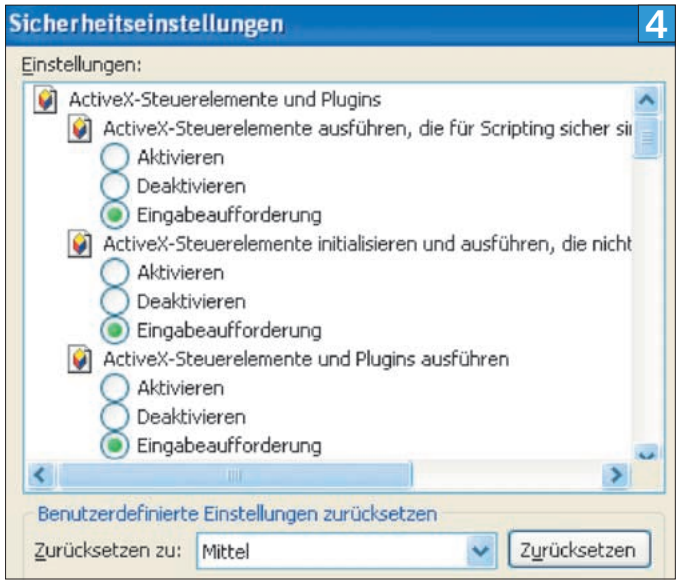
Empfohlene Schutz-Programme

Ad-aware	JAP	WebWasher
Dieses Tool durchkämmt Ihr System nach Spyware und tilgt die Spione von der Festplatte. Doch einige Freeware-Tools funktionieren nach dem Entfernen von verräterischen Komponenten nicht mehr richtig. Dafür bietet Ad-aware eine Backup-Funktion.	JAP schützt Ihre Privatsphäre beim Surfen. Das Tool versteckt die Internetverbindung eines Anwenders unter denen der anderen. Dadurch lässt sich eine Verbindung nicht mehr einem bestimmten Benutzer zuordnen.	WebWasher schützt Ihren Rechner vor Cookies und WebBugs. Zudem können mit dem Programm lästige Pop-up-Werbungen, Werbebanner und animierte Bilder blockiert werden. Dadurch erhöht sich die Surfgeschwindigkeit.
Freeware für Windows WEBCODE 17579	**Freeware für Windows, Mac OS und Linux** http://anon.inf.tu-dresden.de	**Freeware für Windows, Mac OS und Linux** WEBCODE 15804

YAW	PGP	ZoneAlarm
Geben Sie Dialern keine Chance. YAW (Yet Another Warner) verhindert unerwünschte Überraschungen bei der nächsten Telefonrechnung. Die Software überwacht das System nicht nur auf Dialer-Aktivitäten, sondern hilft auch bei der Suche und beim Entfernen bereits vorhandener Missetäter.	PGP (Pretty Good Privacy) ist die wohl bekannteste Software zum Verschlüsseln von E-Mails und Dateien. Bei der kostenlosen Version müssen einige Einschränkungen hingenommen werden. So lassen sich Attachments nicht automatisch verschlüsseln. Auch die Plug-In-Funktion für Outlook und Outlook Express fehlt.	Neben einem Virenscanner gehört auch eine Firewall-Software auf den PC. Eine verbreitete Desktop-Firewall ist ZoneAlarm. Mit ihr schützen Sie den PC vor unerwünschten Zugriffen aus dem Internet. Neben dem kostenpflichtigen ZoneAlarm Pro gibt es eine Gratisversion mit kleinerem Funktionsumfang.
Freeware für Windows WEBCODE 20556	**Freeware für Windows, Download unter** www.pgp.com/products/de/freeware.html	**Freeware für Windows** WEBCODE 16670



Im Internet Explorer können Sie genau festlegen, welche Cookies Sie akzeptieren wollen und welche nicht



Schützen Sie sich vor schädlichen Programmen aus dem Web, indem Sie dem Internet Explorer die Ausführung von ActiveX-Elementen verbieten

Cookies: Leider sind virtuelle Cookies (zu Deutsch «Kekse») überhaupt nicht so schmackhaft wie ihre realen Pendants. Die digitalen Kekse finden sich auf zahlreichen Webseiten. Es handelt sich um kleine Textdateien, die Informationen über Besuche auf einer bestimmten Homepage enthalten. Auch eingetippte Informationen können in Cookies hinterlegt werden. Surfen Sie erneut auf die Website, ruft diese die Infos wieder ab. Dadurch ist es möglich, dass Sie auf Seiten wie www.amazon.de sofort als Benutzer XYZ erkannt werden. Cookies sind geeignete Hilfsmittel, um ausführliche Benutzerprofile zu erstellen, und werden deshalb gerne für Werbezwecke verwendet.

Möchten Sie die Datenspione nicht auf Ihrer Festplatte haben, können Sie ihnen im Internet Explorer unter EXTRAS/INTERNETOPTIONEN/ALLGEMEIN/COOKIES LÖSCHEN den Garaus machen, Screen 1, Seite 29.

Im Register DATENSCHUTZ bestimmen Sie, wie der Browser mit Cookies umgehen soll, Screen 3. Allzu strenge Einstellungen sind nicht empfehlenswert, da viele Websites anschliessend nicht mehr richtig funktionieren. Verwenden Sie lieber zusätzlich eine Software wie WebWasher. Das Programm besitzt einen effizienten und gut konfigurierbaren Cookie-Filter.

WebBugs: WebBugs sind winzige, transparente Bilddateien in der Grösse eines Pixels. Damit sind sie für die Surfer nicht sichtbar. Wird ein WebBug beim Besuch einer Homepage aufgerufen, sendet er Informationen wie → IP-Adresse, Browser-Typ, Adresse der Homepage und Aufrufzeit an den Webserver. Dadurch lassen sich statistische Informationen über Besucher sammeln. Dies ist eigentlich nicht weiter tragisch. Auch die PCtipp-Homepage verwendet WebBugs, um die Zahl der Seitenbesuche zu erfassen, eine wichtige Grösse für Werbekunden.

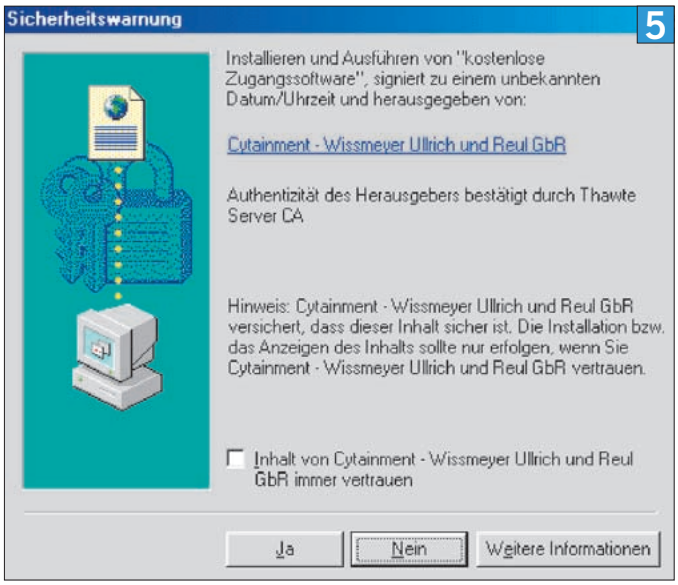
Gefährlich wird es, wenn WebBugs zusammen mit Cookies eingesetzt werden. Letztere sind in der Lage, persönliche Angaben zu speichern. WebBugs können diese Infos zusammen mit den anderen Daten an den Webseitenbetreiber senden. So ist es möglich, noch genauere Benutzerprofile zu erstellen. Die grösste Gefahr von WebBugs wehren Sie ab, indem Sie Cookies löschen oder filtern. Falls Sie die «Kekse» lieber ganz blockieren möchten, setzen Sie am besten WebWasher ein. Das Programm kann neben Cookies auch WebBugs filtern.

ActiveX: Mit Hilfe von ActiveX lassen sich Webseiten um Anwendungen und Multimediaeffekte erweitern. Ein bekanntes Beispiel ist die Windows-Update-Site. Sie weiss dank ActiveX, welche Patches auf einem bestimmten System installiert werden müssen. Unterstützt wird die Technologie hauptsächlich vom Internet Explorer, da sie von Microsoft stammt. Leider hat sie einen grossen Nachteil: Ruft der Internet Explorer auf einer Website ein ActiveX-Programm auf, wird dieses auf den Rechner geladen und dort ausgeführt. Dabei erhält es die gleichen Rechte wie der Benutzer, kann also gegebenenfalls auf wichtige Systemfunktionen und -ressourcen zugreifen.

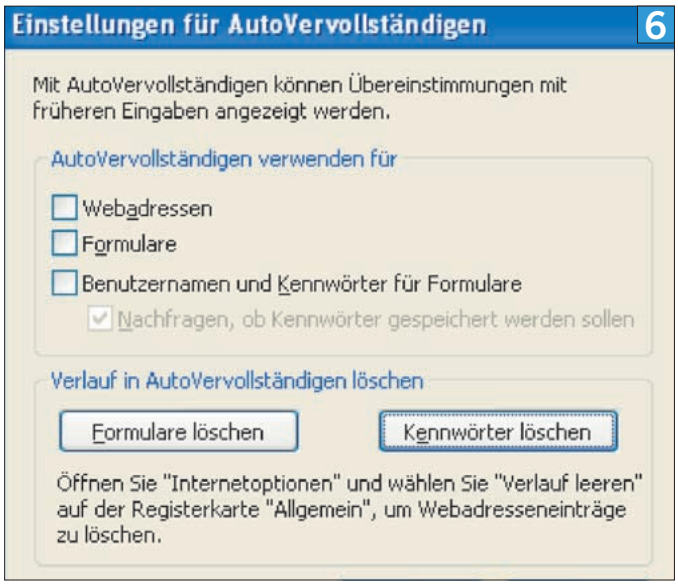
Dies ist ein immenses Sicherheitsrisiko. Schädliche Software kann so unbemerkt auf den Computer geschmuggelt und dort installiert werden. Ein typisches Beispiel sind etwa Dialer, die sich sehr gerne auf diese Weise in ein System einschleichen (siehe nächster Abschnitt). Wenn Sie den Internet Explorer verwenden, sollten Sie aus Sicherheitsgründen sowohl «Active Scripting» als auch die Ausführung und den Download von «ActiveX-Steuerelementen» einschränken, Screen 4. Eine genaue Anleitung dazu finden Sie im Artikel «Sicher und voll funktionsfähig» auf Seite 71.

Dialer: Diese kleinen Programme fanden sich früher hauptsächlich auf Erotik- und Hackerseiten. Vermehrt verbergen sie sich aber auch auf (scheinbar) seriösen Websites. Meist tarnen sie sich als Zugangs-Software, Screen 5. Diese muss angeblich zuerst heruntergeladen werden, bevor Sie einen bestimmten Dienst nutzen können. Ganz freche Exemplare installieren sich mit ActiveX gleich selbst und ohne zu fragen auf dem PC.

Einmal auf der Festplatte, können sie einen teuer zu stehen kommen. Wird ein Dialer aktiviert, wählt er sich auf eine Mehrwertdienstnummer ein (0900, 0901 oder 0906). Je nach Höhe der Nummerngebühren häuft sich schon nach einigen Minuten ein hübsches Sümmchen an. Da ADSL- und Kabelmodems sich nicht über herkömmliche Telefonnummern ins Internet einwählen, bleiben sie von dieser Plage verschont.



Seien Sie bei Webseiten, die Download und Installation einer «Zugangssoftware» verlangen, besonders vorsichtig. Meist verbirgt sich dahinter ein Dialer



Die Funktion «AutoVervollständigen» ist zwar bequem, birgt aber auch ein grosses Risiko. Am besten deaktivieren Sie die Funktion

Anwender mit ISDN- oder Analog-Modem sollten sich hingegen vor diesen Abzock-Tools schützen. Verwenden Sie dazu eine Anti-Dialer-Software wie YAW (Yet Another Warner). Diese überwacht Ihre Internetverbindung und kann ausgehende Nummernbereiche sperren. Auch das Beseitigen von Dialern ist mit der Software kein Problem. Als zusätzliche Sicherheitsmassnahme können Sie bei Ihrem Telefonanbieter ausgehende Nummern mit der Vorwahl 0900, 0901 und 0906 kostenlos sperren lassen.

Halten Sie sich auch an folgende goldene Regel: Laden Sie Programme nur von Seiten herunter, die Sie kennen und denen Sie vertrauen. Weitere Informationen und Tipps zu Dialern finden Sie in «Dialer-Tricks enttarnt!», PCtipp 2/2003, Seite 32 (WEBCODE **pdf030232**).

Anonym im Web: Viele Anwender glauben, anonym durchs weltweite Datenmeer zu surfen. Dem ist aber nicht so. Wer sich ins Internet einwählt, erhält vom Provider eine so genannte IP-Adresse zugeteilt. Dank dieser Adresse lässt sich ein PC während einer Internetsitzung eindeutig identifizieren, weil alle Daten, die zwischen ihm und dem Webserver ausgetauscht werden, diese IP-Adresse tragen. Hat jemand Zugriff auf die Logfiles des Providers, kann er herausfinden, wann Sie eine bestimmte Seite besucht haben.

Wer wirklich unerkannt im Web surfen möchte, sollte deshalb einen Anonymisierungsdienst verwenden. Bekannt und sehr gut ist JAP. Es handelt sich um ein Programm der Universität Dresden. Weitere Infos finden Sie in der Box «Empfohlene Schutz-Programme», S. 29.

Daten eingeben: Im World Wide Web trifft man immer wieder auf Sites, welche die Eingabe von Daten verlangen. Sie fordern eine Registrierung, damit sich beispielsweise bestimmte Dienste nutzen lassen oder z. B. die Gewinnchancen bei Wettbewerben verbessern. Seien Sie nicht zu vertrauensselig: Je mehr Sie von sich preisgeben, desto ausführlichere Benutzerprofile können über Sie erstellt werden. Besonders freche Firmen verkaufen ihre Datensammlungen auch weiter.

Geben Sie nur an, was wirklich verlangt wird. Versuchen Sie es mit fiktiven Informationen. Bei einigen Webseiten ist dies möglich. Besondere Vorsicht ist bei Angaben wie Kreditkartennummern geboten. Überprüfen Sie Impressum und AGBs der Website und achten Sie darauf, dass die Daten verschlüsselt übermittelt werden: Die Adresse der Website sollte mit https:// beginnen (nicht nur mit http://). Zudem zeigen die meisten Browser bei sicheren Seiten ein geschlossenes Schlosssymbol an, Icon links. Beim Internet Explorer sehen Sie dieses in der Statusleiste am unteren Fensterrand.

Hüten Sie Ihre E-Mail-Adresse gut. Sie kann sonst schnell einmal auf der Empfängerliste eines Spammers landen. Als Folge davon erhalten Sie täglich lästige Werbung in Ihren virtuellen Posteingang. Am besten verwenden Sie für Angaben im Web eine anonyme Zweitadresse. Solche Adressen holen Sie sich bei Gratisdiensten wie www.gmx.ch, www.web.de oder www.hotmail.ch.

Tipp: Wenn Sie Ihren Computer nicht allein benutzen, sollten Sie beim Besuch von Webseiten auf das automatische Ausfüllen von Passwörtern und Formularen verzichten. Im Internet Explorer deaktivieren Sie dieses Feature unter Extras/Internetoptionen/Inhalte/AutoVervollständigen, Screen 6. Hier finden Sie ferner eine Option, um bereits gespeicherte Passwörter zu löschen.

Sicher mailen

Eine weitere grosse Gefahrenquelle für Virenifektionen und andere Schädlinge sind E-Mail-Nachrichten. Gerne schleusen sich Plagegeister über Mailanhänge oder so genannte HTML-Mails auf dem Rechner ein. Mit den richtigen Programmeinstellungen und dem Wissen um die Bedrohungen lässt sich das Risiko aber beträchtlich reduzieren.

HTML-Mails: E-Mails können als reiner Text oder im HTML-Format versendet werden. Letzteres ist eigentlich nichts anderes als eine Webseite, die ebenfalls mit der Webseitenbeschreibungssprache HTML (HyperText Markup Language) erstellt wird. Daher besteht auch die Möglichkeit, → Scripts, ActiveX-Kontrollen und WebBugs einzubauen.

Zur Anzeige von HTML-Nachrichten verwenden die meisten Mailprogramme einen Webbrowser. Outlook und Outlook Express benutzen beispielsweise den Internet Explorer. Sie übernehmen damit leider auch die Sicherheitsschwächen dieses Browsers. Am besten verhindern Sie die Ausführung von unerwünschtem Code, indem Sie die Anzeige von HTML-Mails deaktivieren. In Outlook tun Sie dies mit Extras/Optionen/Einstellungen/E-Mail-Optionen/Standardnachrichten im Nur-Text-Format lesen, in Outlook Express wählen Sie Extras/Optionen/Lesen/Alle Nachrichten als Nur-Text lesen.

Möchten Sie nicht vollständig auf den Empfang von HTML-Mails verzichten, sollten Sie ▶

FACHCHINESISCH

IP-Adresse

Computer benötigen während einer Internetsitzung eine eindeutige IP-Adresse, damit sie mit anderen Rechnern kommunizieren können. Diese ist aus mehreren Nummernblöcken aufgebaut (z. B. 212.98.56.278). Unterschieden wird zwischen statischen und dynamischen Adressen. Letztere wechseln bei jeder Einwahl.

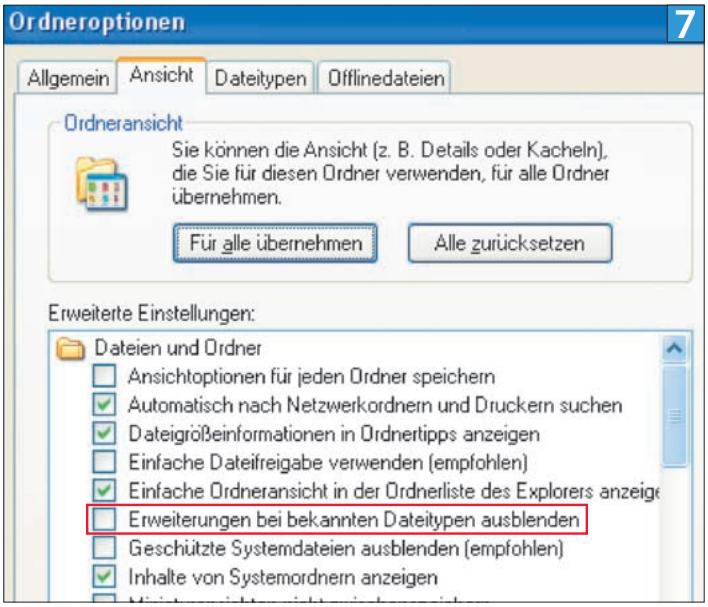
Script

Ein Script ist ein Computer-Programm. Seine Anweisungen müssen im Gegensatz zu anderen Programmiersprachen nicht zuerst übersetzt (kompiliert) werden, sondern lassen sich von anderen Anwendungen direkt ausführen (interpretieren). Eine typische Script-Sprache ist beispielsweise ActiveX.

zumindest die Sicherheitseinstellungen Ihrer Mailsoftware verschärfen. Wählen Sie dazu im Internet Explorer unter EXTRAS/INTERNETOPTIONEN/SICHERHEIT die Webinhaltszone EINGESCHRÄNKTE SITES an und klicken Sie anschliessend auf STUFE ANPASSEN. Kontrollieren Sie, ob die Sicherheitsstufe «Hoch» eingestellt ist. In Outlook und Outlook Express wählen Sie anschliessend unter EXTRAS/OPTIONEN/SICHERHEIT jeweils die Option «Zone für eingeschränkte Sites».

Die Attachment-Falle: Viele Viren verbreiten sich über Mailanhänge. Ein Doppelklick auf ein Attachment reicht, um sich eine virtuelle Grippe einzufangen. Bevor Sie einen Anhang öffnen, sollten Sie ihn immer zuerst auf Ihrer Festplatte speichern und ein aktualisiertes Antiviren-Programm darüber laufen lassen. Aber selbst mit einer Antiviren-Software sind Sie nicht gegen alle Krankheiten gefeit. Ganz neue Schädlinge sind eventuell noch nicht in der Datenbank des Antiviren-Herstellers aufgenommen. Vielleicht haben Sie vergessen, Ihr Schutz-Programm zu aktualisieren? Begegnen Sie Mailanhängen immer mit einer gesunden Portion Vorsicht. Öffnen Sie keine Files von unbekannten Absendern.

Viren verschicken sich auch gerne unter falschem Absender. So gaukeln sie vor, von einer vertrauten Person zu stammen. Seien Sie bei allen nicht angeforderten Dateien misstrauisch. Vor allem, wenn diese eine auffällige Dateierweiterung wie .exe oder .com tragen. Bei welchen anderen Erweiterungen eine Warnglocke klingeln sollte, verrät Ihnen im Artikel «Schon Windows schützt» die Box «Gefährliche Dateitypen», Seite 60.



Stellen Sie Windows so ein, dass auch bekannte Dateierweiterungen angezeigt werden

Deaktivieren Sie im Windows-Explorer unter EXTRAS/ORDNEROPTIONEN (Windows 98 ANSICHT/OPTIONEN) im Register ANSICHT das Kästchen «Erweiterungen bei bekannten Dateitypen ausblenden», Screen 7. So stellen Sie sicher, dass Windows Ihnen wirklich alle Dateierweiterungen anzeigt.

Verschlüsselung: Nicht nur der Zoll kontrolliert Pakete auf ihren Inhalt, auch neugierige Menschen öffnen gerne mal Post, die nicht für sie bestimmt ist. Dasselbe ist auch bei E-Mails möglich.

Wie einfach dies geht, zeigt ein Fall, der Ende letzten Jahres vor dem Bundesgericht verhandelt wurde: Ein Mitarbeiter hatte während der krankheitsbedingten Abwesenheit seines Chefs eine Umleitung für dessen E-Mails eingerichtet. So konnte er fortan munter die Korrespondenz seines Vorgesetzten mitverfolgen, ohne dass dieser etwas bemerkte.

Hätte der Chef für seine E-Mails eine Verschlüsselungs-Software wie Pretty Good Privacy (PGP) verwendet, wäre der Nachrichtentext für den Mitarbeiter nur Zeichensalat gewesen. Kritische und vertrauliche Nachrichten sollten Sie unbedingt verschlüsseln. Eine genaue Anleitung zu PGP finden Sie in «Sicher ist sicher», PCtipp 2/2003, Seite 40 (WEBCODE **pdf020340**).

Spyware

Heute finden Benutzer zu fast jedem Anwendungsbereich kostenlose Software im Internet. Leider sind die Hersteller dieser Tools nicht immer so uneigennützig, wie man zunächst glauben möchte. Werbeeinblendungen in den Programmen sind noch verständlich. Schliesslich müssen die Programmierer auch von etwas leben. Weniger erfreulich sind Programme, die so genannte Spyware mit auf die Festplatte installieren.

Spyware stammt hauptsächlich von grossen Marketingfirmen. Sie wird dazu verwendet, im Hintergrund Informationen über den Benutzer zu sammeln (z. B. Surfgewohnheiten, Hardware-Profile etc.), um diesen besser zu bewerben. Auch die kostenlose Version des bekannten Tauschbörsen-Tools «Kazaa Media Desktop» beinhaltet Spyware, nämlich das Programm «GAIN AdServer» der Marketingfirma Claria (ehemals Gator). Dieses sammelt Daten über das Surfverhalten des Anwenders.

Achten Sie deshalb beim Installieren von Freeware immer darauf, welche zusätzlichen Tools enthalten sind. Halbwegs seriöse Anbieter geben solche Infos auf ihrer Website oder bei der Installation an. Verwenden Sie zusätzlich ein Programm wie Ad-aware. Es hilft Ihnen beim Erkennen, Aufspüren und Vernichten von Spyware.

Tauschbörsen

Zugegeben, Online-Tauschbörsen haben durchaus ihren Reiz. Sie bieten unzählige Filme, Musik-Files und Programme – und das alles gratis. Die Provider fördern zudem die Download-Freude der Anwender, indem sie im ewigen Kampf um Kunden die Geschwindigkeit von ADSL- und Kabel-Anschlüssen immer weiter erhöhen. Online-Tauschbörsen bergen aber mehrere Gefahren. File-Sharing-Tools wie das bereits erwähnte Kazaa sind zwar kostenlos, kommen aber vielfach mit Spyware daher. Hier gilt es, genau aufzupassen, welche Software zusätzlich installiert wird.

Wer sich nicht genügend schützt, kann sich über Online-Tauschbörsen auch schnell einen Virus einfangen. So ist bei einer heruntergeladenen Datei nie sicher, ob es sich wirklich um das richtige File handelt. Denn die Quelle ist fast immer unbekannt. Gerade bei EXE-Dateien ist das ein gewaltiges Risiko. Auch Netzwerkviren haben leichtes Spiel. Solange Daten «gesaugt» werden, ist der Rechner ständig mit dem Internet verbunden.

Was sich zudem viele Anwender immer noch zu wenig bewusst sind: Tauschbörsen-User bewegen sich in einer rechtlichen Grauzone. Oft handelt es sich bei den angebotenen Musik- und Filmdateien um illegale Kopien. Wer selbst Kopien von Songs und Filmen anbietet, macht sich strafbar. Jeder Benutzer sollte sich deshalb genau überlegen, ob und wie er überhaupt Online-Tauschbörsen nutzen soll. Weitere Informationen über diese Thematik bietet der Artikel «Lieber nehmen als geben», PCtipp 11/2003, Seite 28 (WEBCODE **pdf031128**). ■