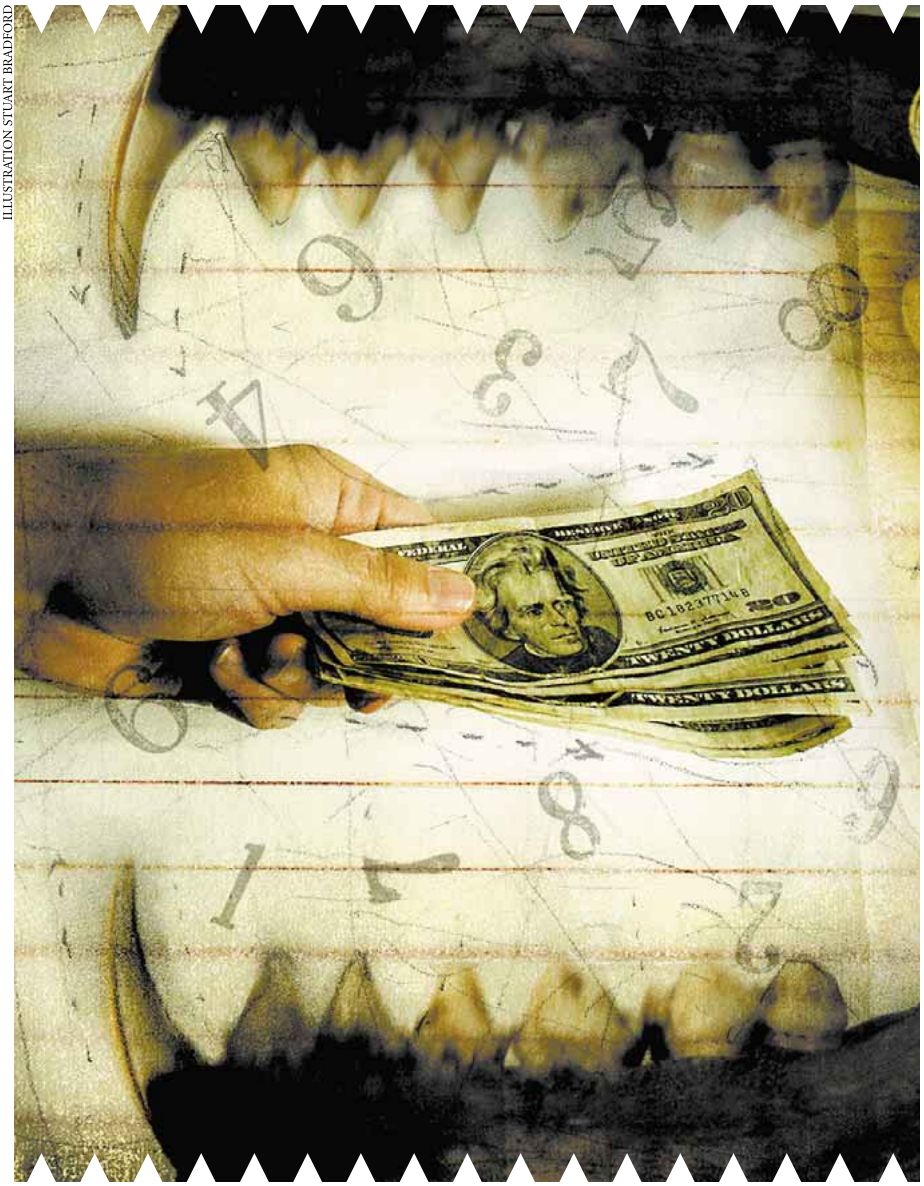
ILLUSTRATION STUART BRADFORD



Dialer-Tricks enttarnt!

Unseriöse Anbieter lassen sich immer gemeinere Maschen einfallen, um Anwendern teure Einwahlprogramme auf den Rechner zu schmuggeln.

von Sascha Zäch

Früher begegnete man Dialern vor allem auf Erotikseiten. Heute ist dem nicht mehr so. Gerade in den letzten Monaten mehrten sich in Internet-Foren Beschwerden von Benutzern, denen hohe Telefonrechnungen ins Haus flatterten, obwohl sie weder freiwillig einen Dialer heruntergeladen noch eine Sex-Site besucht haben. Schuld daran sind die zunehmend gemeinen Tricks von unredlichen Dialer-Anbietern. Diese tarnen ihre Abzock-Programme als nützliche Software oder bewerben diese mit seriös anmutenden E-Mails. Einige nutzen gar Sicherheitsmängel im Internet Explorer, um unbemerkt teure Internetverbindungen auf dem Anwender-PC einzurichten. Auf den folgenden Seiten erfahren Sie mehr über die Funktionsweise von Dialern, die Tricks der Betrüger sowie Schutz- und Entfernungsmassnahmen.

Ursprünglich waren Dialer als einfache Lösung für das automatische Einrichten eines Internetzugangs gedacht. Anstatt alle Einstellungen von Hand einzugeben, genügte ein Doppelklick auf das Dialersymbol, um alle notwendigen Verbindungsdaten automatisch einzurichten.

Da für viele Internetzugänge eine Telefonnummer eingetragen werden muss, dienen Dialer auch als anonymes Abrechnungssystem für kostenpflichtige Internetangebote: Der Anwender muss weder Kreditkarten-Informationen noch persönliche Daten angeben. Sein Modem wählt einfach eine Mehrwert-Dienstnummer und der gewünschte Betrag wird automatisch via Telefonrechnung abgebucht. Gerade dieses nützliche System hat schon nach kurzer Zeit viele Abzocker auf den Plan gerufen.

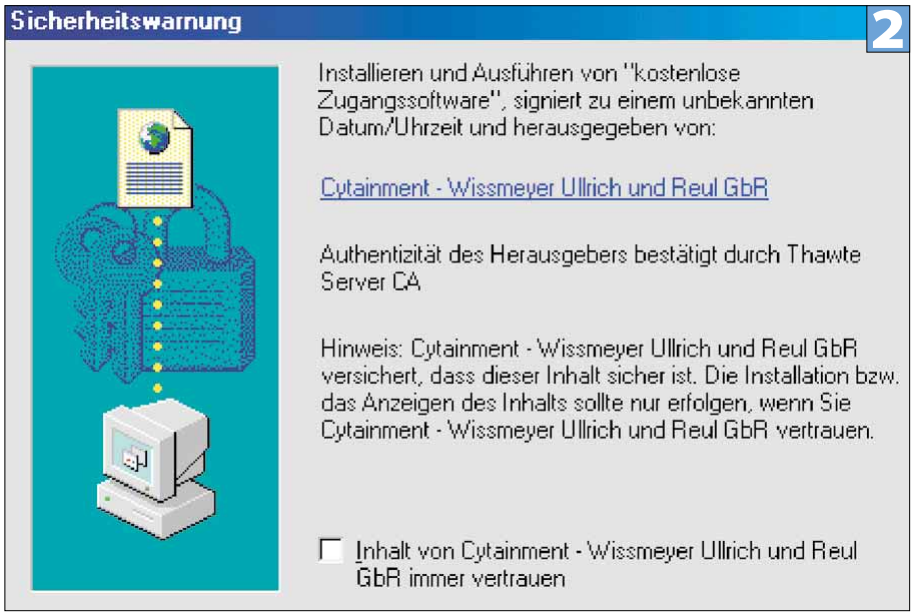
Dialer funktionieren nur über Wählzugänge, das heisst über Analog- oder ISDN-Modems. Besitzer von ADSL- oder Kabelzugängen können diese Programme zwar herunterladen und installieren, da jedoch keine herkömmliche Telefonverbindung für die Datenübertragung aufgebaut wird, haben Dialer keine Möglichkeit, um sich einzuwählen – ausser, es ist zusätzlich ein noch aktives Analog- oder ISDN-Modem am Computer angeschlossen.

In der Schweiz sind die Mehrwert-Dienstnummern dem internationalen Standard angepasst. Sie beginnen mit den Vorwahlen 0900 (für Business, Marketing), 0901 (für Unterhaltung) oder 0906 (für Erwachsenenunterhaltung). Zugeteilt werden sie vom Bakom (Bundesamt für Kommunikation). Momentan gibt es leider noch keine gesetzlich geregelte Obergrenze für die Höhe der Telefongebühren. Laut Bakom sind Anbieter bekannt, die bis zu 10 Franken pro Minute oder eine Pauschale von mehr als hundert Franken pro Anruf verrechnen, **Screen 1**.

Wenigstens war man bis jetzt vor der Gefahr, sich unbemerkt einen teuren ausländischen Dialer einzufangen, gefeit. Es sind nur wenige Fälle bekannt, in denen Programme automatisch die

Einwähl-Programme

Super-Schnäppchen? Pro Einwahl sind bei diesem Dialer 25 Franken zu bezahlen. Dazu kommt noch der Minutenpreis von 20 Rappen.



Der Ausdruck «kostenlose Zugangssoftware» und Hinweise auf die Authentizität des Anbieters wiegen den Anwender in falscher Sicherheit. Das Wort Dialer wird überhaupt nicht erwähnt.

notwendige Landeskennzahl eingetragen haben. Die geplante Einführung der «Universal International Premium Rate Numbers» durch die Genfer Telefonorganisation ITU wird dies zum Leidwesen vieler Anwender schon bald ändern. Die neuen Mehrwert-Dienstnummern sollen international erreichbar sein und mit der Vorwahl 00979 beginnen.

Das Bakom hat verschiedene Richtlinien erlassen, an die sich seriöse Dialer-Anbieter halten müssen (siehe Box «Was ist ein guter Dialer?», rechts). Stellen Sie fest, dass die Vorgaben nicht beachtet werden, sollten Sie dies unbedingt dem Bakom melden (**http://www.bakom.ch/**). Je mehr Informationen Sie dabei über den Missetäter bereithalten (Name des Dialers, Herkunft, Bildschirmfoto mit Gebührenzähler etc.), desto wahrscheinlicher kann das Bakom eine Sperrung der betreffenden Nummer verfügen.

Auch bei allfälligen Streitigkeiten über die Bezahlung einer zu hohen Telefonrechnung müssen Sie diese Angaben unbedingt vorweisen. Das Bakom rät in einem solchen Fall zudem, Ihrer Telefongesellschaft den nicht streitbaren Teil der Rechnung zu bezahlen, da dann Ihr Zugang nicht abgeschaltet werden darf. Leider bieten auch die Richtlinien des Bakoms nur einen Minimalschutz vor betrügerischen Dialern. Unseriöse Anbieter arbeiten mit den übelsten Tricks, um an das schnelle Geld zu kommen.

Die übelsten Dialer-Tricks

Das Wissen um diese Tricks verhindert, dass Sie ahnungslos in eine Dialer-Falle tappen. Der PCtip hat sich in Foren wie Dialerschutz.de (**http://www.dialerschutz.de/**) und Dialerhilfe.de (**http://www.dialerhilfe.de/**) umgesehen und die gemeinsten Abzockermaschen zusammengetragen. Viele der Tricks sind erst in den letzten Monaten aufgetaucht und zeigen, wie unverfroren Dialer-Anbieter zunehmend arbeiten. Jeweils anschliessend finden Sie Tipps, wie Sie sich am besten gegen Dialer schützen können.

Trick 1: Gebührenspielerei

Sehr beliebt sind Gebührenspielereien: Die angegebenen Preise erscheinen auf den ersten Blick niedrig, entpuppen sich aber beim zweiten Hinsehen als Sekunden- und nicht Minutenbeträge. Ähnliche Zahlenspiele kommen auch bei Telefonnummern vor. Über Netzvorwahlen wird versucht, eine 0900er-Nummer zu verschleiern. Besondere Vorsicht ist bei Pauschalgebühren geboten, da diese nicht zeitabhängig sind, sondern schon für eine einzige Einwahl gelten. Hier rechnen die Anbieter mit der Unachtsamkeit der Anwender. Ein Klick auf VERBINDEN genügt, um den gesamten Betrag einzukassieren.

So schützen Sie sich: Vor der bewussten Verwendung eines Dialers sollten Sie Abrechnungsart und Telefonnummer genau überprüfen.

Trick 2: Vorgetäuschte Seriosität

Beim Surfen im Internet öffnet sich ein Download-Fenster. Dieses lässt Sie jedoch im Unklaren darüber, dass es sich bei dem Programm um einen Dialer handelt. Weder Gebühren noch Geschäftsbedingungen sind zu erkennen. Einige Anbieter versuchen, der Software mit Sicherheitszertifikaten einen Hauch von Seriosität zu geben, **Screen 2**. Diese Hinweise sind völlig nutzlos: Auch ein «sicherer» Dialer kostet Geld.

So schützen Sie sich: Achten Sie beim Herunterladen von Software und Plug-Ins darauf, ob es sich um ein Produkt handelt, das Sie wirklich unbedingt benötigen. Werden Sie aus den Hinweisen nicht schlau oder verstehen Sie nicht, was das Programm soll, verzichten Sie auf den Download. Laden Sie keine Inhalte herunter, die aus unbekannten Quellen stammen.

Trick 3: Angstmacherei

Der Dialer wird als nützliche Software getarnt. Ein bekanntes Täuschungsmanöver: Beim Surfen öffnet sich ein Fenster, das Ihnen den Inhalt Ihrer Festplatte zeigt und behauptet, dass dieser öffentlich einsehbar sei. Ein entsprechendes Sicherheitsprogramm ist natürlich gerade zur Hand. In Wirklichkeit kann der Harddiskinhalt nur von Ihnen gelesen werden. Der angebotene Patch entpuppt sich als Dialer. Die Liste solcher Fälle ist lang. Ob Sicherheits-Update, simulierte Fehlermeldung oder Warnhinweise: Verun- ▶

Richtlinien

Was ist ein guter Dialer?

- **Die Mehrwert-Dienstnummer darf nur für Dienste der entsprechenden Kategorie verwendet werden (z. B. «Business»).**
- **Bei jeder schriftlichen oder verbalen Bekanntgabe der Nummer muss der Preis (inkl. Mehrwertsteuer) in Franken und Rappen pro Minute klar aufgeführt sein.**
- **Die Kennzahl 0900, 0901 oder 0906 muss zusammenhängend und vom Rest der Angebotsnummer deutlich getrennt angegeben sein.**
- **Die auflaufenden Verbindungsgebühren müssen immer im Bildschirm-Vordergrund zu sehen sein. Dies gilt auch für Mehrfachverbindungen über ISDN.**
- **Die Gebühren müssen in einer Schriftgrösse von mindestens 14 Punkt dargestellt werden.**
- **Nach dem Schliessen des Browsers muss die Verbindung automatisch getrennt werden.**
- **Ohne Zustimmung des Anwenders darf sich der Dialer nicht als Standardverbindung einrichten.**

▶ sicherung und Angstmacherei sind beliebte Mittel, um Anwender zum Download eines Dialers zu bewegen, **Screen 3**.

So schützen Sie sich: Glauben Sie nicht alles, was Ihnen im Web an den Kopf geworfen wird. Geraten Sie bei Warnhinweisen oder Meldungen über Sicherheitslücken nicht sofort in Panik, sondern erkundigen Sie sich zuerst auf Websites der betreffenden Produkthersteller und auf News-Seiten von PC-Magazinen, ob derartige Probleme bekannt sind. Dort finden Sie meist die passenden Sicherheits-Updates.

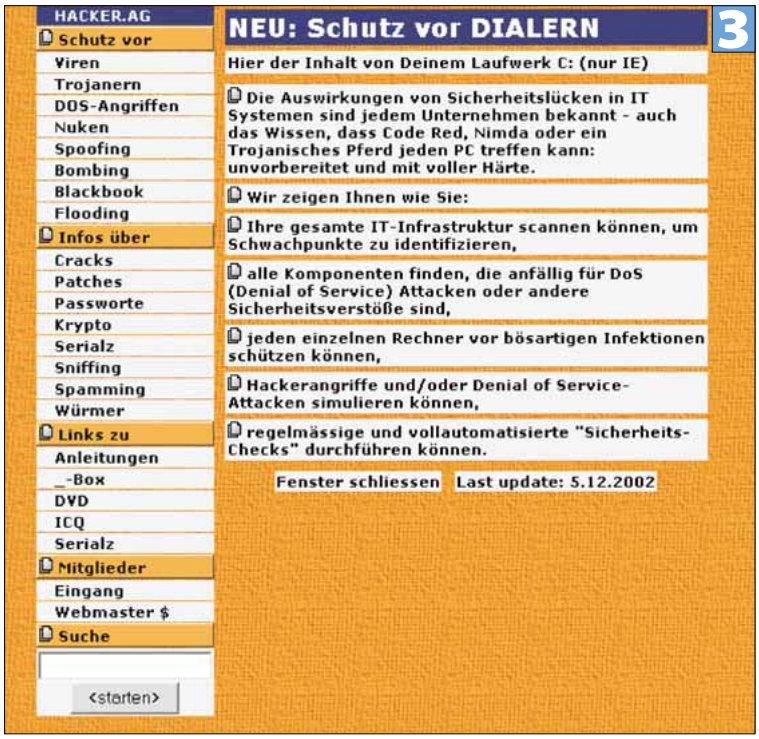
Trick 4: Gecrackte Dialer

Im Internet sind Gerüchte über so genannte «gecrackte» Dialer im Umlauf. Diese seien so manipuliert worden, dass sie gratis den Zugang zu kostenpflichtigen Angeboten ermöglichen.

So schützen Sie sich: Eine glatte Lüge – gecrackte Dialer gibt es nicht. Sie sind technisch nicht möglich.

Trick 5: Automatische Installation

Einige besonders «clevere» Anbieter haben sich überlegt, dass es besser wäre, den Anwender gar nicht mehr um die Download-Erlaubnis zu fragen. Der Dialer wird automatisch und unbemerkt im Hintergrund installiert. Dazu benutzen



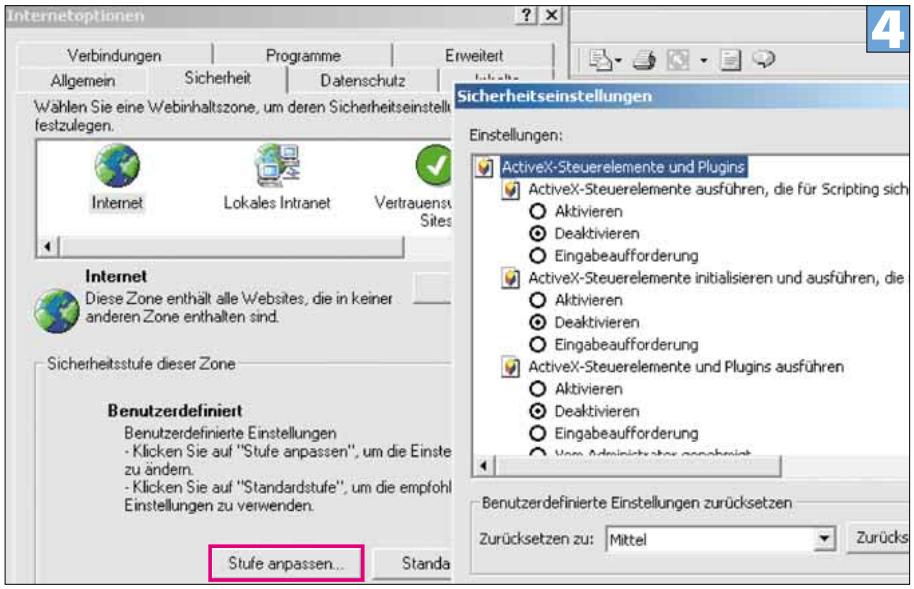
Die Website Hacker.ag gibt perfiderweise vor, Sicherheits- und Anti-Dialer-Tools anzubieten. Sie können hier jedoch nur eines herunterladen – Dialer.

Einwähl-Programme

Anbieter die Programmiersprache → **ActiveX**: Sobald ein Anwender auf eine Homepage surft, wird ein Befehl ausgeführt, der den Programm-Download selbstständig startet.

So schützen Sie sich: Da ActiveX von Microsoft entwickelt wurde, funktioniert dieser Trick nur beim Internet Explorer. Sie können sich also dagegen schützen, indem Sie einen alternativen Browser (z. B. Netscape, Mozilla, Opera) verwenden. Ist Ihnen jedoch der Internet Explorer ans Herz gewachsen, sollten Sie die Ausführung von ActiveX deaktivieren oder wenigstens einschränken. Wählen Sie in der Menüleiste EXTRAS/INTERNET-OPTIONEN/SICHERHEIT/STUFE ANPASSEN und deaktivieren Sie alle Einträge, in denen «ActiveX-Steuerelemente» vorkommen, **Screen 4**.

Ausserdem empfiehlt es sich, für die «Java-Einstellungen» eine «Hohe Sicherheit» anzukreuzen, «Active Scripting» zu deaktivieren und für «Einfügeoperationen über ein Script zulassen», «Scripting von Java-Applets» sowie «Installation von Desktop-Elementen» eine «Eingabeaufforderung» zu verlangen. Auch bei anderen Browsern ist es besser, «JavaScript» und «Active Scripting» zu deaktivieren. Durch diese strengen Sicherheitseinstellungen kann es bei Webseiten zu Darstellungs- und Ausführungsfehlern kommen, doch macht diese Einbusse den Schutz vor Dialern allemal wett. Weniger restriktiv, aber gleichfalls sicher: An Stelle von «deaktivieren» verlangen Sie überall eine «Eingabeaufforderung».



Deaktivieren Sie im Internet Explorer unbedingt die «ActiveX-Steuerelemente». So verhindern Sie unautorisierte Programm-Downloads.

Die E-Mail scheint auf den ersten Blick von einer vertrauten Person zu kommen. Klickt man auf den mitgeschickten Link, landet man auf der Seite eines Dialer-Anbieters.

Trick 6: Getarnte Bestätigung

Die Download-Bestätigung eines Dialers wird auf einer seriös wirkenden Homepage als Textlink, Bild oder Pop-Up getarnt. Sobald Sie mit der Maus darauf klicken, wird das Programm heruntergeladen.

So schützen Sie sich: Hier helfen ebenfalls die vorhin beschriebenen Sicherheitseinstellungen, da so kein unautorisierter Download mehr möglich ist.

Trick 7: Die E-Mail-Falle

Viele Dialer-Hersteller arbeiten vermehrt mit Spammern zusammen, um ihre Programme möglichst schnell und grossflächig zu verbreiten. Das Problem: Gerade in der Spam-Szene gibt es viele schwarze Schafe, die vor unlauteren Methoden nicht zurückschrecken.

So sind z. B. E-Mails im Umlauf, die vorgeben, von einer bekannten, seriösen Firma zu stammen. Sie fordern den Anwender auf, ein Attachment zu installieren oder über einen mitgeschickten Link eine Webseite zu besuchen, **Screen 5**. Was der Anwender herunterlädt, ist natürlich ein Dialer. Eine andere gemeine Methode sind Grusskarten-Mails. Neugierig, wie man ist, möchte man gerne wissen, wer einem die nette Nachricht schickt, und klickt auf den angegebenen Link. Auf der Site angekommen, müssen Sie für die korrekte Anzeige zuerst ein Plug-In installieren – das sich wieder einmal als Dialer entpuppt.

So schützen Sie sich: Seien Sie bei Attachments und Textlinks vorsichtig. Wenn Sie den Absender einer E-Mail nicht kennen, sollten Sie keine Anhänge öffnen. Versuchen Sie bei scheinbar seriösen Anbietern, die einen Download empfehlen, herauszufinden, von wo die Nachricht wirklich kommt. Wie das geht, erfahren Sie im Artikel «Mails auf dem Seziertisch», PCtip 7/2002, ab Seite 40 (**http://www.pctip.ch/archiv/2002/7.asp**).

Passen Sie die Sicherheitseinstellungen Ihres Mail-Programms an. Programme wie Outlook, Outlook Express oder Netscape Mail können → **HTML**-Nachrichten darstellen. Dadurch ist es unlauteren Anbietern möglich, mittels ActiveX oder anderen Programmiersprachen unbemerkt einen Dialer auf Ihrem PC zu installieren. Schützen Sie sich davor, indem Sie in Outlook unter EXTRAS/OPTIONEN/SICHERHEIT/ZONENEINSTELLUNGEN die Option «Eingeschränkte Sites» wählen (Outlook Express: EXTRAS/OPTIONEN/SICHERHEIT/ZONE FÜR EINGESCHRÄNKTE SITES). Auch in anderen Mail-Programmen sollten Sie das Ausführen von Skriptbefehlen unterbinden.

Trick 8: Manipulierte Registry

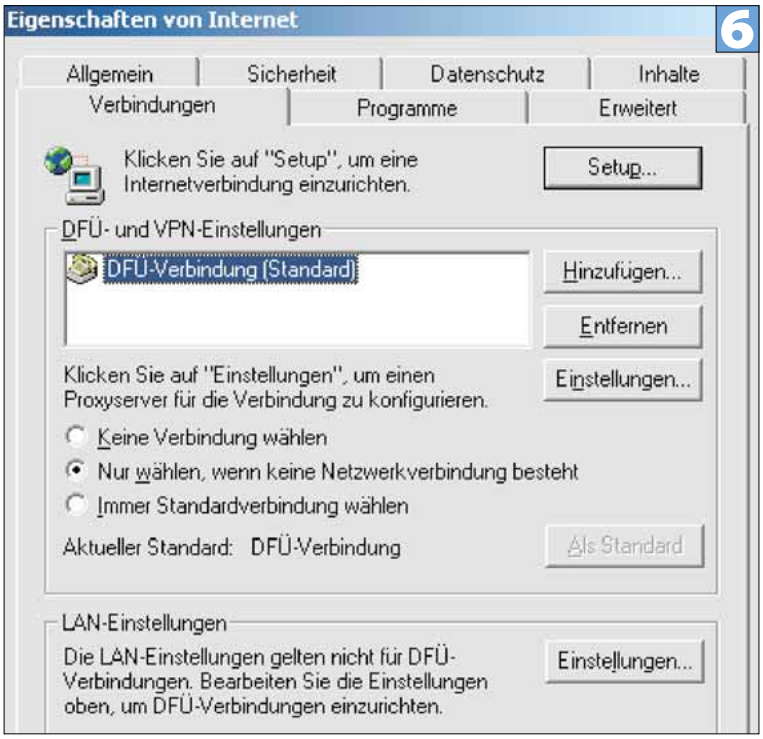
Besonders unverfrorene Dialer-Programme nehmen Änderungen an der Systemkonfiguration vor. Sie manipulieren die → **Registry** oder ▶

Fachchinesisch

ActiveX
Eine von Microsoft entwickelte Programmiersprache, die es ermöglicht, Befehle auf Webseiten auszuführen. Sie funktioniert aber nur mit dem Internet Explorer.

HTML
Die HyperText Markup Language (HTML) ist eine Sprache zur Beschreibung von Webseiten. Browser wie der Internet Explorer setzen den Textcode in ein grafisches Erscheinungsbild um.

Registry
Spezielle Datenbank, die von Windows verwaltet wird. Auf Grund der Registry weiss Windows beispielsweise, wie gewisse Dateitypen bearbeitet werden müssen.



Die INTERNET OPTIONEN zeigen Ihnen, welche DFÜ-Verbindungen auf Ihrem Rechner installiert sind.

▶ den Autostart-Ordner. So gelingt es ihnen, sich kurzerhand zur Standardverbindung zu erklären oder sich bei jedem Windows-Neustart sofort ins Internet einzuwählen. In anderen Fällen tickt der Gebührenzähler der Software auch nach dem scheinbaren Trennen der Verbindung munter weiter.

So schützen Sie sich: Wenden Sie die erwähnten Sicherheitsmassnahmen an, so ist die Wahrscheinlichkeit gering, sich überhaupt einen Dialer einzufangen. Werfen Sie zur zusätzlichen Sicherheit vor und während jeder Internetsitzung einen kurzen Blick auf Ihre Standard-→**DFÜ-Verbindung**. Sie finden diese unter START/EINSTELLUNGEN/SYSTEMSTEUERUNG/INTERNETOPTIONEN/VERBINDUNGEN (Windows XP: START/SYSTEMSTEUERUNG/INTERNETOPTIONEN/VERBINDUNGEN), **Screen 6**.

Fachchinesisch

DFÜ-Verbindung

Über die DFÜ-Verbindung wird eine Verbindung zu einem Netzwerk oder dem Internet aufgenommen. Dabei können nur Geräte benutzt werden, die das Telefonnetz verwenden (z. B. Analog- oder ISDN-Modem).

Klicken Sie auf EINSTELLUNGEN und danach auf EIGENSCHAFTEN. Im folgenden Dialogfenster überprüfen Sie im Register ALLGEMEIN, welche Telefonnummer die Verbindung jeweils wählt, **Screen 7**.

Kontrollieren Sie regelmässig die Windows-Taskleiste am unteren Bildschirmrand, den

Einwähl-Programme

Desktop und den Autostart-Ordner (START/PROGRAMME/AUTOSTART). Unbekannte Symbole weisen evtl. auf einen Dialer hin, **Screen 8**. Siehe auch Box «Suchen, finden und löschen», unten.

Lassen Sie den akustischen Einwahlton Ihres Modems eingestellt, damit Sie immer wissen, wann eine Internetverbindung aufgebaut wird. Als zusätzliche Massnahme lohnt sich eine regelmässige Überprüfung Ihrer Telefonrechnung. Swisscom (**http://www.swisscom-fixnet.ch/fx/content/billing/ebilling/index_DE.html**) und Sunrise (**http://internet.sunrise.ch/de/internet/int_acc.asp**) bieten diese Möglichkeit beispielsweise online an.

Trick 9: DFÜ-Netzwerk ausgetrickst

Neu und besonders beunruhigend sind Meldungen über Dialer, die das DFÜ-Netzwerk austricksen. Sie löschen den eigenen Eintrag nach der Internetverbindung und richten ihn erst wieder bei einer erneuten Internetsitzung ein. Erreicht wird dies durch ein Zusatzprogramm, das beim Herunterladen des Dialers mitinstalliert wird. So genannte → **CAPI**- und → **TAPI**-Dialer sollen es sogar schaffen, die Softwareschnittstellen von ISDN-Karten direkt anzusprechen. Ein Eintrag ins DFÜ-Netzwerk ist dadurch nicht mehr notwendig. Übel sind auch DLL-Dialer. Sie installieren beim erstmaligen Besuch einer Website oder beim Öffnen einer E-Mail heimlich ein Programm, das eine DLL-Datei auf dem Rechner anlegt. Surft ein Anwender auf eine entsprechend präparierte Website, wird automatisch ein Dialer heruntergeladen – selbst wenn ActiveX nun ausgeschaltet ist.

So schützen Sie sich: Auch hier gilt: Halten Sie sich an alle bisher beschriebenen Schutzmassnahmen! Dann ist es fast unmöglich, dass sich ein Dialer unbemerkt in Ihrem System einnistet.

Weitere Schutzmassnahmen sind das Sperren von Mehrwert-Dienstnummern und die Verwendung von Schutzprogrammen. Schweizer Telekom-Firmen sind gesetzlich verpflichtet, 0906er-Nummern gratis zu sperren. Es muss nur ein entsprechender Antrag bei der Swisscom oder beim jeweiligen Anbieter gestellt werden. Die Blockierung anderer Mehrwert-Dienstnummern (0900/0901) ist kostenpflichtig. Während für die Sperrung meist ein einfacher Anruf genügt, ist für die Entsperrung ein schriftlicher Antrag erforderlich.

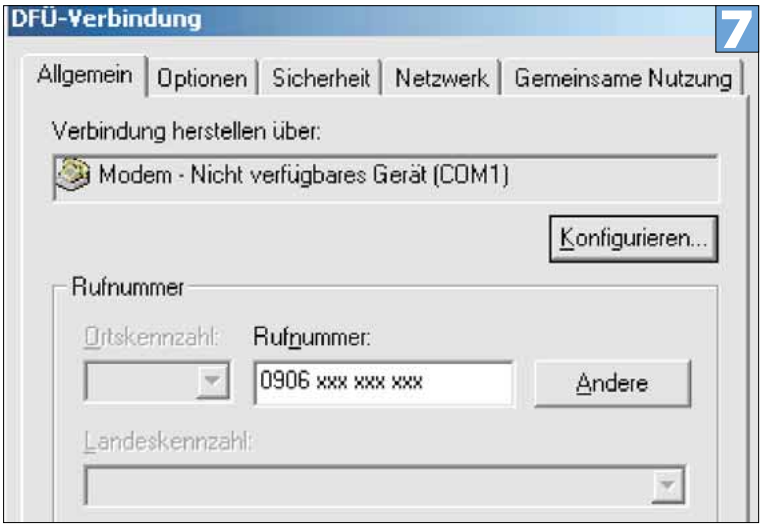
Schutzprogramme, auch Dialer-Blocker genannt, überwachen das DFÜ-Netzwerk auf neue Verbindungen und verhindern, dass teure bzw. unbekannte Telefonnummern gewählt werden. Bewährt hat sich die kostenlose Software YAW (Yet Another Warner, **http://www.pctip.ch/downloads/dl/20556.asp**) sowie der 0190-Warner 3.20 (**http://www.pctip.ch/downloads/dl/23008.asp**), der auch Schutz gegen CAPI/TAPI-Dialer bietet. Dieser Warner ist trotz seines Namens auch in der Schweiz einsetzbar.

Fachchinesisch

CAPI/TAPI

CAPI (Common Application Program Interface) und TAPI (Telephony Application Program Interface) sind Schnittstellen, über die mittels Software ISDN-Geräte angesprochen werden können.

Die 0906er-Nummer weist auf einen Dialer hin. Wie Sie diesen entfernen können, lesen Sie in der Box unten.



Das Symbol «birthday» ist ein schlechtes Geburtstagsgeschenk. Nach einem Doppelklick installiert sich ein Dialer.

Falls sich bereits ein Dialer auf Ihrem PC eingeschlichen hat, dann hilft Ihnen die Box «Suchen, finden und löschen», unten, weiter. Dort finden Sie die wichtigsten Infos, um Ihre Festplatte von den lästigen Programmen zu säubern. Sehr ausführliche Hinweise zum Entarnen und Entfernen von Dialern bietet auch der PCtip-Artikel «Cyber-Sex zum Hochtarif», PCtip 4/2002, **http://www.pctip.ch/archiv/2002/4.asp**.

Dialer entfernen

Suchen, finden und löschen

Anzeichen für eine mögliche «Dialer-Infektion»:

- Im DFÜ-Netzwerk ist eine Verbindung mit Mehrwert-Dienstnummer eingetragen (siehe «Trick 8: Manipulierte Registry», Seite 35).
- Unbekannte Symbole in der Taskleiste, auf dem Schreibtisch, im Windows-Startmenü oder im Autostart-Verzeichnis (START/PROGRAMME/AUTOSTART).
- Das Modem wählt sich selbstständig ins Internet ein.
- Die Startseite des Browsers hat sich bei der letzten Internetsitzung geändert.

Dialer finden:

- Überprüfen Sie das DFÜ-Netzwerk auf Mehrwert-Dienstnummern (siehe «Trick 8: Manipulierte Registry», Seite 35). Notieren Sie sich den Verbindungs-Namen.
- Durchsuchen Sie Taskleiste, Desktop, Startmenü und Autostart-Verzeichnis (START/PROGRAMME/AUTOSTART) nach unbekannten Einträgen. Notieren Sie suspekte Namen.
- Suchen Sie auf der Harddisk mit START/SUCHEN/NACH DATEIEN ODER ORDNERN nach Dialer-Dateien.
- Teilweise tragen sich Dialer auch in der Registry ein, da sie hier schwerer zu finden und zu entfernen sind. Suchen Sie nach den verdächtigen Namen: Klicken Sie auf START/AUSFÜHREN und geben Sie regedit ein. Wählen Sie dann HKEY_CURRENT_USER/Software.

Dialer löschen:

- Bei seriösen Dialern können Sie die Software über eine programmeigene «Löschen»-Funktion entfernen.
- Wenn Ihnen der Name der Dialer-Datei bekannt ist, löschen Sie das Programm über START/EINSTELLUNGEN/SYSTEMSTEUERUNG/SOFTWARE (Windows XP: START/SYSTEMSTEUERUNG/SOFTWARE).
- Klicken Sie im DFÜ-Netzwerk den betreffenden Eintrag an und löschen Sie ihn mit *Delete*. Wie Sie ins DFÜ-Netzwerk gelangen, lesen Sie in «Trick 8: Manipulierte Registry», Seite 35.
- Einträge im Autostart-Verzeichnis lassen sich mit einem einfachen Rechtsklick und LÖSCHEN entfernen.
- Dialer-Dateien, die Sie auf der Festplatte entdecken, können Sie mit *Delete* löschen.
- Benutzen Sie Freeware-Programme wie «RegCleaner», http://www.pctip.ch/downloads/dl/19257.asp, um in der Registry dubiose Dateien zu entfernen.