Was weiß Microsoft?

Aktivierung per Call-Center

Wer Windows per Telefon aktiviert, diktiert dem Call-Center-Mitarbeiter eine 50-stellige Nummer. Diese errechnet sich unter anderem aus der Produkt-ID und einem Hash-Wert (Prüfsumme) der Hardware-Konfiguration. Der Call-Center-Mitarbeiter überprüft die Zahl und gibt den zugehörigen Entsperr-Code durch, den der Anwender dann in den Aktivierungs-Dialog einträgt.

Hersteller verkaufen es als Kundenservice, Anwender befürchten die totale Kontrolle: Viele Programme senden ohne Rückfrage Daten nach Hause. Lesen Sie, was der PC verschickt und wie Sie sich vor zu viel Neugier schützen.

Von Thorsten Eggeling, Andreas Kroschel und Christian Löbering

Der PC-Anwender wird immer durchsichtiger. Microsoft arbeitet zusammen mit den Hardware-Herstellern AMD, HP und Intel an der Technologie NGSCB (Next Generation Secure Computing Base), die mehr Sicherheit am PC verspricht. Bedeutet das besseren Schutz vor Viren, Würmern oder Spam? Nein, es geht vorrangig um besseren Schutz der Software-Hersteller und Medien-Anbieter vor Raubkopierern. NGSCB soll bereits nächstes Jahr mit dem XP-Nachfolger Longhorn ausgeliefert werden und sieht eine Zertifizierungspflicht in vielen Bereichen des PC-Alltags vor – auf Kosten der Privatsphäre der Anwender. Denn die nötigen Zertifikate werden voraussichtlich an die Daten eines bestimmten Systems gebunden sein.

Schon heute Realität

Was wie Science Fiction klingt, ist aber längst vorbereitet und teilweise Realität: Spyware protokolliert die Surfgewohnheiten, um Werbe-Popups abzusetzen. Windows XP übermittelt bei der Aktivierung eindeutig identifizierbare Hardware-Komponenten. Downloads vom Microsoft Server fordern eine Gültigkeitsprüfung und verweigern sich gegebenenfalls mit einem „Validation Failure“. Musikstücke kommerzieller Anbieter sind per DRM (Digital Rights Management) geschützt und lassen sich nur auf einem PC ab-

spielen – auf jedem nicht berechtigten PC bleiben sie stumm ...
Die Hersteller versichern, dass sie keine personenbezogenen Daten übermitteln und den Rechner nicht ausspionieren. Doch können Sie ihnen trauen? Lesen Sie auf den folgenden Seiten, wie weit Microsoft und Co. bereits jetzt gehen und wie Sie herausfinden, was Ihr Rechner alles über Sie ausplaudert.

Windows plaudert

Ob bei der Aktivierung, beim Update, beim Download vom Microsoft-Server oder beim Einsatz des Windows Media Players: Windows telefoniert recht gerne nach Hause. Aktuell reichen die übermittelten Daten nicht aus, um auf eine bestimmte Person – sprich: auf Sie persönlich – zu schließen, aber schon heute gibt es Ausnahmen. Wir untersuchen im ersten Teil Web-Aktionen, die praktisch jeden Windows-Anwender betreffen.

1. Windows-Aktivierung: Relativ harmlos

Seit Windows XP präpariert Microsoft seine Systeme mit Zeitbomben. Wer sich nicht spätestens 30 Tage nach der Installation beim Hersteller meldet und eine legal erworbene Version nachweist, kann das System nicht mehr starten. Diese Aktivierung wird über den Befehl „Msoobe.EXE /a" im Verzeichnis \Windows\System32\oobe angestoßen.
Anwender, die möglichst wenig preisgeben wollen, wählen bei der Aktivierung am besten die telefonische Variante: Außer der vom System errechneten 50-stelligen Nummer erfährt der Call-Center-Mitarbeiter bei Microsoft nichts.
Die Internet-Aktivierung sendet deutlich mehr. Die Kommunikation zwischen Ihrem System und dem Aktivierungs-Server erfolgt über ein mit SSL (Secure Sockets Layer) verschlüsseltes HTTP-Protokoll. Unsere Schwester-Redaktion Tecchannel (www.tecchannel.de) hat den Datenstrom mit einem eigenen Tool abgefangen und analysiert. Das System kontaktiert den Aktivierungs-Server über drei Anfragen, die vom Server jeweils bestätigt werden müssen. Übertragen wird dabei die Produkt-ID Ihres Systems, wie sie unter „Arbeitsplatz, Eigenschaften" angezeigt wird. Diese Zahl errechnet sich aus dem Product-Key, den Sie bei der Installation eingegeben haben. Seit Service Pack 1 vollständig übertragen werden außerdem der Product-Key sowie die Spracheinstellungen des Systems und Informationen zur Hardware-Konfiguration. Das sind beispielsweise die eindeutige (MAC-)Adresse des Netzwerk-Adapters und die Seriennummer der CPU.
Das wäre mehr als ausreichend, um genau einen PC-Anwender zu identifizieren, jedoch gehen diese individuellen Konfigurationsdaten nicht direkt in den Datenstrom ein, sondern durchlaufen vor der Übertragung einen Hashing-Algorithmus. Die so generierte Zahl ist zwar eindeutig, lässt aber keinen Rückschluss mehr auf die ursprünglichen Werte der einzelnen Komponenten zu. Folglich kann Microsoft Sie, Ihr System und die darauf installierte Software über die Aktivierung nicht ausspionieren. -cl

Überblick Datenspione

PC WELT Meinung von Thorsten Eggeling

Software ist Vertrauenssache

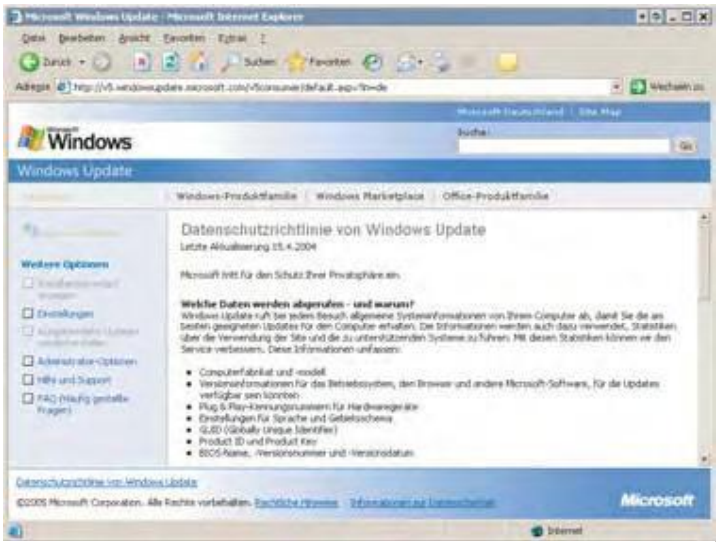
Was ein Programm auf Ihrem PC tut, weiß so ganz genau eigentlich nur der Programmierer der Software. Wer den Quelltext einer Anwendung nicht besitzt, ist ihrem Wirken auf Gedeih und Verderb ausgeliefert. Ob der Zugriff auf eine bestimmte Datei oder einen Registry-Zweig gefährlich oder harmlos ist, ob ein Programm heimlich Ihre persönlichen Daten sammelt oder Ihr Verhalten im Internet protokolliert, ist nur mit größtem Aufwand zu analysieren. Hier bleibt nur das Vertrauen in die Lizenzbestimmungen und Datenschutzerklärungen des Herstellers.
Wenn es um hochsensible Daten geht, ist daher nur der Umstieg auf Open-Source-Software ein konsequenter Ausweg. Denn selbst wenn Firmen wie Microsoft ausgewählten Personen, Institutionen und Behörden Einblick in den Windows-Quellcode gewähren, kann niemand mit Sicherheit sagen, ob das Produkt auf der Festplatte tatsächlich diesem Quellcode entspricht. Zudem gelangen mit jedem Update und Service Pack veränderte und neue Programme auf den PC, die bisher unbekannte Funktionen enthalten können.
Natürlich können theoretisch auch Open-Source-Anwendungen schädlichen Code oder Spionage-Funktionen enthalten. Deshalb sollten Sie auch hier – und ebenso bei Free- und Shareware – nur Programme aus vertrauenswürdigen Quellen einsetzen. Auch wenn Sie selber die Code-Zeilen nicht interpretieren können oder wollen: Nur ein offener Quellcode ermöglicht Kontrolle und damit mehr Sicherheit.

Update ist Pflicht

Auch wenn Ihnen der Gedanke nicht gefällt, Infos an Microsoft zu schicken: Regelmäßige Updates sind Pflicht, da Sie sonst Viren und Würmern Tür und Tor öffnen. Das kann im ungünstigsten Fall dazu führen, dass Ihr PC zum Spam-Zombie mutiert und beliebige Infos an beliebige Leute verschickt. Da scheint der Datenaustausch mit Microsoft die bessere Wahl.

Microsofts Copy-Kill

Jedes Service Pack enthält eine Black-List mit illegalen Product-Keys. Wer eine dieser Nummern verwendet, kann das Service Pack nicht installieren. Ähnliches passiert beim Windows-Update und nun auch beim herkömmlichen Download. Microsoft erweitert die Black-List kontinuierlich. Ziel ist es wohl, Raubkopierer generell von den Updates abzuklemmen. Somit erhalten Sicherheitslücken den zweifelhaften Nutzen, raubkopierte Systeme unbrauchbar zu machen oder in Spam-Schleudern zu verwandeln.



Datenschutz oder Datenklau? Microsoft bedient sich mit vollen Händen auf Ihrem Rechner, wenn Sie Ihr System aktualisieren (Punkt 2)

2. Windows-Update sendet mehr als nötig

Weniger zahm als die in ▷ Punkt 1 beschriebene Aktivierung verhält sich die Windows-Update-Funktion. Wenn Sie www.windowsupdate.com besuchen oder die Funktion „Automatische Updates" verwenden, sendet ein Active-X-Control eine Anfrage an den Update-Server.

Wir haben festgestellt: Die übermittelten Informationen gehen weit über das nötige Maß hinaus. Neben zweckmäßigen Infos aus der Registry wie der Version des Systems, des Browsers und anderer Microsoft-Software, für die Windows-Updates verfügbar sein können, meldet Ihr PC die Spracheinstellungen, den Product-Key, die Bios-Version und bereits installierte Updates.

Alles noch tolerabel, aber zusätzlich übermittelt das Active-X-Control auch die Guid-Nummer (Globally Unique Identifier) sowie die IP-Adresse. Bei der Guid handelt es sich um einen für jedes System eindeutigen Hex-Wert mit 32 Zeichen. Normalerweise kann dieser Wert zwar nicht direkt mit Ihnen als Person in Verbindung gebracht werden, unter bestimmten Bedingungen aber doch – wenn Sie Ihre Win-Installation registrieren (nicht nur aktivieren) oder einen Microsoft-Newsletter abonnieren. Technisch ist es dann kein Problem mehr, etwa beim Update übermittelte Daten auf individuelle Personen mit Namen und Adresse zurückzuführen.

Wir gehen davon aus, dass Microsoft derzeit von dieser technischen Möglichkeit keinen Gebrauch macht. Laut Microsoft dient es ferner nur statistischen Zwecken, dass die Update-Site die IP-Adressen mitprotokolliert. Dennoch halten wir eine Produkt-Registrierung für ebenso verzichtbar wie jedwede MS-Newsletter. -cl

3. MS-Downloads: Eindeutig zweideutig

Microsoft lässt nichts unversucht, um die schwarzen Kopier-Schafe aus der Windows-Gemeinde auszuschließen. Der neueste Streich heißt „Genuine Microsoft Windows" – eine derzeit noch optionale Gültigkeitsprüfung der Windows-Installation beim Besuch der Download-Site von Microsoft (www.microsoft.com/downloads). Wenn diese Kür irgendwann zur Pflicht wird und Ihr System diese Prüfung nicht besteht, bleibt der Download-Server für Sie geschlossen.

Wenn Sie heute etwa versuchen, den Media Player 10 herunterzuladen, wird Ihnen empfohlen, die Gültigkeitsprüfung durchzuführen. Dabei sendet Ihr PC ähnlich wie beim Update (▷ Punkt 2) Infos über System und Bios sowie die Produkt-ID. Anhand dieser Werte ermittelt der Algorithmus, ob Sie eine legale oder eine raubkopierte Windows-Version verwenden. Zusätzlich wird auch die eindeutige Guid wie beim Windows-Update übermittelt – das könnte die übermittelten Daten eindeutig zuordenbar machen.

Achtung! Die Guid wird auch dann vor dem Download gesendet, wenn Sie die als optional deklarierte Überprüfung Ihrer Windows-Installation ablehnen. -cl

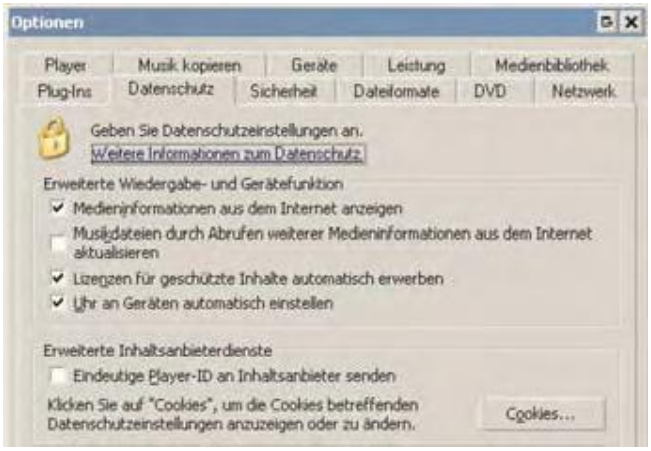
4. Media Player: Derzeit ruhig gestellt

Die Versionen 7 und 8 des Windows Media Players sind beim Einlegen von Audio-CDs recht gesprächig:

Gratis-Tools gegen Spionage

Tool	Preis	Win-Betriebssysteme	Internet (Download)	Sprache	Seite
Ad-Aware SE Personal 1.05	gratis*	98/ME, NT 4, 2000, XP	www.lavasoft.de (2,6 MB)	englisch	78
Ethereal 0.10.9	gratis	98/ME, NT 4, 2000, XP	www.ethereal.com (8,7 MB)	englisch	81
Filemon 6.12	gratis	2000, XP	www.sysinternals.com (92 KB)	englisch	81
Regmon 6.12	gratis	2000, XP	www.sysinternals.com (86 KB)	englisch	80
Winpcap 3.0	gratis	95/98/ME, NT 4, 2000, XP	http://winpcap.polito.it (431 KB)	englisch	81

auf CD und unter www.pcwelt.de * für private Nutzung



Stummer Player: Beim Media Player 9 und 10 ist das Übermitteln der „eindeutigen Player-ID" standardmäßig deaktiviert (Punkt 4)

Beim Anfordern der Titelinformationen im Internet (CDDB-Abfrage) schicken sie freigiebig die Guid des Systems an Microsoft. Die Versionen 9 und 10 halten sich in diesem Punkt zurück. Standardmäßig ermittelt der Player in den jüngsten Versionen bei allen nicht per DRM (Digital Rights Management) geschützten Medien nur noch die CDDB-Informationen anhand der unbedenklichen Medien-ID der eingelegten CD. Das Übermitteln der Guid ist weiterhin als Option vorgesehen („Extras, Optionen, Datenschutz, Eindeutige Player-ID an Inhaltsanbieter senden"), da manche Musikdienste diese Information verlangen. Im Normalfall besteht kein Grund, diese Option zu aktivieren. -cl

Internet-Software

Von Browser und Mailprogramm erwarten Sie, dass sie Daten mit dem Internet austauschen – das ist schließlich ihre Aufgabe. Das bedeutet aber nicht, dass Sie keinen Einfluss auf Art und Umfang dieser Daten nehmen sollten. Wenn Sie etwa in einem Formular Ihre richtige Mailadresse nicht preisgeben wollen, steht es Ihnen frei, eine gefälschte einzutragen – sofern Sie nicht auf eine Antwort angewiesen sind. Doch selbst Formulare können unsichtbare Felder enthalten, die ebenfalls übertragen werden.

Das ist nicht das einzige Beispiel: Ständig übertragen Sie Daten an einen Server, sei es die Passwort-Eingabe bei Ebay oder das Mailpasswort. Auch beim Versenden einer Mail wird Ihr Text unverschlüsselt übertragen und kann theoretisch an jeder Zwischenstation bis zum Empfänger gelesen werden.

5. Versteckte Informationen in Formularen

Wenn Sie die Felder eines Web-Formulars ausfüllen und es absenden, sind Sie darüber informiert, welche Daten Sie senden – sollte man denken. In Wirklichkeit enthalten solche Formulare oft versteckte Felder.

Ganz einfach können Sie das bei Google testen. Um die Formularfelder der Seite komplett zu sehen, benötigen Sie den Browser Firefox. Gehen Sie damit auf die Google-Startseite www.google.de, und geben Sie einen beliebigen Begriff in die Suchmaske ein, ohne die Abfrage zu senden. Rufen Sie nun aus dem Menü „Extras" den Punkt „Seiteninformationen" auf. Auf der Registerkarte „Formulare" sehen Sie in der oberen Maske alle Formulare, die auf der Seite enthalten sind. Bei Google ist das nur das Suchformular, das mit „f" benannt ist.

Formular unter der Lupe: Felder vom Typ „hidden" sind unsichtbar. Der Wert landet nach dem Senden dennoch beim Server (Punkt 5)

Browser-Geschwätz

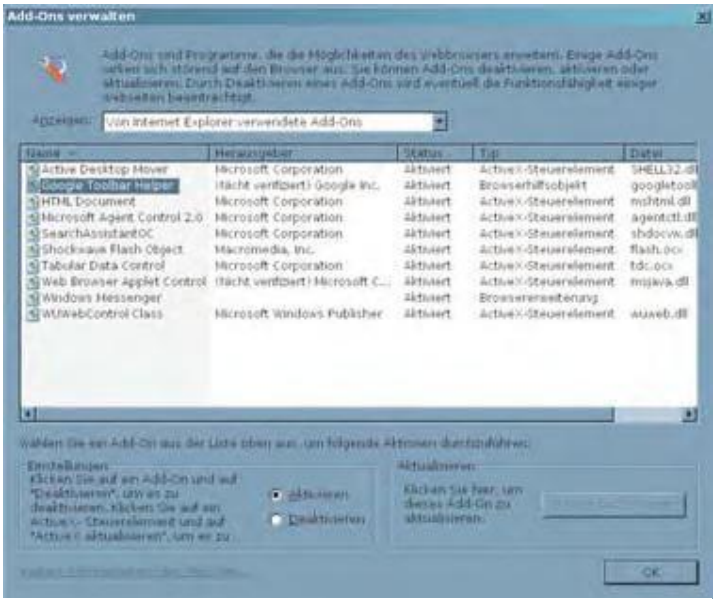
Wenn der Browser eine Web-Seite anfordert, beantwortet er als Gegenleistung einige Fragen des jeweiligen Servers. Hauptsächlich geht es um Name, Version, Plug-ins und Sprache des Browsers. Sind Sie nicht direkt, sondern per Link auf eine Seite gegangen, gibt der Browser außerdem preis, von welcher Seite er gerade kommt.

Erweiterungen und Add-ons

Erweiterungen und Add-ons sind kleine Programme, die nicht selbständig, sondern innerhalb Ihres Browsers laufen. Ihr Zweck ist es, dessen Funktionen zu erweitern. Allerdings ist der Mechanismus, über den sich Add-ons mit dem Browser verbinden, ein gutes Versteck für Malware. Den in der PC-WELT vorgestellten Erweiterungen und Add-ons können Sie jedoch trauen, wir empfehlen nichts ungetestet.

Spyware-Infektion

Spyware nistet sich bevorzugt in den Internet Explorer ein. Das heißt aber nicht zwangsläufig, dass sie auf diesem Weg auf den Rechner gekommen ist. Auch vom Anwender installierte Software kann den Parasiten mitbringen. Besonders vorsichtig müssen Sie bei Software für Tauschbörsen sein – hier gibt es mehr dubiose Quellen als seriöse Anbieter.



Browser-Add-ons: An sich sind sie zur Erweiterung der Möglichkeiten des IE gedacht, doch kann sich über sie auch Spyware einnisten (Punkt 6)

Wenn Sie es anklicken, erscheinen in der unteren Maske alle enthaltenen Felder. Eines ist als „hidden" (versteckt) gekennzeichnet. Es überträgt die Zeichenkette „de", was als harmlos einzustufen ist: Google ermittelt den Wert aus Ihren Einstellungen und verwendet ihn, um Ihnen die Ergebnisseite in deutscher Sprache zu präsentieren.
Was Sie außerdem sehen: Auch Radio Buttons (Optionsfelder, die Sie per Klick aktivieren) und Schaltflächen sind Formularfelder. Also senden Sie auch auf Web-Seiten, bei denen es keine ausfüllbaren Felder gibt, mit jeder Betätigung eines Buttons ein Formular ab. Mit der vorgestellten Methode können Sie auch dann, wenn Sie irgendwo zur schlichten Bestätigung mit „OK" aufgefordert werden, alle dabei versendeten Daten vorher überprüfen. -akr

6. Browser: Toolbars und Erweiterungen

Am Anfang war die Google Toolbar: Das praktische Tool zur Suchmaschine trug durch seine einfache Bedienung mit zur Beliebtheit von Google bei. Inzwischen gibt es über tausend Browser-Add-ons, die teilweise als Toolbar ausgeführt sind. Davon ist allerdings die überwiegende Mehrheit Spyware und übermittelt etwa, wenn Sie eine Suchmaschine bedienen, den Suchbegriff auch an einen Werbe-Server, der Sie gezielt mit Pop-ups versorgt. Spyware entfernen können Sie mit Tools wie **Ad-Aware** (auf CD). Es erkennt und entfernt schädliche Browser-Add-ons. Tipp: Die Professional-Version von Ad-Aware ist als Bestandteil der F-Secure Internet Security Suite auf CD.
Eine Gesamtübersicht über die installierten Add-ons bietet der Internet Explorer ab Windows XP SP 2. Im Menü „Extras" rufen Sie dazu den Punkt „Add-ons verwalten" auf. Unter „Anzeigen" können Sie zwischen allen verfügbaren und den momentan geladenen Add-ons wechseln. Es ist aber nicht möglich, über diese Dialogbox Add-ons zu de-installieren. Immerhin können Sie sie deaktivieren, falls Sie die manuelle Methode einem Tool wie Ad-Aware vorziehen. Setzen Sie in diesem Fall jedes Add-on, das Sie nicht kennen oder das Ihnen suspekt vorkommt, auf „Deaktivieren". Web-Detektive können auch mit den im

Personen-Daten zurückverfolgen

„Sehr geehrter Herr X. Sie haben 10.000 Euro gewonnen." Solche Anschreiben landen fast täglich in den Briefkästen. Unerwünschte Werbeschreiben sind schließlich nicht nur ein Computer-Phänomen, sondern auch in der realen Welt in unterschiedlichsten Formen anzutreffen. Wie die mehr oder weniger seriösen Anbieter zu Namen und Adressen kommen, bleibt ihr Geheimnis. Im Bereich zwischen Telefonbuch, professionellen Adressenhändlern und Mafia ist alles möglich. Wer freigiebig mit seinen Daten umgeht, ist besonders betroffen. Gewinnspiele, Versandhaus-Bestellungen und Kreditanfragen funktionieren nun einmal nicht, ohne dass der Interessent seine Anschrift hinterlässt. Dabei gibt es sicher vertrauenswürdige Anbieter, die ein fehlendes Kreuz vor „Meine Daten nicht Dritten zugänglich machen" ernst nehmen. Da Vertrauen zwar gut, Kontrolle aber bekanntlich besser ist, sollten Sie eine Möglichkeit einbauen, Datenmissbrauch aufzudecken. Das geht ganz einfach: Bestellungen oder Anfragen bei Firma A führen Sie als <Vorname> A. <Nachname>, bei Firma B. als <Vorname> B. <Nachname> durch. Beim Versand einer Ware bereitet das „gefälschte" Mittel-Initial in der Regel keine Probleme. Wenn Sie später eine Werbung erhalten, die an <Vorname> A. <Nachname> adressiert ist, wissen Sie, dass nur Firma A Ihre Adresse weitergegeben haben kann. Juristisch ist diese Information sicher nicht verwertbar. Aber eine Firma, die das Vertrauen des Kunden offensichtlich missbraucht hat, sollte für künftige Geschäfte nicht mehr in Frage kommen. -te

Abschnitt „Analyse“ (ab ▷ dieser Seite) beschriebenen Verfahren nach verdächtigen Aktivitäten scannen. Da es sich bei Spyware um Browser-Add-ons handelt, heißt das Programm, das gegen Ihren Willen Daten sendet, Iexplore.EXE – also der Internet Explorer. Unter allen Servern, die Iexplore.EXE kontaktiert, müssen Sie den herausfiltern, der nichts mit der aufgerufenen URL zu tun hat. Auf diese Weise bekommen Sie entweder den Finanzierer von Spyware vor die Flinte oder unschuldige, aber verseuchte Spam-Schleudern.

Firefox? Für diesen Browser sind derzeit noch keine Erweiterungen bekannt, die Spyware enthalten. Technisch möglich sind sie jedoch, und damit nur eine Frage der Verbreitung und Zeit. -akr

7. Unverschlüsselte Mailpasswörter

Die meisten Mailanbieter akzeptieren sowohl die verschlüsselte als auch eine unverschlüsselte Anmeldung am Konto. Vor letzterer sei dringend gewarnt: Das Passwort senden Sie zwar eigentlich nur zum Provider, ein böswilliger Kollege oder Mitbewohner kann es jedoch abfangen – die Überwachung des Netzwerkverkehrs (▷ Punkt 11) funktioniert auch im LAN. Da der Lauscher nicht nur das Passwort erfährt, sondern nebenbei auch Benutzernamen und Server, kann er so Ihr Mailkonto benutzen und missbrauchen.

Übertragen Sie deshalb beim Senden und Empfangen das Passwort stets verschlüsselt. In Outlook Express beispielsweise gehen Sie dazu auf „Extras, Konten“, wählen für jedes eingerichtete Konto den Punkt „Eigenschaften“ und aktivieren jeweils auf der Registerkarte „Erweitert“ die Option „Dieser Server erfordert eine sichere Verbindung (SSL)“. Gängige Mailprogramme bieten vergleichbare Optionen.

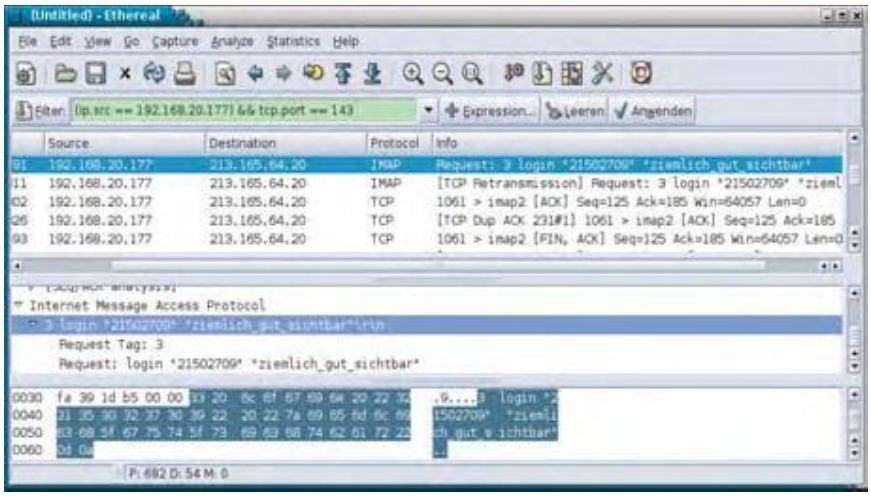
Das Gleiche gilt für Web-Formulare (▷ Punkt 5): Wann immer Ihnen die Wahlmöglichkeit angeboten wird, geben Sie das Passwort für eine anmeldepflichtige Seite nur ein, wenn Sie über SSL (▷ Seite 80) mit ihr verbunden sind. Sie erkennen das an einem gelben Vorhängeschloss in der Statusleiste des Browsers. -akr

Analyse

Updates, Aktivierung, Registrierung, digitale Rechte, Spyware … schon heute treibt sich zu viel auf dem PC herum, was Ihre Daten ins Web befördern will. Was dabei jeweils genau geschieht, bleibt dem Anwender verborgen. Es gibt jedoch Mittel und Wege, herauszufinden, welche Software Daten sendet, wofür sie sich interessiert und wie viel sie tatsächlich weiß. Denn: Mehr als sie weiß, kann sie nicht senden. Dadurch lassen sich Spione enttarnen.

8. Diese Anwendungen nutzen das Internet

Welche Programme die Internet-Verbindung zum Übertragen von Daten nutzen, stellen Sie am besten mit Hilfe einer Personal Firewall fest, etwa McAfee Firewall (auf der CD zur PC-WELT 3/2005). Beim



Den Nachbarn belauscht: Ein unverschlüsselt übertragenes Mailpasswort ist leicht abzufangen. Dasselbe gilt für den zugehörigen Benutzernamen (Punkt 7)

Der Nutzen von SSL

SSL ist nicht nur für die verschlüsselte Übertragung gut, sondern erlaubt, über das Server-Zertifikat auch die Identität des Servers zu überprüfen. Klicken Sie deshalb eine Zertifikatswarnung nie einfach weg, sondern lesen Sie sie genau durch. Sind Sie nicht sicher, ob Sie mit dem richtigen Server verbunden sind, brechen Sie die Aktion lieber ab.

Mail ist immer lesbar

Auch bei einer verschlüsselten Verbindung zum Mailserver wird der eigentliche Text einer Mail immer im Klartext übertragen. Das bedeutet, dass man ihn an jeder Zwischenstation bis hin zum Empfänger abfangen kann. Eine Mail sollte deshalb nur Informationen enthalten, die Sie auch auf eine Postkarte schreiben würden. Andernfalls verschlüsseln Sie besser die Mail selbst, etwa mit PGP.

Schnüffler

Netzwerk-Schnüffel-Programme wie Ethereal stellen Daten aus Netzwerkpaketen für Menschen lesbar dar. Ein großer Teil der Daten, die über die Leitung gehen, dient jedoch nur dazu, die Verbindung zu verwalten. So müssen sich beispielsweise Webserver und Web-Browser erst einmal auf die passende Art der Kommunikation einigen. Das Aufspüren einer bestimmten Übertragung erfordert daher Geduld und Zeit.

Blockade: Firewalls sperren bei Bedarf den Internet-Zugriff (Punkt 8)

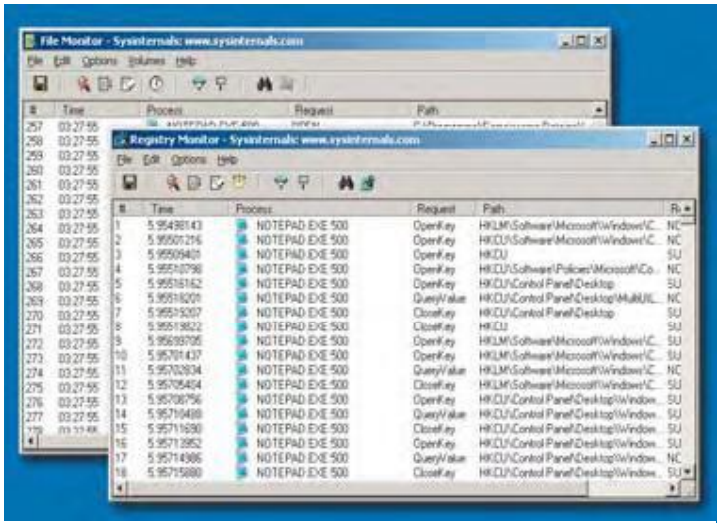
Start einer Internet-Anwendung meldet sich die Firewall, und Sie erlauben dann dem Programm den Zugriff oder blockieren ihn.
Einige Firewalls fragen jedoch nicht bei jedem Programm nach. McAfee Personal Firewall etwa durchsucht eine Online-Datenbank mit bekannten Anwendungen und lässt diese automatisch zu. Wenn Sie konsequent bei jeder Anwendung gefragt werden möchten, gehen Sie auf „Datei, Einstellungen“ und die Registerkarte „Warneinstellungen“. Wählen Sie unter „Empfehlungen“ den Wert „Empfehlungen nicht verwenden“. -te

9. Was geht tatsächlich über die Leitung?

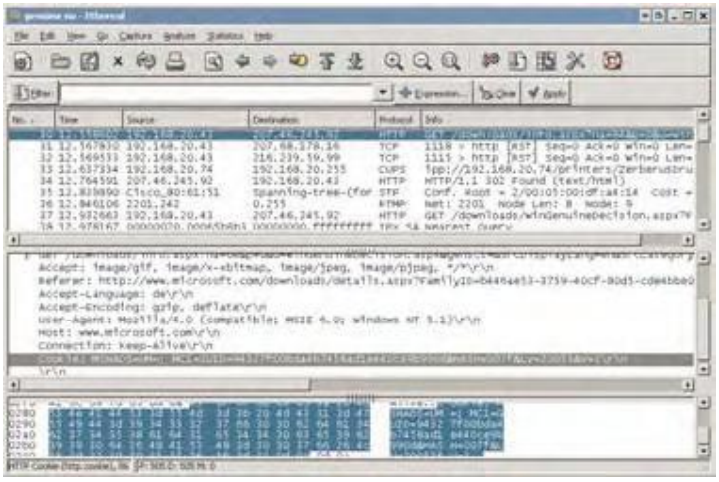
Wofür eine Software das Internet nutzt und was sie dabei überträgt, ist nicht ganz einfach zu analysieren. Die direkte Methode ist das Mitschneiden der gesendeten Daten (▷ Punkt 11). Dabei fallen jedoch große Datenmengen an, die sich nur sehr schwer analysieren lassen. Wenn die Daten verschlüsselt sind, können Sie letztlich nichts erkennen. Sie erfahren damit aber auf jeden Fall, welche Datenmenge ein Programm an welchen Server schickt. Geht es beispielsweise nur um wenige hundert Byte, sendet das Programm sicher keine komplette Liste der installierten Soft- und Hardware Ihres Rechners. Wenn das Programm nicht nur den Server des Herstellers, sondern zusätzlich Server von Fremdanbietern kontaktiert, ist das ein Indiz für eine mögliche Spionagetätigkeit.
Eine indirekte Methode, Programmaktivitäten zu überwachen, ist die Aufzeichnung aller Datei- und Registry-Zugriffe (▷ Punkt 10). Darüber lässt sich genau ermitteln, für welche Informationen sich ein Programm interessiert. So ist es beispielsweise verdächtig, wenn ein Add-on, das nur zum Optimieren des Internet Explorers gedacht ist, in der Registry den Zweig „Hkey_ Local_Machine\Software\Microsoft\Office“ ausliest. Bei einem Tool für Microsoft Office dagegen wäre dieser Vorgang nicht ungewöhnlich. -te

10. Zugriffe auf Registry & Dateien aufzeichnen

Eine Firewall kann zwischen schädlichen und nützlichen Internet-Zugriffen nicht unterscheiden. Eine potenzielle Spionage-Aktion blockiert sie genauso wie die Prüfung auf Updates. Wenn Sie eine bestimmte Anwendung im Verdacht haben, dass sie unerlaubt Daten von der Festplatte liest, müssen Sie den Vorgang selbst untersuchen.
1. Registry-Zugriffe protokollieren Sie mit **Regmon 6.12** (auf CD). Das Programm benötigt keine Installation. Entpacken Sie es einfach in einen beliebigen Ordner, und starten Sie es – die Protokollierung beginnt sofort. Da System und Anwendungen ständig auf die Registry zugreifen, füllt sich das Fenster aber schnell mit nutzlosen Informationen. Klicken Sie daher in der Symbolleiste auf das Icon „Capture“, oder betätigen Sie <Strg>-<E>. Klicken Sie auf das Icon „Clear“, um die Anzeige zu löschen.
Gehen Sie dann auf das Icon „Filter/Highlight“ (oder <Strg>-<L>), und tragen Sie unter „Include“ den Namen des zu analysierenden Programms ein. Regmon richtet sich nach dem Namen der ausführbaren Datei. Heißt eine Software beispielsweise Foobar.EXE, genügt die Eingabe von „foobar“. Groß- und Kleinschreibung spielt keine Rolle. Unter „Highlight“ können Sie zusätzlich ein Filterkriterium eingeben, etwa den Namen eines Registry-Zweigs. Wenn dieser in der Liste auftaucht, färbt Regmon die Zeile rot ein. Klicken Sie zum Abschluss auf „OK“, und beginnen Sie die Aufzeichnung mit <Strg>-<E>. Starten Sie das Programm, das Sie überwachen wollen. Die Registry-Zugriffe erscheinen in der Liste. Bei Bedarf speichern Sie die Liste über „File, Save“ in einer Logdatei, die Sie in einem Editor öffnen und besser durchsuchen können.



Detektivarbeit: Mit Regmon und Filemon (beide auf CD) ermitteln Sie, auf welche Registry-Zweige und Dateien ein Programm zugreift (Punkt 10)



Leitung abhören: Mit Ethereal (auf CD) kontrollieren Sie den Netzwerkehr. Ist dieser verschlüsselt, sehen Sie nur Datenmüll (Punkt 11)

2. Dateizugriffe analysieren Sie mit **Filemon 6.12** (auf CD). Auch dieses Tool müssen Sie nur in ein beliebiges Verzeichnis entpacken, dann starten Sie Filemon.EXE. Die Bedienung ähnelt der von Regmon. Auch hier stoppen Sie die Protokollierung mit der Tastenkombination <Strg>-<E>. Rufen Sie dann den Filter-Dialog mit <Strg>-<L> auf, und geben Sie unter „Include" den Programmnamen ein. Der Wert unter „Highlight" dient wieder der Hervorhebung eines Suchbegriffs. Schließen Sie den Dialog, drücken Sie <Strg>-<E>, und starten Sie die zu prüfende Anwendung. -te

11. Netzwerkverkehr komplett überwachen

Das Protokollieren von Netzwerkverbindungen mit dem kostenlosen Tool **Ethereal 0.10.9** (auf CD) funktioniert unter Windows XP bisher nur mit Geräten, die sich wie Netzwerkkarten verhalten: PCI-Ethernet-Karten (DSL-Anschluss), Wireless-LAN-Karten oder auch externe Netzwerkadapter. Mit Modems arbeitet das Programm nicht zusammen. Unter Windows 98 oder Windows ME gibt es diese Einschränkung nicht.

Ethereal benötigt den kostenlosen Treiber **Winpcap 3.0** (auf CD). Ethereal und Winpcap lassen sich beide problemlos per Setup-Programm installieren. Da Ethereal aus der Linux-Welt stammt, sehen die Menüs etwas anders aus, als bei Windows-Programmen üblich. Sie starten die Protokollierung über das Menü mit „Capture, Start". Im folgenden Dialog stellen Sie in der Auswahl unter „Interface" Ihre Netzwerkkarte ein.

Wenn Sie per Modem oder ISDN online gehen, wählen Sie „PPP-Adapter" (nur Windows 98/ME). Sollten zwei PPP-Adapter in der Liste auftauchen und Ethereal mit keinem von beiden funktionieren, müssen Sie unter „Systemsteuerung, Netzwerk" den „DFÜ-Adapter#2" entfernen – in aller Regel benötigen Sie auch nur einen „DFÜ-Adapter"-Eintrag. Dann sollte Ethereal problemlos arbeiten und im Hauptfenster alle Datenpakete anzeigen, die über Ihre Leitung gehen.

Ethereal zeigt standardmäßig alle Daten, die Ihren Rechner verlassen und ihn erreichen. Daher sollten Sie zur besseren Übersicht sämtliche Internet-Programme beenden und nur jene Anwendung laufen lassen, die Sie analysieren möchten. Um aus den Daten die relevanten Informationen herauszufischen, sind allerdings detektivischer Spürsinn und reichlich Geduld gefordert. -te

Winpcap

Winpcap ist ein kostenloser Treiber, den viele Netzwerkanalyse-Programme verwenden. Er klemmt sich zwischen Anwendung und Netzwerkkarten-Treiber und belauscht dabei den vorbeifließenden Netzwerkverkehr. Die Anwendung bekommt davon nichts mit, und die Netzwerkleistung verringert sich auch nicht merklich.

Da Windows ein Modem als virtuellen Netzwerk-Adapter behandelt (PPP-Verbindung), ist auch hier das Protokollieren der Daten möglich. Mit der aktuellen Treiberversion 3.0 (auf CD) klappt das bisher nur unter Windows 95/98/ME. In der Version 3.1 Beta ist eine experimentelle Unterstützung für PPP-Verbindungen auch unter Windows 2000/XP/2003 enthalten. Diese Version arbeitete bei unseren Versuchen allerdings nicht problemlos mit der Ethereal-Version 0.10.9 zusammen.