

PC PROFESSIONELL

DM 8,50/€ 4,35 10/2001

Mit
CD

Belgien: bfr 205,-/€ 5,08
 Italien: Lit 12.000/€ 6,20
 Niederlande: hfl 10,75/€ 4,88
 Spanien: Pts 1.000,-/€ 5,01
 Schweiz: CHF 8,50

Griechenland: Dr 2.100,-/€ 6,16
 Luxemburg: lfr 205,-/€ 5,08
 Österreich: ATS 67,-/€ 4,87

VOLLVERSION

Ontrack System Suite

Version 2000

GRATIS
auf CD



- Sytem-Tuning
- Crash-Protection
- Virenschutz
- Uninstaller, u.v.m.

* kostenlose Registrierung nötig



► s. 198

SMS mit dem Palm! ➔ s. 104

- Mit PDA und Handy günstig ins Internet
- 20 PDAs im Test



4-Megapixel-Digicam ➔ s. 228

Digicam
von Sony
zu gewinnen!



Express-Hilfe bei PC-Crash

Profi-Tricks
EXKLUSIV

So decken Sie Hardware-Fehler schnell auf
Die besten Tricks gegen Ärger mit dem PC

Boom: Flüster-PC ➔ s. 66

Lärmstopp für Lüfter, Festplatten & Co
Test: 10 superleise PCs im Soundlabor

Achtung, Web-Spione!

Abwehr-
Software
auf CD!

► s. 132

So schützen Sie Ihre vertraulichen Daten
6 Anonymizer-Programme
im großen Labor-Test



4 391164 608505

10

Mit Tarnkappe

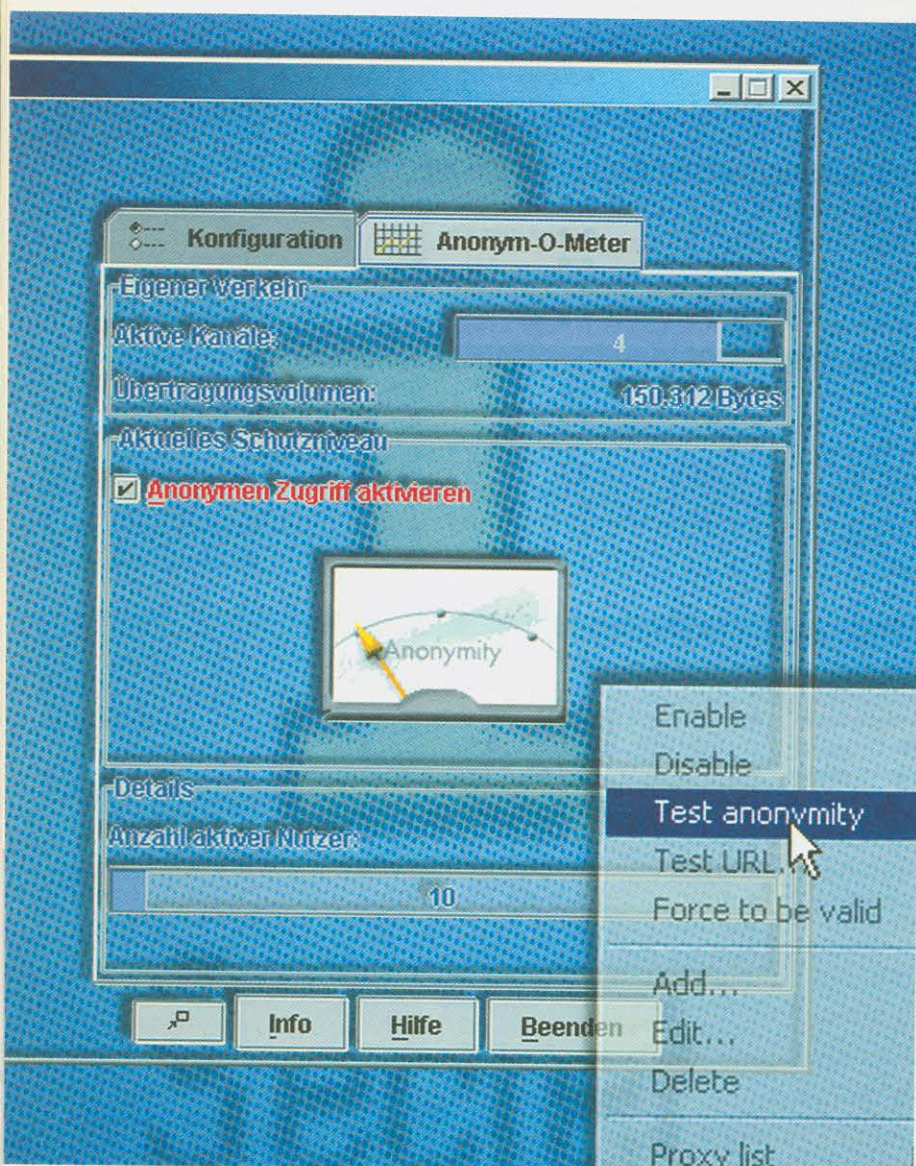
Anonymizer-Software wirbt mit absoluter Anonymität beim Websurfen »durch top-geheime Technik«. Der PCpro-Test zeigt, dass die Browser-Tools zwar effektiv vor Spam und Cookies schützen, aber auch eine Sicherheit versprechen, die es so im Internet nicht gibt.

Olaf Pursche, Marco Zierl

Wer sich im Netz bewegt, hinterlässt immer Spuren, wie die IP-Adresse des eingeloggtten Rechners, eventuell die E-Mail-Adresse und viele andere Daten. Neben lästigem Spam ermöglichen diese Datenspuren Social Hacking, also das gezielte Suchen nach Äußerungen in News-Foren oder dem Erkunden des Surf-Verhaltens einer bestimmten Person – beispielsweise vom zukünftigen IT-Arbeitgeber in Auftrag gegebene Ermittlungen vor einer Einstellung. Hier sollen die im Test vertretenen Programme dem Surfer Anonymität verschaffen. Auf den Hersteller-Homepages versprechen sie das spurlose Surfen im Web und den Schutz vor Späh-Attacken. Im PCpro-Labor zeigen sich aber große Unterschiede zwischen den Persönlichkeitsschützern. Wirkliche Datensicherheit bieten letztlich nur zwei der fünf Kandidaten, Freedom 2.2 (www.freedom.net) von Zero Knowledge und Stealther 2.6 von Photonon (www.stealther.de). Drei von fünf Produkten im Test gewährleiten diese Sicherheit nicht in zufrieden stellendem Maße, da sie die IP-Adresse des Users preisgeben.

Kritiker und Datenschützer diskutieren derzeit heftig über staatliche Maßnahmen. Diese stellen für sie Einschränkungen der informationellen Selbstbestimmung dar. Genannt werden in diesem Zusammenhang häufig Gesetze wie die Telekommunikationsüberwachungsverordnung (TKÜV) oder andere Erlasse. So forderten die Innenminister des Bundes und der Länder im November vergangenen Jahres zum Zweck der Strafverfolgung für Provider und Betreiber von Servern eine Protokollierungspflicht. Erfasst werden dabei die IP-Adresse sowie deren Nutzungszeitraum, also das komplette Surf-Verhalten. Die Provider sollen diese Daten eine gewisse Zeit speichern. Dabei ist jeder überwachbar, der sich im Internet bewegt. Ausführliche Informationen zu diesem Thema geben beispielsweise das Bundeswirtschafts- und -Innenministerium unter www.sicherheit-im-internet.de oder das virtuelle Datenschutzbüro (www.datenschutz.de).

Auch Firmen arbeiten an Nutzerprofilen, um Werbung gezielt an den Kunden zu bringen, Surfer länger auf der Homepage zu halten oder die gewonnenen Daten zu verkaufen. Anonymizer sind daher nicht nur etwas für Straftäter und Paranoiker. Sie sind für alle interessant, die nicht mit Spam überschüttet werden oder ihr Recht auf Datenschutz durchsetzen wollen.



durchs Netz

Geschwätzige Browser

Ein Browser kann nur Daten empfangen, wenn er Informationen herausgibt. Dazu gehört generell die IP-Adresse, zu der die angeforderten Daten geschickt werden sollen. Häufig stehen diese Fenster zum Internet allerdings sperrangelweit offen und geben wesentlich mehr Informationen über ihre Nutzer heraus, als zum Surfen wirklich notwendig wäre.

Der Browser verrät regelmäßig die Art und Version der genutzten Internet-Zugangssoftware, das Betriebssystem, auf dem diese arbeitet, die zuletzt besuchte Website, die Monitorauflösung und die Einstellungen bezüglich Java und Javascript sowie die VB-Script-Einstellung des Browsers. Darüber hinaus übermittelt er die IP-Adresse, die im harmlosesten Fall Informationen über den Internet-Provider enthält. Auch temporäre Dateien wie der Cache und die komplette Browser-History können so ganz leicht ausgelesen werden.

Profiling für jedermann

Schlimmstenfalls ist es möglich, durch eine Who-is-Abfrage beim Internet Service Provider Telefonnummer, den Benutzernamen und weitere personenbezogene Daten des Registrierten zu erhalten – nämlich dann, wenn beim Surfen eine auf den Surfer registrierte Domain preisgegeben wird, was beim normalen Internet-Anwender jedoch eine höchst seltene Konstellation sein dürfte. Hat der Anwender seine E-Mail-Adresse in den Browser eingetragen, wird auch diese bei Anfragen automatisch angegeben. Allerdings lässt sie sich auch problemlos über Adress-Suchmaschinen, wie beispielsweise den Meat-E-Mail-Search-Agent der Universität Hannover (<http://mesa.rzrn.uni-hannover.de>), herausfinden.

Ansatzpunkt Browser

Im PCpro-Test werden sechs Programme unter die Lupe genommen, die laut Herstelleraussage ein sicheres Surfen erlauben. So bewirbt Photono seinen Anonymizer Stealthther auf der Homepage (www.stealthther.de) als »top-geheime Technik, welche höchstwahrscheinlich auch der weltbekannte Hacker Kevin Mitnick (www.kevinmitnick.com) sowie der israelische Geheimdienst nutzt.« Zumindest was Mitnick angeht, ist das allerdings recht unwahrscheinlich – er sitzt nämlich derzeit im Gefängnis.

Anonym bewegen Surfer sich im Internet dann, wenn zwei Tatsachen gegeben sind: Zuerst

müssen die eigene IP-Adresse sowie Host- und Rechnername maskiert werden. Sonst kann im Server-Log der angeforderten Webseite gesehen werden, wer von wo und wann welche Seite mit welchen Parametern aufgerufen hat.

Als zweiter Punkt müssen alle Daten, die den Rechner verlassen, verschlüsselt gesendet werden. Nur so kann jeder sicher sein, dass im Netzwerk, beim ISP oder auf dem Weg durch das Internet die Daten nicht doch abgefangen und gelesen werden.

Zusätzlich sollte der Datenverkehr über mindestens drei Punkte verlaufen, sodass der mittlere Rechner keine Verbindung mit dem Client oder dem Zielrechner hatte. Im Testfeld bietet der Testsieger Freedom 2.2 durch das firmeneigene Freedom Network dieses hohe Sicherheitsniveau. Dabei ist die absolute Wahrung der Identität allerdings abhängig vom Hersteller Zero Knowledge – der im Übrigen selbst Name, Adresse, E-Mail, Telefonnummer und Kreditkartennummer des Kunden sehen will. Sollte Zero Knowledge diese Daten herausgeben und werden zusätzlich Partnerfirmen zur Herausgabe der Logdateien und der verschlüsselten Daten gezwungen, dann ist eine Dekodierung der Daten wieder möglich, wenn auch nur mit extrem hohem Aufwand. Trotzdem bleibt das Restrisiko, denn dieser letzte Schwachpunkt bleibt in jedem Fall bestehen.

OPU

INHALT

Produkt (Hersteller)

- 134** Anonymity 2.52 (Inetprivacy)
- 136** Freedom 2.2 (Zero Knowledge)
- 136** Multiproxy 1.2 (Mike Mishkin)
- 136** Secretmaker 1.62 (Secretmaker)
- 137** Stealthther 2.6 (Photono Software)

133 Empfehlung

133 Gesamtwertung

134 Einzelwertung

137 Außer Konkurrenz:

Java Anon Proxy (TU Dresden)

137 Tipps & Tricks: Installationshilfe

138 Alternativen: Unsichtbar ohne Software

142 Laboregebnisse

143 Lab Notes

143 Ausstattung

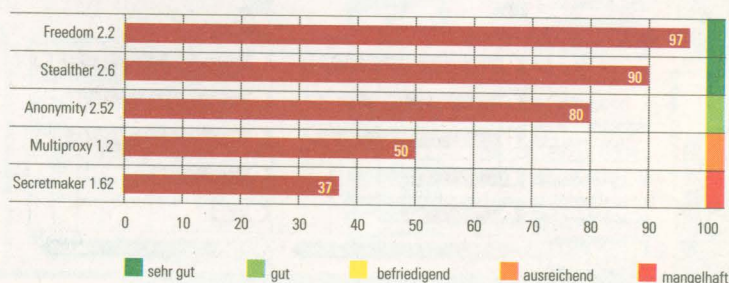
EMPFEHLUNG



Freedom 2.2

Bestes Programm im Test ist Freedom 2.2 von der Firma Zero Knowledge. Neben der einfachen Installation und der übersichtlichen Bedienung überzeugen hier die umfangreichen Sicherheitsfunktionen, mit mehreren konfigurierbaren Identitäten. Weitere Features sind Cookie-Manager, Personal Firewall und E-Mail-Verschlüsselung, um jedes Sicherheitsrisiko auszuschließen. Der wichtigste Pluspunkt ist die komplette Verschlüsselung aller ausgehenden Daten. Freedom gewährleistet dies über unabhängige Server im eigenen Netzwerk. Durch 128-Bit-Verschlüsselung über ausgewählte Server bietet Freedom ein sehr hohes Maß an Anonymität.

GESAMTWERTUNG



EINZELWERTUNG

So bewertet PCpro

PCpro vergleicht im Labortest fünf Produkte zum anonymen Surfen in den Bereichen Sicherheit, Bedienung und Funktionsumfang. Es treten alle Produkte an, die als Anonymizer gehandelt werden beziehungsweise zum Download bereitstehen. Der Test von Java Anon Proxy findet außer Konkurrenz und ohne Wertung statt, da er auf einer Proxy-Mixed-Kaskade basiert, die sich noch in der Entwicklung befindet.

Sicherheit

Mit 60 Prozent wird die Sicherheit und Anonymität, die die Produkte dem User bieten, am höchsten gewichtet. Die Sicherheit des Produkts erstreckt sich auf die Bereiche Variablen-Maskierung, Blockieren von Cookies und Verschlüsselung von eingehenden und ausgehenden Daten. Volle Punktzahl gibt es nur, wenn alle Cookies geblockt werden und alle sensiblen Variablen wie IP-Adresse und Host-Name während des Surfers im Web nicht weitergegeben werden. Bei Programmen, die eine Verbindung über einen oder mehrere unterschiedliche anonyme Proxy-Server pro Session herstellen, ist ein ausführlicher Test auf Anonymität der eingetragenen Server besonders wichtig. Weiterhin müssen für die volle Punktzahl alle Daten auch verschlüsselt übertragen werden können. Standard ist hier eine 128-Bit-

Verschlüsselung. Die höchste Sicherheit bieten dabei Produkte, die eine verschlüsselte Verbindung über mehrere unabhängige Server herstellen.

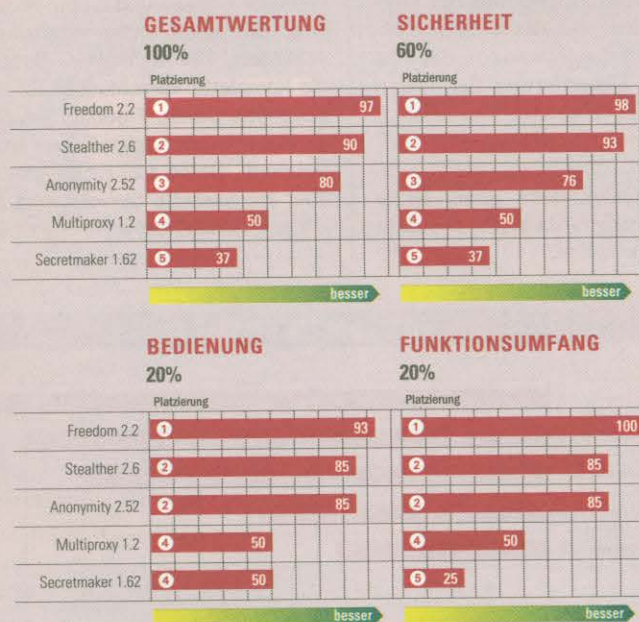
Bedienung

Die Bedienung der Programme wird mit 20 Prozent berücksichtigt. Neben einer einfachen Installation kommt es auf eine leichte Einrichtung und eine übersichtliche Benutzeroberfläche an. Falls eine Änderung in den Proxy-Einstellungen des Browsers notwendig ist, sollen die Produkte an einer zentralen Stelle darauf hinweisen und den notwendigen Port und die Adresse anzeigen. Weiterhin ist eine zentrale Funktion zum An- und Abschalten der Anonymisierung wichtig – sonst muss der Benutzer jedes Mal die Browser-Einstellungen verändern, wenn er keinen Proxy verwenden möchte. Pluspunkte gibt es für eine ausführliche lokale Hilfe.

Funktionsumfang

Der Funktionsumfang macht 20 Prozent der Gesamtwertung aus. Hier untersuchen die PCpro-Tester, welche zusätzlichen Funktionen zur Sicherheit und Anonymität im Internet zur Verfügung stehen. Punkte gibt es beispielsweise für komfortable Cookie- und Proxy-Manager sowie für alle Features, die zu zusätzlicher Sicherheit oder besserer Bedienbarkeit der Produkte beitragen.

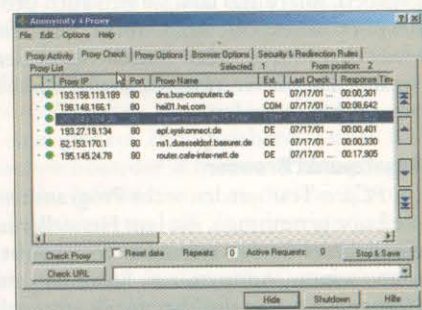
Marco Zierl/OPU



INETPRIVACY

Anonymity 2.52

Anonyme Proxies verwaltet das Programm von Inetprivacy (www.inetprivacy.com). Nach der Installation muss ein lokaler Proxy auf Port 80 liegen, damit dieser zum Verbindungsaufbau genutzt werden kann. Die eingetragenen Proxy-Server lassen sich dann unter den verschiedensten Kriterien auswählen. So ist es möglich, Proxies auszuschließen, die bestimmte HTTP-Variablen verwenden und weiterleiten. Inetprivacy liefert einen gut zu bedienenden Anonymisierer, der im Test befriedigende Sicherheitswerte aufweist. Dafür versieht ihn der Hersteller mit zahlreichen Zusatz-Features. Die Software unterstützt die Übertragungsprotokolle HTTPS und FTP. Jedoch ist es schwierig, Proxies zu finden, die FTP und HTTPS zur Verfügung stellen. Alle Proxies lassen sich auf Verfügbarkeit, Anonymität und Geschwindigkeit testen. Ausgewählte Server werden in eine Favoriten-Liste aufgenommen und in der System-Tray direkt angewählt. Die Software wählt bei jeder Verbindung automatisch einen neuen Server an. Anonymity 2.52 bietet eine Liste mit Hunderten von Proxy-Servern und kann das Verzeichnis automatisch überprüfen. Eigene Einträge sind zudem importierbar. In einem eigenen Fenster werden die gesendeten Browser-Requests mit den übertragenen HTTP-Variablen angezeigt. Ein weiteres Fenster zeigt die ein- und ausgehenden Verbindungen. Cookies werden global blockiert, eine Möglichkeit, bestimmte Cookies oder Domains durchzulassen, besteht nicht. Sämtliche ausgehenden Browser-Variablen können manipuliert und ersetzt werden.



Anonymity 2.52 bietet die umfangreichsten Proxy-Optionen im Testfeld.

Sicherheit (60%)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Bedienung (20%)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Funktionsumfang (20%)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Gesamturteil	GUT				



Freedom 2.2 erlaubt das Anlegen unterschiedlicher anonymer Identitäten.

ZERO KNOWLEDGE

Freedom 2.2

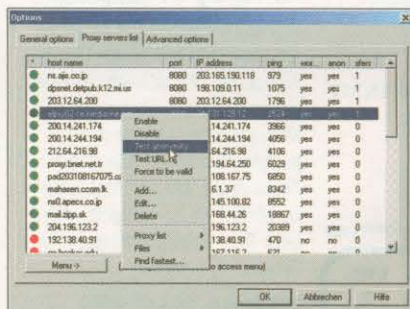
Um eine komplette Internet-Sicherheits-Suite handelt es sich im Gegensatz zum übrigen Testfeld bei Freedom 2.2. Das anonyme Surfen ist nur ein Nebenaspekt des Sicherheitskonzepts. Hier reiht sich ein sinnvolles Feature an das nächste. Das sehr gute Sicherheitsangebot wird durch eine gute Bedienbarkeit aufgewertet. Freedom unterstützt alle wichtigen Protokolle und Standards, neben HTTP und FTP auch Telnet, Gopher und IRC. Zusätzlich bietet die Suite eine Personal Firewall, E-Mail-Verschlüsselung, automatisches Stoppen von Spam und Bannern über eine Liste von Ad-Servern. Der Manager ermöglicht das Blockieren, Durchlassen und selektierte Löschen von Cookies. Der integrierte Keyword-Manager meldet sich automatisch, wenn bestimmte Schlüsselwörter – beispielsweise Nachname oder E-Mail-Adresse – verschickt werden sollen. Außerdem bietet ein Monitor-Screen die Überwachung aller Verbindungen. Der gesamte Datenverkehr erfolgt 128-Bit-verschlüsselt über Server des Freedom-Networks. Der Benutzer kann die Route festlegen und bis zu drei unterschiedliche Server hintereinander schalten. Da Freedom infolgedessen alle Pakete nun dreifach verschlüsselt und jeder Server so nur die ihm zugewiesene Verschlüsselungsschicht entschlüsseln kann, wird ein Höchstmaß an Sicherheit erreicht. Die Hälfte der Server wird dabei von Zero Knowledge (www.freedom.net) selbst betrieben. Die restlichen Server pflegen offizielle Partner des Herstellers.

Sicherheit (60%)	■ ■ ■ ■ ■
Bedienung (20%)	■ ■ ■ ■ ■
Funktionsumfang (20%)	■ ■ ■ ■ ■
Gesamterteil	SEHR GUT

MIKE MISHKIN

Multiproxy 1.2

Multiproxy ist ein Tool zur Verbindung mit anonymen Proxy-Servern. Lokal trägt es sich nach Installation als Proxy-Server im Browser ein. Der Port ist frei wählbar. Hier hören die guten Features dann allerdings auf. Im Lieferumfang ist keine aktuelle Proxy-Liste enthalten, sodass zuerst die Herstellerseite (www.multiproxy.org) zu besuchen ist. Dort muss der User sich umständlich eine Liste mit anonymen Proxies von Hand aus der Webseite kopieren, im Texteditor speichern und dann in den Multiproxy laden. Doch gerade die Hersteller-Homepage gehört mit zahlreichen Werbeeinblendungen und Cookies zu den Seiten, wegen denen Surfer Anonymisierungs-Software einsetzen sollten. Anschließend ist die Proxy-Liste auf Verfügbarkeit, Geschwindigkeit und Anonymität zu prüfen. Die Einträge lassen sich komfortabel verwalten und überprüfen. Über den Export der überprüften Liste lassen sich aktuelle Verzeichnisse erzeugen und weitergeben. Multiproxy kann lediglich Proxy-Server verwalten und ansprechen. Das Blockieren von Cookies oder die Veränderung von Browser-Variablen ist nicht möglich. Das ist für auf Anonymität bedachte User nicht akzeptabel. Allerdings wird das Programm auch nicht als reines Sicherheits-Tool beworben. Die Möglichkeit, ausschließlich anonyme Proxy-Server anzuwählen, ist nur ein Feature, das für Anonymisierung sorgt. Die Auswahl des Proxy-Servers kann entweder zufällig oder nach Reaktionszeit erfolgen. Zusätzlich kann der Server in eingestellten Sekundenintervallen automatisch wechseln.



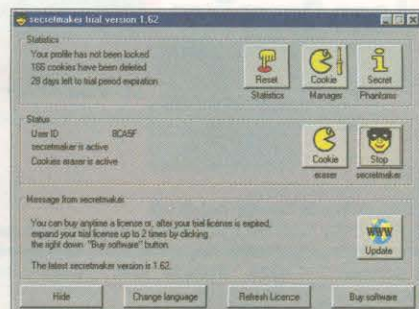
In der Proxy-Liste testet Multiproxy die Server automatisch auf Anonymität.

Sicherheit (60%)	■ ■ ■ ■ ■
Bedienung (20%)	■ ■ ■ ■ ■
Funktionsumfang (20%)	■ ■ ■ ■ ■
Gesamterteil	AUSREICHEND

SECRETMAKER

Secretmaker 1.62

»Innovative Software-Lösungen«, mit denen Anwender sich »unbeschwert im Internet bewegen können«, verspricht Secretmaker auf seiner Homepage (www.secretmaker.com). Der PC-Pro-Test zeigt jedoch: Das genaue Gegenteil ist der Fall, denn die Software gewährleistet die Sicherheit des Surfers nur mangelhaft. Nach Installation, Schlüsselanforderung und dem obligatorischen Re-Boot startet das Programm automatisch in der System-Tray. Secretmaker dagegen maskiert die HTTP-Variablen mithilfe so genannter Phantome und gibt ihnen neue, nichts sagende Namen, die keine Rückschlüsse zulassen. Im Test zeigt sich, dass dabei unter anderem Domain- und Host-Name maskiert werden, nicht aber die IP-Adresse des Benutzers. Damit ist für die Sicherheit des Surfers nichts gewonnen. Die Phantom-Tabelle erweckt nur den Anschein, als könnten noch Einträge hinzugefügt werden, an der Weitergabe der eigenen IP-Adresse lässt sich allerdings nichts ändern. Cookies blockt Secretmaker dagegen mit einem eigenen Cookie Eraser sauber ab. Der Benutzer kann hier in einem komfortablen Manager einzelne Cookies auswählen, die nicht geblockt werden sollen. Die restlichen Einträge löscht Secretmaker temporär. Es fehlen in dem Programm sowohl Hilfe, Installationsroutine als auch Informationen über den Hersteller. Die Homepage hält nur eine E-Mail-Adresse als einzigen Kontakt bereit. Über die Funktionsweise des Programms gibt eine PDF-Datei auf der Webseite Auskunft, die allerdings durch das Fehlen von technischen Informationen negativ auffällt.



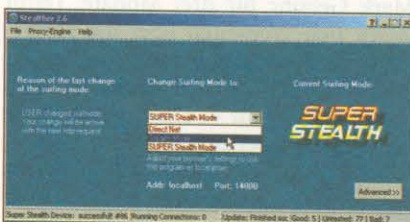
Der Cookie-Manager erlaubt das gezielte An- und Abschalten von gespeicherten Cookies.

Sicherheit (60%)	■ ■ ■ ■ ■
Bedienung (20%)	■ ■ ■ ■ ■
Funktionsumfang (20%)	■ ■ ■ ■ ■
Gesamterteil	MANGELHAFT

PHOTONO SOFTWARE

Stealthther 2.6

Als lokaler Proxy-Server für HTTP-Anfragen wird Stealthther nach der Installation im Browser eingetragen. Der Port 80 darf dabei nicht von einem anderen Dienst belegt sein, sonst reagiert das Programm mit einer Fehlermeldung. Das macht die ansonsten gute Bedienung zumindest bei der Installation etwas unkomfortabel. Stealthther leitet die HTTP-Anfrage an einen öffentlichen Proxy-Server und maskiert so die Weitergabe von IP-Adresse, Domain- und Host-Name. In einem Proxy-Manager können die verwendeten Server auf Geschwindigkeit und Anonymität getestet und Einträge gelöscht oder neue hinzugefügt werden. Cookies blockt das Programm ebenfalls. In einem Manager gibt der Benutzer zusätzliche Domains an, von denen Cookies akzeptiert werden. In der Experten-Registerkarte der Einstellungen wählt der Nutzer aus, nach welchem Kriterium die Auswahl des Proxy-Servers erfolgen soll. Am sichersten ist die zufällige Auswahl bei jedem Request. Aus Geschwindigkeitsgründen ist es sinnvoll, nur Server mit einer schnellen Antwortzeit zu wählen. Die kostenpflichtige Vollversion von Stealthther (www.stealthther.com) verschlüsselt im Super Stealth Mode den gesamten Datenverkehr über mehrere hintereinander geschaltete anonyme Super Stealth Nodes in Verbindung mit öffentlichen Proxies. Benutzer können entscheiden, ob sie Teil des Netzes werden wollen. Dadurch erreicht das Programm die zweitbeste Platzierung im Sicherheitstest. Stealthther kann auch als Proxy für das gesamte Netzwerk fungieren. Dazu muss der Anwender lediglich die IP-Adressen aller erlaubten Rechner unter *Settings* eingeben.



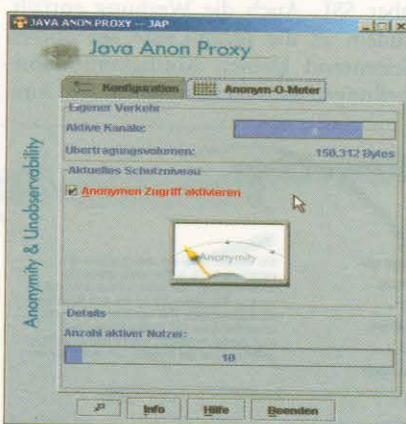
Verwendete Proxies lassen sich in einer Liste verwalten und auf ihre Geschwindigkeit überprüfen.



AUSSER KONKURRENZ

Java Anon Proxy

Das Projekt »Anonymität im Internet« der Deutschen Forschungsgesellschaft verbirgt sich hinter Java Anon Proxy (anon.inf.tu-dresden.de). Entwickelt wird an der TU Dresden. Die in Java programmierte Software wird als lokaler Proxy-Server in den Browser-Einstellungen eingetragen. Die Internet-Kommunikation (HTTP, HTTPS, FTP) läuft dann über einen von mehreren speziellen Java-Anon-Proxy-Servern, der Anfragen weiterleitet und für die Anonymisierung sorgt. Geplant ist das Implementieren einer so genannten Mix-Proxy-Kaskade über mindestens drei unabhängige Proxies. Diese sollen von unabhängigen Institutionen betrieben werden. Dadurch ist eine Weiterverfolgung der Daten zwischen Client und Webserver so gut wie unmöglich, da immer eine Station zwischengeschaltet ist, die nur den jeweils anderen Server kennt. Beteiligte Institutionen müssen eine Selbstverpflichtung unterzeichnen, weder Log-Files zu speichern noch Daten mit anderen Mix-Diensten auszutauschen. In der gegenwärtigen Version, die für jedes Java-fähige Betriebssystem vorliegt, ist der Mix allerdings noch nicht implementiert. Die Möglichkeiten des Programms sind aufgrund der Arbeitsweise noch gering, und es muss auf die Integration der Mix-Proxy-Kaskade gewartet werden. Darum wird Java Anon Proxy hier außer Konkurrenz getestet. Der Benutzer kann eine Liste von unterstützten Proxies herunterladen, eine Auswahl treffen oder einen manuellen Server eingeben. Die für die nahe Zukunft geplante Technik ist viel versprechend, aufgrund der fehlenden Umsetzung ist ein normaler Proxy-Manager mit Verbindung über anonyme Proxies aber zur Zeit die bessere Alternative. Cookies blockiert das Programm nicht.



Java Anon Proxy zeigt in einem Anonym-O-Meter das aktuelle Schutzniveau an.

TIPPS & TRICKS

Installationshilfe

Die Anonymizer lassen sich nicht so einfach installieren wie Standardapplikationen. Der Anwender muss zuerst einige Einstellungen im Browser verändern.

Einige der hier getesteten Programme wie Anonymity 2.52 oder Multiproxy 1.2 benötigen eine Änderung der Proxy-Einstellungen. PCpro beschreibt, was genau bei der Installation für die Browser Netscape, IE und Opera zu beachten ist.

Internet Explorer

Öffnen Sie das Menü *Extras/Internetoptionen*. Wählen Sie dort die Registerkarte *Verbindungen*. Klicken Sie in der Liste der DFÜ-Einstellungen auf die Verbindung, die Sie verwenden möchten. Wenn Sie unterschiedliche Verbindungen zum Zugang ins Internet benutzen, sollten Sie die Proxy-Einstellungen für die anderen Verbindungen ebenfalls ändern. Klicken Sie anschließend auf *Einstellungen*. Im Bereich *Proxyserver* wählen Sie *Proxyserver verwenden* und klicken dann auf *Erweitert*.

Im folgenden Einstellungsmenü geben Sie für jeden Verbindungstyp die Adresse und die Port-Nummer ein. Programme wie Anonymity 2.52 oder Multiproxy 1.2 benötigen die Adresse des lokalen Rechners (entweder 127.0.0.1 oder localhost) sowie die jeweilige Port-Nummer.

Wenn Sie einen bestimmten anonymen Proxy im Internet verwenden möchten, können Sie die Adresse auch direkt eintragen. Die Verbindung erfolgt dann ausschließlich über diesen Proxy-Server.

Netscape 6

Öffnen Sie mit *Bearbeiten/Einstellungen* das Einstellungsfenster. Klicken Sie darin auf den Bereich *Erweitert* und dann auf *Proxies*. Tragen Sie hier 127.0.0.1 und die Port-Nummer des verwendeten Programms ein. Einige Programme unterstützen nur HTTP, die anderen Protokolle sollten Sie in diesem Fall frei lassen. Wahlweise können Sie auch den Namen eines anonymen Proxy-Servers eintragen, wenn Sie keine spezielle Software verwenden.

Opera

Öffnen Sie mit *Datei/Einstellungen* das Einstellungs-menü. Wählen Sie den Eintrag *Verbindungen* und klicken Sie dort auf *Proxy-Server*. Geben Sie hier die jeweilige Adresse oder 127.0.0.1 für ihren Rechner sowie die korrekte Port-Nummer ein.

ANONYMIZER

Laborergebnisse

Das PCpro-Labor testet alle Anonymisierer mit eigens in Java programmierten dynamischen Webseiten. Die Tests finden unter Verwendung unterschiedlicher Internet-Zugänge und im LAN statt.

Um die Anonymisierungsfunktionen der Programme ausführlich zu testen, wird im PCpro-Labor ein Webserver unter Windows 2000 Server aufgesetzt. So können alle während den Internet-Sitzungen bei Betriebssystem und Browser aus- und eingehenden Daten protokolliert werden. Die Ergebnisse lassen sich auf alle Windows-Versionen übertragen. Über Webseiten, die die Tester mit Java-Server-Pages programmierten, werden alle Informationen über die überwachten Clients angefordert, die sich mit dem Server verbinden. Dazu gehören sensible Daten wie Rechner- und Servername, IP-Adresse sowie der User-Agent. Eine weitere im Labor erstellte Test-Website versucht wiederholt, Cookies zu setzen, diese zu übertragen, auszulesen und auf die Festplatte der mit den Anonymizern versehenen Rechner zu schreiben. Als Client verwenden die PCpro-Tester zuerst einen Computer unter Windows 2000, der sich über eine ISDN- und eine Internet-by-Call-Verbindung in das Internet einwählt. Von dort rufen die Tester die Websites auf dem PCpro-Labor-Server auf.

Als zweiter Test-Client dient ein Rechner unter Windows 2000 Server, der über ein LAN und T-DSL mit dem Internet verbunden ist. So untersuchen die Tester zusätzlich über Netzwerkmonitor die übertragenen Daten sowie die angeforderten Verbindungen und Server. Damit wird überprüft, ob bei den Testprogrammen wirklich alle Daten den Rechner verschlüsselt verlassen. Die Adressen der angesteuerten Rechner zeigen auf, ob noch zusätzliche Verbindungen – beispielsweise zum Hersteller – aufgebaut werden. Auf diese Weise kann auch das Verhalten von PCs überprüft werden, die über ein lokales Netzwerk eine Verbindung in das Internet aufbauen.

Installation

Unproblematisch gestaltet sich die Installation bei fast allen Programmen. Lediglich Secretmaker verfügt über keine Installationsroutine und verwendet einfach die aufgerufene Datei. Wird das Programm per CD aufgerufen und diese danach entfernt, lässt sich Secretmaker nach dem nächsten Booten nicht mehr starten. Freedom Platinum benötigt ein zweimaliges Re-Booten, bevor das Programm die Internet-Verbindung erkennt. Auf dem Testrechner mit T-DSL läuft Freedom nicht, da laut Herstellerangaben nur DFÜ-Wahlzugang und TCP-/IP-

Verbindungen unterstützt werden.

Bei Programmen, die Verbindungen über anonyme Proxy-Server herstellen, hängt die Qualität und Geschwindigkeit hauptsächlich von der Aktualität der Proxy-Listen ab. Im Test kann über die mitgelieferte Auswahl von Multiproxy zum Testzeitpunkt kein einziger Server erreicht werden. Für wenig versierte Nutzer ist dieses Programm damit nicht zu gebrauchen. Hervorragend löst Stealther das Problem: Mit einer Menüfunktion kann eine aktuelle Proxy-Liste vom Hersteller angefordert werden. Diese importiert das Programm dann automatisch.

Anonymität

Gewaltig variieren die Anonymitätsfunktionen im Test. Java Anon Proxy und Multiproxy maskieren jeweils nur IP-Adresse und Rechnername, lassen aber das Setzen und Lesen von Cookies uneingeschränkt zu. Sogar einen Totalausfall leistet sich Secretmaker, das als einziges Programm im Test die IP-Adresse unverändert weitergibt. Zudem blockiert der integrierte Manager lediglich das Lesen und Schreiben von Cookies. Vom Server gesendete Daten lässt das Programm trotzdem durch, sodass während einer Session ein Identifizieren möglich ist. Alle anderen Programme im Test blockieren die Java-Applets konsequent. Bei einigen Websites sind Cookies allerdings notwendig, soll die Site in vollem Umfang genutzt werden. Stealther glänzt in diesem Punkt mit

Cookie-Control, wodurch auch ein selektives Lesen, Schreiben und Setzen von Cookies möglich ist.

Datenverschlüsselung über mehrere Server unterstützen lediglich Stealther und Freedom. Freedom überlässt deren Auswahl dem Benutzer – als zweiter und dritter Knotenpunkt sind im Test allerdings nur zwei bis drei Einträge vorhanden. Stealther sendet die Daten bei jeder Anfrage über unterschiedliche, hintereinander geschaltete Server.

Surfverhalten

Leicht beeinträchtigt wird aus nachvollziehbaren Gründen bei allen Programmen die Surfgeschwindigkeit. Einzige Ausnahme ist Secretmaker. Eine realitätsnahe Geschwindigkeitsmessung ist im Vergleich allerdings nicht möglich, denn die Performance ist abhängig vom ISP, den verwendeten Proxy-Servern und dem aktuellen Internet-Verkehr. Diese Faktoren lassen sich im Testlabor nicht kontrollieren. Bei verschlüsselten Datenübertragungen ist der Geschwindigkeitseinbruch am deutlichsten messbar. Freedom erreicht im Test trotzdem regelmäßig konstante, zufrieden stellende Performance. Die Wartezeiten im Super Stealth Mode von Stealther veranlasst die PCpro-Tester hingegen teilweise zum Herunterschalten in den normalen Tarnmodus von Stealther. Eine Performance-steigernde Möglichkeit stellt das Einschränken der verwendeten Proxy-Server mit einer bestimmten minimalen Antwortzeit dar.

Marco Zierl/OPU

Add	Port	Last test	Working	Anonymous	Speed
211.61.250.240	80	17.07.2001 17:2	Yes	YES	00:00:01
195.101.182.50	80	17.07.2001 17:2	Yes	YES	00:00:02
195.163.2.83	80	17.07.2001 17:2	Yes	YES	00:00:02
195.31.167.2	80	17.07.2001 17:2	Yes	YES	00:00:02
212.4.0.12	3128	17.07.2001 17:2	Yes	YES	00:00:02
www.kit.com	8080	17.07.2001 17:2	Yes	YES	00:00:02
mail.hrvn.net	80	17.07.2001 17:2	Yes	YES	00:00:02
mail.hrvn.net	80	17.07.2001 17:2	Yes	YES	00:00:02
195.215.134.225	80	17.07.2001 17:2	Yes	YES	00:00:03
211.117.28.36	80	17.07.2001 17:2	Yes	NO	00:00:03
www.kit.com	3128	17.07.2001 17:2	Yes	NO	00:00:03
www.kit.com	80	17.07.2001 17:2	Yes	YES	00:00:03

Programme wie Stealther 2.6 oder auch Freedom 2.2 erlauben die Auswahl der Proxy-Server.



AUSSTATTUNG

Programm Hersteller	Anonymity 2.52 Inetprivacy Software	Freedom 2.2 Zero Knowledge	Multiproxy 1.2 Multiproxy	Secretmaker 1.62 Secretmaker	Stealthier 2.6 Photon-Software	Java Anon Proxy TU Dresden
Gesamtwert	gut	sehr gut	ausreichend	mangelhaft	sehr gut	außer Konkurrenz
Preis	35 Dollar (privat), 65 Dollar (kommerziell)	60 Dollar	Freeware	60 Mark jährlich	80 Mark	Freeware
Internet	www.inetprivacy.com	www.freedom.net	www.multiproxy.org	www.secretmaker.com	www.stealthier.com	anon.inf.tu-dresden.de
Info	support@inetprivacy.com	support@freedom.net	mike@multiproxy.org	secretmaker.support@secretmaker.com	thorsten@photon-software.de	jap@inf.tu-dresden.de
Unterstützte Protokolle						
HTTP	●	●	●	●	●	●
HTTPS (secure HTTP)	●	●	●	○	○	●
FTP	●	●	●	○	○	●
Sicherheits-Grundfunktionen						
Blockieren der IP-Adresse	●	●	●	○	●	●
Blockieren des Host-Namens	●	●	●	●	●	●
Blockieren von neuen Cookies	●	●	○	●	●	○
Löschen existierender Cookies	●	●	○	●	●	○
Blockieren von Session-Cookies	●	●	○	○	●	○
Verändern/Blockieren User-Agent	●	○	○	○	○	○
Automatischer Server-Wechsel möglich	●	○	●	○	●	○ (Mix-Kaskade)
Verwendung ausschließlich anonymer Proxy-Server	●	○ (Freedom Network)	●	○	●	○
Hintereinanderschalten mehrerer Server	○	● bis zu drei	○	○	●	○
Verschlüsselte Datenübertragung	○	●	○	○	●	○
Mischen anonymer Server und verschlüsselter Server	○	○	○	○	●	○
Zusatzfunktionen						
Cookie-Manager	○	●	○	●	●	○
Proxy-Manager hinzufügen, löschen, importieren	●	● (Freedom Network)	●	○	●	○
Proxy-Geschwindigkeits-Test	●	○	●	○	●	○
Proxy-Anonymitätstest	●	○	●	○	●	●
Als Proxy-Server im LAN einsetzbar	●	○	●	○	●	●
Proxy-Port wählbar	●	○	●	○	○	●
Browservariablen direkt veränderbar	●	○	○	●	○	○
Umschalten direkte Verbindung/ sichere Verbindung	●	●	○	●	●	●
Zusatzfeatures	Favoriten-Liste in der System-Tray mit direkter Umschaltmöglichkeit zu bestimmten Proxies	Form Filler, Login-Manager, Personal Firewall, E-Mail-Verschlüsselung, AD-Manager, Verschlüsseln von News, IRC, Telnet, Blockieren von Spam, Keyword-Warnung beim Übertragen von persönlichen Daten			automatischer Download, neuester Proxy-Server	

● = ja ○ = nein

LAB NOTES

Anonymität
ist ein Grundrecht

Während die einen eine ausgeprägte Paranoia an den Tag legen, an der sich hervorragend verdienen lässt, denken andere, wer nichts zu verbergen hat, könne auf Anonymität im Netz verzichten. »Das Recht auf informationelle Selbstbestimmung schützt davor, aus dem Bereich

der Anonymität in den einer persönlichen Bekanntheit gerückt zu werden«, entschied allerdings schon 1994 der Bundesgerichtshof. Anonymität im Internet ist also ein Grundrecht. Liefen 1987 Bürger noch Sturm gegen die Volkszählung, hinterlassen heute viele Nutzer völlig sorglos weit sensible Daten für ein Internet-Preisausschreiben. Aber gerade in einem weltweiten Computer-Netz möchte ich gewährleisten

sehen, dass nicht jeder auf meine-Daten zugreifen kann. Hier können Anonymizer gute Dienste leisten. Jeder Internet-Nutzer kann sich so aktiv um seine informationelle Selbstbestimmung kümmern. Doch auch passiv muss sie gewährleistet sein: Wer bei Preisausschreiben seine Daten abgibt oder sich lautstark in News-Foren äußert, darf sich später nicht wundern, wenn er Spam-Mails erhält.



Olaf Pursche, PCpro-Redaktion: »Anonymizer gehören nicht in die Schmutzdecke.«